

THE AVERAGE CHARACTER DEGREE AND AN IMPROVEMENT OF THE ITÔ-MICHLER THEOREM

NGUYEN NGOC HUNG AND PHAM HUU TIEP

ABSTRACT. The classical Itô-Michler theorem states that the degree of every ordinary irreducible character of a finite group G is coprime to a prime p if and only if the Sylow p -subgroups of G are abelian and normal. In an earlier paper [HT], we used the notion of average character degree to prove an improvement of this theorem for the prime $p = 2$. In this follow-up paper, we obtain a full improvement for all primes.

1. INTRODUCTION

The classical Itô-Michler theorem [Ito, Mic1] on character degrees of finite groups asserts that the degree of every ordinary irreducible character of a finite group G is coprime to a prime p if and only if the Sylow p -subgroups of G are abelian and normal. Using the notion of the so-called *average character degree* introduced by Isaacs, Loukaki, and Moretó in [ILM], we proposed in [HT] a new direction, described below, to improve this theorem.

As usual, we use $\text{Irr}(G)$ to denote the set of all ordinary irreducible characters of G . Following [HT], let

$$\text{Irr}_p(G) := \{\chi \in \text{Irr}(G) \mid \chi(1) = 1 \text{ or } p \mid \chi(1)\}$$

and

$$\text{acd}_p(G) := \frac{\sum_{\chi \in \text{Irr}_p(G)} \chi(1)}{|\text{Irr}_p(G)|}$$

so that $\text{acd}_p(G)$ is the average degree of linear characters and irreducible characters of G with degree divisible by p . The Itô-Michler theorem is then equivalent to the statement that $\text{acd}_p(G) = 1$ if and only if the Sylow p -subgroups of G are abelian and normal.

We have observed that the normality of the Sylow p -subgroups of G can still be achieved when $\text{acd}_p(G)$ is close to 1. In particular, we showed in [HT] that if $\text{acd}_2(G) < 4/3$ then G has a normal Sylow 2-subgroup. On the other hand, the Sylow p -subgroups are not abelian no matter how $\text{acd}_p(G)$ is close to 1, as shown by the extraspecial p -groups.

Date: September 27, 2019.

2010 Mathematics Subject Classification. Primary 20C15, 20D10, 20D05.

Key words and phrases. finite groups, simple groups, character degrees, normal subgroups, Sylow subgroups, Itô-Michler theorem.

The second author gratefully acknowledges the support of the NSF (grant DMS-1840702) and the Joshua Barlaz Chair in Mathematics.

The paper is partially based upon work supported by the NSF under grant DMS-1440140 while the authors were in residence at MSRI (Berkeley, CA), during the Spring 2018 semester. We thank the Institute for the hospitality and support.

The authors are grateful to the referee for insightful comments on the paper.

The main result of this paper is a generalization of the aforementioned result to all primes. For any given prime p , a key numerical invariant in this result is the integer $\ell(p)$, which is defined to be the smallest positive integer ℓ such that $\ell p + 1$ is a prime power. Such an integer exists by Dirichlet's theorem. Clearly, $\ell(2) = \ell(3) = \ell(7) = 1$; moreover, $\ell(p) = 1$ if and only if $p = 2$ or p is a Mersenne prime. On the other hand, $\ell(5) = \ell(11) = \ell(13) = 2$, and $\ell(17) = 6$.

Theorem A. *Let p be a prime and let G be a finite group with*

$$\text{acd}_p(G) < \frac{2\ell(p)p}{\ell(p)p + 1}.$$

Then G has a normal Sylow p -subgroup.

The bound in Theorem A is best possible. Indeed, by the definition of $\ell(p)$, there is a prime r and an integer $m \geq 1$ such that $\ell(p)p = r^m - 1$. Note that the cyclic group C_{r^m-1} admits a faithful action on the elementary abelian r -group C_r^m , leading to a semi-direct product $G = C_r^m \rtimes C_{r^m-1}$ with $\text{acd}_p(G) = 2\ell(p)p/(\ell(p)p + 1)$, and G has a non-normal Sylow p -subgroup.

Of course if a finite group G has a normal Sylow p -subgroup, then G is p -solvable. In fact, we have to establish p -solvability before proving normality of Sylow p -subgroups. The bound of $\text{acd}_p(G)$ for p -solvability in the following theorem is indeed best possible, shown by A_5 for $p = 2, 3$ and $\text{PSL}_2(p)$ for $p \geq 5$. Recall that $\mathbf{O}^{p'}(G)$ is the minimal normal subgroup of G whose quotient is a p' -group.

Theorem B. *Let p be a prime and set $a_2 := 5/2$, $a_3 := 7/3$ and $a_p := (p + 1)/2$ if $p \geq 5$. Let G be a finite group such that $\text{acd}_p(G) < a_p$. Then $\mathbf{O}^{p'}(G)$ is solvable and, in particular, G is p -solvable.*

We need to use the classification of finite simple groups to prove Theorem B. In particular, the classification is used to show the existence of an extendible irreducible character of degree divisible by p in non-abelian simple groups (see Theorem 3.1). We believe that this extendibility-divisibility result will be useful in other purposes as well.

A similar statement to Theorem B may still be true if we restrict our attention to only real-valued characters or even strongly real characters, and this would significantly improve the results in [MT, T]. However, to prove it, one would first need to prove a real, respectively strongly real, version of Theorem 3.1, which seems very difficult to prove at the moment.

In view of Theorem A, it is reasonable to conjecture that the index $[G : \mathbf{N}_G(P)]$ is bounded in terms of $\text{acd}_p(G)$, where P is a Sylow p -subgroup of G . Even the weaker statement that the number of non-abelian composition factors of G of order divisible by p is bounded in terms of $\text{acd}_p(G)$ seems highly nontrivial to prove.

2. PRELIMINARIES

Throughout the paper, let $n_d(G)$ denote the number of irreducible characters of degree d of a finite group G . The following lemma controls the number $n_1(G)$ of linear characters in a special situation.

Lemma 2.1. *Let G be a finite group with a non-abelian minimal normal subgroup N . Assume that there is some $\mu \in \text{Irr}(N)$ such that μ is extendible to the inertia subgroup $I_G(\mu)$. Then $n_1(G) \leq n_d(G)[G : I_G(\mu)]$ where $d := \mu(1)[G : I_G(\mu)]$.*

Proof. This is Proposition 2.3(i) of [HT]. $\square$

The following lemma allows us to focus on special subsets of $\text{Irr}_p(G)$ in a number of situations:

Lemma 2.2. *Let G be a finite group, p be a prime and let $\text{Irr}^*(G)$ be a subset of $\text{Irr}_p(G)$ that contains all linear characters of G . Suppose that $\text{acd}_p(G) \leq p$. Then*

$$\text{acd}_p(G) \geq \frac{\sum_{\chi \in \text{Irr}^*(G)} \chi(1)}{|\text{Irr}^*(G)|}.$$

In particular, if $N \triangleleft G$, $N \leq G'$, and $\text{acd}_p(G) \leq p$, then $\text{acd}_p(G/N) \leq \text{acd}_p(G)$.

Proof. Let

$$A := \sum_{\chi \in \text{Irr}_p(G)} \chi(1), \quad B := |\text{Irr}_p(G)|, \quad C := \sum_{\chi \in \text{Irr}_p(G) \setminus \text{Irr}^*(G)} \chi(1), \quad D := |\text{Irr}_p(G) \setminus \text{Irr}^*(G)|.$$

By assumption, $A/B = \text{acd}_p(G) \leq p$ and so $A \leq pB$. On the other hand, as $\text{Irr}^*(G)$ contains all linear characters of G , $C \geq pD$. It follows that

$$\text{acd}_p(G) = A/B \geq \frac{A - B}{C - D} = \frac{\sum_{\chi \in \text{Irr}^*(G)} \chi(1)}{|\text{Irr}^*(G)|},$$

proving the first statement. For the second statement, note that the subset $\text{Irr}_p(G/N)$ of $\text{Irr}_p(G)$ contains all linear characters of G . $\square$

The next lemma will be used frequently. It is well known, but we include a proof for completeness.

Lemma 2.3. *Let S be a non-abelian simple group and let $N := S \times \cdots \times S$, a direct product of k copies of S . Suppose that $\lambda \in \text{Irr}(S)$ is extendible to $I_{\text{Aut}(S)}(\lambda)$. Then $\chi := \lambda \times \cdots \times \lambda \in \text{Irr}(N)$ is extendible to $I_{\text{Aut}(N)}(\chi)$.*

Proof. Let $\text{Orb}(\lambda)$ denote the orbit of λ in the action of $\text{Aut}(S)$ on $\text{Irr}(S)$. As $\text{Aut}(N)$ acts transitively on the simple direct factors of N , the orbit of χ under the action of $\text{Aut}(N)$ is

$$\text{Orb}(\chi) := \{\lambda_1 \times \lambda_2 \times \cdots \times \lambda_k \in \text{Irr}(N) \mid \lambda_i \in \text{Orb}(\lambda)\}.$$

By assumption, χ is invariant under $I_{\text{Aut}(S)}(\lambda) \wr S_k$. On the other hand, as $\text{Aut}(N) = \text{Aut}(S) \wr S_k$, we have

$$[\text{Aut}(N) : I_{\text{Aut}(S)}(\lambda) \wr S_k] = [\text{Aut}(S) : I_{\text{Aut}(S)}(\lambda)]^n = |\text{Orb}(\lambda)|^n = |\text{Orb}(\chi)|.$$

Therefore we conclude that $I_{\text{Aut}(N)}(\chi) = I_{\text{Aut}(S)}(\lambda) \wr S_k$.

Let $\tilde{\lambda} \in \text{Irr}(I_{\text{Aut}(S)}(\lambda))$ be an extension of λ . Suppose that $\tilde{\lambda}$ is afforded by a $\mathbb{C}I_{\text{Aut}(S)}(\lambda)$ -module V . Then $I_{\text{Aut}(N)}(\chi) = I_{\text{Aut}(S)}(\lambda) \wr S_k$ acts naturally on $V^{\otimes k}$ and it follows that the character afforded by the $\mathbb{C}I_{\text{Aut}(N)}(\chi)$ -module $V^{\otimes k}$ is an extension of χ , which means that χ is extendible to $I_{\text{Aut}(N)}(\chi)$. $\square$

The next proposition will be critical in the proof of p -solvability of finite groups with small acd_p . The proof follows the idea of [T, Theorem 3.5].

Proposition 2.4. *Let G be a finite group with a minimal normal subgroup $N \cong S_1 \times \cdots \times S_n$, where $n \geq 2$ and the S_i 's are all isomorphic to a non-abelian simple group S . Let K be the kernel of the action of G on $\{S_1, \dots, S_n\}$. If $|G/K|$ is divisible by a prime p , then there exists $\mu \in \text{Irr}(N)$ such that $\mu(1) \geq 12$, μ is extendible to a character of $I_G(\mu)$, and $[G : I_G(\mu)]$ is divisible by p .*

Proof. Consider the faithful action of G/K on the set $\{S_1, S_2, \dots, S_n\}$. As $p \mid |G/K|$, by [CD, Lemma 8], there are two disjoint subsets Ω_1 and Ω_2 of $\{S_1, S_2, \dots, S_n\}$ such that

$$(2.1) \quad p \mid [(G/K) : \text{Stab}_{G/K}(\Omega_1, \Omega_2)] = [G : \text{Stab}_G(\Omega_1, \Omega_2)].$$

Without loss we may assume that $\mathbf{C}_G(N) = 1$. Set

$$N_1 := \prod_{S_i \in \Omega_1} S_i, \quad N_2 := \prod_{S_i \in \Omega_2} S_i.$$

By [T, Theorem 3.2], we can find two irreducible characters, say α and β , of S of distinct degrees ≥ 3 , each of which is extendible to its inertia subgroup in $\text{Aut}(S)$. Consider the irreducible characters

$$\tilde{\alpha} := \alpha \times \cdots \times \alpha \in \text{Irr}(N_1), \quad \tilde{\beta} := \beta \times \cdots \times \beta \in \text{Irr}(N_2).$$

Using Lemma 2.3, we deduce that $\tilde{\alpha}$ and $\tilde{\beta}$ are extendible to their respective inertia subgroups $I_{\text{Aut}(N_1)}(\tilde{\alpha})$ and $I_{\text{Aut}(N_2)}(\tilde{\beta})$. It then follows that $\tilde{\alpha} \otimes \tilde{\beta} \in \text{Irr}(M)$ is extendible to its inertia subgroup in $\text{Aut}(N_1) \times \text{Aut}(N_2)$. Let

$$N_3 := \prod_{S_i \notin \Omega_1 \cup \Omega_2} S_i,$$

and consider

$$\mu := \tilde{\alpha} \times \tilde{\beta} \times 1_{N_3} \in \text{Irr}(N).$$

Since α and β are non-principal and have distinct degrees, we see that

$$N, N_1 N_2 \triangleleft J \leq \text{Stab}_G(\Omega_1, \Omega_2) = \mathbf{N}_G(N_1) \cap \mathbf{N}_G(N_2)$$

for $J := I_G(\mu)$. Observe that

$$N_3 \triangleleft \mathbf{C}_J(N_1 N_2), \quad N_1 N_2 \cap \mathbf{C}_J(N_1 N_2) = 1.$$

Hence we can extend μ canonically to the character $\tilde{\mu}$ of

$$N \mathbf{C}_J(N_1 N_2) = N_1 N_2 \times \mathbf{C}_J(N_1 N_2)$$

that is trivial on $\mathbf{C}_J(N_1 N_2)$ and can be viewed as the character $\tilde{\alpha} \otimes \tilde{\beta}$ of

$$N \mathbf{C}_J(N_1 N_2) / \mathbf{C}_J(N_1 N_2) \cong N_1 \times N_2.$$

Since $N \mathbf{C}_J(N_1 N_2) \triangleleft J$ and $J / \mathbf{C}_J(N_1 N_2)$ embeds in $\text{Aut}(N_1) \times \text{Aut}(N_2)$, the aforementioned extendibility of $\tilde{\alpha} \otimes \tilde{\beta}$ implies that $\tilde{\mu}$ extends to $J = I_G(\mu)$.

Finally, since $J \leq \text{Stab}_G(\Omega_1, \Omega_2)$, we have $p \mid [G : J]$ by (2.1). Also, as α and β have distinct degrees at least 3, we have $\mu(1) \geq 12$, and the proof is complete. $\square$

3. p -SOLVABILITY

As mentioned in the introduction, we need the classification of finite simple groups to prove the p -solvability. Indeed, the classification is needed in the next two theorems, whose proofs are deferred to Section 5.

Theorem 3.1. *Let p be a prime and let S be a non-abelian simple group of order divisible by p . Then there exists $\theta \in \text{Irr}(S)$ such that $p \mid \theta(1)$ and θ is extendible to a character of $I_{\text{Aut}(S)}(\theta)$.*

Theorem 3.2. *Let p be a prime and let S be a non-abelian simple group of order not divisible by p . Then there exists a non-principal character $\theta \in \text{Irr}(S)$ such that θ is extendible to a character of $I_{\text{Aut}(S)}(\theta)$ and $p \nmid |I_{\text{Aut}(S)}(\theta)|$.*

With Theorem 3.1 in hand, we obtain the following.

Theorem 3.3. *Let G be a finite group with a non-abelian minimal normal subgroup N of order divisible by a prime p . Then there exists $\mu \in \text{Irr}(N)$ such that $p \mid \mu(1)$ and μ is extendible to $I_G(\mu)$.*

Proof. Suppose that $N \cong S \times S \times \cdots \times S$, a direct product of r copies of a non-abelian simple group S with $p \mid |S|$. With no loss of generality, we may assume that $\mathbf{C}_G(N) = 1$. Then $N \leq G \leq \text{Aut}(N) = \text{Aut}(S) \wr S_r$.

By Theorem 3.1, we can find a character $\theta \in \text{Irr}(S)$ such that $p \mid \theta(1)$ and θ is extendible to $I_{\text{Aut}(S)}(\theta)$. Let $\mu := \theta \times \cdots \times \theta \in \text{Irr}(N)$. Now using Lemma 2.3, we have that μ is extendible to a character of $I_{\text{Aut}(N)}(\mu)$, which implies that μ is extendible to a character of $I_G(\mu) = G \cap I_{\text{Aut}(N)}(\mu)$. Finally we note that $p \mid \mu(1)$ since $p \mid \theta(1)$. $\square$

Theorem 3.4. *Let p be an odd prime and set $a_p := 7/3$ if $p = 3$ and $a_p := (p+1)/2$ if $p \geq 5$. Let G be a finite group such that $\text{acd}_p(G) < a_p$. Then G is p -solvable.*

Proof. (i) Assume that the statement is false and let G be a minimal counterexample. In particular, G is not p -solvable. Take a minimal normal subgroup N of G such that $N \leq G'$. By Lemma 2.2, $\text{acd}_p(G/N) \leq \text{acd}_p(G) < a_p$. The minimality of G then implies that G/N is p -solvable, which in turns implies that N is not p -solvable since G is not. This means that N is a direct product of r copies of a non-abelian simple group, say S , with $p \mid |S|$.

Applying Theorem 3.3, we can now find a $\mu \in \text{Irr}(N)$ such that $p \mid \mu(1)$ and μ is extendible to a character of $I_G(\mu)$, and the latter induced to G yields an irreducible character of G of degree $d := \mu(1)[G : I_G(\mu)]$. It then follows from Lemma 2.1 that

$$n_1(G) \leq n_d(G)[G : I_G(\mu)].$$

Clearly, $(p-1)[G : I_G(\mu)] \leq 2p[G : I_G(\mu)] - p - 1$. Therefore,

$$(p-1)n_1(G) \leq (p-1)n_d(G)[G : I_G(\mu)] \leq n_d(G)(2p[G : I_G(\mu)] - p - 1).$$

Since $\mu(1) \geq p$, we then have $p[G : I_G(\mu)] \leq d$, and so

$$(p-1)n_1(G) \leq (2d - p - 1)n_d(G).$$

Now let $\text{Irr}^*(G) := \{\chi \in \text{Irr}(G) \mid \chi(1) = 1 \text{ or } d\}$. Since $\text{acd}_p(G) \leq p$, by Lemma 2.2 we have

$$\text{acd}_p(G) \geq \frac{\sum_{\chi \in \text{Irr}^*(G)} \chi(1)}{|\text{Irr}^*(G)|} = \frac{n_1(G) + dn_d(G)}{n_1(G) + n_d(G)} \geq \frac{p+1}{2}.$$

This is a contradiction when $p \geq 5$.

(ii) It now remains to consider the case $p = 3$. Note that A_5 and $\text{PSL}_2(7)$ are the only non-abelian simple groups with an irreducible character of degree 3. If $S = \text{PSL}_2(7)$, then it has an irreducible character of degree 6 that is extendible to a character of $\text{Aut}(\text{PSL}_2(7))$. Therefore, if $N \cong S^r$ is not isomorphic to A_5 , then from the construction of μ in the proof of Theorem 3.3, we have $\mu(1) = \theta(1)^r \geq 6$. We can now repeat the arguments in (i) to get $\text{acd}_3(G) \geq 7/2 > a_3$, and this violates the hypothesis.

(iii) The only case left is $p = 3$ and $N \cong A_5$. We then observe that N has two distinct irreducible characters, say μ_1 and μ_2 , of degree 3 that are fused under $S_5 \cong \text{Aut}(N)$. Here $I_{\text{Aut}(N)}(\mu_1) = I_{\text{Aut}(N)}(\mu_2) = N$ and $I_G(\mu_1) = I_G(\mu_2)$ has index 1 or 2 in G . Note that $\mathbf{C}_G(N) \cap N = 1$, $N\mathbf{C}_G(N) \leq I_G(\mu_1)$, and $G/N\mathbf{C}_G(N) \hookrightarrow \text{Out}(N) = C_2$. Suppose $[G : I_G(\mu_1)] = 2$. Then $I_G(\mu_1) = N \times \mathbf{C}_G(N)$ and so μ_1 extends to $I_G(\mu_1)$. It follows that G has an irreducible character of degree 6 lying above μ_1 , and $n_1(G) \leq 2n_6(G)$ by Lemma 2.1. Arguing as above, we obtain easily that $\text{acd}_3(G) \geq 8/3$. On the other hand, if $[G : I_G(\mu_1)] = 1$ then G does not induce an outer automorphism of $N = A_5$, and so $G \cong N \times \mathbf{C}_G(N)$. In this case, the outer tensor product of each $\mu_{1,2}$ with a linear character of $\mathbf{C}_G(N)$ yields an irreducible character of degree 3 of G , hence

$$n_1(G) = n_1(\mathbf{C}_G(N)), \quad n_3(G) \geq 2n_1(\mathbf{C}_G(N)),$$

and so $n_1(G) \leq n_3(G)/2$. It now follows that $\text{acd}_3(G) \geq 7/3 = a_3$, a contradiction. $\square$

We are now ready to prove Theorem B, which is restated below.

Theorem 3.5. *Let p be a prime and set $a_2 := 5/2$, $a_3 := 7/3$ and $a_p := (p+1)/2$ if $p \geq 5$. Let G be a finite group such that $\text{acd}_p(G) < a_p$. Then $\mathbf{O}^{p'}(G)$ is solvable.*

Proof. The case $p = 2$ was already proved in [HT, Theorem 1.2]. Therefore we may assume that p is odd.

Let G be a minimal counterexample to the statement. In particular, $\mathbf{O}^{p'}(G)$ is not solvable. Let N/N_1 be a non-abelian chief factor of G inside $\mathbf{O}^{p'}(G)$ such that $|N|$ is smallest possible. Then clearly N must be perfect, so that $N_1 \triangleleft N = N' \triangleleft G'$. It follows by Lemma 2.2 that

$$\text{acd}_p(G/N_1) \leq \text{acd}_p(G) < a_p,$$

and thus, by the minimality of G , we have $N_1 = 1$. This means that N is a non-abelian minimal normal subgroup of G . Suppose that

$$N = S_1 \times S_2 \times \cdots \times S_n,$$

where the S_i 's are all isomorphic to a non-abelian simple group S .

By Theorem 3.4 we know that G is p -solvable. So S is a p' -group. Since N is non-abelian, we have $N \not\leq \mathbf{C}_G(N)$, which implies that $\mathbf{O}^{p'}(G) \not\leq \mathbf{C}_G(N)$. It then follows that $|G/\mathbf{C}_G(N)|$ is divisible by p .

Now let K be the kernel of the transitive action of G on the set $\{S_1, S_2, \dots, S_n\}$ of the n simple direct factors of N . Since $\mathbf{C}_G(N) \leq K$, we deduce that

$$\text{either } p \mid |K/\mathbf{C}_G(N)| \text{ or } p \mid |G/K|.$$

Let us first consider the case $p \mid |G/K|$. Then $n \geq 2$ and, by Proposition 2.4, we can find $\mu \in \text{Irr}(N)$ such that $\mu(1) \geq 12$, μ is extendible to a character of $I_G(\mu)$, and $[G : I_G(\mu)]$ is divisible by p . Lemma 2.1 then implies that $n_1(G) \leq n_d(G)[G : I_G(\mu)]$, where $d := \mu(1)[G : I_G(\mu)] \geq 12[G : I_G(\mu)]$ is divisible by p . Now we can proceed as in the proof of Theorem 3.4 to show that $\text{acd}_p(G) \geq a_p$, and this is a contradiction.

We now may assume that $p \mid |K/\mathbf{C}_G(N)|$. Recall that S is a p' -group. Therefore, by Theorem 3.2, we can find $\theta \in \text{Irr}(S)$ such that θ is extendible to a character of $I_{\text{Aut}(S)}(\theta)$ and $p \nmid |I_{\text{Aut}(S)}(\theta)|$. Arguing as in the proof of Theorem 3.3 and viewing N as a subgroup of $G/\mathbf{C}_G(N)$, we then can show that $\mu := \theta \times \dots \times \theta \in \text{Irr}(N)$ is extendible to a character of

$$I_{G/\mathbf{C}_G(N)}(\mu) = (G/\mathbf{C}_G(N)) \cap I_{\text{Aut}(N)}(\mu),$$

where $I_{\text{Aut}(N)}(\mu) = I_{\text{Aut}(S)}(\theta) \wr S_n$. In particular, μ extends to a character of $I_G(\mu)$.

We claim that $[G : I_G(\mu)]$ is divisible by p . Recall that K is the kernel of the action of G on $\{S_1, S_2, \dots, S_n\}$. Hence $K/\mathbf{C}_G(N)$ is contained in $\text{Aut}(S)^n$, the base subgroup of the wreath product $\text{Aut}(N) = \text{Aut}(S) \wr S_n$. It follows that the index

$$\left[\frac{K}{\mathbf{C}_G(N)} : \left(\frac{K}{\mathbf{C}_G(N)} \cap I_{\text{Aut}(N)}(\mu) \right) \right] = \left[\frac{K}{\mathbf{C}_G(N)} : \left(\frac{K}{\mathbf{C}_G(N)} \cap I_{\text{Aut}(S)}(\theta)^n \right) \right]$$

is divisible by p since $p \mid |K/\mathbf{C}_G(N)|$ and $p \nmid |I_{\text{Aut}(S)}(\theta)|$. In particular, the index

$$\begin{aligned} [G : I_G(\mu)] &= [(G/\mathbf{C}_G(N)) : I_{G/\mathbf{C}_G(N)}(\mu)] \\ &= \left[\frac{G}{\mathbf{C}_G(N)} : \left(\frac{G}{\mathbf{C}_G(N)} \cap I_{\text{Aut}(N)}(\mu) \right) \right] \end{aligned}$$

is also divisible by p , as claimed above.

Now we again apply Lemma 2.1 to have $n_1(G) \leq n_d(G)[G : I_G(\mu)]$, where $d := \mu(1)[G : I_G(\mu)]$ is divisible by p . When $p \geq 5$ we can argue as in p. (i) of the proof of Theorem 3.4 to show that $\text{acd}_p(G) \geq a_p$. Suppose $p = 3$. Then, as N is a p' -group, N must be a simple Suzuki group. Hence, we can choose μ so that $\mu(1) \geq 6$, which implies that $\text{acd}_3(G) > 7/3 = a_3$, again a contradiction. $\square$

4. NORMALITY OF SYLOW p -SUBGROUPS

We start with a lemma.

Lemma 4.1. *Let p be a prime and let $G = N \rtimes H$ where N is an abelian group. Assume that $\text{acd}_p(G) \leq p$. Then, in the action of H on $\text{Irr}(N) \setminus \{1_N\}$, there exists an orbit $\mathcal{O}$ such that $|\mathcal{O}| = 1$ or $p \mid |\mathcal{O}|$ and*

$$\frac{|\mathcal{O}|(f+1)}{|\mathcal{O}|+f} \leq \text{acd}_p(G),$$

where f is the number of H -orbits on $\text{Irr}(N) \setminus \{1_N\}$ whose sizes are 1 or divisible by p .

Proof. (i) Let $\{1_N = \alpha_0, \alpha_1, \dots, \alpha_f, \alpha_{f+1}, \dots, \alpha_g\}$ be a set of representatives of the H -orbits on $\text{Irr}(N)$, where $\{\alpha_0, \alpha_1, \dots, \alpha_f\}$ are representatives of those orbits whose sizes are 1 or divisible by p . For each $0 \leq i \leq g$, let I_i be the inertia subgroup of α_i in G , and set

$$n_{i,p} := \sum_{p|k} n_k(I_i/N), \quad s_{i,p} := \sum_{\lambda \in \text{Irr}(I_i/N), p|\lambda(1)} \lambda(1).$$

Since G splits over N , every I_i also splits over N , and in fact $I_i = N/\text{Ker}(\alpha_i) \times I_H(\alpha_i)$ as N is abelian. It follows that α_i extends to a unique linear character β_i of I_i that is trivial at $I_H(\alpha_i)$. Gallagher's theorem then provides us with a bijective mapping $\lambda \mapsto \lambda\beta_i$ from $\text{Irr}(I_i/N)$ to the set of irreducible characters of I_i lying above α_i . By the Clifford correspondence, we then obtain a bijection $\lambda \mapsto (\lambda\beta_i)^G$ from $\text{Irr}(I_i/N)$ to the set of irreducible characters of G lying above α_i . We note that $(\lambda\beta_i)^G(1) = [G : I_i]\lambda(1)$, and hence $p \mid (\lambda\beta_i)^G(1)$ if and only if either $p \mid [G : I_i]$ or $p \mid \lambda(1)$.

(ii) Now we take $\text{Irr}^*(G)$ to be the set of irreducible characters $(\lambda\beta_i)^G$, where $\lambda \in \text{Irr}(I_i/N)$ and exactly one of the following holds:

- (a) $I_i = G$, $\lambda(1) = 1$;
- (b) $p \mid \lambda(1)$;
- (c) p divides $[G : I_i]$ and $\lambda(1) = 1$.

By its construction and the above discussion, $\text{Irr}^*(G)$ is contained in $\text{Irr}_p(G)$ and contains all linear characters of G . As $\text{acd}_p(G) \leq p$, Lemma 2.2 applies to $\text{Irr}^*(G)$. Note that the number of linear characters in $\text{Irr}^*(G)$ is $\sum_{i: G=I_i} n_1(I_i/N)$ (as they all come from type (a)). On the other hand, the non-linear characters in $\text{Irr}^*(G)$ come from types (b) and (c), and so the number of them is $\sum_{i: p|[G:I_i]} n_1(I_i/N) + \sum_{i=0}^g n_{i,p}$. It follows from Lemma 2.2 that

$$\sum_{\chi \in \text{Irr}^*(G)} \chi(1) \leq \text{acd}_p(G) \left(\sum_{i=0}^f n_1(I_i/N) + \sum_{i=0}^g n_{i,p} \right).$$

On the other hand,

$$\sum_{\chi \in \text{Irr}^*(G)} \chi(1) = \sum_{i=0}^f [G : I_i] n_1(I_i/N) + \sum_{i=0}^g [G : I_i] s_{i,p}$$

Since $s_{i,p} \geq p n_{i,p}$, it follows that

$$\sum_{\chi \in \text{Irr}^*(G)} \chi(1) \geq \sum_{i=0}^f [G : I_i] n_1(I_i/N) + p \sum_{i=0}^g [G : I_i] n_{i,p}$$

Therefore, we obtain

$$\text{acd}_p(G) \left(\sum_{i=0}^f n_1(I_i/N) + \sum_{i=0}^g n_{i,p} \right) \geq \sum_{i=0}^f [G : I_i] n_1(I_i/N) + p \sum_{i=0}^g [G : I_i] n_{i,p}$$

Using the hypothesis $\text{acd}_p(G) \leq p$, we deduce that

$$\text{acd}_p(G) \sum_{i=0}^f n_1(I_i/N) \geq \sum_{i=0}^f [G : I_i] n_1(I_i/N),$$

which is equivalent to

$$(4.1) \quad (\text{acd}_p(G) - 1)n_1(G/N) \geq \sum_{i=1}^f ([G : I_i] - \text{acd}_p(G))n_1(I_i/N)$$

since $I_0 = G$.

Now, observe that $n_1(G/N) = [(G/N) : (G/N)']$ and $n_1(I_i/N) = [(I_i/N) : (I_i/N)']$. Therefore $n_1(G/N) \leq [G : I_i]n_1(I_i/N)$ for every $1 \leq i \leq f$. Thus

$$n_1(G/N) \leq \frac{1}{f} \sum_{i=1}^f [G : I_i]n_1(I_i/N).$$

Together with (4.1), we deduce that

$$\frac{\text{acd}_p(G) - 1}{f} \sum_{i=1}^f [G : I_i]n_1(I_i/N) \geq \sum_{i=1}^f ([G : I_i] - \text{acd}_p(G))n_1(I_i/N).$$

Therefore, there must exist some index $1 \leq j \leq f$ so that

$$\frac{\text{acd}_p(G) - 1}{f} [G : I_j] \geq [G : I_j] - \text{acd}_p(G).$$

This is equivalent to

$$\frac{[G : I_j](f + 1)}{[G : I_j] + f} \leq \text{acd}_p(G),$$

and the proof is complete. $\square$

Finally we can prove the main theorem.

Theorem 4.2. *Let p be a prime and G a finite group. Let $\ell(p)$ be the smallest positive integer such that $\ell(p)p + 1$ is a prime power. If*

$$\text{acd}_p(G) < b_p := \frac{2\ell(p)p}{\ell(p)p + 1},$$

then G has a normal Sylow p -subgroup.

Proof. Since the theorem has been proved for $p = 2$ in [HT, Theorem 1.1], we assume from now on that p is odd. We will argue by induction on $|G|$. Let G be a finite group with $\text{acd}_p(G) < b_p$. By Theorem 3.5, we know that $\mathbf{O}^{p'}(G)$ is solvable.

First we consider the case $G' \cap \mathbf{O}^{p'}(G)$ is trivial. Then $\mathbf{O}^{p'}(G)$ can be viewed as a subgroup of G/G' , and thus it is abelian. It follows that the Sylow p -subgroup of $\mathbf{O}^{p'}(G)$ is normal in G , and we are done.

From now on we will assume that $G' \cap \mathbf{O}^{p'}(G)$ is nontrivial. In particular, we can choose a minimal normal subgroup N of G that is inside both G' and $\mathbf{O}^{p'}(G)$. Observe that $N \cong C_r^m$

is elementary abelian since $\mathbf{O}^{p'}(G)$ is solvable. Furthermore, $\text{acd}_p(G/N) \leq \text{acd}_p(G) < b_p$ by Lemma 2.2. The induction hypothesis now implies that G/N has a normal Sylow p -subgroup, say P_1/N . If N is a p -group then P_1 is a normal Sylow p -subgroup of G , and we are done.

So we will assume that N is an elementary abelian p' -group, and so $P_1 = N \rtimes P$ for a Sylow p -subgroup of P_1 . By Frattini's argument we have $G = P_1 \mathbf{N}_G(P) = N \mathbf{N}_G(P)$. If N is contained in the Frattini subgroup $\Phi(G)$ of G , we would have $G = \mathbf{N}_G(P)$, which means that $P \trianglelefteq G$, and we are done. So it remains to consider the case that $N \not\leq \Phi(G)$. We then choose a maximal subgroup H of G such that $N \not\leq H$, so that $G = NH$. Now $N \cap H \trianglelefteq H$, and $N \cap H \trianglelefteq N$ as N is abelian. It follows that $N \cap H \trianglelefteq G$, and thus $N \cap H = 1$ by the minimality of N . We conclude that G is a split extension of N by H .

Recall $P_1 = N \rtimes P \trianglelefteq G$. Suppose we can find a non-principal irreducible character λ of N that is P_1 -invariant. Then, for every $g \in P_1$ and $n \in N$, we have

$$\lambda(n) = \lambda^g(n) = \lambda(gng^{-1}),$$

and thus $\lambda([g, n]) = 1$. Since λ is not the principal character, we deduce that $[N, P_1] \leq \text{Ker}(\lambda)$ is a proper subgroup of N . The minimality of N then implies that $[N, P_1] = 1$ since $[N, P_1] \triangleleft G$. This means that $P_1 = N \times P$, and we can again conclude that $P \trianglelefteq G$.

We may now assume that every P_1 -orbit, whence every H -orbit, on $\text{Irr}(N) \setminus \{1_N\}$, has size divisible by p . We now can apply Lemma 4.1 to deduce that, in the action of H on $\text{Irr}(N) \setminus \{1_N\}$, there is an orbit $\mathcal{O}$ such that $p \mid |\mathcal{O}|$ and

$$(4.2) \quad \frac{|\mathcal{O}|(f+1)}{|\mathcal{O}|+f} \leq \text{acd}_p(G),$$

where f is the number of H -orbits on $\text{Irr}(N) \setminus \{1_N\}$. If furthermore $f \geq 2$, then

$$\frac{|\mathcal{O}|(f+1)}{|\mathcal{O}|+f} \geq \frac{3p}{p+2} > b_p > \text{acd}_p(G),$$

contradicting (4.2). Thus $f = 1$, and so $|\mathcal{O}| = |\text{Irr}(N) \setminus \{1_N\}| = r^m - 1$. By the definition of $\ell(p)$, we have $|\mathcal{O}| \geq \ell(p)p$, and so

$$\frac{|\mathcal{O}|(f+1)}{|\mathcal{O}|+f} = \frac{2\ell(p)p}{\ell(p)p+1} = b_p > \text{acd}_p(G),$$

again contradicting (4.2). $\square$

5. PROOF OF THEOREMS 3.1 AND 3.2

Note that Theorem 3.1 has been established for $p = 2$ in [HT], and p must be odd in Theorem 3.2. We therefore assume that $p > 2$ for the rest of the paper.

We first observe the following, which handles Theorem 3.1 in several cases.

Lemma 5.1. *Theorem 3.1 holds if $\text{Out}(S)$ is cyclic.*

Proof. By the Ito-Michler theorem, for every prime divisor p of $|S|$, there exists an irreducible character θ of S with $p \mid \theta(1)$. Since $I_{\text{Aut}(S)}(\theta)/S$ is a subgroup of $\text{Out}(S)$, out hypothesis on $\text{Out}(S)$ implies that $I_{\text{Aut}(S)}(\theta)/S$ is cyclic. [Isa, Corollary 11.22] in turns then implies that θ is extendible to $I_{\text{Aut}(S)}(\theta)$, as desired. $\square$

Lemma 5.1 implies Theorem 3.1 (at least) for the alternating groups A_n with $n \geq 7$ and all sporadic simple groups, since their outer automorphism groups are trivial or of order 2. For the same reason, Theorem 3.2 also holds for these simple groups. Therefore we may henceforth assume that S is a simple group of Lie type, say in characteristic r . We will assume furthermore that $S \neq \mathrm{Sp}_4(2)' \cong A_6, {}^2F_4(2)'$ as these cases can be confirmed easily using [Atl].

To prove Theorem 3.1, we will produce a set of irreducible characters of S , each of which is extendible to its inertia subgroup in $\mathrm{Aut}(S)$, such that the product of their degrees is divisible by every prime divisor of $|S|$. According to [F], the Steinberg character St of degree $|S|_r$ of S extends to $\mathrm{Aut}(S)$. Therefore, we only need to produce such a set of irreducible characters of S such that the product of their degrees is divisible by every prime divisor of $|S|_{r'}$.

We remark that many characters in the required set that we are about to construct are in fact real-valued or even strongly real (that is, of Frobenius-Schur indicator 1). We hope that this property will be useful in other applications.

5.1. Theorem 3.1 for classical groups in odd characteristic. Let $\mathcal{G}$ be a simple algebraic group of adjoint type defined over a field of characteristic r and $F : \mathcal{G} \rightarrow \mathcal{G}$ a Steinberg endomorphism such that $S = [G, G]$ for $G := \mathcal{G}^F$. Let $(\mathcal{G}^*, F^*)$ be dual to $(\mathcal{G}, F)$ and set $G^* := \mathcal{G}^{*F^*}$. According to the Deligne-Lusztig theory [C, DM] on complex representations of finite groups of Lie type, the set of irreducible complex characters of G is partitioned into rational series $\mathcal{E}(G, (s))$, which are labeled by conjugacy classes (s) of semisimple elements of G^* . For any semisimple element $s \in G^*$, there is a bijection $\chi \mapsto \psi$ from $\mathcal{E}(G, (s))$ to $\mathcal{E}(\mathbf{C}_{G^*}(s), (1))$ such that

$$\chi(1) = [G^* : \mathbf{C}_{G^*}(s)]_{r'} \psi(1).$$

Since $\mathcal{G}^*$ is simply connected, $\mathbf{C}_{\mathcal{G}^*}(s)$ is connected, and the character in $\mathcal{E}(G, (s))$ corresponding to the trivial character of $\mathcal{E}(\mathbf{C}_{G^*}(s), (1))$, denoted by χ_s , is called the semisimple character associated to s . The characters in $\mathcal{E}(G, (1))$ are unipotent characters of G . It is well known that the unipotent characters restricts irreducibly to S and thus we also call them unipotent characters of S . Unipotent characters of finite groups of Lie type have been completely described in [C, Sections 13.8 and 13.9] and we will use these descriptions without further notice.

We will frequently use the following property of unipotent characters:

Lemma 5.2. [M, Theorem 2.4] *Let S be a simple group of Lie type. Then every unipotent character of S extends to its inertia subgroup in $\mathrm{Aut}(S)$.*

Let us also recall the following fact, which was established in [T].

Lemma 5.3. *In the above notation, let s be a real semisimple element of order relatively prime to $\mathbf{Z}(G^*)$. Then χ_s is real-valued and restricts irreducibly to S . Furthermore, if $\chi_s(1)$ is odd, then $\theta := (\chi_s)_S$ is extendible to a (strongly real) character of $I_{\mathrm{Aut}(S)}(\theta)$.*

Proof. See [T, Lemma 2.2 and Proposition 5.1]. □

5.1.1. $S = \text{PSL}_n(q)$. A) First we consider $\text{PSL}_2(q)$ with $q \geq 5$. As the alternating groups of degree 5 and 6 were already handled, we assume that $q \neq 5, 9$. Irreducible characters of two-dimensional linear groups are well known, see [W] for instance. According to [W, p. 8], when q is odd, irreducible characters of degrees $q \pm 1$ of $\text{PSL}_2(q)$ can be labeled by:

- (i) $\chi_i, 1 \leq i \leq (q-3)/2$ and i even, of degree $q+1$,
- (ii) $\theta_j, 1 \leq j \leq (q-1)/2$ and j even, of degree $q-1$,

Here, for the reader's convenience, we use the same notation as in [W]. Let φ be the field automorphism of order f of $\text{PSL}_2(q)$. Then, by [W, Lemma 4.8], the character $\chi_i \in \text{Irr}(\text{PSL}_2(q))$ is invariant under φ^k where $1 \leq k \leq f$ if and only if $(p^f - 1) \mid i(p^k - 1)$ or $(p^f - 1) \mid i(p^k + 1)$; and the character $\theta_j \in \text{Irr}(\text{PSL}_2(q))$ is invariant under φ^k if and only if $(p^f + 1) \mid j(p^k - 1)$ or $(p^f + 1) \mid j(p^k + 1)$. It is then routine to check that, when $q \neq 5, 9$, the characters χ_2 and θ_2 are not invariant under any field automorphism. It is well known that every irreducible character of $\text{PSL}_2(q)$ of degree $q \pm 1$ is invariant under the diagonal automorphism. Thus,

$$I_{\text{Aut}(S)}(\chi_2) = I_{\text{Aut}(S)}(\theta_2) = \text{PGL}_2(q).$$

As $\text{PGL}_2(q)/S \cong C_2$, both χ_2 and θ_2 are extendible to $\text{PGL}_2(q)$ and we now have a required set $\{\text{St}_S, \chi_2, \theta_2\}$.

B) Now we can suppose $n \geq 3$. Case IIa of the proof of [MT, Proposition 4.7] produces a regular semisimple element $s_1 \in G^*$ such that the semisimple character $\chi_{s_1} \in \text{Irr}(G)$ satisfies $\theta_1 = (\chi_{s_1})_S \in \text{Irr}(S)$ and $I_{\text{Aut}(S)}(\theta_1) = G$. Moreover,

$$|\mathbf{C}_{G^*}(s)| = (q^m - 1)(q - 1)^{n-m-1},$$

where $m \in \{n, n-1\}$ is chosen to be odd. We then have

$$\theta_1(1) = [G^* : \mathbf{C}_{G^*}(s_1)]_{r'} = \frac{\prod_{i=2}^n (q^i - 1)}{(q^m - 1)(q - 1)^{n-m-1}}.$$

Suppose that $n = 3$. Consider the semisimple character $\chi_{s_2} \in \text{Irr}(\text{PGL}_3(q))$ where $s_2 \in G^* = \text{SL}_3(q)$ is a diagonal matrix with eigenvalues $-1, -1, 1$. As s_2 is real of order 2 and $|\mathbf{Z}(G^*)| = \gcd(3, q-1)$, Lemma 5.3 implies that $\theta_2 := (\chi_{s_2})_S$ is irreducible. Moreover,

$$\theta_2(1) = [G^* : \mathbf{C}_{G^*}(s_2)]_{r'} = \frac{(q^2 - 1)(q^3 - 1)}{(q - 1)(q^2 - 1)} = q^2 + q + 1,$$

which is odd. Lemma 5.3 again yields that θ_2 is extendible to $I_{\text{Aut}(S)}(\theta_2)$.

Now suppose that $n \geq 4$. Then part (c) of the proof of [NT1, Proposition 5.5] yields a character $\theta_2 \in \text{Irr}(S)$ of degree

$$\theta_2(1) = \begin{cases} (q^n - 1)(q^{n-1} - 1)/(q - 1)^2, & \text{if } q \equiv 1 \pmod{4}, \\ (q^n - 1)(q^{n-1} - 1)/(q^2 - 1), & \text{if } q \equiv 3 \pmod{4}, \end{cases}$$

such that θ_2 is extendible to $\text{Aut}(S)$. The set $\{\text{St}_S, \theta_1, \theta_2\}$ now satisfies our requirement for all $n \geq 3$.

5.1.2. $S = \text{PSU}_n(q)$ with $n \geq 3$. It was shown in part IIb of the proof of [MT, Proposition 4.7] that there is a regular semisimple element $s_1 \in G^*$ so that the semisimple character $\chi_{s_1} \in \text{Irr}(G)$ satisfies the conditions $\theta_1 = (\chi_{s_1})_S \in \text{Irr}(S)$ and $I_{\text{Aut}(S)}(\theta_1) = G$. Moreover,

$$|\mathbf{C}_{G^*}(s_1)| = (q^m + 1)(q + 1)^{n-m-1},$$

where $m \in \{n, n-1\}$ is chosen to be odd. We then have

$$\theta_1(1) = [G^* : \mathbf{C}_{G^*}(s_1)]_{r'} = \frac{\prod_{i=2}^n (q^i - (-1)^i)}{(q^m + 1)(q + 1)^{n-m-1}}.$$

When $n = 3$, a similar construction as in the $\text{PSL}_3(q)$ case yields a character $\theta_2 \in \text{Irr}(S)$ of degree $q^2 - q + 1$ and θ_2 extends to $I_{\text{Aut}(S)}(\theta_2)$, and we obtain the required set $\{\text{St}_S, \theta_1, \theta_2\}$.

So we can assume that $n \geq 4$. According to the proof of [DNT, Theorem 2.1], $\text{Aut}(S)$ has a rank 3 permutation character $\rho = 1 + \alpha + \beta$ such that α_S and β_S are both irreducible. Moreover,

$$\alpha(1) = \frac{q^2(q^n - (-1)^n)(q^{n-3} - (-1)^{n-3})}{(q + 1)(q^2 - 1)}$$

and

$$\beta(1) = \frac{q^3(q^{n-1} - (-1)^{n-1})(q^{n-2} - (-1)^{n-2})}{(q + 1)(q^2 - 1)}.$$

We now have the set $\{\theta_1, \alpha_S, \beta_S\}$ with desired properties.

5.1.3. $S = \text{PSp}_{2n}(q)$, $\Omega_{2n+1}(q)$ with $n \geq 2$. It was shown in the proof of [MT, Proposition 4.5] that if s is a semisimple element of G^* of order a *primitive prime divisor* of $q^{2nf} - 1$ (see [Zs] for the definition and existence of such divisors), then the semisimple character $\chi_s \in \text{Irr}(G)$ restricts irreducibly to S and $I_{\text{Aut}(S)}(\theta) = G$ with $\theta := (\chi_s)_S$. Furthermore, $|\mathbf{C}_{G^*}(s)| = q^n + 1$, which implies that

$$\theta(1) = [G^* : \mathbf{C}_{G^*}(s)]_{r'} = (q^n - 1) \prod_{i=1}^{n-1} (q^{2i} - 1).$$

On the other hand, S has a unipotent character χ , parametrized by the symbol $\begin{pmatrix} 1 & n \\ 0 & 0 \end{pmatrix}$, of degree

$$\chi(1) = \frac{q(q^n + 1)(q^{n-1} - 1)}{2(q - 1)},$$

see [N, Corollary 3.2]. Lemma 5.2 asserts that χ is extendible to $I_{\text{Aut}(S)}(\chi)$ (which is in fact $\text{Aut}(S)$ in this case). Now the set $\{\theta, \chi\}$ fulfills our requirements.

5.1.4. $S = P\Omega_{2n}^\pm(q)$ with $n \geq 4$ even. The case $S = P\Omega_{2n}^-(q)$ with $2|n$ can be handled similarly as in the symplectic case with the note that the unipotent character χ is parametrized by the symbol $\begin{pmatrix} 1 & n-1 \\ - & - \end{pmatrix}$ and has degree

$$\chi(1) = \frac{q(q^n + 1)(q^{n-2} - 1)}{q^2 - 1},$$

see [N, Proposition 3.3].

Now we consider $S = P\Omega_{2n}^+(q)$ with $2|n$. When $n \geq 6$, part 6.5 of the proof of [T, Theorem 3.1] produces characters $\theta_{1,2} \in \text{Irr}(S)$ such that $I_{\text{Aut}(S)}(\theta_{1,2}) = G$ and $\theta_{1,2}$ are extendible to G . Furthermore

$$\theta_1(1) = \frac{(q^n - 1) \prod_{i=1}^{n-1} (q^{2i} - 1)}{(q^2 + 1)(q^{n-2} + 1)},$$

and

$$\theta_2(1) = \begin{cases} \frac{(q^n - 1) \prod_{i=1}^{n-1} (q^{2i} - 1)}{(q + \varepsilon)(q^{n-1} + \varepsilon)}, & \text{if } q \geq 5, \\ \frac{(q^n - 1) \prod_{i=1}^{n-1} (q^{2i} - 1)}{26(3^{n-3} - 1)}, & \text{if } q = 3, \end{cases}$$

where $q \equiv \varepsilon \pmod{4}$. The set $\{\text{St}_S, \theta_1, \theta_2\}$ satisfies our requirements.

Finally we consider $S = P\Omega_8^+(q)$. This group has three unipotent characters, parametrized by the symbols $\begin{pmatrix} 1 \\ 3 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 & 2 \\ 1 & 3 \end{pmatrix}$, and $\begin{pmatrix} 0 & 2 \\ 1 & 3 \end{pmatrix}$ of degrees

$$q(q^2 + 1)^2, \frac{1}{2}q^3(q - 1)^4(q^2 + q + 1), \text{ and } \frac{1}{2}q^3(q + 1)^4(q^2 - q + 1),$$

respectively. These three characters form our desired set.

5.1.5. $S = P\Omega_{2n}^\varepsilon(q)$ with $n \geq 5$ odd. As shown in part 6.7 of the proof of [T, Theorem 3.1], there exists a character $\theta \in \text{Irr}(S)$ which extends to a semisimple character of G of degree

$$\theta(1) = \prod_{i=1}^{n-1} (q^{2i} - 1).$$

Moreover $I_{\text{Aut}(S)}(\theta) = G$.

We have mentioned in the previous subsection that $S = P\Omega_{2n}^-(q)$ has a unipotent character χ parametrized by the symbol $\begin{pmatrix} 1 & n-1 \\ 1 \end{pmatrix}$ and has degree

$$\chi(1) = \frac{q(q^n + 1)(q^{n-2} - 1)}{q^2 - 1}.$$

On the other hand, $S = P\Omega_{2n}^+(q)$ has a unipotent character χ parametrized by the symbol $\begin{pmatrix} n-1 \\ 1 \end{pmatrix}$ of degree

$$\chi(1) = \frac{q(q^n - 1)(q^{n-2} + 1)}{q^2 - 1},$$

see [N, Proposition 3.4]. We now have the set $\{\theta, \chi\}$ as required.

5.2. Theorem 3.1 for classical groups in even characteristic. In this subsection, S is a simple classical group defined over a field $\mathbb{F}_q$ in characteristic 2, with $q = 2^f$. Departing from the viewpoint of S as $[G, G]$ used in §5.1, here we can find a simple simply connected algebraic group $\mathcal{H}$ and a Steinberg endomorphism $F : \mathcal{H} \rightarrow \mathcal{H}$ such that $S = H/\mathbf{Z}(H)$ for $H := \mathcal{H}^F$. Let $(\mathcal{H}^*, F^*)$ be dual to $(\mathcal{H}, F)$, and let $H^* := \mathcal{H}^{*F^*}$. The following lemma is a part of [T, Proposition 7.1].

Lemma 5.4. *In the above notation, assume that $s \in [H^*, H^*]$ is a real semisimple element such that $\mathbf{C}_{G^*}(s)$ is connected. Then the semisimple character $\chi_s \in \text{Irr}(H)$ is trivial at $\mathbf{Z}(H)$ and hence it can be viewed as a character of S . Moreover, it is extendible to a (strongly real) character of its inertia subgroup in $\text{Aut}(S)$.*

Note that $\text{Out}(S)$ can be read off from [GLS, Theorem 2.5.12]. Due to Lemma 5.1, we only need to consider the groups $\text{PSL}_n(q)$ with $n \geq 3$, $\text{PSU}_n(q)$ with $n \geq 3$, $\text{Sp}_4(q)$, and $\Omega_{2n}^+(q)$.

5.2.1. $S = \text{PSL}_n(q)$ with $n \geq 3$. First we suppose $n = 3$. As the case $S = \text{PSL}_3(8)$ can be checked easily using [Atl], we assume that $2 < q = 2^f \neq 8$. By [Zs], we can then find a primitive prime divisor $\ell > 3$ of $2^{2f} - 1$. Choose a real semisimple element $s \in \text{PSL}_2(q) < [H^*, H^*]$ of order ℓ and consider the associated semisimple character $\chi_s \in \text{Irr}(\text{SL}_3(q))$ of degree

$$\chi_s(1) = [H^* : \mathbf{C}_{H^*}(s)]_{2'} = q^3 - 1.$$

By Lemma 5.4, χ_s can be viewed as a character of S and it is extendible to its inertia subgroup in $\text{Aut}(S)$. We also note that $\text{PSL}_3(q)$ has a unipotent character $\chi^{(1,2)}$ of degree $q(q+1)$. The set $\{\chi_s, \chi^{(1,2)}\}$ fulfills the requirements.

When $S = \text{PSL}_6(2)$, we simply take the set of three unipotent characters parametrized by the partitions $(1, 5)$, $(2, 4)$, and $(1, 2, 3)$ of degrees 62, 588, and 6480, respectively. When $S = \text{PSL}_7(2)$, we take the set of three unipotent characters parametrized by the partitions $(1, 6)$, $(2, 5)$, and $(1, 1, 5)$ of degrees 126, 2540, and 5208, respectively.

Now we may assume that $n \geq 4$ and $(n, q) \neq (6, 2), (7, 2)$. Choose $m \in \{n-1, n\}$ to be even. The assumption of n and q implies by [Zs] that $2^{mf} - 1$ has a primitive prime divisor, say ℓ . Following part 7.3 of the proof of [T, Theorem 3.1], we choose an element $s \in \text{PSL}_n(q) = [H^*, H^*]$ with a preimage of order ℓ in $\text{Sp}_m(q) < \text{SL}_n(q) = L$. This element s is real and $\mathbf{C}_G(s)$ is connected, and therefore χ_s , viewed as a character of S , extends to its inertia subgroup in $\text{Aut}(S)$. Furthermore,

$$\chi_s(1) = [H^* : \mathbf{C}_{H^*}(s)]_{r'} = \frac{\prod_{i=2}^n (q^i - 1)}{(q-1)^{n-m-1} (q^m - 1)}.$$

The required set of characters will be $\{\chi_s, \chi^{(1, n-1)}, \chi^{(2, n-2)}\}$, where χ^α denotes the unipotent character of S parametrized by partition $\alpha \vdash n$. Note that

$$\chi^{(1, n-1)}(1) = \frac{q(q^{n-1} - 1)}{q - 1} \text{ and } \chi^{(2, n-2)}(1) = \frac{q^2(q^n - 1)(q^{n-3} - 1)}{(q-1)(q^2 - 1)}.$$

5.2.2. $S = \text{PSU}_n(q)$ with $n \geq 3$. The case $S = \text{PSU}_3(q)$ can be argued similarly as in the $\text{PSL}_3(q)$ case: here we can find two irreducible characters of degrees $q^3 + 1$ and $q(q-1)$ satisfying our conditions. So we suppose that $n \geq 4$. Again as in the linear case, one can construct a real semisimple element $s \in [H^*, H^*] = \text{PSU}_n(q)$ with an inverse image in $\text{Sp}_m(q) < \text{SU}_n(q)$ of order ℓ , where $m \in \{n, n-1\}$ is even and ℓ is a primitive prime divisor of $2^{mf} - 1$ if $4 \mid m$ and a primitive prime divisor of $2^{mf/2} - 1$ if $4 \nmid m$. Then, as shown in part 7.3 of the proof of [T, Theorem 3.1], the semisimple character $\chi_s \in \text{Irr}(S)$ extends to its inertia subgroup in $\text{Aut}(S)$, and

$$\chi_s(1) = [H^* : \mathbf{C}_{H^*}(s)]_{r'} = \frac{\prod_{i=2}^n (q^i - (-1)^i)}{(q+1)^{n-m-1} (q^m - 1)}.$$

This χ_s together with the unipotent characters $\chi^{(1,n-1)}, \chi^{(2,n-2)}$ of degrees

$$\chi^{(1,n-1)}(1) = \frac{q(q^{n-1} - (-1)^{n-1})}{q+1} \text{ and } \chi^{(2,n-2)}(1) = \frac{q^2(q^n - (-1)^n)(q^{n-3} - (-1)^{n-3})}{(q+1)(q^2-1)}.$$

will form a required set.

5.2.3. $S = \mathrm{Sp}_4(q)$ with $q \geq 4$. This group has three unipotent characters parametrized by the symbols $\begin{pmatrix} 0 & 1 & 2 \\ & 1 & \end{pmatrix}$, $\begin{pmatrix} 0 & 2 \\ & 1 \end{pmatrix}$, and $\begin{pmatrix} 0 & 1 \\ & 2 \end{pmatrix}$ of degrees

$$\frac{1}{2}q(q-1)^2, \frac{1}{2}q(q+1)^2, \text{ and } \frac{1}{2}q(q^2+1),$$

respectively. It is easy to check that every prime divisor of $|S|$ divides at least one of these degrees. Note that $\mathrm{Sp}_4(2)' \cong \mathbb{A}_6$ was already considered before.

5.2.4. $S = \Omega_{2n}^+(q)$ with $n \geq 4$. As the case $S = \Omega_8^+(2)$ can be checked directly using [Atl], we assume that $(n, q) \neq (4, 2)$. We then have $H \cong S \cong H^*$. Let ℓ be a primitive prime divisor of $2^{(2n-2)f} - 1$ and choose s to be a real semisimple element of G of order ℓ . This can be done since all semisimple elements of $\Omega_{2n}^\pm(q)$ are real when n is even, by [TZ, Proposition 3.1]. When n is odd, we just choose $s_1 \in \Omega_{2n-2}^-(q) < \Omega_{2n}^+(q)$. We now have a semisimple character of S of degree

$$\chi_s(1) = [H^* : \mathbf{C}_{H^*}(s)]_{r'} = \frac{(q^n - 1) \prod_{i=1}^{n-1} (q^{2i} - 1)}{(q+1)(q^{n-1} + 1)},$$

which is extendible to its inertia subgroup in $\mathrm{Aut}(S)$, by Lemma 5.4. On the other hand, S has a unipotent character parametrized by $\begin{pmatrix} 0 & 1 \\ & 1 \end{pmatrix}$ of degree

$$\frac{q^{2n} - q^2}{q^2 - 1},$$

see [N, Proposition 3.4]. This unipotent character and χ_s above will satisfy our conditions.

5.3. **Theorem 3.1 for exceptional groups of Lie type.** By Lemma 5.1, we only need to consider families with possible non-cyclic outer automorphism group, which are $G_2(3^f)$, $F_4(2^f)$, $E_6(q)$, and $E_7(q)$. However, our arguments below can be applied to all exceptional groups of Lie type.

Unipotent characters of groups of exceptional type are well known. It turns out that there are always unipotent characters of S such that the product of their degrees is divisible by $|S|$. To write down their degrees simply, let us denote Φ_k the k^{th} cyclotomic polynomial evaluated at q , and use the notation in [C, Section 13.9].

For $S = G_2(q)$ with $q = 3^f$, the characters $\phi_{1,3'}$, $G_2(\theta)$, and $\phi_{1,6}$ of degrees

$$\frac{1}{3}q\Phi_3\Phi_6, \frac{1}{3}\Phi_1^2\Phi_2^2, q^6,$$

respectively, satisfy our requirement. For $S = F_4(q)$ with $q = 2^f$, the characters $\phi_{8,3'}$, $F_4[i]$, and $\phi_{1,24}$ of degrees

$$q^3\Phi_4^2\Phi_8\Phi_{12}, \frac{1}{4}q^4\Phi_1^4\Phi_2^4\Phi_3^2\Phi_6^2, q^{24},$$

respectively, will do the job. For $S = E_6(q)$, we choose the characters $\phi_{81,6}$, $\phi_{1,36}$, $E_6[\theta]$, and $E_6[\theta^2]$ of degrees

$$q^6 \Phi_3^3 \Phi_6^2 \Phi_9 \Phi_{12}, \quad q^{36}, \quad \frac{1}{3} q^7 \Phi_1^6 \Phi_2^4 \Phi_4^2 \Phi_5 \Phi_8, \quad \frac{1}{3} q^7 \Phi_1^6 \Phi_2^4 \Phi_4^2 \Phi_5 \Phi_8,$$

respectively. Finally, for $S = E_7(q)$, we choose the characters $\phi_{27,2}$, $\phi_{189,5}$, $\phi_{1,63}$, $E_6[\theta]$, and $E_6[\theta^2]$ of degrees

$$q^2 \Phi_3^2 \Phi_6^2 \Phi_9 \Phi_{12} \Phi_{18}, \quad q^5 \Phi_3^2 \Phi_6^2 \Phi_7 \Phi_9 \Phi_{12} \Phi_{14} \Phi_{18}, \quad q^{63}, \\ \frac{1}{3} q^7 \Phi_1^6 \Phi_2^6 \Phi_4^2 \Phi_5 \Phi_7 \Phi_8 \Phi_{10} \Phi_{14}, \quad \frac{1}{3} q^7 \Phi_1^6 \Phi_2^6 \Phi_4^2 \Phi_5 \Phi_7 \Phi_8 \Phi_{10} \Phi_{14},$$

respectively.

Theorem 3.1 is now completely proved.

5.4. Proof of Theorem 3.2. Finally we prove Theorem 3.2, which we restate:

Theorem 5.5. *Let p be a prime and let S be a non-abelian simple group of order not divisible by p . Then there exists a non-principal character $\theta \in \text{Irr}(S)$ such that θ is extendible to a character of $I_{\text{Aut}(S)}(\theta)$ and $p \nmid |I_{\text{Aut}(S)}(\theta)|$.*

Proof. We already mentioned above that the theorem is obvious for the alternating groups and sporadic simple groups. Hence we will assume that S is a simple group of Lie type, defined over a field of $q = r^f$ elements.

First we suppose that q is odd. As in §5.1, we have $S = [G, G]$ where $G = \mathcal{G}^F$ with $\mathcal{G}$ a simple algebraic group of adjoint type defined over a field of characteristic r and $F : \mathcal{G} \rightarrow \mathcal{G}$ a Steinberg endomorphism. It has already been shown in Subsection 5.1 that, when G is a classical group in odd characteristic, it possesses a semisimple character χ_s where s is a semisimple element of the dual group G^* such that $\theta := (\chi_s)_S \in \text{Irr}(S)$ and $I_{\text{Aut}(S)}(\theta) = G$. Indeed, the proofs of [MT, Propositions 4.4, 4.5, and 4.7] produced such a character for all simple groups of Lie type in odd characteristic. So we are done when q is odd.

Now suppose that q is even. Recall that the order of $\text{Out}(S)$ is dfg , where d is the order of the group of diagonal automorphisms, f is the order of the cyclic group of field automorphisms (generated by a Frobenius automorphism), and g is the order of the group of graph automorphisms coming from automorphisms of the Dynkin diagram, see [GLS, Theorem 2.5.12]. Furthermore, $|S|$ is always divisible by d and g . If $p \nmid f$, then we can consider any non-principal character $\theta \in \text{Irr}(S)$ that extends to $I_{\text{Aut}(S)}(\theta)$ constructed in the proof of Theorem 3.1 and observe that $p \nmid |I_{\text{Aut}(S)}(\theta)|$.

So we may assume that $p \mid f$. The proof of [T, Proposition 5.8] constructed a (real) semisimple element $s \in G^*$ of order coprime to $|\mathbf{Z}(G^*)|$ such that the G^* -conjugacy class of s is not invariant under $\rho^{f/p}$, where ρ is a generator of the cyclic group of field automorphisms. By Lemma 5.3 and [T, Proposition 5.1(iii)], the semisimple character χ_s (of degree $[G^* : \mathbf{C}_{G^*}(s)]_{2'}$, which is odd) then restricts irreducibly to S , and $\theta := (\chi_s)_S$ extends to a (strongly real) character of $I_{\text{Aut}(S)}(\theta) = I_{\text{Aut}(S)}(\chi_s)$. Moreover, as the G^* -conjugacy class of s is not invariant under $\rho^{f/p}$, we have $p \nmid [I_{\text{Aut}(S)}(\chi_s) : S]$, and so the character θ fulfills our requirements. $\square$

5.5. Final remarks. By inspecting the unipotent characters and their degrees of Lie-type groups of low rank, it seems to us most of the prime divisors of such a group S divide the degree of a unipotent character of S . For instance, if $S \neq {}^2B_2(q)$ is a simple group of exceptional type, every prime divisor of $|S|$ divides the degree of a unipotent character of S , see [C, §13.9].

For classical groups, the same assertion is not true for linear groups, unitary groups, and non-split orthogonal groups in even dimension. However, it looks plausible that, when S is a symplectic group, an orthogonal group in odd dimension, or a split orthogonal group in even dimension, every prime divisor of $|S|$ divides the degree of a unipotent character of S . It would be useful to confirm this phenomenon, as it helps to conveniently establish results on divisibility and extendibility of characters, like Theorems 3.1 and 3.2.

REFERENCES

- [C] R. W. Carter, ‘*Finite groups of Lie type. Conjugacy classes and complex characters*’, Wiley and Sons, New York et al, 1985, 544 pp.
- [CD] C. Casolo and S. Dolfi, Products of primes in conjugacy class sizes and irreducible character degrees, *Israel J. Math.* **174** (2009), 403–418.
- [Atl] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, ‘*Atlas of finite groups*’, Clarendon Press, Oxford, 1985.
- [CN] J. Cossey and H. N. Nguyen, Controlling composition factors of a finite group by its character degree ratio, *J. Algebra* **403** (2014), 185–200.
- [DM] F. Digne and J. Michel, ‘*Representations of finite groups of Lie type*’, London Mathematical Society Student Texts 21, 1991, 159 pp.
- [DNT] S. Dolfi, G. Navarro, and Pham Huu Tiep, Primes dividing the degrees of the real characters, *Math. Z.* **259** (2008), 755–774.
- [F] W. Feit, Extending Steinberg characters, Linear algebraic groups and their representations, *Contemp. Math.* **153** (1993), 1–9.
- [GLS] D. Gorenstein, R. Lyons, and R. Solomon, ‘*The classification of the finite simple groups*’, Mathematical Surveys and Monographs, vol. 40, American Mathematical Society, Providence, RI, 1994.
- [HT] N. N. Hung and Pham Huu Tiep, Characters of even degree and normal Sylow 2-subgroups, *Math. Proc. Cambridge Philos. Soc.* **162** (2017), 353–365.
- [HLS] N. N. Hung, M. L. Lewis, and A. A. Schaeffer Fry, Finite groups with an irreducible character of large degree, *Manuscripta Math.* **149** (2016), 523–546.
- [Isa] I. M. Isaacs, ‘*Character theory of finite groups*’, AMS Chelsea Publishing, Providence, Rhode Island, 2006.
- [ILM] I. M. Isaacs, M. Loukaki, and A. Moretó, The average degree of an irreducible character of a finite group, *Israel J. Math.* **197** (2013), 55–67.
- [Ito] N. Itô, Some studies on group characters, *Nagoya Math. J.* **2** (1951), 17–28.
- [M] G. Malle, Extensions of unipotent characters and the inductive McKay condition, *J. Algebra* **320** (2008), 2963–2980.
- [MT] S. Marinelli and Pham Huu Tiep, Zeros of real irreducible characters of finite groups, *Algebra Number Theory* **7** (2013), 567–593.
- [Mic1] G. O. Michler, Brauer’s conjectures and the classification of finite simple groups, *Lecture Notes in Math.* **1178**, Springer, Berlin, 1986, 129–142.
- [MN] A. Moretó and H. N. Nguyen, On the average character degree of finite groups, *Bull. Lond. Math. Soc.* **46** (2014), 454–462.
- [NT1] G. Navarro and Pham Huu Tiep, Degrees of rational characters of finite groups, *Adv. Math.* **224** (2010), 1121–1142.

- [N] H. N. Nguyen, Low-dimensional complex characters of the symplectic and orthogonal groups, *Comm. Algebra* **38** (2010), 1157–1197.
- [T] Pham Huu Tiep, Real ordinary characters and real Brauer characters, *Trans. Amer. Math. Soc.* **367** (2015), 1273–1312.
- [TZ] Pham Huu Tiep and A. E. Zalesski, Real conjugacy classes in algebraic groups and finite groups of Lie type, *J. Group Theory* **8** (2005), 291–315.
- [W] D. L. White, Character degrees of extensions of $\mathrm{PSL}_2(q)$ and $\mathrm{SL}_2(q)$, *J. Group Theory* **16** (2013), 1–33.
- [Zs] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284.

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF AKRON, AKRON, OH 44325, USA
E-mail address: `hungnguyen@uakron.edu`

DEPARTMENT OF MATHEMATICS, RUTGERS UNIVERSITY, PISCATAWAY, NJ 08854, USA
E-mail address: `tiep@math.rutgers.edu`