UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Sede amministrativa: Universitá degli studi di Padova

Dipartimento di Matematica

Scuola di Dottorato in Scienze Matematiche

Curriculum Matematica

Ciclo XXIX

SOME PROPERTIES OF ZETA FUNCTIONS ASSOCIATED TO PROFINITE GROUPS

Direttore della Scuola: Cm.mo Prof. Pierpaolo Soravia

Coordinatore d'indirizzo: Ch.mo Prof. Franco Cardin

Supervisore: Ch.mo Prof. Andrea Lucchini

Dottorando: Leone Cesare Cimetta

Contents

Abstract

Consider a profinite group containing only finitely many open subgroups of index n, for any n: then it is possible to define two formal Dirichlet series associated to the group, the normal subgroup zeta function and the normal probabilistic zeta function.
First, we deal with the problem of the absolute convergence of the latter, then we examine the profinite groups in which these series coincide, and 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.
This evidence gives us sufficient motivation to focus on finitely generated pro-p groups, as classifying normally ζ-reversible pro-p groups is the key to determine a classification of pronilpotent groups with this property: we show that normally ζ-reversible uniform pro-p groups (where p is an odd prime) are abelian and torsion-free.
Later on, we use an explicit classification of analytic p-adic pro-p groups of small dimension and a formula for their subgroup zeta function to prove that a conjecture by Damian and Lucchini holds for these groups.
Finally, we present some experimental results, obtained using the software GAP, concerning the behaviour (and in particular the distibution of the real zeros) of the probabilistic zeta function of finite groups.

Chapter 1

Bibliographic references and motivations

In this thesis we shall discuss the properties of four Dirichlet series associated to a finitely generated profinite group G. These series deal with two important problems arised in the last century, which both had a great development in the last decades: the subgroup growth of a profinite group and the probability of selecting a generating set randomly choosing a given number of elements of the group.

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 $\{a_n(G)\}_n$ the sequence counting the number of open subgroups of index n in G, and by $\zeta_G(s)$ the Dirichlet series associated with this sequence. Thus

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

where s is a complex variable. The study of the subgroup sequence $\{a_n(G)\}_n$ and the corresponding subgroup zeta function $\zeta_G(s)$ started with [25] and 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.

Another sequence of integers can be associated to G: considering the Möbius function $\mu(\cdot, G)$ of the lattice of open subgroups of G defined recursively by $\mu(G,G) = 1$ and $\sum_{H\leq K\leq_O G} \mu(K,G) = 0$ for any proper open subgroup $H <_O G$, we can set $b_n(G) = \sum_{|G:H|=n,\ H\leq_O G} \mu(H,G)$. Again we can consider the corresponding Dirichlet generating function

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

Important results on the Möbius function in a lattice $\mathcal{L}$ like Crapo's closure theorem (see for example [9]) allows us to state that $\mu(H,G) \neq 0$ only if H is intersection of maximal elements in $\mathcal{L}$: so, if we consider instead of $\mathcal{L}$ the lattice $\mathcal{L}^*$ composed by G and the intersections of maximal elements in $\mathcal{L}$, we get the same μ and thus the same $p_G(s)$. In particular, as the Frattini subgroup $\Phi(G)$ is the intersection of all maximal subgroups of G, we get $\mu(H,G) = \mu(H/\Phi(G), G/\Phi(G))$, so $p_G(s) = p_{G/\Phi(G)}(s)$.
The formal inverse of $p_G(s)$ is the probabilistic zeta function which was first introduced and studied by A. Mann in [38] for finitely generated profinite groups and by N. Boston in [4] in the case of finite groups.
If G is a finite group and t is a positive integer, $p_G(t)$ has an important probabilistic meaning: P. Hall proved in [27] that, in this case, $p_G(t)$ is equal to the probability that t random elements of G generate G.

Theorem 1. [27, Section 2.1] Let G be a finite group and $t \in \mathbb{N}$. Then $p_G(t)$ is equal to the probability that t randomly chosen elements of G generate G.

Proof. Let $H \leq G$ and $\Phi_H(t)$ be the number of ordered t-uples $(x_1, \cdots, x_t) \in H^t$ generating H. Then the functions

$$f : \mathcal{L} \to \mathbb{N} \quad \text{mapping} \quad H \mapsto \Phi_H(t)$$

and

$$F : \mathcal{L} \to \mathbb{N} \quad \text{mapping} \quad K \mapsto |K|^t$$

satisfy

$$F(K) = \sum_{H \leq K \leq G} f(H)$$

whence, by Möbius inversion formula, we get

$$f(K) = \sum_{H \leq K \leq G} \mu(H,K) F(H).$$

In particular, for $K = G$ we have

$$\Phi_G(t) = \sum_{H \leq G} \mu(H,G) |H|^t,$$

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

□

Using this probabilistic meaning, it is quite easy to compute $p_G(t)$ for many classes of finite groups.

Theorem 2. Let G be a p-group and $d(G) = d$. Then

$$p_G(t) = \prod_{j=0}^{d-1} \left(1 - p^{j-t}\right).$$

Proof. We already know that

$$p_G(t) = p_{G/\Phi(G)}(t) = p_{C_p^d}(t).$$

We can now identify the t-uples in C_p^d which generate C_p^d with matrices in $M_{d\times t}$ of rank d: counting them is equivalent to count linearly independent d-uples in C_p^t, so

$$\Phi_{C_p^d}(t) = \left(p^t - 1\right)\left(p^t - p\right)\cdots\left(p^t - p^{d-1}\right) = \prod_{j=0}^{d-1}\left(p^t - p^j\right),$$

$$p_G(t) = p_{C_p^d}(t) = \frac{\Phi_{C_p^d}(t)}{p^{td}} = \prod_{j=0}^{d-1}\left(1 - p^{j-t}\right).$$

□

It is possible to find in literature important results stating it is possible to express the Dirichlet polynomial $p_G(s)$associated to a finite direct product of finite non-abelian simple groups from the Dirichlet polynomials associated to the simple groups:

Theorem 3. [4, Section 3] Let S be a finite non-abelian simple group, then

$$p_{S^t}(s) = \prod_{i=0}^{t-1}\left(p_S(s) - \frac{i|\operatorname{Aut}(S)|}{|S|^s}\right).$$

Theorem 4. [5, Proposition 1] Let G_1, G_2 be finite groups with no common composition factors, then

$$p_{G_1\times G_2}(s) = p_{G_1}(s)p_{G_2}(s).$$

Motivated by the results for finite groups, A. Mann stated in [38] a conjecture which implies that $p_G(s)$ has a similar probabilistic meaning for a wide class of profinite groups. Precisely, let t be a positive integer, let ν be the normalised Haar measure uniquely defined on the profinite group G^t. Consider the set $\Omega_G(t)$ of generating t-uples in G (in the topological sense), then $\Omega_G(t)$ is the complement in G^t of the open subset $\bigcup_{H<_O G} H^t$, so it is closed and hence measurable. We can thus define $\mathrm{Prob}_G(t) = \nu(\Omega_G(t))$, the probability that a t-uple in G generates G itself. We say that G is positively finitely generated (PFG) if there exists a positive integer t such that $\mathrm{Prob}_G(t) > 0$.
Mann considered the infinite sum

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

As it stands, this is not well defined, but he conjectured that this sum is absolutely convergent if G is positively finitely generated. If this occurs, then

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 PFG, 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. A. Lucchini proved in [37] that Mann's conjecture holds if G is a profinite group with polynomial subgroup growth.

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, E. Detomi and A. Lucchini proved in [15] that a finitely generated profinite group G is prosoluble if and only if the sequence $\{b_n(G)\}$ is multiplicative (i.e. $b_n(G)b_m(G) = b_{nm}(G)$ whenever $(n, m) = 1$).

Although computing $\zeta_G(s)$ and $p_G(s)$ is in general a hard issue, there are some cases in which it is quite easy. 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 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 now what is the relation between $\zeta_G(s)$ and $p_G(s)$ and, in particular, which profinite groups G share with $\widehat{\mathbb{Z}}$ the property that $\zeta_G(s)$ is the multiplicative inverse of $p_G(s)$. Motivated by this question, E. Damian and A. Lucchini introduced in [10] the notion of ζ-reversible profinite groups.

Definition 5. 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 [10] 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 [10] 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.

The aim of this thesis is to study a property concerning two slightly differently defined Dirichlet series: as the coefficients of both Dirichlet series are defined from the lattice of all open subgroups of G, it seems natural to ask what is the result if we consider a sublattice of this lattice. In response to this question, E. Detomi and A. Lucchini introduced in [16] some generalizations of the subgroup and the probabilistic zeta functions, in particular they considered the lattice of all open normal subgroups of G.
Let G be a profinite group with the property that for each positive integer n, G contains only finitely many open normal subgroups of index n. For any $n \in \mathbb{N}$ we can denote by $a_n^{\triangleleft}(G)$ the number of open normal subgroups of G; moreover, we can define a Möbius function $\mu^{\triangleleft}(\cdot, G)$ in the lattice of the open normal subgroups of G and thus define the coefficients $b_n^{\triangleleft}(G) = \sum_{|G:H|=n, H \trianglelefteq_O G} \mu^{\triangleleft}(H, G)$. Again the

properties of the sequences $\{a_n^{\lhd}(G)\}_{n\in\mathbb{N}}$ and $\{b_n^{\lhd}(G)\}_{n\in\mathbb{N}}$ can be encoded by the corresponding Dirichlet generating functions

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

called, respectively, the normal subgroup zeta function and the inverse of the normal probabilistic zeta function of G. Many properties of $\zeta_G(s)$ and $p_G(s)$ can be easily extended to $\zeta_G^{\lhd}(s)$ and $p_G^{\lhd}(s)$. Let $\mathcal{N}(G)$ be the intersection of all maximal normal subgroups of G: if $N \trianglelefteq_O G$, then $\mu^{\lhd}(N,G) \neq 0$ only if $\mathcal{N}(G) \leq N$, moreover $\mu^{\lhd}(N,G) = \mu^{\lhd}(N/\mathcal{N}(G), G/\mathcal{N}(G))$. In particular, $p_G^{\lhd}(s) = p_{G/\mathcal{N}(G)}^{\lhd}(s)$. Again $p_G^{\lhd}(s)$ has a probabilistic meaning: if G is a finite group and $t \in \mathbb{N}$, then $p_G^{\lhd}(t)$ is the probability that t randomly chosen elements of G normally generate G, i.e. they generate a subgroup whose normal closure is G (see [16, Section 3]). Moreover, Detomi and Lucchini determined in [16] an useful factorization of $p_G^{\lhd}(s)$ for finite G.

Theorem 6. [16, Proposition 3.1] Let G be a finite group and let

$$G/\mathcal{N}(G) \cong \prod_{i=1}^{m} S_i^{n_i}$$

where S_i are non-isomorphic simple groups. Then

$$p_G^{\lhd}(t) = \prod_{i=1}^{m} p_{S_i^{n_i}}^{\lhd}(t).$$

Moreover, for a simple group S,

$$p_{S_i^{n_i}}^{\lhd} = \begin{cases} (1-1/|S|^t)^{n_i} & \text{if S is not abelian;} \\ \prod_{j=1}^{n_i}(1-p^{j-1}/p^t) & \text{if S is abelian of order p.} \end{cases}$$

Proof. We can assume without loss of generality that $\mathcal{N}(G) = 1$, so that $G = \prod_{i=1}^{m} S_i^{n_i}$. Let π_i be the natural projection of G onto $S_i^{n_i}$, then a t-uple $(x_i, \cdots, x_t) \in G^t$ normally generates G if and only if $(\pi_i(x_1), \cdots, \pi_i(x_t))$ normally generates $S_i^{n_i}$ for each i. Then, if we call $\Phi_G^{\lhd}(t)$ the number of t-uples which normally generate G, we get

$$\Phi_G^{\lhd}(t) = \prod_{i=1}^{m} \Phi_{S_i^{n_i}}^{\lhd}(t)$$

and dividing by $|G|^t = \prod_{i=1}^{m} |S_i^{n_i}|^t$ we have

$$p_G^{\lhd}(t) = \prod_{i=1}^{m} p_{S_i^{n_i}}^{\lhd}(t).$$

If $S \cong C_p$, then

$$p_{S^n}^{\lhd}(t) = p_{S^n}(t) = \prod_{i=1}^{n} \left(1 - \frac{p^{i-1}}{p^t}\right)$$

by Theorem 2. If S is a simple non-abelian, let $S^n = S_1 \times \cdots \times S_n$ and let ρ_i be the projection of S^n onto S_i: then a t-uple $(y_1, \cdots, y_t)$ normally generates S^n if and only if

$$\langle \rho_i(y_1), \cdots, \rho_i(y_t) \rangle \neq 1$$

for every i, hence

$$p^{\triangleleft}_{S^n}(t) = \left(1 - \frac{1}{|S|^t}\right)^n.$$

□

In [16, Section 4] the definitions and properties of $\zeta_G(s)$ and $p_G(s)$ for profinite groups, introduced by Mann in [38], are extended to $\zeta^{\triangleleft}_G(s)$ and $p^{\triangleleft}_G(s)$. From now on assume that G is a profinite group such that $a^{\triangleleft}_n(G)$ is finite for every $n \in \mathbb{N}$, so that we can always define the two formal series $\zeta^{\triangleleft}_G(\cdot)$ and $p^{\triangleleft}_G(\cdot)$. Notice that, while finite generation of G is a sufficient condition to assure G has only a finite number of subgroups of index n for every $n \in \mathbb{N}$, here it is not possible to generalize this result with the condition that G is normally finitely generated. For example, $(\mathrm{Alt}(5))^{\aleph_0}$ is normally finitely generated (by the elements of the diagonal), but has an infinite number of open normal subgroups of index 60. As it is stated in [16, Section 4], a sufficient (but not necessary) condition to ensure the finiteness of $a^{\triangleleft}_n(G)$ for every n is that G is topologically finitely generated.

Again, let t be a positive integer and ν be the normalised Haar measure uniquely defined on the profinite group G^t; consider the set $\Omega^{\triangleleft}_G(t)$ of normally generating t-uples in G (in the topological sense). Then we define $\mathrm{Prob}^{\triangleleft}_G(t) = \nu(\Omega^{\triangleleft}_G(t))$, the probability that a t-uple in G normally generates G itself. We say that G is positively finitely normally generated (PFNG) if there exists a positive integer t such that $\mathrm{Prob}^{\triangleleft}_G(t) > 0$. It is easy to see that a group can be normally finitely generated even if $\mathrm{Prob}^{\triangleleft}_G(t) = 0$ for every $t \in \mathbb{N}$. For example, as we have already seen $(\mathrm{Alt}(5))^{\aleph_0}$ is normally finitely generated but it is simple to prove that

$$\mathrm{Prob}^{\triangleleft}_G(t) \leq \inf_n \mathrm{Prob}^{\triangleleft}_{(\mathrm{Alt}(5))^n}(t) = \lim_n \left(1 - \frac{1}{60^t}\right)^n = 0$$

for every $t \in \mathbb{N}$.
Let $m^{\triangleleft}_n(G)$ be the number of open maximal subgroups of G with index n. Moreover, for any simple group S, define $\gamma_G(S)$ to be the maximal integer n, if it exists, such that the direct product S^n is an epimorphic image of G; otherwise set $\gamma_G(S) = \infty$. In [16] the authors prove that, if G is a PFNG group, then $\gamma_G(S)$ is finite for every simple group G and $m^{\triangleleft}_n(G)$ is finite for every integer n. Moreover, generalizing a result by A. Mann and A. Shalev, they prove that a profinite group is PFNG is and only if has polynomial normal maximal subgroup growth, i.e. the sequence $\{m^{\triangleleft}_n(G)\}$ is polynomially bounded.

If a group is PFNG, then $\mathrm{Prob}^{\triangleleft}_G(t)$ admits an useful factorisation.

Theorem 7. [16, Proposition 4.1] A profinite group G is PFNG if and only if the sequence $\{m^{\triangleleft}_n(G)\}$ is polynomially bounded. Moreover, if G is PFNG then

the infinite products

$$A(G,s) = \prod_{p \text{ prime}} \prod_{i=1}^{\gamma_G(C_p)} \left(1 - \frac{p^{i-1}}{p^s}\right),$$

$$B(G,s) = \prod_{S \text{ non-abelian}} \left(1 - \frac{1}{|S|^s}\right)^{\gamma_G(S)}$$

are absolutely convergent in some right half plane of the complex plane and

$$\mathrm{Prob}_G^{\triangleleft}(t) = A(G,t)B(G,t)$$

for large integer t.

Looking for sufficient conditions for a group to be PFNG, the authors proved in [16, Lemma 4.1] that the free profinite group on d generators is positively normally $d+1$-generated, so in particular every finitely generated profinite group is PFNG. In this class of profinite groups it is possibile to finally extend the probabilistic meaning of $p_G^{\triangleleft}(s)$ we proved for finite groups.

Theorem 8. [16, Proposition 5.1] If G is PFNG, then $p_G^{\triangleleft}(s)$ is absolutely convergent in some complex half plane and $p_G^{\triangleleft}(s) = A(G,s)B(G,s)$. In particular, $p_G^{\triangleleft}(t) = \mathrm{Prob}_G^{\triangleleft}(t)$ when the integer t is large enough.

Finally, the last result in [16] characterize the groups such that the probabilistic and the normal probabilistic zeta functions coincide.

Theorem 9. [16, Proposition 5.3] The group G is pronilpotent if and only if $p_G^{\triangleleft}(s) = p_G(s)$.

We are now ready to define the property we are going to discuss in the main part of the thesis, generalizing the definition of ζ-reversible profinite groups given in [10].

Definition 10. A profinite group G is normally ζ-reversible if $\zeta_G^{\triangleleft}(s)p_G^{\triangleleft}(s) = 1$.

We conjecture that a profinite group is normally ζ-reversible if and only if it is abelian and torsion-free.

After presenting some ausiliary results in the following chapter, we will deal with the problem of the absolute convergence of $p_G^{\triangleleft}(s)$ in the first section of the third chapter, in order to improve the result in Theorem 8.
In the following sections of the third chapter we will try to give evidence to a weaker conjecture, stating that a normally ζ-reversible profinite group is pronilpotent.
An evidence for this weaker conjecture will be given by the following theorem.

Theorem 11. 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 nonabelian simple group, then G is pronilpotent. In particular, any prosoluble normally ζ-reversible profinite group is pronilpotent.

The main results we will prove in the third chapter are the following:

Theorem 12. A non trivial normally ζ-reversible profinite group cannot be perfect.

Theorem 13. 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 51): suppose that a normally ζ-reversible profinite group G admits a finite nonabelian 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.

The evidence we present in the third chapter gives us sufficient motivation to focus on finitely generated pro-p groups, as classifying normally ζ-reversible pro-p groups is the key to determine a classification of pronilpotent groups with this property: motivated by some interesting results in [10], in the forth chapter we will extend to normally ζ-reversible groups some of the results contained in that paper. Moreover, by proving the following theorem we will show that, in the class of uniform pro-p groups (where p is an odd prime) our stronger conjecture holds.

Theorem 14. Let G be a uniform pro-p group for an odd prime p, then G is normally ζ-reversible if and only if $G \cong \mathbb{Z}_p^n$ for some integer n.

In the third section of the forth chapter we will use an explicit classification of analytic p-adic pro-p groups of small dimension (provided by J. González-Sánchez and B. Klopsh in [23]) and a formula for their subgroup zeta function (given by B. Klopsh and C. Voll in [33]) to prove that the main conjecture in [10] holds for these groups. The main result in this section is the following:

Proposition 15. Let G be a finitely generated torsion-free pro-p group, with $\dim(G) \leq 3$. Then G is ζ-reversible if and only if $d(G) = d(H)$ for all $H \leq_O G$.

Finally, in the fifth chapter we will enlist and try to classify some properties of the probabilistic zeta function of finite simple groups of small order.

Chapter 2

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:

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

where $a_n^* = a_n$ if n is a π-number, $a_n^* = 0$ otherwise. It is easy to see that this is indeed an endomorphism: it clearly respects the sums; moreover, let $\sum \frac{\gamma_i}{i^s}$ be the convolution product of $\sum \frac{\alpha_i}{i^s}$ and $\sum \frac{\beta_i}{i^s}$.
Suppose $n \notin \pi$, then $\gamma_n^* = 0 = \sum_{d|n} \alpha_d^* \beta_{n/d}^*$, as at least one among $d, n/d$ is not a π-number. Conversely, if $n \in \pi$, then $d, n/d \in \pi$ for all possible $d|n$, so $\gamma_n^* = \gamma_n = \sum_{d|n} \alpha_d \beta_{n/d} = \sum_{d|n} \alpha_d^* \beta_{n/d}^*$.

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 $F(s)^{-1}$ is multiplicative.

We will need two more results on Dirichlet series:

Proposition 16. [Reference: P. Clark, Theorem 7] Let $f(s) = \sum_{n\in\mathbb{N}} \frac{f_n}{n^s}$ be a Dirichlet series which is absolutely convergent in the complex right halfplane $\mathcal{R}(s) > \sigma_0$. Suppose there is an infinite sequence $\{s_k\}$ of complex numbers, such

that $\sigma_k := \mathcal{R}(s_k) > \sigma_0$, $\sigma_k \to \infty$ and $f(s_k) = 0$ for any k. Then $f_n = 0$ for all $n \in \mathbb{N}$.

Proof. Suppose by contradiction that $f_n \neq 0$ for some $n \in \mathbb{N}$, let N be the least of such n. Then

$$f(s) = \frac{f_N}{N^s} + \sum_{n=N+1}^{\infty} \frac{f_n}{n^s},$$

$$f_N = N^s f(s) - N^s \sum_{n=N+1}^{\infty} \frac{f_n}{n^s}.$$

If we take $s = s_k$ for any $k \in \mathbb{Z}^+$, we get

$$f_N = -N^{s_k} \sum_{n=N+1}^{\infty} \frac{f_n}{n^{s_k}}.$$

Fix $\sigma > \sigma_0$, choose k such that $\sigma_k > \sigma$. Then $\sum_{n=N+1}^{\infty} |f_n| n^{-\sigma} < \infty$ as the series is absolutely convergent for $\mathcal{R}(s) > \sigma_0$, in particular

$$|f_N| \leq N^{\sigma_K} \sum_{n=N+1}^{\infty} |f_n| n^{-\sigma_k} \leq \frac{N^{\sigma_k}}{(N+1)^{\sigma_k - \sigma}} \sum_{n=N+1}^{\infty} |f_n| n^{-\sigma} \leq C \left(\frac{N}{N+1} \right)^{\sigma_k}$$

for some constant C independent from n, k. As N is a constant, letting $\sigma_k \to \infty$ the right hand side tends to 0, so $f_N = 0$, a contradiction. □

Corollary 17. [Reference: P. Clark, Corollary 8] Let $f(s) = \sum_{n \in \mathbb{N}} \frac{f_n}{n^s}$ be a Dirichlet series which is absolutely convergent in the complex right halfplane $\mathcal{R}(s) > \sigma_0$. Suppose that for some s with $\mathcal{R}(s) > \sigma_0$ we have $f(s) \neq 0$. Then there exists a right halfplane in which $f(s)$ is absolutely convergent and never 0.

Proof. If such a halfplane did not exist, we would have an infinite sequence $\{s_k\}$ of complex numbers, with real parts tending to infinity, such that $f(s_k) = 0$ for all k. By Proposition 16 this implies that $f_n = 0$ for all n, a contradiction. □

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

Lemma 18. 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 [42], stating that, if $n \geq 25$, then there is a prime p such that $n \leq p \leq 6n/5$.

Definition 19. Given a perfect group G, there exists a unique perfect group F, called the universal central extension of G, and a unique surjective morphism $f : F \to G$ such that

$$\ker(f) \leq \mathrm{Z}(F) \tag{2.1}$$

and that f is universal with Property (2.1). The kernel of such a f is called the Schur multiplier of G and is denoted by $M(G)$. Moreover, the Schur multiplier of a finite group is finite too.

We will need some bounds to the order of modules.

Theorem 20 (Palfy-Wolf's Theorem)**.** [55, Theorem 1.6] Let V be a nontrivial faithful, completely reducible $\mathbb{F}(G)$ module for a nilpotent group G and a field $\mathbb{F}$ of nonzero characteristic. Then

$$|G| \leq \frac{|V|^{\beta}}{2} \quad \text{for} \quad \beta = \frac{\ln(32)}{\ln(9)}$$

.

Lemma 21. [52, Theorem 1.1] A_n for $n > 8$ has exactly one faithfut irreducible representation of minimal degree on a field of characteristic 2; such degree is $n-2$ if n is even, it is $n-1$ otherwise.

Lemma 22. [53, Theorem 1.1] A_n for $n > 6$ has exactly one faithfut irreducible representation of minimal degree on a field of characteristic $p > 2$; such degree is $n-2$ if $p|2$, it is $n-1$ otherwise.

We will also need this classic result on transitive permutation groups:

Lemma 23. The center of a transitive permutation group is semiregular.

Proof. Let $G \leq S_t$ transitive, $\pi \in G$, $\sigma \in Z(G)$: notice that, given a point x, σ stabilizes πx if and only if $\sigma = \pi^{-1}\sigma\pi$ stabilizes x. So $\mathrm{Stab}_{Z(G)}(x) = \mathrm{Stab}_{Z(G)}(\pi x)$ for every $\pi \in G$, but by the transitivity of G it follows that an element of $Z(G)$ fixing x also fixes every other point, hence it must be the identity. □

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 24. [30, 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 [30] and leading to the conclusion that a finite simple group is in general uniquely determined by some partial information on its order encoded by the some arithmetical invariants (called Artin invariants). We will make a large use of these results, so we recall here some related definitions.

Definition 25. 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 26. [30, 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 27. Let G be a finite group and $p = p(G)$ its dominant prime, then

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

is called the logarithmic proportion of G.

Proposition 28. [30, 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 29. 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 30. [30, Lemma 4.2] Given $n, \alpha \in \mathbb{N}$, 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 31. 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 [30, 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 [30, Proposition 4.5] and [30, Lemma 4.6], we obtain:

Theorem 32. 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 33. 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 $n_i \ln(p_i) \ln(3) > n_1 \ln(p_1) \ln(2)$.

The good contributors of the finite simple groups are classified in [6].

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

Definition 34. 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 $1 \leq e \leq n - 1$.

The following theorem is due to K. Zsigmondy [56]:

Theorem 35 (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 $s \geq 2$.

2. $n = 6$, $a = 2$.

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

Chapter 3

Pronilpotency of normally ζ-reversible groups

3.1 Convergence of $p_G^{\triangleleft}$

Let G be a profinite group: recall that we need to work under the hypothesis that $a_n^{\triangleleft}(G)$ is finite for every $n \in \mathbb{N}$. This has strong consequences on the topological structure of the group G: in [54, Proposition 4.1.3] it is shown that a group with this property is countably based, i.e. has a topological countable basis for its open sets; moreover, the following results hold.

Theorem 36. [54, Proposition 4.1.3] Let G be a profinite group with only finitely many open normal subgroup of index n for every $n \in \mathbb{N}$: then there is a chain

$$G = N_0 \triangleright N_1 \triangleright \cdots$$

of open normal subgroups comprising a base of open neighbourhoods of 1.

Proof. Clearly, G has only countably many open normal subgroups: let us call them $H_1, H_2, \cdots$, then we can set

$$N_n := \bigcap_{i \leq n} H_i$$

for $i \geq 1$. □

It is now possible to generalize the result in [38, Theorem 1] and prove the following:

Proposition 37. Let G be a profinite group. Then there exists a discending chain

$$G = N_0 \triangleright N_1 \triangleright \cdots$$

of open normal subgroups such that

$$\mathrm{Prob}_G^{\triangleleft}(t) = \inf_i \mathrm{Prob}_{G/N_i}^{\triangleleft}(t) = \lim_i \mathrm{Prob}_{G/N_i}^{\triangleleft}(t).$$

Proof. We will prove that the chain in Theorem 36 satifies our thesis. Consider one of the groups N_i in the chain: then $\mathrm{Prob}^{\triangleleft}_{G/N_i}(t)$ is the ratio of the number $\Phi^{\triangleleft}_{G/N_i}(t)$ of t-uples normally generating G/N_i to $|G/N_i|^t$. Now, the set of all t-uples normally generating G is contained in the union of the cosets of N_i^t determined by t-uples normally generating G/N_i, thus $\mathrm{Prob}^{\triangleleft}_{G}(t) \leq \mathrm{Prob}^{\triangleleft}_{G/N_i}(t)$. In particular, if $\inf_i \mathrm{Prob}^{\triangleleft}_{G/N_i}(t) = 0$, then also $\mathrm{Prob}^{\triangleleft}_{G}(t) = 0$. Suppose now that $\inf_i \mathrm{Prob}^{\triangleleft}_{G/N_i}(t) > 0$, then every finite quotient G/N_i can be normally generated by t elements, therefore so can G (otherwise there would exist i such that $\mathrm{Prob}^{\triangleleft}_{G/N_i}(t) = 0$). Let $\Phi^{\triangleleft}_{G,i}(t)$ be the sets of t-uples in G normally generating G (mod N_i), i.e. the sets of t-uples $(g_1, \cdots, g_t)$ such that $(g_1N_i, \cdots, g_tN_i)$ normally generates G/N_i: then $\Phi^{\triangleleft}_{G}(t) = \bigcap_i \Phi^{\triangleleft}_{G,i}(t)$ and $\Phi^{\triangleleft}_{G,i} \geq \Phi^{\triangleleft}_{G,i+1}(t)$, so

$$\nu(\Phi^{\triangleleft}_{G}(t)) = \inf_i \nu(\Phi^{\triangleleft}_{G,i}(t)) = \lim_i \nu(\Phi^{\triangleleft}_{G,i}(t))$$

where ν is the normalized Haar measure on G we have introduced in the previous chapter. Thus $\mathrm{Prob}^{\triangleleft}_{G}(t) = \inf_i \mathrm{Prob}^{\triangleleft}_{G/N_i}(t)$. □

Now, we have $\mathrm{Prob}^{\triangleleft}_{G}(t) = \lim_i \mathrm{Prob}^{\triangleleft}_{G/N_i}(t) = \lim_i p^{\triangleleft}_{G/N_i}(t)$. Notice that

$$p^{\triangleleft}_{G/N_i}(t) = \sum_{H/N_i \trianglelefteq G/N_i} \frac{\mu^{\triangleleft}(H/N_i, G/N_i)}{|G/N_i : H/N_i|^t} = \sum_{N_i \trianglelefteq H \trianglelefteq G} \frac{\mu^{\triangleleft}(H,G)}{|G:H|^t},$$

hence

$$\mathrm{Prob}^{\triangleleft}_{G}(t) = \lim_i p^{\triangleleft}_{G/N_i}(t) = \lim_i \sum_{N_i \trianglelefteq H \trianglelefteq G} \frac{\mu^{\triangleleft}(H,G)}{|G:H|^t}. \tag{3.1}$$

Consider now the infinite sum

$$\sum_{H \trianglelefteq_O G} \frac{\mu^{\triangleleft}(H,G)}{|G:H|^s} : \tag{3.2}$$

if this sum is absolutely convergent, then we can change the order of its summands and group them in any different way without changing the value of the series. With a suitable ordering, and with a suitable insertion of parentheses, we get from it the Dirichlet series

$$p^{\triangleleft}_{G}(s) = \sum_n \frac{b^{\triangleleft}_n}{n^s} = \sum_n \sum_{H \trianglelefteq_O G, |G:H|=n} \frac{\mu^{\triangleleft}(H,G)}{|G:H|^s} = \sum_{H \trianglelefteq_O G} \frac{\mu^{\triangleleft}(H,G)}{|G:H|^s},$$

moreover, computing the limit in Equation (3.1) under this hypothesis of absolute convergence, we get

$$\mathrm{Prob}^{\triangleleft}_{G}(t) = \lim_i \sum_{N_i \trianglelefteq H \trianglelefteq G} \frac{\mu^{\triangleleft}(H,G)}{|G:H|^t} = \sum_{H \trianglelefteq_O G} \frac{\mu^{\triangleleft}(H,G)}{|G:H|^t}.$$

Hence, the absolute convergence of (3.2) allow us to state that (in the absolute convergence domain) $\mathrm{Prob}^{\triangleleft}_{G}(t) = p^{\triangleleft}_{G}(t)$ expresses the probability that t randomly chosen elements of G normally generate G. Hence, $p^{\triangleleft}_{G}(s)$ interpolate

in its (complex) absolute convergence domain the function $\mathrm{Prob}_G^{\triangleleft}(t)$, which is defined only on positive integer, thus generalizing the interpolation problem proposed by Mann in [39] for $p_G(s)$.
It is thus natural to look for sufficient conditions to ensure this convergence. This question has already been posed for the infinite sum

$$\sum_{H \leq_O G} \frac{\mu(H,G)}{|G:H|^s} \tag{3.3}$$

by A. Mann in [38] and [39]: in particular, Mann proved in [39] that (3.3) absolutely converges in some complex right half-plane if and only if $|\mu(H,G)|$ is bounded by a polynomial function in the index of H and the number of open subgroups of index n such that $\mu(H,G) \neq 0$ grows at most polynomially in n. It comes natural to ask if this result can be extended to the normal case, and the answer is affirmative. Moreover, it is possible to prove that (3.2) absolutely converges in some complex right half-plane if and only if $G/\mathcal{N}(G)$ is finitely generated. We will need the following results:

Theorem 38. [27] Let S be a finite nonabelian simple group, let $\Phi_k(S)$ be the number of ordered k-uples of elements of S which generate all S. Then S^n is d-generated if and only if

$$n \leq \frac{\Phi_d(S)}{|\operatorname{Aut}(S)|}.$$

Proposition 39. Let H_1, H_2 be finite groups with no common composition factors. If $\{x_1, \cdots, x_d\} \subseteq H_1$ and $\{y_1, \cdots, y_d\} \subseteq H_2$ are generating sets for H_1 and H_2 respectively, then $\{(x_1,y_1), \cdots, (x_d,y_d)\}$ is a generating set for $H_1 \times H_2$. In particular, if H_1, H_2 are both d-generated, then $H_1 \times H_2$ is d-generated too.

Proof. Let X be the subgroup of $H_1 \times H_2$ generated by $\{(x_1,y_1), \cdots, (x_d,y_d)\}$, and let π_1, π_2 be the canonical projections of $H_1 \times H_2$ onto H_1 and H_2, respectively. Then $\pi_1(X) = H_1$, $\pi_2(X) = H_2$, so H_1 and H_2 are epimorphic images of $X \leq H_1 \times H_2$. Let Ω_1, Ω_2, Ω, Ω^* be the sets of all composition factors, counted with multiplicity, of H_1, H_2, $H_1 \times H_2$ and X, respectively. Clearly $\Omega = \Omega_1 \dot{\cup} \Omega_2$, moreover $\Omega_1, \Omega_2 \subseteq \Omega^*$ thus

$$\Omega^* \subseteq \Omega = \Omega_1 \dot{\cup} \Omega_2 \subseteq \Omega^*,$$

whence in particular $\Omega^* = \Omega$ and so $X = H_1 \times H_2$. □

Theorem 40. Let $c_n^{\triangleleft}(G)$ be the number of open normal subgroups of index n such that $\mu^{\triangleleft}(H,G) \neq 0$. Then the following are equivalent:

(i) the infinite sum (3.2) absolutely converges in some right complex half plane;

(ii) $\mu^{\triangleleft}(H,G)$ and $c_n^{\triangleleft}(G)$ are polynomially bounded in $|G:H|$ and in n respectively (i.e., there exist $c_1, c_2 \in \mathbb{N}$ such that $|\mu^{\triangleleft}(H,G)| \leq |G:H|^{c_1}$ and $c_n^{\triangleleft}(G) \leq n^{c_2}$ for every $H \trianglelefteq_O G$ and every $n \in \mathbb{N}$);

(iii) G is PFNG;

(iv) G has maximal normal subgroups growth, i.e. there exists $c \in \mathbb{N}$ such that $m_n^{\triangleleft}(G) \leq n^c$ for every n;

(v) $G/\mathcal{N}(G)$ is finitely generated.

Proof.

(i)⇒(ii) If the series absolutely converges for some $s \in \mathbb{C}$, then $\dfrac{\mu^{\triangleleft}(H,G)}{|G:H|^s} \longrightarrow 0$, in particular $|\mu^{\triangleleft}(H,G)| \leq |G:H|^{\Re(s)}$ for $|G:H|$ big enough. This means we can find c_1 such that $|\mu^{\triangleleft}(H,G)| \leq |G:H|^{c_1}$ for all $H \trianglelefteq_O G$. Moreover, $\mu^{\triangleleft}(\cdot, G)$ assumes integer values, so it has absolute value at least 1 on the subgroups on which it does not vanish: thus

$$\frac{c_n^{\triangleleft}(G)}{n^s} \leq \sum_{H \trianglelefteq_O G, |G:H|=n} \frac{|\mu^{\triangleleft}(H,G)|}{n^s} \longrightarrow 0,$$

and thus $c_n^{\triangleleft}$ is polynomially bounded.

(ii)⇒(i) If there exist such c_1, c_2, then

$$\sum_{H \trianglelefteq_O G} \frac{|\mu^{\triangleleft}(H,G)|}{|G:H|^s} \leq \sum_{H \trianglelefteq_O G, \mu^{\triangleleft}(H,G) \neq 0} |G:H|^{c_1-s} \leq \sum_n \sum_{j=1}^{c_n^{\triangleleft}(G)} n^{c_1-s} = \sum_n n^{c_1+c_2-s},$$

which is absolutely convergent for $\Re(s) > c_1 + c_2 + 1$.

(iii)⇔(iv) By [16, Proposition 4.1], a profinite group is PFNG if and only if it the sequence $\{m_n^{\triangleleft}(G)\}_{n \in \mathbb{N}}$ of the numbers of maximal open normal subgroups of G of index n (or, equivalently, of finite simple quotients of G of order n) is polynomially bounded.

(iv)⇒(ii) Let N be an open normal subgroup of G of index n such that $\mu^{\triangleleft}(N,G) \neq 0$: then N is intersection of maximal open normal subgroups of G, in particular $\mathcal{N}(G) \leq N$ and G/N is a direct product of finite simple groups, say $G/N \cong S_1 \times \cdots \times S_t \times C_{p_1}^{\alpha_1} \times \cdots \times C_{p_r}^{\alpha_r}$, where the S_i's are finite nonabelian simple groups and the p_i's are all different primes.
Using the correspondence between open normal subgroups of G containing N and open normal subgroups of G/N, it is easy to see that $\mu^{\triangleleft}(N,G) = \mu^{\triangleleft}(1, G/N)$. So, it suffices to bound the absolute value of $\mu^{\triangleleft}(1, G/N)$, which is the coefficient of the term $\dfrac{1}{|G/N|^s}$ in

$$p_{G/N}^{\triangleleft}(s) = \prod_{i=1}^{t} \left(1 - \frac{1}{|S_i|^s}\right) \prod_{j=1}^{r} \prod_{k=1}^{\alpha_j} \left(1 - \frac{p_j^{k-1}}{p_j^s}\right),$$

that is $\pm \prod_{j=1}^{r} p_j^{\alpha_j(\alpha_j-1)/2}$. Now, the number of open normal subgroups of G/N of index p_i must be bounded by p_i^c, that is

$$1 + \cdots + p_i^{\alpha_i - 1} = \frac{p_i^{\alpha_i} - 1}{p_i - 1} \leq p_i^c,$$

so $\alpha_i \leq c$ for all i and

$$|\mu^{\triangleleft}(N,G)| = \prod_{j=1}^{r} p_j^{\alpha_j(\alpha_j-1)/2} \leq n^{(c-1)/2},$$

thus $\mu^{\triangleleft}(N,G)$ has polynomial growth.
Let us prove $c_n^{\triangleleft}(G)$ has polynomial growth: as we said, if N is an open normal subgroup of G of index n such that $\mu^{\triangleleft}(N,G) \neq 0$, then it is intersection of maximal open normal subgroups of G, say $N = M_1 \cap \cdots \cap M_k$. We may choose the maximal subgroups $M_1, \cdots, M_k$ in such a way that $|G:N| = \prod_{i=1}^{k} |G:M_i|$. There are at most n possible factorizations $n = m_1 \cdots m_k$ (see for example [40]) and at most $m_{m_i}^{\triangleleft} \leq m_i^c$ maximal normal subgroups M_i of G with $|G:M_i| = m_i$, so there are at most $n \cdot n^c = n^{c+1}$ possibilities for N.

(i)⇒(iii) Suppose G is not PFNG, then $p_G^{\triangleleft}(t) = \mathrm{Prob}_G^{\triangleleft}(t) = 0$ for any $t \in \mathbb{N}$ big enough: then $b_n^{\triangleleft} = 0$ for every n by Proposition 16, a contradiction.

(v)⇒(iv) Suppose $d\left(G/\mathcal{N}(G)\right) = d$, let us show that $m_n^{\triangleleft}(G)$ is polynomially bounded in n.
If $n = p$ is a prime, then $G/G'G^p \cong C_p^m$ for some m and

$$m = d\left(G/G'G^p\right) \leq d\left(G/\mathcal{N}(G)\right) = d.$$

It follows

$$m_p^{\triangleleft}(G) = m_p^{\triangleleft}(G/G'G^p) = \frac{p^m - 1}{p-1} \leq p^d.$$

Notice that if S is a non-abelian simple group and $m = \gamma_G(S)$, then $d(S^m) \leq d(G/\mathcal{N}(G)) = d$: in particular, by Theorem 38

$$m \leq \frac{\Phi_d(S)}{|\operatorname{Aut}(S)|} \leq |S|^{d-1}.$$

Let now n be a natural number which is not a prime. By the previous observation

$$m_n^{\triangleleft}(G) = \sum_{|S|=n} \gamma_G(S) \leq \sum_{|S|=n} |S|^{d-1}.$$

As there are at most two non-isomorphic non-abelian simple groups of order n (see for example [30, Theorem 5.1]), we can conclude that

$$m_n^{\triangleleft}(G) \leq 2n^{d-1} \leq n^d.$$

(iv)⇒(v) Let $G/\mathcal{N}(G) = \prod_i S_i^{\gamma_G(S_i)}$.
If $S \cong C_p$ then, as G has polynomial maximal normal subgroup growth, we have

$$\frac{p^{\gamma_G(S)} - 1}{p-1} = m_p^{\triangleleft}(G) \leq p^c,$$

whence $\gamma_G(S) \leq c+1$ and thus $S^{\gamma_G(S)}$ is at most $c+1$-generated.
Let now S be a non-abelian simple composition factor of G: in [41] it is proved that if S is a finite simple group, then $p_S(2) \geq \frac{53}{90}$. Therefore,

$$\gamma_G(S) \leq m_{|S|}^{\triangleleft}(G) \leq |S|^c \leq \frac{53}{90}|S|^{c+1} = \frac{\frac{53}{90}|S|^{c+3}}{|S|^2} \leq \frac{p_S(c+3)|S|^{c+3}}{|\operatorname{Aut}(S)|} = \frac{\Phi_{c+3}(S)}{|\operatorname{Aut}(S)|}$$

so by Theorem 38 $S^{\gamma_G(S)}$ is $c+3$-generated.
We have thus $G/\mathcal{N}(G) = \prod S_i^{\gamma_G(S_i)}$, where $S_i^{\gamma_G(S_i)}$ is at most $c+3$-generated for any i. Then $G/\mathcal{N}(G)$ is $c+3$-generated itself by Proposition 39.

□

Corollary 41. Let G a finitely generated profinite group: then the sum (3.2) absolutely converges in some right complex half plane. In particular, for $t \in \mathbb{N}$ big enough $p_G^{\triangleleft}(t)$ is the probability that t randomly chosen elements of G generate G.

3.2 A reduction to a question on finite groups

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 [16, Section 5] that

$$p_G^{\triangleleft}(s) = A_G(s)B_G(s). \tag{3.4}$$

Now consider the two series

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

We recall that in [15] it is proved that a finitely generated profinite group G is prosoluble if and only if the sequence $\{b_n(G)\}$ is multiplicative: there is a useful corresponding result characterizing profinite groups such that the sequence $\{b_n^{\triangleleft}(G)\}$ is multiplicative.

Theorem 42. [16, Proposition 5.2] The series $p_G^{\triangleleft}(s)$ is multiplicative if and only if there is no open normal subgroup $N \triangleleft G$ such that G/N is simple non-abelian.

In particular, $A(G,s) = p_{G/G'} = p_{G/G'}^{\triangleleft}$ is multiplicative, and so is its inverse $\Gamma_G(s)$.

Lemma 43. If G is a normally ζ-reversible profinite group, then

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

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

$$1 = (\zeta_G^{\triangleleft}(s)p_G^{\triangleleft}(s))_p = \zeta_{G,p}^{\triangleleft}(s)p_{G,p}^{\triangleleft}(s) = \zeta_{G,p}^{\triangleleft}(s)A_{G,p}(s)B_{G,p}(s).$$

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

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

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 $\Gamma_G(s) = \prod_p \zeta_{G,p}^{\triangleleft}(s)$. □

Lemma 44. If G is a normally ζ-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 $1 \leq i \leq r$, 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 $1 \leq i \leq r$. 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 $|\mathcal{N}_q| = a_q^{\triangleleft}(G)$; moreover $a_q^{\triangleleft}(G) = \gamma_q(G)$ by Lemma 43. Hence

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

□

Corollary 45. Assume that G is normally ζ-reversible group profinite. If there is no open normal subgroup $N \triangleleft G$ such that G/N is a nonabelian simple group, then G is pronilpotent.

Proof. 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 (3.4), we have $\Gamma_G(s) = A_G(s)^{-1} = p_G^{\triangleleft}(s)^{-1} = \zeta_G^{\triangleleft}(s)$, i.e $\gamma_n(G) = a_n^{\triangleleft}(G)$ for every $n \in \mathbb{N}$. We conclude from Lemma 44 that G/N is nilpotent for every open normal subgroup N of G. □

Remark 46. Notice that if G is a prosolvable group, then there is no open normal subgroup $N \triangleleft G$ such that G/N is simple non-abelian; thus, every prosolvable normally ζ-reversible group is pronilpotent.

Our claim is to give a characterisation of profinite normally ζ-reversible groups. In particular, we will deal with the following conjecture:

Conjecture 47. 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.

From now on, let G be a normally ζ-reversible profinite group, We will denote with Σ_G the set (which we are assuming non-empty) of the finite nonabelian simple groups which are continuous epimorphic images of G and with Ω_G the set of the orders of the elements of Σ_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.
Now consider $\zeta_G^{\triangleleft}(s), p_G^{\triangleleft}(s)$: this two series only depend on the contribution of open normal subgroups of index in π, that is the open normal subgroups of G containing M, corresponding to the open normal subgroups of G/M. Therefore $\zeta_{G,\pi}^{\triangleleft}(s) = \zeta_{G/M}^{\triangleleft}(s)$ and $p_{G,\pi}^{\triangleleft}(s) = p_{G/M}^{\triangleleft}(s)$. Then,

$$\zeta_{G/M}^{\triangleleft}(s) p_{G/M}^{\triangleleft}(s) = \zeta_{G,\pi}^{\triangleleft}(s) p_{G,\pi}^{\triangleleft}(s) = (\zeta_G^{\triangleleft}(s) p_G^{\triangleleft}(s))_p = 1,$$

hence G/M is still a normally ζ-reversible group and represents a counterexample to Conjecture 47. Hence, 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 $S \in \Sigma_G$. It is well known (see for example [8]) that 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 nonabelian simple groups 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. Then:

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

and

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

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 $a_n^{\triangleleft}(G) = a_n^*$.

Lemma 48. 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

$$a_n^{\triangleleft}(G) = a_n^* = \gamma_n(G) + \sum_{m_i r = n} t_i \gamma_r(G). \tag{3.5}$$

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 (3.5), $a_n^{\triangleleft}(G) = a_n^*$, 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

$$a_{m^2}^{\triangleleft}(G) = a_{m^2}^* = \gamma_{m^2}(G) + \sum_{m_i r = m^2} t_i \gamma_r(G) + \binom{t}{2} + t. \tag{3.6}$$

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

Lemma 49. 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. $\sum_{m_i r = m^2} t_i \gamma_r(G)$ 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.

Proof. (1) and (2) can be verified as in lemma 48. Moreover, we know that there are t open normal subgroups $N_1, \cdots, N_t$ such that $G/N_1, \cdots, G/N_t$ are simple non-abelian of order m: to prove (3), we must show that G/M is a direct product of two non-abelian simple groups of order m if and only if $M = N_i \cap N_j$ for one of the $\binom{t}{2}$ possibile choices of two indices $i \neq j$. Consider $S_1 = G/N_1$ and $S_2 = G/N_2$, let $M = N_1 \cap N_2$: clearly G/M is a subdirect product of $S_1 \times S_2$, moreover $N_1/M, N_2/M \trianglelefteq G/M$, so necessarily $G/M \cong S_1 \times S_2 = G/N_1 \times G/N_2$. Conversely, let $M \triangleleft G$ such that $G/M \cong S_1 \times S_2$ for some simple non-abelian S_1, S_2 of order m: then G/M has exactly two non-trival open normal subgroups, $M_1/M \cong S_1$ and $M_2/M \cong S_2$, but then they must have trivial intersection, that is $M_1 \cap M_2 = M$. Furthermore, $M_1, M_2 \trianglelefteq G$ and $S_1 \cong M_1/M \cong G/M_2$, $S_2 \cong M_2/M \cong G/M_1$, thus M is intersection of open normal subgroups of G such that the correspondant quotients of G are simple non-abelian groups of order m. □

Notice that the last summand in (3.6) consists of t open normal subgroups of index m^2 that does not fill in any of the three classes described in Lemma 49: let M be one of these groups and let $H = G/M$.

Proposition 50. H has a unique minimal normal subgroup.

Proof. Suppose by contradiction that H has two different minimal normal subgroups N_1, N_2: then they must have trivial intersection and $H = H/(N_1 \cap N_2)$ is a subdirect product of $H/N_1 \times H/N_2$; moreover, by Lemma 48 there exist 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 $G/N_2 \cong X_2 \cap Y_2$. It follows that H is 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 49, a contradiction. □

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

Theorem 51. If Conjecture 47 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 is not nilpotent, nor a direct product of two nonabelian simple groups, nor a direct product of a nilpotent group and a nonabelian simple group.

3. H contains a unique minimal normal sugroup N.

4. 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 $\pi(S) = \pi(T)$.

3.3 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 51 that:

Proposition 52. 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 53. If H is a finite group satisfying the statement of Proposition 52, then $N = \operatorname{soc} H$ is abelian.

Proof. Suppose by contradition that N is not abelian: 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 18, 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 nonabelian finite 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 52.

2. S is not an alternating group and has a transitive (faithful) action of degree u. In particular S has a primitive action of degree $v \leq u$, hence, by [45], $|S| \leq 4^v \leq 4^u$. By Proposition 52, $|T| \leq |S|$, hence

$$|L|^u = |N| = \frac{|T|^2}{|S|} \leq |S| \leq 4^u,$$

but then $|L| \leq 4$, contradiction.

The only possibility is then $L \cong C_p$ for some prime p, that is N is elementary abelian. □

We have so proved that N is elementary abelian and an irreducible H/K-module (with respect to the conjugacy action).

Corollary 54. If there exists a perfect normally ζ-reversible profinite group, then there exists a triple (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 52, taking $V = \operatorname{soc} H$ (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 [28, Proposition 5.6] stating that, if a group J has an abelian Sylow p-subgroup, then p does not divide $|J' \cap \mathrm{Z}(J)|$: since $H' = H$ and $\mathrm{Z}(H) = \operatorname{soc} H \cong V$, 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.
In particular, using results on the dominant primes of S and T and lower bonds for the degree of irreducible representations of finite groups of Lie type in cross characteristic, we will prove that T and S, we will prove that both S, T are simple groups of Lie type (Propositions 56, 60 and 61) and $a = 1$ (Proposition 66): finally we will reduce to the case $|T|^2 = p|S|$, where the dominant primes of S, T (which coincide with their characteristics) are different, and we will find a contradiction using arithmetic arguments.

Suppose by contradiction that there exists a triple (S, T, V) satisfying the properties in Corollary 54.

Remark 55. Since $|S|p^a = |T|^2$, every prime divisor of $|S|$ different from p divides $|S|$ with even multiplicity.

Proposition 56. S is a simple group of Lie type.

Proof. By Remark 55, 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 sporadic groups and for alternating groups $\mathrm{Alt}(m)$, for $m \leq 10$. For the remaining alternating groups, we deduce from Lemma 18 that there are two primes p, q dividing $\mathrm{Alt}(n) = n!/2$ with multiplicity exactly one. □

Proposition 57. 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 [34] and improved later by Seitz and Zalesskii [48] and Tiep [50]. 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 $|S| = \frac{1}{d} q^{n(n+1)/2} \prod_{i=2}^{n+1} (q^i - 1) < q^{n^2+2n}$. First assume $n \neq 1$ and exclude the exceptional cases $(n, q) = (2, 2), (2, 4), (3, 2), (3, 3)$. By [50, Table II] we have $d_p(S) \leq \frac{q^{n+1} - q}{q - 1} - 1$. But then, if $(n, q) \neq (2, 3)$, $\ln(|S|) < (n^2 + 2n)\ln(q) < \left(\frac{q^{n+1} - q}{q - 1} - 1\right) \ln(2) \leq a \cdot \ln(p)$, in contradiction with our request $|V| < |S|$.
For $n \neq 1$, we left the possibilites $(n, q) = (2, 2), (2, 3), (2, 4), (3, 2), (3, 3)$, but for these cases there are at least two primes dividing $|S|$ with odd multiplicites, so they must be excluded by Remark 55. If $n = 1$, we can use the bound $\delta(S) \leq \frac{q-1}{(2, q-1)}$ in [34, Table 1], thus $\ln(|S|) < 3\ln(q) < \frac{q-1}{(2, q-1)} \ln(2) \leq a \cdot \ln(p)$, which holds for $q \geq 31$; for the other cases it is again easy to check that the corresponding groups, apart from $A_1(17)$, have order divisible with odd multiplicity by at least two primes, so they must be excluded by Remark 55. For $S = A_1(17)$, we should have $p = 17$ and the condition $|V| < |T| < |S|$ forces $a = 1$, against the hypothesis.
For the other Lie types, apart from a finite number of cases, there are the following bounds to $|S|$ and $\delta(S)$, (extracted by [50, Table II] for $A_n(q)$, $B_n(q)$, $D_n(q)$, ${}^2D_n(q)$, $G_2(q)$, ${}^3D_4(q)$, $F_4(q)$ and from [50, Table I] for the remaining cases) which allow, in all cases but a finite number, to conclude that $|S| < p^{\delta(S)} \leq p^a = |V|$, contradicting our request that $|V| < |S|$.
In Table 3.1 the reader can find bounds for the other families of finite simple groups of Lie type, which can thus be discussed with similar arguments.

Table 3.1: Bounds for $|S|$ and $\delta(S)$ in Proposition 57

Group	Bound on $\lvert S\rvert$	$\delta(S)$
$A_n(q)$	$\lvert S\rvert < q^{n^2+2n}$	$\frac{q^{n+1}-q}{q-1} - 1$
${}^2A_n(q)$	$\lvert S\rvert < q^{n^2+2n}$	$\left[\frac{q^{n+1}-1}{q+1}\right]$
$B_n(q)$, $q > 3$	$\lvert S\rvert < q^{2n^2+n}$	$\frac{q^{2n}-1}{q^2-1} - 2$
$B_n(q)$, $q = 3$	$\lvert S\rvert < q^{2n^2+n}$	$\frac{(q^n-1)(q^n-q)}{q^2-1}$
$C_n(q)$, odd q	$\lvert S\rvert < q^{2n^2+n}$	$\frac{q^n-1}{2}$
$C_n(q)$, even q	$\lvert S\rvert < q^{2n^2+n}$	$\frac{(q^n-1)(q^n-q)}{2(q+1)}$
$D_n(q)$, $q > 3$	$\lvert S\rvert < q^{2n^2-n}$	$\frac{(q^n-1)(q^{n-1}+q)}{q^2-1} - 2$
$D_n(q)$, $q \leq 3$	$\lvert S\rvert < q^{2n^2-n}$	$\frac{(q^n-1)(q^{n-1}-1)}{q^2-1}$
${}^2D_n(q)$	$\lvert S\rvert < q^{2n^2-n}$	$\frac{(q^n+1)(q^{n-1}-q)}{q^2-1} - 1$
${}^2B_2(q)$	$\lvert S\rvert < q^5$	$(q-1)\sqrt{\frac{q}{2}}$
${}^3D_4(q)$	$\lvert S\rvert < q^{32}$	$q^5 - q^3 + q - 1$
$G_2(q)$	$\lvert S\rvert < q^{14}$	$q^3 - 1$
${}^2G_2(q)$	$\lvert S\rvert < q^7$	$q(q-1)$
$F_4(q)$, odd q	$\lvert S\rvert < q^{52}$	$q^8 + q^4 - 2$
$F_4(q)$, even q	$\lvert S\rvert < q^{52}$	$\frac{(q^3-1)(q^8-q^7)}{2}$
${}^2F_4(q)$	$\lvert S\rvert < q^{26}$	$(q^5-q^4)\sqrt{\frac{q}{2}}$
$E_6(q)$	$\lvert S\rvert < q^{78}$	$q^{11} - q^9$
${}^2E_6(q)$	$\lvert S\rvert < q^{78}$	$\frac{q^8}{20}(q^4+1)(q^3-1)$
$E_7(q)$	$\lvert S\rvert < q^{133}$	$q^{17} - q^{15}$
$E_8(q)$	$\lvert S\rvert < q^{248}$	$q^{29} - q^{27}$

The exceptional cases that remain to discuss are the following: ${}^2A_2(3)$, ${}^2A_2(4)$, ${}^2A_3(2)$, ${}^2A_3(3)$, ${}^2A_4(2)$, ${}^2A_5(2)$, ${}^2A_6(2)$, $B_2(5)$, $B_2(7)$, $B_3(3)$, $C_2(3)$, $C_2(4)$, $C_2(5)$, $C_2(7)$, $C_3(2)$, $C_3(3)$, $C_4(2)$, $C_4(3)$, $D_4(2)$, ${}^2B_2(8)$, $G_2(3)$, $G_2(4)$, $F_4(2)$, ${}^2E_6(2)$. These groups, apart from ${}^2A_3(2)$, $B_2(5)$, $B_2(7)$, all have order divisible with odd multiplicity by at least two primes, so they can be excluded by Remark 55.
For $S = {}^2A_3(2) \cong B_2(3)$ or $C_2(3)$, we should have $p = 5$ and the condition $p^a = |V| < |T| < |S|$ forces $a \in \{1, 3, 5\}$ and $|T| = 2^3 \cdot 3^2 \cdot 5^b$, for $b \leq 3$. The only correspondence with the order of a simple group is for $a = b = 1$, against the hypothesis; analogously we can exclude $S = B_2(5)$, $C_2(5)$ and $B_2(4) \cong C_2(4)$. Finally, for $S = B_2(7)$ or $C_2(7)$, a direct computation shows that the only possibility is $V \cong C_5^2$ but, by [50, Table II], $\delta(B_2(7)) \geq \frac{7^4-1}{7^2-1} - 2 = 48 > 2$ and

$\delta(C_2(7)) \geq \dfrac{7^2-1}{2} - 2 = 22 > 2$, contradiction.
Therefore, if $a \neq 1$, then p coincides with the characteristic of S. □

Proposition 58. The dominant prime of S coincides with the characteristic of S.

Proof. By Proposition 26, 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 both divides $|S| = (q-1)q(q+1)/2$ with odd multiplicity, against Remark 55.

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

Proof. Suppose $a \neq 1$: by Proposition 57 and 58, 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 60. T is not an alternating group.

Proof. Let $T = \mathrm{Alt}(m)$, $m \geq 5$. First assume $m \leq 9$. We use [8, p. 239–242] to check that if $|S|$ is a finite simple group with $\pi(S) = \pi(\mathrm{Alt}(m))$ and $|\mathrm{Alt}(m)|^2 = |S|p^a$ 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 [30, 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 59, $a = 1$, so

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

Let $|T|_2 = 2^t$, $|T|_q = q^h$, then $2^t > q^h$ (as 2 is the dominant prime of T) and, by (3.7), $q^{2h} > 2^{2t-1}$ (as q is the dominant prime of S), whence $q^{2h+1} > 2^{2t}$.

Joining these inequalities we get $q^h < 2^t < q^{h+1/2}$, whence $h\ln(q) < t\ln(2) < \left(h+\frac{1}{2}\right)\ln(q)$, and so

$$1 < \frac{t\ln(2)}{h\ln(q)} < 1 + \frac{1}{2h} \leq \frac{3}{2} < \frac{\ln(3)}{\ln(2)}. \tag{3.8}$$

By (3.8), q is a good contributor to T, but [6, Theorem 3.8] enlists all good contributors to alternating groups, and for $m \geq 10$ it must be

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

Recall that $2^t = |\mathrm{Alt}(m)|_2$ and $q^h = |\mathrm{Alt}(m)|_q$, where q is the dominant prime of $|\mathrm{Alt}(m)|_{2'}$: thus, the values of t, h are determined by m: in particular, [6, 3.2] gives useful bounds (both upper and lower) for t, h which are linear functions of m.
Suppose $q = 5$, then (3.8) can be rewritten into $2t\ln(2) < (2h+1)\ln(5)$ which, as can be directly computed, is false for the six possible values of m.
Suppose $q = 3$, then (3.8) becomes

$$2t\ln(2) < (2h+1)\ln(3) \tag{3.9}$$

and for $m \geq 16$ we have $t \geq \frac{15m-65}{16}$ and $h < \frac{m}{2}$ by the already cited [6, 3.2] which, joined with (3.9), give $m < \frac{65\ln(2)+8\ln(3)}{15\ln(2)-8\ln(3)} < 34$. For $m \leq 33$ it is easy to directly verify that (3.9) is true only for $m \in \{10, 11, 15\}$: for $m = 10$ or $m = 11$ we have $2^t = 2^7$, $3^h = 3^4$, so the contribution of 2 to the order of S is $2^{13} > 3^8$, so the dominant prime of S is 2, contradiction; for $m = 15$ it should be $|S| = 2^{19} \cdot 3^{12} \cdot 5^6 \cdot 7^4 \cdot 11^2 \cdot 13^2$, so its logaritmic proportion is lower than $1/3$, but then, by Proposition 28, S is not of Lie type, a contradiction.
Thus, $m \geq 10$ and S and T both have dominant prime 2. We claim that $p \neq 2$: indeed, assume by contradiction $p = 2$.
If $m = 10$, then $3^8 = |S|_3 < |S|_2 = 2^{14-a}$ as 2 is the dominant prime of S, whence $a = 1$, making $\lambda(S) < 1/3$, thus contradicting Proposition 28.
For $m \geq 11$ we have $\lambda(\mathrm{Alt}(m)) < 1/3$, as reported in [30, Table $L.4$], then

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

contradicting again Proposition 28.
Thus S and T both have dominant prime 2 and p is odd. By Proposition 28

$$\left(\frac{m}{e}\right)^m < \frac{m!}{2} = |T| < |S| \leq |S|_2^3 \leq |T|_2^6. \tag{3.10}$$

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

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

and, since it is an integer, it must be $l \leq m-2$. This result, joined with (3.10), gives $m < e \cdot 2^{6-12/m}$, whence $m \leq 165$.
Since $p \neq 2$, we have $|S|_2 = |T|_2^2$ and, by Proposition 28,

$$\frac{1}{3} \leq \frac{\ln(|S|_2)}{\ln(|S|)} = \frac{\ln(|T|_2^2)}{\ln(|T|)^2 - a\ln(p)}. \tag{3.11}$$

Moreover 3 is dominant prime of $|\mathrm{Alt}(m)|_{2'}$ for every $m \geq 10$ (see [6, Theorem 3.7 (b)]), so

$$p^a \leq \frac{|T|_3^2}{3}. \tag{3.12}$$

From (3.11) and (3.12) we finally get

$$\frac{1}{3} \leq \frac{\ln(|T|_2^2)}{\ln(|T|)^2 - \ln(|T|_3^2) + \ln(3)} = \frac{\ln(|T|_2)}{\ln(|T|_{3'}) + \ln(3)/2} \tag{3.13}$$

and it is easy to verify that, in the given range $10 \leq m \leq 165$, (3.13) 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 $|S|_2 = |\mathrm{Alt}(m)|_2^2$: the groups satisfying these conditions for $10 \leq m \leq 14$ or $16 \leq m \leq 21$ are listed in Table 3.2. Some of them have order divisible by a prime greater than m, the others have order not divisible by a prime lower than m; in both cases, the order of S cannot have the same prime divisors as the order of $\mathrm{Alt}(m)$.

Table 3.2: Possible S when $T = \mathrm{Alt}(m)$ with $10 \leq m \leq 21$, $m \neq 15$

m	$\lvert S\rvert_2$	Possible S	Primes dividing $\lvert S\rvert$	Primes not dividing $\lvert S\rvert$
10, 11	2^{14}	${}^2B_2(2^7)$, $A_1(2^{14})$	$127 = 2^7 - 1$	
12, 13	2^{18}	$G_2(2^3)$, ${}^2B_2(2^9)$, $A_1(2^{18})$, $A_2(2^6)$, $A_3(2^3)$	$73 \mid 2^9 - 1$	
		$B_3(2^2)$	$17 \mid 2^8 - 1$	
		${}^2A_2(2^6)$	$37 \mid 2^{18} + 1$	
		${}^2A_3(2^3)$	$19 \mid 2^9 + 1$	
14	2^{20}	$D_5(2)$, $B_2(2^5)$, $A_1(2^{20})$, $A_4(2^2)$	$31 \mid 2^5 - 1$	
		${}^2D_5(2)$, ${}^2A_4(2^2)$	$17 \mid 2^8 - 1$	
16, 17	2^{28}	$B_2(2^7)$, $A_1(2^{28})$, $A_7(2)$	$127 = 2^7 - 1$	
		${}^2A_7(2)$	$43 \mid 2^7 + 1$	
18, 19	2^{30}	$A_1(2^{30})$, $A_2(2^{10})$, ${}^2A_2(2^{10})$, $A_3(2^5)$, ${}^2A_3(2^5)$, $A_4(2^3)$, ${}^2A_4(2^3)$		17
		${}^2D_6(2)$, $A_5(2^2)$	$31 = 2^5 - 1$	
		${}^2A_5(2^2)$	$41 \mid 2^{10} + 1$	
		${}^2B_2(2^{15})$		3
		$G_2(2^5)$		5
		$D_6(2)$		13
20, 21	2^{34}	$A_1(2^{34})$		7
		${}^2B_2(2^{17})$		3

Finally, for $m = 24$ the condition on the logarithmic proportion imposes that $p = 3$ and $a = 19$, whence $|S| = 2^{42} \cdot 3 \cdot 5^8 \cdot 7^6 \cdot 11^4 \cdot 13^2 \cdot 17^2 \cdot 19^2 \cdot 23^2$. Moreover, for $|S|_2 = 2^{42}$ the possibilities are $G_2(2^7)$, $D_7(2)$, ${}^2D_7(2)$, $A_1(2^{42})$, $A_2(2^{14})$, $A_3(2^7)$, ${}^2A_3(2^7)$, $A_6(2^2)$, ${}^2A_6(2^2)$ (which would all get to $|S|_3 > 3$), ${}^2B_2(2^{21})$ (whose order is not divisible by 3) and ${}^2A_2(2^{14})$ (whence $|S|_5 = 25$), implying again a contradiction in all cases. □

Proposition 61. T is not a sporadic simple group.

Proof. At first, we will prove that S and T have the same dominant prime. Suppose the dominant primes do not coincide: then, since $|T|^2 = |S|p^a$, p coincides with the dominant prime of T and, by Corollary 59, $a = 1$. So we have

$$|T|^2 = p\,|S|\,. \tag{3.14}$$

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 (3.14), $q^{2h} > p^{2t-1}$ (as q is the dominant prime of S), so we get

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

By Corollary 54(6), it must be $t > 1$, so

$$1 < \frac{t\ln(p)}{h\ln(q)} < \frac{t}{t-1/2} < \frac{\ln(3)}{\ln(2)}. \tag{3.15}$$

This implies that q is a good contributor to T. The good contributors to sporadic simple groups are listed in [6, Theorem 1]: it is easy to verify that these good contributors does not satisfy (3.15), 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 28.
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 59 and $\lambda(S) > 1/3$ by Proposition 28, so

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

whence

$$2 \leq a \leq \left\lfloor \frac{3\ln(|T|_p) - \ln(|T|)}{\ln(p)} \right\rfloor =: a_*(T). \tag{3.16}$$

The values of $a_*(T)$ for every sporadic simple group T are listed in Table 3.3.

Table 3.3: Values of $a_*(T)$ in Proposition 61

T	p	$a_*(T)$
M	2	-42

B	2	11
F_{3+}	3	-3
Fi_{23}	3	-1
Fi_{22}	2	5
F_3	3	-6
Ly	5	-6
Co_3	3	-4
F_5	2	-6
He	2	-2
McL	3	-1
HS	2	1
J_4	2	-4
J_3	3	-2
J_2	2	1
J_1	19	-2
M_{12}	2	1
M_{24}	2	2
Co_1	2	1
M_{23}	2	-3
Co_2	2	8
M_{22}	2	2
M_{11}	2	-1
Suz	2	0
Ru	2	4
$O'N$	2	-12
${}^2F_4(2)'$	2	8

Confronting these values with Equation (3.16) we get that

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

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 $|T|_2^2 = 2^a|S|_2$ and $2 \leq a \leq a_*(T)$: the groups satisfying these conditions are listed in Table 3.4, but we can see that all of them contradict the assumption that $|S|$, $|T|$ have the same prime divisors.

Table 3.4: Possible S for sporadic T when $a \neq 1$ in Proposition 61

T	a	$\lvert S\rvert_2$	Possible S	Divisors of $\lvert S\rvert$, not of $\lvert T\rvert$	Divisors of $\lvert T\rvert$, not of $\lvert S\rvert$
M_{22}	2	2^{12}	$G_2(2^2)$, ${}^3D_4(2)$, $B_2(2^3)$	$13 \mid 2^6+1$	
			${}^2D_4(2)$, $A_1(2^{12})$, $A_2(2^4)$, ${}^2A_2(2^4)$, $A_3(2^2)$, ${}^2A_3(2^2)$	$17 = 2^4+1$	
			$D_4(2)$		11
M_{24}	2	2^{18}	$G_2(2^3)$, ${}^2B_2(2^9)$, $A_1(2^{18})$, $A_2(2^6)$, $A_3(2^3)$	$73 \mid 2^9-1$	

			$B_3(2^2)$	$17 = 2^4 + 1$	
			${}^2A_2(2^6)$	$37 \mid 2^{18} + 1$	
			${}^2A_3(2^3)$	$19 \mid 2^9 + 1$	
Ru	2	2^{26}	${}^2B_2(2^{13})$, $A_1(2^{26})$	$8191 = 2^{13} - 1$	
	3	2^{25}	$B_5(2)$, $A_1(2^{25})$	$31 = 2^5 - 1$	
	4	2^{24}	$F_4(2)$, $G_2(2^4)$, $D_4(2^2)$, ${}^2D_4(2^2)$, $B_2(2^6)$, $A_1(2^{24})$, $A_2(2^8)$, ${}^2A_2(2^8)$, $A_3(2^4)$, ${}^2A_3(2^4)$	$17 = 2^4 + 1$	
			${}^3D_4(2^2)$	241	
Fi_{22}	2	2^{32}	$B_2(2^8)$, $B_4(2^2)$, $A_1(2^{32})$	$17 = 2^4 + 1$	
	3	2^{31}	$A_1(2^31)$		7
	4	2^{30}	${}^2B_2(2^{15})$, $G_2(2^5)$, $D_6(2)$, ${}^2D_6(2)$, $A_5(2^2)$, $A_1(2^{30})$, $A_2(2^{10})$, ${}^2A_2(2^{10})$, $A_3(2^5)$, ${}^2A_3(2^5)$, $A_4(2^3)$	$31 = 2^5 - 1$	
			${}^2A_5(2^2)$	$41 \mid 2^{10} + 1$	
			${}^2A_4(2^3)$	$19 \mid 2^9 + 1$	
	5	2^{29}	$A_1(2^{29})$		7
Co_2	2	2^{34}	${}^2B_2(2^{17})$, $A_1(2^{34})$		7
	3	2^{33}	$A_1(2^{33})$, $A_2(2^{11})$, ${}^2A_2(2^{11})$	$89 \mid 2^{11} - 1$	
	4	2^{32}	$B_2(2^8)$, $B_4(2^2)$, $A_1(2^{32})$	$17 = 2^4 + 1$	
	5	2^{31}	$A_1(2^{31})$		7
	6	2^{30}	${}^2B_2(2^{15})$, $G_2(2^5)$, $D_6(2)$, ${}^2D_6(2)$, $A_5(2^2)$, $A_1(2^{30})$, $A_2(2^{10})$, ${}^2A_2(2^{10})$, $A_3(2^5)$, ${}^2A_3(2^5)$, $A_4(2^3)$	$31 = 2^5 - 1$	
			${}^2A_5(2^2)$	$41 \mid 2^{10} + 1$	
			${}^2A_4(2^3)$	$19 \mid 2^9 + 1$	
	7	2^{29}	$A_1(2^{29})$		7
	8	2^{28}	$A_1(2^{28})$, $A_7(2)$, $B_2(2^7)$	$127 = 2^7 - 1$	
			${}^2A_7(2)$	$43 \mid 2^7 + 1$	
${}^2F_4(2)'$	2	2^{20}	$D_5(2)$, $B_2(2^5)$, $A_1(2^{20})$, $A_4(2^2)$	$31 = 2^5 - 1$	
			${}^2D_5(2)$	$17 = 2^4 + 1$	
			${}^2A_4(2^2)$	$41 \mid 2^{10} + 1$	
	3	2^{19}	$A_1(2^{19})$		5
	4	2^{18}	$A_1(2^{18})$, $A_2(2^6)$, $A_3(2^3)$, $G_2(2^3)$, ${}^2B_2(2^9)$	$73 \mid 2^9 - 1$	
			$B_3(2^2)$	$17 = 2^4 + 1$	
			${}^2A_2(2^6)$	$37 \mid 2^{18} + 1$	
			${}^2A_3(2^3)$	$19 \mid 2^9 + 1$	
	5	2^{17}	$A_1(2^{17})$		5
	6	2^{16}	$A_1(2^{16})$, $B_2(2^4)$, $B_4(2)$	$17 = 2^4 + 1$	
	7	2^{15}	$A_1(2^{15})$, $A_2(2^5)$, ${}^2A_2(2^5)$, $A_5(2)$	$31 = 2^5 - 1$	
			${}^2A_5(2)$	$11 \mid 2^5 + 1$	
	8	2^{14}	${}^2B_2(2^7)$, $A_1(2^{14})$	$127 = 2^7 - 1$	
B	2	2^{80}	$B_2(2^{20})$, $A_1(2^{80})$		7

			$D_5(2^4)$, ${}^2D_5(2^4)$, $A_4(2^8)$, ${}^2A_4(2^8)$	$257 = 2^8 + 1$	
			$B_4(2^5)$	$41 \mid 2^{10} + 1$	
	3	2^{79}	$A_1(2^{79})$		7
	4	2^{78}	${}^2B_2(2^{39})$, $A_1(2^{78})$, $A_2(2^{26})$, ${}^2A_2(2^{26})$, $A_3(2^{13})$, ${}^2A_3(2^{13})$, $A_{12}(2)$	$8191 = 2^{13} - 1$	
			${}^2A_{12}(2)$	$43 \mid 2^7 + 1$	
	5	2^{77}	$A_1(2^{77})$		7
	6	2^{76}	$B_2(2^{19})$, $A_1(2^{76})$		7
	7	2^{75}	$A_5(2^5)$, ${}^2A_5(2^5)$, $B_5(2^3)$, $A_1(2^{75})$	$151 \mid 2^{15} - 1$	
			$A_2(2^{25})$, ${}^2A_2(2^{25})$		13
	8	2^{74}	${}^2B_2(2^{37})$, $A_1(2^{74})$		7
	9	2^{73}	$A_1(2^{73})$		7
	10	2^{72}	$F_4(2^3)$, $G_2(2^{12})$, $E_6(2^2)$, ${}^3D_4(2^6)$, $D_4(2^6)$, ${}^2D_4(2^6)$, $D_9(2)$, $B_2(2^{18})$, $A_1(2^{72})$, $A_2(2^{24})$, $A_3(2^{12})$, $A_8(2^2)$	$73 \mid 2^9 - 1$	
			${}^2E_6(2^2)$, ${}^2D_9(2)$, $B_3(2^8)$, $B_6(2^2)$, ${}^2A_2(2^{24})$, ${}^2A_3(2^{12})$, ${}^2A_8(2^2)$	$257 = 2^8 + 1$	
	11	2^{71}	$A_1(2^{71})$		7

Thus, $a = 1$. In particular, $|S| = |T|^2 / p$ so we can get the value of $\lambda(S)$ for every possible T, p. A direct computation shows that, if T is one of the groups M, F_{3+}, F_3, Ly, F_5, Co_3, $O'N$, J_4, J_1, M_{23}, then $\lambda(S) < 1/3$ for every possible p, thus contradicting Proposition 28, so we can exclude those groups. Furthermore, the same computation shows that, if T is one of the groups Fi_{23}, Suz, He, McL, J_3, M_{11}, then p is not the dominant prime of T. For the remaining cases, S should be a simple group of Lie type: the groups satisfying these conditions are listed in Table 3.5, but we can see that all of them contradict the assumption that $|S|$, $|T|$ have the same prime divisors.

Table 3.5: Possible S for sporadic T when $a = 1$ in Proposition 61

T	p	$\lvert S\rvert_{p(S)}$	Possible S	Divisors of $\lvert S\rvert$, not of $\lvert T\rvert$	Divisors of $\lvert T\rvert$, not of $\lvert S\rvert$
M_{11}	$\neq 2$	2^8	$A_1(2^8)$, $B_2(2^2)$	$17 = 2^4 + 1$	
J_3	$\neq 3$	3^{10}	$A_1(3^{10})$, ${}^2A_4(3)$	$61 \mid 3^5 + 1$	
			$A_4(3)$	$13 \mid 3^3 - 1$	
He	$\neq 2$	2^{20}	$D_5(2)$, $B_2(2^5)$, $A_1(2^{20})$, $A_4(2^2)$	$31 = 2^5 - 1$	
			${}^2D_5(2)$	$11 \mid 2^5 + 1$	
			${}^2A_4(2^2)$	$41 \mid 2^{10} + 1$	
McL	$\neq 3$	3^{12}	$G_2(3^2)$, ${}^3D_4(3)$, $D_4(3)$, ${}^2D_4(3)$, $B_2(3^3)$, $A_1(3^{12})$, $A_2(3^4)$, $A_3(3^2)$	$13 \mid 3^3 - 1$	

			${}^2A_2(3^4)$	$41 \mid 3^4+1$	
			${}^2A_3(3^2)$	$73 \mid 3^6+1$	
Fi_{23}	$\neq 3$	3^{26}	$A_1(3^{26})$	$53 \mid 3^{26}+1$	
Suz	$\neq 2$	2^{26}	$A_1(2^{26})$, ${}^2B_2(2^{13})$	$53 \mid 2^{26}+1$	
Co_1	$\neq 2$	2^{42}	${}^2B_2(2^{21})$		3
			$D_7(2)$, ${}^2D_7(2)$	$31 = 2^5-1$	
			$G_2(2^7)$, $A_1(2^{42})$, $A_2(2^{14})$, ${}^2A_2(2^{14})$, $A_3(2^7)$, ${}^2A_3(2^7)$, $A_6(2^2)$	$43 \mid 2^7+1$	
			${}^2A_6(2^2)$	$113 \mid 2^{14}+1$	
	2	2^{41}	$A_1(2^{41})$	$83 \mid 2^{41}+1$	
HS	$\neq 2$	2^{18}	$G_2(2^3)$, ${}^2B_2(2^9)$, $A_1(2^{18})$, $A_2(2^6)$, $A_3(2^3)$	$73 \mid 2^9-1$	
			$B_3(2^2)$	$17 = 2^4+1$	
			${}^2A_2(2^6)$	$37 \mid 2^{18}+1$	
			${}^2A_3(2^3)$	$19 \mid 2^9+1$	
	2	2^{17}	$A_1(2^{17})$	$131071 = 2^{17}-1$	
M_{24}	$\neq 2$	2^{20}	$D_5(2)$, $B_2(2^5)$, $A_1(2^{20})$, $A_4(2^2)$	$31 = 2^5-1$	
			${}^2D_5(2)$	$17 = 2^4+1$	
			${}^2A_4(2^2)$	$41 \mid 2^{10}+1$	
	2	2^{19}	$A_1(2^{19})$	$524287 = 2^{19}-1$	
M_{12}	$\neq 2$	2^{12}	$G_2(2^2)$, ${}^3D_4(2)$, $D_4(2)$, ${}^2D_4(2)$, ${}^2A_2(2^4)$, ${}^2A_3(2^2)$	$17 = 2^4+1$	
			$B_2(2^3)$, $A_1(2^{12})$, $A_2(2^4)$, $A_3(2^2)$	$7 = 2^3-1$	
	2	2^{11}	$A_1(2^{11})$	$23 \mid 2^{11}-1$	
J_2	$\neq 2$	2^{14}	${}^2B_2(2^7)$, $A_1(2^{14})$	$127 = 2^7-1$	
	2	2^{13}	$A_1(2^{13})$	$8191 = 2^{13}-1$	
B	$\neq 2$	2^{82}	${}^2B_2(2^{41})$, $A_1(2^{82})$		7
	2	2^{81}	$B_3(2^9)$, $B_9(2)$, $A_1(2^{81})$, $A_2(2^{27})$, ${}^2A_2(2^{27})$	$73 \mid 2^9-1$	
Fi_{22}	$\neq 2$	2^{34}	${}^2B_2(2^{17})$, $A_1(2^{34})$		7
	2	2^{33}	$A_1(2^{33})$, $A_2(2^{11})$, ${}^2A_2(2^{11})$	$23 \mid 2^{11}-1$	
M_{22}	$\neq 2$	2^{14}	${}^2B_2(2^7)$, $A_1(2^{14})$	$127 = 2^7-1$	
	2	2^{13}	$A_1(2^{13})$	$8191 = 2^{13}-1$	
Ru	$\neq 2$	2^{28}	$A_1(2^{28})$, $A_7(2)$, $B_2(2^7)$	$127 = 2^7-1$	
			${}^2A_7(2)$	$43 \mid 2^7+1$	
	2	2^{27}	$B_3(2^3)$, $A_1(2^{27})$, $A_3(2^9)$, ${}^2A_3(2^9)$	$73 \mid 2^9-1$	
Co_2	$\neq 2$	2^{36}	${}^2F_4(2^3)$, $G_2(2^6)$, ${}^2E_6(2)$, ${}^3D_4(2^3)$, $D_4(2^3)$, ${}^2D_4(2^3)$, $B_2(2^9)$, $A_1(2^{36})$, $A_2(2^{12})$, $A_3(2^6)$, ${}^2A_8(2)$	$19 \mid 2^9+1$	
			$E_6(2)$, $A_8(2)$	$73 \mid 2^9-1$	
			$B_3(2^4)$, ${}^2A_2(2^{12})$	$241 \mid 2^{12}+1$	
			$B_6(2)$	$31 = 2^5-1$	
			${}^2A_3(2^6)$	$37 \mid 2^{18}+1$	

	2	2^{35}	$A_1(2^{35})$		7
${}^2F_4(2)'$	$\neq 2$	2^{22}	${}^2B_2(2^{11})$, $A_1(2^{22})$	$23 \mid 2^{11}-1$	
	2	2^{21}	$A_1(2^{21})$, $A_2(2^7)$, $A_6(2)$, ${}^2A_6(2)$	$7 = 2^3-1$	
			${}^2A_2(2^7)$	$43 \mid 2^7+1$	

□

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

Lemma 62. 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 26, 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 58, 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 32. We have

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

   We must have $\alpha_1 = k$. Moreover $\Phi_k(2) = 2^k - 1 = q$, as k is prime, and the multiplicity of $\Phi_k(2)$ in the factorization of $|S|$ is 2, so $\alpha_2 = \alpha_1$, contradicting Theorem 32 (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 $(q(q-1)(q-2))^2 = |S|\,q^a$, in particular $q^2 = q^a\,|S|_q$. As $|S|$ and $|T|$ have the same prime divisors, q must divide $|S|$, so $a = 1$, but then $|S| = q(q-1)^2(q-2)^2$ 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 62, Proposition 57 and Proposition 58 it follows:

Corollary 63. If $a \neq 1$, then p coincides with the characteristic and dominant primes of S and T.

Lemma 64. Let $\alpha_1(T), \alpha_1(S)$ be the greatest indexes in the cyclotomic decompositions of $|T|$ and $|S|$ described in Theorem 32. 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 32. 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 58 and $(p_T, \alpha_1(T)) = (2^k - 1, 2)$ by Lemma 62. 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 55. 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 $|S| \cdot p^a = |T|^2$ 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 59, 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 $|T|^2 = |S| \cdot p^a$ cannot be verified. □

Lemma 65. The characteristic p_S of S does not coincide with the prime p.

Proof. Suppose $p = p_S$. By Proposition 58, p coincides with the dominant prime of S, and consequently, since $|S| = |T|^2 \cdot p^a$, with the dominant prime of T; but then, by Lemma 62, p coincides also with the characteristic of T. By Lemma 64 and Theorem 32 (3), we get that $\alpha_1(T) = \omega(|T|)$ and $\alpha_1(S) = \omega(|S|)$. By Remark 31, $\omega(|S|) = \omega(|T|)$, so we conclude that $\alpha_1(T) = \alpha_1(S)$. Again by Lemma 64, 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 $|T|^2 = |S| \cdot p^a$. □

Proposition 66. $a = 1$.

Proof. Suppose $a \neq 1$: then, by Corollary 63, p is the characteristic and dominant prime of both S and T, contradicting Lemma 65. □

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 (see [24, Table 4.1]) whose order coincides with the denominator d_S of the cyclotomic factorization of the order of S. By Lemma 65, $p \neq p_S$, thus p divides d_S.

Lemma 67. If S, T have the same dominant prime u and $u \neq p$, then u coincides with the characteristic of T.

Proof. By Proposition 26, 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

$$((2^k - 1)2^k(2^{k-1} - 1))^2 = |S|\, p.$$

   By Proposition 58, the characteristic of S coincides with $u = 2$, hence, considering the cyclotomic factorization of $|S|$ described in Theorem 32, we have $\alpha_1(S) = k$ and $\Phi_k(2) = 2^k - 1 = q$. By Theorem 32 (1), $\Phi_k(2)$ divides $|S|$ with multiplicity 1, so necessarily $p = q$ by Remark 55. On the other hand, p divides d_S and, by Theorem 32 (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

$$q^2(q - 1)^2(q - 2)^2 = |S|\, p.$$

   By Proposition 58, 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

$$q^2(q - 1)^2(q - 2)^2 = |A_1(q^2)|2 = q^2(q^2 - 1)(q^2 + 1),$$

   whence $(q - 1)(q - 2)^2 = (q + 1)(q^2 + 1)$, but this is impossible.

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 68. S and T have different dominant primes.

Proof. Suppose that r is the dominant prime of S and T. Then, by Lemma 65, $r \neq p$ and therefore $|T|_r^2 = |S|_r$ and, by Remark 31, $\omega(S) = \omega(T)$. Moreover, by Lemma 64 and Theorem 32 (3), $\alpha_1(S) = \omega(S)$ and $\alpha_1(T) = \omega(T)$, whence $\alpha_1(S) = \alpha_1(T) = \alpha$. By Proposition 58 and Lemma 67, r is also the characteristic of both S and T. Again by Lemma 64, 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 $|S|p = |T|^2$, so we must have that $r = p$ and that p divides $|S|$ with multiplicity 1, in contradiction with Corollary 54 (6). □

Now we are ready to conclude our proof. We have reduced to the case $|T|^2 = p|S|$, where the dominant primes of T and S (which coincide with their characteristics) 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

$$p^t < r^h < p^{t+1}, \tag{3.17}$$

and consequently, since $t > 1$ by Corollary 54 (6),

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

thus p is a good contributor of S. By [6, 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. $A_1(r), A_2(r), {}^2A_2(r)$.

Nevertheless, we have already excluded the case $S =^2 A_3(2) \cong B_2(3)$ in Proposition 58; we can also exclude ${}^2A_4(2)$, ${}^2A_4(3)$, $B_3(2)$, $D_4(2)$, $G_2(3)$ by Corollary 54(6), as $d_S = 1$ for all of them; we can exclude $A_3(3)$, ${}^2A_3(3)$, ${}^2A_5(2)$, $B_3(3)$, $C_3(3)$, $D_4(3)$ by Remark 55, as there are at least two primes dividing their orders with odd multiplicity; we can exclude also ${}^2A_3(7)$, $B_2(5)$, $B_2(9)$ by Remark 55, as $43, 13, 41 \neq 2 = p$ rispectively divide their order with multiplicity 1; finally, if $S = B_2(7)$ then $|S|$ would be a square, thus contradicting $|T|^2 = |S|p$.
The only remaining cases are thus $A_1(r)$, $A_2(r)$, ${}^2A_2(r)$: the multiplicity of r in $|S|$ is respectively $1, 3, 3$ so, by Remark 55, in these three cases r is a square, $r = v^2$.
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 excludes 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 (3.17) we deduce $(v^2 - 1)_2 < v^2 < 2(v^2 - 1)_2$: if there is a prime $s \neq 2$ dividing $v^2 - 1$, it follows $v^2 < (v^2 - 1)(2/s) < v^2 - 1$, a contradiction, thus $v + 1$ and $v - 1$ are both powers of 2, the only possibility is $v = 3$, whence $S \cong A_1(9)$, 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 both divide $|S|$ with multiplicity 1. In the remaining case $M(S) = (3, v^2 - 1)$, so it must be $v^2 - 1 = 0 \mod 3$ 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 (3.17) 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.

3.4 Normally ζ-reversible groups with only alternating simple nonabelian images

In this section we will prove Conjecture 47 in the hypothesis that all the nonabelian simple composition factors of G are alternating. Once again, suppose G is a counterexample to the conjecture. It follows immediately from Theorem 51 that:

Proposition 69. 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. $|H| = |\operatorname{Alt}(m)|^2$.
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 $H/N \cong X \times \operatorname{Alt}(n)$; in the latter case $\pi(m!) = \pi(n!)$ i.e. there is no prime q with $m < q \leq n$.
4. Either N is abelian or $N \cong \operatorname{Alt}(u)^t$ 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 final contradiction. In particular, we will prove that H is non solvable (Proposition 70) and N is abelian (Proposition 71), thus H/N is not nilpotent and by Proposition 69.(3) there exist two subgroups X_1 and X_2 of H such that X_1/N is nilpotent, $X_2/N \cong \operatorname{Alt}(n)$ and $H/N \cong X_1/N \times X_2/N$; we will prove that N is not central in X_2 (Lemma 72) and, using Clifford's theory, we will find a contradiction.

Proposition 70. H is not solvable.

Proof. Suppose H is solvable: then it is not nilpotent by Theorem 51, but its quotients are all nilpotents by Lemma 48, as they cannot have nonabelian simple composition factors. Thus the unique minimal normal subgroup N is an elementary abelian p-group for some p and $H = N \rtimes A$, for some p'-group A with $A \leq \operatorname{Aut}(N)$ (see for example [47, Ex. 7, page 268]). Then, by Theorem 20, $|H| = |A| \cdot |N| \leq \dfrac{|N|^{1+\beta}}{2}$ with $\beta = \dfrac{\ln(32)}{\ln(9)}$, so

$$\frac{\ln(|H|)}{\ln(|N|)} \leq \frac{\ln(288)}{\ln(9)} - \frac{\ln(2)}{\ln(|N|)}. \tag{3.18}$$

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 [30, 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 (3.18). A direct computation shows that Equation (3.18) is false also in case $|H| = |\operatorname{Alt}(5)|^2$; moreover, Equation (3.18) is false in case $|H| = |\operatorname{Alt}(8)|^2$ if $p \neq 2$. Finally, if $|H| = |\operatorname{Alt}(8)|^2$, $|N| = |H|_2 = 2^{12}$, then $A \leq \operatorname{Aut}(C_2^{12})$, $|A| = 3^4 \cdot 5^2 \cdot 7^2$. Let $Q \in \operatorname{Syl}_5(A)$, then Q is an abelian Sylow subgroup of the nilpotent group of automorphisms A, so $Q \leq \operatorname{Z}(A)$, so $Q \leq \operatorname{End}(C_2^{12})^*$, in particular Q is cyclic. Hence there exists $g \in \operatorname{Aut}(C_2^{12})$ of order 25, its minimal polynomial divides $x^{25} - 1 = \Phi_{20}(x)\Phi_4(x)\Phi_1(x)$ and has degree at most 12, so it must be $\Phi_4(x)$, a contradiction with the order of g. □

Proposition 71. $N = \operatorname{soc} H$ is abelian (and thus H/N is not nilpotent).

Proof. Suppose by contradition 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. Now, notice that $C_H(N) \trianglelefteq N_H(N) = H$ and $C_H(N) \cap N = \operatorname{Z}(N) = \operatorname{Z}(L^t) = 1$, thus $C_H(N) = 1$ as N is minimal normal. Hence we have

$$L^t \cong N \triangleleft H = H/C_H(N) \leq \operatorname{Aut}(N) \cong \operatorname{Aut}(L) \wr \operatorname{Sym}(t);$$

recall that $\operatorname{Aut}(\operatorname{Alt}(u)) = \operatorname{Sym}(u)$ for $u \neq 6$, $\operatorname{Aut}(\operatorname{Alt}(6)) = \operatorname{Sym}(6).C_2$ (see for example [8]), so

$$\begin{cases} \operatorname{Alt}(u)^t \triangleleft H \leq \operatorname{Sym}(u) \wr \operatorname{Sym}(t) & \text{if } u \neq 6 \\ \operatorname{Alt}(6)^t \triangleleft H \leq (\operatorname{Sym}(6).C_2) \wr \operatorname{Sym}(t) & \text{if } u = 6. \end{cases} \tag{3.19}$$

If $t = 1$, then by (3.19) we have $|\operatorname{Alt}(m)|^2 = |H| = 2^j \cdot u!$, for some j, but by Lemma 18 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 69 we can write $H/N = X_1/N \times X_2/N$, where X_1/N is nilpotent and X_2/N is either 1 or $S \cong \operatorname{Alt}(n)$ 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 18, we can find two primes p, q as follows:

$$\begin{cases} \dfrac{n}{2} < p < q \leq n & \text{if } X_2/N \cong \operatorname{Alt}(n); \\ \dfrac{m}{2} < p < q \leq n & \text{if } X_2/N = 1. \end{cases} \tag{3.20}$$

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 $t > 2$, 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. Furthermore, $H/N \leq Aut(N)/N \cong Aut(L^t)/Inn(L^t) \cong Out(L^t) = Out(L) \wr S_t$. As $\operatorname{Aut}(L)$ is a 2-group, there exists a group M such that $N \leq M \trianglelefteq H$, M/N is a 2-group, $H/M \leq S_t$. In particular, H/M is transitive: suppose it has an orbit $\Omega \subsetneq \{1, \cdots, t\}$, then $N_\Omega = \prod_{i \in \Omega} L_i \trianglelefteq H$, contradicting the minimal normality of $N \cong L^t$. Now, as $|H/N|_{2'} = |H/M|_{2'} \cdot |M/N|_{2'} = |H/M|_{2'}$, then $|H/M|_p = p^2$ and $|H/M|_q = q^2$; then, recalling that $H/M = X_1M/M \times X_2M/M$, it is easy to see that

$|X_2M/M|_{p,q}$ divides $|X_2/N|_{p,q}$, which divides $p \cdot q$. This implies $p \cdot q$ must divide order of the nilpotent group X_1M/M, so $p \cdot q$ also divides the order of its center, and furthermore it divides $|Z(H/M)|$. Now, $Z(H/M)$ is semiregular by Lemma 23, so we can find this bound for t:

$$t = \left|H/M : \mathrm{Stab}_{H/M}(x)\right| \geq \left|Z(H/M) : \mathrm{Stab}_{Z(H/M)}(x)\right| = |Z(H/M)| \geq p \cdot q.$$

Furthermore, we find that

$$60^{\frac{m^2}{4}} \leq 60^{p \cdot q} \leq |L|^t \leq |H| = (m!)^2 \leq m^{2m}, \tag{3.21}$$

and it is easy verify that this is false for all $m \geq 5$, a contradiction.
We are still left the two cases in which we have not defined p, q. If $m = 6$ or $n = 6$ (so $m \leq 6$), then by Equation (3.19) $|\operatorname{Alt}(u)|^3$ divides $|Alt(6)|^2$, whence $\operatorname{Alt}(u)$ is not divisible by 5, a contradiction. If $m = 10$ or $n = 10$, then we can choose $p = 7$, analogously to the previous case we have $p \leq t$ and $|H/N| \geq |H/M| \geq t \geq 7$, thus

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

which leads again to a contradiction.
So N is abelian, whence X_2/N cannot be trivial, otherwise H would be solvable, contradicting Proposition 70. □

Combining Proposition 69 with Lemma 70 and Lemma 71, we can conclude that there exist 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. $X_2/N \cong \operatorname{Alt}(n)$.
4. N is an elementary abelian p-group.

Lemma 72. *N is not central in X_2.*

Proof. Assume, by contradiction, $N \leq Z(X_2)$. Notice that $\operatorname{Frat}(X_2)$ is a nilpotent normal subgroup of H, so either $\operatorname{Frat}(X_2) = 1$ or $\operatorname{Frat}(X_2) = N$.
In the first case, we would have $X_2 = N \times S$, with $S \cong \operatorname{Alt}(n)$. But then S would be normal in H, against the fact that N is the unique minimal normal subgroup of G. If $\operatorname{Frat}(X_2) = N$, then X_2 is a perfect central extension of N, so in particular $|N|$ divides the order of the Schur multiplier of $\operatorname{Alt}(n)$, 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 18, there exists a prime dividing $n!$ with multiplicity 1. □

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

Proposition 73. $n \leq 8$.

Proof. Suppose $n \geq 9$: by Lemma 21 and Lemma 22, the dimension of a non-trivial 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

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

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 $\mathrm{Aut}\, N$. 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 $|N| \cdot |\mathrm{Alt}(n)|$ divides $|H| = \left(\frac{m!}{2}\right)^2$ (i.e. $2|N|n!$ divides $(m!)^2$). This means that N is a completely reducible $\mathrm{Alt}(n)$-module of relatively small order. Furthermore, we will use some bounds to the degrees of representations classified in [31], [52] and [53] to determine the minimal values for the dimesions of N as S-module.

- Suppose $m = n = 8$: then $|N|$ divides $20160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$; the minimal dimension for $3, 5, 7$ is 7, for 2 it is 4, thus $|N| = 2^r$ for $4 \leq r \leq 6$. On the other hand, $\mathrm{Alt}(8)$ has no irreducible representation of degree 5 on C_2, thus N can be written as a $C_2 A_8$-module as $N = M_1 \oplus \cdots \oplus M_t$ with $M_1 \in \{4, 6\}$. As $\dim_{C_2} N \leq 6$, we must have $\dim_{C_2} M_i \leq 2$ for every $i \geq 2$, in particular $N^* = M_2 \oplus \cdots \oplus M_t \leq Z(X)$, therefore $N^* \triangleleft H$, and the only possibility is $N^* = 1$, that is $N = M_1$.
  Suppose $|N| = 2^6$, then

$$|X_1/N| = \frac{|H/N|}{|X_2/N|} = \frac{|H|}{|X_2/N| \cdot |N|} = 3^2 \cdot 5 \cdot 7.$$

Furthermore, analogously to the case $n \geq 9$, $X_1 = N \rtimes K$, for odd $|K|$; $C_K(N)$ is normal in $N_K(N) = K$ and does commute with N, so $C_K(N) \trianglelefteq N \rtimes K = X_1$. Suppose $C_K(N) \neq 1$, then

$$1 \neq C_K(N) \leq O_{2'}(X_1) \operatorname{char} X_1 \trianglelefteq H,$$

in particular $O_{2'}(X_1) \trianglelefteq H$, against the unicity of N as minimal normal subgroup; thus $C_K(N) = 1$, whence $C_{X_1}(N) = N$. Then $GL(6,2)$ should contain an element of order $3 \cdot 5 \cdot 7$, but this is false, as can be easily verified.
The remaining case is $|N| = 2^4$, then

$$|X_1/N| = \frac{|H/N|}{|X_2/N|} = \frac{|H|}{|X_2/N| \cdot |N|} = 2^2 \cdot 3^2 \cdot 5 \cdot 7;$$

X_1/N is nilpotent, so it is the direct product of its Sylow subgroups, in particular it contains a subgroup X_1^*/N of order $3^2 \cdot 5 \cdot 7$ such that $X_1^*/N \operatorname{char} X_1/N \triangleleft H$, thus $X_1^*/N \triangleleft H$. Analogously to the previous case, we can prove $C_{X_1^*}(N) = N$. then $GL(4,2)$ should contain an element of order $3 \cdot 5 \cdot 7$, false again.

- Suppose $m = 7, n = 8$: then $|N|$ divides $315 = 3^2 \cdot 5 \cdot 7$, while the minimal dimension for $3, 5, 7$ is 7, a contradition.
- Suppose $m = n = 7$: then $|N|$ divides $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$, but the minimal dimension for 2 is 4, for $3, 5, 7$ they are $3, 4$, a contradiction.
- Suppose $m = n = 6$: then $|N|$ divides $360 = 2^3 \cdot 3^2 \cdot 5$, the minimal dimension for 2 is 4, thus $|N| = 3^2$, so we have a faithful action of A_6 on the solvable group $GL(2,3)$, a contradiction.
- Suppose $m = 5, n = 6$: then $|N|$ divides $10 = 2 \cdot 5$, but it cannot have dimension 1, a contradiction.
- Suppose $m = n = 5$: then $|N|$ divides $60 = 2^2 \cdot 3 \cdot 5$, it cannot have dimension 1 so $|N| = 4$, but $GL(2,2)$ has no element of order 5, a contradiction again.

Chapter 4

ζ-reversible and normally ζ-reversible pro-p groups

4.1 General results for normally ζ-reversible groups

The evidence we have found in the previous chapter gives us sufficient motivation to focus on finitely generated pro-p groups, as classifying normally ζ-reversible pro-p groups is the key to determine a classification of pronilpotent groups with this property. With this purpose, in this chapter we will try to extend some results on ζ-reversible groups reported in [10].

From now on, let G be a finitely generated profinite group and let $\mathcal{L}^{\triangleleft}(G) \subseteq \mathcal{L}(G)$ be the lattice of all open normal subgroups of G.

Moreover, for $H \trianglelefteq_O G$, we can consider the lattice $\mathcal{L}(H)$ of all open subgroups of H and hence define $\mathcal{L}^G(H) := \mathcal{L}^{\triangleleft}(G) \cap \mathcal{L}(H)$ as the poset of all open normal subgroups of G which are contained in H. It is a lattice, so there is a Möbius function μ^G associated to it. Thus we are able to define $b_n^G(H) = \sum_{K \leq_O H, K \trianglelefteq_O G, |H:K|=n} \mu^G(K,H)$ and hence

$$p_H^G(s) = \sum_n \frac{b_n^G(H)}{n^s}.$$

Notice that $b_n^G(G) = b_n^{\triangleleft}(G)$ for all $n \in \mathbb{N}$ and $p_G^G(s) = p_G^{\triangleleft}(s)$. By Crapo's Closure Theorem, $\mu^G(\cdot, H)$ has nonzero values only on intersections of maximal elements of $\mathcal{L}^G(H)$: let H^* be the intersection of all maximal elements in $\mathcal{L}^G(H)$, then

$$\mu^G(K,H) = \begin{cases} \mu^{G/H^*}(K/H^*, H/H^*) & \text{if } H^* \leq K, \\ 0 & \text{otherwise.} \end{cases} \tag{4.1}$$

Notice that Equation (4.1) implies in particular:

Proposition 74. Let $H \in \Omega$, then $p_H^G(s) = p_{H/H^*}^{G/H^*}(s)$.

In [10] it is proved that a finitely generated profinite group G is ζ-reversible

if and only if

$$\sum_{m|n}\left(\sum_{|G:H|=m} b_{n/m}(G)-b_{n/m}(H)\right)=0$$

for all $n\in\mathbb{N}$. Furthermore, as a consequence, it is stated that, if $p_H(s)=p_G(s)$ for all $H\leq_O G$, then G is ζ-reversible. In this section, we will essentially adapt the main results in section 1 of [10] to the normal case, slightly changing some arguments, to achieve similar results for normally ζ-reversible groups.

Proposition 75. Consider the Dirichlet series $K_G^{\triangleleft}(s)=\sum_n \frac{k_n^{\triangleleft}}{n^s}$, with

$$k_n^{\triangleleft}=\sum_{m|n}\left(\sum_{H\trianglelefteq_O G,|G:H|=m} b_{n/m}^G(G)-b_{n/m}^G(H)\right).$$

Then G is normally ζ-reversible if and only if $k_n^{\triangleleft}=0$ for all $n\in\mathbb{N}$.

Proof. Consider the Dirichlet series $\sum_n \frac{\rho_n^{\triangleleft}}{n^s}$, with

$$\rho_n^{\triangleleft}=\sum_{m|n}\left(\sum_{H\trianglelefteq_O G,|G:H|=m} b_{n/m}^G(H)\right).$$

Then, we have

$$\rho_n^{\triangleleft}=\sum_{m|n}\left(\sum_{H\trianglelefteq_O G,|G:H|=m}\left(\sum_{K\leq_O H,K\trianglelefteq_O G,|H:K|=n/m}\mu^G(K,H)\right)\right)$$

$$=\sum_{K\trianglelefteq_O G,|G:K|=n}\left(\sum_{H\trianglelefteq_O G:K\leq_O H}\mu^G(K,H)\right)=\begin{cases}1 & \text{if } n=1,\\ 0 & \text{if } n\neq 1.\end{cases}$$

Now consider the Dirichlet series $\sum_n \frac{\tau_n^{\triangleleft}}{n^s}$, with

$$\tau_n^{\triangleleft}=\sum_{m|n}\left(\sum_{H\trianglelefteq_O G,|G:H|=m} b_{n/m}^G(G)\right)=\sum_{m|n} b_{n/m}^{\triangleleft}(G)a_m^{\triangleleft}(G).$$

Notice that G is normally ζ-reversible if and only if $\tau_1^{\triangleleft}=1$ and $\tau_n^{\triangleleft}=0$ for all $n>1$, i.e. if and only if $k_n^{\triangleleft}=\tau_n^{\triangleleft}-\rho_n^{\triangleleft}=0$ for all $n\in\mathbb{N}$, i.e. if and only if

$$\sum_{m|n}\left(\sum_{H\trianglelefteq_O G,|G:H|=m} b_{n/m}^G(G)-b_{n/m}^G(H)\right)=0 \tag{4.2}$$

for every $n\in\mathbb{N}$.

□

From Proposition 75 another result easily arises:

Proposition 76. If $p_G^{\triangleleft}(s) = p_H^G(s)$ for every $H \in \Omega$, then G is normally ζ-reversible.

Moreover, for $H \trianglelefteq_O G$ we can consider the Dirichlet series

$$K_{G,H}^{\triangleleft}(s) = \frac{p_G^G(s) - p_H^G(s)}{|G:H|^s} = \sum_n \frac{d_n^{\triangleleft}(H)}{n^s}$$

and, as $a_n^{\triangleleft}(G)$ is finite for every n, we can get another well defined Dirichlet series:

$$K_{G,m}^{\triangleleft}(s) = \sum_{H \trianglelefteq_O G, |G:H| \leq m} K_{G,H}^{\triangleleft}(s) = \sum_n \frac{k_{m,n}^{\triangleleft}}{n^s}.$$

From a first confront between the first summands of $K_G^{\triangleleft}(s)$ and $K_{G,m}^{\triangleleft}(s)$, for a fixed m, it is clear that $k_{m,n}^{\triangleleft} = k_n^{\triangleleft}$ for every $n \leq m$: as a consequence, if G is normally ζ-reversible, then $k_{m,n}^{\triangleleft} = \sum_{H \trianglelefteq_O G, |G:H| \leq m} d_n^{\triangleleft}(H) = 0$ for $n \leq m$.
Clearly, by its definition $d_n^{\triangleleft}(H) = 0$ if n does not divide $|G:H|$, and $d_1^{\triangleleft}(H) = d_{|G:H|}^{\triangleleft}(H) = 0$: therefore, considering the case $m = n$, we can state:

Proposition 77. If G is normally ζ-reversible, then $\sum_{H \in \Delta_m^{\triangleleft}} d_m^{\triangleleft}(H) = 0$, where $\Delta_m^{\triangleleft}$ is the set of all proper open subgroups $H \trianglelefteq_O G$, $H \neq G$ whose index is a proper divisor of m.

Now, analogously to the approach followed in [10], we would like to prove that the converse of the second statement of Proposition 76 holds:

Conjecture 78. G is normally ζ-reversible if and only if $p_G^{\triangleleft}(s) = p_H^G(s)$ for every $H \trianglelefteq_O G$.

This would give us a further condition to use in order to characterize normally ζ-reversible groups. Obviously, for an abelian G, normal ζ-reversibility and ζ-reversibility coincide, furthermore $p_G^{\triangleleft}(s) = p_G(s)$ and $p_H^G(s) = p_H(s)$. In this case, we get from proposition 75 some ζ-reversible examples like $\mathbb{Z}_p$, $\hat{\mathbb{Z}}$ and their products.
Furthermore, we can easily get some local results on the subgroups of small index of normally ζ-reversible groups.
Let G be a normally ζ-reversible group, let p be a prime dividing the order of G as a supernatural number with multiplicity at least 2: then equation (4.2) implies (choosing $n = p^2$)

$$\sum_{m|p^2} \left(\sum_{H \trianglelefteq_O G, |G:H|=m} b_{p^2/m}^G(G) - b_{p^2/m}^G(H) \right) = 0 \tag{4.3}$$

It is easy to see that the summands corresponding to $m \in \{1, p^2\}$ have sum 0, thus equation (4.3) becomes

$$\sum_{H \trianglelefteq_O G, |G:H|=p} b_p^G(G) - b_p^G(H) = 0$$

$$\sum_{H\trianglelefteq_O G,|G:H|=p}\left(\sum_{K\trianglelefteq_O G,|G:K|=p}\mu^G(K,G)-\sum_{L\trianglelefteq_O H,L\trianglelefteq_O G,|H:L|=p}\mu^G(L,H)\right)=0$$

$$\sum_{H\trianglelefteq_O G,|G:H|=p}\left(\sum_{K\trianglelefteq_O G,|G:K|=p}(-1)-\sum_{L\trianglelefteq_O H,L\trianglelefteq_O G,|H:L|=p}(-1)\right)=0$$

$$a_p^{\triangleleft}(G)^2=\sum_{H\trianglelefteq_O G,|G:H|=p}\ \sum_{L\trianglelefteq_O H,L\trianglelefteq_O G,|H:L|=p}1$$

Let us define $[p-p]_G:=|\{(H,L):L\triangleleft_O H\triangleleft_O G,L\triangleleft_O G,|H:L|=|G:H|=p\}|$, so that we can write equation (4.3) as

$$a_p^{\triangleleft}(G)^2=[p-p]_G. \tag{4.4}$$

Now we are interested in estimating $[p-p]_G$, so let $L\triangleleft_O G$, with $|G:L|=p^2$: then G/L is isomorphic to C_p^2 or C_{p^2}. In particular, we can choose L in $a_{p^2}^{\triangleleft}(G)=q_1(p,G)+q_2(p,G)$ different ways, where $q_1(p,G):=|\{L\triangleleft_O G:G/L\cong C_{p^2}\}|$ and $q_2(p,G):=|\{L\triangleleft_O G:G/L\cong C_p^2\}|$.
If $G/L\cong C_{p^2}$, there is a unique possible H such that $L\triangleleft_O H\triangleleft_O G,L\triangleleft_O G,|H:L|=|G:H|=p$; if $G/L\cong C_p^2$, it is easy to see that there are $p+1$ possibilities for H: we can thus rewrite equation (4.4) as

$$a_p^{\triangleleft}(G)^2=[p-p]_G=q_1(p,G)+(p+1)q_2(p,G).$$

We want now to determine the values of $q_1(p,G),q_2(p,G)$, to describe more precisely the subgroup growth of G. With the usual notation, let $N(G)$ be the intersection of all maximal normal subgroups of G and let n be the multiplicity of C_p as a simple composition factor of $G/\mathcal{N}(G)$. Then,

$$\zeta_{G,p}^{\triangleleft}=\left(p_{G,p}^{\triangleleft}\right)^{-1}=\prod_{i=0}^{n-1}\left(1-\frac{p^i}{p^s}\right)^{-1}=\prod_{i=0}^{n-1}\left(1+\frac{p^i}{p^s}+\frac{p^{2i}}{p^{2s}}+\cdots\right).$$

We can now easily compute the coefficient $a_{p^2}^{\triangleleft}(G)$:

$$a_{p^2}^{\triangleleft}(G)=\sum_{i=0}^{n-1}p^{2i}+\sum_{j=0}^{n-1}\sum_{k=j+1}^{n-1}p^j\cdot p^k=\frac{p^{2n}-1}{p^2-1}+\sum_{j=0}^{n-1}p^j\cdot p^{j+1}\cdot\sum_{k=0}^{n-j-2}p^k$$

$$=\frac{p^{2n}-1}{p^2-1}+\sum_{j=0}^{n-1}p^{2j+1}\frac{p^{n-j-1}-1}{p-1}=\frac{p^{2n}-1}{p^2-1}+\frac{1}{p-1}\left(\sum_{j=0}^{n-1}p^{n+j}-\sum_{j=0}^{n-1}p^{2j+1}\right)$$

$$=\frac{p^{2n}-1}{p^2-1}+\frac{p^n}{p-1}\cdot\frac{p^n-1}{p-1}-\frac{p}{p-1}\frac{p^{2n}-1}{p^2-1}=\frac{(p^{n+1}-1)(p^n-1)}{(p+1)(p-1)^2}.$$

Finally,

$$\begin{cases}q_1(p,G)+(p+1)q_2(p,G)=\left(a_p^{\triangleleft}(G)\right)^2=\left(\dfrac{p^n-1}{p-1}\right)^2\\ q_1(p,G)+q_2(p,G)=a_{p^2}^{\triangleleft}(G)=\dfrac{(p^{n+1}-1)(p^n-1)}{(p+1)(p-1)^2},\end{cases}$$

whence

$$\begin{cases} q_1(p,G) = p^{n-1}\dfrac{p^n-1}{p-1} \\ q_2(p,G) = \dfrac{(p^n-1)(p^{n-1}-1)}{(p+1)(p-1)^2}. \end{cases}$$

Summing up the results in this section:

Theorem 79. Let G be a normally ζ-reversible group, let p be a prime such that p^2 divides $|G|$ as a supernatural number. Let n be the multiplicity of C_p as a simple composition factor of $G/\mathcal{N}(G)$. Then:

1. G has $p^{n-1}\dfrac{p^n-1}{p-1}$ open normal subgroups of index p^2 with cyclic quotient;
2. G has $\dfrac{(p^n-1)(p^{n-1}-1)}{(p-1)^2(p+1)}$ open normal subgroups of index p^2 with non-cyclic quotient.

4.2 Normally ζ-reversible pro-p groups

In this section we want to determine sufficient conditions on pro-p groups to be normally ζ-reversible: in particular, we would like to investigate when a pro-p group G has the property that $p_G^{\triangleleft}(s) = p_H^G(s)$ for every $H \leq_O G$, so that we can apply Proposition 75.

Definition 80. Let $H \trianglelefteq G$ and consider a subset $T \subset H$: we will say that T is a G-normal generating set of H if the minimal normal subgroup of H containing T and normal in G is $\langle T \rangle^G = H$. We will define $d_G(H)$ as the minimal cardinality of a G-normal generating set of H.

Lemma 81. Let G be a finitely generated pro-p group, $H \trianglelefteq_O G$. Then

(i) $p_G^{\triangleleft} = p_H^G$ if and only if $d_G(H) = d(G)$;

(ii) $d_G(H) = d\left(\dfrac{H}{[H,G]}\right)$.

Proof. Let us start by proving (i). Let M be a open maximal G-invariant subgroup of H: then, H/M is a minimal normal subgroup of G/M, therefore $H/M \leq \mathrm{Z}(G/M)$, $H/M \cong C_p$. In particular $[H/M, G/M] = 1$ (thus $[H,G] \leq M$) and $H^p \leq M$. Consider now the intersection H^* of all open maximal G-invariant subgroups of H: we have proved that $\hat{H} := [H,G]H^p \leq H^*$.
Now, $\hat{H} \trianglelefteq G$ and $H/\hat{H}$ is elementary abelian, as $H^pH' \leq \hat{H}$; moreover, as $\hat{H}$ contains all commutators in $[H,G]$, G centralizes $H/\hat{H}$. We claim that $H^* \leq \hat{H}$. Let $H/\hat{H} \cong C_p^n$, then $H/\hat{H}$ has n maximal normal subgroups $K_i/\hat{H}$ with trivial intersection; G centralizes $K_i/\hat{H}$, thus $K_1, \cdots, K_n$ are maximal G-invariant subgroups of H with intersection $\hat{H}$: in particular $H^* \leq \hat{H}$, whence we can conclude $H^* = \hat{H} = [H,G]H^p$.
Now we can show that $d_{G/H^*}(H/H^*) = d_G(H)$. Let $\langle h_1, \cdots, h_d \rangle^G H^* = G$, suppose by contradiction $\langle h_1, \cdots, h_d \rangle^G \neq G$, then there exists an open maximal G-invariant subgroup $M \leq H$ such that $\langle h_1, \cdots, h_d \rangle^G \leq M$, but then

$\langle h_1, \cdots, h_d \rangle^G H^* \leq MH^* = M$, a contradiction.
Now, by Proposition 74, $p_H^G(s) = p_{H/H^*}^{G/H^*}(s)$; moreover, we have seen that G/H^* acts trivially on H/H^*, thus $p_{H/H^*}^{G/H^*}(s) = p_{H/H^*}(s)$; therefore,

$$p_H^G(s) = p_{H/H^*}(s) = p_{C_p^{d_G(H)}}(s) = \prod_{i=0}^{d_G(H)-1} \left(1 - \frac{p^i}{p^s}\right)$$

and, as $p_G^{\triangleleft}(s) = \prod_{i=0}^{d(G)-1} \left(1 - \frac{p^i}{p^s}\right)$, the conclusion easily follows.
Finally, to prove (ii), notice that

$$d_G(H) = d\left(\frac{H}{H^p[H,G]}\right) = \log_p \left|\frac{H}{H^p[H,G]}\right| = \log_p \left|\frac{H}{[H,G]} : \frac{H^p[H,G]}{[H,G]}\right| = d\left(\frac{H}{[H,G]}\right).$$

□

Theorem 82. If G is a finitely generated pro-p group, then the following are equivalent.

(i) $p_G^{\triangleleft} = p_H^G$ for every $H \trianglelefteq_O G$;

(ii) $d_G(H) = d(G)$ for every $H \trianglelefteq_O G$;

(iii) $G \cong \mathbb{Z}_p^n$ for some n.

Proof. The equivalence between (i) and (ii) is an immediate consequence of Lemma 81; moreover, it is trivial to see that (iii) implies (ii), so we only need to show that the converse is true.
First, we will prove that, if $d_G(H) = d(G)$ for every open normal subgroup H of G, then the abelian part G/G' of G is torsion free. Suppose by contradiction that $\{x_1, \cdots, x_r\}$ is a generating set of G/G' and x_1 has finite order, say p^k, let N/G' be the subgroup generated by all $\{x_2, \cdots, x_r\}$. Now, G/N is cyclic, so $G' = [G, N]$; then, by Lemma 81(ii),

$$d_G(N) = d\left(\frac{N}{[N,G]}\right) = d\left(\frac{N}{G'}\right) = d\left(\frac{G}{G'}\right) - 1 < d(G),$$

a contradiction.
Suppose now that $G' \neq 1$. Then, $\gamma_3(G) = [G', G]$ must be a proper subgroup of G' (otherwise the lower central series of G would stop before getting to the trivial group); let $M/\gamma_3(G)$ be a maximal subgroup of the abelian group $G'/\gamma_3(G)$, then clearly $G'/M \cong C_p$. Define $Q = \Phi(G) = G^p[G, G]$: first notice that $[Q, G] = [G^p, G][G', G]$ and, by Hall-Petresco's formula (see [26], [44]), $[G^p, G] \leq [G, G]^p \gamma_{p+1}(G)$. Finally, $\gamma_{p+1}(G) \leq \gamma_3(G) \leq M$ and $[G, G]^p \leq M$ (as $|G' : M| = p$), thus we get

$$[Q, G] = [G^p, G]\gamma_3(G) \leq [G, G]^p \gamma_{p+1}(G)\gamma_3(G) \leq M.$$

This implies in particular that there is a projection $\frac{Q}{[Q,G]} \to \frac{Q}{M}$, so we must have

$$d\left(\frac{Q}{[Q,G]}\right) \geq d\left(\frac{Q}{M}\right). \tag{4.5}$$

Now, as G/G' is torsion free, then $G/G' \cong \mathbb{Z}_p^k$, with $k = d(G)$: moreover,

$$\frac{Q}{G'} = \frac{G^p[G,G]}{[G,G]} = \left(\frac{G}{[G,G]}\right)^p \cong \bigoplus_{i=1}^{k} \mathbb{Z}_p.$$

Consider now the short exact sequence

$$0 \to \frac{G'}{M} \xrightarrow{\epsilon} \frac{Q}{M} \xrightarrow{\pi} \frac{Q}{G'} \to 0 : \tag{4.6}$$

we have shown $\dfrac{Q}{G'}$ is a free $\mathbb{Z}_p$-module, in particular it is projective, so the short exact sequence (4.6) splits and thus $\dfrac{Q}{M} = \dfrac{G'}{M} \oplus \dfrac{Q}{G'}$ as $\mathbb{Z}_p$-modules. Using this result together with Equation (4.5), we get

$$d_G(Q) = d\left(\frac{Q}{[Q,G]}\right) \geq d\left(\frac{Q}{M}\right) = d\left(\frac{G'}{M}\right) + d\left(\frac{Q}{G'}\right) = 1 + d(G), \tag{4.7}$$

a contradiction. □

Notice that, by Theorem 82, for pro-p groups Conjecture 78 becomes:

Conjecture 83. A profinite pro-p group G is normally ζ-reversible if and only if $G \cong \mathbb{Z}_p^n$ for some $n \in \mathbb{N}$.

We can state the following result:

Lemma 84. Let G be a finitely generated pro-p group. Then the following are equivalent:

(i) G is normally ζ-reversible;

(ii) G has the same normal subgroup ζ function as $\mathbb{Z}_p^{d(G)}$;

(iii) G has the same normal subgroup growth as a finitely generated torsion free abelian pro-p group.

Proof. To see that (i) is equivalent to (ii) it is sufficient to see that

$$p_G^{\triangleleft}(s) = p_G(s) = \prod_{0 \leq i \leq d(G)-1} \left(1 - \frac{p^i}{p^s}\right) = \left(\zeta^{\triangleleft}_{\mathbb{Z}_p^{d(G)}}(s)\right)^{-1},$$

so G is normally ζ-reversible if and only if

$$\zeta_G^{\triangleleft}(s) = \left(p_G^{\triangleleft}(s)\right)^{-1} = \zeta^{\triangleleft}_{\mathbb{Z}_p^{d(G)}}(s).$$

It is trivial to see that (ii) implies (iii); to prove that the converse holds it suffices to see that, if there exists $d \in \mathbb{N}$ such that G and $\mathbb{Z}_p^d$ have the same normal subgroup growth, then

$$\frac{p^{d(G)} - 1}{p - 1} = b_p^{\triangleleft}(G) = b_p^{\triangleleft}(\mathbb{Z}_p^d) = \frac{p^d - 1}{p - 1},$$

thus $d(G)$=d. □

Now we need some preliminary results.

Definition 85. Let G be a pro-p group. Then $N \leq G$ is powerfully embedded in G if p is odd and $[N, G]$ is a subgroup of the topological closure of N^p or $p = 2$ and $[N, G]$ is a subgroup of the topological closure of N^4.
A pro-p group G is called powerful if it is powerfully embedded in itself.
A finitely generated torsion-free powerful pro-p group is called uniform.
Analogously, a $\mathbb{Z}_p$-lattice L (i.e. a lattice whose points are uples of elements of $\mathbb{Z}_p$) is powerful if p is odd and $[L, L] \subseteq pL$ or $p = 2$ and $[L, L] \subseteq 4L$.

Powerful pro-p groups can be seen as a generalization of abelian pro-p groups and they have some really useful properties: two important results are the following (see for example [29]).

Lemma 86. Quotients of powerful pro-p groups are powerful. The derived group of a powerful pro-p group is powerfully embedded in it.

Proposition 87 (Shalev's Interchanging Property)**.** Let N, M be powerfully embedded in a pro-p group G. Then $[N, M^p] = [N, M]^p = [N^p, M]$ if $p > 2$, $[N, M^4] = [N, M]^4 = [N^4, M]$ if $p = 2$.
In particular, if G is a powerful pro-p group, then $[G, G^p] = [G, G]^p$ if $p > 2$, $[G, G^4] = [G, G]^4$ if $p = 2$.

We recall that the rank of a profinite group G is defined as $\mathrm{rk}(G) = \sup_{H \leq G} d(H)$; it can be proved that, if G is a pro-p group of finite rank, then it contains an open unifom subgroup U, and every U with such property has the same number of generators. This allows us to present a new invariant, which we call the dimension of G, defined as $\dim(G) := d(U)$: clearly, $\dim(G) \leq \mathrm{rk}(G)$.
Lazard proved in [35] that if G is a uniform group, then every element $x \in G_{n+1} = G^{p^n}$ admits a unique p^nth root in G, which we can denote by $x^{p^{-n}}$. Moreover, G can be equipped with the structure of a Lie algebra via the operations

$$x + y := \lim_{n \to \infty} \left(x^{p^n} y^{p^n} \right)^{p^{-n}},$$

$$[x, y]_{\mathrm{Lie}} := \lim_{n \to \infty} [x^{p^n}, y^{p^n}]^{p^{-2n}},$$

and with the structure of an associative algebra with the product given by the Hausdorff Formula,

$$\Phi(x, y) := \log(\exp(x) \cdot \exp(y)).$$

The original group operation $\cdot$ coincides with Φ on all G and with $+$ on all abelian subgroups of G: furthermore, if $\{g_1, \cdots, g_d\}$ is a minimal set of generators for the group G, then $(G, +)$ constitutes a free $\mathbb{Z}_p$-module whith basis $\{g_1, \cdots, g_d\}$. To avoid confusion, we will denote by $L(G)$ the set G equipped with the Lie algebra structure: $L(\cdot)$ is an isomorphism between the category of uniform pro-p groups and the category of powerful $\mathbb{Z}_p$-lattices.
A crucial role in this correspondence is played by the saturable subgroups of G. Saturable pro-p groups were first introduced by Lazard in [35]: here we present the equivalent definition provided by González-Sánchez in [21].

Definition 88. Let G be a finitely generated pro-p group. We say that G is p-valued if there exists a map $\omega : G \to \mathbb{R}_{>0} \cup \{\infty\}$, which we call valuation, such that the following properties hold for all $x, y \in G$:

(i) $\omega(x) > (p-1)^{-1}$,

(ii) $\omega(x) = \infty$ if and only if $x = 1$,

(iii) $\omega(xy^{-1}) \geq \min\{\omega(x), \omega(y)\}$,

(iv) $\omega([x,y]) \geq \omega(x) + \omega(y)$,

(v) $\omega(x^p) = \omega(x) + 1$.

If a p-valued pro-p group G is p-radical with respect to ω (that is, if for every $x \in G$ with $\omega(x) > p(p-1)^{-1}$ there exists $y \in G$ such that $x = y^p$), then G is called saturable.

Clearly, properties (ii) and (v) impose p-valued pro-p groups are torsion-free. Moreover, saturable pro-p groups have really similar properties to uniform pro-p groups, to the extent that, for many years, they were wrongly thought to be equivalent properties, before it was proved that all uniform pro-p groups are saturable but the converse does not hold. In particular, Lazard showed in [35] that, if H is a saturable pro-p group, then $L(H)$ is a $\mathbb{Z}_p$-lattice.
In [21] González-Sánchez provided a useful characterization of saturable groups.

Definition 89. Let G be a pro-p group: a potent filtration of G is a decreasing central series N_i, $i \in \mathbb{N}$, of closed normal subgroups of G with trivial intersection such that $[N_i, \overbrace{G, \cdots, G}^{p-1}] \subseteq N_{i+1}^p$. A closed normal subgroup N of G is called PF-embedded in G if there is a potent filtration of G starting at N (i.e. such that $N_1 = N$). G is called a PF-group if it is PF-embedded in itself.

Theorem 90. [21, Theorem A] Let G be a torsion-free finitely generated pro-p group. Then G is saturable if and only if it is a PF-group.

This characterization of saturable pro-p groups allows us to introduce some further lemmas.

Lemma 91. Let G be a powerful pro-p group and $N \trianglelefteq_O G$. Then there exists a powerful T such that $N \leq T \leq G$ and $[N,T]^p = [T,T]^p$ if $p > 2$, $[N,T]^4 = [T,T]^4$ if $p = 2$.

Proof. Let us start by proving the thesis holds for finite p-groups. Let $N \trianglelefteq G$, then consider the set of all powerful K such that $N \leq K \leq G$: it is non empty and finite, so we can take a minimal element T in it. We can thus apply Theorem 5.1 in [22], stating that, if H is a finite powerful p-group and $N \triangleleft H$, then by one of the following holds:

1. $[H,H]^p = [N,H]^p$ if $p > 2$, $[H,H]^4 = [N,H]^4$ if $p = 2$ (we will say for brevity's sake that (H,N) respects Property 1).
2. There exists a proper powerful subgroup P of H such that N is contained in P.

Now, by minimality of T, necessarily (T,N) respects Property 1.
Let us prove now the Lemma in the general case, so let G be a profinite group, $N \trianglelefteq_O G$. Take $K \leq_O N$, $K \trianglelefteq_O G$, then we know there exists a powerful M/K such that $(M/K, N/K)$ respects Property 1: let $T(K)/K$ be maximal with both

properties. If $L \leq_O K$, $L \trianglelefteq_O G$, then we can analogously construct a $T(L)/L$ maximal with the properties of being powerful and such that $(T(L)/L, N/L)$ respects Property 1. Notice that this implies $T(L)/K \cong \dfrac{T(L)/L}{K/L}$ is powerful and

$$[T(L), T(L)]^p K = ([T(L), T(L)]^p L)\, K = ([N, T(L)]^p L)\, K = [N, T(L)]^p K,$$

thus $T(L)/K$ respects the same two properties as $T(K)/K$. Thus, by maximality of $T(K)/K$, necessarily $T(L) \leq T(K)$. Let now $N \geq K_1 \geq K_2 \geq \cdots$ be a subgroup descending series such that $K_i \trianglelefteq_O G$, let $T_i := T(K_i)$: then $N \leq \cdots T_i \leq T_{i-1} \leq \cdots T_2 \leq T_1 \leq G$. As $|G/N|$ is finite, there must exist $n_0 \in \mathbb{N}$ such that $T_n = T_{n_0} =: T$ for every $n \geq n_0$. This means in particular that T/K_i is powerful for every $i \geq n_0$. But then T is the inverse limit of an inverse sistem of powerful finite p-groups in which all the maps are surjective, hence T is powerful (see for example Corollary 3.3 in [17]). Furthermore, $[T, T]^p$ and $[N, T]^p$ are closed subgroups of G, hence

$$[T, T]^p = \bigcap_i [T, T]^p K_i = \bigcap_i [N, T]^p K_i = [N, T]^p,$$

hence (T, N) also respects Property 1. □

Lemma 92. Let p be an odd prime and let G be a uniform pro-p group, then the following hold:

(i) If $N \trianglelefteq_O G$, then N is saturable;

(ii) If $x \in G$, then $\left\langle x, G^{p^i} \right\rangle$ is uniform for any $i \in \mathbb{N}$ (in particular, it is saturable).

Proof. (i) Let $N \trianglelefteq_O G$, then we can find T as in Lemma 91. Define

$$N_i = [N, \overbrace{T, \cdots, T}^{i-1}]$$

First notice that, as T is powerful, by Shalev's Interchanging property

$$[T, T, T] = [T', T] \leq [T^p, T] = [T, T]^p \tag{4.8}$$

Moreover, let us prove that

$$[[N, T]^p, \overbrace{T, \cdots, T}^{i-1}] \leq [N, \overbrace{T, \cdots, T}^{i}]^p \tag{4.9}$$

By Lemma 86 and Shalev's interchanging property,

$$[T, T, T]^p = [[T, T]^p, T] = [[N, T]^p, T]; \tag{4.10}$$

by Hall-Petresco's identity (see [26] and [44]) we have

$$[[N, T]^p, T] \leq [[N, T], T]^p \gamma_{p+1}([N, T]),$$

so

$$[[N,T]^p,T] \leq [N,T,T]^p[T,\overbrace{[N,T],\cdots,[N,T]}^{p}]. \tag{4.11}$$

Moreover, notice that $[[N,T],T] \leq [[T,T],T] \leq [T,T]^p = [N,T]^p$, whence $[N,T]$ is powerfully embedded in T: as a consequence,

$$[T,\overbrace{[N,T],\cdots,[N,T]}^{p}] \leq [[N,T]^p,\overbrace{[N,T],\cdots,[N,T]}^{p-1}] \leq [T^p,\overbrace{[N,T],\cdots,[N,T]}^{p-1}]$$

$$= [T,\overbrace{[N,T],\cdots,[N,T]}^{p-1}]^p \leq \cdots \leq [T,T,T]^{p^2}. \tag{4.12}$$

Now, summing up Equations (4.10), (4.11) and (4.12), we get

$$[T,T,T]^p \leq [N,T,T]^p[T,T,T]^{p^2},$$

but $[T,T,T]^{p^2}$ is the Frattini subgroup of $[T,T,T]^p$, so necessarily

$$[N,T,T]^p = [T,T,T]^p = [[T,T]^p,T] = [[N,T]^p,T].$$

Iterating $i-2$ times we get Equation (4.9).
Now, $N_1 = N$ and, by Equations (4.8) and (4.9),

$$N_{i+1} = [N,\overbrace{T,\cdots,T}^{i}] \leq [\overbrace{T,\cdots,T}^{i+1}] \leq [[T,T]^p,\overbrace{T,\cdots,T}^{i-2}]$$

$$= [[N,T]^p,\overbrace{T,\cdots,T}^{i-2}] \leq [N,\overbrace{T,\cdots,T}^{i-1}]^p = N_i^p.$$

Therefore,

$$[N_i,\overbrace{N,\cdots,N}^{p-1}] \leq [N_i,\overbrace{T,\cdots,T}^{p-1}] \leq [N_i,T,T] = [N,\overbrace{T,\cdots,T}^{i+1}] = N_{i+2} \leq N_{i+1}^p.$$

thus N is a PF-group and so it is saturable by Theorem 90.
Thus, we have proved N_i is a potent filtration for N in itself, so N is a PF-group and thus it is saturable by Theorem 90.

(ii) Let now $x \in G$, call $H = \left\langle x, G^{p^i} \right\rangle$. Then

$$[H,H] = [H,G^{p^i}] \leq [G,G^{p^i}] \leq G^{p^{i+1}} \leq H^p,$$

thus is it a powerful subgroup of a uniform group, so it is uniform.

□

Notice that, if G has the same normal subgroup growth of a torsion-free abelian pro-p group, then all sublattices of $L(G)$ are normal subgroups of G. We have thus proved the following result:

Proposition 93. Suppose p is an odd prime and G is a uniform pro-p group. Let

$$\mathcal{A}(G) = \{N \trianglelefteq_O G\},$$

$$\mathcal{B}(G) = \{H \leq_O G | H \text{ is saturable}\},$$
$$\mathcal{C}(G) = \{H \leq_O G | L(H) \text{ is a Lie sublattice of } L(G)\},$$
$$\mathcal{D}(G) = \{H \leq_O G | L(H) \text{ is a sublattice of } L(G)\} :$$

then

$$\mathcal{A}(G) \subseteq \mathcal{B}(G) \subseteq \mathcal{C}(G) \subseteq \mathcal{D}(G);$$

moreover, if G has the same normal subgroup growth as $\mathbb{Z}_p^d$, then

$$\mathcal{A}(G) = \mathcal{B}(G) = \mathcal{C}(G) = \mathcal{D}(G).$$

Now we are ready to prove that Conjecture 83 holds for uniform pro-p groups.

Theorem 94. Let p be an odd prime and suppose G is a uniform pro-p group with the same normal subgroup growth as $\mathbb{Z}_p^n$, for some $n \in \mathbb{N}$: then $G \cong \mathbb{Z}_p^n$. In particular, every normally ζ-reversible uniform pro-p group is isomorphic to $\mathbb{Z}_p^n$, for some n.

Proof. As uniform groups are torsion-free, we have to prove that G is abelian. Suppose G' is not trivial, then there exist $a, b \in G$ such that $[a, b] \neq 1$. Notice that $G \backslash G^p, G^p \backslash G^{p^2}, \cdots$ form a partition of G, so $1 \neq c = [a, b] \in G^{p^i} \backslash G^{p^{i+1}}$ for some $i \in \mathbb{N}$.
Suppose $c \notin \langle a, b \rangle$, then $H_1 = \left\langle b, G^{p^{i+1}} \right\rangle$ is saturable by Lemma 92(ii), but it is not normal ($c \notin H_1$ but $c \in \langle b, b^a \rangle$), contradicting Proposition 93.
Suppose now $c \in \langle a, b \rangle$ and consider the projection

$$G \longrightarrow G/G^{p^{i+1}} \text{ mapping } g \mapsto \overline{g} = gG^{p^{i+1}}.$$

Consider the cyclic groups $\langle \overline{a} \rangle, \langle \overline{b} \rangle \leq G/G^{p^{i+1}}$: they have trivial intersection (as $c \notin G^{p^{i+1}}$), thus $\overline{c}$ cannot be contained in both of them. Suppose $\overline{c} \notin \langle \overline{a} \rangle$, then $H_2 = \left\langle a, G^{p^{i+1}} \right\rangle$ is saturable (by Lemma 92(ii)) but not normal ($a^b \notin H_2$), contradicting Proposition 93. □

4.3 ζ-reversible pro-p groups of small dimension

In [10] E. Damian and A. Lucchini introduced the definition of ζ-reversible groups and proved that if $d(H) = d(G)$ for any $H \leq_O G$, then G is ζ-reversible: moreover, motivated by the partial evidence given by several examples of ζ-reversible groups, they stated the following conjecture:

Conjecture 95. [10, Conjecture 2] A finitely generated pro-p group G is ζ-reversible if and only if $d(H) = d(G)$ for any $H \leq_O G$.

If this conjecture holds, then it is possible to list all finitely generated ζ-reversible pro-p groups, as a classification of finitely generated pro-p groups with constant generating number on open subgroups have been proposed by B. Klopsch and I. Snopce in [32]:

Theorem 96. [32, Theorem 1.1] Let G be a finitely generated pro-p group and let $d := d(G)$. Then $d(H) = d$ for any $H \leq_O G$ if and only if G is isomorphic to one of the groups in the following list:

1. the abelian group $\mathbb{Z}_p^d$, for $d \geq 0$;
2. the metabelian group $\langle y \rangle \ltimes A$, for $d \geq 2$, where $\langle y \rangle \cong \mathbb{Z}_p$, $A \cong \mathbb{Z}_p^{d-1}$ and y acts on A as scalar multiplication by λ, with $\lambda = 1 + p^s$ for some $s \geq 1$, if $p > 2$, and $\lambda = \pm(1 + 2^s)$ for some $s \geq 2$, if $p = 2$;
3. the group $\langle \omega \rangle \ltimes B$ of maximal class, for $p = 3$ and $d = 2$, where $\langle \omega \rangle \cong C_3$, $B = \mathbb{Z}_3 + \mathbb{Z}_3\omega = \mathbb{Z}_3^2$ for a primitive third root of unity 1 and where ω acts on B as multiplication by ω;
4. the metabelian group $\langle y \rangle \ltimes A$, for $p = 2$ and $d \geq 2$, where $\langle y \rangle \cong \mathbb{Z}_2$, $A \cong \mathbb{Z}_2^{d-1}$ and y acts on A as scalar multiplication by -1.

The authors proved in [10, Corollary 2.2] that a finitely generated pro-p group G with $d(G) = d$ is ζ-reversible if and only if it has the same subgroup zeta function as $\mathbb{Z}_p^d$. This characterization proved to be really useful in order to find further results in support of Conjecture 95: in particular, they showed that the conjecture holds for powerful pro-p groups and for 2-generated pro-p groups.

In this section we will extend this result to a wider class of finitely generated pro-p groups: we will show that Conjecture 95 holds for torsion-free p-adic analytic groups of dimension at most 3, for $p > 3$. The study of p-adic analytic pro-p groups has greatly arised in the last decades, starting with [35]. They are defined as groups with the structure of an analytic manifold over $\mathbb{Q}_p$ such that group multiplication and inversion are both analytic functions. Many characterizations have been provided in the last years: refining a result by Lazard, Klopsch noticed that p-adic analytic pro-p groups are topological groups which are isomorphic to closed subgroups of a Sylow pro-p subgroup of $\mathrm{GL}_d(\mathbb{Z}_p)$ for a suitable degree d. The most useful characterization, which sums up the work of Lubotzky, Mann and Lazard on p-adic analytic groups is the following (see for example [17]):

Theorem 97. A pro-p group is p-adic analytic if and only if it has finite rank.

González-Sánchez and Klopsch proved in [23] that a torsion-free p-adic analytic pro-p group of dimension less than p is a PF-group, hence it is saturable: this means, as we have seen in the previous section, that many properties of the group can be derived from the study of the correspondent Lie algebra. In particular, this result allowed the authors to provide a classification of torsion-free p-adic analytic groups of dimension at most 3, for $p > 3$.
Shortly after, Klopsch and Voll gave in [33] a formula to calculate the subgroup zeta function of such groups, starting again by the associated Lie algebras: the formula involves p-adic integrals and Igusa's local zeta functions (see [18] and [51]). Following the notation in [33], let us define $\zeta_p(s) = \left(1 - p^{-1}\right)^{-1}$: by [10, Corollary 2.2], a finitely generated profinite group G is ζ-reversible if and only if

$$\zeta_G(s) = \prod_{i=1}^{d(G)} \zeta_p(s - i + 1).$$

Summing up the results contained in [23, Proposition 7.1, Theorem 7.4, Section 7.3], we have the following results:

Theorem 98. • Let G be a torsion-free p-adic analytic pro-p group of dimension 1: then it is the infinite procyclic group $G \cong \mathbb{Z}_p$.

- Let G be a torsion-free p-adic analytic pro-p group of dimension 2 for $p > 2$: then $G \cong \mathbb{Z}_p^2$ or G belongs to the infinite family, parameterised by $k \in \mathbb{N}$,

$$G(k) = \left\langle x, y | [x, y] = y^{p^k} \right\rangle.$$

Theorem 99. • Let G be a soluble torsion-free p-adic analytic pro-p group of dimension 3 for $p > 3$, then G is one of the following:

1. $G_0(\infty) = \langle x_1, x_2, x_3 | [x_1, x_2] = [x_1, x_3] = [x_2, x_3] = 1 \rangle \cong \mathbb{Z}_p^3$;
2. $G_0(k) = \left\langle x, y, z | [x, y] = z^{p^k}, [x, z] = [y, z] = 1 \right\rangle$ for some $k \in \mathbb{N}$;
3. $G_1(k) = \left\langle x, y_1, y_2 | [y_1, y_2] = 1, [y_1, x] = y_1^{p^k}, [y_2, x] = y_2^{p^k} \right\rangle$ for some $k \in \mathbb{N}$;
4. $G_2(k, r, d) = \left\langle x, y_1, y_2 | [y_1, y_2] = 1, [y_1, x] = y_1^{p^k} y_2^{p^{k+r} d}, [y_2, x] = y_1^{p^{k+r}} y_2^{p^k} \right\rangle$ for some $k, r \in \mathbb{N}$, $d \in \mathbb{Z}_p$;
5. $G_3(k, r, d) = \left\langle x, y_1, y_2 | [y_1, y_2] = 1, [y_1, x] = y_2^{p^k d}, [y_2, x] = y_1^{p^k} y_2^{p^{k+r}} \right\rangle$ for some $k, r \in \mathbb{N}_0$, $d \in \mathbb{Z}_p$ such that $k \geq 1$, or $r \geq 1$ and $d \in p\mathbb{Z}_p$;
6. $G_4(k, r) = \left\langle x, y_1, y_2 | [y_1, y_2] = 1, [y_1, x] = y_2^{p^{k+r}}, [y_2, x] = y_1^{p^k} \right\rangle$ such that $k, r \in \mathbb{N}_0$ and $k + r \geq 1$;
7. $G_5(k, r) = \left\langle x, y_1, y_2 | [y_1, y_2] = 1, [y_1, x] = y_2^{p^{k+r} \rho}, [y_2, x] = y_1^{p^k} \right\rangle$ such that $k, r \in \mathbb{N}_0$, $k + r \geq 1$ and $\rho \in \mathbb{Z}_p^*$.

- Let G be an insoluble torsion-free p-adic analytic pro-p group of dimension 3 for $p > 3$, then G is isomorphic to $\mathrm{SL}_2(\mathbb{Z}_p)$ or to $\mathrm{SL}_1^1(\Delta_p)$, a Sylow pro-$p$ subgroup of $\mathrm{SL}_1(\mathbb{D}_p)$ and $\mathbb{D}_p$ denotes a central division algebra of index 2 over $\mathbb{Q}_p$.

Klopsch and Voll proved in [33] that for three-dimensional saturable p-adic analytic pro-p groups it is possible to determine a ternary quadratic form $f(x) \in \mathbb{Z}_p[x_1, x_2, x_3]$ and hence compute a p-adic integral, namely Igusa's local zeta function,

$$Z_f(s) = \int_{\mathbb{Z}_p^3} |f(x)|_p^s d\mu.$$

This function will provide sufficient information to find the subgroup zeta function of the group:

Theorem 100. [33, Theorem 1.1] Let G be a torsion-free three-dimensional p-adic analytic group. Then there is a ternary quadratic form $f(x) \in \mathbb{Z}[x_1, x_2, x_3]$, unique up to equivalence, such that

$$\zeta_G(s) = \zeta_{\mathbb{Z}_p^3}(s) - Z_f(s-2)\zeta_p(2s-2)\zeta_p(s-2)p^{2-s}\left(1 - p^{-1}\right)^{-1}, \qquad (4.13)$$

where $Z_f(s)$ is Igusa's local zeta function associated to f.

We have $d(G) = 3$ for all the three-dimensional p-adic analytic pro-p groups listed in Theorem 99, so using Equation (4.13) it is easy to determine if one of them is ζ-reversible only considering its Igusa's local zeta function.

Corollary 101. Let G be a torsion-free p-adic analytic pro-p group of dimension 3 for $p > 3$, let $f(x)$ be the ternary quadratic form associated to G and $Z_f(s)$ the correspondent Igusa's local zeta function. Then G is ζ-reversible if and only if $Z_f(s) = 0$.

We are ready to state the main Theorem in this section:

Proposition 102. Let G be a finitely generated torsion-free pro-p group, with $\dim(G) \leq 3$ and $\dim(G) < p$. Then G is ζ-reversible if and only if $d(G) = d(H)$ for all $H \leq_O G$.

Proof. If $d(H) = d(G)$ for every $H \leq_O G$, then G is ζ-reversible by [10, Proposition 1.4].
Conversely, let G be a ζ-reversible torsion-free pro-p group of dimension at most 3: then $p_G(s)$ is a Dirichlet polynomial, hence the coefficients of $\zeta_G(s) = (p_G(s))^{-1}$ are polynomially bounded, so by the profinite version of PSG theorem (see [36, 10.3]) G has finite rank, hence G is p-adic analytic by Theorem 97.
If $\dim(G) < 3$, then G must be one of the groups listed in Theorem 98: it is easy to see that they are all ζ-reversible and already classified in Theorem 96 (first and second class of groups), hence $d(H) = d(G)$ for all $H \leq_O G$. If $\dim(G) = 3$, then $Z_f(s) = 0$ by Corollary 101: then, by the classification in Theorem 99 and the computation of Igusa's zeta function in [33, Chapter 4] it follows that G is one among the groups $G_0(\infty) \cong \mathbb{Z}_p^3$ and $G_1(k)$, and it is easy to see that the latter corresponds to the second class of groups listed in Theorem 96, hence again $d(H) = d(G)$ for all $H \leq_O G$. □

Chapter 5

The real zeros of $p_G(x)$ as a real function for a finite group G

5.1 General facts on $p_G(x)$

In this chapter we will investigate some properties of the Dirichlet polynomial $p_G(s)$ associated to a finite group G. As we pointed out in the first chapter, there are several results in literature linking aritmetic properties of the coefficients of $p_G(s)$: in a similar way, we can expect to find relations between the structure of a group G and the analytic behaviour of $p_G(s)$ as a complex or real function. To this purpose we will try to investigate the behaviour, and in particular the real zeros, of $p_G(s)$ as a real function.

There are some trivial general information about $p_G(x)$ we can easily sum up without computing the Dirichlet polynomial. From now on, given a finite group G, let M be the largest positive integer such that $b_M(G) \neq 0$. Then,

$$\lim_{x\to+\infty} p_G(x) = 1 + \lim_{x\to+\infty} \left(\sum_{n=2}^{M} \frac{b_n(G)}{n^x} \right) = 1,$$

$$\lim_{x\to-\infty} p_G(x) = \lim_{x\to-\infty} \left(\sum_{n=1}^{M} \frac{b_n(G)}{n^x} \right) = \mathrm{sgn}(b_M(G))\infty.$$

Moreover, notice that if $p_G(s) = \sum_n \frac{b_n}{n^s}$, then $p'_G(s) = \sum_n -\frac{b_n \ln(n)}{n^s}$ is a Dirichlet polynomial itself.

Furthermore notice that, given a positive integer t, if $(x_1, \cdots, x_t)$ is a generating t-uple of G then $(x_1, \cdots, x_t, y)$ is a generating $t+1$-uple of G for any $y \in G$: this implies in particular $\Phi_G(t)|G| \leq \Phi_G(t+1)$, so

$$p_G(t) = \frac{\Phi_G(t)}{|G|^t} = \frac{\Phi_G(t)|G|}{|G|^{t+1}} \leq \frac{\Phi_G(t+1)}{|G|^{t+1}} = p_G(t+1),$$

thus $p_G(\cdot)$ is monotone not decreasing on positive integers.

Notice that p_G is monotonic on all $\mathbb{R}$ only if G is cyclic (otherwise there would be at least two integer zeros), while the converse is not true in general ($p_{C_6}(x)$ is not monotonic). If p_G is not monotonic on all $\mathbb{R}$, then by Corollary 17 there is a right complex halfplane in which the Dirichlet polynomial $p'_G(s)$ is never vanishing: as we already know p_G is increasing on natural numbers, this means that there exists $x_+ \in \mathbb{R}$ such that the real-valued function $p_G(x)$ is monotone increasing on $[x_+, +\infty[$, and that x_+ is minimal with such property. An analogous consideration on $p^-_G(s) := p_G(-s)$ allows us to state the existence of some maximal $x_- \in \mathbb{R}$ such that $p_G(x)$ is monotone (increasing or decreasing depending on the sign of the biggest non-trivial coefficient $b_M(G)$) on $]-\infty, x_-]$. *It is interesting to ask if it is possible to provide both a lower bound and an upper bound for* x_+.

Suppose G is a soluble group. Then, as it was proved by Gaschütz in [20], $p_G(s)$ is a product of factors of the form $1 - c_i/q_i^s$, where every c_i is a positive integer and every q_i is a prime power. Then every factor brings a real zero with multiplicity 1, namely $\log_{q_i}(c_i) = \dfrac{\ln c_i}{\ln q_i}$, and a vertical line of complex zeros in the complex plane, namely

$$\frac{\ln c_i}{\ln q_i} + \frac{2k\pi}{\ln q_i} i$$

for any integer k. From now on we will focus on real zeros of the Dirichlet polynomial: nevertheless, it is natural to ask if this regularity of the complex zeros is a characteristic of soluble groups or can be extended also to the non soluble ones. In particular, for a non soluble group G, *do all the complex zeros of* $p_G(s)$ *lie in vertical lines of the complex plane passing through a real zero?* Moreover, given a group G, *can* $p_G(x)$ *have infinite real zeros? Can the difference between a zero greater than* $d(G)$ *and* $d(G)$ *be arbitrarily big?*

We can now move to non soluble groups: given a finite group G, we consider one of its chief series, that is a series of subgroups

$$1 = N_r \lhd \cdots \lhd N_1 \lhd N_0 = G$$

such that N_i/N_{i+1} is a minimal normal subgroup of G/N_{i+1} for any i and $\bigcap_i N_i = 1$. Detomi and Lucchini proved in [14], using the concept of crown introduced by Gaschütz, that the Dirichlet polynomial can be decomposed as the product of Dirichlet polynomials computed on the chief factors N_i/N_{i+1} of one of its chief series, and this decomposition is independent from the choice of the chief series. The Dirichlet polynomials computed on the chief factors are not far from the Dirichlet polynomials associated to finite simple groups: thus, for the rest of the chapter we will focus on finite non-abelian simple groups S and we will try to classify them via the real roots of the function $p_S(x)$.

Since $p_G(s)$ was introduced by Hall in 1936, several properties of the Dirichlet polynomial have been pointed out. J. Shareshian showed in [49] that $p'_S(1) = 0$ (that is, S has a zero in 1 with multiplicity at least 2) for any non-abelian simple

group S, thus proving a conjecture formulated by Boston in [4]. A natural question arises: *is it possible to characterize all finite simple groups whose Dirichlet polynomial has a zero in* 1 *with multiplicity at least* 3*?*

More recently, M. Patassini gave in [43] an explicit formula for $p_S(s)$ when $S \cong A_1(q)$ for some prime power q; moreover, he proved that $p_S(-1) \neq 0$ for S finite simple group of the form $A_1(q)$, ${}^2B_2(q)$ or ${}^2G_2(q)$. In 2010 B. Benesh collected in [3] various information and open problems from different works about the probabilistic zeta function of finite groups.

Summing up the information we listed about $p_S(x)$, we can determine the behaviour of the function for $|x|$ big enough, but around the interval $[0, 1]$ there are still plenty of possibilities. To further explore the behaviour of the Dirichlet polynomial, we will need to compute it: as in most cases there is not an explicit general formula for it, we will use GAP to provide it. Programs giving this results for groups with small order can be found in literature: they rely on the TableOfMarks($\cdot$) command, which lists the conjugacy classes of a given finite group. In [3, Section 5] Benesh proposes a basic program for GAP that returns $p_G(s)$ as a string, for a finite G. The program is quite efficient for G groups of small order and can compute the requested function for finite simple groups of order at most $|A_1(181)|$.

```
PG:=function(G)
local i,tom,mob,ord,len,finalstring;
tom:=TableOfMarks(G);
mob:=MoebiusTom(tom).mu;
ord:=OrdersTom(tom);
len:=LengthsTom(tom);
finalstring:="";
for i in [1..Length(mob)] do
if IsBound(mob[i]) then
finalstring:=Concatenation(finalstring,"+",String(len[i]*mob[i]),
"/",String(Order(G)/ord[i]),"^s);
fi;
od;
return finalstring;
end;
```

Looking at the graph of the function for some examples of S of small order, we can see that they seem to have really different behaviours in a neighbourhood of $]0, 1[$.

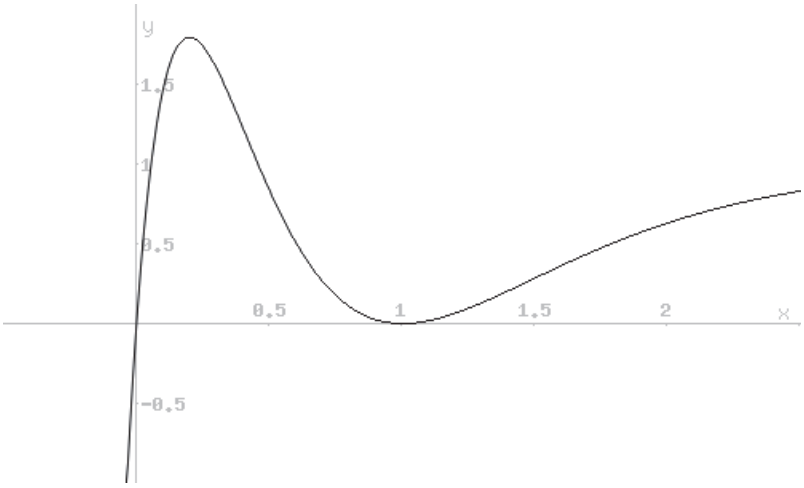

Figure 5.1: Dirichlet polynomial associated to $A_1(5) \cong \mathrm{Alt}(5)$

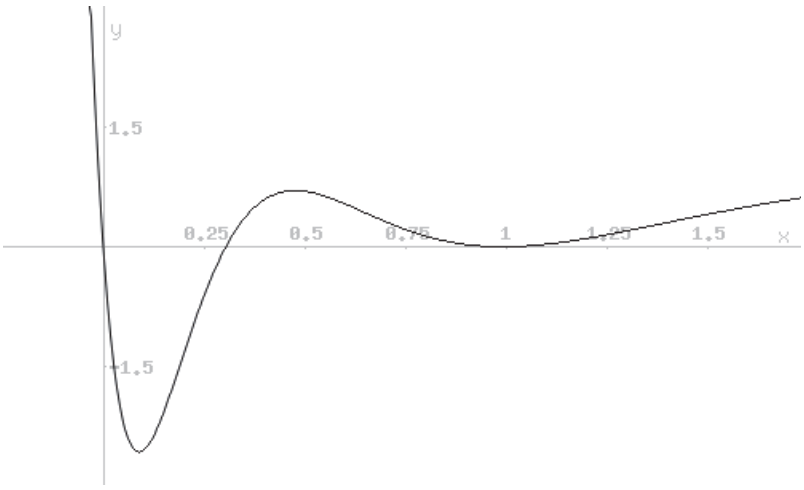

Figure 5.2: Dirichlet polynomial associated to $A_1(11)$

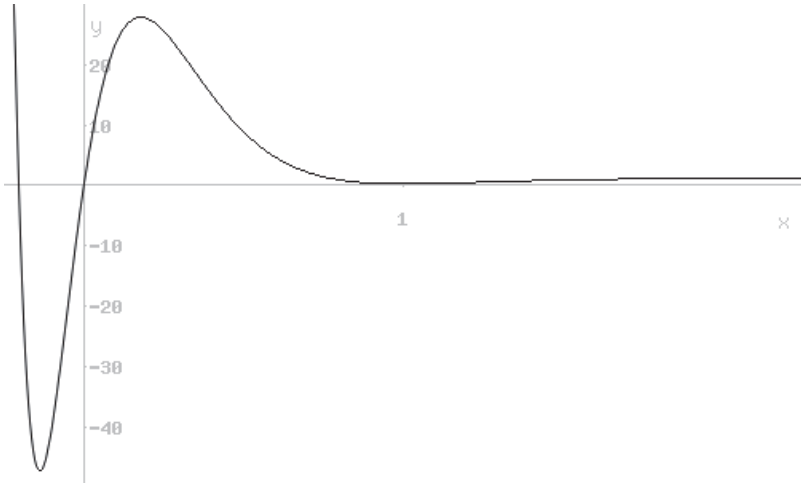

Figure 5.3: Dirichlet polynomial associated to $A_1(25)$

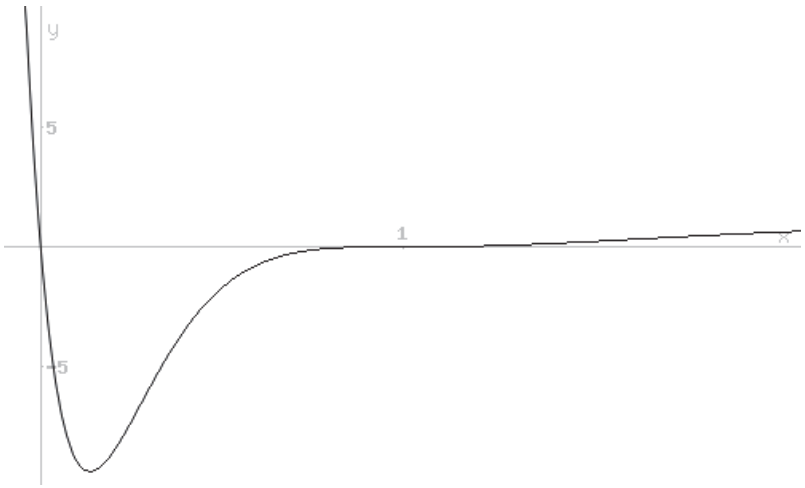

Figure 5.4: Dirichlet polynomial associated to $A_1(9) \cong \mathrm{Alt}(6)$

5.2 Properties of $p_{A_1(q)}(x)$

Patassini listed in [43, Section 7] the Dirichlet polynomials of the groups of type $A_1(q)$: we can try to classify these groups looking at the graph of the real function $p_S(x)$. The explicit computation of $p_{A_1(q)}$ for $q \leq 181$ gives us enough evidence to conjecture that there are only four possible classes of graphs, each one represented by one of the images above: we will identify such classes calling them Z_1, Z_2, Z_3, Z_4.

The Dirichlet polynomials associated to the groups in class Z_1 (see for example the graph of $p_{A_1(5)}(x)$ in Figure 5.1) have no other real zeros except 0, 1; they have negative values only for $x < 0$, have a local maximum between 0 and 1 and a local minimum in 1.

The Dirichlet polynomials associated to the groups in class Z_2 (see for example the graph of $p_{A_1(11)}(x)$ in Figure 5.2) have a non-integer zero $0 < \tilde{x} < 1$; they have negative values only for $0 < x < \tilde{x}$, have a local maximum between $\tilde{x}$ and 1 and local minimums in 1 and between 0 and $\tilde{x}$.

The Dirichlet polynomials associated to the groups in class Z_3 (see for example the graph of $p_{A_1(25)}(x)$ in Figure 5.3) have a non-integer zero $\tilde{x} < 0$; they have negative values only for $\tilde{x} < x < 0$, have a local maximum between 0 and 1 and local minimums in 1 and between $\tilde{x}$ and 0.

The Dirichlet polynomials associated to the groups in class Z_4 (see for example the graph of $p_{A_1(9)}(x)$ in Figure 5.4) have no other real zeros except 0, 1; they have negative value only for $0 < x < 1$, have a local minimum between 0 and 1 and a saddle in 1.

As it is apparent looking at them, the graphs of the Dirichlet polynomials of groups in the classes Z_2 and Z_3 have a very similar structure; moreover, Z_4 is a sort of limit case where the third root $\tilde{x}$ coincides with 1, and we have a zero of multiplicity (at least) 3 in 1.

In order to give explicit formulas to compute $p_{A_1(q)}$, in [43, Section 7] Patassini provided a classification of simple group of the form $A_1(q)$, for a prime power $q = p^f$, based on the exponent f and on the congruence classes of p: the following table shows that, as it is expected, there is a strong connection between this classification (in the left column) and the type of graph of $p_{A_1(q)}$.

Table 5.1: Class of $p_{A_1(q)}(x)$ for $q \leq 181$

q	Z_1	Z_2	Z_3	Z_4
$q = 5$	5			
$q = 7$	7			
$q = 9$				9
$q = 11$		11		
$q = p$, $p \cong \pm 2(5)$,	13, 37, 43, 53, 67, 83, 107,			

$p \cong \pm 3(8)$	$157, 163, 173$			
$q = p$, $p \cong \pm 2(5)$, $p \cong \pm 1(8)$	$17, 23, 47$, $73, 97, 103$, $113, 137, 167$			
$q = p$, $p \cong \pm 1(5)$, $p \cong \pm 3(8)$		19	$29, 59, 61, 101$, $109, 131, 139$, $149, 179, 181$	
$q = p$, $p \cong \pm 1(5)$, $p \cong \pm 1(8)$		$31, 41, 71$ $79, 89, 151$		
$q = p^2$, $p > 5$, $p \cong \pm 2(5)$		$49, 169$		
$q = p^2$, $p \cong 0, \pm 1(5)$		121	25	
$q = 2^f$, $f > 1$	$8, 16, 32, 128$	64		
$q = p^f$, $p = 3, 5$, odd $f > 1$	$27, 125$			
$q = p^f$, $p >= 3$, even $f \geq 4$		81		
$q = p^f$, $p > 5$ odd $f > 1$				

While it is not trivial to prove that the classification in the four classes above holds for all simple groups of the form $A_1(q)$, the existence of other zeros of $p_{A_1(q)}$ apart from $0, 1$ can be easily detected from the formulas in [43, Section 7]: it is sufficient to compute the values of $p'_G(0)$, $p''_G(1)$. Let S be a finite simple group and consider

$$p_S(x) = \sum_{n=1}^{M} \frac{b_n(S)}{n^x}.$$

Recall that $\lim_{x \to -\infty} p_S(x) = \mathrm{sgn}(b_M(S))\infty$, thus for x small enough $p_S(x)$ has the same sign as $b_M(S)$; moreover, if $p'_S(0), p''_S(1) \neq 0$, then there exist a right and a left neighbourhoods of 0 whose elements respectively have the same and the opposite sign of $p'_S(0)$ and a left neighbourhood of 1 whose elements have the same sign as $p''_S(1)$.
This implies in particular that

1. if $\mathrm{sgn}(b_M(S)) = \mathrm{sgn}(p'_S(0))$, then p_S has a zero $\tilde{x} < 0$;
2. if $p'_S(0), p''_S(1) \neq 0$ and $\mathrm{sgn}(p'_S(0)) \neq \mathrm{sgn}(p''_S(1))$, then p_S has a non-integer zero $0 < \tilde{x} < 1$.

In the following table we list the signs of $b_M(S)$, $p'_S(0)$, $p''_S(1)$, with $S \cong A_1(p^f)$ for some f.

Table 5.2: Signs of $b_M(S)$, $p'_S(0)$, $p''_S(1)$, for some $S \cong A_1(p^f)$

f	p	$\mathrm{sgn}(b_M(S))$	$\mathrm{sgn}(p'_S(0))$	$\mathrm{sgn}(p''_S(1))$
$f=1$	$p \cong 0, \pm 2$ (5)	$-$	$+$	$+$
	$p \cong \pm 1$ (5) and $p \cong \pm 1$ (8) or $p \in \{11, 19\}$	$+$	$-$	$+$
	$p \cong \pm 1$ (5), $p \cong \pm 3$ (8) and $p \notin \{11, 19\}$	$+$	$+$	$+$
$f=2$	3	$+$	$-$	0
	5	$+$	$+$	$+$
	$p > 5$	$+$	$-$	$+$
f odd prime	any p	$-$	$+$	$+$
$f=6$	any p	$+$	$-$	$+$
$f=2^k$, $k>1$	$p=2$	$-$	$+$	$+$
	p odd	$+$	$-$	$+$

We can easily sum up the results in Table 5.2:

Remark 103. (i) In the following cases the Dirichlet polynomial $p_S(s)$ associated to $A_1(q)$ has a real zero $0 < \tilde{x}(q) < 1$: $q = 11$; $q = 19$; $q = p$ for $p \cong \pm 1$ (5) and $p \cong \pm 1$ (8); $q = p^2$ for $p > 5$; $q = p^6$ for any p; $q = p^{2^k}$ for $k > 1$ and $p \geq 3$.

(ii) In the following cases $p_S(s)$ has a real zero $\tilde{x}(q) < 0$: $q = 25$; $q = p$, with $p \cong \pm 1$ (5), $p \cong \pm 3$ (8) and $p \neq 11, 19$.

Consider one of the infinite families for q described in Table 5.2 for which we have proved the existence of a third real root $\tilde{x}(q) \notin \{0, 1\}$: it is natural to ask if $\tilde{x}(q)$ tends to a limit, when $q \to \infty$. It is possible to use the formulas in [43, Section 7] to compute $\tilde{x}(q)$ with sufficient approximation for large q. It may be expected that, in all the cases listed in Remark 103, $\tilde{x}(q)$ tends to 0 or 1: this is true in most cases, as it is easy to verify that the root $\tilde{x}(q)$ tends to 1 when q increases to $+\infty$ in all the infinite families in Corollary 103 for even f; on the other side, the situation seems different for $f = 1$. Consider the case in which $q = p$ for $p \cong \pm 1$ (5) and $p \cong \pm 1$ (8): then $\tilde{x}(q)$ tends to a limit which is $\approx 0,24378$. Consider now the case in which $q = p$ for $p \cong \pm 1$ (5) and $p \cong \pm 3$ (8): then $\tilde{x}(q)$ tends to a limit which is $\approx -0,1029$. *It would be interesting to find out whether this limits have an algebraic meaning.*

5.3 Properties of $p_S(x)$ for other families of non-abelian finite simple groups

If we remove the hypothesis that $S \cong A_1(q)$, it is immediately clear that the four classes $Z_1, \cdots, Z_4$ are no more sufficient to describe the possible graphs: e.g., $p_{\mathrm{Alt}(7)}(x)$ has two different non-integer zeros $0 < \tilde{x}_1 < \tilde{x}_2 < 1$, while $p_{M_{12}}(x)$ has a zero $\tilde{x} > 1$, and $p_{\mathrm{Alt}(9)}(x)$ has two different non-integer zeros $\tilde{x}_1 < 0$ and $\tilde{x}_2 > 1$. We can thus list further families of graphs for $p_S(x)$.

The Dirichlet polynomials associated to the groups in class Z_5 have two non-integer real zeros $0 < \tilde{x}_1 < \tilde{x}_2 < 1$; they have negative values only for $x < 0$ or $\tilde{x}_1 < x < \tilde{x}_2$.

The Dirichlet polynomials associated to the groups in class Z_6 have two non-integer real zeros $\tilde{x}_1 < 0 < 1 < \tilde{x}_2$; they have negative values only for $x < \tilde{x}_1$ or $0 < x < \tilde{x}_2$ and $x \neq 1$.

The Dirichlet polynomials associated to the groups in class Z_7 have a non-integer zero $\tilde{x} > 1$; they have negative values only for $0 < x < \tilde{x}$ and $x \neq 1$.

The Dirichlet polynomials associated to the groups in class Z_8 have a non-integer zero $0 < \tilde{x} < 1$; they have negative value only for $x < 0$ or $\tilde{x} < x < 1$ and they have a saddle in 1.

Again, the graphs of Z_5 and Z_6 have essentially the same structure, while Z_8 is a sort of limit case, with a zero of multiplicity at least 3 in 1.

We classify in the following Table the graphs of p_S, for S finite simple group of small order, non-isomorphic to $A_1(q)$.

Table 5.3: Class of $p_S(x)$

S	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_7	Z_8
Alt$(\cdot)$			8		7	9	10	
$A_2(\cdot)$	3, 4	7	5					
${}^2A_2(\cdot)$	3, 4						5	
${}^2A_3(\cdot)$	2							
$C_2(\cdot)$								4
$C_3(\cdot)$							2	
${}^2B_2(\cdot)$	8							
Sporadic	M_{11}	M_{22}	J_1				M_{12}	

Finally, this short chapter gives some partial answers to the questions we posed at the beginning, while it leaves some most of them still open.

Notice that, among the finite simple groups we considered, the only ones such that $p_S(x)$ has a zero in 1 with multiplicity 3 are $A_1(9) \cong$ Alt(6) and $C_2(4)$: it is still an open problem to characterize all simple groups with this property. One can ask if it is possible to find finite perfect groups with a zero in 1 with arbitrarily large multiplicity, and the answer is affirmative.

Remark 104. Let $S_1 \cdots, S_k$ be non-isomorphic finite simple groups, let us define $G = \prod_{i=1}^{k} S_i$; then

$$p_{S_i}(0) = p_{S_i}(1) = p'_{S_i}(1) = 0,$$

moreover, by Theorem 4

$$p_G(s) = \prod_{i=1}^{k} p_{S_i}(s)$$

so, by Leibniz's formula, we have

$$p_G^{(n)}(0) = 0,$$

$$p_G^{(m)}(1) = 0$$

for every $n \leq k-1$ and every $m \leq 2k-1$.

We found examples of finite simple groups S such that p_S has a zero greater than 1 (the ones in classes Z_6 and Z_7) and other ones such that p_S has a zero smaller than -1 (e.g. $A_2(5)$). It seems natural to ask if we can find a simple group S such that p_S has a zero greater than 2 (the zeros of the computed examples are all smaller than that) or smaller than -2: motivated by the examples we have found, we can state the following conjecture.

Conjecture 105. Let G be a finite group and let $\tilde{x}$ be a real zero of the Dirichlet polynomial $p_G(x)$: then $|\tilde{x}| < d(G)$.

Furthermore, suppose G is not cyclic: then we have shown that for every finite group G there exists $x_+ \in \mathbb{R}$ such that p_G is monotonic increasing on $[x_+, +\infty[$. In general, we know that

$$p_S(d(G)-2) = p_S(d(G)-1) = 0,$$

so

$$x_+ > d(G) - 2. \tag{5.1}$$

If the group is simple, we have seen that $0 < x_+ < 1$ for S in the classes Z_4, Z_8, while $x_+ = 1$ for S in the classes Z_1, Z_2, Z_3, Z_5, Z_6 and $x_+ > 1$ for S in the class Z_7. It is in fact easy to refine the bound in Equation (5.1) in the following (trivial) way:

Remark 106. Let S be a finite non-abelian simple group and $x_+ \in \mathbb{R}$ be the minimal value such that p_S is increasing on $[x_+, +\infty[$: then $x_+ > 0$. Furthermore, if $p_S''(1) \neq 0$, then 1 is a local extremal point for $p_S(x)$, in particular $x_+ \geq 1$.

It is natural to ask if there is actually a better refinement for the bound in Equation (5.1)*, both in the simple and in the general case.*

Bibliography

[1] M. Aschbacher, Finite group theory. Second edition. Cambridge Studies in Advanced Mathematics, 10. Cambridge University Press, Cambridge, 2000.

[2] A. Ballester-Bolinches and L. M. Ezquerro, Classes of finite groups. Mathematics and Its Applications (Springer), 584. Springer, Dordrecht, 2006.

[3] B. Benesh, The probabilistic zeta function. Computational group theory and the theory of groups, II, 1–9, Contemp. Math., 511, Amer. Math. Soc., Providence, RI, 2010.

[4] N. Boston, A probabilistic generalization of the Riemann zeta function, Analytic number theory, Vol. 1 (Allerton Park, IL, 1995) **138** (1996), 155–162.

[5] K. Brown, The coset poset and probabilistic zeta function of a finite group, J. Algebra 225 (2000), no. 2, 989–1012.

[6] F. Buekenhout, Good contributors to the order of the finite simple groups. Arch. Math. (Basel) 44 (1985), no. 4, 289–296.

[7] R. W. Carter, Simple groups of Lie type. Pure and Applied Mathematics, Vol. 28. John Wiley and Sons, London–New York-Sydney, 1972.

[8] 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.

[9] H. M. Crapo, Möbius inversion in lattices. Arch. Math. (Basel) 19 1968, 595–607 (1969).

[10] 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).

[11] E. Damian and A. Lucchini, Recognizing the alternating groups from their probabilistic zeta function, Glasgow Math. J. (2004) 46 595–599.

[12] E. Damian and A. Lucchini, The probabilistic zeta function of finite simple groups. J. Algebra 313 (2007), no. 2, 957–971.

[13] E. Damian, A. Lucchini and F. Morini, Some properties of the probabilistic zeta function of finite simple groups, Pacific. J. Math., 215 (2004), 3–14.

[14] 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.

[15] E. Detomi and A. Lucchini, Profinite groups with multiplicative probabilistic zeta function, J. London Math. Soc. (2) 70 (2004), no. 1, 165–181.

[16] E. Detomi and A. Lucchini, Some generalizations of the probabilistic zeta function. Ischia group theory 2006, 56–72, World Sci. Publ., Hackensack, NJ, 2007.

[17] J. D. Dixon, M. P. F. Du Sautoy, A. Mann, D. Segal, Analytic pro-p groups. Second edition. Cambridge Studies in Advanced Mathematics, 61. Cambridge University Press, Cambridge, 1999.

[18] M. P. F. du Sautoy and L. Woodward, Zeta functions of groups and rings. Lecture Notes in Mathematics, vol. 1925, Springer, Heidelberg (2008).

[19] W. Feit and J. G. Thompson, Solvability of groups of odd order. Pacific J. Math. 13 1963, 775–1029.

[20] W. Gaschütz, Die Eulersche Funktion endlicher auflösbarer Gruppen. Illinois J. Math. 3 1959 469–476.

[21] J. González-Sánchez, On p-saturable groups, J. Algebra 315 (2007), 809–823.

[22] J. González-Sánchez and A. Jaikin-Zapirain, On the structure of normal subgroups of potent p-groups. J. Algebra 276 (2004), no. 1, 193–209.

[23] J. González-Sánchez and B. Klopsch, Analytic pro-p groups of small dimensions. J. Group Theory 12 (2009), no. 5, 711–734.

[24] D. Gorenstein, Finite simple groups. An introduction to their classification. University Series in Mathematics. Plenum Publishing Corp., New York, 1982.

[25] F. Grunewald, D. Segal and G. C. Smith, Subgroups of finite index in nilpotent groups, Invent. Math. 93 (1988), no. 1, 185–223.

[26] P. Hall, A contribution to the theory of groups of prime-power orders. Proc. Loud. Math. Soc., II 26, 29–95 (1933).

[27] P. Hall, The eulerian functions of a group, Quart. J. Math. (1936), no. 7, 134–151.

[28] I. M. Isaacs, Character theory of finite groups. Pure and Applied Mathematics, No. 69. Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1976.

[29] E. I. Khukhro, p-Automorphisms of Finite p-groups, Cambridge University Press, Cambridge, 1998.

[30] 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.

[31] P. Kleidman and M. Liebeck, The subgroup structure of the finite classical groups. London Mathematical Society Lecture Note Series, 129. Cambridge University Press, Cambridge, 1990.

[32] B. Klopsch and I. Snopce, Pro-p groups with constant generating number on open subgroups, J. Algebra 331 (2011), 263–270.

[33] B. Klopsch and C. Voll, Zeta functions of three-dimensional p-adic Lie algebras. Math. Z. 263 (2009), no. 1, 195–210.

[34] V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups. J. Algebra 32 (1974), 418–443.

[35] M. Lazard, Groupes analytiques p-adiques. Inst. Hautes Études Sci. Publ. Math. No. 26 1965 389–603.

[36] A. Lubotzky and D. Segal, Subgroup growth. Progress in Mathematics, 212. Birkhauser Verlag, Basel, 2003.

[37] A. Lucchini, Profinite groups with nonabelian crowns of bounded rank and their probabilistic zeta function, Israel J. Math. 181 (2011), 53–64.

[38] A. Mann, Positively finitely generated groups, Forum Math. 8 (1996), no. 4, 429–459.

[39] A. Mann, A probabilistic zeta function for arithmetic groups, Internat. J. Algebra Comput. 15 (2005), 1053–1059.

[40] L. E. Mattics and F. W. Dodd. A bound for the number of multiplicative partitions. Amer. Math. Monthly 93 (1986), 125–126.

[41] N. E. Menezes, M. Quick and C. M. Roney-Dougal, The probability of generating a finite simple group. Israel J. Math. 198 (2013), no. 1, 371–392.

[42] J. Nagura, On the interval containing at least one prime number. Proc. Japan Acad. 28, (1952). 177–181.

[43] M. Patassini, The probabilistic zeta function of $\mathrm{PSL}(2,q)$, of the Suzuki groups ${}^2B_2(q)$ and of the Ree groups ${}^2G_2(q)$. Pacific J. Math. 240 (2009), no. 1, 185–200.

[44] J. Petresco, Sur les commutateurs, Math. Z. 61 (1954), 348–356.

[45] C. E. Praeger and J. Saxl, On the orders of primitive permutation groups. Bull. London Math. Soc. 12 (1980), no. 4, 303–307.

[46] J. Puchta, Groups with multiplicative subgroup growth. Israel J. Math. 122 (2001), 149–156.

[47] D. J. S. Robinson, A course in the theory of groups. Second edition. Graduate Texts in Mathematics, 80. Springer-Verlag, New York, 1996.

[48] 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.

[49] J. Shareshian, On the probabilistic zeta function for finite groups, J. Algebra, 210 (1998), 703–770.

[50] 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.

[51] C. Voll, Functional equations for zeta functions of groups and rings. Ann. of Math. (2) 172 (2010), no. 2, 1181–1218.

[52] 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.

[53] A. Wagner, The faithful linear representations of least degree of S_n and A_n over a field of odd characteristic. Math. Z. 154 (1977), no. 2, 103–114.

[54] J. S. Wilson, Profinite groups. London Mathematical Society Monographs. New Series, 19. The Clarendon Press, Oxford University Press, New York, 1998.

[55] T. R. Wolf, Solvable and nilpotent subgroups of $GL(n, q^m)$. Canad. J. Math. 34 (1982), no. 5, 1097–1111.

[56] K. Zsigmondy, Zur Theorie der Potenzreste. (German) Monatsh. Math. Phys. 3 (1892), no. 1, 265–284.