Groups with few \( p' \)-character degrees

Eugenio Giannelli

\textit{Dipartimento di Matematica e Informatica}

\textit{U. Dini, Viale Morgagni 67/a}

\textit{Firenze, Italy}

eugenio.giannelli@unifi.it

Noelia Rizo

\textit{Departament de Matemàtiques}

\textit{Universitat de València}

\textit{46100 Burjassot, València, Spain}

noelia.rizo@uv.es

A. A. Schaeffer Fry

\textit{Department of Mathematical and Computer Sciences}

\textit{Metropolitan State University of Denver}

\textit{Denver, CO 80217, USA}

aschaef6@msudenver.edu

Abstract

We prove a variation of Thompson’s Theorem. Namely, if the first column of the character table of a finite group \( G \) contains only two distinct values not divisible by a given prime number \( p > 3 \), then \( O_{p'}(G) = 1 \). This is done by using the classification of finite simple groups.

\textit{Mathematics Classification Number:} 20C15, 20C33

\textit{Keywords:} Character degrees, Finite simple groups.

1 Introduction

Many problems in the character theory of finite groups deal with character degrees and prime numbers. For instance, the Itô-Michler theorem ([13],[20]) asserts that a prime \( p \) does not divide \( \chi(1) \) for any \( \chi \in \text{Irr}(G) \) if and only if the group \( G \) has a normal abelian Sylow \( p \)-subgroup. As usual, we denote by \( \text{Irr}(G) \) the set of complex irreducible characters of \( G \) and by \( \text{Irr}_{p'}(G) \) the subset of \( \text{Irr}(G) \) consisting of irreducible characters of degree coprime to \( p \). If we write \( \text{cd}(G) \) for the set of character degrees of \( G \) and \( \text{cd}_{p'}(G) \) for the subset of \( \text{cd}(G) \) consisting of those character degrees not divisible by \( p \), the Itô-Michler theorem deals with the situation when \( \text{cd}_{p'}(G) = \text{cd}(G) \). At the opposite end of the spectrum, we have a theorem of Thompson ([29]) showing that if \( \text{cd}_{p'}(G) = \{1\} \), then \( G \) has a normal \( p \)-complement. In [1], Berkovich showed that in this situation, \( G \) is solvable, using the Classification of Finite Simple Groups.

In [9], a variation on Thompson’s theorem for two primes is studied. Namely, it is shown there that if \( G \) has only one character with degree coprime to two different primes, then \( G \) is trivial. In this paper, we offer another variation on Thompson’s theorem by describing finite groups \( G \) such that \( |\text{cd}_{p'}(G)| = 2 \). Thompson’s theorem may equivalently be viewed in terms of \( O_{p'}(G) \), where \( O_{p'}(G) = O_{p'}(O_p(G)) \). Namely, Thompson’s theorem says that if \( \text{cd}_{p'}(G) = \{1\} \) then \( O_{p'}(G) = 1 \). Similarly, we will denote by \( O_{p'q'}(G) \) the group \( O_{p'}(O_{q'}(G)) \) and prove a corresponding statement for the case \( |\text{cd}_{p'}(G)| = 2 \).

**Theorem A.** Let \( G \) be a finite group and let \( p > 3 \) be a prime. Suppose that \( |\text{cd}_{p'}(G)| = 2 \). Then \( G \) is solvable and \( O_{p'q'}(G) = 1 \).
We remark that Theorem A answers Problem 5.3 of [21], which suggested that groups satisfying $|\text{cd}_p(G)| = 2$ must be $p$-solvable. It is already said in [21] that there are many examples of non-solvable groups satisfying $|\text{cd}_2(G)| = 2$ (the symmetric group on 5 letters is the smallest one). For $p = 3$, we have that if $G$ is the automorphism group of $\text{PSL}_2(27)$, then $|\text{cd}_3(G)| = 2$, for instance.

We also remark that, for a given prime $p$, we can find examples of non-solvable groups $G$ satisfying $|\text{cd}_p(G)| = 3$. For instance, the alternating group on 5 letters, $A_5$, satisfies that $|\text{cd}_p(A_5)| = 3$ for $p = 2, 3, 5$. For $p > 5$, we have that $|\text{cd}_p(\text{PGL}_2(p))| = 3$.

Further, unlike many statements on character degrees, Theorem A does not immediately seem to correspond to a dual statement for conjugacy classes. For instance, we observe that $A_5$ has exactly two conjugacy classes of size coprime to 5.

As in the case of the result of Berkovich, our proof of Theorem A uses the Classification of Finite Simple Groups. In particular, we need the following result on simple groups.

**Theorem B.** Let $S$ be a non-abelian simple group and let $p > 3$ be a prime. Then there exist nonlinear $\alpha, \beta \in \text{Irr}_p(S)$ such that $\alpha$ extends to $\text{Aut}(S)$, $\beta(1) \nmid \alpha(1)$, and $\beta$ is $P$-invariant for every $p$-subgroup $P \leq \text{Aut}(S)$.

We obtain Theorem B as a corollary to the following stronger statement, after dealing with the exceptions separately.

**Theorem C.** Let $S$ be a non-abelian simple group and let $p > 3$ be a prime dividing $|S|$. Assume that $S$ is not one of $A_5, A_6$ for $p = 5$ or one of $\text{PSL}_2(q), \text{PSL}_3(q), \text{PSP}_4(q)$, or $2^2B_2(q)$. Then there exist two nontrivial characters $\alpha, \beta \in \text{Irr}_p(S)$ such that $\alpha(1) \neq \beta(1)$ and both $\alpha$ and $\beta$ extend to $\text{Aut}(S)$.

This article is structured as follows. In Section 2, we prove Theorem A assuming that Theorem B is true and show that Theorem C (and hence Theorem B) holds for sporadic groups. In Section 3, we prove Theorem B for the alternating groups. Finally, in Section 4, we prove Theorem B for simple groups of Lie type and we conclude by using the Classification of Finite Simple Groups.

**Acknowledgement** The authors would like to thank Gabriel Navarro for many useful conversations on this topic. They would also like to thank the Mathematisches Forschungsinstitut Oberwolfach and the organizers of the 2019 MFO workshop “Representations of Finite Groups”, where part of this work was completed. The second author is supported by a Fellowship FPU of Ministerio de Educación, Cultura y Deporte. The third author is partially supported by a grant from the National Science Foundation (Award No. DMS-1801156).

## 2 Reduction to simple groups

In this section we assume Theorem B and we prove Theorem A. We will need the following result, which is essentially Lemma 4.1 of [23]. We provide a proof for the reader’s convenience.

**Lemma 2.1.** Let $Q$ be a finite group acting on a finite group $N$ and suppose that $N = S_1 \times \cdots \times S_t$, where the $S_i$'s are transitively permuted by $Q$. Let $Q_1$ be the stabilizer of $S_1$ in $Q$ and let $T = \{a_1, \ldots, a_t\}$ be a transversal for the right cosets of $Q_1$ in $Q$ with $S_i = S_1^{a_i}$. Let $\psi \in \text{Irr}(S_1)$ be $Q_1$-invariant. Then

$$\gamma = \psi^{a_1} \times \psi^{a_2} \times \cdots \times \psi^{a_t} \in \text{Irr}(N)$$

is $Q$-invariant.
Proof. First, we have that $Q$ acts transitively on $T$, and we use the notation $a_i \cdot q$ to indicate the unique element of $T$ such that $Q_1(a_i, q) = Q_1(a_i, q)$ for $a_i \in T$ and $q \in Q$. Now notice that $Q$ acts on $N$ as follows: if $q \in Q$ and $S_i^q = S_j$ (that is, if $a_i \cdot q = a_j$), then $(x_1, \ldots, x_t)^q = (y_1, \ldots, y_t)$, where $y_j = x_j^q$. Let $q \in Q$, and let $\sigma \in S_i$ be the permutation defined by $a_i \cdot q = a_{\sigma(i)}$, so $x_i^q = y_{\sigma(i)}$. Then

$$\gamma^{-1}(x_1, \ldots, x_t) = (\psi^{a_1} \times \psi^{a_2} \times \cdots \times \psi^{a_t})^{-1}(y_1, \ldots, y_t) = \psi^{a_1}(y_1) \cdots \psi^{a_t}(y_t) = \psi^{a_1}(x_{\sigma^{-1}(1)}) \cdots \psi^{a_t}(x_{\sigma^{-1}(t)})$$

$$= \psi^{a_1 q^{-1}}(x_{\sigma^{-1}(1)}) \cdots \psi^{a_t q^{-1}}(x_{\sigma^{-1}(t)})$$

$$= \psi^{a_1 q^{-1}}(x_{\sigma^{-1}(1)}) \cdots \psi^{a_t q^{-1}}(x_{\sigma^{-1}(t)})$$

$$= \psi^{a_1 q^{-1}}(x_{\sigma^{-1}(1)}) \cdots \psi^{a_t q^{-1}}(x_{\sigma^{-1}(t)})$$

$$= \gamma(x_1, \ldots, x_t).$$

\[ \square \]

**Theorem 2.2.** Let $G$ be a finite group and let $p > 3$ be a prime. Suppose that $|\text{cd}_p(G)| = 2$. Then $G$ is solvable.

**Proof.** We argue by induction on $|G|$. Write $\text{cd}_p(G) = \{1, m\}$. Let $N$ be a minimal normal subgroup of $G$. Then either $N$ is abelian or $N$ is semisimple. It is clear that $|\text{cd}_p(G/N)| \leq |\text{cd}_p(G)|$. Hence by induction and Proposition 9 of [1] we have that $G/N$ is solvable.

Suppose that $N = S_1 \times S_2 \times \cdots \times S_t$ where $S_i \cong S$, a non-abelian simple group. Write $H = \text{N}_G(S_1)$ and $S_i = S_i^H$, where $G = \bigcup_{i=1}^t Hx_i$ is a disjoint union. By Theorem B, there exist $\alpha \in \text{Irr}_p(S_1)$ with $\alpha(1) \neq 1$, extending to $\text{Aut}(S_1)$, and $\beta \in \text{Irr}_p(S_1)$ $P$-invariant for every $p$-subgroup $P \leq \text{Aut}(S_1)$, with $\beta(1) \neq \alpha(1)$.

Now let $\theta = \alpha x_1 \times \cdots \times \alpha x_t \in \text{Irr}(N)$. By Lemma 5 of [2] we have that $\theta$ extends to $G$. Let $\tilde{\theta} \in \text{Irr}(G)$ extending $\theta$. Then $\tilde{\theta}(1) = \theta(1) = \alpha(1)^t$ is not divisible by $p$ and hence, by hypothesis, $\tilde{\theta}(1) = m$.

Let $Q \in \text{Syl}_p(G)$ and write $\{T_1, \ldots, T_r\}$ for a set of representatives of the action of $Q$ on $\{S_1, \ldots, S_t\}$, with $T_1 = S_1$. Write $O(T_i)$ for the orbit of $T_i$ under the action of $Q$. Rearrange $S_1, S_2, \ldots, S_t$ in such a way that $O(T_1) = \{S_1, S_2, \ldots, S_{l_1}\}$, $O(T_2) = \{S_{l_1+1}, \ldots, S_{l_1}\}$, etc. Notice that $l_1 + l_2 + \cdots + l_r = t$. Write $N_1 = S_1 \times S_2 \times \cdots \times S_{l_1}$, $N_2 = S_{l_1+1} \times \cdots \times S_{l_2}$, etc. Notice that $Q$ normalizes $N_i$ and $N = N_1 \times N_2 \times \cdots \times N_r$.

Now, let $U = \{q_1, q_2, \ldots, q_t\}$ be a transversal for the right cosets of $Q_1 = Q \cap N_G(S_1)$ in $Q$ such that $S_j = S_j^q$ for $j = 1, 2, \ldots, l_1$, and define $\gamma_1 \in \text{Irr}(N_1)$ as follows:

$$\gamma_1 = \beta q_1 \times \beta q_2 \times \cdots \times \beta q_{l_1} \in \text{Irr}(N_1)$$

By Lemma 2.1 we have that $\gamma_1$ is $Q$-invariant. If $T_1 = S_{1}^{x_1}$ proceed analogously with $\beta x_k$ to define $\gamma_k \in \text{Irr}(N_k)$ (notice that $\beta x_k$ is $Q_k$-invariant, where $Q_k = N_G(S_{1}^{x_k}) \cap Q$). By Lemma 2.1, we have that $\gamma_i$ is $Q$ invariant for all $i = 1, 2, \ldots, r$.

Now, let

$$\gamma = \gamma_1 \times \cdots \times \gamma_r \in \text{Irr}(N).$$

We claim that $\gamma$ is $Q$-invariant. Indeed, let $q \in Q$ and let $n_1 n_2 \cdots n_r \in N$, with $n_i \in N_i$. Since $Q$ normalizes $N_i$ for all $i$, we have:

\[ \]
Notice that $\gamma(1) = \beta(1)^4$ and hence, $\gamma \in \text{Irr}_p(N)$. Then $\gcd(\alpha(\gamma) \gamma(1), [QN : N]) = 1$ and since $\gamma$ is $Q$-invariant, we have that $\gamma$ extends to $\hat{\gamma} \in \text{Irr}(NQ)$. Since $\hat{\gamma}(1)$ and $[G : NQ]$ are not divisible by $p$, there exists $\chi \in \text{Irr}(G[\hat{\gamma}])$ of $p'$-degree. But $\chi \in \text{Irr}(G[\gamma])$, and hence $\gamma(1) | \chi(1)$. Since $\gamma(1) \neq 1$, we have that $\chi(1) \neq 1$, and therefore $\chi(1) = m$. Hence $\beta(1)^{1} = \gamma(1)$ divides $\chi(1) = m = \alpha(1)^4$, and $\beta(1) | \alpha(1)$. This contradiction shows that $N$ is abelian and hence $G$ is solvable.

The following is the second part of Theorem A.

**Theorem 2.3.** Let $G$ be a finite group and let $p > 3$ be a prime. Suppose that $|\text{cd}_{p'}(G)| = 2$. Then $O^{p'\text{pp}'}(G) = 1$.

**Proof.** Let $K = O^p(G)$, $L = O^{pp}(K) = O^{pp}(G)$, $N = O^p(L) = O^{ppp}(G)$ and $W = O^{pp}(N) = O^{p'pp'}(G)$, and write $\text{cd}_{p'}(G) = \{1, m\}$. Let $W/X$ be a chief factor of $G$. Then $W/X$ is a minimal normal subgroup of $G/X$ and since $G$ is solvable, we have that $W/X$ is abelian. Now, if a prime $q$, different from $p$, divides $[W : X]$, we have that $W/X$ has a normal $q$-complement $H/X$ and $[W : H]$ is not divisible by $p$, a contradiction with the fact that $W = O^{pp}(G)$. Hence $W/X$ is a $p'$-group.

Now, if $X > 1$, since $\text{cd}_{p'}(G/X) \subseteq \text{cd}_{p'}(G)$, by induction and Thompson’s theorem we have that $O^{p'\text{pp}'}(G/X) = X$ and hence $W = X$, a contradiction. Therefore we may assume that $X = 1$.

Let $Y$ be a complement of $W$ in $N$. By the Frattini argument, we have that $G = N\text{N}_C(Y) = WN_C(Y)$. Since $W$ is abelian, we have that $\text{cd}_W(Y) \leq G$ and then $W \cap \text{N}_C(Y) = YW(Y) = 1$. Hence $W$ is complemented in $G$ and by Problem 6.18 of [11], every $\lambda \in \text{Irr}(W)$ extends to $G\chi$.

Let $P$ be a Sylow $p'$-subgroup of $G$, let $1_{W} = \lambda_1, \lambda_2, ..., \lambda_i$ be representatives of the action of $P$ on $\text{Irr}(W)$ and let $O_i$ be the $P$-orbit of $\lambda_i$. Then

$$1 + \sum_{i=2}^{t} |O_i| \lambda_i(1)^2 = \sum_{i=1}^{t} |O_i| \lambda_i(1)^2 = \sum_{\chi \in \text{Irr}(W)} \lambda(1)^2 = [W : 1] \mod p.$$ 

Then there exists $i > 1$ such that $|O_i| \lambda_i(1)^2$ is not divisible by $p$. Since $|O_i| = |P : P_{\lambda_i}|$, we have that $|O_i| = 1$ and hence there is $1_{W} \neq \lambda \in \text{Irr}(W)$ $P$-invariant. Let $T = G\chi$ and let $\hat{\lambda}$ be an extension of $\lambda$ to $T$. Then $\lambda^G \in \text{Irr}(G)$ and $\hat{\lambda}^G(1) = [G : T]$. But $P \subseteq T$ and hence $[G : T] = p'$. By hypothesis, $|G : T| = m$.

If $\lambda$ is $N$ invariant, we have that

$$\lambda(n^{-1}w^{-1}nw) = \lambda^{n}(w^{-1})\lambda(w) = \lambda(1)$$

and $[N, W] \subseteq \ker(\lambda)$. But $[N, W] \leq G$ and $[N, W] \subseteq W$. Since $W$ is a minimal normal subgroup of $G$ we have that $[N, W] = W$ or $[N, W] = 1$. If $[N, W] = 1$, we have that $[Y, W] \subseteq [N, W] = 1$ and hence by Lemma 4.28 of [12] we have that $W = 1$ and we are done. Thus we may assume that $[N, W] = W$. Then $W \subseteq \ker(\lambda)$, which contradicts the fact that $\lambda \neq 1_{W}$. Hence $N \nsubseteq T$.

If $\text{cd}_{p'}(G/N) = \{1, m\}$, by Thompson’s theorem we are done. Then we may assume that $\text{cd}_{p'}(G/N) = \{1, m\}$. Let $\chi \in \text{Irr}(G/N)$ with $\chi(1) = m$ and let $\epsilon \in \text{Irr}(TN/N)$ lying under $\chi$ of $p'$-degree. Since $N \subseteq \ker(\epsilon)$, we have that $\epsilon_T$ is irreducible and $\rho = \epsilon_T \hat{\lambda} \in \text{Irr}(T\lambda)$. Thus $\rho^G \in \text{Irr}(G|\lambda)$ and

$$\rho^G(1) = [G : T]\epsilon(1) = [G : T]\epsilon(1)$$

is not divisible by $p$. Then $|G : T|\epsilon(1) = m = |G : T|$, and $\epsilon$ is linear. Now, since $\chi$ is an irreducible constituent of $\epsilon^G$ we have that

$$m = \chi(1) \leq \epsilon^G(1) = |G : TN| < |G : T| = m.$$ 

This contradiction shows that $W = 1$. 

\[ \square \]
We end this section with the following, which can be seen using the GAP Character Table Library.

**Proposition 2.4.** Let $S$ be a simple sporadic group or the Tits group $^2F_4(2)'$. Then Theorem C holds for $S$.

### 3 Alternating Groups

The aim of this section is to prove Theorem B for alternating groups. We achieve this goal by proving the slightly stronger Proposition 3.5.

We begin by recalling some basic facts in the representation theory of symmetric and alternating groups. The irreducible characters of the symmetric group $S_n$ are labelled by partitions of $n$. We let $\mathcal{P}(n)$ be the set of partitions of $n$. Given $\lambda = (\lambda_1, \ldots, \lambda_r) \in \mathcal{P}(n)$, we denote by $\chi^\lambda$ the corresponding irreducible character of $S_n$. We sometimes use the notation $\lambda \vdash n$ to say that $\lambda \in \mathcal{P}(n)$ and we use the symbol $\lambda \vdash \mu \nvdash n$ to mean that $\chi^\lambda \in \text{Irr}_p(S_n)$, for some prime number $p$. Given $\lambda \in \mathcal{P}(n)$ we let $\lambda'$ be the conjugate partition of $\lambda$. We recall that the restriction to the alternating group $(\chi^\lambda)_{A_n}$ is irreducible if, and only if, $\lambda \neq \lambda'$ (see [14, Thm. 2.5.7]). Moreover, if $\lambda, \mu \in \mathcal{P}(n)$ then $(\chi^\lambda)_{A_n} = (\chi^\mu)_{A_n}$ if, and only if, $\mu \in \{\lambda, \lambda'\}$.

Given $\lambda \in \mathcal{P}(n)$ we denote by $[\lambda]$ its corresponding Young diagram. The node $(i, j)$ of $[\lambda]$ lies in row $i$ and column $j$. As usual, we denote by $h_{i,j}(\lambda)$ the hook-length corresponding to $(i,j)$. We let $\mathcal{H}(\lambda)$ be the multiset of hook-lengths in $\lambda$. By the hook-length formula [14, Thm. 2.3.21] we know that $\chi^\lambda(1) = n!(\prod_{h \in \mathcal{H}(\lambda)} h)^{-1}$.

Given $e \in \mathbb{N}$ we let $\mathcal{H}^e(\lambda)$ be the multiset of hook-lengths in $\lambda$ that are divisible by $e$. The $e$-core $C_e(\lambda)$ of $\lambda$ is the partition of $n - e|\mathcal{H}^e(\lambda)|$ obtained from $\lambda$ by successively removing hooks of length $e$. A useful consequence of work of Macdonald [16] is stated here (see [9, Lemma 2.4] for a short proof).

**Lemma 3.1.** Let $p$ be a prime and let $n$ be a natural number with $p$-adic expansion $n = \sum_{j=0}^k a_j p^j$. Let $\lambda$ be a partition of $n$. Then $\lambda \vdash \mu \nvdash n$ if and only if $|\mathcal{H}^p(\lambda)| = a_k$ and $C_p^p(\lambda) \vdash \mu' - p^k n - a_k p^k$.

We let $\mathcal{L}(n) = \{\lambda \in \mathcal{P}(n) \mid \lambda_2 \leq 1\}$. Elements of $\mathcal{L}(n)$ are usually called hook partitions. We denote by $\mathcal{L}_p(n)$ the set consisting of all those hook partitions of $n$ whose corresponding irreducible character of $S_n$ has degree coprime to $p$. In the following proposition we completely describe the elements of $\mathcal{L}_p(n)$ and we give a closed formula for $|\mathcal{L}_p(n)|$. This might be known to experts in the area, but we were not able to find an appropriate reference in the literature.

**Proposition 3.2.** Let $n \in \mathbb{N}$ and let $n = \sum_{j=1}^k a_j p^j$ be its $p$-adic expansion, where $0 \leq n_1 < n_2 < \cdots < n_k$ and $1 \leq a_j \leq p - 1$ for all $j \in \{1, \ldots, k\}$. Then

$$|\mathcal{L}_p(n)| = a_1 p^{n_1} \cdot \prod_{j=2}^k (a_j + 1).$$

Moreover, for $\lambda, \mu \in \mathcal{L}(n)$ we have that $\chi^\lambda(1) = \chi^\mu(1)$ if and only if $\lambda \in \{\mu, \mu'\}$.

**Proof.** We proceed by induction on $k$, the $p$-adic length of $n$. Suppose first that $k = 1$. If $n_1 = 0$ then $n = a_1 < p$ and therefore $|\mathcal{L}_p(n)| = |\mathcal{L}(n)| = a_1$. On the other hand, if $n_1 > 0$ and $\lambda \in \mathcal{L}(n)$ then $h_{(1,1)}(\lambda) = n = a_1 p^{n_1}$. It follows that $|\mathcal{H}^{p^{n_1}}(\lambda)| = a_1$ and that $C_p^{p^{n_1}}(\lambda) = \emptyset$. Using Lemma 3.1 we conclude that $\lambda \in \mathcal{L}_p(n)$ and hence that $\mathcal{L}(n) = \mathcal{L}_p(n)$. Therefore, we have that
$|\mathcal{L}_p(n)| = a_1 p^{n_1}$. Let us now assume that $k \geq 2$. Let $m := n - a_k p^{n_k}$ and let $\gamma \in \mathcal{L}_p(m)$. We denote by $A_\gamma$ the subset of $\mathcal{L}_p(n)$ defined as follows:

$$A_\gamma = \{ \lambda \in \mathcal{L}_p(n) \mid C_p^{n_k}(\lambda) = \gamma \}.$$

Observing that the $p^{n_k}$-core of a hook partition is a hook partition and using Lemma 3.1 we deduce that

$$\mathcal{L}_p(n) = \bigcup_{\gamma \in \mathcal{L}_p(m)} A_\gamma,$$

where the above union is clearly disjoint. Given $\gamma \in \mathcal{L}_p(m)$ we notice that the set $A_\gamma$ consists of all those hook partitions of $n$ that are obtained from $\gamma$ by adding $x$-many $p^{n_k}$-hooks to the first row of $[\gamma]$ and $(a_k - x)$-many to the first column of $[\gamma]$. In particular

$$A_\gamma = \{ \lambda_x \mid x \in \{0, 1, \ldots, a_k\} \}, \text{ where } \lambda_x = (\gamma_1 + xp^{n_k}, 1^{n - \gamma_1 - xp^{n_k}}).$$

We conclude that $|A_\gamma| = a_k + 1$, for all $\gamma \in \mathcal{L}_p(m)$. This, combined to the inductive hypothesis shows that:

$$|\mathcal{L}_p(n)| = |\mathcal{L}_p(m)| \cdot (a_k + 1) = (a_1 p^{n_1} \prod_{j=2}^{k-1} (a_j + 1)) \cdot (a_k + 1) = a_1 p^{n_1} \cdot \prod_{j=2}^{k} (a_j + 1).$$

The second statement is a consequence of a very well known fact. Namely that for $\lambda = (n - x, 1^x) \in \mathcal{L}(n)$ we have that $\chi_{\lambda}(1) = \left(\frac{n - 1}{x}\right)$. (This can be easily deduced from the hook length formula). 

Given a natural number $n$ and $S \subseteq \mathcal{P}(n)$ we let $\text{cd}(S) = \{\chi_{\lambda}(1) \mid \lambda \in S\}$. Moreover, we let $\text{cd}_{p}^{\text{ext}}(A_n)$ be the set consisting of all the degrees of irreducible characters of $A_n$ of degree coprime to $p$ that extend to $S_n$. Here we find a lower bound to $|\text{cd}_{p}^{\text{ext}}(A_n)|$.

**Proposition 3.3.** Let $n \in \mathbb{N}$. Then $|\text{cd}_{p}^{\text{ext}}(A_n)| \geq |\mathcal{L}_p(n)|/2$.

**Proof.** A hook-partition $\lambda \in \mathcal{L}(n)$ is such that $\lambda = \chi'$ if and only if $\lambda$ is odd and $\lambda = ((n + 1)/2, 1^{(n-1)/2})$. Moreover, the set $\mathcal{L}_p(n)$ is clearly closed under conjugation of partitions. It follows that $((n + 1)/2, 1^{(n-1)/2}) \in \mathcal{L}_p(n)$ if and only if $|\mathcal{L}_p(n)|$ is odd. Let $S = \{ \lambda \in \mathcal{L}_p(n) \mid \lambda_1 > \lambda'_1 \}$. The above discussion shows that $|S| = |\mathcal{L}_p(n)|/2$. The second statement of Proposition 3.2 implies that $|\text{cd}(S)| = |\mathcal{L}_p(n)|/2$. We observe that if $\lambda \in S$ then $(\chi^{s})_{A_n}$ is irreducible of degree coprime to $p$ and clearly extends to $S_n$. In other words, $(\chi^{s})_{A_n}(1) \in \text{cd}_{p}^{\text{ext}}(A_n)$. Moreover, for $\lambda, \mu \in S$ we have that $(\chi^{s})_{A_n}(1) = (\chi^{t})_{A_n}(1)$ if and only if $\lambda = \mu$. Thus we conclude that $|\text{cd}_{p}^{\text{ext}}(A_n)| \geq |\text{cd}(S)| = |S| = |\mathcal{L}_p(n)|/2$, as desired. 

In order to verify that Theorem C holds for alternating groups, we aim of to show that $|\text{cd}_{p}^{\text{ext}}(A_n)| \geq 3$, for all $n \geq 7$. Propositions 3.2 and 3.3 give in most of the cases a much larger lower bound than the one needed. In fact, Proposition 3.5 below is a consequence of these propositions, together with the analysis of the cases where $n \in \mathbb{N}$ is such that $|\mathcal{L}_p(n)|/2 \leq 2$.

The following facts are easy applications of the hook-length formula and are important to deal with the few exceptional cases mentioned above.

**Lemma 3.4.** Let $n, t, c \in \mathbb{N}$ be such that $c \in \{2, 3\}$, $n \geq 4 + c$ and $0 \leq t \leq n - 2c$. Let $\lambda(t)$ be the partition of $n$ defined as $\lambda(t) := (n - c - t, c, t^1) \in \mathcal{P}(n)$. If $0 \leq t \leq \left[\frac{n-\frac{1}{2}-c}{2}\right]$, then $\chi_{\lambda(t)}(1) < \chi_{\lambda(t+1)}(1)$. 

6
Proof. To ease the notation we let $m := \lambda(t)_{1} = n - c - t$. The (strange) hypothesis $0 \leq t \leq \left\lfloor \frac{n-1-c}{2} \right\rfloor$ is equivalent to say that $\lambda(t+1)_{1} \geq \lambda(t+1)^{(1)}$. In turn this is equivalent to say that $0 \leq t \leq m-4$.

If $c = 2$ then using the hook length formula we observe that

$$\frac{\chi^{\lambda(t+1)}(1)}{\chi^{\lambda}(1)} = \frac{m(m-2)(t+2)}{(m-1)(t+3)(t+1)} \geq \frac{(m-2)^2}{(m-1)^2} \cdot \frac{m}{m-3} > 1,$$

where the first inequality is obtained by replacing $t$ with $m - 4$. The proof of the statement for $c = 3$ is completely similar and therefore it is omitted.

We care to remark that a more general statement (with arbitrary $c \in \mathbb{N}$) does not hold, as for instance is shown by the pair $(6, 5, 1, 1)$ and $(5, 5, 1, 1)$. 

**Proposition 3.5.** Let $n \geq 7$ be a natural number and let $p > 3$ be a prime, then $|\text{cd}^{\text{ext}}_{P}(A_{n})| \geq 3$.

Proof. Let $n = \sum_{j=1}^{k} a_{j}p^{n_{j}}$ be the $p$-adic expansion of $n$, where $0 \leq n_{1} < n_{2} < \cdots < n_{k}$ and $1 \leq a_{j} \leq p - 1$ for all $j \in \{1, \ldots, k\}$. Suppose that

$$n \notin \{1 + p^{n_{2}} + p^{n_{3}}, 2 + p^{n_{2}}, 1 + a_{2}p^{n_{2}} \mid a_{2} \in \{1, 2, 3\}\},$$

since $n \geq 7$, then $|\text{cd}^{\text{ext}}_{P}(A_{n})| \geq 3$, by Propositions 3.2 and 3.3. To conclude the proof, we analyze the remaining cases one by one.

Suppose first that $n = 1 + ap^{k}$, for some $a \in \{1, 2, 3\}$. Let $t \in \mathbb{N}$ be such that $0 \leq t \leq \left\lfloor \frac{n-6}{2} \right\rfloor$ and let $\lambda(t) = (n - 2 - t, 2, 1^{t})$. Observe that $\lambda(t) \neq (\lambda(t))^{(1)}$. By Lemma 3.4 we have that

$$1 < \chi^{\lambda(0)}(1) < \chi^{\lambda(1)}(1) < \cdots < \chi^{\lambda(\left\lfloor \frac{n-6}{2} \right\rfloor)}(1) < \chi^{\lambda(\left\lfloor \frac{n-2}{2} \right\rfloor+1)}(1).$$

Moreover, since $h_{(1,1)}(\lambda(t)) = ap^{k}$ and $C_{P}(\lambda(t)) = (1)$, then Lemma 3.1 implies that $\chi^{\lambda(t)} \in \text{Irr}_{P}(S_{n})$, for all $t \in \{0, 1, \ldots, \left\lfloor \frac{n-6}{2} \right\rfloor\}$. Since $n = 1 + ap^{k} \geq 7$ it follows that $n \geq 8$ and hence that $\left\lfloor \frac{n-6}{2} \right\rfloor \geq 1$. Since $\lambda(t)$ is never equal to the trivial partition, we conclude that $|\text{cd}^{\text{ext}}_{P}(A_{n})| \geq 3$.

Let $k, h \in \mathbb{N}$ be such that $k < h$, and suppose that $n = 1 + p^{k} + p^{h}$. To ease the notation we let $m = 1 + p^{k}$. By Lemma 3.1 it is easy to observe that

$$P_{P}(m) = \{(p^{k} - t, 2, 1^{t-1}) \mid t \in \{1, \ldots, p^{k} - 2\}\} \cup \{(m), (1^{m})\}.$$ 

Since $p \geq 5$ we have that $|P_{P}(m)| \geq 3$. For each $\gamma \in P_{P}(m)$ we let

$$\lambda(\gamma) := (\gamma_{1} + p^{h}, \gamma_{2}, \ldots, \gamma_{t}) \in P(n).$$

Using Lemma 3.1 it is now routine to check that $\lambda(\gamma) \nmid \gamma \ n$. Moreover, since $p^{h} > m$ we have that $\lambda(\gamma) \neq (\lambda(\gamma))^{(1)}$ for all $\gamma \in P_{P}(m)$. Therefore, using again Lemma 3.4 we conclude that also in this case $|\text{cd}^{\text{ext}}_{P}(A_{n})| \geq 3$.

Finally suppose that $n = 2 + p^{k}$, for some $k \in \mathbb{N}$. Let $t \in \mathbb{N}$ be such that $0 \leq t \leq \left\lfloor \frac{n-7}{2} \right\rfloor$ and let $\lambda(t) = (n - 3 - t, 3, 1^{t})$. Observe that $\lambda(t) \neq (\lambda(t))^{(1)}$. Since $h_{(1,1)}(\lambda(t)) = p^{k}$ and $C_{P}(\lambda(t)) = (2)$, by Lemma 3.1 we deduce that $\chi^{\lambda(t)} \in \text{Irr}_{P}(S_{n})$, for all $t \in \{0, 1, \ldots, \left\lfloor \frac{n-7}{2} \right\rfloor\}$. If $p^{k} \neq 5$ then $n \geq 9$ and hence $\left\lfloor \frac{n-7}{2} \right\rfloor \geq 1$. Since $\lambda(t)$ is never equal to the trivial partition, using Lemma 3.4 we conclude that $|\text{cd}^{\text{ext}}_{P}(A_{n})| \geq 3$. If $p^{k} = 5$ then direct verification shows that $|\text{cd}^{\text{ext}}_{P}(A_{7})| \geq 3$.

We are now ready to prove Theorem B.

**Corollary 3.6.** Theorem B holds for all simple non-abelian alternating groups.
Proof. Let \( n \geq 5 \). Since \( p > 3 \) a Sylow \( p \)-group \( P \) of \( \text{Aut}(A_n) \) is necessarily contained in \( A_n \). Hence all irreducible characters of \( A_n \) are \( P \)-invariant. With this in mind, we observe that for all \( n \geq 7 \) Theorem B follows from Proposition 3.5. If \( n = 5 \) then (in accordance with the notation used in the statement of Theorem B) we choose \( \alpha = (\chi^{(4,1)})_{A_5} \) and \( \beta \) an irreducible constituent of \( (\chi^{(3,1,1)})_{A_5} \). Similarly for \( n = 6 \) we observe that Theorem B holds by choosing \( \alpha = (\chi^{(4,2)})_{A_6} \) and \( \beta \) an irreducible constituent of \( (\chi^{(3,2,1)})_{A_6} \).

\[ \square \]

4 Simple Groups of Lie Type

Throughout this section, we will adopt the following notation. Let \( S \) be a simple group of Lie type, by which we mean that there is a simply connected simple linear algebraic group \( G \) defined over \( \mathbb{F}_q \) such that \( S = G/Z(G) \), where \( G := G^F \) is the group of fixed points of \( G \) under a Steinberg endomorphism \( F \). Here \( \overline{\mathbb{F}}_q \) is an algebraic closure of the field \( \mathbb{F}_q \) with \( q \) elements, and \( q \) is a power of some prime. We further write \( G^* = (G^*)^F \), where \( (G^*, F^*) \) is dual to \( (G, F) \).

We denote by \( \iota : G \hookrightarrow \hat{G} \) a regular embedding, as in [5, Chapter 15], and let \( \iota^* : \hat{G} \rightarrow G^* \) be the dual surjection of algebraic groups. When \( F \) is a Frobenius endomorphism, we may extend \( F \) to a Frobenius endomorphism on \( \hat{G} \), which we also denote by \( F \), and we let \( \hat{G} := \hat{G}^F \) and \( \hat{G}^* := (\hat{G}^*)^F \) be the corresponding group of Lie type and its dual, respectively. Then \( G \triangleleft \hat{G} \) and the automorphisms of \( G \) are generated by the inner automorphisms of \( \hat{G} \) (known as inner-diagonal automorphisms of \( G \)) together with graph and field automorphisms.

When \( G \) is of type \( A_{n-1} \), we use the notation \( \text{PSL}_n^\epsilon(q) \) with \( \epsilon \in \{ \pm 1 \} \) to denote \( \text{PSL}_n(q) \) for \( \epsilon = 1 \) and \( \text{PSU}_n(q) \) for \( \epsilon = -1 \). We will also use the corresponding notation for \( \text{SL}_n(q), \text{GL}_n(q), \) and \( \text{PGL}_n(q) \).

The goal of this section is to prove the following, which is Theorem B for groups of Lie type.

**Theorem 4.1.** Let \( S \) be a simple group of Lie type defined over \( \mathbb{F}_q \) and let \( p > 3 \) be a prime dividing \( |S| \). Assume that \( S \) is not one of \( \text{PSL}_2(q), \text{PSL}_3(q), \text{PSp}_4(q), \) or \( 2B_2(q) \). Then there exist two nontrivial characters \( \chi_1, \chi_2 \in \text{Irr}_p(S) \) such that \( \chi_1(1) \neq \chi_2(1) \) and both \( \chi_1 \) and \( \chi_2 \) extend to \( \text{Aut}(S) \).

To deal with the exceptions in Theorem 4.1, we prove the following, which is Theorem C.

**Theorem 4.2.** Let \( S \) be a simple group of Lie type defined over \( \mathbb{F}_q \) and let \( p > 3 \) be a prime dividing \( |S| \). Then there exist two nontrivial characters \( \chi_1, \chi_2 \in \text{Irr}_p(S) \) such that \( \chi_2(1) \mid \chi_1(1) \), \( \chi_1 \) extends to \( \text{Aut}(S) \), and \( \chi_2 \) is invariant under every \( p \)-group of \( \text{Aut}(S) \).

4.1 Defining Characteristic

We begin by fixing some notation for this section. Let \( q = p^a \) be a power of a prime \( p > 3 \). We fix \( a := p^b \cdot m \) where \( (m, p) = 1, b \geq 0, \) and \( m \geq 1 \). In what follows, it will be useful to consider certain elements of \( \mathbb{F}_q^\times \). For a positive integer \( n \), we will denote by \( \zeta_n \) an element of order \( p^n - 1 \) in \( \mathbb{F}_q^\times \) and by \( \xi_n \) an element of order \( p^n + 1 \) in \( \mathbb{F}_q^\times \). In particular, \( \zeta_1 \in \mathbb{F}_p^\times \subseteq \mathbb{F}_q^\times, \) \( \zeta_m \in \mathbb{F}_q^\times, \) and \( \xi_m \in \mathbb{F}_{q^2}^\times \setminus \mathbb{F}_q^\times \). We also have \( \xi_1 \in \mathbb{F}_{q^2}^\times \) and further \( \xi_1 \in \mathbb{F}_q^\times \) if and only if \( q \) is a square.

4.1.1 Establishing the Basic Strategy

Suppose that \( F \) is a Frobenius map. In what follows, we will often proceed following ideas like those in [25, Theorem 4.5(4)] and [26, Proposition 6.4] to construct characters of \( S = G/Z(G) \) satisfying
our desired properties, using characters of \( \widetilde{G} \). Namely, if \( s \) is a semisimple element of \( \widetilde{G} \), there exists a unique so-called semisimple character \( \widetilde{\chi}_s \) of \( \rho \)-degree associated to the \( \widetilde{G}^s \)-conjugacy class of \( s \), and \( \widetilde{\chi}_s(1) = [\widetilde{G}^s : C_{\widetilde{G}^s}(s)]\rho \). If further \( s \in [G^s, \widetilde{G}^s] \), then \( \widetilde{\chi}_s \) is trivial on \( Z(\widetilde{G}) \), using [22, Lemma 4.4]. Furthermore, the number of irreducible constituents of \( \chi := \widetilde{\chi}_s|_G \) is exactly the number of irreducible characters \( \theta \in \text{Irr}(\overline{G}/G) \) satisfying \( \overline{\theta} = \widetilde{\chi}_s \), and we have \( \text{Irr}(\overline{G}/G) = \{ \chi_z | z \in Z(\widetilde{G}^s) \} \) and \( \mathcal{E}(\overline{G}, s)\chi_z = \mathcal{E}(\overline{G}, sz) \) for such \( z \in Z(\widetilde{G}^s) \), by [7, 13.30]. Then \( \chi \) is irreducible if and only if \( s \) is not \( \widetilde{G}^s \)-conjugate to \( sz \) for any nontrivial \( z \in Z(\widetilde{G}^s) \). Finally, if \( \varphi \in \text{Aut}(\overline{G}) \) and \( \varphi^* : \overline{G}^s \to \overline{G}^s \) is dual to \( \varphi \), then [24, Corollary 2.4] tells us that \( \chi^* = \chi_{\varphi^*(s)} \).

Therefore, in the context of proving Theorem 4.1, we will be interested in showing that there exist two nontrivial semisimple elements \( s_1, s_2 \in \widetilde{G}^s \) such that:

1. \( s_1, s_2 \) are contained in \([\widetilde{G}^s, \widetilde{G}^s]\);
2. for \( i = 1, 2 \), \( s_i \) is not conjugate to \( s_i z \) for any nontrivial \( z \in Z(\widetilde{G}^s) \);
3. the \( \widetilde{G}^s \)-classes of \( s_1 \) and \( s_2 \) are \( \text{Aut}(\widetilde{G}^s) \)-invariant; and
4. \( |C_{\widetilde{G}^s}(s_1)|^\rho \neq |C_{\widetilde{G}^s}(s_2)|^\rho \).

In the context of Theorem 4.2, we will need to replace (3) and (4) with:

3'. the \( \widetilde{G}^s \)-class of \( s_1 \) is \( \text{Aut}(\widetilde{G}^s) \)-invariant and that of \( s_2 \) is fixed by \( p \)-elements of \( \text{Aut}(\widetilde{G}^s) \); and
4'. \( |C_{\widetilde{G}^s}(s_1)|^\rho \nmid |C_{\widetilde{G}^s}(s_2)|^\rho \).

### 4.1.2 The Proofs in Defining Characteristic

**Proposition 4.3.** Let \( S \) be a simple group of Lie type defined in characteristic \( p > 3 \) not in the list of exclusions of Theorem 4.1. Then the conclusion of Theorem 4.1 holds for \( S \) and \( p \).

**Proof.** First assume \( S \) is one of \( G_2(q), F_4(q), \) or \( ^3D_4(q) \). The character degrees in these cases are available at [15], and the generic character tables are available in CHEVIE [8]. Here \( \text{Aut}(S)/S \) is cyclic generated by a field automorphism, so characters extend to \( \text{Aut}(S) \) if and only if they are invariant under \( \text{Aut}(S) \). In the case of \( G_2(q) \), there is a unique character of degree \( (q^4 + q^2 + 1) \) and a unique character of degree \( (q^5 + \epsilon) \), where \( \epsilon = \pm 1 \) is such that \( q \equiv \epsilon \pmod{6} \), so the statement holds for \( G_2(q) \). Similarly, \( F_4(q) \) has a unique character of degree \( (q^8 + q^4 + 1) \) and a unique character of degree \( (q^2 + 1)(q^4 + 1)(q^8 + q^4 + 1) \). Since \( ^3D_4(q) \) has a unique character of degree \( (q^8 + q^4 + 1) \), it suffices in this case to find another member of \( \text{Irr}_{\rho}(S) \) invariant under field automorphisms. Taking \( k \) to be such that \( \gamma^k \in \overline{F}_{\rho}^\times \), where \( \gamma \) generates \( \overline{F}_{\rho}^\times \), this is accomplished by \( \chi_{13}(k) \) in CHEVIE notation, which has degree \( (q + 1)(q^8 + q^4 + 1) \).

Hence we may assume \( S \) is not in the above list, and by Section 3, we may assume that \( S \) is not isomorphic to an alternating group. Also note that we may assume \( G \) does not have an exceptional Schur multiplier. Let \( D \leq \text{Aut}(\overline{G}) \) be as in [27, Notation 3.1], so that \( D \) is generated by appropriate graph and field automorphisms and \( \text{Aut}(G) \) is generated by \( D \) and the inner automorphisms of \( \overline{G} \).

Since \([\overline{G} : G]\) is coprime to \( p \), we see by Clifford theory that the set of members of \( \text{Irr}(\overline{G}) \) lying above members of \( \text{Irr}_{\rho}(G) \) is exactly the set \( \text{Irr}_{\rho}(\overline{G}) \). By [27, Proposition 3.4], for every \( \chi \in \text{Irr}_{\rho}(\overline{G}) \), there is a character \( \chi_0 \in \text{Irr}(\overline{G} | \chi) \) such that \( (\overline{G} \times D)_{\chi_0} = \overline{G}_{\chi_0} \rtimes D_{\chi_0} \) and \( \chi_0 \) extends to \( G \rtimes D_{\chi_0} \). Further, if \( \chi_{\overline{G}} = \chi_0 \) and \( \widetilde{\chi} \) is \( D \)-invariant, it further follows that \( \chi_0 \) extends to \( \overline{G} \rtimes D \), following the proof of [27, Lemma 2.13], since the factor set constructed there for the projective representation of \( (\overline{G} \rtimes D)_{\chi_0} \) extending \( \chi_0 \) is trivial in this case.
Hence it suffices to show that there exist $D$-invariant $\tilde{\chi}_1, \tilde{\chi}_2 \in \text{Irr}_p(\tilde{G})$ that are trivial on $Z(G)$, have different degrees, and satisfy that $\tilde{\chi}_1|_G$ and $\tilde{\chi}_2|_G$ are irreducible. In particular, it suffices to find $s_1$ and $s_2$ as described in Section 4.1.1 satisfying conditions (1)-(4). For condition (2), we note that by [3, Corollary 2.8(a)], it suffices to show that $C_{G^s}(u^s(s_i))$ are connected, and hence by [19, Exercise 20.16(c)], to choose $s_i$ such that $(\{s_i\}, |Z(G)|) = 1$.

First, suppose that $G$ is not of type $A_r$. Let $\Phi$ and $\Delta := \{\alpha_1, \alpha_2, \cdots, \alpha_q\}$ be a system of roots and simple roots, respectively, for $\tilde{G}^s$, with respect to a maximal torus $\tilde{T}^s$, following the standard model described in [10, Remark 1.8.8]. Note that we may assume that $|\Delta| \geq 3$ if $\Phi$ is type $B_r$ or $C_r$, $|\Delta| \geq 4$ if $\Phi$ is type $D_r$, and otherwise $\Phi$ is type $E_6$, $E_7$, or $E_8$. Further, our assumptions imply that if the Dynkin diagram for $\Phi$ has a nontrivial graph automorphism, then all members of $\Delta$ have the same length and that automorphism has order 2 unless $\Phi$ is of type $D_4$.

Given $\alpha \in \Phi$, let $\alpha$ denote the corresponding coroot, following the notation of [10]. Notice that for $\alpha \in \Phi$ and $t \in \mathbb{F}_q^\times$, we have $h_\alpha(t) \in [\tilde{G}^s, \tilde{G}^s]$. (See, for example, [10, Theorem 1.10.1(a)].) Let $\delta \in \mathbb{F}_q^\times$ be such that $|\delta|$ is prime to $|Z(G)|$, if possible. Otherwise, we have $\Phi$ is type $E_7$, $B_r, C_r$, or $D_r$ and $p - 1$ is a power of 2. (Note that if $G$ is type $E_6$, and $p - 1$ is a power of 3, then $p = 2$, contradicting our assumption that $p > 3$.) In these latter cases, let $\delta$ be an element of $\mathbb{F}_p^\times$ with order prime to $|Z(G)|$ dividing $p + 1$.

We define $s'_1 := h_{\alpha_1}(\delta)h_{\alpha_2}(\delta) \cdots h_{\alpha_{r-1}}(\delta)h_{\alpha_r}(\delta)$. Let $\beta$ be a member of $\Delta$ as follows. For $\Phi$ of type $E_6, E_7, E_8, or E_9$, let $\beta := \alpha_i$. If $\Phi$ is of type $C_r$ or $D_r$, let $\beta := \alpha_i$. If $\Phi$ is type $B_r$, let $\beta := \alpha_i$. Let $s'_2 := h_{\beta}(\delta)$ for $\Phi$ not of type $D_r$; $s'_2 := h_{\alpha_1}(\delta)h_{\alpha_2}(\delta)$ for $\Phi$ of type $D_r$ with $\ell \geq 5$; and $s'_2 := h_{\alpha_1}(\delta)h_{\alpha_2}(\delta)h_{\alpha_3}(\delta)$ for $\Phi$ of type $D_4$. Note then that for $i = 1, 2, s'_i$ is fixed under graph automorphisms and $([s'_i], |Z(G)|) = 1$.

If $\delta \in \mathbb{F}_q^\times$, we see that the $s'_i$ are $F^s$-fixed, and we write $s_i := s'_i$. Otherwise, the elements $\alpha_1 + \cdots + \alpha_q$ and $\beta$ are members of $\Phi$, and in the case of $D_r$, we have $\alpha_1 + \alpha_{r-1} = 2e_2 - 1$ and for $\ell = 4, \alpha_1 + \alpha_3 + \alpha_4 = e_1 - e_2 + 2e_3$. In the first case, let $\tilde{w} \in N_{\tilde{G}^s}(\tilde{T}^s)$ induce the corresponding reflection in the Weyl group of $\tilde{G}^s$. In the case of $\alpha_1 + \alpha_{r-1}$ in type $D_r$, we may take $\tilde{w}$ to be the product of members of $N_{\tilde{G}^s}(\tilde{T}^s)$ inducing the reflections in the Weyl group of $\tilde{G}^s$ for $\ell$ and $\alpha_{r-1}$, and similarly for $\alpha_1 + \alpha_3 + \alpha_4$ in the case of $D_4$. In any case, we have $s_i := s_i^{q^i}$ is $F^s$-fixed, where $g \in \tilde{G}^s$ satisfies $g^{-1}F^s(g) = \tilde{w}$. (Note that such a $g$ exists by the Lang-Steinberg theorem.) Hence $s_1$ and $s_2$ are members of $[\tilde{G}^s, \tilde{G}^s]$.

Further, we have constructed $s_1$ and $s_2$ to be fixed under graph automorphisms and such that $[C_{G^s}(s_1)]_{q^s} \neq [C_{G^s}(s_2)]_{q^s}$. The latter can be seen by analyzing the root information in [10] and using the fact that $C_{\tilde{G}^s}(s_i)$ has root system $\Phi_{s_i}$ where $\Phi_{s_i}$ consists of $\alpha \in \Phi$ with $\alpha(s_i) = 1$ (see [7, Proposition 2.3]). Let $F_p$ denote a generating field automorphism such that $F_p(h_\alpha(t)) = h_\alpha(t^p)$ for $\alpha \in \Phi$ and $t \in \mathbb{F}_q^\times$. Then for $i = 1, 2$, $s'_i$ is $\tilde{G}^s$-conjugate to $F_p(s'_i)$, taking for example $\tilde{w}$ as the conjugating element when $s'_i \neq F_p(s'_i)$. Hence $s_i$ is also $\tilde{G}^s$-conjugate to $F_p(s_i)$. Since the $C_{G^s}(s_i)$ are connected, this yields that the $s_i$ are $\tilde{G}^s$-conjugate to $F_p(s_i)$, using [7, (3.25)]. Then $s_1$ and $s_2$ are semisimple elements satisfying (1)-(4), as desired.

Now let $\Phi$ be of type $A_{r-1}$, so that $G \cong \tilde{G}^s \cong \text{GL}_n(q)$, $G \cong [\tilde{G}^s, \tilde{G}^s] = \text{SL}_n(q)$, and $G^s \cong \text{PGL}_n(q)$, with $\epsilon \in \{\pm 1\}$ and $n \geq 4$. If $(p, \epsilon) \neq (5, +1)$, let $\delta \in \mathbb{C}_{p-\epsilon}$, viewed as a subgroup of $\mathbb{F}_q^\times$, be such that $\delta = 1$ in case $\epsilon = 1$ and $\delta = 1$ in case $\epsilon = -1$. Note that $|\delta| > 4$, from the conditions on $p$. If $(p, \epsilon) = (5, +1)$, let $\delta$ be an element of order 6 in $\mathbb{F}_{25}$. Then in any case, we have $\delta$ chosen such that $|\delta| > 4$.

Recall that the class of a semisimple element in $\text{GL}_n(q)$ is determined by its eigenvalues. Let $s_1 \in \tilde{G}^s$ have eigenvalues $\{\delta, \delta^{-1}, 1, 1, \ldots, 1\}$ and $s_2$ have eigenvalues $\{\delta, \delta^{-1}, 1, 1, \ldots, 1\}$. Then $C_{G^s}(s_1) \cong \text{GL}_{n-2}(q) \times \text{GL}_1(q^2)$ and $C_{G^s}(s_2) \cong \text{GL}_n(q) \times \text{GL}_2(q)^2$, unless $\epsilon = -1$ and $q$ is
square or \((p, \epsilon) = (5, +)\) and \(q\) is nonsquare, in which case \(C_{\tilde{G}^s}(s_1) \cong \GL_n^{G}(q) \times \GL_1(q^2)\) and \(C_{\tilde{G}^s}(s_2) \cong \GL_n^{G}(q) \times \GL_2(q^2)\). In any case, we therefore have \(|C_{\tilde{G}^s}(s_1)|_{\mu} \neq |C_{\tilde{G}^s}(s_2)|_{\mu}|. Since the graph automorphism acts via inverse-transpose on \(\GL_n(q)\) and the generating field automorphism acts on semisimple elements by raising the eigenvalues to the power of \(p\), we see that the \(\tilde{G}^s\)-classes of \(s_1\) and \(s_2\) are each \(\text{Aut}(\tilde{G}^s)\)-invariant. Further, as \(s_1\) and \(s_2\) have determinant 1, they are contained in \([\tilde{G}^s, \tilde{G}^s] = \text{SL}_n(q)\).

Now, in this case, \(Z(\tilde{G}^s)\) is comprised of matrices of the form \(\mu \cdot I_n\), where \(\mu\) is an element of \(C_q-\epsilon\), viewed as a subgroup of \(F_q^*\). Since \(|\delta| \neq 2\), we see by comparing eigenvalues that \(s_1\) cannot be conjugate to \(s_2\) for any nontrivial \(z \in Z(\tilde{G}^s)\). Now, if \(s_2 z\) is conjugate to some \(z \in Z(\tilde{G}^s)\), then there is some \(\mu\) as above such that \(\delta \mu = \delta^{-1}\) and \(\delta^{-1} \mu = \delta\), except possibly if \(n = 6\), in which case \(\delta \mu = 1\) is another possibility. In the latter case, \(\mu = \delta^{-1}\), so \(s_2 z\) has eigenvalues \(\{1, 1, \delta^{-2}, \delta^{-2}, \delta^{-1}, \delta^{-1}\}\), so we must have \(\delta^{-2} = \delta\), contradicting \(|\delta| > 4\). Hence we are in the case \(\delta \mu = \delta^{-1}\) and \(\delta^{-1} \mu = \delta\). Then \(\mu = \delta^{-2} = \delta^2\), again contradicting \(|\delta| > 4\). Hence in all cases, we have exhibited the desired elements \(s_1, s_2 \in \tilde{G}^s\), and the proof is complete.

We remark that the conclusion of Theorem 4.1 fails for \(\text{PSL}_2(q)\) and \(\text{PSL}_3(q)\) when \(q\) is a square. Indeed, in these cases, the only option for \(\text{Aut}(\tilde{G}^s)\)-invariant semisimple classes of \(\tilde{G}^s\) would be comprised of elements with eigenvalues \(\{\delta, \delta^{-1}\}\) and \(\{\delta, \delta^{-1}, \pm 1\}\), respectively, where \(\delta^2 = \delta\) or \(\delta^{-1}\).

If \(q\) is a square, both options would yield \(\delta \in \mathbb{F}_q\), so all corresponding semisimple characters have the same degree. However, we can show the following:

**Lemma 4.4.** Let \(S \cong \text{PSL}_2(q), \text{PSL}_3(q), \text{or} \ PSp_4(q)\) with \(q\) a power of a prime \(p > 3\). Then the conclusion of Theorem 4.2 holds for \(S\) and \(p\). Moreover, if \(q\) is not square and further \(p \neq 5\) in the case of \(\text{PSL}_2(q)\), then the conclusion of Theorem 4.1 holds for \(S\) and \(p\).

**Proof.** Note that since \(p > 3\), the graph and diagonal automorphisms are not in a \(p\)-subgroup of \(\text{Aut}(S)\). In particular, the only \(p\)-elements of \(D\) are induced from field automorphisms of \(p\)-power order. Arguing as in the proof of Proposition 4.3, it suffices to show that there are two semisimple elements \(s_1, s_2\) of \(\tilde{G}^s\) satisfying conditions (1), (2), (3'), and (4') from Section 4.1.1. Throughout the proof, let \(q = p^a\) where \(a = p^b m\) with \((m, p) = 1\).

(i) First suppose that \(p > 5\) and \(S \cong \text{PSL}_3(q)\). Note that since \(p > 5\), both \(\zeta_1\) and \(\xi_m\) have order larger than 4. Let \(s_1 \in \tilde{G}^s\) have eigenvalues \(\{\zeta_1, \zeta_1^{-1}\}\), and \(s_2\) have eigenvalues \(\{\xi_m, \xi_m\^{-1}\}\). Then \(s_1\) and \(s_2\) satisfy conditions (1), (2), (3'), and (4') from Section 4.1.1. Here \(C_{\tilde{G}^s}(s_1) \cong \GL_2(q^2)\), and the corresponding semisimple characters have degrees \(\chi_1(1) = q + 1\) and \(\chi_2(1) = q - 1\), respectively. This proves the first statement when \(p > 5\) and \(S \cong \text{PSL}_3(q)\).

(ii) Next let \(p = 5\) and \(S \cong \text{PSL}_2(q)\). First suppose \(m > 1\). Here we may take \(s_1 \in \tilde{G}^s\) to have eigenvalues \(\{\zeta_1, \zeta_1^{-1}\}\), and take \(s_2\) to have eigenvalues \(\{\xi_m, \xi_m^{-1}\}\) if \(2 \mid m\) and eigenvalues \(\{\xi_m, \xi_m^{-1}\}\) if \(2 \nmid m\). Then if \(2 \mid m\), we have \(C_{\tilde{G}^s}(s_1) \cong \GL_1(q^2)\) and \(C_{\tilde{G}^s}(s_2) \cong \GL_1(q^2)\). When \(2 \nmid m\), the centralizers of \(s_1\) and \(s_2\) are reversed. In either case, however, we obtain \(\chi_1\) and \(\chi_2\) satisfying the required conditions, as above.

Now let \(m = 1\), so \(q = 5^k\). Then \(q \equiv 1 \pmod{4}\) and \(q \equiv -1 \pmod{3}\). We obtain an \(\text{Aut}(S)\)-invariant character \(\chi_2\) constructed using \(s_1\) as in the case in the previous paragraph. Here \(\chi_1(1) = q - 1\). Further, we see from the generic character table that there is a character of degree \((q + 1)/2\) which is invariant under every field automorphism, completing the proof of the first statement for \(\text{PSL}_2(q)\).

(iii) Now let \(S\) be \(\text{PSL}_3(q)\), with \(p \geq 5\). Notice that an element \(s \in \tilde{G}^s\) with eigenvalues \(\{\delta, \delta^{-1}, 1\}\) with \(|\delta| \geq 4\) cannot be conjugate to \(s_2\) for any nontrivial \(z \in Z(\tilde{G}^s)\), as then the sets \(\{\delta, \delta^{-1}, 1\}\) and \(\{\delta u, \delta^{-1} u, \mu\}\) are the same for some \(\mu \in C_{q-\epsilon}\), yielding \(\delta^2 = 1\). Note \(|\delta| \geq 4\) since \(p \geq 5\). Hence we may construct \(s_1\) and \(s_2\) analogously to case (i) above. Namely, let \(s_1\) have eigenvalues \(\{\zeta_1, \zeta_1^{-1}, 1\},\)

11
and let $s_2$ have eigenvalues $\{\xi_m, \xi_m^{-1}, 1\}$. Then $s_1$ and $s_2$ satisfy properties (1),(2),(3’),(4’) of Section 4.1.1. Here $C_{G^*}(s_1) \cong \text{GL}_1(q)^3$ in case $\epsilon = 1$, and $C_{G^*}(s_1) \cong \text{GL}_1(q^2) \times \text{GU}_1(q)$ in case $\epsilon = -1$. Further, $C_{G^*}(s_2) \cong \text{GL}_1(q^2) \times \text{GL}_1(q)$ in case $\epsilon = 1$ and $C_{G^*}(s_2) \cong \text{GU}_1(q)^3$ in case $\epsilon = -1$. Hence $\chi_1(1) = (q + 1)(q^2 + eq + 1)$ and $\chi_2(1) = (q - 1)(q^2 + eq + 1)$.

(iv) Now let $S = \text{PSp}_4(q)$. The character table of $G = \text{Sp}_4(q)$ and of $\tilde{G} = \text{CSp}_4(q)$ are available in [28] and [4], respectively. From this we see that the characters in the families $\chi_8(k)$ and $\chi_6(\ell)$ with $k \in \{1, \ldots, (q - 3)/2\}$, $\ell \in \{1, \ldots, (q - 1)/2\}$ in the notation of [28], with degrees $(q + 1)(q^2 + 1)$ and $(q - 1)(q^2 + 1)$, respectively, contain $Z(G)$ in the kernel and extend to $\tilde{G}$. Further, comparing notations shows these extensions are invariant under the same field automorphisms as the characters of $G$. Choosing $k$ and $\ell$ such that $\gamma^k = \zeta_1$ and $\eta^\ell = \xi_m$, where $\gamma$ generates $\mathbb{F}_q^*$ and $\eta$ generates the cyclic group of size $q + 1$ in $\mathbb{F}_q^*$, we see that $\chi_1 := \chi_8(k)$ and $\chi_2 := \chi_6(\ell)$ satisfy the desired properties.

(v) Finally, let $q$ be nonsquare, and further assume $p > 5$ in the case $S \cong \text{PSL}_2(q)$. Let $s_1$ be as in part (i) in the case $\text{PSL}_2(q)$ and as in part (iii) for $\text{PSL}_2(q)$. Let $s_2$ in $\tilde{G}$ have eigenvalues $\{\xi_1, \xi_1^{-1}\}$ or $\{\xi_1, \xi_1^{-1}, 1\}$, respectively. In this case $\xi_1 \in \mathbb{F}_q^2 \setminus \mathbb{F}_q^*$ has order larger than 4. These elements satisfy conditions (1)-(4) discussed in Section 4.1.1. In particular, when $S \cong \text{PSL}_2(q)$, the semisimple characters corresponding to $s_1$ and $s_2$ have degrees $q + 1$ and $q - 1$, respectively. When $S \cong \text{PSL}_2(q)$, the semisimple characters corresponding to $s_1$ and $s_2$ have degrees $(q + 1)(q^2 + 1)$ and $(q - 1)(q^2 + 1)$, respectively. Then in these cases, as in the proof of Proposition 4.3, the conclusion of Theorem 4.1 holds.

Now let $S = \text{PSp}_4(q)$. Here we let $\chi_1$ be as in (iv), and let $\chi_2$ be the character $\chi_6(\ell)$, where $\ell$ is now chosen so that $\eta^\ell = \xi_1$ is a $p + 1$ root of unity in $\mathbb{F}_q^2 \setminus \mathbb{F}_q$. Then $\chi_1$ and $\chi_2$ both extend to $\text{Aut}(S)$ and have different degrees, completing the proof.

$\square$

4.2 Non-Defining Characteristic

In this section, we address the proofs of Theorems 4.1 and 4.2 in the case $p \nmid q$.

Proposition 4.5. Let $S$ be a simple group of Lie type defined over $\mathbb{F}_q$ not in the list of exclusions of Theorem 4.1, and let $p > 3$ be a prime dividing $|S|$ but not dividing $q$. Or let $S = 2B_2(q^2)$ where $q^2 := 2^{2m+1}$ and let $p > 3$ be a prime dividing $|S|$ but not dividing $q^2 - 1$. Then the conclusion of Theorem 4.1 holds for $S$ and $p$.

Proof. By [18, Theorem 2.4], every unipotent character of $S$ extends to its inertia group in $\text{Aut}(S)$, so it suffices to find two unipotent characters with different degrees in $\text{Irr}_p(S)$ that are invariant under $\text{Aut}(S)$. Since the Steinberg character $\text{St}_S$ is one such character, we aim to exhibit another nontrivial unipotent character of $p'$-degree invariant under $\text{Aut}(S)$.

Further, [18, Theorem 2.5], yields that every unipotent character of $S$ is invariant under $\text{Aut}(S)$ unless $S$ is a specifically stated exception for one of $D_n(q)$ with $n$ even, $B_2(q)$ with $q$ even, $G_2(q)$ with $q$ a power of 3, or $F_4(q)$ with $q$ even.

The unipotent characters of classical groups are indexed by partitions in case of type $A_{n-1}$ and $2A_{n-1}$ and by “symbols” in the other types. Discussions of these symbols and the corresponding character degrees are available in [6, Section 13.8]. In Table 1, we list the unipotent characters for each classical type that extend to $\text{Aut}(S)$ by [18, Theorems 2.4 and 2.5]. Further, $p > 3$ cannot divide the degree of both characters listed simultaneously, which can be seen, for example, by an application of [17, Lemma 5.2]. Hence taking $\chi_1 = \text{St}_S$ and $\chi_2$ the character listed whose degree is not divisible by $p$, the desired statement holds in the case of classical types.

Similarly, for groups of exceptional type, Suzuki and Ree groups, and $3D_4(q)$, by observing the explicit list of unipotent character degrees in [6, Section 13.9], we see that there is likewise always a
second unipotent character with degree not divisible by $p$, except in the case of $2B_2(q^2)$ or $2G_2(q^2)$ with $p | (q^2 - 1)$. Further, these can again be chosen not to be one of the exceptions listed in [18, Theorem 2.5]. When $S = 2G_2(q^2)$ and $p | (q^2 - 1)$, we may consider instead the unique character of degree $q^4 - q^2 + 1$, which must be invariant under Aut$(S)$, and hence extends since Aut$(S)/S$ is cyclic.

Together, note that Propositions 4.3 and 4.5 prove Theorem 4.1. We also note the following, which follows from the proof of Lemma 4.4 and ideas from Proposition 4.5, together with the fact that PSL$_3^4(q)$ has a unipotent character of degree $q(q + 1)$.

**Lemma 4.6.** Let $p > 3$ be a prime and let $S \cong$ PSL$_2(q)$ or PSL$_3^4(q)$ be simple with $q$ a power of a prime $r > 3$, where $r \neq p$. Then the conclusion of Theorem 4.2 holds for $S$ and $p$. Moreover, the conclusion of Theorem 4.1 holds for $S$ and $p$ in the following situations:

- $S = \text{PSL}_2(q)$, $r > 5$, and $p \nmid (q + 1)$ or $q$ is not square;
- $S = \text{PSL}_3(q)$ and $p \nmid (q + 1)$ or $q$ is not square;
- $S = \text{PSU}_3(q)$.

To complete the proof of Theorem 4.2, we need to consider $2B_2(2^{2n+1})$, PSL$_2(q)$, and PSL$_3^4(q)$ when $q$ is a power of 2 or 3 and $p \nmid q$. These are treated in the next two Lemmas.

**Lemma 4.7.** Let $p > 3$ be a prime and let $S \cong$ PSL$_2(q)$ or PSL$_3^4(q)$ be simple with $q$ a power of 2 or 3. Then the conclusion of Theorem 4.2 holds for $S$ and $p$.

**Proof.** Let $r \in \{2, 3\}$. Note that we omit the cases PSL$_2(r)$, since $S$ is simple. As before, we take $\chi_1 = \text{St}_S$, and show that there exists $\chi_2$ satisfying the desired properties.

First suppose that $q = rp^b$ for some positive integer $b$. Notice then that $p \nmid (q^2 - 1)$. Indeed, otherwise we have $p | \Phi_{2p^c}(r)$ or $p | \Phi_{1p^c}(r)$ for some nonnegative integer $c$, and hence by [17, Lemma
5.2], we have \( r \) has order 1, 2, or a power of \( p \) modulo \( p \). Since the latter is impossible, it follows that \( p \mid (r^2 - 1) \), which is impossible since \( p > 3 \) and \( r < 3 \). If \( S = \text{PSL}_2(q) \), we may take \( \chi_2 \) to be the unipotent character of degree \( q^2 + \epsilon q \), and in fact the conclusion of Theorem 4.1 holds in this case using [18, Theorems 2.4 & 2.5]. In the case \( S = \text{PSL}_2(q) \) and \( r = 3 \), we have \( q \equiv -1 \pmod{4} \), and we may take \( \chi_2 \) to be a character of degree \( (q - 1)/2 \), which is fixed by the field automorphisms. In the case \( r = 2 \) and \( S \simeq \text{PSL}_2(q) \), let \( s \in \tilde{G}^s \) have eigenvalues \( \{\delta, \delta^{-1}\} \) where \( |\delta| = 3 \). Then the corresponding semisimple character of \( \tilde{G} \) restricts to \( \text{SL}_2(q) \approx \text{PSL}_2(q) \) irreducibly, is fixed by field automorphisms, and has degree \( q \pm 1 \). Letting \( \chi_2 \) be the corresponding irreducible character of \( S \), we are done in this case.

So we may assume \( q = r^a \) where \( r \in \{2, 3\} \), and \( a = p^n m \) with \( m > 1 \) and \( (m, p) = 1 \). Let \( S = \text{PSL}_2(q) \). If \( p \nmid (q + \epsilon) \), we may again take \( \chi_2 \) to be the unipotent character of degree \( q^2 + \epsilon q \), and the conclusion of Theorem 4.1 holds. So assume that \( p \mid (q + \epsilon) \). Arguing similarly to above, we see that this excludes the case \((r, m) = (2, 2)\) if \( \epsilon = -1 \), so we may further assume \((r, m) \neq (2, 2)\) if \( \epsilon = -1 \). Taking \( s \in \tilde{G}^s \) to have eigenvalues \( \{\delta, \delta^{-1}\} \) with \( |\delta| = r^m + \epsilon \), we may argue as before to obtain a character \( \chi_2 \) of \( S \) with degree \( (q - \epsilon)(q^2 + \epsilon q + 1) \), which is not divisible by \( p \), that is invariant under every \( p \)-element of \( \text{Aut}(S) \).

Now let \( S = \text{PSL}_2(q) \). Then taking \( s_i \in \tilde{G}^s \) for \( i = 1, 2 \) to have eigenvalues \( \{\delta_i, \delta_i^{-1}\} \) with \( |\delta_1| = r^m - 1 \) and \( |\delta_2| = r^m + 1 \), we obtain characters with degree \( (q + 1) \) and \( (q - 1) \) of \( S \) that are invariant under \( p \)-elements of \( \text{Aut}(S) \). Since \( p > 3 \) cannot divide both of these character degrees, we may make an appropriate choice for \( \chi_2 \), which completes the proof.

**Lemma 4.8.** Let \( S \) be a simple Suzuki group \( ^2B_2(q^2) \) with \( q^2 = 2^{2n+1} \) and let \( p > 3 \) be a prime dividing \( q^2 - 1 \). Then the conclusion of Theorem 4.2 holds for \( S \) and \( p \).

**Proof.** As before, we may take \( \chi_1 \) to be the Steinberg character. Now, since \( \text{Aut}(S)/S \) is cyclic of size \( 2n + 1 \), generated by field automorphisms, it suffices to exhibit a character \( \chi_2 \) with degree coprime to \( p \) that is invariant under field automorphisms of \( p \)-power order. Let \( 2n + 1 = p^n m \) with \( (m, p) = 1 \). Arguing as in Lemma 4.7, we see \( m > 1 \), since \( p \mid (q^2 - 1) \). Hence letting \( s \) be such that \( \gamma^s \) has order \( 2^m - 1 \), where \( \gamma \) has order \( q^2 - 1 \), we may take \( \chi_2 \) to be the character \( \chi_3(s) \) in CHEVIE notation. Then \( \chi_2 \) has degree \( q^4 + 1 \) and is invariant under \( p \)-elements of \( \text{Aut}(S) \).

Theorem 4.2 now follows by combining Lemmas 4.4, 4.6, 4.7, and 4.8 with Theorem 4.1, which completes the proofs of Theorems A-C.

**References**


