J. Group Theory **17** (2014), 317–335
DOI 10.1515/jgt-2013-0037 

# Rationality of the probabilistic zeta functions of finitely generated profinite groups

Duong Hoang Dung and Andrea Lucchini

Communicated by Nigel Boston

**Abstract.** We prove that if the probabilistic zeta function $P_G(s)$ of a finitely generated profinite group $G$ is rational and all but finitely many nonabelian composition factors of $G$ are groups of Lie type in a fixed characteristic or sporadic simple groups, then $G$ contains only finitely many maximal subgroups.

## 1 Introduction

Let $G$ be a finitely generated profinite group. As $G$ has only finitely many open subgroups of a given index, for any $n \in \mathbb{N}$ we may define the integer $a_n(G)$ as

$$a_n(G) = \sum_H \mu_G(H),$$

where the sum is over all open subgroups $H$ of $G$ with $|G : H| = n$. Here $\mu_G(H)$ denotes the Möbius function of the poset of open subgroups of $G$, which is defined by recursion as follows: $\mu_G(G) = 1$ and $\mu_G(H) = -\sum_{H<K} \mu_G(K)$ if $H < G$. Then we associate to $G$ a formal Dirichlet series $P_G(s)$, defined as

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

Hall in [9] showed that if $G$ is a finite group and $t$ is a positive integer, then $P_G(t)$ is equal to the probability that $t$ random elements of $G$ generate $G$ or in other words

$$P_G(t) = \mathrm{Prob}_G(t) := \frac{|\Omega_G(t)|}{|G^t|},$$

where $\Omega_G(t)$ is the set of generating $t$-tuples in $G$. In [13] Mann conjectured that $P_G(s)$ has a similar probabilistic meaning for a wide class of profinite groups. More precisely define $\mathrm{Prob}_G(t) = \mu(\Omega_G(t))$, where $\mu$ is the normalised Haar

Research partially supported by MIUR-Italy via PRIN "Group theory and applications".

measure uniquely defined on the profinite group $G^t$ and $\Omega_G(t)$ is the set of generating $t$-tuples in $G$ (in the topological sense) and say that $G$ is positively finitely generated if there exists a positive integer $t$ such that $\mathrm{Prob}_G(t) > 0$. Mann conjectured that if $G$ is positively finitely generated, then $P_G(s)$ converges in some right half-plane and $P_G(t) = \mathrm{Prob}_G(t)$, when $t \in \mathbb{N}$ is large enough. The second author proved in [12] that this conjecture is true if $G$ is a profinite group with polynomial subgroup growth. But even when the convergence is not ensured, the formal Dirichlet series $P_G(s)$ encodes information about the lattice generated by the maximal subgroups of $G$ and combinatorial properties of the probabilistic sequence $\{a_n(G)\}$ reflect aspects of the structure of $G$. For example in [4] it is proved that a finitely generated profinite group $G$ is prosolvable if and only if the sequence $\{a_n(G)\}$ is multiplicative. Notice that if $H$ is an open subgroup of $G$ and $\mu_G(H) \neq 0$, then $H$ is an intersection of maximal subgroups of $G$. This implies in particular that if $G$ contains only finitely many maximal subgroups (i.e. if the Frattini subgroup $\mathrm{Frat}\, G$ of $G$ has finite index in $G$), then there are only finitely many open subgroups $H$ of $G$ with $\mu_G(H) \neq 0$ and consequently $a_n(G) = 0$ for all but finitely many $n \in \mathbb{N}$ (i.e. $P_G(s)$ is a finite Dirichlet series). A natural question is whether the converse is true. An affirmative answer has been given in the case of prosolvable groups [6]. In fact a stronger result holds: if $G$ is a finitely generated prosolvable group, then $P_G(s)$ is rational (i.e. $P_G(s) = A(s)/B(s)$ with $A(s)$ and $B(s)$ finite Dirichlet series) if and only if $G/\mathrm{Frat}\, G$ is a finite group. This has been generalized in [7] to the finitely generated profinite groups with the property that all but finitely many factors in a composition series are either abelian or alternating groups. In this paper we prove two other results of the same nature.

**Theorem 1.1.** *Let $G$ be a finitely generated profinite group. Assume that there exist a prime $p$ and a normal open subgroup $N$ of $G$ such that the nonabelian composition factors of $N$ are simple groups of Lie type over fields of characteristic $p$. Then $P_G(s)$ is rational if and only if $G/\mathrm{Frat}(G)$ is a finite group.*

**Theorem 1.2.** *Let $G$ be a finitely generated profinite group. Assume that there exists a normal open subgroup $N$ of $G$ such that the nonabelian composition factors of $N$ are sporadic simple groups. Then $P_G(s)$ is rational if and only if $G/\mathrm{Frat}(G)$ is a finite group.*

In particular, if $G$ contains a normal open subgroup $N$ all of whose nonabelian composition factors are isomorphic, then we may apply the main theorem in [6] if $N$ is prosolvable, the main theorem in [7] if $N$ has a composition factor of alternating type, Theorem 1.1 if $N$ has a composition factor of Lie type and Theorem 1.2 if a sporadic simple groups appears as a composition factor of $G$ and deduce the following corollary.

**Corollary.** *Let $G$ be a finitely generated profinite group. Assume that there exists a normal open subgroup $N$ of $G$ such that the nonabelian composition factors of $N$ are all isomorphic. Then $P_G(s)$ is rational if and only if $G/\operatorname{Frat}(G)$ is a finite group.*

The idea of the proof is the following. In [3, 5] it is proved that $P_G(s)$ can be written as formal product $P_G(s) = \prod_i P_i(s)$ of finite Dirichlet series associated with the non-Frattini factors in a chief series of $G$. On the other hand $G/\operatorname{Frat}(G)$ is finite if and only if a chief series of $G$ contains only finitely many non-Frattini factors. So the strategy is to prove that the product $\prod_i P_i(s)$ cannot be rational if it involves infinitely many nontrivial factors. A consequence of the Skolem–Mahler–Lech Theorem (see Proposition 2.2) can help us in this task. However Proposition 2.2 concerns infinite product of finite Dirichlet series involving only one nontrivial summand, but only the finite Dirichlet series associated to the abelian chief factors of $G$ have this property, while in general the finite series $P_i(s)$ are quite complicated. So we need to produce suitable "short" approximations $P_i^*(s)$ of the series $P_i(s)$, in such a way that the rationality of their product is preserved: the tool to achieve such approximation is a slight modification of a result already employed in [7] for a similar purpose (see Proposition 2.3). This requires a delicate analysis of the subgroup structure of the almost simple groups of Lie type, based in particular on the properties of the parabolic subgroups, and some information on the maximal subgroups of the sporadic simple groups.

## 2 Infinite products of formal Dirichlet series

Let $\mathcal{R}$ be the ring of formal Dirichlet series with integer coefficients. We will say that $F(s) \in \mathcal{R}$ is rational if there exist two finite Dirichlet series $A(s), B(s)$ with $F(s) = A(s)/B(s)$.

For every set $\pi$ of prime numbers, we consider the ring endomorphism of $\mathcal{R}$ defined by

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

where $a_n^* = 0$ if $n$ is divisible by some prime $p \in \pi$, $a_n^* = a_n$ otherwise. We will use the following remark:

**Remark 2.1.** For every set $\pi$ of prime numbers, if $F(s)$ is rational, then $F^\pi(s)$ is rational.

The following result is a consequence of the Skolem–Mahler–Lech Theorem.

**Proposition 2.2** ([6, Proposition 3.2]). *Let $I \subseteq \mathbb{N}$ and let $q, r_i, c_i$ be positive integers for each $i \in I$. Assume that*

(i) *for every $n \in \mathbb{N}$, the set $\{i \in I \mid r_i \text{ divides } n\}$ is finite,*

(ii) *there exists a prime $t$ such that $t$ does not divide $r_i$ for any $i \in I$.*

*If the product*

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

*is rational, then $I$ is finite.*

The following slight modification of [7, Proposition 4.3] can be proved in exactly the same way and will play a significant role in our arguments.

**Proposition 2.3.** *Let $F(s)$ be a product of finite Dirichlet series $F_i(s)$, indexed over a subset $I$ of $\mathbb{N}$:*

$$F(s) = \prod_{i \in I} F_i(s), \quad \text{where } F_i(s) = \sum_{n \in \mathbb{N}} \frac{b_{i,n}}{n^s}.$$

*Let $q$ be a prime and $\Lambda$ the set of positive integers divisible by $q$. Assume that there exists a positive integer $\alpha$ and a set $\{r_i\}_{i \in I}$ of positive integers such that if $n \in \Lambda$ and $b_{i,n} \neq 0$ then $n$ is an $r_i$-th power of some integer and $v_q(n) = \alpha r_i$ (where $v_q(n)$ is the $q$-adic valuation of $n$). Define*

$$w = \min\{x \in \mathbb{N} \mid v_q(x) = \alpha \text{ and } b_{i,x^{r_i}} \neq 0 \text{ for some } i \in I\}.$$

*If $F(s)$ is rational, then the product*

$$F^*(s) = \prod_{i \in I} \left(1 + \frac{b_{i,w^{r_i}}}{(w^{r_i})^s}\right)$$

*is also rational.*

## 3 Preliminaries and notations

Let $G$ be a finitely generated profinite group and let $\{G_i\}_{i \in \mathbb{N}}$ be a fixed countable descending series of open normal subgroups with the property that $G_0 = G$, $\bigcap_{i \in \mathbb{N}} G_i = 1$ and $G_i/G_{i+1}$ is a chief factor of $G/G_{i+1}$ for each $i \in \mathbb{N}$. In particular, for each $i \in \mathbb{N}$, there exist a simple group $S_i$ and a positive integer $r_i$ such that $G_i/G_{i+1} \cong S_i^{r_i}$. Moreover, as described in [5], for each $i \in \mathbb{N}$, a finite Dirichlet series

$$P_i(s) = \sum_{n \in \mathbb{N}} \frac{b_{i,n}}{n^s} \tag{3.1}$$

is associated with the chief factor $G_i/G_{i+1}$ and $P_G(s)$ can be written as an infinite formal product of the finite Dirichlet series $P_i(s)$:

$$P_G(s) = \prod_{i\in\mathbb{N}} P_i(s). \tag{3.2}$$

Moreover, this factorization is independent of the choice of chief series (see [3,5]) and $P_i(s) = 1$ unless $G_i/G_{i+1}$ is a non-Frattini chief factor of $G$.

We recall some properties of the series $P_i(s)$. If $S_i$ is cyclic of order $p_i$, then

$$P_i(s) = 1 - \frac{c_i}{(p_i^{r_i})^s},$$

where $c_i$ is the number of complements of $G_i/G_{i+1}$ in $G/G_{i+1}$. It is more difficult to compute the series $P_i(s)$ when $S_i$ is a nonabelian simple group. In that case an important role is played by the group $L_i = G/C_G(G_i/G_{i+1})$. This is a monolithic primitive group and its unique minimal normal subgroup is isomorphic to $G_i/G_{i+1} \cong S_i^{r_i}$. If $n \neq |S_i|^{r_i}$, then the coefficient $b_{i,n}$ in (3.1) depends only on $L_i$; more precisely we have

$$b_{i,n} = \sum_{\substack{|L_i:H|=n \\ L_i = H\,\mathrm{soc}(L_i)}} \mu_{L_i}(H).$$

It is not easy to compute these coefficients $b_{i,n}$ even for $n \neq |S_i|^{r_i}$. Some help comes from the knowledge of the subgroup $X_i$ of $\mathrm{Aut}\, S_i$ induced by the conjugation action of the normalizer in $L_i$ of a composition factor of the socle $S_i^{r_i}$ (note that $X_i$ is an almost simple group with socle isomorphic to $S_i$). More precisely, given an almost simple group $X$ with socle $S$, we can consider the following finite Dirichlet series:

$$P_{X,S}(s) = \sum_n \frac{c_n(X)}{n^s}, \quad \text{where } c_n(X) = \sum_{\substack{|X:H|=n \\ X=SH}} \mu_X(H). \tag{3.3}$$

**Lemma 3.1** ([10, Theorem 5]). *Let $S_i$ be a nonabelian simple group and let $\pi$ be a set of primes containing at least one divisor of $|S_i|$. If $n$ is not divisible by $|S_i|$ and $b_{i,n} \neq 0$, then there exists an $m \in \mathbb{N}$ with $n = m^{r_i}$ and $b_{i,n} = c_m(X_i) \cdot m^{r_i - 1}$. This implies*

$$P_i^\pi(s) = P_{X_i,S_i}^\pi(r_i s - r_i + 1).$$

We will give now a description of the finite Dirichlet series $P_{X,S}^{\{p\}}(s)$ when $S$ is a simple group of Lie type over a field of characteristic $p$ and $X$ is an almost simple group with socle $S$. We follow the notations from [1]. Recall that a simple

group of Lie type $S$ is the subgroup $A^F$ of fixed points under a Frobenius map $F$ of a connected reductive algebraic group $A$ defined over an algebraically closed field of characteristic $p > 0$. In particular, $S$ is defined over a field $\mathbb{K} = \mathbb{F}_q$ of characteristic $p$. As explained in [1, Section 3.4] a Dynkin diagram can be associated to the simple group $S$ and to the corresponding Lie algebra; moreover (see [1, Section 13.3]) to the map $F$, a symmetry $\rho$ on the Dynkin diagram of $A^F$ is associated ($\rho$ is trivial in the untwisted case). Let $I := \{\mathcal{O}_1, \dots, \mathcal{O}_k\}$ be the set of the $\rho$-orbits on the nodes of the Dynkin diagram. For every subset $J \subseteq I$, let $J^* := \bigcup_{i \in J} \mathcal{O}_i$ be a $\rho$-stable subset of the set of nodes of the Dynkin diagram and one may associate an $F$-stable parabolic subgroup $P_J$ of $S$ with $J^*$. As described in [1, Chapter 9], we may associate to $J$ a polynomial $T_{W_J}(x)$ with the property that $T_{W_J}(q) = |P_J|$. More precisely, in the notations of [1, Section 9.4],

$$T_{W_J}(x) = \sum_{w \in W_J} x^{l(w)}.$$

We have that:

**Theorem 3.2** ([14, Theorem 17]). *Let $S$ be a simple group of Lie type defined over a field $\mathbb{K} = \mathbb{F}_q$ of characteristic $p$ and let $X$ be an almost simple group with socle $S$. Then*

$$P_{X,S}^{\{p\}}(s) = (-1)^{|I|} \sum_{J \subseteq I} (-1)^{|J|} \left( \frac{T_W(q)}{T_{W_J}(q)} \right)^{1-s}.$$

*In particular, if $X$ does not contain nontrivial graph automorphisms, then*

$$P_{X,S}^{\{p\}}(s) = P_S^{\{p\}}(s).$$

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

**Definition 3.3.** Let $n \in \mathbb{N}$ with $n > 1$. 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 [15]:

**Theorem 3.4** (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:*

(i) $n = 2$, $a = 2^s - 1$, *where* $s \geq 2$.

(ii) $n = 6$, $a = 2$.

Observe that there may be more than one primitive prime divisor of $a^n - 1$; we denote by $\langle a, n\rangle$ the set of these primes.

Let $p$ be a prime, $r$ be a prime distinct from $p$ and $m$ be an integer which is not a power of $p$. We define

$$\zeta_p(r) = \min\{z \in \mathbb{N} \mid z \geq 1 \text{ and } p^z \equiv 1 \mod r\},$$
$$\zeta_p(m) = \max\{\zeta_p(r) \mid r \text{ prime}, r \neq p, r \mid m\}.$$

The value of $\zeta_p(S) := \zeta_p(|S|)$ when $S$ is a simple group of Lie type over $\mathbb{F}_q$ and $q = p^f$ is given in [11, Table 5.2.C].

**Proposition 3.5.** *Let $X$ be an almost simple group with socle $S$, where $S$ is a simple group of Lie type defined over a field of characteristic $p$. Assume that $\zeta_p(S) > 1$ and $\zeta_p(S) > 6$ if $p = 2$. Let $\tau \in \langle p, \zeta_p(S)\rangle$. Consider the Dirichlet series*

$$P_{X,S}^{\{p\}}(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

(a) *If $a_n \neq 0$, then $\tau$ divides $n$. More precisely, $v_\tau(n) = v_\tau(p^{\zeta_p(S)} - 1)$.*

(b) *If $m > \zeta_p(S)$ and a primitive prime divisor of $p^m - 1$ divides $n$, then $a_n = 0$.*

(c) *If $n$ is the smallest positive integer such that $n \neq 1$ and $a_n \neq 0$, then $a_n < 0$.*

*Proof.* The difficult part of this proposition is (a). We use Theorem 3.2 and the description of the polynomials $T_W(t)$ and $T_{W_J}(t)$ given in [1, Sections 9.4 and 14.2] and in [14, Section 3] (see in particular Table 1). It turns out that if $q = p^f$, then $f$ divides $\zeta_p(S)$ and for each $J \subseteq I$, the polynomial $T_{W_J}(t)$ can be written as a product of suitable cyclotomic polynomials $\Phi_u(t)$ with $u \leq \zeta_p(S)/f$. Moreover $\Phi_{\zeta_p(S)/f}(t)$ appears with multiplicity exactly 1 in the factorization of $T_W(t)$ and does not divide $T_{W_J}(t)$ if $J \neq I$. This means that if $\tau \in \langle p, \zeta_p(S)\rangle$ and $J \neq I$, then

$$\begin{aligned} v_\tau(T_W(q)/T_{W_J}(q)) &= v_\tau(\Phi_{\zeta_p(S)/f}(p^f)) \\ &= v_\tau(p^{\zeta_p(S)} - 1). \end{aligned}$$

Now (b) follows from the fact that if $m > \zeta_p(S)$, then no prime divisor of $p^m - 1$ divides $|S|$. Finally (c) follows from the fact that by the way in which $a_n$ is defined, the minimality of $n$ implies that the subgroups $H$ involved in the definition of $a_n$ are maximal, thus $\mu_X(H) = -1$ and $a_n < 0$. □

Combining the previous proposition with Lemma 3.1, we obtain the following.

**Corollary 3.6.** *Assume that $G_i/G_{i+1} \cong S_i^{r_i}$ is a chief factors of $G$, where $S_i$ is a simple group of Lie type defined over a field of characteristic $p$. Assume that $\zeta_p(S_i) > 1$ and $\zeta_p(S_i) > 6$ if $p = 2$. If $\tau \in \langle p, \zeta_p(S_i)\rangle$, then we have:*

(a) *If $b_{i,n} \neq 0$ and $(n, p) = 1$, then $\tau$ divides $n$. More precisely,*

$$v_\tau(n) = r_i \cdot v_\tau(p^{\zeta_p(S_i)} - 1).$$

(b) *If $m > \zeta_p(S)$ and a primitive prime divisor of $p^m - 1$ divides $n$, then $b_{i,n} = 0$.*

(c) *If $n$ is the smallest positive integer $> 1$ such that $(n, p) = 1$ and $b_{i,n} \neq 0$, then $b_{i,n} < 0$.*

## 4 Proofs of Theorem 1.1 and Theorem 1.2

We now begin the proofs of our main results. We assume that $G$ is a finitely generated profinite group $G$ with the property that $P_G(s) = \sum_n a_n/n^s$ is rational. As described in Section 3, $P_G(s)$ can be written as a formal infinite product of finite Dirichlet series $P_i(s) = \sum_{n\in\mathbb{N}} b_{i,n}/n^s$ corresponding to the factors $G_i/G_{i+1}$ of a chief series of $G$. Let $J$ be the set of indices $i$ such that $G_i/G_{i+1}$ is a non-Frattini chief factor. Since $P_i(s) = 1$ if $i \notin J$, we have

$$P_G(s) = \prod_{j\in J} P_j(s).$$

For $C(s) = \sum_{n=1}^{\infty} c_n/n^s \in \mathcal{R}$, we define $\pi(C(s))$ to be the set of primes $q$ for which there exists at least one multiple $n$ of $q$ with $c_n \neq 0$. Notice that if $C(s)B(s) = A(s)$, then $\pi(C(s)) \subseteq \pi(A(s)) \cup \pi(B(s))$. In particular, if $C(s)$ is rational, then $\pi(C(s))$ is finite. Let $\mathcal{S}$ be the set of the finite simple groups that are isomorphic to a composition factor of some non-Frattini chief factor of $G$. The first step in the proofs of Theorems 1.1 and 1.2 is to show that $\mathcal{S}$ is finite. The proof of this claim requires the following result.

**Lemma 4.1** ([7, Lemma 3.1]). *Let $G$ be a finitely generated profinite group and let $q$ be a prime with $q \notin \pi(P_G(s))$. Then $G$ has no maximal subgroup of index a power of $q$. In particular, if $q$ divides the order of a non-Frattini chief factor of $G$, then this factor is not a $q$-group.*

Let $\pi(G)$ be the set of the primes $q$ with the properties that $G$ contains at least an open subgroup $H$ whose index is divisible by $q$. Obviously $\pi(P_G(s)) \subseteq \pi(G)$. By [7, Lemma 3.2] and the classification of the finite simple groups, $\mathcal{S}$ is finite if and only if $\pi(G)$ is finite.

**Lemma 4.2.** *If $G$ satisfies the hypotheses of either Theorem* 1.1 *or Theorem* 1.2*, then the sets $\mathcal{S}$ and $\pi(G)$ are finite.*

*Proof.* Since $P_G(s)$ is rational, we have that $\pi(P_G(s))$ is finite. Therefore, it follows from Lemma 4.1 that $\mathcal{S}$ contains only finitely many abelian groups. If $G$ satisfies the hypotheses of Theorem 1.2, then a nonabelian group in $\mathcal{S}$ is either one of the 26 sporadic simple groups or is isomorphic to a composition factor of the finite group $G/N$. In any case we have only finitely many possibilities. Consider now the case when $G$ satisfies the hypothesis of Theorem 1.1 and assume by contradiction that $\mathcal{S}$ is infinite. This is possible only if the subset $\mathcal{S}^*$ of the simple groups in $\mathcal{S}$ that are of Lie type over a field of characteristic $p$ is infinite. In particular, the set $\Omega = \{\zeta_p(S) \mid S \in \mathcal{S}^*\}$ is infinite (see [11, Table 5.2C]). Let

$$I := \{j \in J \mid S_j \in \mathcal{S}^*\},$$
$$A(s) := \prod_{i \in I} P_i(s),$$
$$B(s) := \prod_{i \notin I} P_i(s).$$

Notice that $\pi(B(s)) \subseteq \bigcup_{S \in \mathcal{S} \setminus \mathcal{S}^*} \pi(S)$ is a finite set. Since $P_G(s) = A(s)B(s)$ and $\pi(P_G(s))$ is finite, it follows that the set $\pi(A(s))$ is finite. According to Theorem 3.4, if $m$ is large enough (for example if $m > 6$), then the set $\langle p, m\rangle$ is nonempty. We can find a positive integer $m \in \Omega$ such that $\langle p, m\rangle \neq \emptyset$ but $\langle p, m\rangle \cap \pi(A(s)) = \emptyset$. Notice that if $m \neq u$, then $\langle p, m\rangle \cap \langle p, u\rangle = \emptyset$. Let $\Gamma_m$ be the set of the positive integers $n$ such that there exists a $\tau \in \langle p, m\rangle$ dividing $n$ but no prime in $\langle p, u\rangle$ divides $n$ if $u > m$. Notice that if $b_{i,n} \neq 0$, then $\zeta_p(S_i) = m$ if and only if $n \in \Gamma_m$. Set

$$r := \min\{r_i \mid S_i \in \mathcal{S}^* \text{ and } \zeta_p(S_i) = m\},$$
$$I^* := \{i \in I \mid r_i = r \text{ and } S_i \in \mathcal{S}\},$$
$$\beta := \min\{n > 1 \mid n \in \Gamma_m \text{ and } b_{i,n} \neq 0 \text{ for some } i \in I^*\}.$$

By Corollary 3.6, if $i \in I$ and $b_{i,\beta} \neq 0$, then $\zeta_p(S_i) = m$, $r_i = r$ and $b_{i,\beta} < 0$. Hence the coefficient $c_\beta$ of $1/\beta^s$ in $A(s)$ is

$$c_\beta = \sum_{i \in I,\, r = r_i} b_{i,\beta} = \sum_{i \in I^*} b_{i,\beta} < 0.$$

On the other hand, again by Corollary 3.6, all the primes in $\langle p, m\rangle$ divide $\beta$. But then $\langle p, m\rangle \subseteq \pi(A(s))$, which is a contradiction. So we have proved that $\mathcal{S}$ is finite. By [7, Lemma 3.2], it follows that $\pi(G)$ is also finite. □

The previous result allows us to employ the following.

**Proposition 4.3.** *Let $G$ be a finitely generated profinite group and assume that the set $\pi(G)$ is finite. For each $n$, there are only finitely many non-Frattini factors in a chief series whose composition length is at most $n$. Moreover there exists a prime $t$ such that no non-Frattini chief factor of $G$ has composition length divisible by $t$.*

*Proof.* Since $\pi(G)$ is finite, the set $\mathcal{S}$ of the composition factors of $G$ is also finite and therefore there exists a $u \in \mathbb{N}$ such that $|S| \leq u$ for each $S \in \mathcal{S}$. Now suppose, for a contradiction, that a chief series of $G$ contains infinitely many non-Frattini chief factors of composition length at most $n$. Let $X/Y$ be one of them: since $X/Y$ is non-Frattini, there exists a proper supplement $H/Y$ of $X/Y$ in $G/Y$. Clearly $|G : H| \leq |X/Y| \leq u^n$. In this way we construct infinitely many subgroups of index at most $u^n$, which is not possible since a finitely generated profinite group contains only finitely many subgroups of a given index. The second part of the statement is [7, Corollary 5.2]. □

For a simple group $S \in \mathcal{S}$, let $I_S = \{j \in J \mid S_j \cong S\}$. Our aim is to prove that, under the hypotheses of Theorems 1.1 and 1.2, $J$ is a finite set. We have already proved that $\mathcal{S}$ is finite, so it suffices to prove that $I_S$ is finite for each $S \in \mathcal{S}$. First we consider the case when $S$ is abelian.

**Lemma 4.4.** *Assume that $G$ is a finitely generated profinite group such that $P_G(s)$ is rational and $\pi(G)$ is finite. Then for any prime $q$, if $S$ has a subgroup with index a power of $q$, then $I_S$ is finite. In particular, if $S$ is cyclic, then $I_S$ is finite.*

*Proof.* Let $\mathcal{S}_q$ be the set of the nonabelian simple groups in $\mathcal{S}$ containing a proper subgroup of $q$-power index. A theorem proved by Guralnick [8] implies that if $T \in \mathcal{S}_q$, then there exists a unique positive integer $\alpha(T)$ with the property that $T$ contains a subgroup of index $q^{\alpha(T)}$. Consider the set $\pi$ of all the primes different from $q$. By Lemma 3.1, there exist positive integers $c_i$ and nonnegative integers $d_i$ such that

$$P_G^{\pi}(s) = \prod_{i \in I_S} \left(1 - \frac{c_i}{q^{r_i s}}\right) \prod_{T \in \mathcal{S}_q} \left(\prod_{j \in I_T} \left(1 - \frac{d_j}{q^{\alpha(T) r_j s}}\right)\right). \tag{4.1}$$

Since $\mathcal{S}$ is finite, the set $\{\alpha(T) \mid T \in \mathcal{S}_q\}$ is finite. Moreover, by Proposition 4.3, there is a prime number $t$ such that no element in

$$\{r_i \mid i \in I_S\} \cup \{\alpha(T) r_j \mid T \in \mathcal{S}_q \text{ and } j \in I_T\}$$

is divisible by $t$. Since $P_G(s)$ is rational, $P_G^{\pi}(s)$ is also rational. But then, by Proposition 2.2, the number of nontrivial factors in the product at the right side of equation (4.1) is finite. In particular, $I_S$ is a finite set. □

*Proof of Theorem* 1.1. Let $\mathcal{T}$ be the set of the almost simple groups $X$ such that there exist infinitely many $i \in J$ with $X_i \cong X$ and let $I = \{i \in J \mid X_i \in \mathcal{T}\}$. The hypotheses of Theorem 1.1 combined with Lemma 4.4 imply that $J \setminus I$ is finite. We have to prove that $J$ is finite; this is equivalent to showing that $I = \emptyset$. But then, in order to complete our proof, it suffices to prove the following claim.

**Claim.** *For every* $n \in \mathbb{N}$, $I_n = \{i \in I \mid \zeta_p(S_i) = n\} = \emptyset$.

Assume that the claim is false and let $m$ be the smallest integer such that the set $I_m \neq \emptyset$. Since $J \setminus I$ is finite and $P_G(s) = \prod_{i \in J} P_i(s)$ is rational, also the series $\prod_{i \in I} P_i(s)$ is rational. In particular, the following series is rational:

$$Q(s) = \prod_{i \in I} P_i^{\{p\}}(s).$$

We distinguish three different cases:

(1) $m = 1$, $p = 2^t - 1$, $t \geq 2$,

(2) $m \leq 5$, $p = 2$,

(3) all the other possibilities.

Assume that (1) occurs. By [11, Table 5.2.C] if $\zeta_p(S) = 1$, then $S \cong \mathrm{PSL}_2(p)$. In particular, $S$ has a subgroup of index a power of 2 and $I_S$ (and consequently $I_1$) is finite by Lemma 4.4.

In case (3), it follows by Theorem 3.4 that $\langle p, t\rangle \neq \emptyset$ for every $t > m$; we set

$$\pi = \bigcup_{t > m} \langle p, t\rangle.$$

In case (2), $\langle p, t\rangle \neq \emptyset$ whenever $t > 6$ and we set

$$\pi = \bigcup_{t > 6} \langle p, t\rangle.$$

The Dirichlet series $H(s) = Q^{\pi}(s)$ is rational. By Corollary 3.6, if $i \in I_t$ and $\tau \in \langle p, t\rangle$, then

$$P_i^{\{\tau, p\}}(s) = 1;$$

in particular $P_i^{\pi}(s) = 1$ whenever $\langle p, t\rangle \subseteq \pi$. This implies

$$H(s) = \begin{cases} \prod_{i \in I_m} P_i^{\{p\}}(s) & \text{in case (3),} \\ \prod_{\substack{i \in I_u \\ m \leq u \leq 5}} P_i^{\{2\}}(s) & \text{in case (2).} \end{cases}$$

Assume that case (3) occurs and let $\tau \in \langle p, m\rangle$. By Lemma 3.1 and Corollary 3.6, if $i \in I_m$, $(p, y) = 1$ and $b_{i,y} \neq 0$, then $y = x^{r_i}$ and $v_\tau(x) = v_\tau(p^m - 1)$. Let

$$w = \min\{x \in \mathbb{N} \mid v_\tau(x) = v_\tau(p^m - 1) \text{ and } b_{i,x^{r_i}} \neq 0 \text{ for some } i \in I_m\}.$$

By Corollary 3.6, for each $i \in I_m$, if $b_{i,w^{r_i}} \neq 0$, then $b_{i,w^{r_i}} < 0$. Moreover, if $b_{i,w^{r_i}} \neq 0$ and $X_j \cong X_i$, then $b_{j,w^{r_j}} \neq 0$, so the set $\Sigma_m = \{i \in I_m \mid b_{i,w^{r_i}} \neq 0\}$ is infinite. Applying Proposition 2.3, we obtain a rational product

$$H^*(s) = \prod_{i \in \Sigma_m} \left(1 + \frac{b_{i,w^{r_i}}}{w^{r_i s}}\right), \quad \text{where } b_{i,w^{r_i s}} < 0 \text{ for all } i \in \Sigma_m.$$

By Propositions 2.2 and 4.3, $H^*(s)$ is a finite product, i.e. $\Sigma_m$ is finite, which is a contradiction.

Finally assume that case (2) occurs. If $\zeta_p(S) \leq 5$, then $S$ is one of the following groups:

$$\mathrm{PSL}_6(2),\ \mathrm{U}_4(2),\ \mathrm{PSp}_6(2),\ \mathrm{P}\Omega_8^+(2),\ \mathrm{PSL}_3(4),\ \mathrm{SL}_5(2),\ \mathrm{PSL}_4(2),\ \mathrm{PSL}_3(2).$$

The explicit description of the Dirichlet series $P_{X,S}^{\{2\}}(s)$ when $S \leq X \leq \mathrm{Aut}(S)$ and $S$ is one of the simple groups in the previous list is included in the Appendix. Notice in particular that if $i \in \Lambda = \bigcup_{m \leq 5} I_m$, then

$$\pi(P_i^{\{2\}}(s)) \subseteq \{3, 7, 5, 31\}.$$

First consider

$$\Lambda_{31} = \{i \in \Lambda \mid 31 \in \pi(P_i^{\{2\}}(s))\}$$

and let

$$\begin{aligned} w &= \min\{x \in \mathbb{N} \mid x \text{ is odd}, v_{31}(x) = 1 \text{ and } b_{i,x^{r_i}} \neq 0 \text{ for some } i \in \Lambda\}, \\ &= \min\{x \in \mathbb{N} \mid x \text{ is odd}, v_{31}(x) = 1 \text{ and } b_{i,x^{r_i}} \neq 0 \text{ for some } i \in \Lambda_{31}\}. \end{aligned}$$

Note that if $i \in \Lambda_{31}$ and $n$ is minimal with the properties that $n$ is odd, $b_{i,n^{r_i}} \neq 0$ and $v_{31}(n) = 1$, then $b_{i,n^{r_i}} < 0$ (see Appendix). So if $b_{i,w^{r_i}} \neq 0$, then $b_{i,w^{r_i}} < 0$; moreover, by applying Proposition 2.3, we obtain a rational product

$$\begin{aligned} H^*(s) &= \prod_{i \in \Lambda} \left(1 + \frac{b_{i,w^{r_i}}}{w^{r_i s}}\right) \\ &= \prod_{i \in \Lambda_{31}} \left(1 + \frac{b_{i,w^{r_i}}}{w^{r_i s}}\right), \quad \text{where } b_{i,w^{r_i}} \leq 0 \text{ for all } i \in \Lambda_{31}. \end{aligned}$$

By Propositions 2.2 and 4.3, the set $\Lambda_{31}^* = \{i \in \Lambda_{31} \mid b_{i,w^{r_i}} \neq 0\}$ is finite, but this implies that $\Lambda_{31} = \emptyset$. Indeed, if $\Lambda_{31} \neq \emptyset$, then there exists at least one index $i$ with $i \in \Lambda_{31}^*$, moreover by assumption there are infinitely many $j$ with $X_j \cong X_i$ and all of them belong to $\Lambda_{31}^*$. Since $\Lambda_{31} = \emptyset$, if $i \in \Lambda$, then $S_i$ is isomorphic to one of the following: $\mathrm{U}_4(2), \mathrm{PSp}_6(2), \mathrm{P}\Omega_8^+(2), \mathrm{PSL}_3(4), \mathrm{PSL}_4(2), \mathrm{PSL}_3(2)$. It follows from the Appendix that if $i \in \Lambda$, $x$ is odd and $b_{i,x^{r_i}} \neq 0$, then $v_7(x) \leq 1$. But then, we may repeat the same argument as above and consider

$$\Lambda_7 = \{i \in \Lambda \mid 7 \in \pi(P_i^{\{2\}}(s))\}$$

and

$$w := \min\{x \in \mathbb{N} \mid x \text{ is odd, } v_7(x) = 1 \text{ and } b_{i,x^{r_i}} \neq 0 \text{ for some } i \in \Lambda_7\}.$$

Arguing as before we deduce that $\Lambda_7 = \emptyset$. We can see from the Appendix that this implies $S_i \cong U_4(2)$ for all $i \in \Lambda$ and

$$H^{\{5\}}(s) = \prod_{i \in \Lambda} \left(1 - \frac{3^{3r_i}}{3^{3r_i s}}\right).$$

Again, by Propositions 2.2 and 4.3, $\Lambda$ is finite and consequently $\Lambda = \emptyset$. □

*Proof of Theorem* 1.2. Let $\mathcal{T}$ be the set of the almost simple groups $X$ such that $\operatorname{soc} X$ is a sporadic simple groups and there exist infinitely many $i \in J$ with $X_i \cong X$ and let $I = \{i \in J \mid X_i \in \mathcal{T}\}$. As in the case of Theorem 1.1, we have to prove that $I = \emptyset$. For an almost simple group $X$, let $\Omega(X)$ be the set of the odd integers $m \in \mathbb{N}$ such that

- $X$ contains at least one subgroup $Y$ such that $X = Y \operatorname{soc} X$ and $|X : Y| = m$,
- if $X = Y \operatorname{soc} X$ and $|X : Y| = m$, then $Y$ is a maximal subgroup if $X$.

Note that if $m \in \Omega(X)$, $X = Y \operatorname{soc} X$ and $|X : Y| = m$, then $\mu_X(Y) = -1$; in particular, one has $c_m(X) < 0$. Combined with Lemma 3.1, this implies that if $m \in \Omega(X_i)$, then $b_{i,m^{r_i}} < 0$. Certainly $\Omega(X)$ is not empty and its smallest element is the smallest index $m(X)$ of a supplement of $\operatorname{soc} X$ in $X$ containing a Sylow 2-subgroup of $X$. When $S = \operatorname{soc} X$ is a sporadic simple group, the value of $m(X)$ can be read from [2], where, for each of these groups, the list of the maximal subgroups and their indices are given; the precise values are given in Table 1. In few cases we need to know another integer $n(X)$ in $\Omega(X)$, given in Table 2. For a fixed prime $p$, let

$$\Lambda_p = \{i \in I \mid p \in \pi(P_i^{\{2\}}(s))\}.$$

If $i \in \Lambda_{31}$, then 31 divide $|S_i|$ and $S_i \in \{\mathrm{J}_4, \mathrm{Ly}, \mathrm{O'N}, \mathrm{BM}, \mathrm{M}, \mathrm{Th}\}$. Moreover, $31^2$ does not divide $|S_i|$ so if $n$ is odd, divisible by 31 and $b_{i,n} \neq 0$, then $n = x^{r_i}$

and $v_{31}(x) = 1$. Let $m_i = n(S_i)$ if $S_i \cong \mathrm{Th}$, $m_i = m(S_i)$ otherwise. Since $m_i$ is the smallest odd number divisible by 31 and equal to the index in $X_i$ of a supplement of $S_i$, we get

$$\begin{aligned} w &= \min\{x \in \mathbb{N} \mid x \text{ is odd}, v_{31}(x) = 1 \text{ and } b_{i,x^{r_i}} \neq 0 \text{ for some } i \in I\} \\ &= \min\{x \in \mathbb{N} \mid x \text{ is odd}, v_{31}(x) = 1 \text{ and } b_{i,x^{r_i}} \neq 0 \text{ for some } i \in \Lambda_{31}\} \\ &= \min\{m_i \mid i \in \Lambda_{31}\}. \end{aligned}$$

But then by Proposition 2.3, the following Dirichlet series is rational:

$$\prod_{i \in \Lambda_{31}} \left(1 + \frac{b_{i,w^{r_i}}}{(w^{r_i})^s}\right).$$

We have $b_{i,w^{r_i}} < 0$ if $m_i = w$, $b_{i,w^{r_i}} = 0$ otherwise. By applying Propositions 2.2 and 4.3, we get that $\{i \in \Lambda_{31} \mid m_i = w\}$ is a finite set, and this implies $\Lambda_{31} = \emptyset$.

Now consider $\Lambda_{23}$. Since $\Lambda_{31} = \emptyset$, if $i \in \Lambda_{23}$, then

$$S_i \in \{\mathrm{M}_{23}, \mathrm{M}_{24}, \mathrm{Co}_1, \mathrm{Co}_2, \mathrm{Co}_3, \mathrm{Fi}_{23}, \mathrm{Fi}'_{24}\}.$$

We can repeat the argument used to proved that $\Lambda_{31} = \emptyset$. Let $m_i = n(S_i)$ if $S_i \cong \mathrm{Co}_1$, $m_i = m(X_i)$ otherwise and let $w = \min\{m_i \mid i \in \Lambda_{23}\}$. By applying Propositions 2.2 and 4.3, we get that $\{i \in \Lambda_{23} \mid m_i = w\}$ is a finite set, and this implies $\Lambda_{23} = \emptyset$.

Now we consider $\Lambda_{11}$. Since $\Lambda_{31} \cup \Lambda_{23} = \emptyset$, if $i \in \Lambda_{11}$, then

$$S_i \in \{\mathrm{M}_{11}, \mathrm{M}_{12}, \mathrm{M}_{22}, \mathrm{J}_1, \mathrm{HS}, \mathrm{Suz}, \mathrm{McL}, \mathrm{HN}, \mathrm{Fi}_{22}\}.$$

Let $m_i = n(X_i)$ if $S_i \cong \mathrm{Fi}_{22}$ or $S_i \cong \mathrm{Fi}'_{24}$, $m_i = m(X_i)$ otherwise, and let

$$w = \min\{m_i \mid i \in \Lambda_{11}\}.$$

As before, by applying Propositions 2.2 and 4.3, we get that $\{i \in \Lambda_{23} \mid m_i = w\}$ is a finite set, and this implies $\Lambda_{11} = \emptyset$. Continuing our procedure, we consider the set $\Lambda_{17}$: if $i \in \Lambda_{17}$, then $S_i \in \{\mathrm{J}_3, \mathrm{He}\}$ and we can take $w = \min\{m(X_i) \mid i \in \Lambda_{17}\}$ and deduce that $\Lambda_{17} = \emptyset$. Next we take $w = m(\mathrm{Ru})$ to prove $\Lambda_{29} = \emptyset$ and finally we take $w = m(\mathrm{J}_2)$ to prove $\Lambda_7 = \emptyset$. □

## Appendix: Exceptional cases

In this section, we give explicit formulae for $P^{(2)}_{X,S}(s)$ when $X$ is an almost simple group whose socle $S$ is of Lie type over a field of characteristic 2 and $\zeta_2(S) \leq 5$. To achieve this we use Theorem 3.2 and the description of the polynomials $T_W(t)$

and $T_{W_J}(t)$ given in [1, Sections 9.4 and 14.2] and in [14, Section 3] (see in particular Table 1). Just to see an example, consider the case $S = \mathrm{PSL}_4(2)$. Then $I = \{1, 2, 3\}$ is the set of the nodes of the Dynkin diagram. According to [14, Table 1]

$$T_W(2) = (2^4 - 1)(2^3 - 1)(2^2 - 1) = 3^2 \cdot 5 \cdot 7.$$

Moreover,

$$T_{W_J}(2) = (2^3 - 1)(2^2 - 1) = 3 \cdot 7$$

if $J \in \{\{1, 2\}, \{2, 3\}\}$,

$$T_{W_J}(2) = (2^2 - 1)(2^2 - 1) = 3^2$$

if $J = \{1, 3\}$, and

$$T_{W_J}(2) = (2^2 - 1) = 3$$

if $J$ is one of the three subsets of $I$ of cardinality 1, $T_{W_\emptyset}(2) = 1$. Hence

$$P_S^{(2)}(s) = 1 - 2(3 \cdot 5)^{(1-s)} - (5 \cdot 7)^{(1-s)} + 3(3 \cdot 5 \cdot 7)^{(1-s)} - (3^2 \cdot 5 \cdot 7)^{(1-s)}.$$

(i) $S = \mathrm{PSL}_6(2)$. If $X$ contains a graph automorphism, then

$$\begin{aligned} P_{X,S}^{(2)}(s) = 1 &- (3^2 \cdot 7 \cdot 31)^{(1-s)} - (3 \cdot 5 \cdot 7^2 \cdot 31)^{(1-s)} - (3^3 \cdot 7 \cdot 31)^{(1-s)} \\ &+ 2(3^4 \cdot 7^2 \cdot 31)^{(1-s)} + (3^3 \cdot 5 \cdot 7^2 \cdot 31)^{(1-s)} \\ &- (3^4 \cdot 5 \cdot 7^2 \cdot 31)^{(1-s)}. \end{aligned}$$

If $X$ does not contain graph automorphisms, then

$$\begin{aligned} P_{X,S}^{(2)}(s) = 1 &- 2(3^2 \cdot 7)^{(1-s)} - (3^2 \cdot 5 \cdot 31)^{(1-s)} - 2(3 \cdot 7 \cdot 31)^{(1-s)} \\ &+ 3(3^2 \cdot 7 \cdot 31)^{(1-s)} + 6(3^2 \cdot 5 \cdot 7 \cdot 31)^{(1-s)} \\ &+ (3 \cdot 5 \cdot 7^2 \cdot 31)^{(1-s)} - 4(3^3 \cdot 5 \cdot 7 \cdot 31)^{(1-s)} \\ &- 6(3^2 \cdot 5 \cdot 7^2 \cdot 31)^{(1-s)} + 5(3^3 \cdot 5 \cdot 7^2 \cdot 31)^{(1-s)} \\ &- (3^4 \cdot 5 \cdot 7^2 \cdot 31)^{(1-s)}. \end{aligned}$$

(ii) $S = \mathrm{PSL}_5(2)$. If $X$ contains a graph automorphism then

$$P_{X,S}^{(2)}(s) = 1 - (3 \cdot 5 \cdot 31)^{(1-s)} - (3^2 \cdot 7 \cdot 31)^{(1-s)} + (3^2 \cdot 5 \cdot 7 \cdot 31)^{(1-s)}.$$

If $X$ does not contain graph automorphisms, then

$$\begin{aligned} P_{X,S}^{(2)}(s) = 1 &- 2(31)^{(1-s)} - 2(5\cdot 31)^{(1-s)} + 3(3\cdot 5\cdot 31)^{(1-s)} \\ &+ 3(5\cdot 7\cdot 31)^{(1-s)} - 4(3\cdot 5\cdot 7\cdot 31)^{(1-s)} \\ &+ (3^2\cdot 5\cdot 7\cdot 31)^{(1-s)}. \end{aligned}$$

(iii) $S = \mathrm{PSL}_4(2)$. If $X$ contains a graph automorphism then

$$P_{X,S}^{(2)}(s) = 1 - (3^2\cdot 7)^{(1-s)} - (3\cdot 5\cdot 7)^{(1-s)} + (3^2\cdot 5\cdot 7)^{(1-s)}.$$

If $X$ does not contain graph automorphisms, then

$$P_{X,S}^{(2)}(s) = 1 - 2(3\cdot 5)^{(1-s)} - (5\cdot 7)^{(1-s)} + 3(3\cdot 5\cdot 7)^{(1-s)} - (3^2\cdot 5\cdot 7)^{(1-s)}.$$

(iv) $S = \mathrm{PSL}_3(2)$. If $X$ contains a graph automorphism, then

$$P_{X,S}^{(2)}(s) = 1 - (3\cdot 7)^{(1-s)}.$$

If $X$ does not contain graph automorphisms, then

$$P_{X,S}^{(2)}(s) = 1 - 2(7)^{(1-s)} + (3\cdot 7)^{(1-s)}.$$

(v) $S = \mathrm{PSL}_3(4)$. If $X$ contains a graph automorphism, then

$$P_{X,S}^{(2)}(s) = 1 - (3\cdot 5\cdot 7)^{(1-s)}.$$

If $X$ does not contain graph automorphisms, then

$$P_{X,S}^{(2)}(s) = 1 - 2(3\cdot 7)^{(1-s)} + (3\cdot 5\cdot 7)^{(1-s)}.$$

(vi) $S = \mathrm{PSp}_6(2)$. We have

$$\begin{aligned} P_{X,S}^{(2)}(s) = 1 &- (3^2\cdot 7)^{(1-s)} - (3^3\cdot 5)^{(1-s)} - (3^2\cdot 5\cdot 7)^{(1-s)} \\ &+ 3(3^3\cdot 5\cdot 7)^{(1-s)} - (3^4\cdot 5\cdot 7)^{(1-s)}. \end{aligned}$$

(vii) $S = \mathrm{U}_4(2)$. We have

$$P_{X,S}^{(2)}(s) = 1 - (3^3)^{(1-s)} - (3^2\cdot 5)^{(1-s)} + (3^3\cdot 5)^{(1-s)}.$$

(viii) $S = \mathrm{P}\Omega_8^+(2)$. We have

$$\begin{aligned} P_{X,S}^{(2)}(s) = 1 &- 3(3^2\cdot 5)^{(1-s)} - (3\cdot 5^2\cdot 7)^{(1-s)} + 3(3^3\cdot 5^2)^{(1-s)} \\ &+ 3(3^3\cdot 5^2\cdot 7)^{(1-s)} - 4(3^4\cdot 5^2\cdot 7)^{(1-s)} \\ &+ (3^5\cdot 5^2\cdot 7)^{(1-s)}. \end{aligned}$$

| $X$ | $\lvert X\rvert$ | $m(X)$ |
|---|---|---|
| $M_{11}$ | $2^4 \cdot 3^2 \cdot 5 \cdot 11$ | $11$ |
| $M_{12}$ | $2^6 \cdot 3^3 \cdot 5 \cdot 11$ | $3^2 \cdot 5 \cdot 11$ |
| $\mathrm{Aut}(M_{12})$ | $2^7 \cdot 3^3 \cdot 5 \cdot 11$ | $3^2 \cdot 5 \cdot 11$ |
| $M_{22}$ | $2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$ | $7 \cdot 11$ |
| $\mathrm{Aut}(M_{22})$ | $2^8 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$ | $7 \cdot 11$ |
| $M_{23}$ | $2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$ | $23$ |
| $M_{24}$ | $2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$ | $3 \cdot 11 \cdot 23$ |
| $J_1$ | $2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$ | $5 \cdot 11 \cdot 19$ |
| $J_2$ | $2^7 \cdot 3^3 \cdot 5^2 \cdot 7$ | $3^2 \cdot 5 \cdot 7$ |
| $\mathrm{Aut}(J_2)$ | $2^8 \cdot 3^3 \cdot 5^2 \cdot 7$ | $3^2 \cdot 5 \cdot 7$ |
| $J_3$ | $2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$ | $3^4 \cdot 17 \cdot 19$ |
| $\mathrm{Aut}(J_3)$ | $2^8 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$ | $3^4 \cdot 17 \cdot 19$ |
| $J_4$ | $2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$ | $11^2 \cdot 29 \cdot 31 \cdot 37 \cdot 43$ |
| HS | $2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$ | $3 \cdot 5^3 \cdot 11$ |
| Aut(HS) | $2^{10} \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$ | $3 \cdot 5^3 \cdot 11$ |
| Suz | $2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$ | $3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ |
| Aut(Suz) | $2^{14} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$ | $3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ |
| McL | $2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$ | $5^2 \cdot 11$ |
| Aut(McL) | $2^8 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$ | $5^2 \cdot 11$ |
| Ru | $2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$ | $3^2 \cdot 5^3 \cdot 13 \cdot 29$ |
| He | $2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$ | $5 \cdot 7^3 \cdot 17$ |
| Aut(He) | $2^{11} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$ | $3^2 \cdot 5^2 \cdot 7^2 \cdot 17$ |
| Ly | $2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$ | $5^3 \cdot 31 \cdot 37 \cdot 67$ |
| O'N | $2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$ | $3^2 \cdot 7^2 \cdot 11 \cdot 19 \cdot 31$ |
| Aut(O'N) | $2^{10} \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$ | $3^2 \cdot 7^2 \cdot 11 \cdot 19 \cdot 31$ |
| $Co_1$ | $2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$ | $3^6 \cdot 5^3 \cdot 7 \cdot 13$ |
| $Co_2$ | $2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$ | $3^4 \cdot 5^2 \cdot 23$ |
| $Co_3$ | $2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$ | $3^3 \cdot 5^2 \cdot 11 \cdot 23$ |
| $Fi_{22}$ | $2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$ | $3^7 \cdot 5 \cdot 13$ |
| $\mathrm{Aut}(Fi_{22})$ | $2^{18} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$ | $3^7 \cdot 5 \cdot 13$ |

*continued on next page*

| $X$ | $\lvert X\rvert$ | $m(X)$ |
|---|---|---|
| $\mathrm{Fi}_{23}$ | $2^{18}\cdot 3^{13}\cdot 5^2\cdot 7\cdot 11\cdot 13\cdot 17\cdot 23$ | $3^4\cdot 17\cdot 23$ |
| $\mathrm{Fi}'_{24}$ | $2^{21}\cdot 3^{16}\cdot 5^2\cdot 7^3\cdot 11\cdot 13\cdot 17\cdot 23\cdot 29$ | $3^{13}\cdot 5\cdot 7^2\cdot 13\cdot 17\cdot 29$ |
| $\mathrm{Aut}(\mathrm{Fi}'_{24})$ | $2^{22}\cdot 3^{16}\cdot 5^2\cdot 7^3\cdot 11\cdot 13\cdot 17\cdot 29$ | $3^{13}\cdot 5\cdot 7^2\cdot 13\cdot 17\cdot 29$ |
| HN | $2^{14}\cdot 3^6\cdot 5^6\cdot 7\cdot 11\cdot 19$ | $3^4\cdot 5^4\cdot 7\cdot 11\cdot 19$ |
| Aut(HN) | $2^{15}\cdot 3^6\cdot 5^6\cdot 7\cdot 11\cdot 19$ | $3^4\cdot 5^4\cdot 7\cdot 11\cdot 19$ |
| Th | $2^{15}\cdot 3^{10}\cdot 5^3\cdot 7^2\cdot 13\cdot 19\cdot 31$ | $3^8\cdot 5^2\cdot 7\cdot 13\cdot 19$ |
| BM | $2^{41}\cdot 3^{13}\cdot 5^6\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 31\cdot 47$ | $3^7\cdot 5^3\cdot 7\cdot 13\cdot 17\cdot 19\cdot 31\cdot 47$ |
| M | $2^{46}\cdot 3^{20}\cdot 5^9\cdot 7^6\cdot 11^2\cdot 13^3\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71$ | $3^{11}\cdot 5^5\cdot 7^4\cdot 11\cdot 13^2\cdot 17\cdot 19\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71$ |

Table 1. Sporadic simple groups.

| $X$ | $n(X)$ |
|---|---|
| $\mathrm{Co}_1$ | $3^4\cdot 5^2\cdot 7\cdot 11\cdot 13\cdot 23$ |
| $\mathrm{Fi}_{22}$ | $3^5\cdot 5\cdot 7\cdot 11\cdot 13$ |
| $\mathrm{Fi}'_{24}$ | $3^9\cdot 5\cdot 11\cdot 7^2\cdot 13\cdot 17\cdot 23\cdot 29$ |
| $\mathrm{Aut}(\mathrm{Fi}'_{24})$ | $3^9\cdot 5\cdot 11\cdot 7^2\cdot 13\cdot 17\cdot 23\cdot 29$ |
| Th | $3^8\cdot 5^2\cdot 7\cdot 13\cdot 19\cdot 31$ |

Table 2. The integer $n(X)$.

## Bibliography

[1] R. W. Carter, *Simple Groups of Lie Type*, Pure Appl. Math. 28, John Wiley & Sons, London, 1972.

[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of Finite Groups*, Oxford University Press, Eynsham, 1985.

[3] 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.

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

[5] E. Detomi and A. Lucchini, Crowns in profinite groups and applications, in: *Noncommutative Algebra and Geometry*, Lect. Notes Pure Appl. Math. 243, Chapman & Hall/CRC, Boca Raton (2006), 47–62.

[6] E. Detomi and A. Lucchini, Profinite groups with a rational probabilistic zeta function, *J. Group Theory* **9** (2006), no. 2, 203–217.

[7] E. Detomi and A. Lucchini, Non-prosoluble profinite groups with a rational probabilistic zeta function, *J. Group Theory* **10** (2007), no. 4, 453–466.

[8] R. Guralnick, Subgroups of prime power index in a simple group, *J. Algebra* **81** (1983), 304–311.

[9] P. Hall, The eulerian functions of a group, *Q. J. Math.* **7** (1936), 134–151.

[10] P. Jiménez-Seral, Coefficients of the probabilistic function of a monolithic group, *Glasg. Math. J.* **50** (2008), no. 1, 75–81.

[11] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Ser. 129, Cambridge University Press, Cambridge, 1990.

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

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

[14] M. Patassini, On the irreducibility of the Dirichlet polynomial of a simple group of Lie type, *Israel J. Math.* **185** (2011), 477–507.

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

Received December 23, 2012; revised June 21, 2013.

**Author information**

Duong Hoang Dung, Dipartimento di Matematica,
Università degli studi di Padova,
Via Trieste 63, 35121 Padova, Italy;
and Mathematisch Instituut, Leiden Universiteit,
Niels Bohrweg 1, 2333 CA Leiden, The Netherlands.
E-mail: dhdung1309@gmail.com

Andrea Lucchini, Dipartimento di Matematica,
Università degli studi di Padova,
Via Trieste 63, 35121 Padova, Italy.
E-mail: lucchini@math.unipd.it