Chapter 1

Introduction

1.1 Historical introduction

In the last two decades, there has been a growing interest in the use of probability in finite groups. Probabilistic methods have proved useful in the solutions of several problems concerning finite groups, mainly involving simple groups and permutation groups. We refer to Dixon [Dix02] and Shalev [Sha98a, Sha01] for more detailed surveys.

Our subject apparently begins with a series of seven papers (see [ET65, ET67a, ET67b, ET68, ET71, ET70, ET72]) of Erdős and Turán in which they studied the properties of random permutations. For example, they showed that most permutations in the symmetric groups $\mathrm{Sym}(n)$ have order about $n^{\frac{1}{2}\log n}$ and have about $\log n$ cycles. Dixon used Erdős-Turán theory to prove in [Dix69] an old conjecture of Netto that two randomly chosen elements of the alternating group $\mathrm{Alt}(n)$ generate $\mathrm{Alt}(n)$ with probability tending to 1 as $n \to \infty$. Dixon then conjectured that for every finite simple group S, the probability $P(S,2)$ that two random elements generate the group S tends to 1 as $|S| \to \infty$. Using the classification of finite simple groups, the latter conjecture was proved by W. M. Kantor and A. Lubotzky in [KL90a] for the classical and small exceptional groups of Lie type, and by M. Liebeck and A. Shalev in [LS95] for the remaining ones (see [Sha98a] for more details).

Whereas for finite groups we can compute the probability by simply counting the number of elements, this is not so for infinite groups. Let us start with a simple problem (see [Man04]). We will abuse the word "probability" before having a correct definition. We will need, as it will be explained later, to move from abstract groups to their profinite

completions. Let $G = \mathbb{Z}$, the infinite cyclic group. This group can be generated by one element, but as only two elements of its infinitely many elements are such generators, the probability that one element generates $\mathbb{Z}$ seems to be 0. So let $p = P(\mathbb{Z}, 2)$ be the probability that two elements generate $\mathbb{Z}$. Choosing two elements at random, they generate some subgroup $n\mathbb{Z}$. Again, the probability that $n = 0$ seems to be 0, so with probability 1, our pair of integers generates a non-trivial subgroup. They lie in $n\mathbb{Z}$ with probability $1/n^2$. Once they lie in $n\mathbb{Z}$, recalling that $n\mathbb{Z} \cong \mathbb{Z}$, they generate $n\mathbb{Z}$ with the same probability p. Hence

$$1 = p\left(\sum_{n=1}^{\infty} \frac{1}{n^2}\right) = p\zeta(2).$$

where $\zeta(s)$ is the Riemann zeta function. So we have that $p = 1/\zeta(2) = 6/\pi^2$. In the same way, we also get that $P(\mathbb{Z}, k) = 1/\zeta(k)$. Applying this to $k = 1$ gives a proof of the divergence of the series $\sum_n 1/n$.

With the same argument as above, one obtains that

$$\sum_{n=1}^{\infty} \frac{a_n(\mathbb{Z}^d)}{n^k} = \zeta(k)\zeta(k-1)\cdots\zeta(k-d+1)$$

where $a_n(\mathbb{Z}^d)$ is the number of subgroup of index n in $\mathbb{Z}^d$ for each n.

On infinite groups, in order to compute probabilities, we need probability measures. As we have seen, our argument needs a probability measure defined on $\mathbb{Z}$ that is both translation invariant and countably additive. And it is easy to see that such a measure does not exist. But on a compact group, it exists and it is known as the Haar measure. More precisely, we will be considering profinite groups, i.e., inverse limits of finite groups. Let us first introduce profinite groups and Haar measures on them.

A *topological group* is a group G which is also a topological space, such that the maps $g \mapsto g^{-1} : G \to G$ and $(g, h) \mapsto gh : G \times G \to G$ are both continuous. An easy example of a topological group is a finite group endowed with the discrete topology. A *profinite group* is a compact Hausdorff topological group whose open subgroups form a base for the neighborhoods of the identity. For such a group G, a subgroup is open if and only if it is closed and has finite index. Hence the family of all open subgroups of G intersects in $\{1\}$. Moreover, a subset of G is open if and only if it is a union of cosets of open normal subgroups.

A second definition of profinite groups is based on the concept of an *inverse limit*. We recall briefly what it is. A *directed set* is a partially ordered set $(I, \leq)$ with the property that for every $i, j \in I$, there exists $k \in I$ such that $k \geq i$ and $k \geq j$. An *inverse system* of sets (or groups, rings or topological spaces) over I is a family of sets (or groups, etc.) $(G_i)_{i \in I}$ with maps (respectively homomorphisms, continuous maps) $\phi_{ij} : G_i \to G_j$ whenever $i \geq j$, satisfying $\varphi_{ii} = Id_{G_i}$ and $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$ whenever $i \geq j \geq k$, where "$f \circ g$ means do g first, then f". The *inverse limit*

$$\varprojlim G_i = \varprojlim (G_i)_{i \in I}$$

is the subset (or subgroup, etc.) of the Cartesian product $\prod_{i \in I} G_i$ consisting of all (g_i) such that $\varphi_{ij}(g_i) = g_j$ whenever $i \geq j$. Hence, if for each i, we let π_i be the projection from $\varprojlim G_k$ to G_i, then for $i \geq j$, we have that $\varphi_{ij} \circ \pi_i = \pi_j$. The inverse limit is universal in the sense that if Y is an object with projections $\lambda_i : Y \to G_i$ satisfying $\varphi_{ij} \circ \lambda_i = \lambda_j$ then there is a unique morphism $\phi : Y \to \varprojlim G_i$ such that $\pi_i \circ \phi = \lambda_i$ for each $i \in I$.

If each G_i is a finite group endowed with the discrete topology and $\prod_{i \in I} G_i$ is given the product topology, then $\varprojlim G_i$ becomes a topological group, and this topological group is profinite.

If I is a family of normal subgroups of finite index of a given group G which is closed under taking finite intersections, we may order I by reverse inclusion, i.e., $N \geq M$ whenever $N \subseteq M$, and obtain an inverse system $(G/N)_{N \in I}$. The maps $\varphi_{N,M}$ are the natural epimorphisms $G/N \to G/M$ for $N \subseteq M$. We now come to the equivalence of the two definitions of profinite groups.

Proposition 1.1.1. *[DdSMS99, Proposition 1.3] If G is a profinite group then G is (topologically) isomorphic to $\varprojlim_{N \lhd_o G} (G/N)$ where $N \lhd_o G$ means that N is an open normal subgroup of G. Conversely, the inverse limit of any inverse system of finite groups is a profinite group.*

For a given abstract group G, $\varprojlim (G/N)$, where N ranges over all normal subgroups of G of finite index, is called the *profinite completion* of G, denoted by $\widehat{G}$. If G is *residually finite*, i.e., the intersection of all above N's is trivial, then G is embedded into its profinite completion (see [Wil98], Proposition 1.4.4).

A typical example for a profinite group is $\mathbb{Z}_p$, the group of p-adic integers, where p is

a fixed prime. We can express $\mathbb{Z}_p$ as the following.

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \left\{ (x_n)_{n\geq 0} \in \prod_{n\geq 0} \mathbb{Z}/p^n\mathbb{Z} : \text{for all } n,\, x_{n+1} \equiv x_n \mod p^n \right\}.$$

The profinite completion $\widehat{\mathbb{Z}}$ of $\mathbb{Z}$ is

$$\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \left\{ (x_n)_{n\geq 1} \in \prod_{n=1}^{\infty} \mathbb{Z}/n\mathbb{Z} : \text{for all } n|m,\, a_m \equiv a_n \mod n \right\}.$$

It is also true that

$$\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p.$$

Profinite groups are of interest to number theorists since they in fact arise in number theory as Galois groups of (finite or infinite) Galois extensions of fields, with an appropriate topology. Historically, this is the original motivation for the study of profinite groups, and Galois theory remains the main area of applications of results in profinite groups (see [Wil98, Chapter 3]).

On a profinite group G, there exist Haar measures and they are different from each other by a multiplicative constant. Hence, up to a positive multiplicative constant, there exists a unique normalized Haar measure μ such that $\mu(G) = 1$. Thus, we can consider G as a probability space. If H is an open subgroup of G, then $|G : H| < \infty$ and H is closed, hence measurable. Note that $\mu(H) = \mu(gH) = \mu(Hg)$ and since we may write $G = \bigcup Hg$ as a disjoint union of right cosets of H, we have that $1 = \mu(G) = |G : H|\mu(H)$ and so

$$\mu(H) = \frac{1}{|G : H|}.$$

If H is a closed subgroup of infinite index in G, then H is contained in the intersection of a decreasing sequence of open subgroups, say $H_1 > H_2 > \cdots$, and thus

$$\mu(H) \leq \lim_{i\to\infty} \frac{1}{|G : H_i|} = 0.$$

If $X = \bigcup x_{ij}H_j \bigcup K_l y_{kl}$ is the union of a finite collection of cosets of open subgroups, which we call basic open sets, we can find an open normal subgroup N contained in $\bigcap H_j \cap \bigcap K_l$, and then X is equal to the union of finitely many, say n, cosets of N, in which case

$$\mu(X) = n\mu(N) = \frac{n}{|G : N|}.$$

If X is a union of countable family of basic open sets, we can write X as ascending union $X = \bigcup_{i=1}^{\infty} X_i$ where each X_i is a finite union as above and obtain

$$\mu(X) = \lim_{i \to \infty} \mu(X_i)$$

In particular, if the set $\mathcal{N}$ of all open normal subgroups is countable, this determines the measure for every open set of G. Thus also of every closed sets since $\mu(G \setminus X) = 1 - \mu(X)$. In this case, G is said to be *countably based*. This applies for example when G is finitely generated. For a detailed treatment of Haar measure on profinite groups, the reader is referred to [FJ08, Chapter 18].

When talking about generators of a profinite group, we mean generators as a topological group, i.e., X generates G means that G is the smallest closed subgroup of G containing X. The closure of an arbitrary subset X is $\overline{X} = \bigcap XN$, with N ranging over all open normal subgroups of G. If follows that X generates G if and only if each finite factor G/N is generated by XN/N. Thus G is generated by d elements, say, if and only if each finite factor group G/N can be generated by d elements (see [Wil98, Proposition 4.2.1]).

Let G be a profinite group and μ the normalized Haar measure on G or on some direct power G^k. Fix k and write

$$X(G,k) = \{(x_1, \cdots, x_k) \in G^k | \overline{\langle x_1, \cdots, x_k \rangle} = G\}$$

to denote the set of all k-tuples topologically generating the group G. Since a subset T fails to generate G if and only if T is contained in some maximal open subgroup of G, it is clear that

$$G^k \setminus X(G,k) = \bigcup_{M \max G} M^k$$

where $M \max G$ means that M is a maximal proper open subgroup of G. This is an open subset of G^k so $X(G,k)$ is closed, and hence measurable. We may therefore define

$$P(G,k) = \mu(X(G,k))$$

to be the *probability that a random k-tuple generates G*. Thus $0 \leq P(G,k) \leq 1$, and if $P(G,k) > 0$ then $d(G) \leq k$, where $d(G)$ is the minimal number of generators of G.

Definition 1.1.2. *A group G is called positively finitely generated (PFG) if $P(G,k) > 0$ for some choice of $k \in \mathbb{N}$.*

Hence a PFG group is finitely generated. However, for a d-generated group G, it does not always hold that $P(G,d) > 0$. For example, the group $G = \widehat{\mathbb{Z}}$ is a one-generator group and (see [Bos96])

$$P(\widehat{\mathbb{Z}},k) = \begin{cases} 1/\zeta(k) & , k > 1 \\ 0 & , k = 1 \end{cases}$$

and hence $P(\widehat{\mathbb{Z}},1) = 0$. Kantor and Lubotzky proved in [KL90a, Proposition 11] that the free profinite group of rank d is not PFG if $d \geq 2$. It was observed by Fried and Jarden in 1986 (first edition of [FJ08]) that procyclic groups are PFG. This was extended by Kantor and Lubotzky in [KL90a, Proposition 12] to finitely generated abelian profinite groups. In his 1996 paper, Mann proved that finitely generated prosoluble groups are PFG ([Man96, Theorem 10]), and so are the profinite completions of the groups $\mathrm{SL}(k,R)$ where $k \geq 3$ and R the ring of integers in an algebraic number field. He also indicated that a similar result holds for other simple arithmetic groups that have the congruence subgroup property ([Man96, Theorem 15]). Moreover, Borovik, Pyber and Shalev showed in [BPS96] that finitely generated profinite groups not involving all finite groups as quotients of open subgroups are PFG.

One could ask for necessary and sufficient conditions for a profinite group to be PFG. The following concept is a useful tool for characterizing PFG groups:

Definition 1.1.3. *Let G be a group (not necessarily profinite). We say that G has polynomial maximal subgroup growth (PMSG) if there exists a number s, such that for all numbers n, the number $m_n(G)$ of maximal subgroups of G of index n is at most n^s.*

Mann observed in [Man96, Theorem 3] that if G has PMSG then G is PFG. Let us sketch the proof of this fact. If k elements do not generate the group G then they belong to some maximal M of G. The probability for this event is $|G:M|^{-k}$. Hence

$$1 - P(G,k) \leq \sum_{M \max G} |G:M|^{-k} = \sum_{n>1} m_n(G) n^{-k}.$$

If $m_n(G) \leq n^\alpha$ then by choosing $k \geq \alpha + 2$ we see that

$$1 - P(G,k) \leq \sum_{n>1} n^{\alpha-k} \leq \sum_{n>1} n^{-2} < 1$$

which implies that $P(G,k) > 0$. The converse holds but it is not trivial.

Theorem 1.1.4 ([MS96, Theorem 4])**.** *A profinite group is positively finitely generated if and only if it has polynomial maximal subgroup growth.*

Proof. Let us sketch the main stages of the proof. Suppose G is PFG and fix k with $P(G,k) > 0$. Our aim is to show that $m_n(G)$ grows at most polynomially with n.

Step 1 Use the Classification of Finite Simple Groups and the O'Nan-Scott theorem to show that there is a constant c such that the number of core-free maximal subgroups of index n in an arbitrary finite group is at most cn^5. Here, a maximal subgroup M is called core-free if its normal core $\mathrm{core}_G(M) := \bigcap_{g\in G} M^g$ is trivial.

Step 2 Since G is PFG, G is finitely generated. Hence G has at most countably many maximal subgroups. We say that two maximal subgroups are equivalent if they have the same normal core. In each equivalence class, choose a representative with minimal index in G. Let $\{M_i\}_{i\in\mathbb{N}}$ be the set of representatives and for each n, let $q_n(G)$ be the number of indices i such that $|G : M_i| = n$.

Apply the Borel-Cantelli Lemma to deduce that $q_n(G)$ grows polynomially.

Borel-Cantelli Lemma. *Let X_i be a series of events in a probability space X with probabilities p_i $(i \geq 1)$.*

(i) if $\sum p_i = \infty$ and X_i are pairwise independent then with probability 1 infinitely many of the events X_i happen.

(ii) if $\sum p_i < \infty$ then with probability 1 only finitely many of the events X_i happen.

We explain how to apply the lemma. Let X be G^k considered as a probability space, and set $X_i = M_i^k$ for each i. It is easy to see that, if the maximal subgroups M, L of G have different cores, then M^k, L^k are independent events in G^k. Therefore the events X_i are pairwise independent. Obviously, the probability that X_i holds is $p_i = |G : M_i|^{-k}$.

We claim that $\sum p_i < \infty$. Suppose otherwise, then by part (i) of the Borel-Cantelli Lemma, with probability 1, infinitely many of the events X_i happen. Hence $x_1, \cdots, x_k$ lie in infinitely many subgroups M_i with probability 1. This certainly implies $P(G,k) = 0$, a contradiction. Therefore $\sum p_i < \infty$.

Now, note that

$$\sum p_i = \sum |G : M_i|^{-k} = \sum q_n(G) n^{-k}$$

It follows that $\sum q_n(G) n^{-k} < \infty$, so $q_n(G) = o(n^k)$.

Step 3 Prove that $m_n(G)$ is bounded in terms of $q_n(G)$.

If M is a maximal subgroup of G of index n then $\mathrm{core}_G(M) = N_i$ for some i such that $|G : M_i| \leq n$. The number of possibilities for i is then $q_2(G) + \cdots + q_n(G)$. Applying Step 1 to G/N_i, we see that for a given N_i, the number of such maximal subgroups M is at most cn^5. On the other hand, by Step 2 we have $q_n(G) = o(n^k)$. The number of possibilities for M is then

$$m_n(G) \leq cn^5(q_2(G) + \cdots + q_n(G)) = o(n^{k+6})$$

□

Theorem 1.1.4 gives us a characterization of PFG groups in terms of maximal subgroup growth. However, a structural characterization of PMSG groups is still missing.

In the very recent paper [JZP11], Jaikin-Zapirain and Pyber give a semi-structural characterization which really describes which groups are PFG. One of those results is the following:

Theorem 1.1.5. *Let G be a finitely generated profinite group. Then G is PFG if and only if there exists a constant c such that for any almost simple group R, any open subgroup H of G has at most $l(R)^{c|G:H|}$ quotients isomorphic to R, where $l(R)$ is the minimal degree of a faithful transitive permutation representation of R.*

The full statement of this result with seven equivalent conditions is stated in [JZP11, Theorem 11.1]. Theorem 1.1.5 immediately implies a positive solution of a well-known open problem of Mann ([Man96]).

Corollary 1.1.6. *[JZP11, Corollary 12.1] Let H be an open subgroup in a PFG group. Then H is also a PFG group.*

In [Man96, Section 5], Mann conjectured that

Conjecture A. *For a PFG group G, the values $P(G,k)$ could be interpolated to an analytic function $P(G,s)$ defined in some right half-plane of the complex plane.*

For example, for $G = \widehat{\mathbb{Z}}$, we have that

$$P(\widehat{\mathbb{Z}},k) = \sum_n \frac{\mu(n)}{n^k} = \frac{1}{\zeta(k)}.$$

Theorem 1.1.7. *[Hal36] If G is a finite group, then the conjecture holds, and*

$$P(G,t) = \sum_{H \leq G} \frac{\mu_G(H)}{|G:H|^t}$$

where μ_G is the Möbius function defined for all subgroups H of G recursively by $\mu_G(G) = 1$ and $\sum_{K \geq H} \mu_G(K) = 0$ if $H < G$.

Proof. Let $\Phi(G,t)$ be the number of ordered t-tuples $(x_1, \cdots, x_t)$ such that $G = \langle x_1, \cdots, x_t \rangle$. Since each t-tuple generates a subgroup of G, we have that

$$\sum_{H \leq G} \Phi(H,t) = |G|^t.$$

Möbius inversion now yields

$$\Phi(G,t) = \sum_{H \leq G} \mu_G(H)|H|^t$$

and hence

$$P(G,t) = \frac{\Phi(G,t)}{|G|^t} = \sum_{H \leq G} \frac{\mu_G(H)}{|G:H|^t}.$$

□

Let G now be a PFG group. As noted already, k elements generate G if and only they do not belong to any maximal subgroup, i.e., they belong to $G \setminus \bigcup_{M \max G} M$. Using the inclusion-exclusion principle, the probability for this is

$$1 - \sum \frac{1}{|G:M|^k} + \sum \frac{1}{|G:M \cap L|^k} - \cdots \tag{S}$$

where $M, L, \cdots$ range over all maximal subgroups of G. This expression makes sense only if each of the infinitely many sums occuring in it converges. We rearrange it as

follows. First, choose a descending subgroup base $\{N_i\}$. Then let X_i be the set of maximal subgroups containing N_i. Then $P(G,k)$ is the limit, as $n \to \infty$, of the probability that a random k-tuple does not lie in a maximal subgroup in the set X_n. This probability is a finite sum, consisting of the terms in (S) that involve only maximal subgroups from X_n, and the limit of this sum can be formally rearranged in the form

$$P(G,k) = \sum \frac{\mu(H)}{|G:H|^k} \tag{M}$$

for some coefficients $\mu(H)$, where H ranges over all open subgroups of finite index of G, these being ordered by starting with the subgroups in X_1, and their intersections, arranged in some way, then adding the other intersections of subgroups in X_2, arranged in some way, then adding the remaining ones coming from X_3, etc. Note that the group G itself is included, with coefficient 1. To get a usual Dirichlet series, we have to add together terms corresponding to subgroups of the same index. The probability $P(G,k)$ is actually equal to the sum of the series (M), provided we group together (in parentheses) for each i the subgroups that are added at the ith stage. Thus a candidate for $P(G,s)$ in Conjecture A is the series (M), with the above insertion of parentheses, and with k replaced by a complex variable s. The question is whether this series converges in some half plane. Different choices of the subgroup basis $\{N_i\}$ lead to different groupings of the terms in (M), so we have also to know if two different bases lead to the same function. In particular, it is very interesting to know when the series (M) is convergent as written (without parentheses), or even absolutely convergent.

Since (M) is obtained by rearranging (S), we see that

(i) a subgroup H can occur in (M) with a non-zero coefficient only if H is an intersection of finitely many maximal subgroups. Such a subgroup H is called a *maximal intersection*.

(ii) for such a subgroup, $\mu(H)$ is the difference between the number of ways to express H as the intersection of an even number of maximal subgroups and the way of express it as the intersection of an odd number of maximal subgroups.

Using (ii), it is easily seen that $\mu(H)$ satisfies the defining equalities for the Möbius function μ_G, and hence $\mu(H) = \mu_G(H)$. Here the Möbius function μ_G is defined on the

lattice of open subgroups of G by $\sum_{H \leq K \leq G} \mu_G(K) = 0$ unless $H = G$, in which case the sum is 1. This gives us another proof for Theorem 1.1.7. Another similar evaluation of $\mu_G(H)$ is given in [Hal36], namely: $\mu_G(H)$ is the difference between the number of chains of subgroups of even length connecting H to G and the number of such chains of odd length.

Let us give another approach to constructing the function $P(G, s)$ by means of infinite products. Let first G be a finite group and let N be a minimal normal subgroup of G. If $N \leq \mathrm{Frat}(G)$, where $\mathrm{Frat}(G)$ is the Frattini subgroup of G, which is the intersection of all maximal subgroups of G, then $P(G, k) = P(G/N, k)$. In the other case, it is shown in [Gas59, Satz 1] that $P(G, k) = P(G/N, k)P_{G,N}(k)$, where $P_{G,N}(k)$ is given by

$$P_{G,N}(k) = 1 + \sum_{r>0} (-1)^r \sum_{i_1 < \cdots < i_r} \frac{\epsilon_{i_1, \cdots, i_r}}{|G : M_{i_1} \cap \cdots \cap M_{i_r}|^k}.$$

Here $M_1, \cdots, M_m$ are the maximal subgroups of G, and $\epsilon_{i_1, \cdots, i_r}$ has the value 1 or 0, according as $HN = G$ or not, where $H = M_{i_1} \cap \cdots \cap M_{i_r}$. Note that $P_{G,N}(k)$ is the probability that a k-tuple generates G, given that it generates G modulo N. By taking a chief series of G and iterating the above formula, we obtain an expression for $P(G, k)$ as a product, indexed by the non-Frattini chief factors in the series. Here a chief series of a finite group G is a series of normal subgroups $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1$ such that each chief factor G_i/G_{i+1}, for $i = 0, \cdots, n-1$, is a minimal normal subgroup of G/G_{i+1}. A chief factor R/S of a finite group G is called non-Frattini if it is not contained in the Frattini subgroup $\mathrm{Frat}(G/S)$.

When G is a profinite group, first of all, we have the following interpretation.

Proposition 1.1.8 ([Man96, Theorem 1])**.** *Let G be a profinite group. Then we have that $P(G, k) = \inf P(G/N, k)$ where N varies over all open normal subgroups of G. Moreover, if $\{N_i\}$ is a subgroup basis for G consisting of normal subgroups, then $P(G, k) = \inf P(G/N_i, k)$.*

Proof. Since open subgroups of profinite groups are of finite index, the groups G/N are all finite. Hence $P(G/N, k)$, for an open subgroup N, is simply the ratio of the number of k-tuples generating the finite group G/N to the number of all k-tuples. Since the set of all k-tuples generating G, as a subset of G^k, is contained in the union of the cosets of N^k determined by k-tuples generating G/N, we have $P(G, k) \leq P(G/N, k)$. Thus if

$\inf P(G/N,k) = 0$ then certainly $P(G,k) = 0$. If $\inf P(G/N,k) > 0$, then G/N can be generated by k elements for each open normal subgroup N, so is G (see [Wil98, Proposition 4.2.1]). Then G has only finitely many open subgroups of a given index (see [RZ10, Proposition 2.5.1]), and only countably many open subgroups in all. Therefore we can find a descending sequence of basic open normal subgroups $\{M_i\}$. Then if S, S_i denote the sets of k-tuples generating G, and generating $G \bmod M_i$, respectively, we have that $S = \bigcap S_i$ and $S_i \supseteq S_{i+1}$. So $\mu(S) = \inf \mu(S_i) = \lim \mu(S_i)$. Since for each open normal subgroup N we have $P(G/N,k) \geq P(G/M_i,k)$ for some i, we have that $P(G,k) = \inf P(G/N,k)$. Finally, if we take $\{N_i\}$ to be any subgroup basis, then each open normal subgroup N contains some N_i, so that $P(G/N,k) \geq P(G/N_i,k)$ and we have $P(G,k) = \inf P(G/N_i,k)$. □

Let G now be a finitely generated profinite group, let $\{N_i\}$ be a normal descending subgroup base and refine $\{N_i\}$ to a chief series (see Section 2.1 for definition). By Proposition 1.1.8, $P(G,k) = \inf P(G/N_i,k)$. This reduces many of our considerations to the case that G is a finite group. For each factor R/S in this series, express $P(G/S,k)$ as a product as above. In the expression for $P_{G/S,R/S}(k)$ we can, without changing its value, replace the maximal subgroups of G/S by the corresponding maximal subgroups of G.

By Proposition 1.1.8, we can express $P(G,k)$ as an infinite product, indexed by the set of non-Frattini factors in our chief series. Now replace k by the complex variable s to obtain a candidate for $P(G,s)$. We have to know if this product converges, and if products associated to different bases are equal.

The subgroups H that occur inside the factors of the product are maximal intersections, but not all maximal intersections occur. Rather, a maximal intersection H occurs only if it satisfies $HR = G$, where R/S is a factor in the given chief series, and S is the first term in this series that is contained in H. The factor R/S is determined by H, but H may occur more than once in the corresponding factor of the product, because it may be expressed in more than one way as a maximal intersection. For each such expression H occurs with a coefficient 1 or -1, according as the number of maximal subgroups involved is even or odd, so H occurs with coefficient $\mu(H)$. We then can write our product as

$$\prod_{R/S} \left(1 + \sum_{G=HR} \frac{\mu_G(H)}{|G:H|^s}\right). \tag{N}$$

Since the factors in the product are probabilities, they lie between 0 and 1, and writing the product as $\prod(1+x_n)$, its convergence is equivalent of the convergence of the sum $\sum x_n$. We see that the convergence of our product is equivalent to the convergence of a sum that looks like (M), but in which only some of the maximal intersections occur.

Proposition 1.1.9. *[Man96, Proposition 18] Given a descending normal subgroup basis, the series* (M) *and product* (N) *have the same domain of convergence, and in this domain, they define the same function.*

Proof. We compare the partial sum S_i of the series consisting of the intersections of maximal subgroups from X_i and the partial product P_i of the factors corresponding to chief factors above N_i. For an integer k, we have $S_i(k) = P_i(k) = P(G/N_i, k)$. Developing the product P_i, it and S_i are Dirichlet polynomials $\sum u_n/n^s$, which have the same value at all large integers, therefore they have the same coefficients u_n, so $S_i(s) = P_i(s)$ for all s. Since the infinite series and product are the limits of S_i and P_i, the Proposition follows. □

If G is a finite soluble group then, as remarked in [Gas59], the formula for $P_{G,N}(k)$ becomes particularly simple. A subgroup H occurs only if it is a maximal subgroup complementing N, so $P_{G,N}(k) = 1 - k(N)/|N|^k$, where $k(N)$ is the number of complements of N (the exact value of $k(N)$ is given in [Gas59]). Therefore, for a prosoluble group the infinite product associated to a chief series takes the form

$$P(G,k) = \prod(1 - k(N)/|N|^k) \tag{P}$$

where the product runs over all complemented chief factors in this chief series. More generally, for any PFG group the factors corresponding to an abelian N have the same form as in (P), and the proof that for prosoluble groups the above product converges ([Man96, Theorem 19]), shows that for any PFG group, the product of the terms corresponding to abelian chief factors converges.

In a more recent paper (see [Man05]), Mann made the conjecture more precise.

Conjecture B. *Let G be a PFG group. Then the infinite series* (M) *converges absolutely in some right half plane.*

Mann also noted in [Man05] the following.

Theorem 1.1.10. *The series* (M) *converges absolutely in some right half plane if and only if G has polynomially bounded Möbius number (PBMN) (see [Luc11a]), i.e., G has the following two properties:*

(1) $\mu_G(H)$ is bounded by a polynomial function in the index of H;

(2) the number $b_n(G)$ of subgroups H of index n satisfying $\mu_G(H) \neq 0$ grows at most polynomially in n.

Proof. If (M) converges absolutely, then $\mu_G(H)/|G : H|^s \to 0$, so μ grows polynomially. Also, since $\mu_G(H)$ is an integer, the subgroups of index n contribute at least b_n/n^s to the series of absolute values, so b_n also grows polynomially. The converse is equally clear. □

Corollary 1.1.11. *If* (M) *converges absolutely in some half plane, then* (N) *also converges absolutely in some half plane, and the two functions are identical in their common domain of convergence.*

Proof. Assume that (M) converges absolutely, so, by Theorem 1.1.10, b_n and μ are bounded by some power n^t. Note that in the term corresponding to $N = R/S$ in the series (N), we have for each subgroup H occurring there, $R/S \cdot H/S = G/S$ so $|G : H| \leq |R/S| = |N|$. It follows that if we write that term as $1 + x_N$, then $|x_N| \leq |N|^{2t-s}$, and $\sum_{|N|\leq n} |x_N| \leq n^{2t+1-s}$. Thus for s large enough, we have $|x_N| < 1$. Therefore the absolute convergence of (N) is equivalent to that of $\sum x_N$, which holds for $s > 2t + 2$.

Now developing the products (N) and collecting together terms with the same value of $|N|$, we get a Dirichlet series, and a similar collection process applied to (M) yields another Dirichlet series. Both series have the same value $P(G, k)$ for all large integers k, therefore the two series are identical, and define the same function. □

Mann also proved in [Man05] that the conditions in Theorem 1.1.10 are satisfied if G is the completion of $\Gamma(R)$ with respect to the congruence topology, with Γ a simple algebraic group defined over $\mathbb{Z}$ and R the ring of integers in some algebraic number field. In [Luc07] it is proved that the properties (1) and (2) hold if G is a finitely generated prosoluble group. In recent paper [Luc11b], Lucchini proved that the conjecture holds if G has polynomial subgroup growth (PSG) (or more generally, if G contains a normal

closed prosoluble subgroup N such that G/N has PSG). Moreover, he also showed in [Luc11b] that the conjecture holds if G is a finitely generated adelic profinite group, i.e., a closed subgroup of the cartesian product $\prod_p \mathrm{SL}(m, \mathbb{Z}_p)$, $m \geq 2$, with $\mathbb{Z}_p$ the ring of the p-adic integers.

In [Luc10], it is proved that in order to decide whether a finitely generated profinite group G has PBMN, it suffices to investigate the behaviour of the Möbius function of the subgroup lattice of the finite monolithic groups, that appear as epimorphic images of G. Here, a finite monolithic group L is a group with a unique minimal normal subgroup. The socle $\mathrm{soc}(G)$ of a finite group G is the subgroup generated by the minimal normal subgroups of G. We say that L is (η_1, η_2)-*bounded* if there exist two constants η_1 and η_2 such that

(1) $b_n^*(L) \leq n^{\eta_1}$, where $b_n^*(L)$ denotes the number of subgroups K of L with $|L : K| = n$ and $L = K \cdot \mathrm{soc}(L)$;

(ii) $|\mu_L(K)| \leq |L : K|^{\eta_2}$ for each $K \leq L$ with $L = K \cdot \mathrm{soc}(L)$.

In [Luc10] the following is proved. Denote by $\Lambda(G)$ the set of finite monolithic groups L such that $\mathrm{soc}(L)$ is nonabelian and L is an epimorphic image of G. A PFG group G has PBMN if and only if there exist η_1 and η_2 such that each $L \in \Lambda(G)$ is (η_1, η_2)-bounded. Let now L be a finite monolithic group with nonabelian socle, then $\mathrm{soc}(L) = S_1 \times \cdots \times S_r$, where the groups S_i are isomorphic simple groups. In the recent paper [Luc11a], Lucchini showed a stronger reduction theorem, which requires us to deal only with almost simple groups: let X_L be the subgroup of $\mathrm{Aut}(S_1)$ induced by the conjugation action of $N_G(S_1)$ on S_1. This X_L is a finite almost simple group, uniquely determined by L (see Chapter 2 for more details). It is proved in [Luc11a] that.

Theorem 1.1.12. *Let L be a monolithic group with nonabelian socle. If the associated almost simple group X_L is (c_1, c_2)-bounded, then L is (η_1, η_2)-bounded with $\eta_1 = 10 + 2(1 + c_1 + c_2)/r$ and $\eta_2 = 2c_2 + 8$.*

Combined with [Luc10, Theorem 1], we have that.

Corollary 1.1.13. *A PFG group has PBMN if there exist c_1 and c_2 such that X_L is (c_1, c_2)-bounded for each L in $\Lambda(G)$.*

This theorem allows us to reformulate the Conjecture B as follows.

Conjecture C. *There exist c_1 and c_2 such that any finite almost simple group is (c_1, c_2)-bounded.*

Recently, Colombo and Lucchini proved in [CL10] that this conjecture is satisfied by the symmetric and alternating groups. This implies

Corollary 1.1.14. *If G is a PFG group and, for each open normal subgroup N of G, all composition factor of G/N are either abelian or alternating groups, then G has PBMN.*

So now, leaving out all analytical concerns, we consider the series (M) as a formal Dirichlet series. Since the group G is finitely generated, it has only finitely many open subgroups of a given index (see [Hal50, Section 2]), for any $n \in \mathbb{N}$ we may define the integer $a_n = \sum_H \mu_G(H)$, where the sum is taken over all open subgroups H of G with $|G : H| = n$. We thus can rewrite the Dirichlet series (M) as

$$P_G(s) := \sum_H \frac{\mu_G(H)}{|G : H|^s} = \sum_{n \in \mathbb{N}} \frac{a_n}{n^s}. \tag{F}$$

The reciprocal of this function is called *the probabilistic zeta function* of G (see [Bos96] and [Man96]). As evidenced by the formula, $P_G(s)$ is tied to the subgroup structure of the group G. Because of this, one can believe that the algebraic combinatorial properties of the series (F) are enough to get back the structural properties of the group G.

As we have seen above, when G is prosoluble, the series (F) becomes the series (P)

$$\prod_N \left(1 - \frac{k(N)}{|N|^s}\right)$$

where $N = R/S$ runs over all non-Frattini chief factors in a chief series of G. Note that when G is prosoluble, being a minimal normal subgroup of a finite soluble group G/S, N is an elementary abelian group and so $|N|$ is a prime power, say q_N. Hence we can rewrite our series as

$$\prod_N \left(1 - \frac{k(N)}{q_N^s}\right).$$

One could ask whether G is a prosoluble group if the associated series of G has the above form. The answer is yes, and in fact we obtain more.

Theorem 1.1.15. *Let G be a finitely generated profinite group. Then the following are equivalent (see [DL04b, Theorem 1] and [Man96])*

(1) The group G is prosoluble.

(2) The series $P_G(s)$ can be written as the product $\prod_i (1 - c_i/q_i^s)$, where $c_i \geq 0$ and q_i is a prime power for each i.

(3) The sequence $\{a_n\}$ is multiplicative, that is, $a_m a_n = a_{mn}$ whenever m and n are coprime.

In particular, Theorem 1.1.15 holds for finite groups. A lot of interesting results have been obtained when G is a finite group. Let us now focus on examples of information one can gain about a finite group G solely from knowing $P_G(s)$. Damian and Lucchini generalized Theorem 1.1.15 to p-soluble groups:

Proposition 1.1.16. *[DL07a] A finite group G is p-soluble if and only if $a_{p^r d} = a_{p^r} a_d$ whenever p and d are coprime.*

One could ask whether we also have a result as in Theorem 1.1.15 for supersolvable groups. In fact, Detomi and Lucchini also described a condition for supersolvable groups.

Proposition 1.1.17. *[DL03b] A finite group G is supersolvable if and only if $P_G(s)$ is a finite product of factors of the form $1 - c_i/p_i^s$ where each p_i is a prime and each c_i is positive.*

This begs the question whether a similar result exists for nilpotent groups, but Gaschütz demonstrated that no such result can exist. Indeed, the functions $P_G(s)$ for $G = C_2 \times C_3 \times C_3$ (nilpotent) and for $G = \mathrm{Sym}(3) \times C_3$ (solvable but not nilpotent) are both equal to

$$\left(1 - \frac{1}{2^s}\right)\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{3}{3^s}\right)$$

Therefore, it is impossible to determine nilpotency strictly from $P_G(s)$. However, Damian and Lucchini did find the following result on nilpotency.

Proposition 1.1.18. *[DL05] A finite group G is nilpotent if and ony if $P_G(H, s)$ divides $P_G(s)$ for all $H \leq G$, where*

$$P_G(H, s) = \sum_{H \leq K \leq G} \frac{\mu_G(K)}{|G : K|^s}.$$

The next piece of data we can get from $P_G(s)$ is the set of primes dividing the order of G.

Proposition 1.1.19. *[DL07a] A prime p divides $|G|$ if and only if p divides n for some n with $a_n \neq 0$.*

We now turn our attention to non-soluble groups, mostly simple groups. The problem of recognizing a simple group from its probabilistic zeta function has been investigated by Lucchini, Damian, Morini in [DL04a, DL06a, DLM04] who proved the following theorem.

Theorem 1.1.20. *Let G be a nonabelian finite simple group, let H be a finite group with trivial Frattini subgroup, and assume that $P_G(s) = P_H(s)$.*

(1) If G is an alternating subgroup or a sporadic simple group, then $G \cong H$.

(2) If G and H are groups of Lie type defined over a field of characteristic p, then $G \cong H$.

Recently Patassini completed this story for the remaining finite simple groups.

Theorem 1.1.21. *[Pat11a, Theorem 1] Let G be a finite simple group and H a finite group. If $P_G(s) = P_H(s)$ then $H/\mathrm{Frat}(H) \cong G$.*

In the very beginning of the history of our subject, Boston conjectured in [Bos96] that $P'_G(1) = 0$ whenever G is a nonabelian simple group. This conjecture was proved and generalized by Shareshian in the following theorem.

Theorem 1.1.22. *[Sha98b] Let G be a finite group. Then $P'_G(1) = 0$ unless $G/O_p(G)$ is cyclic for some prime p.*

As we have known from [Gas59, Satz 1], for any normal subgroup N of a finite group G, the polynomial $P_{G/N}(s)$ divides $P_G(s)$ in the ring of finite Dirichlet series and the quotient $P_G(s)/P_{G/N}(s)$ is nontrivial if N is not in $\mathrm{Frat}(G)$. This implies that $P_G(s)$ is irreducible then $G/\mathrm{Frat}(G)$ is a simple group. We wonder whether the converse holds, in particular whether $P_G(s)$ is irreducible when G is a simple group. The answer is positive for all abelian simple groups since $P_{\mathbb{Z}/p\mathbb{Z}}(s) = 1 - 1/p^s$ for each prime p. Boston showed in [Bos96] that if $G = \mathrm{PSL}(2,7)$ then

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

Hence, the converse is not always true for nonabelian simple groups. However, some results were obtained my Damian, Lucchini and Morini as follows.

Theorem 1.1.23. *[DLM04]*

(1) For any prime $p \geq 5$, the polynomial $P_{Alt(p)}(s)$ is irreducible.

(2) If $p = 2^t - 1$ and $t \equiv 3 \mod 4$ then $P_{PSL(2,p)}(s)$ is reducible.

These were extended by recent results of Patassini appeared in [Pat] and [Pat11b] in the following theorem.

Theorem 1.1.24. *(1) Assume that $k \geq 5$. If $k \leq 4.2 \cdot 10^{16}$ or $k \geq (e^{e^{15}} + 2)^3$, then $P_{Alt(k)}(s)$ is irreducible. If we assume the Riemann Hypothesis, then $P_{Alt(k)}(s)$ is always irreducible.*

(2) Let S be a simple group of Lie type. Then $P_S(s)$ is reducible if and only if $S \cong PSL(2,p)$ for some Mersenne prime p such that $\log_2(p+1) \equiv 3 \mod 4$.

Brown and Bouc found that letting $s = -1$ gives interesting topological information about the group G. The coset poset $\mathcal{C}(G)$ is the poset of the proper cosets of G ordered by inclusion. We can use a simplicial complex $\Delta(\mathcal{C}(G))$ whose simplices are the finite chains in $\mathcal{C}(G)$ to defined the Euler characteristic $\chi(\mathcal{C}(G))$. We may then define the reduced Euler characteristic $\tilde{\chi}(\mathcal{C}(G)) = \chi(\mathcal{C}(G)) - 1$. Thanks to an observation of Bouc (see [Bou00]), Brown pointed the following.

Theorem 1.1.25. *[Bro00] Let G be a finite group. Then*

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

It is well-known that if $\Delta(\mathcal{C}(G))$ is contractible, then its reduced Euler characteristic $\widetilde{\chi}(\mathcal{C}(G))$ is zero. Hence, if $P_G(-1) \neq 0$, then the simplicial complex associated to the group G is non-contractible. In [Bro00], Brown proved the following.

Proposition 1.1.26. *If G is a finite soluble group, then $P_G(-1) \neq 0$.*

Moreover, Brown conjectured that $P_G(-1) \neq 0$ for every finite group G. Recently, Patassini has given several positive answers to this conjecture:

Theorem 1.1.27. *(1) If G is either $PSL(2,q)$ or a Suzuki group ${}^2B_2(q)$ or a Ree group ${}^2G_2(q)$, then $P_G(-1) \neq 0$ (see [Pat09]).*

(2) If G is a classical group that does not contain non-trivial graph automorphisms, then also $P_G(-1) \neq 0$ (see [Pat11c]).

1.2 Thesis problem

Let G be a finitely generated profinite group and $\{G_n\}$ a chief series of G. Since the factor G/G_n is finite, the Dirichlet series $P_{G/G_n}(s)$ is also finite and belongs to the ring $\mathcal{D}$ of Dirichlet polynomials with integer coefficients. As we have seen above for finite groups, the polynomial $P_{G/G_n}(s)$ is a divisor of $P_{G/G_{n+1}}(s)$ in the ring $\mathcal{D}$, and so there is a Dirichlet polynomial $P_n(s)$ such that $P_{G/G_{n+1}}(s) = P_{G/G_n}(s)P_n(s)$, where $P_n(s) = 1$ if G_n/G_{n+1} is a Frattini factor, i.e., $G_n/G_{n+1} \leq \mathrm{Frat}(G/G_{n+1})$. As we will see in Chapter 2, the Dirichlet series $P_G(s)$ can be written as an infinite formal product $P_G(s) = \prod_{n\in\mathbb{N}} P_n(s)$, and if we change the series $\{G_n\}_{n\in\mathbb{N}}$, the factorization remains the same up to reordering the factors.

It is possible that a Dirichlet polynomial can be written as a formal product of infinitely many non-trivial elements of $\mathcal{D}$, for example, $1 = (1-2^{-s})\prod_{n\in\mathbb{N}}(1+2^{-2^n s})$. So it is not clear whether the formal series $P_G(s) = \prod_{n\in\mathbb{N}} P_n(s)$ is finite only when $P_n(s) = 1$ for all but finitely many $n \in \mathbb{N}$. More generally, we can ask whether one can deduce finiteness properties of G from the fact that $P_G(s)$ is finite. It is not true that if $P_G(s) \in \mathcal{D}$ then G must be finite. Indeed, as noted in [Hal36, Theorem 2.3,], $\mu_G(H) \neq 0$ implies that H is an intersection of maximal subgroups of G. Thus $\mathrm{Frat}(G)$ is contained in H, where $\mathrm{Frat}(G)$ is the Frattini subgroup of G, that is the intersection of the closed maximal subgroups of G. It follows that $P_G(s) = P_{G/\mathrm{Frat}(G)}(s)$. For example (see [LS03, Chapter 11]), let G be a pro-p group with $d(G) = d$, we have $G/\mathrm{Frat}(G) \cong \mathbb{F}_p^d$. We can view $\mathbb{F}_p^d$ as a vector space V of dimension d over the field $\mathbb{F}_p$. The generating k-tuples in V are represented by $d \times k$ matrices of rank d over $\mathbb{F}_p$. Since row rank equals column rank, the number of such matrices is just the number of linearly independent d-tuples in $\mathbb{F}_p^k$, which is

$$(p^k-1)(p^k-p)\cdots(p^k-p^{d-1})$$

(this is zero if $k < d$). Dividing by $|V^{(k)}| = p^{kd}$ we get

$$P(G,k) = \prod_{i=0}^{d-1} \left(1 - \frac{p^i}{p^k}\right)$$

and so

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

Hence, this only gives us hope to get back some properties of $G/\mathrm{Frat}(G)$ instead of G from the knowledge of the probablistic zeta function $P_G(s)$. Notice that the following are equivalent:

- G has only finitely many maximal subgroups.
- $\mathrm{Frat}(G)$ has finite index.
- Any chief series contains only finitely many non-Frattini factors.

In particular, if $G/\mathrm{Frat}(G)$ is finite then $P_G(s) = P_{G/\mathrm{Frat}(G)}(s)$ is a finite Dirichlet series. We would like to ask about the converse. In particular, it was conjectured in [DL06c] the following.

Conjecture. *Let G be a finitely generated profinite group. Then $P_G(s)$ is rational, i.e., a quotient of two polynomials, only if $G/\mathrm{Frat}(G)$ is a finite group.*

As we have seen above, $P_G(s)$ can be written as an infinite product $P_G(s) = \prod_{n \in J} P_n(s)$ where J is the set of indices n such that $N_n = G_n/G_{n+1}$ is non-Frattini. A tempting argument is that if $P_G(s)$ is a finite series then $P_n(s) = 1$ for all but finitely many $n \in J$ and $G/\mathrm{Frat}(G)$ is finite. However, it is false. The problem becomes difficult and we should be more careful since we can't exclude that a formal product of infinitely many non-trivial finite Dirichlet series is finite. Let us first consider the local version for the case of prosoluble groups. Assume now that G is a finitely generated prosoluble group, and let p be a fixed prime. One could ask what information about G we may obtain if $a_{p^r} = 0$ for almost all $r \in \mathbb{N}$, and whether G contains only finitely many maximal subgroups of p-power index. Notice that the following are equivalent for a prosoluble group G:

- G contains only finitely many maximal subgroups of p-power index.

- A chief series of G contains only finitely many non-Frattini factors of p-power order.

As we have seen above, $P_G(s)$ has an Euler factorization over the set of all prime numbers

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

where

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

with Ω_p the set of indices n such that $|G_n/G_{n+1}| = p^{r_n}$ and $c_n \neq 0$. Suppose that the p-factor $P_{G,p}(s)$ is a Dirichlet polynomial, or more generally, that $P_{G,p}(s)$ is a rational function of $1/p^s$. Mann asked in [Man96] whether this implies that G has only finitely many maximal subgroups of p-power index. However, the answer to this question is negative. Detomi and Lucchini proved in [DL06c] the following.

Theorem 1.2.1. *There exists a* 2*-generated prosoluble group* G *such that for each prime* p

(1) $P_{G,p}(s)$ *is a Dirichlet polynomial.*

(2) G *contains infinitely many maximal subgroups whose indices are* p*-powers.*

Proof. Let us sketch the construction of this example. First of all, notice that if t_n is the number of irreducible polynomials in $\mathbb{F}_2[x]$ of degree n, then

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

This implies that

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

Let $H = \widehat{\mathbb{Z}^2}$ be the free pro-abelian group of rank 2 and fix an odd prime p. Then

$$P_H(s) = \zeta(s)^{-1}\zeta(s-1)^{-1} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)\left(1 - \frac{p}{p^s}\right).$$

Fix a prime p. For every integer n, the multiplicative group $\mathbb{F}_q^*$ of the finite field $\mathbb{F}_q$ with $q = p^n$ elements acts by right multiplication on the additive group $(\mathbb{F}_q, +)$, which can be viewed as a vector space of dimension n over $\mathbb{F}_p$. Hence the cyclic group C_{p^n-1} has

an irreducible representation of degree n over $\mathbb{F}_p$. Since H has at least $p^n - 1$ normal subgroups K_i with $H/K_i \cong C_{p^n-1}$, there are at least $p^n - 1$ irreducible H-modules, say $M_{p,n,i}$, with $1 \leq i \leq p^n - 1$.

Notice that $t_n \leq 2^n \leq p^n - 1$ if p odd and $t_n \leq 2^{2n} - 1$ for each n. For each prime p and each n, we consider the following t_n pairwise non-isomorphic irreducible H-modules:

$$\begin{array}{cc} M_{p,n,1}, \cdots, M_{p,n,t_n}, & \text{for } p \neq 2; \\ M_{2,2n,1}, \cdots, M_{2,2n,t_n}, & \text{for } p = 2. \end{array}$$

Note that $|M_{p,n,i}| = p^n$ for $p \neq 2$ and $|M_{2,2n,i}| = 4^n$, for each $i = 1, \cdots, t_n$. Now consider

$$G := \left(\prod_{\substack{p \text{ prime} \neq 2, \\ n \in \mathbb{N}, \\ i=1,\cdots t_n}} M_{p,n,i} \times \prod_{\substack{n \in \mathbb{N}, \\ i=1,\cdots t_n}} M_{2,2n,i} \right) \rtimes H.$$

Then G is a 2-generated prosoluble group, with infinitely many non-Frattini chief factors of p-power orders: Ω_p is infinite and G contains infinitely many maximal subgroups of p-power indices. However

$$P_{G,p}(s) = \begin{cases} \left(1 - \frac{1}{p^s}\right)\left(1 - \frac{p}{p^s}\right) \prod_n \left(1 - \frac{p^n}{(p^n)^s}\right)^{t_n} & \text{for } p \neq 2 \\ \left(1 - \frac{1}{2^s}\right)\left(1 - \frac{2}{2^s}\right) \prod_n \left(1 - \frac{4^n}{(4^n)^s}\right)^{t_n} & \text{for } p = 2. \end{cases}$$

Hence

$$P_{G,p}(s) = \begin{cases} \left(1 - \frac{1}{p^s}\right)\left(1 - \frac{p}{p^s}\right) \prod_n \left(1 - \frac{2p}{p^s}\right). & \text{for } p \neq 2 \\ \left(1 - \frac{1}{2^s}\right)\left(1 - \frac{2}{2^s}\right) \prod_n \left(1 - \frac{8}{4^s}\right). & \text{for } p = 2. \end{cases}$$

□

This does not answer our first question whether the finiteness of $P_G(s)$ implies that $G/\mathrm{Frat}(G)$ is a finite group. Indeed, the group G constructed has the property that $P_{G,p}(s)$ is finite for each prime p. However, we also have that $P_{G,p}(s) \neq 1$, so $P_G(s) = \prod_p P_{G,p}(s)$ turns out to be infinite. Nevertheless, our conjecture holds for prosoluble groups.

Theorem 1.2.2. *Let G be a finitely generated prosoluble group. Then the following are equivalent:*

(1) $a_n = 0$ for almost all $n \in \mathbb{N}$.

(2) $P_G(s)$ is a finite Dirichlet series in the ring $\mathcal{D}$.

(3) $P_G(s)$ is a rational Dirichlet series in the ring $\mathcal{D}$.

(4) G contains only finitely many maximal subgroups.

Proof. Let us recall briefly the proof of this Theorem. This will give us ingredients to deal with the conjecture in more general cases.

Let first $\pi(G)$ be the set of prime divisors of the indices of the open subgroups of G. The rationality of $P_G(s) = \prod_p P_{G,p}(s)$ implies that $\pi(G)$ is finite and $P_{G,p}(s)$ is a rational function of $1/p^s$ for all $p \in \pi(G)$. Fix a prime $p \in \pi(G)$ and let

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

We notice that for each $n \in \Omega_p$, the number r_n is the degree of an irreducible representation of the finite soluble group G/G_{n+1} over the field of p elements. We obtain the information about the composition length r_n by the following useful result from representation theory.

Proposition 1.2.3. *[DL06c] Let n be the degree of an irreducible representation of a finite soluble group X over a finite field. Then if q is a prime divisor of n then $q \leq \max\{\pi(X)\}$, where $\pi(X)$ is the set of prime divisors of X.*

So there is a prime t such that t does not divide any n in Ω_p. The proof now relies on the the following fact, which is a consequence of the Skolem-Mahler-Lech theorem (see [DL06c, Proposition 3.2]).

Theorem 1.2.4. *Let $I \subseteq \mathbb{N}$ and let q, r_i, c_i be positive integers for each $i \in I$. Assume that the product*

$$F(s) = \prod_{i \in I} \left(1 - \frac{c_i}{(q^{r_i})^s}\right)$$

is rational. In addition, assume that there exists a prime t such that t does not divide any r_i, $i \in I$ and that for every $n \in \mathbb{N}$, the set $I_n = \{i \in I : r_i \text{ divides } n\}$ is finite. Then I is a finite set.

Applying Theorem 1.2.4, we conclude that Ω_p is finite for each $p \in \pi(G)$. Since $\pi(G)$ is finite, Theorem 1.2.2 is then proved. □

Now, let G be an arbitrary finitely generated profinite group G. We can express $P_G(s)$ as an infinite formal product $P_G(s) = \prod_n P_n(s)$ where $P_n(s)$ is the Dirichlet series associated with the chief factor G_n/G_{n+1}. We would like to prove that if $P_G(s)$ is rational, then $P_n(s) = 1$ for almost all $n \in \mathbb{N}$. This would imply that $G/\mathrm{Frat}(G)$ is finite. In the prosoluble case, we used the Euler factorization $P_G(s) = \prod_p P_{G,p}(s)$. However, $P_G(s)$ admits an Euler factorization over the set of prime numbers if and only if G is prosoluble. Anyway, we can get a kind of Euler factorization over the finite simple groups by collecting together, for any simple group S, all the $P_n(s)$ such that the composition factors of G_n/G_{n+1} are isomorphic to S, as follows:

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

When we try to work with this generalized Euler factorization, we meet several problems. In the prosoluble case, it is easy to prove that if $P_G(s)$ is rational then $\pi(G)$ is finite and $P_{G,p}(s) = 1$ for all but finitely many primes. In the general case, $\pi(G)$ is finite if and only if $P_G^S(s) = 1$ for almost all simple groups S. Non of these two equivalent facts can be easily deduced from the rationality of $P_G(s)$. Even if we know that $P_G(s) = \prod_S P_G^S(s)$ is the product of finitely many Euler factors $P_G^S(s)$, we cannot easily deduce, as in the prosoluble case, that the rationality of $P_G(s)$ implies the rationality of $P_G^S(s)$ for each S. Even if we know that $P_G^S(s) = \prod_{n \in \Omega_S} P_n(s)$, where $\Omega_S = \{n \in \mathbb{N} : G_n/G_{n+1} \cong S^{r_n}\}$, is rational, we cannot apply the same trick (the consequence of Skolem-Mahler-Lech theorem) used in the prosoluble case, because the series $P_n(s)$ are now more complicated and involve many non-trivial terms. In order to deal with this problem, a clever method is to approximate each $P_n(s)$ by $\widetilde{P_n}(s)$ to produce a new series $\widetilde{P_G}(s) := \prod_n \widetilde{P_n}(s)$ which is still rational. For this, the following crucial remarks seem helpful.

Lemma 1.2.5. *Let $F(s) = \prod_{i \in \mathbb{N}} F_i(s) = \sum_n a_n/n^s$ be an infinite product of finite Dirichlet series $F_i(s)$. Define, for each prime p, the following series*

$$F^{(p)}(s) = \sum_{(n,p)=1} \frac{a_n}{n^s} \quad \text{and} \quad F_p(s) = \sum_r \frac{a_{p^r}}{(p^r)^s}$$

If $F(s)$ is rational then $F^{(p)}(s) = \prod_i F_i^{(p)}(s)$ and $F_p(s) = \prod_i F_{i,p}(s)$ are rational.

Notice that one of these reductions was used in prosoluble case as in Theorem (1.2.2). However, for non-prosoluble cases, these approximations do not ensure that we will get a desired product, i.e., these reductions are still not sufficiently strong to produce subseries $\widetilde{P_n}(s)$ of $P_n(s)$ for each n such that each $\widetilde{P_n}(s)$ is of the form $1 - c_n/(w^{r_n})^s$ as in prosoluble cases, with c_n non-negative and w a fixed positive integer, and such that the product $\prod_n \widetilde{P_n}(s)$ is still rational. Notice also that each Dirichlet series $P_n(s)$ for G_n/G_{n+1} nonabelian depends on the structure of G_n/G_{n+1}. More precisely, since G_n/G_{n+1} is a minimal normal subgroup of the finite group G/G_{n+1}, there is a number r_n and a nonabelian simple group S such that $G_n/G_{n+1} \cong S^{r_n}$. So the series $P_n(s)$ depends strongly on the structure of the simple group S. We will be more precise in Chapter 2. In addition, when $G_n/G_{n+1} \cong S^{r_n}$ is nonabelian, the group G/G_{n+1} permutes r_n simple factors isomorphic to S, and so r_n is the degree of a transitive permutation representation.

By a close investigation of subgroup indices in alternating groups, and some new reduction techniques, Detomi and Lucchini obtained the following result.

Theorem 1.2.6 ([DL07b, Theorem 6.1,p. 464])**.** *Let G be a finitely generated profinite group such that almost every composition factor is cyclic or isomorphic to an alternating group. Then $P_G(s)$ is rational only if $G/\mathrm{Frat}(G)$ is a finite group.*

The following four theorems A-D are the main results of the thesis.

Using the same techniques with a deep analysis of the structure of subgroups of simple groups of Lie type over finite fields with same characteristic, we are able to prove the following.

Theorem A. *Let p be a fixed prime and let G be a finitely generated profinite group such that almost every nonabelian composition factor is a simple group of Lie type over a finite field of characteristic p. If $P_G(s)$ is rational then $G/\mathrm{Frat}(G)$ is a finite group.*

However, the techniques used in the proof are not sufficient to deal with the case of simple groups of Lie type over finite fields of varying characteristic. In Chapter 6, we give an example supporting this. However, with the same ingredients, it is possible to obtain the result for $\mathrm{PSL}(2, p)$ as follows.

Theorem B. *Let G be a finitely generated profinite group such that almost every nonabelian*

composition factor is isomorphic to $PSL(2,p)$ *for some odd prime* $p \geq 5$*. Then* $P_G(s)$ *is rational only if* $G/\mathrm{Frat}(G)$ *is finite.*

For the remaining class of finite simple groups, i.e., sporadic simple groups, we obtain the following result.

Theorem C. *If* G *is a finitely generated profinite group such that almost every nonabelian composition factor is isomorphic to a sporadic simple group and* $P_G(s)$ *is rational, then* $G/\mathrm{Frat}(G)$ *is a finite group.*

The techniques used to prove Theorem B and Theorem C can be used to give an affirmative answer for the conjecture in a more general case by mixing up finite simple groups. In particular, the result is as follows.

Theorem D. *Let* G *be a finitely generated profinite group such that almost every nonabelian composition factor is isomorphic either to* $PSL(2,p)$ *for some odd prime* $p \geq 5$*, or to a sporadic simple group, or to an alternating group* $Alt(n)$ *where either* n *is an odd prime or* n *is a power of* 2*. If* $P_G(s)$ *is rational then* $G/\mathrm{Frat}(G)$ *is finite.*