Author: Duong, Hoang Dung
Title: Profinite groups with a rational probabilistic zeta function
Issue Date: 2013-05-14

Chapter 3

Simple groups of Lie type

The aim of this chapter is to give a proof for the following theorem.

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.*

3.1 Simple groups of Lie type

In this section, we will develop machinery to compute explicitly each factor $P_i^{(p)}(s)$ of $P_G^{(p)}(s)$ associated to a nonabelian chief factor $G_i/G_{i+1} \cong S_i^{r_i}$ where S_i is a simple group of Lie type over a field of characteristic p. Moreover, we also give some information about the prime divisors of the denominators in $P_i^{(p)}(s)$. This will help us later in analysing the rationality of the series $P_G(s)$. This section is mostly adapted from Chapter 3 in [Pat11a].

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 $p > 0$.

The simple groups of Lie type can be classified in several ways. For instance, they split into two classes: the Chavelley groups and the Twisted groups (see [Car72]). These groups are completely determined by a simple Lie algebra $\mathcal{L}$ over $\mathbb{C}$, a finite field $\mathbb{K}$ and a symmetry of the Dynkin diagram of $\mathcal{L}$.

In general, for the groups of Lie type, we use the notation of [Car72]. The group is denoted by ${}^kL_l(t^k)$ where $k \in \{1, 2, 3\}$ (if $k = 1$, then k is omitted), L varies over the letters

$A, \cdots, G$, and l is the Lie rank of the Lie algebra, and t^k is a power of a prime number p. In particular, the group ${}^kL_l(t^k)$ is defined over the field $\mathbb{F}_{t^k}$ of characteristic p (so we allow t to be irrational). Finally, we set $q = t$, with the exception given in the Table 3.3. Table 3.3 records the various names we use for the groups of Lie type, which gives us a classification of simple groups of Lie type into classical and exceptional groups.

3.1.1 Basic notions about Lie algebras

Let p be a prime number. Let $\mathbb{K}$ be a field of characteristic p. We denote by S a group of Lie type over the field $\mathbb{K}$. We have that S is either an *untwisted group* or a *twisted group* of Lie type. In both cases, a simple Lie algebra $\mathcal{L}$ over the field $\mathbb{K}$ is associated to S.

If S is an untwisted group of Lie type, then S is a Chevalley group $\mathcal{L}(\mathbb{K})$, which is a certain group of automorphisms of $\mathcal{L}$ over the field $\mathbb{K}$ (see [Car72, Proposition 4.4.3]). If S is a twisted group of Lie type, then S is a subgroup of a Chevalley group $\mathcal{L}(\mathbb{K})$.

Now, let S be our group of Lie type. The following objects are associated to S.

- A Killing form $(-,-)$ on the simple Lie algebra $\mathcal{L}$ over the field $\mathbb{K}$.
- A system of roots Φ in a Cartan subalgebra $\mathcal{C}$ of $\mathcal{L}$ and a system of fundamental roots Π in Φ.
- A Dynkin diagram $\mathcal{D}$, that is a graph with elements in Π as vertices, such that $r \in \Pi$ and $s \in \Pi$ are joined by a bond of strength $\frac{4(r,s)}{(r,r)(s,s)}$ ([Car72]). Table 3.4 shows the classification of simple Lie algebras through their Dynkin diagrams.
- A symmetry ρ of the Dynkin diagram of $\mathcal{L}$. In particular, the order of ρ is 1, 2 or 3. The non-trivial symmetries of the connected Dynkin diagrams are indicated in Table 3.5.

We now give some other notions and remarks on the root systems.

- Given a system of roots Φ and a fundamental system Π in Φ, let Φ^+, Φ^- be the sets of positive and negative roots, respectively, with respect to the fundamental system Φ. We recall that a root $r \in \Phi$ is a linear combination of roots of Π with integer coefficients which are all non-negative if $r \in \Phi^+$ and all non-positive if $r \in \Phi^-$.

- The vector space $\mathcal{C}$ is spanned by Π in $\mathcal{L}$. For $r \in \mathcal{C}$, the linear map $w_r : \mathcal{C} \to \mathcal{C}$ defined by
$$w_r(x) = x - \frac{2(r,x)}{(r,r)} r$$
is called a *reflection*. The Weyl group W of Φ is the subgroup of transformations of $\mathcal{C}$ generated by the reflections $\{w_r : r \in \Phi\}$ (see [Car72, Proposition 2.1.8]). Let $l(w)$ be the length of $w \in W$, defined as the minimal n such that $w = w_{r_1} \cdots w_{r_n}$ for $r_i \in \Pi$, $i \in \{1, \cdots, n\}$. Thus $l(1) = 0$. Moreover, $l(w) = |\Phi^+ \cap w^{-1}(\Phi^-)|$ (see [Car72, Theorem 2.2.2]).

- For a subset K of Π, let $\mathcal{C}_K$ be the subspace of $\mathcal{C}$ spanned by K. Let $\Phi_K = \Phi \cap \mathcal{C}_K$ and let W_K be the subgroup of W generated by the reflections $\{w_r : r \in \Phi_K\}$. Note that Φ_K is a system of roots in $\mathcal{C}_K$, the set K is a fundamental system and the Weyl group of Φ_K is W_K (see [Car72, Proposition 2.5.1]).

- An isometry τ of $\mathcal{C}$ is associated to the symmetry ρ in such a way that $\tau(r)$ is a positive multiple of $\rho(r)$ for each $r \in \Pi$. The isometry τ is uniquely determined by ρ. In particular, we observe that for every $w \in W$, the element $w^\tau = \tau^{-1} w \tau$ belongs to W. Finally, note that ρ and τ are non-trivial if and only if G is twisted.

- Let k be the number of the ρ-orbits of Π. Let $I = \{\mathcal{O}_1, \cdots, \mathcal{O}_k\}$ denote the set of ρ-orbits of Π. For each $J \subseteq I$, let $J^* = \bigcup_{K \in J} K$.

- Let $\mathcal{W}$ denote the subgroup of the Weyl group W consisting of all $w \in W$ such that $w^\tau = w$. For a subset J of I, let $\mathcal{W}_J = W_{J^*} \cap \mathcal{W}$. In particular, if $J = \{\mathcal{O}_i\}$ for some $i \in \{1, \cdots, k\}$, then let $W_i = W_{J^*} = W_{\mathcal{O}_i}$, $\mathcal{W}_i = \mathcal{W}_{J^*} = \mathcal{W}_{\mathcal{O}_i}$ and $\Phi_i = \Phi_{J^*} = \Phi_{\mathcal{O}_i}$.

- Let $\mathcal{D}'$ be the Dynkin diagram of $\mathcal{W}$, that is a graph induced by the Dynkin diagram $\mathcal{D}$ by identifying the nodes in the same ρ-orbit (see [Car72, 13.3.8]). The graph $\mathcal{D}'$ is a graph whose nodes are the elements of I, such that $\mathcal{O}_i \in I$ and $\mathcal{O}_j \in I$ are joined if there exists $r_i \in \mathcal{O}_i$ and $r_j \in \mathcal{O}_j$ such that r_i and r_j are joined in $\mathcal{D}$.

- Let K be a subset of Π. We define D_K to be the set of elements w of W such that $w(r) \in \Phi^+$ for each $r \in K$. For a subset J of I, let $\mathcal{D}_J = D_{J^*} \cap \mathcal{W}$.

- For $J \subseteq I$, let

$$T_{\mathcal{W}_J}(t) = \sum_{w \in \mathcal{W}_J} t^{l(w)}.$$

3.1.2 The parabolic subgroups of a simple group of Lie type

Let S be a simple group of Lie type defined over a field of characteristic p. Denote by B a Borel subgroup of S. A *parabolic subgroup* of S is a subgroup of S containing a Borel subgroup.

The parabolic subgroups are crucial in our study since they are the subgroups of S that contain a Sylow p-subgroup and that are intersection of maximal subgroups. We first state a result about $P_G^{(p)}(s)$ for finite groups.

Lemma 3.1.1 ([DL06a, Lemma 2]). *Let P be a Sylow p-subgroup of a finite group G, where p is a prime number. Suppose that each maximal subgroup of G which contains P, also contains $N_G(P)$. Then*

$$P_G^{(p)}(s) = P_G(P, s-1) = P_G(N_G(P), s-1)$$

where, for any subgroup K of G,

$$P_G(K,s) = \sum_{n \in \mathbb{N}} \frac{a_n(G,K)}{n^s} \quad \text{with} \quad a_n(G,K) = \sum_{\substack{|G:H|=n \\ K \leq H \leq G}} \mu_G(H).$$

Proof. First we claim that $\mu_G(H)|N_H(P)| = \mu_G(H)|N_G(P)|$ for each subgroup $P \leq H \leq G$. Indeed, if $\mu_G(H) = 0$ then we are done. Otherwise, $\mu_G(H) \neq 0$, the subgroup H is an intersection of maximal subgroups of G (see [Hal36, Theorem 2.3]), say $M_1, \cdots, M_t$. Since $P \leq M_i$, by hypothesis we get that $N_G(P) \leq M_i$ for each i. Hence $N_G(P) \leq M_1 \cap \cdots \cap M_t = H$ and so $N_G(P) = N_H(P)$. Now set $\Omega_p = \{H \leq G : v_p(|H|) = v_p(|G|)\}$, where $v_r(n)$ is the r-adic valuation of n. We have that

$$\begin{aligned} P_G^{(p)}(s) &= \sum_{H \in \Omega_p} \frac{\mu_G(H)}{|G:H|^s} = \\ &= \sum_{Q \in \mathrm{Syl}_p(G)} \sum_{Q \leq H} \frac{\mu_G(H)}{|G:H|^s} . \frac{1}{|H : N_H(Q)|} = \\ &= \sum_{Q \in \mathrm{Syl}_p(G)} \sum_{Q \leq H} \frac{\mu_G(H)}{|G:H|^{s-1}} . \frac{1}{|G : N_H(Q)|} = \end{aligned}$$

$$\begin{aligned}
&= \sum_{P \leq H} \frac{\mu_G(H)}{|G:H|^{s-1}} . \frac{|G:N_G(P)|}{|G:N_H(P)|} = \\
&= \frac{1}{|N_G(P)|} \sum_{P \leq H} \frac{\mu_G(H)|N_H(P)|}{|G:H|^{s-1}} = \\
&= \frac{1}{|N_G(P)|} \sum_{P \leq H} \frac{\mu_G(H)|N_G(P)|}{|G:H|^{s-1}} = \\
&= \sum_{P \leq H} \frac{\mu_G(H)}{|G:H|^{s-1}} = P_G(P, s-1).
\end{aligned}$$

This proves the first equality of our statement. The second one immediately follows from the previous remark that if $\mu_G(H) \neq 0$ and $P \leq H$ then $N_G(P) \leq H$. $\square$

There is a deep connection between the system of roots and the parabolic subgroups, as shown in the following proposition.

Proposition 3.1.2. *[Car72, Theorem 8.3.4, Section 8.6, Section 14.1] Let S be a simple group of Lie type over $\mathbb{K}$ and let B be a Borel subgroup of S. Let I be the set of ρ-orbits of Π and let $\mathcal{S}_B(S) = \{H \leq S : H \geq B\}$. Then there is a bijection*

$$\begin{aligned}
\Theta : \mathcal{P}(I) &\rightarrow \mathcal{S}_B(S) \\
J &\mapsto P_J
\end{aligned}$$

such that

- *$P_J \cap P_K = P_{J \cap K}$ for $J, K \subseteq I$ (so the map is a lattice isomorphism).*
- *$P_\emptyset = B$ and $P_I = S$.*
- *$|P_J| = T_{\mathcal{W}_J}(t)$.*

One may associate to J^* an F-stable parabolic subgroup P_J of S, that is a subgroup of S that contains a Sylow p-subgroup and that is an intersection of maximal subgroups of S. The following result gives us an analysis of $P_G^{(p)}(s)$ through the indices of parabolic subgroups of S.

Theorem 3.1.3 ([DL06a, Theorem 3]). *Let $S = {}^kL_l(t^k)$ be a simple group of Lie type of characteristic p. We have that*

$$P_S^{(p)}(s) = (-1)^{o(I)} \sum_{J \subseteq I} (-1)^{o(J)} |S : P_J|^{1-s} = (-1)^{o(I)} \sum_{J \subseteq I} (-1)^{o(J)} \left(\frac{T_{\mathcal{W}_I}(t)}{T_{\mathcal{W}_J}(t)} \right)^{1-s}$$

where $o(J)$ is the number of ρ-orbits in J.

Proof. Let B be an F-stable Borel subgroup of A. The unipotent radical U of B is a Sylow p-subgroup of S and $N_S(U) = B$. As is well known, a maximal subgroup of S which contains U should contain B, hence it is a maximal parabolic subgroup of S, so we can apply the Lemma 3.1.1 to get that

$$P_S^{(p)}(s) = P_S(B, s-1) = \sum_{B \leq H} \frac{\mu_S(H)}{|S : H|^{s-1}}.$$

The map $J \mapsto P_J$ is an isomorphism between the lattice $\mathcal{P}(I)$ of subsets of I ordered by inclusion, and the lattice of subgroups of S containing B. In particular, $\mu_S(P_J) = \mu_{\mathcal{P}(I)}(J) = (-1)^{o(I)-o(J)}$ (see [Sta97, 3.8.3]). As described in [Car72, Chapter 9] and Proposition 3.1.2, to any subset J of I, a parabolic subgroup W_J of the Weyl group W and a polynomial $T_{\mathcal{W}_J}(t)$ are associated with the property that $T_{\mathcal{W}_J}(t) = |P_J|$. So we have

$$\begin{aligned} P_S^{(p)}(s) &= \sum_{B \leq H} \frac{\mu_S(H)}{|S : H|^{s-1}} = \sum_{J \subseteq I} \frac{\mu_S(P_J)}{|S : P_J|^{s-1}} \\ &= \sum_{J \subseteq I} \frac{(-1)^{o(I)-o(J)}}{|S : P_J|^{s-1}} = (-1)^{o(I)} \sum_{J \subseteq I} (-1)^{o(J)} \left(\frac{T_{W_I}(t)}{T_{W_J}(t)} \right)^{1-s}. \end{aligned}$$

□

As we have seen in Proposition 3.1.3, the expression $T_{\mathcal{W}_J}(t)$ depends on the elements of J. However, there is another way to express $T_{\mathcal{W}_J}(t)$, as we will see below.

Let $\mathcal{D}'$ be the graph induced by the Dynkin diagram $\mathcal{D}$ by identifying the nodes in the same ρ-orbit. Let $I := \{\mathcal{O}_1, \cdots, \mathcal{O}_k\}$ be the set of ρ-orbits of the set of nodes of the Dynkin diagram. Denoted by $F_{\mathcal{D}'}(t)$ the polynomial

$$F_{\mathcal{D}'}(t) = \prod_{i=1}^{l} \frac{1 - \epsilon_i t^{m_i+1}}{1 - \epsilon_i t} \tag{3.1}$$

where e_i and m_i are determined as in Table 3.1 (see [Car72, Theorem 10.2.5, Theorem 14.3.1]).

$\mathcal{D}$	$m_1, \cdots, m_l$	$\mathcal{D}'$	$\epsilon_1, \cdots, \epsilon_l$
A_l	$1, \cdots, l$	$\mathcal{D}$	$1, \cdots, 1$
B_l, C_l	$1, 3, 5, \cdots, 2l-1$	${}^2A_l$	$1, -1, \cdots, (-1)^{l+1}$
D_l	$1, 3, 5, \cdots, 2l-3, l-1$	${}^2B_2$	$1, -1$
E_6	$1, 4, 5, 7, 8, 11$	${}^2D_l$	$1, 1, \cdots, 1, -1$
E_7	$1, 5, 6, 9, 11, 13, 17$	${}^3D_4$	$1, 1, \omega, \omega^2$
E_8	$1, 7, 11, 13, 17, 19, 23, 29$	${}^2E_6$	$1, -1, 1, 1, -1, 1$
F_4	$1, 5, 7, 11$	${}^2F_4$	$1, 1, -1, -1$
G_2	$1, 5$	${}^2G_2$	$1, -1$

Table 3.1: m_i and ϵ_i

In Table 3.1, we set $\omega = e^{2\pi i/3}$. In particular, note that $\mathcal{D} = \mathcal{D}'$ if and only if S is untwisted. In this case, the ϵ_i's are all 1.

By [Car72, Theorem 10.2.3 and Theorem 14.2.1], we have that

$$T_{\mathcal{W}_I}(t) = F_{\mathcal{D}'}(t).$$

If $J \subseteq I$, then $J^* = \bigcup_{K \in J} K$ is a ρ-stable subset of the set of nodes of the Dynkin diagram. For $K \subseteq \Pi$, let $\mathcal{D}_K$ be the subdiagram of $\mathcal{D}$ corresponding to the set of roots K. Let $\mathcal{D}'_J$ be the subdiagram of $\mathcal{D}'$ corresponding to the set of nodes J. Let $\mathcal{D}'_{J_1}, \cdots, \mathcal{D}'_{J_k}$ be the connected components of $\mathcal{D}'_J$. Clearly we have that $J = \bigcup_{i=1}^{k} J_i$ and the union is disjoint. Since J^* is a subset of Π, we have that $\mathcal{D}_{J^*}$ is a subdiagram of $\mathcal{D}$.

Suppose that $\mathcal{D}'_J$ is connected, then just one of the following holds:

- $\mathcal{D}_{J^*}$ is connected and $\mathcal{D}'_J$ is the Dynkin diagram $\mathcal{D}''$ of a simple group of Lie type which is untwisted if and only if $\mathcal{D}_{J^*}$ and $\mathcal{D}'_J$ are isomorphic graphs. In this case, we define $F_{\mathcal{D}'_J}(t) = F_{\mathcal{D}''}(t)$.

- $\mathcal{D}_{J^*}$ is not connected, it has $|\rho|$ components and each of its connected component is isomorphic to the Dynkin diagram $\mathcal{D}''$ of an untwisted group. In this case, we define $F_{\mathcal{D}'_J}(t) = F_{\mathcal{D}''}(t^{|\rho|})$.

Proposition 3.1.4. *[Car72, Theorem 10.2.3, Theorem 14.2.1] Under the above notations, for a subset J of I, we have*

$$T_{\mathcal{W}_J}(t) = \prod_{i=1}^{k} F_{\mathcal{D}'_{J_i}}(t). \tag{3.2}$$

Example 1 Let $S = A_3(t)$. The Dynkin diagram $\mathcal{D}$ of S is A_3 and $I = \{\{r_1\}, \{r_2\}, \{r_3\}\}$.

- Since $\mathcal{D}' = A_3$, we have

$$F_{\mathcal{D}'}(t) = \frac{1-t^2}{1-t}\frac{1-t^3}{1-t}\frac{1-t^4}{1-t} = (1+t)^2(1+t^2)(1+t+t^2).$$

- There are three subsets of I of cardinality 2, that are $J^2_{12} = \{\{r_1\}, \{r_2\}\}, J^2_{23} = \{\{r_2\}, \{r_3\}\}$ and $J^2_{13} = \{\{r_1\}, \{r_3\}\}$. The Dynkin diagrams $\mathcal{D}'_{J^2_{12}}, \mathcal{D}'_{J^2_{23}}$ of the first two subsets J^2_{12} and J^2_{23} are connected and the diagrams $\mathcal{D}'_{(J^2_{12})^*}, \mathcal{D}'_{(J^2_{23})^*}$ are isomorphic to A_2. Thus

$$F_{\mathcal{D}'_{J^2_{12}}}(t) = F_{\mathcal{D}'_{J^2_{23}}}(t) = F_{A_2}(t) = \frac{1-t^2}{1-t}\frac{1-t^3}{1-t} = (1+t)(1+t+t^2).$$

  The diagram $\mathcal{D}'_{(J^2_{13})^*}$ is disconnected and contains two connected components isomorphic to A_1, hence

$$F_{\mathcal{D}'_{J^2_{13}}}(t) = (F_{A_1}(t))^2 = \left(\frac{1-t^2}{1-t}\right)^2 = (1+t)^2.$$

- There are three subsets J^1 of I of cardinality 1. The diagram $\mathcal{D}'_{(J^1)^*}$ is isomorphic to A_1, and

$$F_{\mathcal{D}'_{(J^1)^*}}(t) = 1+t.$$

By Theorem 3.1.3, we obtain

$$\begin{aligned} P_S^{(p)}(s) &= 1 - 2((1+t)(1+t^2))^{1-s} - ((1+t^2)(1+t+t^2))^{1-s} + \\ &+ 3((1+t)(1+t^2)(1+t+t^2))^{1-s} - ((1+t)^2(1+t^2)(1+t+t^2))^{1-s}. \end{aligned}$$

3.1.3 The parabolic subgroups of an almost simple group of Lie type

Now we consider a more general setting. Let X be an almost simple group with socle S isomorphic to a simple group of Lie type over a field of characteristic $p > 0$. Let P be a Sylow p-subgroup of X. Thus $P \cap S$ is a Sylow p-subgroup of S and $B = N_S(P \cap S)$ is a Borel subgroup in S. Given a subgroup H of X, denote by $\mathcal{S}_H(X)$ the set of subgroups K of X such that $K \geq H$.

Lemma 3.1.5 ([Car72, Theorem 8.3.3])**.** *Let K be a subgroup of S such that $K \geq B$. Then $N_S(K) = K$.*

Lemma 3.1.6 (See [KL90b])**.** *Let P and B as above. We have that*

1. *$N_X(B) = N_X(P \cap S)$ and $N_X(B)S = X$;*
2. *If M is a maximal subgroup of X such that $M \geq P$ and $MS = X$ then $M \geq N_X(B)$.*

This result implies that

$$\mathcal{S}_{N_X(B)}(X) = \{H \leq X : H \geq N_X(B), HS = X\}.$$

We can generalize Lemma 3.1.1 as follows.

Lemma 3.1.7. *Let r be a prime number, let G be a finite group and let N be a normal subgroup of G. Let R be a Sylow r-subgroup of G. Suppose that if M is a maximal subgroup of G such that $MN = G$ and $R \leq M$, then M contains also $N_G(R)$. Then*

$$P^{(r)}_{G,N}(s) = \sum_{\substack{R \leq H \leq G \\ HN = G}} \frac{\mu_G(H)}{|G : H|^{s-1}}.$$

Proof. The proof is similar to the proof of Lemma 3.1.1 by considering the set $\Omega_r = \{H \leq G : HN = G \text{ and } v_r(|H|) = v_r(|G|)\}$. □

Since $P \cap S \trianglelefteq P$, then $P \trianglelefteq N_X(P) \leq N_X(P \cap S) = N_X(B)$ by Lemma 3.1.6, hence $N_X(P) \leq N_X(B)$. Therefore, Lemma 3.1.6 and Lemma 3.1.7 give us

$$P^{(p)}_{X,S}(s) = \sum_{\substack{P \leq H \leq X \\ HS = X}} \frac{\mu_X(H)}{|X : H|^{s-1}} = \sum_{H \in \mathcal{S}_{N_X(B)}(X)} \frac{\mu_X(H)}{|X : H|^{s-1}}.$$

Let $\mathcal{S}_B^X(S)$ denote the subset of $\mathcal{S}_B(S) = \{H \leq S : H \geq B\}$ given by

$$\mathcal{S}_B^X(S) = \{H \in \mathcal{S}_B(S) : N_X(H) \geq N_X(B)\}.$$

Proposition 3.1.8 ([Pat11a, Proposition 3.9])**.** *The map $\eta : \mathcal{S}_{N_X(B)}(S) \to \mathcal{S}_B^X(S)$ given by $\eta(H) = H \cap S$ is well-defined. Moreover, η is an isomorphism of posets. In particular $N_X(\eta(H)) = H$ for each $H \in \mathcal{S}_{N_X(B)}(X)$.*

Proof. We show that η is well-defined. Let $H \in \mathcal{S}_{N_X(B)}(X)$. Since $H \cap S \trianglelefteq H$ then $N_X(B) \leq H \leq N_X(H \cap S)$. Moreover, $B \trianglelefteq N_X(B) \leq H$ and $B \leq S$, so $B \leq H \cap S$. Thus $H \cap S \in \mathcal{S}_B^X(S)$.

Let $H \in \mathcal{S}_B^X(S)$. By definition, $N_X(B) \leq N_X(H)$. Since $N_X(B)S = X$ by Lemma 3.1.6, $N_X(H)S = X$. This implies $N_X(H) \in \mathcal{S}_{N_X(B)}(X)$. Its image is $\eta(N_X(H)) = N_X(H) \cap S = N_S(H) = H$ by Lemma 3.1.5. Thus η is surjective.

For any $H, K \in \mathcal{S}_{N_X(B)}(X)$ such that $H \cap S = K \cap S$, we have $N_X(H \cap S) = N_X(K \cap S)$. In order to prove that η is injective, it suffices to prove that $N_X(H \cap S) = H$. It is clear that $H \leq N_X(H \cap S)$ since $H \cap S \trianglelefteq H$. Moreover, since $HS = X$, applying Lemma 3.1.5 we get

$$|X : N_X(H \cap S)| = |S : N_X(H \cap S) \cap S| = |S : N_S(H \cap S)| = |S : H \cap S| = |X : H|$$

so $N_X(H \cap S) = H$. Hence, the map η is injective.

Clearly that η is an isomorphism of posets. $\square$

A *parabolic subgroup* of X is a subgroup H of X such that H supplements S in X and contains $N_X(B)$ for some Borel subgroup B of S, i.e., H is an element of the set $\mathcal{S}_{N_X(B)} = \{K \leq X : K \geq N_X(B), KS = X\}$.

Note that the map

$$\begin{aligned} \Theta : \mathcal{P}(I) &\to \mathcal{S}_B(S) \\ J &\mapsto P_J \end{aligned}$$

is an isomorphism of lattices. Since $N_X(B)$ acts by conjugation on $\mathcal{S}_B(S)$, the group $N_X(B)$ also acts on $\mathcal{P}(I)$. In particular, the action is the following : if $J \subseteq I$ and $g \in N_X(B)$, then J^g is the unique subset of I such that $P_{J^g} = P_J^g$. Moreover, the group $N_X(B)$ acts on I :

if $\mathcal{O}$ is a ρ-orbit, then $\{\mathcal{O}^g\} = \{\mathcal{O}\}^g$. Note that if S is twisted, then the action of $N_X(B)$ is trivial. Assume that S is untwisted. The action of $N_X(B)$ on I can be thought of as an action of $N_X(B)$ on Π. So, any element $g \in N_X(B)$ induces a symmetry ϕ_g of the Dynkin diagram $\mathcal{D}$ of S. Since $X = SN_X(B)$, if $h \in X$ then $h = sg$ for some $s \in S$ and $g \in N_X(B)$. If ϕ_g is not trivial, then we say that h is a *non-trivial graph automorphism* of order $|\phi_g|$ in X (the definition does not depend on the choice of g, since the action does not depend on the choice of g). Observe that $\mathcal{S}_B^X(S)$ is the set of fixed points of $\mathcal{S}_B(S)$ under the action of $N_X(B)$.

If X does not contain non-trivial graph automorphisms, then ϕ_g is the trivial symmetry for each $g \in N_X(B)$. In this case, we have $\mathcal{S}_B^X(S) = \mathcal{S}_B(S)$. If X contains a non-trivial graph automorphism, then S is untwisted and ρ is trivial.

Let $\mathcal{P}^X(I)$ be the subposet of $\mathcal{P}(I)$ consisting of the subsets of I which are unions of $N_X(B)$-orbits of elements of I. Moreover, if $J \in \mathcal{P}^X(I)$, let $\widetilde{J}$ be the set of $N_X(B)$-orbits of J and denote by $o(J)$ the size of $\widetilde{J}$. We have the following generalization of Theorem 3.1.3.

Theorem 3.1.9 ([Pat11a, Theorem 3.10])**.** *Let X and S as above. Then*

$$P^{(p)}_{X,S}(s) = (-1)^{o(I)} \sum_{J \in \mathcal{P}^X(I)} (-1)^{o(J)} |S : P_J|^{1-s} = (-1)^{o(I)} \sum_{J \in \mathcal{P}^X(I)} (-1)^{o(J)} \left(\frac{T_{W_I}(t)}{T_{W_J}(t)} \right)^{1-s}.$$

In particular, if X does not contain non-trivial graph automorphisms, then $P^{(p)}_{X,S}(s) = P^{(p)}_{S}(s)$.

Proof. By the above consideration, we obtain an isomorphism of posets $\eta : \mathcal{P}^X(I) \to \mathcal{S}_{N_X(B)}(X)$ given by $\eta(J) = N_X(P_J)$ for $J \in \mathcal{P}^X(I)$. In particular, we get $\mu_{\mathcal{P}^X(I)}(J) = \mu_X(N_X(P_J))$. Note that $\mu_{\mathcal{P}^X(I)}(J) = (-1)^{o(I)-o(J)}$. Indeed, there is an isomophism between the poset $\mathcal{P}^X(I)$ and the poset $\mathcal{P}(\widetilde{I})$ of subsets of $\widetilde{I}$ given by $J \mapsto \widetilde{J}$. Thus $\mu_{\mathcal{P}^X(I)}(J) = \mu_{\mathcal{P}(\widetilde{I})}(\widetilde{J})$, and by [Sta97, 3.8.3], we get $\mu_{\mathcal{P}(\widetilde{I})}(\widetilde{J}) = (-1)^{o(I)-o(J)}$.

Since $N_X(P_J) \cap S = P_J$, we have that $|X : N_X(P_J)| = |S : P_J|$. By Lemma 3.1.7, we obtain

$$\begin{aligned} P^{(p)}_{X,S}(s) &= \sum_{H \in \mathcal{S}_{N_X(B)}(X)} \frac{\mu_X(H)}{|X : H|^{s-1}} = \sum_{J \in \mathcal{P}^X(I)} \frac{\mu_X(N_X(P_J))}{|X : N_X(P_J)|^{s-1}} = \\ &= \sum_{J \in \mathcal{P}^X(I)} (-1)^{o(I)-o(J)} |S : P_J|^{1-s} = (-1)^{o(I)} \sum_{J \in \mathcal{P}^X(I)} (-1)^{o(J)} |S : P_J|^{1-s}. \end{aligned}$$

□

Example 2 Let X be an almost simple group with socle $S \cong A_3(t)$. When X does not contain graph automorphisms, we have $P_{X,S}^{(p)}(s) = P_S^{(p)}(s)$. The series $P_S^{(p)}(s)$ has been described in example 1. Assume now that X contains a graph automorphism. Here the Dynkin diagram $\mathcal{D} = \mathcal{D}'$ is A_3, and $I = \{\{r_1\}, \{r_3\}, \{r_2\}\}$. Since X contains a graph automorphism, the set of $N_X(B)$-orbits of I is $\widetilde{I} = \{\{\{r_1\}, \{r_3\}\}, \{\{r_2\}\}\}$.

- We have

$$F_{\mathcal{D}'}(t) = F_{A_3}(t) = \frac{1-t^2}{1-t}\frac{1-t^3}{1-t}\frac{1-t^4}{1-t} = (1+t)^2(1+t+t^2)(1+t^2).$$

- Let $J_1 = \{\{r_1\}, \{r_3\}\}$. The diagram $\mathcal{D}_{J_1^*}$ has two connected components isomorphic to A_1, thus

$$F_{\mathcal{D}'_{J_1}}(t) = (F_{A_1}(t))^2 = (1+t)^2.$$

- Let $J_2 = \{\{r_2\}\}$. The diagram $\mathcal{D}_{J_2^*}$ is the Dynkin diagram A_1. So

$$F_{\mathcal{D}'_{J_2}}(t) = F_{A_1}(t) = (1+t).$$

By Theorem 3.1.9, we obtain

$$\begin{aligned} P_{X,S}^{(p)}(s) &= 1 - ((1+t^2)(1+t+t^2))^{1-s} \\ &\quad -((1+t)(1+t^2)(1+t+t^2))^{1-s} + ((1+t)^2(1+t^2)(1+t+t^2))^{1-s}. \end{aligned}$$

Now let p be a fixed prime and S a simple group of Lie type defined over a finite field of characteristic p. In our work, we will deal with prime divisors of $|S|$, which contains factors of the form $p^m - 1$ where $m \in \mathbb{N}$. It was proved (see [Zsi92]) that

Proposition 3.1.10. *Let a and n be integers greater than 1. Then there exists a prime divisor r of $a^n - 1$ such that r does not divide $a^j - 1$ for any j, $0 < j < n$, except exactly in the following cases*

- $n = 2, a = 2^t - 1$, *where* $t \geq 2$.

- $n = 6, a = 2$.

If such a prime exists, we call it a *primitive prime divisor* (or *Zsigmondy prime*) for $\langle a, n\rangle$. 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. Notice that a Zsigmondy prime in $\langle a, n\rangle$ divides the cyclotomic polynomial $\Phi_n(a)$ and does not divide any $\Phi_k(a)$ whenever $k < n$.

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

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

The value of $\zeta_p(S) := \zeta_p(|S|)$ where S is a simple group of Lie type over $\mathbb{F}_q$ with $q = p^e$ is given the following table (Table 5.2.C in [KL90b]):

S	$\zeta_p(S)$	exceptions
$L_n(p^e)$ $PSp(n, p^e)$, n even, $n \geq 4$ $P\Omega^-(n, p^e)$, n even, $n \geq 8$	ne	$\zeta_p(L_2(p)) = 1$ if $p+1 = 2^t$ $\zeta(L_6(2)) = 5$ $\zeta_2(PSp(6,2)) = 4$
$U(n, p^e)$, $n \geq 3$	$2ne, n$ odd $2(n-1)e, n$ even	 $\zeta_2(U_4(2)) = 4$
$P\Omega^+(n, p^e)$, n even, $n \geq 8$	$e(n-2)$	$\zeta_2(\Omega^+(8,2)) = 4$
$\Omega(n, p^e)$, qn odd, $n \geq 7$	$e(n-1)$	
${}^2B_2(p^e)$	$4e$	
$G_2(p^e)(p^e \geq 3)$, ${}^2G_2(3^e)(3^e \geq 27)$	$6e$	
$F_4(p^e)$, ${}^2F_4(2^e)$, $E_6(p^e)$, ${}^3D_4(p^e)$	$12e$	
${}^2E_6(p^e)$	$18e$	
$E_7(p^e)$	$18e$	
$E_8(p^e)$	$30e$	

Table 3.2: Level of Zsigmondy primes

Proposition 3.1.11. *Let L be a monolithic group with socle N and assume that $N = S^r$ with S a simple group of Lie type defined over a field of characteristic p. Let $\tau \in \langle p, \zeta_p(S)\rangle$. Consider the Dirichlet series*

$$P_{L,N}^{(p)}(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}.$$

Then

(a) If $b_n \neq 0$ then τ divides n. More precisely, $v_\tau(n) = r\alpha$ with $\alpha = v_\tau(p^{\zeta_p(S)} - 1)$.

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

(c) If $n > 1$ is the smallest positive integer such that $b_n \neq 0$ then $b_n < 0$.

Proof. Let X be the associated almost simple group with socle $\mathrm{soc}(X) = S$ as described in Section 2.2. By Corollary 2.2.9 and by using notations from Theorem 3.1.9, we have that

$$\begin{aligned} P^{(p)}_{L,N}(s) = P^{(p)}_{X,S}(rs - r + 1) &= (-1)^{o(I)} \sum_{J \subseteq I} (-1)^{o(J)} (|S : P_J|^r)^{1-s} \\ &= (-1)^{o(I)} \sum_{J \in \mathcal{P}^X(I)} (-1)^{o(J)} \left(\left(\frac{T_{W_I}(t)}{T_{W_J}(t)} \right)^r \right)^{1-s}. \end{aligned}$$

Notice that $T_{W_I}(t)/T_{W_J}(t)$ is always divisible by the cyclotomic polynomial $\Phi_{\zeta_p(S)/e_S}(t)$ and not divisible by $\Phi_f(t)$ for any $f > \zeta_p/e_S$. Hence (a) and (b) follow. Notice also that the smallest positive integer n such that $b_n \neq 0$ corresponds to the parabolic subgroups P_J of S with $o(I) - o(J) = 1$. This implies immediately that $b_n < 0$ which proves (c). □

3.2 The main result

In this section, we give a proof for **Theorem A**. In this proof, we consider a finitely generated profinite group G such that $P_G(s)$ is rational and we assume that there is a prime p and an open normal subgroup H of which every composition factor is either cyclic or isomorphic to a simple group of Lie type over a field of characteristic p.

We fix a descending normal series $\{G_i\}$ of G with the properties that $\bigcap G_i = 1$ and G_i/G_{i+1} is a chief factor of G/G_{i+1}. Let J be the set of indices i with G_i/G_{i+1} non-Frattini. Then by Section 2.1, the probabilistic zeta function $P_G(s)$ can be factorized as

$$P_G(s) = \prod_{i \in J} P_i(s)$$

where for each i, the finite Dirichlet series $P_i(s) = \sum_n b_{i,n}/n^s$ is associated to the chief factor G_i/G_{i+1}. Let Γ be the set of simple groups that appear as composition factors in non-Frattini chief factors of G. That is, the set of simple groups S_i for $i \in J$. We have the the following crucial result.

Proposition 3.2.1. *The set Γ is finite.*

Proof. Since $P_G(s)$ is rational, the set $\pi(P_G(s))$ is finite. It follows from Lemma 2.6.1 that Γ contains only finitely many abelian groups. Assume by contradiction that Γ is infinite. By our assumption, the subset Γ^* of the simple groups in Γ that are of Lie type over a field of characteristic p is infinite. In particular, the set $\Omega = \{\zeta_p(S) \mid S \in \Gamma^*\}$ is infinite. Let I be the set of indices $i \in J$ such that the composition factors of G_i/G_{i+1} belong to Γ^*. Let $A(s) = \prod_{i \in I} P_i(s)$ and $B(s) = \prod_{i \notin I} P_i(s)$. Notice that $\pi(B(s)) \subseteq \bigcup_{S \in \Gamma \setminus \Gamma^*} \pi(S)$ is a finite set. Since $P_G(s) = A(s)B(s)$ and $\pi(P_G(s))$ is finite, we deduce that $\pi(A(s))$ is finite. In particular, there exists a positive integer $m \in \Omega$ such that $m \geq 7$ and $\langle p, m\rangle \cap \pi(A(s)) = \emptyset$. Note that we choose $m \geq 7$ to ensure that the set $\langle p, m\rangle$ is non empty (see Proposition 3.1.10). Let Γ_m be the set of positive integers n such that no prime in $\langle p, u\rangle$ divides n if $u > m$ and set

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

By Proposition 3.1.11, if $i \in I$ such that $b_{i,\beta} \neq 0$ then $\zeta_p(S_i) = m, r_i = r$ and $b_{i,\beta} < 0$. Hence the coefficient c_β of $1/\beta^s$ in $A(s)$ is

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

On the other hand, again by Proposition 3.1.11 , all primes in $\langle p, m\rangle$ divide m. But then $\langle p, m\rangle \subseteq \pi(A(s))$, which is a contradiction. Therefore Γ is finite. By Corollary 2.6.2, it follows that $\pi(G)$ is also finite. $\square$

Proof of Theorem A. Let $\mathcal{T}$ be the set of almost simple groups X such that there exist infinitely many $i \in J$ with $X_i \cong X$ and let I be the set of the indices i in J such that $X_i \in \mathcal{T}$. Our assumptions combined with Proposition 2.6.3, 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 $n \in \mathbb{N}$, the set $I_n = \{i \in I : \zeta_p(S_i) = n\}$ is empty.*

Proof of the claim. Assume that the claim is false and let m be the smallest integer such that $I_m \neq \emptyset$. Since $J \setminus I$ is finite and $P_G(s)$ is rational, the product $\prod_{i\in I} P_i(s)$ is also 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.

In case (1) or (3), it follows by Theorem 3.1.10 that $\langle p, t\rangle \neq \emptyset$ for every $t > m+1$; we set $\sigma = \bigcup_{t>m+1}\langle p, t\rangle \cup \{p\}$. In case (2), we have $\langle 2, t\rangle \neq \emptyset$ whenever $t > 6$ and we set $\sigma = \bigcup_{t>6}\langle 2, t\rangle \cup \{2\}$. Consider $H(s) = Q^{(\sigma)}(s)$, obtained by applying consecutively the homomorphism $P(s) \mapsto P^{(q)}(s)$ for all the primes $q \in \sigma$. The Dirichlet series $H(s)$ is rational. By Proposition 3.1.11, if $i \in I_t$ and $\tau \in \langle p, t\rangle$, then $P_i^{(\tau,p)}(s) = 1$; in particular $P_i^{(\sigma)}(s) = 1$ whenever $\langle p, t\rangle \subseteq \pi$. This implies

$$H(s) = \begin{cases} \prod_{i\in I_m} P_i^{(p)}(s) & \text{in cases (1) and (3) ,} \\ \prod_{i\in I_u, m\leq u\leq 5} P_i^{(2)}(s) & \text{otherwise.} \end{cases}$$

- Assume that (3) occurs and let $\tau \in \langle p, m\rangle$ exist. By Corollary 2.2.9 and Proposition 3.1.11, if $i \in I_m$, and there exists y such that $(p, y) = 1$ and $b_{i,y} \neq 0$ then $y = x^{r_i}$ and $v_\tau(x) = v_\tau(p^m - 1)$. Let

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

By Proposition 3.1.11, 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 2.4.3, we obtain a rational product

$$H^*(s) = \prod_{i\in\Sigma_m} \left(1 + \frac{b_{i,w^{r_i}}}{w^{r_i s}}\right), \text{ where } b_{i,w^{r_i s}} < 0 \text{ for all } i \in \Sigma_m. \tag{3.3}$$

By Corollary 2.5.5, the product $H^*(s)$ is a finite product, i.e., Σ_m is finite, which is a contradiction.

• Assume that (1) occurs. By Table 3.2, if $\zeta_p(S) = 1$, then $S \cong \mathrm{PSL}(2, p)$. This implies in particular that

$$H(s) = \prod_{i \in I_1} \left(1 - \frac{2^{tr_i}}{2^{tr_i s}}\right).$$

Again by Corollary 2.5.5, we get that I_1 is finite, which is a contradiction.

• Finally assume that the case (2) occurs. By Table 3.2, if $\zeta_p(S) \le 5$, then S is one of the following groups: $\mathrm{PSL}(6,2)$, $U(4,2)$, $\mathrm{PSp}(6,2)$, $P\Omega^+(8,2)$, $\mathrm{PSL}(3,4)$, $\mathrm{PSL}(5,2)$, $\mathrm{PSL}(4,2)$, $\mathrm{PSL}(3,2)$. The explicit description of the Dirichlet series $P^{(2)}_{X,S}(s)$ when $S \le X \le \mathrm{Aut}(S)$ and S is one of the simple groups in the previous list, is included in Appendix 1. Notice in particular that if $i \in \Lambda = \bigcup_{m \le 5} I_m$ 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 1). So if $b_{i,w^{r_i}} \neq 0$ then $b_{i,w^{r_i}} < 0$; moreover, by applying Proposition 2.4.3 we obtain a rational product

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

By Corollary 2.5.5, 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 $\Lambda_{31} \neq 0$, 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 Λ_{31}^*. Since $\Lambda_{31} = \emptyset$, if $i \in \Lambda$, then S_i is isomorphic to one of the following: $U(4,2), \mathrm{PSp}(6,2), P\Omega^+(8,2), \mathrm{PSL}(3,4), \mathrm{PSL}(4,2), \mathrm{PSL}(3,2)$. It follows from Appendix 1, that if $i \in \Lambda$, x is odd and $b_{i,x^{r_i}} \neq 0$, then $v_7(x) \le 1$. 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 Appendix 1 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 Corollary 2.5.5, Λ is finite and consequently $\Lambda = \emptyset$.

$\square$

Appendix 1: exceptional cases

In this section, we give explicit formulas 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 $\zeta_2(S) \leq 5$ (see Example 1 and Example 2 in Section 3 for the illustration of computation).

(i) $S = \mathrm{PSL}(6,2)$. If X contains a graph automorphism then

$$\begin{aligned} P^{(2)}_{X,S}(s) &= 1 - (3^2.7.31)^{(1-s)} - (3.5.7^2.31)^{(1-s)} - (3^3.7.31)^{(1-s)} \\ &+ 2(3^4.7^2.31)^{(1-s)} + (3^3.5.7^2.31)^{(1-s)} - (3^4.5.7^2.31)^{(1-s)}. \end{aligned}$$

If X does not contain graph automorphisms, then

$$\begin{aligned} P^{(2)}_{X,S}(s) &= 1 - 2(3^2.7)^{(1-s)} - (3^2.5.31)^{(1-s)} - 2(3.7.31)^{(1-s)} \\ &+ 3(3^2.7.31)^{(1-s)} + 6(3^2.5.7.31)^{(1-s)} + (3.5.7^2.31)^{(1-s)} \\ &- 4(3^3.5.7.31)^{(1-s)} - 6(3^2.5.7^2.31)^{(1-s)} \\ &+ 5(3^3.5.7^2.31)^{(1-s)} - (3^4.5.7^2.31)^{(1-s)}. \end{aligned}$$

(ii) $S = \mathrm{PSL}(5,2)$. If X contains a graph automorphism then

$$P^{(2)}_{X,S}(s) = 1 - (3.5.31)^{(1-s)} - (3^2.7.31)^{(1-s)} + (3^2.5.7.31)^{(1-s)}.$$

If X does not contain graph automorphisms, then

$$\begin{aligned} P^{(2)}_{X,S}(s) &= 1 - 2(31)^{(1-s)} - 2(5.31)^{(1-s)} + 3(3.5.31)^{(1-s)} \\ &+ 3(5.7.31)^{(1-s)} - 4(3.5.7.31)^{(1-s)} + (3^2.5.7.31)^{(1-s)}. \end{aligned}$$

(iii) $S = \mathrm{PSL}(4,2)$. If X contains a graph automorphism then

$$P^{(2)}_{X,S}(s) = 1 - (3^2.7)^{(1-s)} - (3.5.7)^{(1-s)} + (3^2.5.7)^{(1-s)}.$$

If X does not contain graph automorphisms, then

$$P^{(2)}_{X,S}(s) = 1 - 2(3.5)^{(1-s)} - (5.7)^{(1-s)} + 3(3.5.7)^{(1-s)} - (3^2.5.7)^{(1-s)}.$$

(iv) $S = \mathrm{PSL}(3,2)$. If X contains a graph automorphism then

$$P^{(2)}_{X,S}(s) \quad = \quad 1 - (3.7)^{(1-s)}.$$

If X does not contain graph automorphisms, then

$$P^{(2)}_{X,S}(s) \quad = \quad 1 - 2(7)^{(1-s)} + (3.7)^{(1-s)}.$$

(v) $S = \mathrm{PSL}(3,4)$. If X contains a graph automorphism then

$$P^{(2)}_{X,S}(s) = 1 - (3.5.7)^{(1-s)}.$$

If X does not contain graph automorphisms then

$$P^{(2)}_{X,S}(s) = 1 - 2(3.7)^{(1-s)} + (3.5.7)^{(1-s)}.$$

(vi) $S = \mathrm{PSp}(6,2)$. We have

$$P^{(2)}_{X,S}(s) = 1 - (3^2.7)^{(1-s)} - (3^3.5)^{(1-s)} - (3^2.5.7)^{(1-s)} + 3(3^3.5.7)^{(1-s)} - (3^4.5.7)^{(1-s)}.$$

(vii) $S = \mathrm{U}(4,2)$. We have

$$P^{(2)}_{X,S}(s) = 1 - (3^3)^{(1-s)} - (3^2.5)^{(1-s)} + (3^3.5)^{(1-s)}.$$

(viii) $S = \mathrm{P\Omega}^+(8,2)$. We have

$$\begin{aligned} P^{(2)}_{X,S}(s) \quad &= \quad 1 - 3(3^2.5)^{(1-s)} - (3.5^2.7)^{(1-s)} + 3(3^3.5^2)^{(1-s)} + 3(3^3.5^2.7)^{(1-s)} \\ &- \quad 4(3^4.5^2.7)^{(1-s)} + (3^5.5^2.7)^{(1-s)}. \end{aligned}$$

Lie notation	Other notation	Conditions
$A_n(t)$	$\mathrm{PSL}(n+1,q)$	$n \geq 1, (n,t) \neq (1,2),(1,3)$
${}^2A_n(t^2)$	$\mathrm{PSU}(n+1,q)$	$n \geq 2, (n,t) \neq (2,2)$
$B_n(t)$	$\mathrm{P}\Omega(2n+1,q)$	$n \geq 3, t$ odd
${}^2B_2(t^2)$		$q = t^2 = 2^{2k+1}, k \geq 1$
$C_n(t)$	$\mathrm{PSp}(2n,q)$	$n \geq 2, (n,t) \neq (2,2)$
$D_n(t)$	$\mathrm{P}\Omega^+(2n,q)$	$n \geq 4$
${}^2D_n(t^2)$	$\mathrm{P}\Omega^-(2n,q)$	$n \geq 4$
${}^3D_4(t^3)$		
$E_6(t)$		
${}^2E_6(t^2)$		
$E_7(t)$		
$E_8(t)$		
$F_4(t)$		$t \geq 3$
${}^2F_4(t^2)$		$q = t^2 = 2^{2k+1}, k \geq 1$
$G_2(t)$		$t \geq 3$
${}^2G_2(t^2)$		$q = t^2 = 3^{2k+1}, k \geq 1$

Table 3.3: Classification of simple groups of Lie type

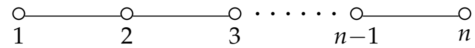
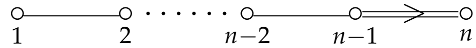
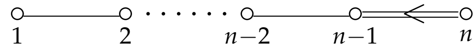
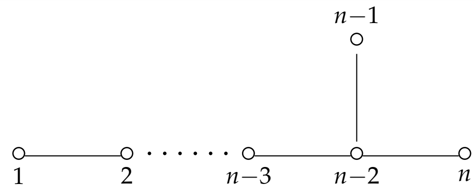
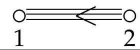
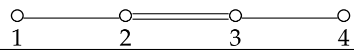
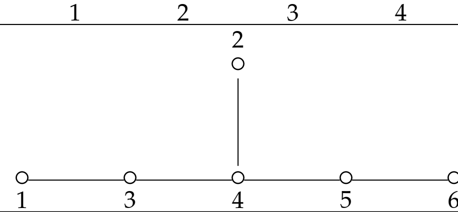
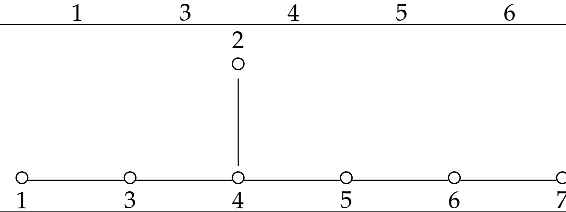
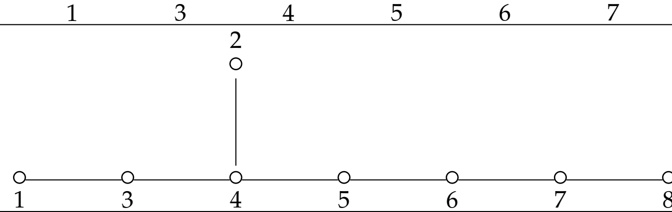
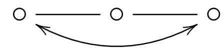
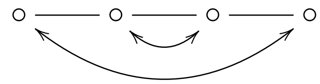
Lie notation	Dynkin diagram
$A_n, n \geq 1$	
$B_n, n \geq 2$	
$C_n, n \geq 3$	
$D_n, n \geq 4$	
G_2	
F_4	
E_6	
E_7	
E_8	

Table 3.4: The classification of simple Lie algebras

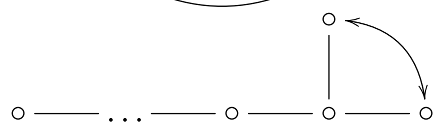
A_{Odd}



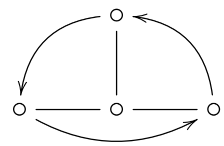
A_{Even}



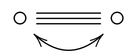
D_n



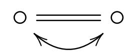
D_4



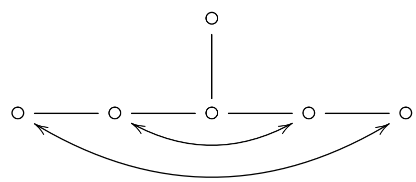
G_2



B_2



E_6



F_4

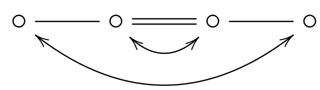


Table 3.5: Symmetries of Dynkin diagrams