On the (non-)contractibility of the order complex of the coset poset of a classical group

Massimiliano Patassini

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

A R T I C L E   I N F O

Article history:
Received 28 April 2009
Available online 20 July 2011
Communicated by Martin Liebeck

MSC:
20D30
20P05
11M41
20D60
20E28
20G40

Keywords:
Probabilistic zeta function
Simplicial complex
Order complex
Contractibility
Coset poset
Classical group
Brown conjecture

A B S T R A C T

Let $G$ be a classical group and suppose that $G$ does not contain non-trivial graph automorphisms. In this paper we prove that the order complex of the coset poset of $G$ is non-contractible. In order to prove it, we show that $P_C(-1)$ does not vanish, where $P_C(s)$ is the Dirichlet polynomial associated to the group $G$.

© 2011 Elsevier Inc. All rights reserved.

1. Introduction

Let $G$ be a finite group. The coset poset $C(G)$ is the poset of the proper cosets of $G$. We can apply topological concepts to the poset $C(G)$ considering the simplicial complex $\Delta(C(G))$ associated to $C(G)$ (the order complex of $C(G)$). We recall that $\Delta(C(G))$ is the simplicial complex whose simplices are finite chains in $C(G)$ (see [16, §1] and [19, §3]). In particular, we can speak of the Euler characteristic $\chi(C(G)) := \chi(\Delta(C(G)))$ and the reduced Euler characteristic $\tilde{\chi}(C(G)) := \chi(C(G)) - 1$. In [2], Brown pointed out a connection between the simplicial complex $\Delta(C(G))$ and the counterpart of the...
probabilistic zeta function of $G$ (see [1] and [14]), the so-called Dirichlet polynomial associated to $G$, defined by

$$P_G(s) = \sum_{k=1}^{\infty} a_k(G) \frac{k^s}{k^s}, \quad \text{where } a_k(G) = \sum_{H \leq G, |G:H|=k} \mu_G(H).$$

Here $\mu_G$ is the Möbius function of the subgroup lattice of $G$, which is defined inductively by $\mu_G(G) = 1$, $\mu_G(H) = -\sum_{K \supset H} \mu_G(K)$. Thanks to an observation of S. Bouc, Brown [2, §3] showed that

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

It is a well-known fact that if $\Delta(C(G))$ is contractible, then its reduced Euler characteristic $\tilde{\chi}(C(G))$ is zero. Hence, if $P_G(-1) \neq 0$, then the simplicial complex associated to the group $G$ is non-contractible. In [2], Brown proved the following.

**Proposition 1.** (See [2].) If $G$ is a finite soluble group, then $P_G(-1) \neq 0$.

A proof of this proposition proceeds as follows. If $N$ is a normal subgroup of $G$, then we define

$$P_{G,N}(s) = \sum_{k \in \mathbb{N}} a_k(G,N) \frac{k^s}{k^s}, \quad \text{where } a_k(G,N) = \sum_{H \leq G, |G:H|=k, NH=G} \mu_G(H).$$

We have that $P_G(s) = P_{G/N}(s)P_{G,N}(s)$ (see [2]). Thus, if $1 = N_0 < N_1 < \cdots < N_k = G$ is a chief series of $G$, applying the above formula repeatedly, we obtain

$$P_G(s) = \prod_{i=0}^{k-1} P_{G/N_i,N_{i+1}/N_i}(s).$$

By a result of [6], we have that $P_{G/N_i,N_{i+1}/N_i}(s) = 1 - \frac{c_i}{|N_i|}$ where $c_i$ is the number of complements of $N_{i+1}/N_i$ in $G/N_i$. Thus, it is clear that $P_G(-1) \neq 0$.

Moreover, Brown conjectured that $P_G(-1) \neq 0$ for every finite group $G$. In the previous paper [17], we proved this conjecture for $G$ equal to $\text{PSL}_2(q)$, to the Suzuki groups $2^B_2(q)$ and to the Ree groups $2^G_2(q)$. At the time of this writing, there is no known finite group $G$ such that $P_G(-1) = 0$.

In this paper, we want to prove the Brown conjecture for the classical groups. We use the definition classical groups, as given in [13] (see also Section 6).

The main result of this paper is the following.

**Theorem 2.** Let $X$ be a classical group that does not contain non-trivial graph automorphisms. The number $P_X(-1)$ does not vanish, so the simplicial complex associated to the coset poset of $X$ is not contractible.

We outline the strategy of the proof. Here we use the notation of Section 6. Suppose that $\Omega \leq X \leq A$. Denote by $\bar{\Omega}$ the reduction modulo scalars. In particular it turns out that $\bar{X} = X/\bar{X}$. Let $1 = Z_0 < Z_1 < \cdots < Z_k = Z(X)$ be a part of the chief series of $X$. As we have seen above, we have

$$P_X(s) = P_{X/Z(X)}(s) \prod_{i=0}^{k-1} P_{G/Z_i,Z_{i+1}/Z_i}(s).$$
Since \( Z_{i+1}/Z_i \) is a minimal normal subgroup of \( G/Z_i \) that is abelian, as above we have that \( P_{G/Z_i,Z_{i+1}/Z_i}(s) = 1 - \frac{c_i}{|Z_i|} \), where \( c_i \) is the number of complements of \( Z_{i+1}/Z_i \) in \( G/Z_i \). So \( P_X(s) \) does not vanish if and only if \( P_X(s) \) does not vanish. Thus we can reduce to the case \( \Omega \leq X \leq \Lambda \).

Assume that \( \Omega \leq X \leq \Lambda \). If \( \Omega \) is soluble, then Proposition 1 implies Theorem 2. Assume that \( \Omega \) is non-abelian simple and let \( G = \Omega \). Clearly, we have \( G \leq X \). Thus we obtain:

\[
P_X(s) = P_{X,G}(s)P_{X/G}(s).
\]

By Schreier conjecture, the group \( X/G \) is soluble. So, by Proposition 1, we have that \( P_{X/G}(-1) \neq 0 \). It remains to show that \( P_{X,G}(-1) \neq 0 \).

Let \( r \) be a prime number and let \( P_{X,G}(s) \) denote the Dirichlet polynomial

\[
\sum_{(k,r)=1} \frac{a_k(X,G)}{k^s}.
\]

Fix a prime number \( p \) and assume that \( G \) is defined over a field of characteristic \( p \). In particular, we have

\[
P_{X,G}(s) = P_{X,G}(s) + \sum_{p|k} \frac{a_k(X,G)}{k^s}.
\]

The first summand \( P_{X,G}(s) \) collects the contribution given by the subgroups \( H \) of \( X \) such that \( H \) contains a Sylow \( p \)-subgroup and \( HG = X \). In order to obtain a good expression for \( P_{X,G}(s) \) we first reduce to the case \( X = G \). Note that \( P_{G,G}(s) = P_G(s) \) and define \( P^{(p)}_G(s) = P^{(p)}_{G,G}(s) \). Sections 2–5 are devoted to the study of value \( P^{(p)}_G(-1) \) when \( G \) is a group of Lie type of characteristic \( p \). The notation introduced in Section 2 applies only to Sections 3–5. Using some classical results of [3] on root systems, we obtain the following theorem.

**Theorem 3.** Let \( G \) be a simple group of Lie type of characteristic \( p \) over \( \mathbb{K} \). Let \( t = |\psi|/|\mathbb{K}| \), where \( \psi \) is the symmetry of the Dynkin diagram associated to \( G \). We have that

\[
|P^{(p)}_G(-1)|_p = t^L|2|_p
\]

where the values of \( L \) are in Table 1 (Section 5).

In Section 6 we introduce the notation for classical groups we will use throughout the rest of the paper. Thus Theorem 3 can be restated for the classical groups as follows.

**Theorem 4.** We have that

\[
|P^{(p)}_G(-1)|_p = q^L|2|_p,
\]

where

\[
L = \begin{cases} 
  n - 1 & \text{in case } \mathbf{L} \text{ or } \mathbf{U} \text{ with } n \text{ even}, \\
  n & \text{in case } \mathbf{U} \text{ with } n \text{ odd}, \\
  \frac{n}{2} & \text{in cases } \mathbf{S} \text{ and } \mathbf{O}^\pm, \\
  \frac{n-1}{2} & \text{in case } \mathbf{O}^o.
\end{cases}
\]
In Sections 7 and 8 we show that, in most cases,

\[ P_{X,G}(-1) - P_{X,G}^{(p)}(-1) \text{ is divisible by } q^L p^{(2,p)}. \]

(†)

In order to prove (†), we investigate the structure of the maximal subgroups \( M \) of \( X \) such that \( MG = X \). In particular, in Section 7 we deal with maximal subgroups \( M \) of \( X \) such that \( M \) does not contain a Sylow \( p \)-subgroup of \( X \). In Section 8, the setting is the following: let \( H \) be a subgroup of \( X \) such that \( HG = X \) and suppose that if \( M \) is a maximal subgroup of \( X \) containing \( H \), then \( M \) contains a Sylow \( p \)-subgroup of \( X \). In this case we prove that \( \mu_G(H) = 0 \) or \( |G : H|_p \) is greater than or equal to \( q^{\beta(n)} \), where

\[
\beta(n) = \begin{cases} 
  n - 1 & \text{if case } L \text{ or } U \text{ holds}, \\
  \frac{n}{2} - \log_q |2|_p & \text{if case } S \text{ holds}, \\
  \frac{n-1}{2} & \text{if case } O^0 \text{ holds}, \\
  \frac{n-2}{2} & \text{if case } O^+ \text{ or } O^- \text{ holds}.
\end{cases}
\]

Section 9 is dedicated to showing that \( P_{X,G}(s) \) is equal to \( P_{\mathcal{G}(s)}^{(p)} \).

Finally, in Section 10 we prove Theorem 2. In most cases, we have that

\[ |P_{X,G}(-1)|_p < |P_{X,G}(-1) - P_{X,G}^{(p)}(-1)|_p, \]

and this implies that \( P_{X,G}(-1) \neq 0 \).

We will use repeatedly, often without mention, the following results on the Möbius function of the subgroup lattice of \( G \).

**Lemma 5.** (See [8].) Let \( G \) be a finite group and \( H \) a subgroup of \( G \). If \( \mu_G(H) \neq 0 \), then \( H \) is intersection of maximal subgroups of \( G \).

**Lemma 6.** (See [10, Theorem 4.5].) Let \( A \) be a finite group and \( B \) a subgroup of \( A \). The index \( |N_A(B) : B| \) divides \( \mu_A(B)/A : BA' \).

Since \( X' \geq G \), then Lemma 6 yields \( |G : H| \) divides \( \mu_G(H)/G : N_G(H) \). So, in particular, \( k \) divides \( a_k(X,G) \).

2. Notation and definitions about groups of Lie type

In the sequel we introduce some notations and definitions we will use throughout Sections 3, 4 and 5.

We point out some general facts about the groups of Lie type and the simple Lie algebras. Everything we need can be found in [3].

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

If \( G \) is an untwisted group of Lie type, then \( G \) is a Chevalley group \( \mathcal{L}(\mathbb{K}) \), which is a certain group of automorphisms of \( \mathfrak{L} \) over the field \( \mathbb{K} \) (see [3, Proposition 4.4.3]).

If \( G \) is a twisted group of Lie type, then \( G \) is a subgroup of a Chevalley group \( \mathcal{L}(\mathbb{K}) \).

Now, let \( G \) be our group of Lie type. To \( G \) the following objects are associated.

- A Killing form \((-,-)\) on the simple Lie algebra \( \mathfrak{L} \) over the field \( \mathbb{K} \).
- A system of roots \( \Phi \) in a Cartan subalgebra \( \mathfrak{U} \) of \( \mathfrak{L} \) and a system of fundamental roots \( \Pi \) in \( \Phi \).
• A Dynkin diagram $\mathcal{D}$, that is a graph with elements of $I$ as nodes, such that $r \in I$ and $s \in I$ are joined by a bond of strength $\frac{4(r, s)^2}{(r, r)(s, s)}$ (see [3, 3.4]).

• A symmetry $\rho$ of the Dynkin diagram of $\mathcal{D}$ (see [3, 13.1]). In particular the order of $\rho$ is 1, 2 or 3 (see [3, 13.4]).

We denote by $t$ the positive number $|\sqrt{2}|$. This definition is the most convenient, although it allows $t$ to be irrational (see [3, 14.1]).

Now, we give some other definitions and remarks on the root systems.

• Given a system of roots $\Psi$ and a fundamental system $\Sigma$ in $\Psi$, let $\Psi^+$, $\Psi^-$ be the sets of positive and negative roots with respect to the fundamental system $\Sigma$. We recall that a root in $r \in \Psi$ is a linear combination of roots of $\Sigma$ with integer coefficients which are all non-negative if $r \in \Psi^+$ and all non-positive if $r \in \Psi^-$ (see [3, 2.1]).

• The vector space $\mathcal{V}$ is spanned by $I$ in $\mathcal{L}$. Let $r \in \mathcal{V}$; a linear map $w_r : \mathcal{V} \to \mathcal{V}$, defined by

$$w_r(x) = x - \frac{2(r, x)}{(r, r)}r,$$

is called a reflection. The Weyl group $W$ of $\Phi$ is the subgroup of transformations of $\mathcal{V}$ generated by the reflections $\{w_r : r \in I\}$. Note that $W$ is generated also by the so-called fundamental reflections $\{w_r : r \in I\}$ (see [3, 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 $r_i \in \Pi$, $i \in \{1, \ldots, n\}$. Thus $l(1) = 0$. Moreover, $l(w) = |\Phi^+ \cap w^{-1}(\Phi^-)|$ (see [3, Theorem 2.2.2]).

• For a subset $K$ of $I$, let $\mathcal{V}_K$ be the subspace of $\mathcal{V}$ spanned by $K$. Let $\Phi_K = \Phi \cap \mathcal{V}_K$ and let $W_K$ be the subgroup of $W$ generated by the reflections $\{w_r : r \in \Phi_K\}$. Note that $\Phi_K$ is a system of roots in $\mathcal{V}_K$, $K$ is a fundamental system and the Weyl group of $\Phi_K$ is $W_K$ [3, Proposition 2.5.1].

• An isometry $\tau$ of $\mathcal{V}$ is associated to the symmetry $\rho$ in such a way that $\tau(r)$ is a positive multiple of $\rho(r)$ for each $r \in I$ (see [3, 13.1]). The isometry $\tau$ is uniquely determined by $\rho$. In particular, observe that for every $w \in W$, the element $w^\tau = \tau^{-1}w\tau$ belongs to $W$. Finally, note that $\rho$ and $\tau$ are non-trivial if and only if $G$ is twisted.

• Let $k$ be the number of the $\rho$-orbits of $I$. Let $I = \{O_1, \ldots, O_k\}$ denote the set of $\rho$-orbits of $I$. For each $J \subseteq I$, let $J^\rho = \bigcup_{K \in J} K$.

• Let $W$ denote the subgroup of the Weyl group $W$ consisting of the $w \in W$ such that $w^\tau = w$ (see [3, 13.1]). For a subset $J$ of $I$, let $W_J = W_J \cap W$. In particular, if $J = \{O_i\}$ for some $i \in \{1, \ldots, k\}$, then let $W_i = W_{O_i} = W_{O_i^+} \cap W_i = W_{O_i} = W_{O_i}$ and $\Phi_i = \Phi_{O_i} = \Phi_{O_i^+}$.

• Let $\mathcal{D}'$ be the Dynkin diagram of $W$, that is a graph induced by the Dynkin diagram $\mathcal{D}$, identifying the nodes in the same $\rho$-orbit (see [3, 13.3.8]). $\mathcal{D}'$ is a graph with as nodes the elements of $I$, such that $K_1 \in I$ and $K_2 \in I$ are joined if there exist $r_1 \in K_1$ and $r_2 \in K_2$ such that $r_1$ and $r_2$ are joined in $\mathcal{D}$.

• Let $K$ be a subset of $I$. 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 $D_J = D_{J^\rho} \cap W$.

• Denote by $L$ the number

$$\sum_{i=1}^k |\Phi_i^+|.$$

• For $J \subseteq I$, let

$$T_{W_J}(t) = \sum_{w \in W_J} t^{l(w)}.$$
Note that here the notation is not the same as in [3], where this expression is denoted by $P_{\mathcal{W}_j}(t)$. We preferred our notation to avoid confusion with $P_{\mathcal{C}}(s)$, the Dirichlet polynomial of $G$.

3. Some technical result on root systems

The following lemma is quite technical. We point out some important facts on root systems.

**Lemma 7.** Using the notation of Section 2, the following hold.

1. The set $\{w(\Phi^+_i) : w \in \mathcal{W} \}$ is a partition of $\Phi$.
2. There exists a unique element $\omega \in W$ such that $\omega(\Phi^+) = \Phi^-$. This element is an involution and $\lambda(\omega) = |\Phi^+|$. In particular, $\omega \in \mathcal{W}$.
3. Let $K \subseteq \Pi$ and let $w \in W_K$. The length $l(w)$ is the same whether $w$ is regarded as an element of the Weyl group $W$ or of the Weyl group $W_K$.
4. Let $i \in \{1, \ldots, k\}$. There exists a unique element $\omega_i \in W_i$ such that $\omega_i(\Phi^+_i) = \Phi^-_i$. Moreover, $\omega_i$ generates $\mathcal{W}_i$ in $W$ and $\{\omega_i : i \in \{1, \ldots, k\}\}$ generates $\mathcal{W}$ in $W$.
5. Let $i \in \{1, \ldots, k\}$ and let $w \in \mathcal{W}$ such that $w(r) \in \Phi^-$ for some $r \in O_i$. We have that $l(w\omega_i) = l(w) - l(\omega_i)$.
6. Let $w \in \mathcal{W}$ and let $r, s \in O_i$ for some $i \in \{1, \ldots, k\}$. The roots $w(r)$ and $w(s)$ have the same sign, i.e. either $w(r), w(s) \in \Phi^+$ or $w(r), w(s) \in \Phi^-$. Moreover, $l(w) = l(d_J) + l(w_J)$.
7. Let $w \in \mathcal{W}$ and let $J$ be a subset of $I$. We have that $w = d_J w_J$ for uniquely determined $d_J \in D_J$ and $w_J \in \mathcal{W}_J$. Moreover, $l(w) = l(d_J) + l(w_J)$.
8. Let $i, j \in \{1, \ldots, k\}$. Let $w$ be an element of $\mathcal{W}$ such that $w(O_i) \subseteq \Phi^-_j$. We have that $\omega_i^w = w\omega_i w^{-1} = \omega_j$.

**Proof.**

1. See Lemma 13.2.1 in [3].
2. See Proposition 2.2.6 in [3]. It remains to show that $\omega \in \mathcal{W}$. Since $\tau$ preserves the sign of each root, we have that $\tau \omega \tau^{-1}(\Phi^+) = \Phi^-$. Hence $\tau \omega \tau^{-1} = \omega$, as required.
3. This is Lemma 9.4.1 in [3].
4. This is Proposition 13.1.2 in [3].
5. This is inside the proof of Proposition 13.1.2 in [3].
6. This is clear since $\tau$ preserves the sign of each root.
7. By Theorem 2.5.8 in [3], we know that $w = d_J w_J$ for uniquely determined $d_J \in D_J$ and $w_J \in \mathcal{W}_J$, and that $l(w) = l(d_J) + l(w_J)$. So, it remains to prove that $w$ can be expressed in the form $w = d_J w_J$ for $d_J \in D_J$ and $w_J \in \mathcal{W}_J$. Suppose $l(w) = 0$, we have that $w = 1$ and $w = 1.1$ is the required factorization. Now, assume $l(w) > 0$ and proceed by induction on $l(w)$. If $w \in D_J$, then $w = w.1$ is the required factorization. If $w \notin D_J$, then there exist $i \in \{1, \ldots, k\}$ and $r \in O_i$ such that $O_i \in J$ and $w(r) \in \Phi^-$. So, by part (5), $l(ww_i) = l(w) - l(w_i) < l(w)$. Hence, by induction, $ww_i = d_J w_J$ for some $d_J \in D_J$ and $w_J \in \mathcal{W}_J$. Clearly $w_J = w_J w_i$ is in $\mathcal{W}_J$, so $w = d_J w_J$ as required.
8. Since $W$ is generated by the fundamental reflections, we have $\omega_i = w_{r_1} \cdots w_{r_n}$ for some $r_i \in O_i$, $l \in \{1, \ldots, n\}$. So, using the definition of reflection, we have

$$\omega_i^w = w_{r_1}^w \cdots w_{r_n}^w = w_{w(r_1)} w_{w(r_2)} \cdots w_{w(r_n)}.$$  

Since $w(r_i) \in \Phi^-_j$ for $l \in \{1, \ldots, n\}$, we have that $\omega_i^w$ is an element of $W_{O_j}$. But $w^w \in \mathcal{W}$, hence $\omega_i^w \in \mathcal{W}_j$. Now, since $w(O_i) \subseteq \Phi^-_j$, then also $w(\Phi^+_i) \subseteq \Phi^-_j$. By definition, we have $\omega_j(\Phi^+_j) = \Phi^-_j$, so, by part (1) of the lemma, we get $w(\Phi^+_i) = \Phi^-_j$. Thus $\omega_i^w(\Phi^+_j) = w\omega_i^w(\Phi^-_j) = w\omega_i^w(\Phi^-_j) = w(\Phi^+_i) = \Phi^-_j$. Since $\omega_i^w(\Phi^+_j) = \Phi^-_j$ and $\omega_i^w \in \mathcal{W}_j$, part (4) yields $\omega_i^w = \omega_j$. \qed
Lemma 8. We have the following.

1. Let \( w \in \mathcal{W} \). Let \( n \in \mathbb{N} \), \( i_j \in \{1, \ldots, k\} \) for \( j \in \{1, \ldots, n\} \) and suppose that \( w = \omega_1 \cdots \omega_n \) is an \( \omega \)-factorization of minimal length of \( w \). We have that

\[
l(w) = \sum_{j=1}^{n} l(\omega_{i_j}) = \sum_{j=1}^{n} |\Phi_{i_j}|.
\]

2. Let \( i \in \{1, \ldots, k\} \) and let \( w \in \mathcal{W} \) such that \( w(r) \in \Phi^- \) for some \( r \in O_i \). We have that \( \omega_i \) appears in each \( \omega \)-factorization of \( w \) of minimal length.

Proof.

(1) The argument is similar to the proof of Theorem 2.2.2 in [3]. It is clear that for any \( u, v \in \mathcal{W} \),

\[
l(u) \leq l(uv) + l(v).
\]

Hence we have

\[
l(w) \leq l(w\omega_n) + l(\omega_n) \leq l(w\omega_1 \omega_{n-1}) + l(\omega_{n-1}) \leq \cdots \leq \sum_{j=1}^{n} l(\omega_{i_j}) = L'.
\] (†)

Thus \( l(w) \leq L' \). Now, by contradiction, assume that \( l(w) < L' \). So, we have that at least one of the inequalities in (†) is strict, i.e. there exists \( m \in \{1, \ldots, n\} \) such that

\[
l(\omega_1 \cdots \omega_m) = l(w\omega_1 \cdots \omega_{m-1}) < l(w\omega_1 \cdots \omega_m) + l(\omega_m) = l(\omega_1 \cdots \omega_{m-1}) + l(\omega_m).
\]

This implies that \( \omega_1 \cdots \omega_m (O_{im}) \subseteq \Phi^+ \). In fact, if \( \omega_1 \cdots \omega_m (r) \in \Phi^- \) for some \( r \in O_{im} \), then

\[
l(\omega_1 \cdots \omega_m) = l(\omega_1 \cdots \omega_{m-1}) + l(\omega_m),
\]

by part (5) of the previous lemma.

Now, \( \omega_m (O_{im}) \subseteq \Phi^- \) and \( \omega_1 \cdots \omega_m (O_{im}) \subseteq \Phi^+ \) imply that there exists a \( j \in \{1, \ldots, m\} \) such that \( \omega_{ij} \cdots \omega_m (O_{im}) \subseteq \Phi^+ \) and \( \omega_{i_{j+1}} \cdots \omega_m (O_{im}) \subseteq \Phi^- \). However, \( \omega_j \) changes the sign of all roots in \( \Phi_j \), but of none in \( \Phi - \Phi_j \). Hence \( \omega_{i_{j+1}} \cdots \omega_m (O_{im}) \subseteq \Phi^- \). By part (8) of the previous lemma, we have that \( \omega_{i_{j+1}} \cdots \omega_m (O_{im}) \omega_{i_{j+1}} \cdots \omega_m (O_{im}) = \omega_{ij} \). Hence \( \omega_{i_{j+1}} \cdots \omega_m = \omega_{i_{j+1}} \cdots \omega_m \), so we get

\[
W = \omega_1 \cdots \omega_{ij} \cdots \omega_m = \omega_1 \cdots \omega_{ij} \cdots \omega_{i_{j+1}} \cdots \omega_m \omega_{i_{j+1}} \cdots \omega_m.
\]

But this is an \( \omega \)-factorization of \( w \) of length \( n - 2 \), a contradiction.
Lemma 9. (See [4, Lemma 2].) Let $p$ be a prime number. Let $P$ be a Sylow $p$-subgroup of a finite group $K$. Then

$$w = \omega_i \cdots \omega_n.$$ 

This means that $\omega_i$ is in the group generated by $\omega_{i_1}, \ldots, \omega_{i_n}$, so $\omega_i \in \langle W_{O_{i_1}}, \ldots, W_{O_{i_n}} \rangle = W_{O_{i_1} \cup \cdots \cup O_{i_n}}$ and $\omega_i \in W_{O_{i}}$ (see [3, Theorem 2.5.6]). But $W_{O_{i_1} \cup \cdots \cup O_{i_n}} \cap W_{O_{i}} = W_{\emptyset} = 1$, a contradiction. So we have $\omega_i \cdots \omega_n(\Phi_i^+) \cap \Phi_i^+ = \emptyset$, hence $w(\Phi_i^+) = \Phi_i^-$. So, by part (8) of the previous lemma, we get $\omega_i^w = \omega_i$, therefore

$$\omega_i = \omega_i \cdots \omega_i \cdots \omega_i.$$ 

Proposition 10. Let $G$ be a group of Lie type over a field $\mathbb{K}$ of characteristic $p$. We have that:

$$P_G^{(p)}(s) = (-1)^{|H|} \sum_{J \subseteq I} (-1)^{|J|} \left( \frac{\mu_G(H)}{T_W(t)} \right)^{1-s}.$$ 

Proof. The argument is the same as in the proof of Theorem 3 in [4]. Let $P$ be a Sylow $p$-subgroup of $G$. The group $G$ possesses a $(B, N)$-pair, where $B = N_G(P)$ (see [3, Proposition 8.2.1 and Theorem 13.5.4]). Since $G$ possesses a $(B, N)$-pair, we know that if a maximal subgroup $M$ of $G$ contains $P$, then $M$ contains also $B = N_G(P)$ (see [3, Theorem 8.3.2]). By Lemma 9, we get that

$$P_G^{(p)}(s) = \sum_{B \leq H \leq G} \frac{\mu_G(H)}{|G : H|^{s-1}}.$$ 

The subgroups of $G$ containing $B$ are called the parabolic subgroups. By [3, Proposition 8.2.2], we associate to a subset $J$ of $I$ a parabolic subgroup $P_J$. Moreover, the map $J \mapsto P_J$ is an isomorphism between the lattice $\mathcal{P}(I)$ and the lattice of subgroups of $G$ containing $N_G(P)$ [3, Theorem 8.3.4]. In particular (see [20, 3.8.3]), we have that $\mu_G(P_J) = \mu_{\mathcal{P}(I)}(J) = (-1)^{|J|-|I|}$. Now by [3, 8.6 and 14.1], we have $T_{W_J}(t) = \frac{[P_J]}{|t|}$. Thus we get:
\begin{align*}
P_G^{(p)}(s) &= \sum_{B \leq H \leq G} \frac{\mu_G(H)}{|G : H|^{s-1}} = \sum_{J \leq I} \frac{\mu_G(P_J)}{|G : P_J|^{s-1}} \\
&= \sum_{J \leq I} (-1)^{|J|-|I|} \left( \frac{T_{WJ}(t)}{T_{WJ}(t)} \right)^{1-s} = (-1)^{|I|} \sum_{J \leq I} (-1)^{|J|} \left( \frac{T_{WJ}(t)}{T_{WJ}(t)} \right)^{1-s}.
\end{align*}

This ends the proof. □

In the sequel, we consider the value of $P_G^{(p)}(s)$ for $s = -1$. First, we obtain an easier expression for $P_G^{(p)}(-1)$.

To do that, we introduce some more definitions. Let $u$ be an element of $\mathcal{W}$. We denote by $I_u$ the subset of $I$ consisting of the orbits $K \in I$ such that $u(K) \subseteq \Phi^+$. By Lemma 7(6), note that $K \subseteq I_u$ if and only if there exists $r \in K$ such that $u(r) \in \Phi^+$. Moreover, let $I_u^c = I - I_u$. Finally, if $v$ is another element of $\mathcal{W}$, then let $I_{u,v} = I_u \cap I_v$.

Mimicking the proof of Proposition 9.4.5 of [3], we obtain the following.

**Lemma 11.** Under the above conditions, we have that

\[
(-1)^{|I|} P_G^{(p)}(-1) = \sum_{J \leq I} (-1)^{|J|} \left( \frac{T_{WJ}(t)}{T_{WJ}(t)} \right)^{2} = \sum_{(u,v) \in \mathcal{W} \times \mathcal{W}} t^{l(u)+l(v)}.
\]

**Proof.** Let $J$ be a subset of $I$. By Lemma 7(7), each element $w$ of $\mathcal{W}$ has a unique expression in the form $w = d_j w_j$, where $d_j \in D_J$ and $w_j \in \mathcal{W}_J$. Moreover, $l(w) = l(d_j) + l(w_j)$. It follows that

\[
T_{WJ}(t) = \sum_{w \in \mathcal{W}} t^{l(w)} = \sum_{d_j \in D_J} \sum_{w_j \in \mathcal{W}_J} t^{l(d_j w_j)} = \sum_{d_j \in D_J} \sum_{w_j \in \mathcal{W}_J} t^{l(d_j) + l(w_j)}
\]

\[
= \sum_{d_j \in D_J} t^{l(d_j)} \sum_{w_j \in \mathcal{W}_J} t^{l(w_j)} = \sum_{d_j \in D_J} t^{l(d_j)} T_{WJ}(t).
\]

Hence, we have

\[
\sum_{J \leq I} (-1)^{|J|} \left( \frac{T_{WJ}(t)}{T_{WJ}(t)} \right)^{2} = \sum_{J \leq I} (-1)^{|J|} \left( \sum_{d_j \in D_J} t^{l(d_j)} \right)^{2}
\]

\[
= \sum_{J \leq I} (-1)^{|J|} \sum_{u,v \in D_J} t^{l(u)} t^{l(v)}
\]

\[
= \sum_{J \leq I} (-1)^{|J|} \sum_{u,v \in \mathcal{W}} t^{l(u)} t^{l(v)}
\]

\[
= \sum_{u,v \in \mathcal{W}} \sum_{J \subseteq I_{u,v}} (-1)^{|J|} t^{l(w)+l(v)}.
\]

The last equality holds since we have that $J \subseteq I_{u,v}$ if and only if $u(J^*) \subseteq \Phi^+$. Finally, it is clear that
\[
\sum_{J \subseteq I_{u,v}} (-1)^{|J|} = \begin{cases} 
1 & \text{if } I_{u,v} = \emptyset, \\
0 & \text{otherwise.}
\end{cases}
\]

The proof is complete. \qed

By the previous lemma, we can write

\[
(-1)^{|l|} p_G^{(p)}(-1) = \sum_{(u,v) \in \mathcal{W} \times \mathcal{W}} t^{l(u) + l(v)} = \sum_{n \in \mathbb{N}} c_n(G)t^n,
\]

where

\[
c_n(G) = \left| \{(u, v) \in \mathcal{W} \times \mathcal{W}: I_{u,v} = \emptyset, l(u) + l(v) = n\} \right|.
\]

The following lemma shows that \(c_n(G) = 0\) for \(n < L\).

**Lemma 12.** Let \(u, v \in \mathcal{W}\). If \(I_{u,v} = \emptyset\), then \(l(u) + l(v) \geq L\).

**Proof.** Since \(I_{u,v} = \emptyset\), for each \(j \in \{1, \ldots, k\}\) we have that \(u(O_j) \subseteq \Phi^-\) or \(v(O_j) \subseteq \Phi^-\). Hence \(u(\Phi_j^+) \subseteq \Phi^-\) or \(v(\Phi_j^+) \subseteq \Phi^-\). This implies that

\[
|\Phi_j^+ \cap u^{-1}(\Phi^-)| + |\Phi_j^+ \cap v^{-1}(\Phi^-)| \geq |\Phi_j^+| \quad (\dagger_0)
\]

for each \(j \in \{1, \ldots, k\}\). Moreover we have

\[
|\Phi^+ \cap w^{-1}(\Phi^-)| \geq \sum_{j=1}^k |\Phi_j^+ \cap w^{-1}(\Phi^-)| \quad (\dagger_1)
\]

for \(w \in \{u, v\}\). Hence we get:

\[
l(u) + l(v) = |\Phi^+ \cap u^{-1}(\Phi^-)| + |\Phi^+ \cap v^{-1}(\Phi^-)|
\]

\[
\geq \sum_{j=1}^k |\Phi_j^+ \cap u^{-1}(\Phi^-)| + |\Phi_j^+ \cap v^{-1}(\Phi^-)| \quad (*)
\]

\[
\geq \sum_{j=1}^k |\Phi_j^+| = L.
\]

The proof is finished. \qed

The following is an easy but important result.

**Lemma 13.** There is a unique element \(v \in \mathcal{W}\) such that \(I_{v,v} = \emptyset\). In particular, \(l(v) = |\Phi^+|\).

Let \(v \in \mathcal{W}\) such that \(I_{v,v} = \emptyset\). Thus \(I_v = \emptyset\), i.e. \(v(\Phi^+) = \Phi^-\). By Lemma 7(2), we have the claim. \qed
The following proposition shows that \( cL(G) = 2 \).

**Proposition 14.** The set of pairs of elements \( u, v \) in \( \mathcal{W} \) such that \( l(u) + l(v) = L \) and \( I_{u,v} = \emptyset \) consists of exactly two pairs.

**Proof.** Let \( u, v \in \mathcal{W} \) such that \( l(u) + l(v) = L \) and \( I_{u,v} = \emptyset \). Since \( l(u) + l(v) = L \), the expression \((*)\) in the proof of Lemma 12 holds with \( = \) instead of \( \geq \). This implies that the expressions \((\dagger_0), (\dagger_1)\) become

\[
|\Phi_j^+ \cap u^{-1}(\Phi^-)| + |\Phi_j^+ \cap v^{-1}(\Phi^-)| = |\Phi_j^+|
\]

for each \( j \in \{1, \ldots, k\} \), and

\[
|\Phi^+ \cap w^{-1}(\Phi^-)| = \sum_{j=1}^{k} |\Phi_j^+ \cap w^{-1}(\Phi^-)|
\]

for \( w \in \{u, v\} \).

We divide the proof into steps.

**Step 1.** The set \( \{I_u^c, I_v^c\} \) is a partition of \( I \).

Let \( j \in \{1, \ldots, k\} \). As at the beginning of the proof of Lemma 12, we have that \( u(O_j) \subseteq \Phi^- \) or \( v(O_j) \subseteq \Phi^- \). Since \( w(O_j) \subseteq \Phi^- \) if and only if \( w(\Phi_j^+) \subseteq \Phi^- \) for each \( w \in \mathcal{W} \), using \((\dagger_0)\), we conclude that exactly one of \( u(O_j) \subseteq \Phi^- \) and \( v(O_j) \subseteq \Phi^- \) holds. Thus we have the claim.

**Step 2.** Let \( i, j \in \{1, \ldots, k\} \), \( i \neq j \). If \( O_i, O_j \in I_u^c \) (resp. \( O_i, O_j \in I_v^c \)), then \( O_i \) and \( O_j \) are not joined in the Dynkin diagram \( \mathcal{D}' \) of \( \mathcal{W} \).

Note that

\[
\Phi^+ \cap u^{-1}(\Phi^-) = \bigcup_{j=1}^{k} (\Phi_j^+ \cap u^{-1}(\Phi^-)),
\]

by \((\dagger_1)\). Assume that \( O_i, O_j \in I_u^c \). For contradiction, suppose that \( O_i \) and \( O_j \) are joined in \( \mathcal{D}' \). So, there exist \( r \in O_i \) and \( s \in O_j \) such that \( 4 \frac{(r,s)^2}{(r,r)(s,s)} \neq 0 \). In particular, this implies that \( \frac{2(r,s)}{(r,r)(s,s)} = -n \) for some \( n \in \mathbb{N} \setminus \{0\} \), such that \( s, r + s, \ldots, nr + s \in \Phi \) (see [3, 3.3 and 3.4]). Now, by hypothesis, we have that \( u(r) \in \Phi^- \) and \( u(s) \in \Phi^- \), so \( u(r+s) \in \Phi^- \). Hence, \( r + s \in \Phi^+ \cap u^{-1}(\Phi^-) = \bigcup_{i=1}^{k} (\Phi_i^+ \cap u^{-1}(\Phi^+)) \), thus \( r + s \in \Phi_i^+ \) for some \( i \in \{1, \ldots, k\} \), a contradiction with \( i \neq j \).

**Step 3.** The partition \( \{I_u^c, I_v^c\} \) of \( I \) is independent on the choice of \( u, v \in \mathcal{W} \) such that \( l(u) + l(v) = L \) and \( I_{u,v} = \emptyset \).

Consider the Dynkin diagram \( \mathcal{D}' \). It is known that \( \mathcal{D}' \) is a connected tree. So there exists a unique partition \( I = J_1 \cup J_2 \) of the set \( I \) of vertices of \( \mathcal{D}' \) such that if two vertices \( K_1, K_2 \) are joined by an edge, then \( K_1 \in J_1 \) if and only if \( K_2 \in J_2 \) (i.e. \( K_1 \) and \( K_2 \) are not in the same block). By Steps 1 and 2, \( \{I_u^c, I_v^c\} \) is such partition.

**Step 4.** Denote by \( \mathcal{I}_u \) the set of \( i \in \{1, \ldots, k\} \) such that \( \omega_i \) appears in each \( \omega \)-factorization of \( u \) of minimal length. Let \( \mathcal{I}_u = \{ j \in \{1, \ldots, k\} : O_j \in I_u^c \} \). We have that \( \mathcal{I}_u = \mathcal{I}_u \). Moreover, if \( i \in \mathcal{I}_u \), then the factor \( \omega_i \) appears with multiplicity one in an \( \omega \)-factorization of \( u \) of minimal length.
Let \( j \in \tilde{I}_u \), so \( O_j \in I_u^L \). By Lemma 8(2), we have that \( \omega_j \) appears in each \( \omega \)-factorization of \( u \) of minimal length. So \( j \in I_u \) and \( \tilde{I}_u \subseteq I_u \). Recall that \( u(O_j) \leq \Phi^- \) if and only if \( u(\Phi_j^+ \) \( \subseteq \Phi^- \). Hence, by (11), we have

\[
I(u) = |\Phi^+ \cap u^{-1}(\Phi^-)| = \sum_{j \in \tilde{I}_u} |\Phi_j^+| \leq \sum_{j \in I_u} |\Phi_j^+|.
\]

Thus, to prove that \( \tilde{I}_u \supseteq I_u \) it is enough to show that

\[
I(u) \geq \sum_{i \in I_u} |\Phi_i^+|,
\]

but this is clear by Lemma 8(1). Moreover, we get \( I(u) = \sum_{i \in \tilde{I}_u} |\Phi_i^+| \). Hence, if \( i \in \tilde{I}_u \), then the factor \( w_i \) appears exactly once in an \( \omega \)-factorization of \( u \) of minimal length.

**Step 5.** Let \( i, j \in I_u \). We have that \( \omega_i \) and \( \omega_j \) commute.

Let \( r \in O_i \) and \( s \in O_j \). By Step 2, since \( O_i, O_j \in I_u^L \), we have that \( O_i \) and \( O_j \) are not joined. So, in particular, \( (s, r) = 0 \). Thus \( w_r \) and \( w_s \) commute. Since \( \omega_i \in W_{O_i} \) and \( \omega_j \in W_{O_j} \), we have \( \omega_i \omega_j = \omega_j \omega_i \), as claimed.

Now, we finish the proof of the proposition.

First, we show that a pair \( u, v \) in \( \mathcal{W} \) such that \( I(u) + I(v) = L \) and \( I_{u,v} = \emptyset \) exists. Take a partition \( L = J_1 \cup J_2 \) of the vertex set of \( D' \) such that if \( K_1, K_2 \) are vertices in \( L \), then \( K_1 \in J_1 \) if and only if \( K_2 \in J_2 \) (i.e. \( \{K_1, K_2\} \) is an edge of \( D' \)). Let \( l_j = \{i: O_i \in J_j\} \) for \( j = 1, 2 \). As in Step 5, we have that if \( i \in l_1 \) and \( j \in l_2 \), then \( \omega_i \) and \( \omega_j \) commute. Thus we define \( u = \prod_{i \in l_1} \omega_i \) and \( v = \prod_{i \in l_2} \omega_i \). It is straightforward to show that \( J_1 = I_u^L \) and \( J_2 = I_v^L \), hence \( I_{u,v} = \emptyset \). Moreover, by Lemma 8(1), we get \( I(u) = \sum_{i \in l_1} |\Phi_i^+| \) and \( I(v) = \sum_{i \in l_2} |\Phi_i^+| \), hence \( I(u) + I(v) = L \).

Now, we show that there exist exactly two such pairs. Note that Steps 4 and 5 hold also interchanging \( u \) and \( v \).

Suppose that \( u' \) and \( v' \) are elements of \( \mathcal{W} \) such that \( I(u') + I(v') = L \) and \( I_{u',v'} = \emptyset \). By Step 3, we have that \( \{I_u^L, I_v^L\} = \{I_u^L, I_v^L\} \).

Suppose that \( I_u^L = I_u^L \) and \( I_v^L = I_v^L \). We claim that \( u = u' \) and \( v = v' \). By Step 4 and \( I_u^L = I_u^L \), we have that an \( \omega \)-factorization of minimal length of \( u \) has the same factors as an \( \omega \)-factorization of minimal length of \( u' \), and each factor has multiplicity one in both the factorizations. By Step 5, these factors commute, hence \( u = u' \). Similarly, \( v = v' \) and we get the claim.

Suppose that \( I_u^L = I_u^L \) and \( I_v^L = I_v^L \). Reasoning as above, we get \( u = v' \) and \( v = u' \).

Thus we get that \( (u', v') \in \{(u, v), (v, u)\} \). By Lemma 13, we know that \( u \neq v \). This ends the proof. \( \square \)

Now, we can prove the main theorem of this section.

**Theorem 15.** Let \( G \) be a simple group of Lie type of characteristic \( p \) over \( \mathbb{K} \). We have that

\[
P^{(p)}_G(-1) = (-1)^{|I|} \sum_{n \in \mathbb{N}} c_n(G) t^n
\]

where \( c_n(G) = |\{(u, v) \in \mathcal{W} \times \mathcal{W}: I_{u,v} = \emptyset, I(w) + I(v) = n\}| \). In particular,

1. If \( n < L \) or \( n \geq |\Phi| \), then \( c_n(G) = 0 \);
2. If \( n \neq |\Phi| \), then \( c_n(G) \) is even;
3. \( c_{|\Phi|}(G) = 1 \);
4. \( c_L(G) = 2 \).
Table 1
Dykin diagrams, fundamental roots and value of \( L \) for \( G \).

<table>
<thead>
<tr>
<th>Untwisted</th>
<th>Twisted</th>
</tr>
</thead>
<tbody>
<tr>
<td>( G )</td>
<td>( \mathcal{D} = \mathcal{D}' )</td>
</tr>
<tr>
<td>( A_k(t) )</td>
<td>( A_k )</td>
</tr>
<tr>
<td>( B_k(t) )</td>
<td>( B_k )</td>
</tr>
<tr>
<td>( C_k(t) )</td>
<td>( C_k )</td>
</tr>
<tr>
<td>( D_k(t) )</td>
<td>( D_k )</td>
</tr>
<tr>
<td>( E_6(t) )</td>
<td>( E_6 )</td>
</tr>
<tr>
<td>( E_7(t) )</td>
<td>( E_7 )</td>
</tr>
<tr>
<td>( E_8(t) )</td>
<td>( E_8 )</td>
</tr>
<tr>
<td>( F_4(t) )</td>
<td>( F_4 )</td>
</tr>
<tr>
<td>( G_2(t) )</td>
<td>( G_2 )</td>
</tr>
</tbody>
</table>

**Proof.** The first assertion is Lemma 11.

Let \( u, v \in \mathcal{W} \) such that \( l_u, v = \emptyset \). Note that, if \( w \in \mathcal{W} \), then \( l(w) \leq |\Phi^+| \).

1. By Lemma 12, if \( n < l \), then \( c_n(G) = 0 \). Furthermore, \( l(u) + l(v) \leq 2|\Phi^+| = |\Phi| \). Hence if \( n > |\Phi| \), then \( c_n(G) = 0 \).

2. Suppose that \( l(u) + l(v) \neq |\Phi| \). By Lemma 13, we have that \( w \neq v \). Hence \( c_n(G) \) is even.

3. Suppose that \( l(u) + l(v) = |\Phi| \). Hence \( l(u) = l(v) = |\Phi^+| \). By Lemma 7(2) we have that \( u = v \) is the unique element such that \( u(\Phi^+) = \Phi^- \). Thus \( c_{|\Phi^+|}(G) = 1 \).

4. This is Proposition 14.

The proof is finished. \( \square \)

5. The value of \( L \) for a simple group of Lie type

In this section we calculate the explicit values of \( L \) for the simple groups of Lie type. These values are given in Table 1. In this table, we use the notation of [3] for the groups of Lie type.

If \( G \) is an untwisted group, then \( \rho \) is trivial. Hence, the unique element of a \( \rho \)-orbit is a fundamental root. Thus, for each \( i \in \{1, \ldots, k\} \), we have that \( O_i = \{r_i\} \) where \( \Pi = \{r_1, \ldots, r_k\} \). So, \( \Phi^+_i = \Phi^-_i = \{r_i\} \). Hence \( L = \sum_{i=1}^{k} |\Phi^+_i| = k = |\Pi| \).

Now, suppose \( G \) is a twisted group of Lie type. To get the value of \( L \), we use the following result.

**Lemma 16.** (See [3, 3.4 and 3.6]) Let \( r, s \in \Pi \) be two fundamental roots. Let \( n_r = \frac{2(r,s)}{(r,r)} \), \( n_s = \frac{2(s,r)}{(s,s)} \) and \( n_{r,s} = n_r n_s \). Suppose that \( n_r \leq n_s \). Exactly one of the following occurs.

- \( n_{r,s} = 0 \). We have that \( n_r = n_s = 0 \) and \( \Phi^+_{[r,s]} = \{r, s\} \). In this case the roots are not joined in the Dynkin diagram \( \mathcal{D} \).
- \( n_{r,s} = 1 \). We have that \( n_r = n_s = -1 \) and \( \Phi^+_{[r,s]} = \{r, s, r + s\} \).
- \( n_{r,s} = 2 \). We have that \( n_r = -2, n_s = -1 \) and \( \Phi^+_{[r,s]} = \{r, s, r + s, 2r + s\} \).
- \( n_{r,s} = 3 \). We have that \( n_r = -3, n_s = -1 \) and \( \Phi^+_{[r,s]} = \{r, s, r + s, 2r + s, 3r + s, 3r + 2s\} \).
- \( n_{r,s} = 4 \). We have that \( r = s \) and \( \Phi^+_{[r]} = \{r\} \).

We give some examples of the calculation of the value of \( L \); the others are obtained with similar argument, using Lemma 16 and Fig. 5. Let \( \Pi = \{r_1, \ldots, r_l\} \). In the sequel, when we say that two roots are joined, we refer to Figs. 1–4.

**Case** \( 2A_l \). We divide this case into two subcases, \( l \) odd and \( l \) even.

Suppose that \( l \) is odd. Thus the orbits are \( O_i = \{r_i, r_{2k-i}\} \) for \( i \in \{1, \ldots, k\} \), so that \( l = 2k - 1 \). Now, if \( i < k \), then \( O_i \) consists of two roots which are not joined in \( \mathcal{D} \). So \( O_i = \Phi^+_i \) for \( i < k \). Moreover,
Fig. 1. Dynkin diagram of $A_{2k-1}$.

Fig. 2. Dynkin diagram of $A_{2k}$.

Fig. 3. Dynkin diagram of $D_4$.

Fig. 4. Dynkin diagram of $G_2$.

Fig. 5. Dynkin diagrams.

$O_k = \{r_k\} = \Phi_k^+$. Hence, we have

$$L = \sum_{i=1}^{k} |\Phi_i^+| = \sum_{i=1}^{k} |O_i| = 2k - 1 = l.$$

A similar argument applies to cases $^2E_6$ and $^2D_l$.

Suppose that $l$ is even. Thus the orbits are $O_i = \{r_i, r_{2k+1-i}\}$ for $i \in \{1, \ldots, k\}$, so that $l = 2k$. As above, if $i < k$, then $O_i = \Phi_i$. Now, consider $O_k = \{r_k, r_{k+1}\}$. By [3, 3.6], we have that $r_k, r_{k+1} = 1$. Hence, by
Lemma 16, \( \Phi_k^+ = \{r_k, r_{k+1}, r_k + r_{k+1}\} \). Thus, we get
\[
L = \sum_{i=1}^{k} |\Phi_i^+| = \sum_{i=1}^{k-1} |O_i| + |\Phi_k^+| = 2(k - 1) + 3 = l + 1.
\]

A similar argument applies in case 2\( F_4 \).

**Case 3\( D_4 \).** In this case \( k = 2 \) and \( O_1 = \{r_1\}, O_2 = \{r_2, r_3, r_4\} \). We have that \( \Phi_1^+ = O_1 \). Since \( r_2, r_3, r_4 \) are pairwise not joined in the Dynkin diagram \( \mathcal{D} \), we have that \( \Phi_2^+ = O_2 \). Thus, \( L = 4 \).

**Case 2\( G_2 \).** In this case \( k = 1 \) and \( O_1 = \{r_1, r_2\} \). Moreover, by [3, 3.6], we have \( n_{r_1, r_2} = 3 \). Thus, by Lemma 16, \( \Phi_k^+ = \{r_1, r_2, r_1 + r_2, 2r_1 + r_2, 3r_1 + r_2, 3r_2 + 2r_2\} \). So, we get \( L = 6 \). A similar argument applies in case 2\( B_2 \).

6. Notation and definition for the classical groups

In this section we give some definitions and notation we will use until the end of the paper. Let \( p \) be a prime number, let \( f \) be a positive integer and let \( q \) be the number \( p^f \). Moreover let \( n \) be an integer greater than or equal to 2. Denote by \( V \) a vector space of dimension \( n \) over \( \mathbb{F} = \mathbb{F}_{q^u} \) where \( u \in \{1, 2\} \). As in [13, §2.1], let \( \kappa \) be a form defined over the vector space \( V \) over \( \mathbb{F}_{q^u} \) and let \( f \) be the bilinear form associated to \( \kappa \). We consider four cases:

- **Case L**: \( \kappa = f \) is identically 0.
- **Case S**: \( \kappa = f \) is a non-degenerate symplectic form.
- **Case O**: \( \kappa = Q \) is a non-degenerate quadratic form; moreover \( f(v, w) = Q(v + w) - Q(v) - Q(w) \).
- **Case U**: \( \kappa = f \) is a non-degenerate unitary form.

The number \( u \) is defined as follows
\[
u = \begin{cases} 2 & \text{if case U holds}, \\ 1 & \text{otherwise}. \end{cases}
\]

Moreover, when case O, we distinguish three cases (see [13, pp. 27–28]):

- **Case O\(^o\)**, if \( n \) is odd (in this case \( q \) is odd).
- **Case O\(^+\)**, if \((V, Q)\) is of Witt defect 0.
- **Case O\(^-\)**, if \((V, Q)\) is of Witt defect 1.

Denote by \( \Gamma(V, \kappa) \) the group of the \( \kappa \)-semisimilarities. Moreover, let
\[
I(V, \kappa) = \{\phi \in \text{GL}(V, \mathbb{F}) : \kappa(\phi(v)) = \kappa(v), \text{ for all } v \in V^l\},
\]
where \( l = 1 \) if \( \kappa \) is quadratic, \( l = 2 \) otherwise. With a little abuse of notation, we denote by \( \mathbb{F}^* \) the group of nonzero scalar linear transformations. If \( K \) is a subgroup of \( \Gamma(V, \kappa) \), denote by \( \overline{K} \) the reduction modulo \( \mathbb{F}^* \cap K \). For example, \( \Gamma(V, \kappa) \) is the factor group \( \Gamma(V, \kappa)/\mathbb{F}^* \). Let \( S(V, \kappa) = I(V, \kappa) \cap \text{SL}(V, \mathbb{F}) \) and let \( \Omega(V, \kappa) \) be the derived subgroup of \( S(V, \kappa) \). In particular, note that \( \overline{\Omega}(V, \kappa) = \overline{S}(V, \kappa) \) unless case O holds (see [13, p. 14]). It turns out that:

- \( \overline{\Omega}(V, \kappa) \cong \text{PSL}_n(q) \), if case L holds;
- \( \overline{\Omega}(V, \kappa) \cong \text{PSU}_n(q) \), if case U holds;
Table 2
Classical simple groups.

<table>
<thead>
<tr>
<th>Case</th>
<th>Notation</th>
<th>Lie notation</th>
<th>Terminology</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>PSL(_n)(q)</td>
<td>(A_{n-1}(q))</td>
<td>linear group</td>
</tr>
<tr>
<td>U</td>
<td>PSU(_n)(q, (q^{2}))</td>
<td>(2A_{n-1}(q))</td>
<td>unitary group</td>
</tr>
<tr>
<td>S</td>
<td>PSp(_n)(q)</td>
<td>(C_n/2(q))</td>
<td>symplectic group</td>
</tr>
<tr>
<td>O(^+)</td>
<td>PΩ(_n)(q)</td>
<td>(D_n/2(q))</td>
<td>orthogonal group</td>
</tr>
<tr>
<td>O(^-)</td>
<td>PΩ(_n)(q)</td>
<td>(2D_n/2(q))</td>
<td></td>
</tr>
<tr>
<td>O(^o)</td>
<td>PΩ(_n)(q)</td>
<td>(B_{n-1}(q))</td>
<td></td>
</tr>
</tbody>
</table>

\[\Omega(V, \kappa) \cong \text{PSp}_n(q), \text{ if case } S \text{ holds;}\]
\[\Omega(V, \kappa) \cong \text{PΩ}_n(q), \text{ if case } O^+ \text{ holds;}\]
\[\Omega(V, \kappa) \cong \text{PΩ}^+\_n(q), \text{ if case } O^- \text{ holds;}\]
\[\Omega(V, \kappa) \cong \text{PΩ}^-\_n(q), \text{ if case } O^- \text{ holds.}\]

Finally, define

\[A = \begin{cases} \Gamma(V, \kappa)(\iota) & \text{in case } L \text{ with } n \geq 3, \\ \Gamma(V, \kappa) & \text{otherwise,} \end{cases}\]

where \(\iota\) is an inverse transpose automorphism (see [13, (2.2.4)]) of the group \(S(V, \kappa) \cong \text{SL}(V)\) when case \(L\) holds.

We recall the following.

Theorem 17. (See [13, Theorems 2.1.3 and 2.1.4].) Assume that \(n \geq 2, 3, 4, 7\) in cases \(L, U, S\) and \(O\) respectively.
Then \(\Omega(V, \kappa)\) is non-abelian simple, except when one of the following holds:

- Case \(L\) and \((n, q) \in \{(2, 2), (2, 3)\} \).
- Case \(U\) and \((n, q) = (3, 2)\).
- Case \(S\) and \((n, q) = (4, 2)\).

Moreover, if \(\Omega(V, \kappa)\) is non-abelian simple, then \(\text{Aut}(\Omega(V, \kappa)) \cong \Gamma(V, \kappa)\), except when one of the following holds:

- Case \(L\) and \(n \geq 3\). In this case \(\text{Aut}(\Omega(V, \kappa))\) has a subgroup of index 2 isomorphic to \(\Gamma\).
- Case \(O^+\) and \(n = 8\).
- Case \(S, n = 4\) and \(q\) even.

Since in the previous sections we used a different notation for the classical groups, we record in Table 2 the correspondence between the new notation and the Lie notation.

Under the assumptions of Theorem 17, when \(\Omega(V, \kappa)\) is non-abelian simple, let

\[G = \Omega(V, \kappa).\]

From now on, we assume that

\[G = \Omega(V, \kappa) \leq X \leq \Gamma(V, \kappa)\]

and we require that \(X\) does not contain non-trivial graph automorphisms (briefly, we say that \(X\) is a classical projective group). This means that \(\Omega(V, \kappa) \leq X \leq \Gamma(V, \kappa)\) and if case \(O^+\) holds, then \(X \leq \ker(\gamma)\). The homomorphism \(\gamma\) is defined as follows. Suppose that case \(O^+\) holds. As in [13, p. 30], let \(U_k\) be the set of totally singular subspace of \(V\) of dimension \(k\). Let \(\sim\) be the relation on \(U_n\) defined
Table 3
Values of \( \bar{\beta}_p(X) \), given the socle \( G \) of \( X \).

<table>
<thead>
<tr>
<th>( S )</th>
<th>( \bar{\beta}_p(X) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{PSL}_2(q) )</td>
<td>( n - 1 )</td>
</tr>
<tr>
<td>( \text{PSL}_3(q) )</td>
<td>( n - 1 )</td>
</tr>
<tr>
<td>( \text{PSp}_n(q) )</td>
<td>( \frac{n}{2} - \log_q</td>
</tr>
<tr>
<td>( \Omega_n^- )</td>
<td>( \frac{n - 1}{2} )</td>
</tr>
</tbody>
</table>

by \( W \sim U \) if \( m - \dim(W \cap U) \) is even. This relation defines a partition \( \{ U_m^1, U_m^2 \} \) of \( U_m \) and gives a homomorphism \( \gamma : \Gamma \rightarrow \text{Sym}(U_m^1, U_m^2) \). In particular, \( U_m^1 \) and \( U_m^2 \) are the two \( G \)-orbits on \( U_m \).

When \( V \) and \( \kappa \) are clear from the contest, we omit them. For example, we shall write \( \Gamma \) instead of \( \Gamma(V, \kappa) \).

In the following sections, we are going to study the subgroups of \( X \) which are supplemented by \( G \), which are intersection of maximal subgroups and which do not contain a Sylow \( p \)-subgroup of \( X \).

We define

\[
\beta_p(X) = \log_q \min \{|X : H|_p : H < X, |X : H|_p > 1, HG = X, \mu_X(H) \neq 0\}.
\]

This number will be crucial in the next two sections and in the proof of our main result. In fact, note that

\[
P_{X,G}(-1) - P_{X,G}^{(p)}(-1) = \sum_{p | k} a_k(X, G)k
\]

and by Lemma 6 we have that \( k \) divides

\[
a_k(X, G) = \sum_{H \leq X : HG = X, |X : H| = k} \mu_X(H).
\]

Hence we have that

\[
|P_{X,G}(-1) - P_{X,G}^{(p)}(-1)|_p \geq q^{\beta_p(X)}.
\]

We shall prove the following theorem, which gives a lower bound of \( \beta_p(X) \).

**Theorem 18.** Let \( X \) be a classical projective group of characteristic \( p \) and let \( G \) be its socle. Let \( \bar{\beta}_p(X) \) be as in Table 3 with the following exceptions:

- for \( G = \text{PSL}_2(q) \) we have \( \bar{\beta}_p(X) = \log_q p \);
- for \( G = \text{PSL}_3(q_0^2) \) we have \( \bar{\beta}_p(X) = 1.5 \);
- for \( G \in \{ \text{PSL}_4(q), \text{PSL}_4(q) \} \), we have \( \bar{\beta}_p(X) = 2 \).

We have that \( \beta_p(X) \geq \bar{\beta}_p(X) \).

The proof of this theorem is given in Proposition 19 and Theorem 20.
Table 4

<table>
<thead>
<tr>
<th>Case</th>
<th>G</th>
<th>L</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>PSL₄(q)</td>
<td>n - 1</td>
</tr>
<tr>
<td>U</td>
<td>PSU₅(q)</td>
<td>2(\frac{n-1}{2}) + 1</td>
</tr>
<tr>
<td>S</td>
<td>PSp₆(q)</td>
<td>\frac{n}{2}</td>
</tr>
<tr>
<td>O₀</td>
<td>PΩ₃(q)</td>
<td>\frac{n-1}{2}</td>
</tr>
<tr>
<td>O±</td>
<td>PΩ₃±(q)</td>
<td>\frac{n}{2}</td>
</tr>
</tbody>
</table>

7. Indices of subgroups of G which are contained in a maximal subgroup that does not contain a Sylow p-subgroup of G

Let X be as in the previous section.

In this section we deal with the maximal subgroups M of X such that MG = X and M does not contain a Sylow p-subgroup of X. By [13], the group M \cap G is a member of one of the classes of geometric subgroups C₁, ..., C₈ or of the class S (see [13] for the notation).

We recall the definition of S (see [13, p. 3]). A subgroup H of X lies in S if and only if the following hold:

a. The socle S of H is a non-abelian simple group.

b. If L is the full covering group of S, and if ρ : L → GL(V) is a representation of L such that ρ(L) = S, then ρ is absolutely irreducible.

c. ρ(L) cannot be realized over a proper subfield of \( \mathbb{F} \).

d. If ρ(L) fixes a non-degenerate quadratic form on V, then G ∈ \{ PΩₙ(q), PΩₙ⁺(q), PΩₙ⁻(q) \}.

e. If ρ(L) fixes a non-degenerate symplectic form on V, but no non-degenerate quadratic form, then G = PSpₙ(q).

f. If ρ(L) fixes a non-degenerate unitary form on V, then G = PSUₙ(q).

g. If ρ(L) does not satisfy the conditions in (d), (e) of (f), then G = PSLₙ(q).

In Table 4 we translate the results of Table 1 in the standard notation for classical groups.

The main task of this section is to prove the following.

Proposition 19. Let X be a classical projective group. Let M be maximal subgroup of X such that MG = X and M does not contain a Sylow p-subgroup of X. Then \( \log_q |X : M| \geq \tilde{\beta}(X) \), where \( \tilde{\beta}(X) \) is as in Theorem 18.

Proof. If case L, \( n = 2 \) holds, then the result follows from [11, p. 213].

Suppose that M is as in the statement. Suppose that M is a member of one of the classes C₁(X), ..., C₈(X). By [13, Proposition 3.1.3], the group M \cap G is a member of the classes C₁(G), ..., C₈(G).

Using the results of [13] on the geometric subgroups of a classical group, we obtain Tables 5–12. Note that in Table 5 we report only the subgroups which do not contain a Sylow p-subgroup of G. Direct calculations show that if M is a member of one of the classes C₁(X), ..., C₈(X), then the proposition holds.

If M does not lie in one of the classes C₁(X), ..., C₈(X), then M is a member of the class S(X) (by Aschbacher’s theorem, see [13, Theorem 1.2.1]). Let S be the socle of M. Since M lies in S, the group S is non-abelian simple. We claim that S ≤ G. In fact, S \cap G is a normal subgroup of S. Hence S \cap G = 1 or S ≤ G. For contradiction, suppose that S \cap G = 1. Thus S is isomorphic to a subgroup of X/G, a contradiction, since X/G is solvable. So we obtain the claim. In particular, if M is a member of the class S(X), then M \cap G is a member of the class S(G).

Using 2.2.9 in [12], we get that either S is in Table 13 or |M| < q^(2n+4). Assume that n is at least 8, 13, 12 and 13 in the cases L, U, S and O respectively. An easy check shows that the proposition holds.
### Table 5

| Case | Type of $M$ | $\log_q |M|_p$ | Conditions |
|------|------------|-------------|-------------|
| $L$  | $GL_m(q) \cong GL_m(q)$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $1 \leq m < \frac{n}{4}$ |
| $U$  | $GU_m(q) \cong GU_m(q)$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $1 \leq m < \frac{n}{4}$ |
| $S$  | $Sp_2(q) \cong Sp_2(q)$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $2 \leq m < \frac{n}{2}$, $m$ even |
| $O^+$ | $O_{2^k}(q) \cong O_{2^k}(q)$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $1 \leq m < n - 2$, $m$ odd |
| $O^-$ | $O_{2^k}(q) \cong O_{2^k}(q)$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $2 \leq m < n - 2$, $m$ even |

### Table 6

| Case | Type of $M$ | $\log_q |M|_p$ | Conditions |
|------|------------|-------------|-------------|
| $L$  | $GL_m(q) : S_n$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $1 \leq m < \frac{n}{4}$ |
| $U$  | $GU_m(q) : S_n$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $1 \leq m < \frac{n}{4}$ |
| $S$  | $Sp_2(q) : S_n$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $2 \leq m < \frac{n}{2}$, $m$ even |
| $O^+$ | $O_{2^k}(q) : S_n$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $1 \leq m < \frac{n}{2}$, $m$ odd |
| $O^-$ | $O_{2^k}(q) : S_n$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $2 \leq m < \frac{n}{2}$, $m$ even |

### Table 7

| Case | Type of $M$ | $\log_q |M|_p$ | Conditions |
|------|------------|-------------|-------------|
| $L$  | $GL_{n/2}(q^r) : r$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $r, n, r$ prime |
| $U$  | $GU_{n/2}(q^r) : r$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $r, n, r$ prime, $r \geq 3$ |
| $S$  | $Sp_{n/2}(q^r) : r$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $r, n, r$ prime, $n/r$ even |
| $O^+$ | $O_{n/2}(q^r) : r$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $q, n, r$ prime, $r \neq n$ |
| $O^-$ | $O_{n/2}(q^r) : r$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $q, n, r$ prime, $n/r \geq 4$, $n/r$ even |
| $O^{+\pm}$ | $O_{n/2}(q^r) : r$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $q, n, r$ prime, $n/r \geq 4$, $n/r$ even |
| $GU_{n/2}(q^r) : r$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $q, n, r$ prime, $n/r \geq 4$, $n/r$ even |

### Table 8

| Case | Type of $M$ | $\log_q |M|_p$ | Conditions |
|------|------------|-------------|-------------|
| $L$  | $GL_{n/2}(q) \cong GL_{n/2}(q)$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $n_1 n_2 = n, 2 \leq n_1 < \sqrt{n}$ |
| $U$  | $GU_{n/2}(q) \cong GU_{n/2}(q)$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $n_1 n_2 = n, 2 \leq n_1 < \sqrt{n}$ |
| $S$  | $Sp_{n/2}(q) \cong Sp_{n/2}(q)$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $n_1 n_2 = n, n_2 \geq 3$ odd, $q$ odd |
| $O^+$ | $O_{n/2}(q) \cong O_{n/2}(q)$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $n_1 n_2 = n, n_2 \geq 4$ even, $q$ odd |
| $O^-$ | $O_{n/2}(q) \cong O_{n/2}(q)$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $n_1 n_2 = n, n_2 \geq 4$ even, $q$ odd |
| $O^{+\pm}$ | $O_{n/2}(q) \cong O_{n/2}(q)$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $n_1 n_2 = n, n_1 \geq 4$, $q$ odd |
| $O^{+\pm}$ | $O_{n/2}(q) \cong O_{n/2}(q)$ | $\frac{n}{m} - \frac{n}{m} |G_0|_p$ | $n_1 n_2 = n, n_2 = n_1$ even |
The proposition holds for the maximal subgroups of $PSL_3(q)$. Case $C_5$:

| Case | Type of $M$ | $\log_2 |M|_p$ | Conditions |
|------|-------------|---------------|------------|
| L    | $GL_n(q^{1/2})$ | $\frac{m(m-1)}{2}$ | $r$ prime |
| U    | $GL_n(q^{1/2})$ | $\frac{m(m-1)}{2}$ | $r \geq 3$ prime |
|      | $Sp_n(q)$       | $\frac{n}{4}$  | $n$ even |
|      | $O^+_2(q)$      | $\frac{m(m-1)}{2}$ | $n$ even, $q$ odd |
|      | $O_n(q)$        | $\frac{(n-1)^2}{4}$ | $n$ odd, $q$ odd |
| S    | $Sp_n(q^{1/2})$ | $\frac{n}{4}$  | $r \mid n$, $r$ prime |
| O^o  | $O_n(q^{1/2})$ | $\frac{m(m-1)}{2}$ | $r \mid n$, $r$ prime |
| O^+  | $O^+_n(q^{1/2})$ | $\frac{m(m-2)}{2} + \log_2 |4|_p$ | $r \mid n$, $r$ prime |

Case $C_6$:

| Case | Type of $M$ | $|M|_p$ | Conditions |
|------|-------------|---------|------------|
| L    | $r^{2m} \cdot Sp_{2m}(r)$ | $\prod_{i=1}^m (2^i - 1)_p$ | $n = r^m$, $r$ prime, $r \neq p$, $f$ odd, $f$ minimal subject to $p^f = (mod \ 2, r)$ (**) |
|      | $3^m, Q_8$  | $2^{|m|_p}$ | (**) plus $n = 3$, $q \equiv 4, 7$ (mod 9) |
|      | $2^{m}, A_6$ | $2^{|2 \cdot 3^2 - 5|_p}$ | (**) plus $n = 4$, $q = p \equiv 5$ (mod 8) |
| U    | $r^{2m} \cdot Sp_{2m}(r)$ | $\prod_{i=1}^m (2^i - 1)_p$ | $n = r^m$, $r$ prime, $r \neq p$, $f$ even, $f$ minimal subject to $p^f = (mod \ 2, r)$ (****) |
|      | $3^m, Q_8$  | $2^{|m|_p}$ | (****) plus $n = 3$, $q \equiv 2, 5$ (mod 9) |
|      | $2^{m}, A_6$ | $2^{|2 \cdot 3^2 - 5|_p}$ | (****) plus $n = 4$, $q = p \equiv -5$ (mod 8) |
| S    | $2^{m+2n} O_{2m}^+(2)$ | $(2^{m+1}) \prod_{i=1}^m (2^i - 1)_p$ | $n = 2^m$, $q = p \geq 3$ |
| O^+  | $2^{m+2n} O_{2m}^+(2)$ | $(2^{m+1}) \prod_{i=1}^m (2^i - 1)_p$ | $n = 2^m$, $q = p \geq 3$ |

Case $C_7$:

| Case | Type of $M$ | $\log_2 |M|_p$ | Conditions |
|------|-------------|---------------|------------|
| L    | $SL_n(q) : S_1$ | $\frac{m(m-1)}{2} + \log_2 |t|_p$ | $n = m^t$, $t \geq 2$, $m \geq 3$ |
| U    | $SL_n(q) : S_1$ | $\frac{m(m-1)}{2} + \log_2 |t|_p$ | $n = m^t$, $t \geq 2$, $m \geq 3$ |
| S    | $Sp_n(q) : S_1$ | $\frac{m(m-1)}{2} + \log_2 |t|_p$ | $n = m^t$, $t \geq 3$, $q$ odd |
| O^o  | $O_n(q) : S_1$ | $\frac{m(m-2)}{2} + \log_2 |t|_p$ | $n = m^t$, $t \geq 2$ |
| O^+  | $O^+_n(q) : S_1$ | $\frac{m(m-2)}{2} + \log_2 |t|_p$ | $n = m^t$, $t \geq 2$, $q$ odd |
|      | $Sp_n(q) : S_1$ | $\frac{m(m-1)}{2} + \log_2 |t|_p$ | $n = m^t$, $t \geq 2$, $q$ even |

Case $C_8$:

| Case | Type of $M$ | $\log_2 |M|_p$ | Conditions |
|------|-------------|---------------|------------|
| L    | $Sp_n(q)$   | $\frac{n}{4}$ | $n$ even |
|      | $O_n(q)$    | $\frac{m(m-2)}{4}$ | $nq$ odd |
|      | $O^+_n(q)$  | $\frac{m(m-2)}{4}$ | $q$ odd, $n$ even |
|      | $PSU_n(q)$  | $\frac{m(m-2)}{4}$ | $q = q^2_0$ |
| S    | $O^+_n(q)$  | $\frac{m(m-2)}{4} + \log_2 |2|_p$ | $q$ even |

Assume that $n = 3$ and case $L$ or $U$ holds. By [15] and [9] we obtain Table 14, where we report the maximal subgroups of $PSL_3(q)$ and $PSU_3(q)$ in the class $S$. It is straightforward to see that the proposition holds for $n = 3$. 
Table 13
Class $S$, some groups.

| Case  | $S$   | $\log_q |\text{Aut}(S)|_p$ | Conditions          |
|-------|-------|--------------------------|---------------------|
| L     | $\text{Alt}_c$ | $\log_q |\mathfrak{cl}|_p$ | $c \in \{n + 1, n + 2\}$, $n \geq 5$ |
| PSL$_2(q)$ | $n + \log_q |2f|_p$ | $n = \frac{q^{2d}-1}{2}$ |
| $\text{PGL}_2(q)$ | $40 + \log_q |2f|_p$ | $n = 16$ |
| $\text{E}_6(q)$ | $36 + \log_q |2f|_p$ | $n = 27$ |
| $M_{24}$ | 10 | $(n, q) = (11, 2)$ |
| U     | $\text{Alt}_c$ | $\log_q |\mathfrak{cl}|_p$ | $c \in \{n + 1, n + 2\}$, $n \geq 5$ |
| S     | $\text{Alt}_c$ | $\log_q |\mathfrak{cl}|_p$ | $c \in \{n + 1, n + 2\}$ |
| $E_7(q)$ | $63 + \log_q |f|_p$ | $n = 56$, $q$ odd |
| $O^{+}$ | $\text{Alt}_c$ | $\log_q |\mathfrak{cl}|_p$ | $c \in \{n + 1, n + 2\}$ |
| $O^{-}$ | $\text{PSL}_2(q)$ | $9 + \log_q |f|_p$ | $n = 8$ |
| $O^{+}$ | $\text{PGL}_2(q)$ | $16 + \log_q |f|_p$ | $n = 16$ |
| $O^{-}$ | $E_7(q)$ | $63 + \log_q |f|_p$ | $n = 56$ |
| $CO_1$ | 21 | $(n, q) = (24, 2)$ |

Table 14
Subgroup $M$ of PSL$_3(q)$ in the class $S$.

| $M$     | $\log_q |M|_p$ | Conditions          |
|---------|----------------|---------------------|
| PSL$_2(7)$ | $2^3 \cdot 3 \cdot 7$ | $p \neq 2$, $q^3 \equiv 1 \pmod{7}$ |
| $\text{Alt}_6$ | $2^3 \cdot 3^2 \cdot 5$ | $q = 4$; if $p \neq 2$, then $f$ even and $p \neq 3$, or $f$ odd and $p \equiv 1, 4 \pmod{15}$ |
| $\text{Alt}_6.2$ | $2^4 \cdot 3^2 \cdot 13$ | $p = 5$, $f$ even |
| $\text{Alt}_7$ | $2^4 \cdot 3^2 \cdot 5 \cdot 7$ | $p = 5$, $f$ even |
| $\text{PSL}_2(7)$ | $3^7 \cdot 13$ | $p^3 \equiv -1 \pmod{7}$ and $q = p \neq 5$ |
| $\text{Alt}_6$ | $q = p = 11, 14 \pmod{15}$ |
| $\text{Alt}_6.2$ | $q = 5$ |
| $\text{Alt}_7$ | $q = 5$ |

Throughout the rest of the proof, assume that if case L or U holds, then $n \geq 4$. Using [18], it is easy to see that the proposition holds in the following cases:

- Case L, $(n, q) \in \{(4, 2), (5, 2)\}$.
- Case U, $(n, q) \in \{(4, 2), (5, 2)\}$.
- Case S, $(n, q) \in \{(4, 3), (4, 4), (6, 2), (8, 2)\}$.
- Case O, $(n, q) = (7, 3)$.
- Case $O^+$, $(n, q) = (8, 2)$.
- Case $O^-$, $(n, q) = (8, 2)$.

Recall the definition of the class $S$. In particular, if $M$ lies in $S$, then there exists an absolutely irreducible representation $\rho : L \to \text{GL}(V)$ such that $\rho(L) = S$, where $L$ is the full covering of $S$.

As in [13, §5.3], for a finite group $S$ and a prime number $r$, let $R_r(S) = \min\{m : L$ has a non-trivial projective representation of degree $m$ in characteristic $r\}$. Moreover, let $\overline{R}_r(S) = \min\{R_r(S) : r$ is a prime number, $r \neq p\}$ and $R(S) = \min\{R_r(S) : r$ is a prime number\}. In particular, we are concerned with the simple groups $S$ such that $R(S) \leq 12$. We report these groups in Tables 15, 16 and 17, using the result of [13, Proposition 5.3.7, Proposition 5.3.8, Theorem 5.3.9 and Proposition 5.4.13].

Suppose that $S$ is not a group of Lie type of characteristic $p$. Using Tables 15 and 16, we find a lower bound of $|X : M|_p$ (the ratio $|G|_p/|\text{Aut}(S)|_p$). It turns out that this lower bound is smaller than $q^d_\rho(X)$ in the following cases:

- Case L, $(n, q) \in \{(4, 2), (5, 2)\}$.
- Case U, $(n, q) \in \{(4, 2), (5, 2)\}$.
Moreover, by definition of the class $M$, $\rho$ belongs to one of the following:

- Case $S$, $(n, q) \in \{(4, 4), (6, 2)\}$.
- Case $O^\pm$, $(n, q) \in \{(8, 2)\}$.

Note that the cases above have been already considered.

Assume that $S$ is a group of Lie type of characteristic $p$ over $\mathbb{F}_r$. Let $\overline{\mathbb{F}}_p$ denote the algebraic closure of $\mathbb{F}_p$. Since $\rho$ is absolutely irreducible, we can think to $V$ as an irreducible projective $\overline{\mathbb{F}}_p S$-module. Moreover, by definition of the class $S$, we have that $V$ cannot be realized over a proper subfield of $\mathbb{F}$. Under these assumptions, by [13, Proposition 5.4.6 and Remark 5.4.7], there exist an integer $k$ and an irreducible projective $\overline{\mathbb{F}}_p S$-module of dimension $r$ such that one of the following holds:

### Table 15
Alternating and sporadic simple groups with $R(S) \leq 12$.

| $S$ | $|\text{Aut}(S)|$ | $R(S)$ |
|-----|-----------------|--------|
| $\text{Alt}_3$ | $2^3 \cdot 3 \cdot 5$ | 2 |
| $\text{Alt}_4$ | $2^3 \cdot 3^2 \cdot 5$ | 2 |
| $\text{Alt}_5$ | $2^4 \cdot 3^2 \cdot 5 \cdot 7$ | 3 |
| $\text{Alt}_6$ | $2^4 \cdot 3^2 \cdot 5 \cdot 7$ | 4 |
| $\text{Alt}_7$ | $2^7 \cdot 3 \cdot 5 \cdot 7$ | 7 |
| $\text{Alt}_{10}$ | $2^8 \cdot 3^4 \cdot 5^2 \cdot 7$ | 8 |
| $\text{Alt}_{11}$ | $2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11$ | 9 |
| $\text{Alt}_{12}$ | $2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11$ | 10 |
| $\text{Alt}_{13}$ | $2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$ | 11 |
| $\text{Alt}_{14}$ | $2^{11} \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$ | 12 |
| $\text{M}_{11}$ | $2^4 \cdot 3^2 \cdot 5 \cdot 11$ | $\geq 5$ |
| $\text{M}_{12}$ | $2^5 \cdot 3^3 \cdot 5 \cdot 11$ | $\geq 6$ |
| $\text{M}_{22}$ | $2^8 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$ | $\geq 6$ |
| $\text{M}_{23}$ | $2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ | $\geq 11$ |
| $\text{M}_{24}$ | $2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ | $\geq 11$ |
| $J_1$ | $2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$ | $\geq 7$ |
| $J_2$ | $2^8 \cdot 3^3 \cdot 5^2 \cdot 7$ | $\geq 6$ |
| $J_3$ | $2^8 \cdot 3^3 \cdot 5 \cdot 17 \cdot 19$ | $\geq 9$ |
| $\text{Suz}$ | $2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$ | $\geq 12$ |

### Table 16
Simple groups of Lie type of characteristic $r$ with $R_r(S) \leq 7$, such that $S$ does not appear in Table 15.

| $S$ | $|\text{Aut}(S)|$ | Lower bound for $R_r(S)$ |
|-----|-----------------|--------------------------|
| $\text{PSL}_3(2)$ | $2^4 \cdot 3 \cdot 7$ | 2 |
| $\text{PSL}_2(7)$ | $2^4 \cdot 3 \cdot 7$ | 3 |
| $\text{PSL}_3(4)$ | $2^8 \cdot 3^2 \cdot 5 \cdot 7$ | 4 |
| $\text{PSU}_4(2)$ | $2^7 \cdot 3^4 \cdot 5$ | 4 |
| $\text{PSp}_4(3)$ | $2^7 \cdot 3^4 \cdot 5$ | 4 |
| $\text{PSL}_2(11)$ | $2^3 \cdot 3 \cdot 5 \cdot 11$ | 5 |
| $\text{PSL}_3(13)$ | $2^3 \cdot 3 \cdot 7 \cdot 13$ | 6 |
| $\text{PSU}_3(3)$ | $2^6 \cdot 3^3 \cdot 7$ | 6 |
| $\text{PSU}_3(3)$ | $2^{10} \cdot 3^3 \cdot 5 \cdot 7$ | 6 |
| $\text{PSL}_2(8)$ | $2^3 \cdot 3^7$ | 7 |
| $\text{PSp}_4(2)$ | $2^9 \cdot 3^4 \cdot 5 \cdot 7$ | 7 |
| $\text{PG}_2^\ast (2)$ | $2^{13} \cdot 3^6 \cdot 5^2 \cdot 7$ | 8 |
| $2\text{B}_2(8)$ | $2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ | 8 |
| $\text{PSL}_2(17)$ | $2^5 \cdot 3^2 \cdot 17$ | 8 |
| $\text{PSL}_3(3)$ | $2^5 \cdot 3^3 \cdot 13$ | 8 |
| $\text{PSL}_2(19)$ | $2^3 \cdot 3^2 \cdot 5 \cdot 19$ | 9 |
| $\text{PSU}_4(2)$ | $2^{11} \cdot 3^4 \cdot 5 \cdot 31$ | 10 |
| $\text{PSL}_2(23)$ | $2^9 \cdot 3 \cdot 11 \cdot 23$ | 11 |
| $\text{PSL}_2(25)$ | $2^3 \cdot 3 \cdot 5 \cdot 13$ | 12 |
| $\text{PSp}_4(5)$ | $2^7 \cdot 3^2 \cdot 5^4 \cdot 13$ | 12 |
| $\text{G}_2(4)$ | $2^{14} \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$ | 12 |
Table 17
Simple groups of Lie type of characteristic $p$ with $R_p(S) \leq 12$.

| $S$         | $\log_q |\text{Aut}(S)\rangle_p$ | $R_p(S)$ | Conditions          |
|------------|-------------------------------|----------|---------------------|
| $\text{PSL}_2(q)$ | $1 + \log_q |f\rangle_p$ | 2        |                     |
| $\text{PSL}_3(q)$ | $\frac{1}{2} + \log_q |2f\rangle_p$ | 3        | $l \leq 12$         |
| $\text{PSL}_4(q)$ | $4 + \log_q |2f\rangle_p$ | 4        |                     |
| $\text{PSp}_4(q)$ | $\frac{1}{2} + \log_q |f\rangle_p$ | 6        |                     |
| $\text{PG}_2(q)$ | $\frac{1}{2} + \log_q |2f\rangle_p$ | 8        | $l \in \{6, 8, 10, 12\}$ |
| $\text{PG}_2^+(q)$ | $\frac{1}{2} + \log_q |2f\rangle_p$ | 8        | $l \in \{10, 12\}$  |
| $\text{PSp}_4^+(q)$ | $3 + \log_q |2f\rangle_p$ | 8        | $p = 3, f \geq 3, f$ odd |
| $\text{PG}_2^+(q)$ | $12 + \log_q |3f\rangle_p$ | 12       |                     |

Table 18
Dimension $t$ of the irreducible projective $\mathbb{F}_qS$ modules with $t \leq 12$, $S$ group of Lie type of characteristic $p$.

<table>
<thead>
<tr>
<th>$S$</th>
<th>Values of $t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{PSL}_2(q)$</td>
<td>some $t \geq 2$</td>
</tr>
<tr>
<td>$\text{PSL}_3(q)$</td>
<td>3 and some $t \geq 6$</td>
</tr>
<tr>
<td>$\text{PSL}_4(q)$</td>
<td>4, 6 and some $t \geq 10$</td>
</tr>
<tr>
<td>$\text{PSL}_5(q)$</td>
<td>5, 10</td>
</tr>
<tr>
<td>$\text{PSL}_6(q), 6 \leq l \leq 12$</td>
<td>$l$</td>
</tr>
<tr>
<td>$\text{PSU}_3(q)$</td>
<td>3 and some $t \geq 6$</td>
</tr>
<tr>
<td>$\text{PSU}_4(q)$</td>
<td>4, 6 and some $t \geq 10$</td>
</tr>
<tr>
<td>$\text{PSU}_5(q)$</td>
<td>5, 10</td>
</tr>
<tr>
<td>$\text{PSU}_6(q), 6 \leq l \leq 12$</td>
<td>$l$</td>
</tr>
<tr>
<td>$\text{PSp}_4(q)$</td>
<td>4, 5 $- \delta_{p,2}$ and some $t \geq 9$</td>
</tr>
<tr>
<td>$\text{PSp}_4^+(q)$</td>
<td>6, 8 (q even)</td>
</tr>
<tr>
<td>$\text{PSp}_5(q), l \in {8, 10, 12}$</td>
<td>$l$</td>
</tr>
<tr>
<td>$\text{PSp}_6(q)$</td>
<td>7, 8</td>
</tr>
<tr>
<td>$\text{PG}_2(q), l \in {9, 11}$</td>
<td>$l$</td>
</tr>
<tr>
<td>$\text{PG}_2^+(q), l \in {8, 10, 12}$</td>
<td>$l$</td>
</tr>
<tr>
<td>$\text{PSp}_6^+(q)$</td>
<td>7</td>
</tr>
<tr>
<td>$\text{PSp}_6^+(q)$</td>
<td>some $t \geq 8$</td>
</tr>
<tr>
<td>$\text{PSp}_4(q)$</td>
<td>some $t \geq 4$</td>
</tr>
</tbody>
</table>

- $r = q^{uk}$ and $\dim(V) = n = t^k$;
- $S$ is of type $2A_1, 2D_2, 2E_6$, $r = q^{uk/2}$, $k$ is odd and $n = t^k$;
- $S$ is of type $3D_4$, $r = q^{uk/3}$, $3 \nmid k$ and $n = t^k$;
- $S$ is of type $2B_2, 2G_2, 2F_4$, $r = q^{uk}$ and $n \geq t^k$.

Again, using Tables 17 and 18, we find that the lower bound of $|X : M|_p$ (the ratio $|G|_p/|\text{Aut}(S)|_p$) is greater that or equal to $q^{\delta_p(X)}$. In particular, when case $O^0$ holds for $n = 7$ we have that if there exists a maximal subgroup $M$ in $S$ with socle isomorphic to $G_2(q)$, then $M = S$. Similarly, when case $O^\pm$ holds for $n = 8$, we have that if there exists a maximal subgroup $M$ in $S$ with socle $S$ isomorphic to $\text{PSp}_6(q)$ or $\text{PG}_2(q)$, then $M = S$. The proof is finished. □

8. On the intersection of maximal subgroups which contain a Sylow $p$-subgroup of $X$

Let $X$ be a projective classical group, as in Section 6. The aim of this section is to prove the following.
Theorem 20. Under the notation of Section 6, let \( H \) be a subgroup of \( X \) such that:

- \( HG = X \),
- if \( M \) is a maximal subgroup of \( X \) and \( M \supseteq H \), then \( M \) contains a Sylow \( p \)-subgroup of \( X \),
- \( H \) does not contain a Sylow \( p \)-subgroup of \( X \).

Then \( \mu_X(H) = 0 \) or \( |X : H|_p \geq q^\beta(n) \), where

\[
\beta(n) = \begin{cases} 
  n - 1 & \text{if case L or U holds,} \\
  \frac{n}{2} - \log_q |2|_p & \text{if case S holds,} \\
  \frac{n}{2} - 1 & \text{if case O^0 holds,} \\
  \frac{n}{2} - 2 & \text{if case O^+ or O^- holds.}
\end{cases}
\]

In order to prove the above theorem, we investigate the structure of maximal subgroups in the class \( C_1(X) \), as described in [13]. In particular, we are interested to the maximal subgroups which contain a Sylow \( p \)-subgroup of \( X \). In most cases, these subgroups are stabilizers of totally singular subspaces of \( V \).

We recall some definitions about the geometry of classical groups (see [13, p. 16]). Let \( W \) be a subspace of \( V \). We say that \( W \) is totally singular if the restriction \( \kappa_W \) of \( \kappa \) to \( W \) is equal to 0. We say that \( W \) is non-degenerate if \( \kappa_W \) is non-degenerate. Writing \((v, w)\) instead of \( f(v, w)\), we denote by \( W^\perp \) the set of \( v \in V \) such that \((v, w) = 0\) for all \( w \in W \).

We need some preliminary technical lemmas.

Lemma 21. (See [13, Propositions 2.3.2, 2.4.1 and 2.5.3].) The space \((V, \kappa)\) has a basis:

- \( \{e_1, \ldots, e_m\} \) if \( n = m \) and case L holds,
- \( \{e_1, \ldots, e_m, f_1, \ldots, f_m\} \) if \( n = 2m \) and cases U, O^+ or S hold,
- \( \{e_1, \ldots, e_m, f_1, \ldots, f_m, x\} \) if \( n = 2m + 1 \) and cases U or O^0 hold,
- \( \{e_1, \ldots, e_m, f_1, \ldots, f_m, y, z\} \) if \( n = 2m + 2 \) and case O^- holds.

In all these cases we have \((e_i, e_j) = (f_i, f_j) = (e_i, x) = (f_i, x) = (e_i, y) = (f_i, y) = (e_i, z) = (f_i, z) = 0 \) and \((e_i, f_j) = \delta_{ij} \) for all \( i, j \). Moreover,

- if case O holds, then \( Q(e_i) = Q(f_i) = 0 \),
- if case U holds, then \( (x, x) = 1 \),
- if case O^0 holds, then \( x \) is non-singular,
- if case O^- holds, then \( Q(y) = 1 \), \( Q(z) = \zeta \) and \((y, z) = 1\), where the polynomial \( X^2 + X + \zeta \) is irreducible over \( \mathbb{F} \).

Lemma 22. Let \( m \) be as in Lemma 21. Let \( l \) and \( h \) be two distinct integer numbers such that \( 1 \leq l, h \leq m \). There exists an element \( \phi_{l,h} \in G \) such that:

1. each subspace of \( \langle e_1, \ldots, e_{l-1} \rangle \) is stabilized by \( \phi_{l,h} \),
2. each totally singular subspace of \( V \) containing \( \langle e_h \rangle \) is stabilized by \( \phi_{l,h} \),
3. \( \phi_{l,h} \) does not stabilizes a subspace of \( V \) containing \( \langle e_l \rangle \) and not containing \( \langle e_h \rangle \).

Proof. Define a linear map \( \phi = \phi_{l,h} : V \to V \) as follows:

- \( \phi(e_i) = e_i + e_h \) and \( \phi(e_i) = e_i \) for \( i \neq l \),
- \( \phi(f_h) = f_h - f_l \) and \( \phi(f_i) = f_i \) for \( i \neq h \),
- \( \phi(x) = x, \phi(y) = y \) and \( \phi(z) = z \) (when they occur).
Note that \( \det(\phi) = 1 \) and \( \kappa(\phi(v)) = \kappa(v) \) for \( v \in V^e \), where \( e = 1 \) if case \( \text{O} \) holds, \( e = 2 \) otherwise. Thus \( (S(V, \kappa) \cap \mathbb{R}^+)\phi \) is an element of \( S(V, \kappa) \). Moreover, if case \( \text{O} \) holds, then it is easy to see that \( (S(V, \kappa) \cap \mathbb{R}^+)\phi \) is a commutator in \( S(V, \kappa) \). Thus we let \( \phi_{i, h} = (S(V, \kappa) \cap \mathbb{R}^+)\phi \in G \). It is straightforward to show that (1) and (3) hold, so we prove only (2). Let \( U \) be a totally singular subspace of \( V \) such that \( e_h \in U \). Let \( w \) be an element of \( U \). Thus \( w = \sum_{i=1}^{m} \alpha_i e_i + \sum_{i=1}^{n} \beta_i f_i + \gamma x + \gamma_1 y + \gamma_2 z \), for some \( \alpha_i, \beta_i, \gamma, \gamma_1, \gamma_2 \in \mathbb{R}_q \). Since \( U \) is totally singular, we have that \( (w, e_h) = 0 \), thus \( \beta_h = 0 \). Hence \( \phi_{i, h}(w) = \alpha_i e_h + w \), so \( \phi_{i, h}(w) \in U \) since \( e_h \in U \). □

The following well-known facts about the spaces with forms will be use often without mention.

Lemma 23. Let \( \kappa \) be a non-degenerate form and let \( W \) and \( U \) be two subspaces of \( V \).

1. \( W \subseteq U \) if and only if \( U^+ \subseteq W^+ \).
2. \( (W + U)^+ = W^+ \cap U^+ \).
3. If \( W \) is totally singular, then \( W \subseteq W^+ \).
4. If \( W \) is totally singular and \( U \subseteq W^+ \), then \( U + W \) is totally singular.
5. \( W \) is non-degenerate if and only if \( W \cap W^+ = 0 \).

We introduce some definitions and notation. Assume that \( H \) is as in Theorem 20. Let \( \mathcal{M}_H(X) \) be the set of maximal subgroups \( M \) of \( X \) containing \( H \) and such that \( MG = X \). We denote by \( \mathcal{L}_H(X) \) the set

\[ \{ W \subseteq V : \text{Stab}_X(W) \supseteq H \} \]

and we let \( \mathcal{L}_H^+(X) = \{ W \in \mathcal{L}_H(X) : W \text{ is totally singular and } W \not\in \{0, V\} \} \). It is clear that \( \mathcal{L}_H^+(X) \subseteq \mathcal{L}_G^+(H) \). Moreover, we have the following.

Proposition 24. (See [13, §4.1.]) Suppose that case \( \text{O}^+ \) does not hold. The map

\[ \text{Stab}_X : \mathcal{L}_H^+(X) \to \mathcal{M}_H(X) \]

gives a one-to-one correspondence between \( \mathcal{L}_H^+(X) \) and \( \mathcal{M}_H(X) \).

Now we turn to the case \( \text{O}^+ \). Recall the notation for \( U_m \) from p. 52. We have the following.

Proposition 25. (See [13, Proposition 4.1.20 and Lemma 2.5.8].) Suppose that case \( \text{O}^+ \) holds. The map

\[ \text{Stab}_X : \mathcal{L}_H^+(X) - U_{m-1} \to \mathcal{M}_H(X) \]

is a one-to-one correspondence.

Now, we focus our attention to the set \( \mathcal{L}_H(X) \). Observe that \( \mathcal{L}_H(X) \) is a sublattice of the lattice of subspace of \( V \). In fact if \( U \) and \( W \) are subspaces of \( V \), then \( \text{Stab}_X(U) \cap \text{Stab}_X(W) \leq \text{Stab}_X(U + W) \cap \text{Stab}_X(U \cap W) \).

In general, the set \( \mathcal{L}_H^+(X) \) is not a lattice. However, if \( Z_1, Z_2 \in \mathcal{L}_H^+(X) \), then

- \( Z_1 \cap Z_2 \in \mathcal{L}_H^+(X) \) if and only if \( Z_1 \cap Z_2 > 0 \);
- \( Z_1 + Z_2 \in \mathcal{L}_H^+(X) \) if and only if there exists a totally singular proper subspace \( T \) of \( V \) such that \( Z_1, Z_2 \leq T \).
Let $\mathcal{L}$ be a subset of the set of vector subspaces of $V$.

- We denote by $\mathcal{L}(+)\mathcal{L}(\cap)$ the subset of $\mathcal{L}$ consisting of the elements $W$ such that there exist $Z_1, Z_2 \in \mathcal{L}$, with $Z_1 \neq W \neq Z_2$ and $W = Z_1 + Z_2$. Similarly, define $\mathcal{L}(\cap)$ as the subset of $\mathcal{L}$ consisting of the elements $W$ such that there exist $Z_1, Z_2 \in \mathcal{L}$, with $Z_1 \neq W \neq Z_2$ and $W = Z_1 \cap Z_2$.

- An element $W$ of $\mathcal{L}$ is said to be redundant in $\mathcal{L}$ if for every $M \subseteq \mathcal{L}$ such that $W \in M$ and $\bigcap_{U \in M} \text{Stab}_X(U) = \bigcap_{U \in \mathcal{L}} \text{Stab}_X(U)$, we have that $\bigcap_{U \in M \setminus \{W\}} \text{Stab}_X(U) = \bigcap_{U \in \mathcal{L}} \text{Stab}_X(U)$.

- We say that $\mathcal{L}$ enjoys the property $\mathcal{P}$ if there exists $W \in \mathcal{L}$ such that for each $Z \in \mathcal{L}$ we have $W \leq Z$ or $W \geq Z$. In this case, $W$ is said to be a $\mathcal{P}$-element of $\mathcal{L}$.

We divide the rest of the section into two parts: $\mathcal{L}_H^{*}(X)$ enjoys the property $\mathcal{P}$ and $\mathcal{L}_H^{*}(X)$ does not enjoy the property $\mathcal{P}$.

\section*{$\mathcal{L}_H^{*}(X)$ enjoys the property $\mathcal{P}$}

We consider the case when $\mathcal{L}_H^{*} = \mathcal{L}_H^{*}(X)$ enjoys the property $\mathcal{P}$. Our aim is to prove the following.

\textbf{Proposition 26.} Let $H$ be as in Theorem 20. Suppose that $\mathcal{L}_H^{*}$ enjoys the property $\mathcal{P}$. Then $\mu_X(H) = 0$.

The proof of this proposition requires some preliminary results.

\textbf{Proposition 27.} Let $H$ be as in Theorem 20 and assume that $H$ is an intersection of maximal subgroups of $X$. Suppose that $W$ is a $\mathcal{P}$-element of $\mathcal{L}_H^{*}$ such that $W \in \mathcal{L}_H^{*}(+) \cup \mathcal{L}_H^{*}(\cap)$. If $W \in \mathcal{L}_H^{*}(+)$ or $\mathcal{L}_H^{*}(+)$ does not contain $\mathcal{P}$-elements of $\mathcal{L}_H^{*}$, then $W$ is redundant in $\mathcal{L}_H^{*}$.

\textbf{Proof.} Suppose that $M$ is a subset of $\mathcal{L}_H^{*}$ such that $W \in M$ and $\bigcap_{U \in M} \text{Stab}_X(U) = \bigcap_{U \in \mathcal{L}_H^{*}} \text{Stab}_X(U)$.

Note that $\bigcap_{U \in \mathcal{L}_H^{*}} \text{Stab}_X(U) = H$

by Propositions 24 and 25.

For a contradiction, assume that $K = \bigcap_{U \in M \setminus \{W\}} \text{Stab}_X(U) > H$.

Note that $M \setminus \{W\} \subseteq \mathcal{L}_K^{*} \subset \mathcal{L}_H^{*}$ and $W$ does not lie in $\mathcal{L}_K^{*}$. Moreover, $W$ does not lie in the lattice $\mathcal{L}_K$. 

Assume \( W \in \mathcal{L}^*_H(+) \). Let \( T \) be the sum of the elements of \( \mathcal{L}^*_K \) which are contained in \( W \), i.e.

\[
T = \sum_{U \in \mathcal{L}^*_K, U \subseteq W} U
\]

(if for each \( U \in \mathcal{L}^*_K \) we have \( U \supseteq W \), then let \( T = 0 \)). Clearly \( T \subseteq W \) and since \( W \not\in \mathcal{L}^*_K \), then \( T < W \). Since \( W \) is a \( \mathcal{P} \)-element, note that

\[
\text{if } U \in \mathcal{L}^*_K, \text{ then } U \subseteq T \text{ or } U > W. 
\]  

(\( \dagger \))

We claim that there exists an element

\[
Y \in \mathcal{L}^*_H - \mathcal{L}^*_K, \text{ such that } Y < W \text{ and } Y \not\subseteq T.
\]

(\( \dagger \dagger \))

Since \( W \in \mathcal{L}^*_H(+) \), there exist \( Z_1, Z_2 \in \mathcal{L}^*_H \) such that \( Z_1 \neq W \neq Z_2 \) and \( Z_1 + Z_2 = W \). Since \( W \not\in \mathcal{L}^*_K \), we have that \( Z_1 \not\in \mathcal{L}^*_K \) or \( Z_2 \not\in \mathcal{L}^*_K \). Suppose that \( Z_1, Z_2 \not\in \mathcal{L}^*_K \). We have that \( T \not\supseteq Z_1 \) or \( T \not\supseteq Z_2 \), otherwise \( T \supseteq Z_1 + Z_2 = W \). So, in the case that \( Z_1, Z_2 \not\in \mathcal{L}^*_K \), let \( Y \in \{ Z_1, Z_2 \} \) be such that \( Y \not\subseteq T \). Now, suppose that \( Z_i \in \mathcal{L}^*_K \). Thus \( Z_{2-i} \notin \mathcal{L}^*_K \) and so \( T \not\supseteq Z_{2-i} \), otherwise \( T = T + Z_i \supseteq Z_{2-i} + Z_i = W \). Hence, in the case that \( Z_i \in \mathcal{L}^*_K \), set \( Y = Z_{2-i} \).

Since \( W \) is totally singular, by Witt’s Lemma [13, Proposition 2.1.6] we may assume that there exists \( k \geq 2 \) such that \( W \) has a basis \( e_1, \ldots, e_k \) which is part of the standard basis given in Lemma 21. Moreover, by (\( \dagger \dagger \)) and \( T < W \), we may assume that there exist \( 0 \leq h \leq l < r \leq k \) such that \( T \cap Y = \langle e_1, \ldots, e_h \rangle, T = T \cap Y \oplus \langle e_{l+1}, \ldots, e_r \rangle \) and \( k - r + l - h \geq 1 \). Define an element \( \phi \in G \) as follows (see Lemma 22):

- if \( l > h \) (i.e. \( T \cap Y < T \)), then let \( \phi = \phi_{l+1} \);
- if \( l = h \) (i.e. \( T \subseteq Y \), so \( Y = T + Y < W \)), then let \( \phi = \phi_{l+1,r+1} \).

By Lemma 22, (\( \dagger \)) and (\( \dagger \dagger \)), we have that

\[
\phi \in \bigcap_{U \in \mathcal{L}^*_K} \text{Stab}_X(U) \cap \text{Stab}_X(W) = H
\]

and \( \phi \notin \text{Stab}_X(Y) \). This is in contradiction with \( Y \in \mathcal{L}^*_H \).

Assume that \( \mathcal{L}^*_H(+) \) does not contain \( \mathcal{P} \)-elements of \( \mathcal{L}^*_H \). This implies that \( W \in \mathcal{L}^*_H(\cap) \). If case \( \mathcal{L} \) holds, then the proof is just the dual of the above case. So we assume that case \( \mathcal{L} \) does not hold, so \( \kappa \) is a non-degenerate form.

Since \( \mathcal{L}^*_H(+) \) does not contain \( \mathcal{P} \)-elements, we have that the elements of the set \( \mathcal{N} = \{ U \leq W : U \in \mathcal{L}^*_H \} \) form a chain of subspaces of \( V \). In fact, for a contradiction suppose that the set \( \mathcal{N} \) is not a chain. Thus there exist two elements \( U_1, U_2 \in \mathcal{N} \) such that \( U_1 \not\subseteq U_2 \) and \( U_2 \not\subseteq U_1 \). Since \( U_1, U_2 \leq W \), we get that \( U_1 + U_2 \) is totally singular, hence \( U_1 + U_2 \in \mathcal{N} \). So \( \mathcal{N}(+) \neq \emptyset \). Let \( A \) be a maximal element in \( \mathcal{N}(+) \). It is straightforward to see that \( A \) is a \( \mathcal{P} \)-element of \( \mathcal{N} \), hence it is a \( \mathcal{P} \)-element of \( \mathcal{L}^*_H \), a contradiction. So, we have that \( \mathcal{N} = \{ U \leq W : U \in \mathcal{L}^*_H \} \) form a chain of subspaces of \( V \).

Note that if the elements of \( \mathcal{L}^*_K \) form a chain of subspaces of \( V \), then

\[
\bigcap_{U \in \mathcal{L}^*_K \cup \{ W \}} \text{Stab}_G(U) = H \cap G
\]

contains a Sylow \( p \)-subgroup of \( G \) (see [13, Corollary 4.1.15]). Hence \( H \) contains a Sylow \( p \)-subgroup of \( X \), against the assumptions. We deduce that the set \( \{ U \supseteq W : U \in \mathcal{L}^*_K \} \) is not empty and it is not a
chain. Let $T$ be the intersection of the elements of $\mathcal{L}_K^*$ that contain $W$, i.e.

$$T = \bigcap_{U \in \mathcal{L}_K^*, U \supseteq W} U.$$ 

We have that $T \supseteq W$ and since $W \not\in \mathcal{L}_K^*$, then $T > W$. Moreover, since $W$ is a $\mathcal{P}$-element,

$$\text{if } U \in \mathcal{L}_K^*, \text{ then } U \supseteq T \text{ or } U < W. \quad (\dagger^3)$$

Arguing as for $(\dagger^3)$, there exists an element $Y$ in $\mathcal{L}_K^* - \mathcal{L}_K^+$, such that $Y > W$ and $Y \not\supseteq T$. \( (\dagger^4) \)

We divide the rest of the proof in three cases, namely case $Y \cap T > W$, case $Y \cap T = W$ and $Y \cap T^\perp \not\supseteq T$, case $Y \cap T = W$ and $Y \cap T^\perp \supseteq T$.

Suppose that $Y \cap T > W$. As above, since $T$ is totally singular, we may assume that there exists $k \geq 2$ such that $T$ has a basis $e_1, \ldots, e_k$ which is part of the standard basis given in Lemma 21. Moreover, by $(\dagger^4)$ we may assume that there exists $0 < h < l < k$ such that $W = \langle e_1, \ldots, e_h \rangle$ and $Y \cap T = \langle e_1, \ldots, e_l \rangle$. Let $\phi = \phi_{h+1,l+1}$ as in Lemma 22. By Lemma 22, $(\dagger^3)$ and $(\dagger^4)$, we have that

$$\phi \in \bigcap_{U \in \mathcal{L}_K^*} \text{Stab}_X(U) \cap \text{Stab}_X(W) = H$$

and $\phi \not\in \text{Stab}_Y(Y)$. This is in contradiction with $Y \in \mathcal{L}_K^*$.

Suppose that $Y \cap T = W$ and $Y \cap T^\perp \not\supseteq T$. Thus pick an element $v$ in $Y \cap T^\perp - T$. Note that $T + \langle v \rangle$ is a totally singular subspace of $V$. As above, we may assume that there exists $k \geq 2$ such that $T$ has a basis $e_1, \ldots, e_k$ and $v = e_k$. Moreover, by $(\dagger^4)$ and $T > W$, we may assume that there exists $0 < l < k - 1$ such that $W = \langle e_1, \ldots, e_l \rangle$. Let $\phi = \phi_{k,k-1}$ as in Lemma 22. By Lemma 22, $(\dagger^3)$ and $(\dagger^4)$, we have that

$$\phi \in \bigcap_{U \in \mathcal{L}_K^*} \text{Stab}_X(U) \cap \text{Stab}_X(W) = H$$

and $\phi \not\in \text{Stab}_Y(Y)$. This is in contradiction with $Y \in \mathcal{L}_K^*$.

Finally, assume that $Y \cap T = W$ and $Y \cap T^\perp \supseteq T$. Since in this case $Y \not\subseteq T^\perp$, we have that $T \not\subseteq Y^\perp$, so $T \cap Y^\perp < T$. Since $T \cap Y^\perp \in \mathcal{L}_K^* - \mathcal{L}_K^+$, if $T \cap Y^\perp > W$, then we argue as in the case $Y \cap T > W$ with $T \cap Y^\perp$ instead of $Y$. Thus we can assume that $T \cap Y^\perp = W$. Now, since $\kappa$ is non-degenerate, $T \cap Y^\perp = W$ implies $T^\perp + Y = W^\perp$. Let $M$ be a maximal totally singular subspace of $V$ containing $T$. Since $\mathcal{L}_K^*$ is not a chain, then $M > T$. Since $M$ is totally singular, we may assume that $M$ has a basis $e_1, \ldots, e_m$ which is part of the standard basis given in Lemma 21. Moreover, we may assume that there exists $0 < l < k < m$ such that $W = \langle e_1, \ldots, e_l \rangle$ and $T = \langle e_1, \ldots, e_k \rangle$. Let $\phi = \phi_{m,k}$ as in Lemma 22. By Lemma 22 and $(\dagger^3)$, we have that

$$\phi \in \bigcap_{U \in \mathcal{L}_K^*} \text{Stab}_X(U) \cap \text{Stab}_X(W) = H.$$

Since $Y \in \mathcal{L}_K^*$, we have that $\phi$ stabilizes $Y$. Note that $f_k \in W^\perp = T^\perp + Y$ and $(v, e_k) = 0$ for each $v \in T^\perp$. Thus there exist $v_1 \in Y$ and $v_2 \in T^\perp$ such that $v_1 + v_2 = f_k$, with $v_1 = \sum_{i=1}^{m} \alpha_i e_i + \sum_{i=1}^{m} \beta_i f_i + \gamma_1 x + \gamma_2 y + \gamma_2 z$ and $\beta_k \neq 0$. This yields $\phi(v_1) - v_1 = \alpha_m e_k - \beta_k f_m$. Thus we have $\alpha_m e_k - \beta_k f_m \in Y \cap T^\perp \subseteq T$, a contradiction since $\beta_k \neq 0$. Hence we obtain $\phi \not\in \text{Stab}_X(Y)$, a contradiction. \( \square \)
Lemma 28. Assume that the elements of $\mathcal{L}^* = \mathcal{L}^*_H(X)$ do not form a chain of subspaces of $V$. Suppose that $\mathcal{L}^*$ enjoys the property $\mathcal{P}$. Then there exists a redundant element in $\mathcal{L}^*$.

Proof. Let $T$ be a $\mathcal{P}$-element in $\mathcal{L}^*$. Since $\mathcal{L}^*$ is not a chain, there exist $U_1, U_2 \in \mathcal{L}^*$ such that $U_1 \not\subseteq U_2$ and $U_1 \not\supseteq U_2$. Hence there are elements of $\mathcal{L}^*$ which are not $\mathcal{P}$-elements.

Assume that $U_1$ is contained in $T$. Let $C$ be the sum of the elements of $\mathcal{L}^*$ which are properly contained in $T$ and which are not $\mathcal{P}$-elements in $\mathcal{L}^*$ (this set is not empty, since it contains $U_1$). By definition we have that $C \subseteq \mathcal{L}^*$. We want to prove that $C$ is a $\mathcal{P}$-element in $\mathcal{L}^*$. Let $Z \in \mathcal{L}^*$. Since $T$ is a $\mathcal{P}$-element, we have $Z \leq T$ or $Z \supseteq T$. If $Z \leq T$, then $Z \supseteq C$. Assume that $Z < T$. If $Z$ is a $\mathcal{P}$-element in $\mathcal{L}^*$, then $C < Z$ or $C \supseteq Z$. If $Z$ is not a $\mathcal{P}$-element in $\mathcal{L}^*$, then $C \supseteq Z$ by definition of $C$. Thus $C$ is a $\mathcal{P}$-element in $\mathcal{L}^*$. This implies also that $C \in \mathcal{L}^* (\ast)$ (using the definition of $C$). So we apply Proposition 27 and we obtain the claim.

If $U_1$ contains $T$, the proof is just the dual (take $C$ to be the intersection of the elements of $\mathcal{L}^*$ which properly contain $T$ and which are not $\mathcal{P}$-elements in $\mathcal{L}^*$). \(\square\)

Now we are ready to prove Proposition 26.

Proof of Proposition 26. If $H$ is not an intersection of maximal subgroups of $X$, then $\mu_X(H) = 0$. So suppose $H$ is an intersection of maximal subgroups. The elements of $\mathcal{L}^*$ do not form a chain of subspaces of $V$ (i.e., a flag) since $H$ does not contain a Sylow $p$-subgroup of $X$ (see, for example, Corollary 4.115(i) in [13]). So we may apply Lemma 28.

By Lemma 28, there exists an element $T \in \mathcal{L}^*$ such that $T$ is a redundant element. Let $\mathcal{M} = \{\text{Stab}_X(W) : W \in \mathcal{L}^*\}$. By Propositions 24 and 25, we have that $\mathcal{M} \supseteq \mathcal{M}_H(X)$. Define

$$\mathcal{\overline{J}} = \left\{ J \subseteq \mathcal{M} : \bigcap_{M \in J} M = H \right\}.$$ 

By a result of [20], we have that

$$\mu_G(H) = \sum_{K \in \mathcal{\overline{J}}} (-1)^{|K|}.$$ 

Now, let

$$\mathcal{J} = \left\{ K \subseteq \mathcal{L}^* : \bigcap_{W \in K} \text{Stab}_G(W) = H \right\}$$

$$\mathcal{J}_T = \left\{ K \subseteq \mathcal{L}^*_H : \bigcap_{W \in K} \text{Stab}_G(W) = H, \ T \in K \right\} \text{ and}$$

$$\mathcal{J}_T' = \left\{ K \subseteq \mathcal{L}^*_H : \bigcap_{W \in K} \text{Stab}_G(W) = H, \ T \not\in K \right\}.$$ 

Since $T$ is a redundant element we have $\mathcal{J}_T' = \{K - \{T\} : K \in \mathcal{J}_T\}$. Since the map

$$\text{Stab}_X : \mathcal{L}^* \to \mathcal{M}$$

is a bijection, the map $\Theta : \mathcal{J} \to \mathcal{\overline{J}}$ defined by $\Theta(K) = \{\text{Stab}_X(W) : W \in K\}$ is a bijection and $|K| = |\Theta(K)|$. Thus, we obtain
Moreover, unitary, symplectic or orthogonal (see [13, pp. 17–18]).

We claim that \( L^* \) does not enjoy the property \( P \). For contradiction, assume that there exists a \( P \)-element \( Z \) in \( L^*_H(G) \). Since \( L^*_H(X) \) does not enjoy the property \( P \), there exist \( T_1 \) and \( T_2 \) distinct maximal elements of \( L^*_H(X) \). If \( Z \) contains \( T_1 \) and \( T_2 \), then \( Z \supset T_1 + T_2 \), a contradiction since \( Z \in L^*_H(G) \) and \( T_1 + T_2 \notin L^*_H(X) \). So suppose that \( Z \) does not contain \( T_1 \). Since \( Z \) is a \( P \)-element in \( L^*_H(G) \), we have that \( Z \leq T_1 \). So the set consisting of the elements \( U \) of \( L^*_H(X) \) such that \( U \geq Z \) is not empty. Thus define

\[
B = \bigcap_{U \in L^*_H(X), U \geq Z} U.
\]

We claim that \( B \) is a \( P \)-element in \( L^*_H(X) \). Let \( W \in L^*_H(X) \). If \( W \leq Z \), then \( W \leq B \) by definition of \( B \). If \( W \geq Z \), then \( W \geq B \) again by definition of \( B \). Thus \( B \) is a \( P \)-element in \( L^*_H(X) \), a contradiction.

Let \( I = I(V, \kappa) = \{ \phi \in \text{GL}(V) : \kappa(\phi(v)) = \kappa(v) \text{ for all } v \in V^1 \} \) where \( I = 1 \) if \( \kappa \) is quadratic, \( I = 2 \) otherwise. Clearly \( G \) is a section of \( I \).

Suppose that \( W \) is a totally singular subspace of \( V \). The form \( \kappa \) induces a form \( \kappa_{W^⊥/W} \) on \( W^⊥/W \). Moreover, \( \kappa_{W^⊥/W} \) is a zero, unitary, symplectic or orthogonal form according to whether \( \kappa \) is zero, unitary, symplectic or orthogonal (see [13, pp. 17–18]).

We introduce some useful definitions.

- Denote by \( I^{(W)} \) the group \( I(W^⊥/W, \kappa_{W^⊥/W}) \).
- If \( W \in L^*_H(X) \cup \{0\} \), then denote by \( L^*_H(W) \) the set of elements \( U \in L^*_H(X) \) such that \( W < U < W^⊥ \). Note that \( L^*_H(0) = L^*_H \). Moreover, if \( U \in L^*_H(W) \), then \( U/W \) is a totally singular subspace of \( W^⊥/W \) (with respect to the induced form \( \kappa_{W^⊥/W} \)).

Let \( W \in L^*_H(X) \). Suppose that \( \phi \) is an element of \( \text{Stab}_I(W) \). Thus \( \phi \) induces an element \( \phi^{(W)} \) of \( I^{(W)} \), defined by \( \phi^{(W)}(v + W) = \phi(v) + W \) for \( v \in W^⊥ \).
Now, assume that \( \phi \) is an element of 
\[
\bigcap_{U \in \mathcal{L}^\ast_H(X)} \text{Stab}_I(U).
\]
This yields \( \phi^{(W)} \) is an element of 
\[
\bigcap_{U \in \mathcal{L}^\ast_H(W)} \text{Stab}_I(W)(U/W).
\]
Now we give a more concrete representation of \( \phi \) using the matrices. The case \( L \) is trivial, so we assume that case \( L \) does not hold. Since \( W \) is totally singular, by Witt's Lemma [13, Proposition 2.1.6] we may assume that there exists \( k \geq 1 \) such that \( W = \langle e_1, \ldots, e_k \rangle \) (see Lemma 21 for the notation). The matrix of a generic element of \( I \) in the basis \( B \) obtained juxtaposing the bases \( B_1 = \langle e_1, \ldots, e_k \rangle, B_2 = \langle e_{k+1}, \ldots, e_m \rangle, B_3 = \langle f_{k+1}, \ldots, f_m \rangle, B_4 = \langle x, y, z \rangle \) and \( B_5 = \langle f_1, \ldots, f_k \rangle \) is
\[
M = \begin{pmatrix}
M_{11} & M_{12} & M_{13} & M_{14} & M_{15} \\
M_{21} & M_{22} & M_{23} & M_{24} & M_{25} \\
M_{31} & M_{32} & M_{33} & M_{34} & M_{35} \\
M_{41} & M_{42} & M_{43} & M_{44} & M_{45} \\
M_{51} & M_{52} & M_{53} & M_{54} & M_{55}
\end{pmatrix}
\]
where \( M_{ij} \) is a matrix with respect to the bases \( B_i \) and \( B_j \) with coefficient in \( \mathbb{F} = \mathbb{F}_{q^u} \). Consider an element \( \phi \in \text{Stab}_I(W) \), and let \( M \) be its matrix. It is clear that \( M_{21} = M_{31} = M_{41} = M_{51} = M_{52} = M_{53} = M_{54} = 0 \). Let
\[
F = \begin{pmatrix}
0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 \\
0 & (-1)^a & 0 & 0 & 0 \\
0 & 0 & 0 & D & 0 \\
(-1)^a & 0 & 0 & 0 & 0
\end{pmatrix}
\]
be the matrix of the form \( f \) associated to \( \kappa \), where \( D \) is a suitable matrix with coefficients in \( \mathbb{F} \) and
\[
a = \begin{cases}
1 & \text{if case S holds,} \\
0 & \text{otherwise.}
\end{cases}
\]
Since \( \phi \in I \), we have that \( MF^{F_{\alpha}} = F \), where \( \alpha \) is the automorphism of \( \mathbb{F}_{q^u} \) defined by \( \lambda^a = \lambda^g \) (see [13, Lemma 2.1.8]). Moreover, if \( \kappa = Q \) is quadratic, then we require that \( Q(\phi(v)) = Q(v) \) for all \( v \in V \). This yields the following facts:

1. The element \( \phi^{(W)} \) of \( I^{(W)} \) has matrix
\[
M' = \begin{pmatrix}
M_{22} & M_{23} & M_{24} \\
M_{32} & M_{33} & M_{34} \\
M_{42} & M_{43} & M_{44}
\end{pmatrix}
\]
with respect to the basis obtained juxtaposing the bases \( \langle e_{k+1} + W, \ldots, e_m + W \rangle, \langle f_{k+1} + W, \ldots, f_m + W \rangle \) and \( \langle x + W, y + W, z + W \rangle \). In particular, \( M' \) is invertible.
(2) \( M_{55} = M_{11}^{-\alpha t} \).

(3) 
\[
\begin{pmatrix}
M_{25} \\
M_{35} \\
M_{45}
\end{pmatrix} = -
\begin{pmatrix}
(1)^a M_{22} & M_{23} & M_{24} \\
(1)^a M_{32} & M_{33} & M_{34} \\
M_{42} & M_{43} & M_{44}
\end{pmatrix}
\begin{pmatrix}
M_{11}^\alpha \\
M_{12}^\alpha \\
D_{14}^\alpha M_{14}^\alpha
\end{pmatrix} M_{11}^{-\alpha t}.
\]

(4) \( M_{15} M_{11}^\alpha + (1)^a M_{11} M_{15}^{-\alpha} = -M_{13} M_{12}^\alpha - (1)^a M_{12} M_{13}^{-\alpha} - M_{14} D_{14} M_{14}^\alpha \).

(5) If case \( \mathbf{O}^+ \) or \( \mathbf{O}^- \) holds, then by \( Q(\phi(f_i)) = Q(f_i) = 0 \) for \( i \in \{1, \ldots, k\} \), we obtain

\[
M_{15}^i M_{55}(i, i) = -\left( M_{25}^i M_{35}(i, i) + M_{45}(1, i) M_{45}(2, i) + M_{45}(1, i)^2 + \zeta M_{45}(2, i)^2 \right).
\]

We summarize the above discussion in the following lemma.

**Lemma 30.** Assume that case \( \mathbf{L} \) does not hold. Let \( \mathcal{B} \) be the basis of \( V \) and let \( M \) be the matrix defined above. An element \( \phi \) of \( \text{Stab}_1(W) \) is completely determined if we give:

- an element \( \psi \) of \( l^{(W)} \), which has a matrix \( M' \) as above;
- the matrices \( M_{11} \in GL_k(F_q^\alpha), M_{12} \in M_{k, m-k}(F_q^\alpha), M_{13} \in M_{k, m-k}(F_q^\alpha) \) and \( M_{14} \in M_{k, n-2m}(F_q^\alpha) \);
- the elements \( B(i, j) \in F_q^\alpha \) for \( 1 \leq i \leq j \leq k \), which are components of the matrix \( B = M_{11}^{-1} M_{15} \). The element \( B(i, i) \) satisfies \( B(i, i)^\alpha + (1)^a B(i, i) = b \) for some \( b \) determined by \( M_{11}, M_{12}, M_{13}, M_{14} \) for \( i \in \{1, \ldots, k\} \). Moreover, if case \( \mathbf{O}^+ \) or \( \mathbf{O}^- \) holds, then \( B(i, i) \) is determined by \( M', M_{11}, M_{12}, M_{13}, M_{14} \) for \( i \in \{1, \ldots, k\} \).

**Proof.** As we have seen in the above discussion, if we give \( M', M_{11}, M_{12}, M_{13}, M_{14} \) and \( M_{15} \), then \( \phi \) is completely determined. By (4) above we get:

\[
B + (1)^a B^{\alpha t} = M_{11}^{-1} M_{15} + (1)^a M_{15} M_{11}^{-\alpha t}
\]

\[
= -M_{11}^{-1} (M_{12} M_{13}^{-\alpha} + (1)^a M_{13} M_{12}^{\alpha} + M_{14} D_{14} M_{14}^{\alpha}) M_{11}^{-\alpha t}.
\]

Note that \( B + (1)^a B^{\alpha t} \) is completely determined by \( M_{11}, M_{12}, M_{13}, M_{14} \). So it is enough to prove that if we give \( B + (1)^a B^{\alpha t} \) and \( B(i, j) \) for \( 1 \leq i \leq j \leq k \), then \( B \) is completely determined. Assume that \( B + (1)^a B^{\alpha t} \) is given. Thus \( B(j, i) + (1)^a B(i, j)^{\alpha} = b_{i,j} \) for some \( b_{i,j} \) fixed, with \( 1 \leq i \leq j \leq k \). Hence we have that \( B(j, i) = b_{i,j} - (1)^a B(i, j)^{\alpha} \) is determined.

Note that for \( i \in \{1, \ldots, k\} \) the element \( B(i, i) \) satisfies the equation \( B(i, i) + (1)^a B(i, i)^{\alpha} = b_{i,i} \). Assume that case \( \mathbf{O}^+ \) or \( \mathbf{O}^- \) holds. Therefore \( \alpha = 1 \), so by (2) and (5) above we have

\[
B(i, i) = M_{11}^{-1} M_{15}(i, i) = M_{15}^i M_{55}(i, i) = M_{11}^i M_{55}(i, i).
\]

Thus \( B(i, i) \) is completely determined by the knowledge of \( M', M_{11}, M_{12}, M_{13} \) and \( M_{14} \).

**Proposition 31.** Let \( W \) be an element of \( \mathcal{L}^\alpha_H(X) \). Suppose that \( \mathcal{L}^{(W)}_H \neq \emptyset \) and \( \mathcal{L}^{(W)}_H \) does not enjoy the property \( \mathcal{P} \). Then one of the following holds:

(1) There exist \( U \) and \( T \) in \( \mathcal{L}^\alpha_H \) such that \( U + T = W \) and \( U \cap T = W \).

(2) There exists \( U \in \mathcal{L}^\alpha_H - \{W, W^\perp\} \) such that \( U^\perp + U = W^\perp \) and \( U^\perp \cap U = W \).

(3) There exist \( T \in \mathcal{L}^{(W)}_H \) and \( U \in \mathcal{L}^{(W)}_H \) such that \( U \cap T = W \), \( \mathcal{L}^{(T)}_H \neq \emptyset \) and \( \mathcal{L}^{(T)}_H \) does not enjoy the property \( \mathcal{P} \).
Proof. Since $L_U^{(W)} \neq \emptyset$ and $L_U^{(T)}$ does not enjoy the property $\mathcal{P}$, there exist $M_1$ and $M_2$ distinct maximal elements in $L_U^{(W)}$. Note that $L_U^{(M_1 \cap M_2)}$ is non-empty. We claim that $L_U^{(M_1 \cap M_2)}$ does not enjoy $\mathcal{P}$. For contradiction, if $Z$ is a $\mathcal{P}$-element in $L_U^{(M_1 \cap M_2)}$, since $M_1$ and $M_2$ are maximal, then $Z \leq M_1$ and $Z \leq M_2$. So $Z \leq M_1 \cap M_2$, a contradiction with $Z \in L_U^{(M_1 \cap M_2)}$.

Assume $M_1 \cap M_2 > W$. Consider the set

$$\mathcal{N} = \{Z \in L_U^{(W)} : Z \leq M_1 \cap M_2, \ L_U^{(Z)} \text{ does not enjoy } \mathcal{P}\}.$$ 

Let $T$ be a minimal element in $\mathcal{N}$. Since $L_U^{(M_1 \cap M_2)}$ is non-empty, also $L_U^{(T)}$ is not empty. Since $T \in L_U^{(W)}$ and $L_U^{(T)}$ does not enjoy the property $\mathcal{P}$, there exists $U \in L_U^{(W)}$ such that $U \cap T < T$. For a contradiction, assume that $U \cap T > W$. Then $U \cap T \in L_U^{(W)}$ and we have that $L_U^{(U \cap T)}$ is not empty. Since $U \cap T < T$ and $T$ is minimal in $\mathcal{N}$, we have that $L_U^{(U \cap T)}$ enjoys $\mathcal{P}$. Thus there exists a $\mathcal{P}$-element $Z$ in $L_U^{(U \cap T)}$. Since $L_U^{(T)} \leq L_U^{(U \cap T)}$ and $L_U^{(T)}$ does not enjoy $\mathcal{P}$, we have that $Z \leq T$. If $Z \leq U$, then $Z \leq U \cap T$, a contradiction with $Z \in L_U^{(U \cap T)}$. If $Z \geq U$, then $U \leq T$, a contradiction. So we obtain $U \cap T = W$ and (3) holds.

Assume $M_1 \cap M_2 = W$. Assume that $M_1 + M_2 = W$. Then (1) holds with $U = M_1$ and $T = M_2$. Now, suppose that $U = M_1 + M_2 < W$. Clearly case L does not hold. The subspace $U \cap U^\perp$ is a totally singular element of $L_U$. We claim that $U \cap U^\perp = W$. For a contradiction, suppose that $U \cap U^\perp > W$. Without loss of generality, we may assume that $M_1 \not\subseteq U \cap U^\perp$. Now, $U \cap U^\perp \leq M_1^\perp$, so $M_1 + U \cap U^\perp$ is an element of $L_U^{(W)}$. This contradicts the maximality of $M_1$. Thus we have $U \cap U^\perp = W$, so $U^\perp + U = W$. Hence (2) holds. □

Let $W$ be an element of $L_U \cup \{0\}$. Suppose that $d = \dim W^\perp / W$. Recall that $I^{(W)} = I(W^\perp / W, \kappa_{W^\perp / W})$. Let

$$H_{I^{(W)}} = \bigcap_{U \in L_U^{(W)}} \text{Stab}_{H_{I^{(W)}}}(U).$$

We have the following.

Proposition 32. If $L_U^{(W)}$ is not empty and $L_U^{(T)}$ does not enjoy the property $\mathcal{P}$, then

$$|I^{(W)} : H_{I^{(W)}}|_p \geq q^{\beta'(d)},$$

where

$$\beta'(d) = \begin{cases} 
  d - 1 & \text{if case L or U holds}, \\
  \frac{d}{2} - \log_q 2 & \text{if case S holds}, \\
  \frac{d-1}{2} & \text{if case O^0 holds}, \\
  \frac{d-2}{2} + \log_q 2 & \text{if case O^+ or O^- holds}.
\end{cases}$$

Proof. Without loss of generality, we assume that $W = 0$. Let $I = I^{(0)}$ and $H_I = H_{I^{(0)}}$. Recall that $n$ is the dimension of $V$. Since $L_U^{(W)}$ is not empty, then $n \geq 2$ and Proposition 31 applies. In Table 19 we report the $p$-part of the order of $I$ (see [13, p. 19]).

In order to prove the proposition, we argue by induction on $n$.

Case (1). Assume that there exist $U$ and $T$ in $L_U^{(n)}$ such that $U + T = V$ and $U \cap T = 0$. If case L holds, then $\text{Stab}_T(T) \cap \text{Stab}_U(U)$ is isomorphic to $\text{GL}_{n_1}(q) \times \text{GL}_{n_2}(q)$, where $n_1 = \dim T$ and $n_2 = \dim U$, and
Thus we have that $Stab$ does not hold. So

$$n \geq \log |I : H|_p + \log_2 |2I|_p$$

do not hold. Then $T$ and $U$ are maximal totally singular subspaces of $V$, so $\dim T = \dim U = n/2$. In particular $n$ is even. By Witt's Lemma [13, Proposition 2.1.6] we may assume that $T = \langle e_1, \ldots, e_m \rangle$ and $U = \langle f_1, \ldots, f_m \rangle$ (see Lemma 21 for the notation). By [13, Lemma 4.1.9], we have that $Stab(T) \cap Stab(U)$ is isomorphic to $GL_{n/2}(q^{u})$. Thus we have that

$$\log_2 |I : H|_p \geq \log_2 |I|_p - \frac{nu(n - 2)}{8} \geq \beta'(n),$$

for $n \geq 2$.

**Case (2). Assume that there exists $U \in L_H \setminus \{0, V\}$ such that $U^\perp + U = V$ and $U^\perp \cap U = 0$.** Clearly, case L does not hold. So $\kappa$ is non-degenerate, and thus $U$ is non-degenerate. Let $k = \dim U$. By [13, §4.1], we obtain Table 20. Thus it is easy to see that

$$\log_2 |I : H|_p \geq \log_2 |I : Stab(U)|_p \geq \beta'(n),$$

for $n \geq 2$ and $n > k$.

**Assume that Case (1) and Case (2) do not hold.** By Proposition 31, there exist $T \in L_H^\perp$ and $U \in L_H^\perp$ such that $U \cap T = 0$, $L_H^T \neq \emptyset$, and $L_H^{(T)}$ does not enjoy the property $P$.

Assume case L holds. Let $T = \langle e_1, \ldots, e_k \rangle$ and $U = \langle e_{k+1}, \ldots, e_h \rangle$, for some $k + 1 \leq h \leq m = n$. In the basis $e_1, \ldots, e_n$ the generic matrix of an element of $H_I$ is of the form

$$\left( \begin{array}{cc} GL(T) & M_{k \times (n-h)}(\mathbb{F}_q) \\ \bigcap & \bigcap \\ H_{I(T)} & \end{array} \right).$$

Thus we have that

$$\log_2 |H_I|_p \leq \log_2 \left( |H_{I(T)}|_p |M_{k \times (n-h)}(\mathbb{F}_q)|_p |GL(T)|_p \right) \leq \log_2 |H_{I(T)}|_p + k(n-h) + \frac{k(k-1)}{2}.$$
This yields
\[ \log_q |I : H_1|_p \geq \log_q |I : H_{(T)}|_p + \log_q |I^{(T)} : H_{(T)}|_p - k(n - h) - \frac{k(k - 1)}{2}. \]

Since \( \dim V/T < n \), by induction we have that
\[ \log_q |I^{(T)} : H_{(T)}|_p \geq \beta'(\dim V/T) = \beta'(n - k) = n - k - 1, \]
so we obtain
\[ \log_q |I : H_1|_p \geq \frac{n(n - 1)}{2} - \frac{(n - k)(n - k - 1)}{2} + n - k - 1 - k(n - h) - \frac{k(k - 1)}{2} \]
\[ \geq n - 1 + k(h - k - 1) \]
\[ \geq n - 1. \]

The last inequality holds since \( k \geq 1 \) and \( h \geq k + 1 \).

Assume case L does not hold. Assume that \( U \cap T^\perp > 0 \). Thus there exists \( v \in U \) such that \( v \in T^\perp \). By Witt's Lemma [13, Proposition 2.1.6] we may assume that \( T = (e_1, \ldots, e_k) \) and \( v = e_{k+1} \). Let \( \phi \) be an element of \( H_1 \). We have that \( \phi(e_{k+1}) = \phi(v) \notin T \) since \( U \cap T = 0 \). Using the notation of Lemma 30, we have that the first column of \( M_{12} \) consists of zeros. By Lemma 30, to completely determine \( \phi \) it is enough to give:

- \( M_{11} \in \text{GL}_k(q^u) \langle \frac{q^{uk(k-1)}}{2} \prod_{i=1}^k (q^{ui} - 1) \text{ choices}) \rangle; \\
- \( M_{12} \in \text{M}_{k, m-k}(\mathbb{F}_{q^u}) \) with the first column filled with zeros \( (q^{uk(m-k-1)} \text{ choices}) \); \\
- \( M_{13} \in \text{M}_{k, m-k}(\mathbb{F}_{q^u}) \langle q^{uk(m-k)} \text{ choices for } M_{13} \rangle; \\
- \( M_{14} \in \text{M}_{k, n-2m}(\mathbb{F}_{q^u}) \langle q^{uk(n-2m)} \text{ choices for } M_{14} \rangle; \\
- B(i, j) \in \mathbb{F}_{q^u} \text{ for } 1 \leq i < j \leq k \langle \frac{q^{uk(k-1)}}{2} \text{ choices}) \rangle; \\
- B(i, i) \in \mathbb{F}_{q^u} \text{ for } i \in \{1, \ldots, k\} \text{ and we have } q^{uk} \text{ choices, where} \]
\[ \lambda = \begin{cases} 1 & \text{if } u = 2 \text{ or case S holds,} \\ 0 & \text{otherwise;} \end{cases} \]

- an element \( \psi \) of \( H_{(T)} \langle |H_{(T)}| \text{ choices}) \).

So we get that
\[ \log_q |H_1|_p \leq uk(n - 2 - k) + \lambda k + \log_q |H_{(T)}|_p. \]

This yields
\[ \log_q |I : H_1|_p \geq \log_q |I : I^{(T)}|_p + \log_q |I^{(T)} : H_{(T)}|_p - uk(n - 2 - k) - \lambda k. \]

Since \( \dim T^\perp/T < n \), by induction we have that
\[ \log_q |I^{(T)} : H_{(T)}|_p \geq \beta'(\dim T^\perp/T) = \beta'(n - 2k), \]
so it is easy to see that

$$\log_q |I : H_I|_p \geq \log_q |I : t(T)|_p + \beta'(n - 2k) - uk(n - 2 - k) - \lambda k = \beta'(n).$$

In the rest of the proof we show that we can always reduce to the case $U \cap T^\perp > 0$.

Assume that $U \cap T^\perp = 0$. Let $R = (U + T) \cap (U + T)^\perp = (U + T) \cap U^\perp \cap T^\perp$. We claim that $R \in \mathcal{L}_H^\ast$. For contradiction, suppose that $R \notin \mathcal{L}_H^\ast$. Since $R = (U + T) \cap (U + T)^\perp$ is totally singular and $R \notin \mathcal{L}_H^\ast$, we must have that $R = 0$. But this is a contradiction since Case (2) does not hold. So we have the claim. In particular, $R > 0$.

Assume that $R \cap T > 0$. Thus $R \cap T \in \mathcal{L}_H^\ast$. Since $\mathcal{L}_H^{(T)} \subseteq \mathcal{L}_H^{(R \cap T)}$, the set $\mathcal{L}_H^{(R \cap T)}$ is not empty. We claim that $\mathcal{L}_H^{(R \cap T)}$ does not enjoy the property $\mathcal{P}$. For a contradiction, assume that $Z$ is a $\mathcal{P}$-element in $\mathcal{L}_H^{(R \cap T)}$. If $Z \supseteq T$, then $Z \in \mathcal{L}_H^{(T)}$, but $\mathcal{L}_H^{(T)}$ does not contain $\mathcal{P}$-elements. So $Z < T$. Since $R \leq U$, then $R + U \in \mathcal{L}_H^{(R \cap T)}$. Since $R \cap U \subseteq T$ and $Z$ is a $\mathcal{P}$-element such that $Z < T$, then $Z < R + U$. So $Z \leq (R + U) \cap T \leq U \cap T \leq R \cap T$, a contradiction. We know that $R \cap T \in \mathcal{L}_H^\ast$, $U \in \mathcal{L}_H^\ast$, $U \leq (R \cap T)^\perp$, $U \cap R = 0$, $\mathcal{L}_H^{(R)}$ is not empty and $\mathcal{L}_H^{(R)}$ does not enjoy $\mathcal{P}$. Therefore, without loss of generality, we may assume that $R \cap T = T$ and argue as in the case $U \cap T^\perp > 0$.

Assume that $R \cap T = 0$. We know that $R, T \in \mathcal{L}_H^\ast$, $R \leq T^\perp$, $R \cap T = 0$, $\mathcal{L}_H^{(T)}$ is not empty and $\mathcal{L}_H^{(T)}$ does not enjoy $\mathcal{P}$. Therefore, without loss of generality, we may assume that $R = U$ and argue as in the case $U \cap T^\perp > 0$.

The proof is finished. □

**Theorem 33.** Let $H$ be as in Theorem 20. Suppose that $\mathcal{L}_H^\ast(X)$ is not empty and $\mathcal{L}_H^\ast(X)$ does not enjoy the property $\mathcal{P}$. Then $|X : H|_p \geq q^{\beta(n)}$.

**Proof.** Since $HG = X$, we have that $|X : H|_p = |G : H \cap G|_p$. By the previous proposition, we know that $|I : H_I|_p \geq q^{\beta(d)}$, where $I = I(V, \kappa)$. Note that $F^\ast \leq H_I$, since a scalar matrix stabilizes each subspace. Let $S = S(V, \kappa)$ (see Section 6 for the notation). By [13, Table 2.1.C], we have that $|I : S|_p = 1$. Thus $|S : H_I \cap S|_p = |I : H_I|_p$. Now, $|F^\ast|_p = 1$, so

$$|S : S \cap H_I|_p = |S : S \cap H_I|_p.$$ 

If case $O$ does not hold, then $G = S$. Since in this case $G \cap H = S \cap H_I$, we have the claim. If case $O$ holds, then $|S : G| = 2$, so we have that $2|G : H \cap G|_p \geq |S : S \cap H_I|_p \geq q^{\beta(n)}$. Thus $|G : H \cap G|_p \geq q^{\beta(n) - \log_q |2|_p} = q^{\beta(n)}$.

**9. Connection between the Dirichlet polynomials of $X$ and of $G$**

Let $X$ and $G$ be as in Section 6. Let $r$ be a prime number. Recall from the introduction that $P_{X,G,r}(s)$ is the Dirichlet polynomial

$$\sum_{(k,r) = 1} \frac{a_k(X, G)}{k^s}.$$ 

The aim of this section is to prove the following proposition.

**Proposition 34.** $P_{X,G,r}(s) = P_{G,r}^{(p)}(s)$.

Here we restate Lemma 9 in a more general way.
Lemma 35. 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 maximal subgroup of \( G \) such that \( MN = G \) and \( R \leq M \), then \( M \) contains also \( N_G(R) \). We have that

\[
P_{G,N}(s) = \sum_{R \leq H \leq G, \ \HN=\G} \frac{\mu_G(H)}{|G : H|^{s-1}}.
\]

Proof. The proof is the same as in [4, Lemma 2], considering just the subgroups \( H \) such that \( \HN=\G \). \(\Box\)

Let \( P \) be a Sylow \( p \)-subgroup of \( X \). Thus \( P \cap G \) is a Sylow \( p \)-subgroup of \( G \) and \( B = N_G(P \cap G) \) is a Borel subgroup in \( G \). Given a subgroup \( K \) of \( X \), denote by \( S_K(X) \) the set of subgroups \( H \) of \( X \) such that \( H \supseteq K \).

Lemma 36. (See [3, Theorem 8.3.3].) Let \( H \) be a subgroup of \( S \) such that \( H \supseteq B \). Then \( N_S(H) = H \).

Lemma 37. Let \( P \) and \( B \) be as above. We have that:

1. \( N_X(B) = N_X(P \cap G) \) and \( N_X(B)G = X \);
2. if \( M \) is a maximal subgroup of \( X \) such that \( M \supseteq P \) and \( MG = X \), then \( M \supseteq N_X(B) \).

Proof. Well known, see [13]. \(\Box\)

Lemma 37 implies that \( S_{N_X(B)}(X) = \{ H \leq X : H \supseteq N_X(B), \ HG = X \} \). We say that the elements of the set \( S_{N_X(B)}(X) \) are the parabolic subgroup of \( X \) over \( N_X(B) \). A parabolic subgroup of \( X \) is an element of \( S_{N_X(B)}(X) \) for some Borel subgroup \( B \) of \( G \).

Now we want to give a better description of the elements of the set \( S_{N_X(B)}(X) \). Let \( S^X_B(G) \) denote the subset of \( S_B(G) \) given by

\[
\{ H \in S_B(G) : N_X(H) \supseteq N_X(B) \}.
\]

We have the following.

Proposition 38. The map \( \eta : S_{N_X(B)}(X) \rightarrow S^X_B(G) \) given by \( \eta(H) = H \cap G \) is well defined. Moreover \( \eta \) is an isomorphism of posets, in particular \( N_X(\eta(H)) = H \) for each \( H \in S_{N_X(B)}(X) \).

Proof. We show that \( \eta \) is well defined. Let \( H \in S_{N_X(B)}(X) \). Clearly \( H \cap G \supseteq N_X(B) \cap G = N_G(B) = B \). Since \( H \cap G \leq H \), we have that \( N_X(H \cap G) \supseteq H \supseteq N_X(B) \). Hence \( H \cap S \in S^X_B(G) \).

We claim that \( \eta \) is surjective. Let \( K \in S^X_B(G) \). By definition \( N_X(K) \supseteq N_X(B) \), so \( N_X(K) \in S_{N_X(B)}(X) \). Finally \( \eta(N_X(K)) = N_X(K) \cap S = N_S(K) = K \) by Lemma 36.

We claim that \( \eta \) is injective. It is enough to prove that \( N_X(\eta(H)) = H \) for each \( H \in S_{N_X(B)}(X) \). As above, we have that \( N_X(H \cap G) \supseteq H \). Since \( HS = X \), using Lemma 36, we get

\[
|X : N_X(H \cap G)| = |G : N_X(H \cap G) \cap G| = |G : N_G(H \cap G)| = |G : H \cap G| = |X : H|,
\]

thus \( N_X(H \cap G) = H \).

It is straightforward to show that the map \( \eta \) is an isomorphism of posets. \(\Box\)

Now we are ready to prove Proposition 34.
Proof of Proposition 34. Since $P \cap G \leq P$, we have that Lemma 37(1) implies that $N_X(P) \leq N_X(B)$. Hence, by Lemmas 37(2) and 35 we get that

$$P_{X,G}^{(p)}(s) = \sum_{H \leq B \leq X} \frac{\mu_X(H)}{|X : H|^{s - 1}} = \sum_{H \in S_{N_X(B)}(X)} \frac{\mu_X(H)}{|X : H|^{s - 1}},$$

observing that if $P \leq H < N_X(B)$, then $H$ is not an intersection of maximal subgroups (by Lemma 37(2)), hence $\mu_X(H) = 0$ (by Lemma 5).

As in the proof of Proposition 10, by [3, Proposition 8.2.2], we associate to a subset $J$ of $I$ a parabolic subgroup $P_J$. Moreover, the map $J \mapsto P_J$ is an isomorphism between the lattice $\mathcal{P}(I)$ (the set of subsets of $I$) and the lattice $S_B(G)$. Since $N_X(B)$ acts by conjugation on $S_B(G)$, the group $N_X(B)$ acts on $\mathcal{P}(I)$ (via the isomorphism $J \mapsto P_J$). 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 $0 \in I$ is a $\rho$-orbit, then $\{0\} = \{0\}^g$. Note that if $G$ is twisted, then the action of $N_X(B)$ is trivial. Assume that $G$ is untwisted. The action of $N_X(B)$ on $I$ can be thought as an action of $N_X(B)$ on $\Pi$. So, any element $g$ of $N_X(B)$ induces a symmetry $\psi_B$ of the Dynkin diagram $\mathcal{D}$ of $S$. Since $X = G N_X(B)$, if $h \in X$, then $h = s g$ for some $s \in G$ and $g \in N_X(B)$. If $\psi_B$ is not trivial, then $h$ is a non-trivial graph automorphism.

By definition, the group $X$ does not contain non-trivial graph automorphism, hence the action of $N_X(B)$ on $I$ is trivial. So we have $S_X^G(G) = S_B(G)$.

Now, by Proposition 38, the posets $S_{N_X(B)}(X)$ and $S_B(G)$ are isomorphic so we obtain:

$$P_{X,G}^{(p)}(s) = \sum_{H \in S_{N_X(B)}(X)} \frac{\mu_X(H)}{|X : H|^{s - 1}} = \sum_{B \leq K \leq G} \frac{\mu_G(K)}{|G : K|^{s - 1}} = P_G^{(p)}(s).$$

This concludes the proof. □

10. Proof of the main theorem

This section is devoted to the proof of Theorem 2. Recall the notation from Section 6. Since $G$ is a normal subgroup of $X$, we have that $P_X(s) = P_{X,G}(s)P_{X,G}(s)$. Note that in order to prove Theorem 2 it suffices to show that $P_G(X)(-1) \neq 0$. In fact, since $G/X$ is soluble, we have that $P_{G/X}(X)(-1) \neq 0$, by Proposition 1.

In the first part of this section we deal with some particular cases. In the second part we concentrate on the general case.

We recall the following lemma on the existence of Zsigmondy primes.

Lemma 39. (See [21].) Let $a, n \in \mathbb{N}, a, n \geq 2$. There exists a prime divisor $q$ of $a^n - 1$ such that $q$ does not divide $a^i - 1$ for all $0 < i < n$, except in the following cases:

- $n = 2$, $a = 2^s - 1$ with $s \geq 2$.
- $n = 6$, $a = 2$.

When this prime divisor exists, it is called a Zsigmondy prime for $(a, n)$.

Recall that $\mathcal{M}_G(X)$ is the set of maximal subgroups of $X$ containing $H$ and supplementing $G$. When we write $\mathcal{M}_K(G)$ we mean the set of maximal subgroups of $G$ containing $K$.

Proposition 40. Assume $n = 2$ and case I holds. We have that $P_{X,G}(X)(-1) \neq 0$. 

Table 21

$P_X(-1)$ for some groups.

<table>
<thead>
<tr>
<th>$X$</th>
<th>$P_X(-1)$</th>
<th>$X$</th>
<th>$P_X(-1)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{PSL}_2(4) \cong \text{PSL}_2(5)$</td>
<td>$-1560$</td>
<td>$\text{PGL}_2(9)$</td>
<td>$-37080$</td>
</tr>
<tr>
<td>$\text{PGL}_2(5) \cong \text{PGL}_2(4)$</td>
<td>$1560$</td>
<td>$\text{PSL}_2(9)$</td>
<td>$-95400$</td>
</tr>
<tr>
<td>$\text{PSL}_2(7) \cong \text{PSL}_2(2)$</td>
<td>$-2856$</td>
<td>$\text{M}_{10}$</td>
<td>$-37080$</td>
</tr>
<tr>
<td>$\text{PGL}_2(7) \cong \text{PGL}_2(3)$</td>
<td>$-8904$</td>
<td>$\text{PGL}_2(9)$</td>
<td>$111240$</td>
</tr>
<tr>
<td>$\text{PSL}_2(8)$</td>
<td>$-123984$</td>
<td>$\text{PSL}_2(11)$</td>
<td>$133320$</td>
</tr>
<tr>
<td>$\text{PGL}_2(8)$</td>
<td>$247968$</td>
<td>$\text{PGL}_2(11)$</td>
<td>$244200$</td>
</tr>
<tr>
<td>$\text{PSL}_2(9)$</td>
<td>$95400$</td>
<td>$\text{PSL}_2(49)$</td>
<td>$3318554400$</td>
</tr>
</tbody>
</table>

**Proof.** In Table 21 we report the values of $P_X(-1)$ for the almost simple group $X$ such that $\text{PSL}_2(q) \leq X \leq T$, with $q \leq 11$, and $\text{PSL}_2(49)$.

For the rest of the proof, we suppose that $q > 11$ and $X \neq \text{PSL}_2(49)$.

Assume $f = 1$. Let $P$ be a Sylow $p$-subgroup of $X$. Let $M$ be a maximal subgroup of $X$ such that $M$ contains $P$ and $MG = X$. By Lemma 37, we have that $N_X(P) \leq M$, so we can apply Lemma 35. By [13, Proposition 4.1.16], we have that $M = N_X(M \cap G)$ and $M \cap G$ is a maximal subgroup of $G$. Since $M \cap G = N_G(P \cap G)$ we have that $M \cap G = \{M \cap G\}$ and so $M \cap X = \{M\}$. Applying Lemma 35, we deduce that

$$P_G^{(p)}(s) = 1 - \frac{1}{|G : M \cap G|^{-1}} = 1 - \frac{1}{|X : M|^{-1}} = P_{X,G}(s).$$

By [17, part (1) of the proof of Proposition 8], we get

$$P_{X,G}^{(p)}(s) = 1 - \frac{p + 1}{(p + 1)^2}.$$

Hence we have

$$P_{X,G}(-1) = -2p - p^2 + \sum_{p \mid k} a_k(X, G)k \equiv -2p \pmod{p^2},$$

so $P_{X,G}(-1) \neq 0$.

Now, assume $f \geq 2$ and $q \neq 49$. As in [17, case $m = 1$ of the proof of Proposition 16], let $t$ be a Zsigmondy prime for $\langle p, 2f \rangle$ (see Lemma 39 for the notation). In particular, for $f = 2$,

if $5^3$ divides $p^2 + 1$, let $t = 5$;
otherwise, let $t$ be a Zsigmondy prime for $\langle p, 4 \rangle$ distinct from 5.

Let $T$ be a Sylow $t$-subgroup of $X$. Let $\delta = (q - 1, 2)$. By [17, case $m = 1$ of the proof of Proposition 16], we have:

(a) $P_G(s) = 1 - \frac{q(q-1)/2}{q(q-1)/2} + \sum_{\ell \mid q} \frac{a_{\ell}(G)}{\ell^\delta}$.

(b) Let $K$ be a maximal subgroup of $G$. We have that $|G : K|$ is divisible by $t$ if and only if $K$ is not isomorphic to $D_{2(q+1)/\ell}$. In particular, if $K$ is not isomorphic to $D_{2(q+1)/\ell}$, we have $v_t(|G : K|) > v_t(|G|)/2$, where $v_t : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is the $t$-adic valuation map.

(c) Let $K_1$ and $K_2$ be two distinct maximal subgroups isomorphic to $D_{2(q+1)/\ell}$. We have that $v_t(|G : K_1 \cap K_2|) > v_t(|G|)/2$.

(d) The group $N_G(T \cap G)$ is a maximal subgroup of $G$ isomorphic to $D_{2(q+1)/\ell}$. 

Moreover, by [7], we have that

(*) if $M$ is a maximal subgroup of $X$ and $M \cap G$ is isomorphic to a subgroup of $D_{2(q+1)/5}$, then $M \cap G$ is isomorphic to $D_{2(q+1)/5}$.

In particular, if $M$ is in $\mathcal{M}_T(X)$, by (d) we have that $M \cap G = N_G(T \cap G)$ and $M = N_X(N_G(T \cap G))$. So we obtain $N_X(T \cap G) \leq N_X(N_G(T \cap G)) = M$ and since $N_X(T) \leq N_X(T \cap G)$, we get $N_X(T) \leq M$. Moreover, by (b), (d) and $M = N_X(M \cap G)$, we have that $\mathcal{M}_{T \cap G}(G) = \{M \cap G\}$ and so $\mathcal{M}_T(X) = \{M\}$.

Using (a) and applying Lemma 35, we deduce that

$$P_{X,G}^{(s)}(s) = 1 - \frac{1}{|q(q-1)/2|^{s-1}} = 1 - \frac{1}{|G : M \cap G|^{s-1}} = 1 - \frac{1}{|X : M|^{s-1}} = P_{X,G}^{(s)}(s).$$

Now, let $H$ be a subgroup of $X$ such that $HG = X$ and $H$ does not contain a Sylow $t$-subgroup of $X$. We have that $|X : H| = |G : H \cap G|$. Suppose that $M$ is a maximal subgroup of $X$ containing $H$. By (*) we have that $M \cap G$ is not isomorphic to a subgroup of $D_{2(q+1)/5}$. Thus, by (b) and (c), we obtain $v_t(|X : H|) = v_t(|G|)/2$. Arguing as in [17, case $m = 1$ of the proof of Proposition 16], we get

$$v_t(P_{X,G}^{(s)}(-1)) = v_t(P_{G}^{(s)}(-1)) = v_t(|G|)$$

and

$$P_{X,G}(-1) = P_{X,G}^{(s)}(-1) + \sum_{t|k} a_k(X, G) k \neq 0 \pmod{v_t(|G|)+1},$$

so $P_{X,G}(-1) \neq 0$.

Finally, let $q = 49$ and $X > G$. We show that $r = 5$ fulfills the requirements of the proposition. Let $M$ be a maximal subgroup of $X$ such that $MS = X$ and $|X : M|_{5} = 1$. By [7, Theorems 1.3, 1.4, 1.5 and 3.5], we have that $M$ is conjugated to $N_X(D_{50})$. Let $M_1$ and $M_2$ be two distinct maximal subgroups of $X$ such that $M_1S = M_2S = X$ and $|X : M_1|_{5} = |X : M_2|_{5} = 1$. We claim that $|X : M_1 \cap M_2| > 1$. For a contradiction, suppose that $M_1 \cap M_2$ contains a Sylow $5$-subgroup of $X$. Since $M_1$ and $M_2$ are conjugated to $N_X(D_{50})$, they contain a cyclic normal subgroup $C$ of order 25. Thus $C \leq X$, a contradiction. Hence we get

$$P_{X,5}^{(s)}(s) = 1 - 1176^{1-s}.$$

Now, if $M$ is a maximal subgroup of $X$ such that $MS = X$ and $|X : M|_{5} > 1$, then we have that $|X : M|_{5} = 5^2$ (see [7, Theorems 1.3, 1.4, 1.5 and 3.5]). Arguing as above, we get $|P_{X,G}(-1)|_{5} = |P_{X,5}^{(s)}(-1)|_{5} = 25$, thus $P_{X,G}(-1) \neq 0$. □

**Proposition 41.** Assume $n \geq 3$. We have that $|P_{X,G}(-1)|_{p} = q^{l-2}|p|$, with $L$ as in Table 4. Hence $P_{X,G}(-1) \neq 0$.

**Proof.** We have already considered the case $G \cong PSL_3(2) \cong PSL_2(7)$. Using [5], the result holds in cases $L$ and $U$ with $(n, q) = (4, 2)$, and in case $S$ with $(n, q) = (6, 2)$.

For the rest of the proof, suppose that if case $L$ or $U$ holds, then $(n, q) \neq (4, 2)$ and if case $S$ holds, then $(n, q) \neq (6, 2)$. Moreover, assume $G \not\cong PSL_3(2)$. Recall that we defined

$$\beta_p(X) = \log_q \min\{|X : H|_{p}: H < X, \ |X : H|_{p} > 1, \ HG = X, \ \mu_X(H) \neq 0\}.$$

By Lemma 6, we have that $a_k(X, G)$ is a multiple of $k$. So, since

$$P_{X,G}(-1) = P_{X,G}^{(s)}(-1) + \sum_{p|k} a_k(X, G) p,$$
in order to prove the proposition, it is enough to show that

\[ \left| P_{X,G}^{(p)}(-1) \right|_p < q^{2\beta_p(X)}. \]

By Proposition 34 and Theorem 15, we obtain:

\[ \left| P_{X,G}^{(p)}(-1) \right|_p = \left| P_G^{(p)}(-1) \right|_p = q^L |2|_p. \]

By Theorem 18 and some straightforward computations, we have that

\[ q^{2\beta_p(X)} \geq q^{2\beta_p(X)} > q^L |2|_p. \]

Thus we conclude that \( \left| P_{X,G}(-1) \right|_p = |2|_p q^L. \)

References