CHARACTERS AND GENERATION OF SYLOW 2-SUBGROUPS

GABRIEL NAVARRO, NOELIA RIZO, A. A. SCHAEFFER FRY, AND CAROLINA VALLEJO

Abstract. We show that the character table of a finite group G determines whether a Sylow 2-subgroup of G is generated by 2 elements, in terms of the Galois action on characters. Our proof of this result requires the use of the Classification of Finite Simple Groups and provides new evidence for the so-far elusive Alperin–McKay–Navarro conjecture.

1. Introduction

One of the main themes in Finite Group Representation Theory is the study of how the values of characters in a p-block B of a finite group G affect the structure of a defect group D of B, and vice versa. This topic was already suggested by R. Brauer in his famous list of problems on Modular Representation Theory [2], which is still a source of inspiration for unveiling global/local connections in finite groups. In particular, the structure of p-blocks with cyclic group (for any p), and with dihedral, semidihedral or quaternion defect groups (for $p = 2$) are cornerstones of the theory, by pioneering work of R. Brauer, E. C. Dade, and J. B. Olsson in the 1970's (prior to the Classification of Finite Simple Groups).

After studying cyclic defect groups or defect 2-groups D such that D/D' has order 4 (these are dihedral, semidihedral or quaternion), where $D' = [D, D]$ is the derived subgroup of D, it is logical to study 2-blocks in which D is generated by two elements, a hypothesis that naturally generalizes at the same time both of the previous conditions. While for a given $n \geqslant 3$, there are just three isomorphism classes of groups D of order 2^n with $|D : D'| = 4$, it is interesting to remark that the number of non-isomorphic 2-generated groups of order 2^n grows exponentially with n (see [19]).

Note that a non-cyclic 2-group D is 2-generated if, and only if, $|D : \Phi(D)| = 4$, where $\Phi(D)$ is the Frattini subgroup of D. Our aim in this paper is to show that it is possible to characterize when $|P : \Phi(P)| = 4$ by means of the values of the odd-degree irreducible characters in the principal 2-block of G, where P is a Sylow p-subgroup of G.

2010 *Mathematics Subject Classification.* 20C20, 20C15.

Key words and phrases. Sylow 2-subgroups, character tables, Principal blocks, Alperin–Galois–McKay conjecture.

The first, second and fourth authors are partially supported by the Spanish Ministerio de Ciencia e Innovación PID2019-103854GB-I00 and FEDER funds. The third author is partially supported by the National Science Foundation under Grant No. DMS-1801156. The fourth author also acknowledges support by Spanish Ministerio de Ciencia e Innovación MTM2017-82690-P and the ICMAT Severo Ochoa project SEV-2015-0554. Part of this work was supported by the National Security Agency under Grant No. H98230-19-1-0119, The Lyda Hill Foundation, The McGovern Foundation, and Microsoft Research, while the second, third, and fourth authors were in residence at the Mathematical Sciences Research Institute in Berkeley, California, during the summer of 2019.

Let $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ be the Galois automorphism that cubes 2-power roots of unity and fixes odd-order roots of unity. The following global/local result is the main theorem of this paper.

Theorem A. *Let G be a finite group, let B be the principal 2-block of G, and let $P \in \mathrm{Syl}_2(G)$. Then $|P : \Phi(P)| = 4$ if and only if the number of σ-invariant odd-degree irreducible characters in B is 4.*

The statement of Theorem A is yet another consequence of the Alperin–McKay–Navarro conjecture [29], a conjecture that has turned out to be a quite useful motivation for contributions to [2, Problem 12] (see, for instance, [32, 35, 37, 39, 40]). In fact, it is also possible to prove that the Alperin–McKay–Navarro conjecture implies that $|P : \Phi(P)| = 9$ if and only if the number of τ-invariant, $3'$-degree characters in the principal 3-block of a group G with Sylow 3-subgroup P is 6 or 9; where here τ is the Galois automorphism that fixes $3'$-order roots of unity and raises 3-power roots of unity to the fourth power. It seems that a proof of this result would require additional techniques. It also remains a challenge to find a corresponding statement for primes larger than 3, or for a greater number of generators, if indeed they exist.

Our proof of Theorem A requires the Classification of Finite Simple Groups and a delicate reduction to almost simple groups of the problem. In particular, we believe that the results in Section 4 in this paper represent a contribution to the general problem of understanding the action of Galois automorphisms on the characters in blocks of nonabelian simple groups.

In view of the fact that 2-blocks with a defect group P with $|P : P'| = 4$ have a bounded, and quite small, number of irreducible Brauer characters (see Section 6.2 of [7]), it is natural to ask if the same happens if we instead assume that $|P : \Phi(P)| = 4$. The following elegant counterexample is due to G. Malle, and it is not so easy to find. Let $n = 2^a$ and let H be the Singer cycle in $\mathrm{SL}_n(2)$, of order $2^n - 1$. Then its normalizer contains a regular unipotent element u (of order n). The principal 2-block of the semidirect product of the natural module V with $H\langle u\rangle$ has a Sylow 2-subgroup P with $|P : \Phi(P)| = 4$ and at least $\frac{2^n-2}{n} + 1$ irreducible 2-Brauer characters.

Acknowledgements. This work started at the University of Birmingham, after a question of Ben Fairbairn. The first author would like to thank David Craven and Chris Parker for the kind hospitality. The second, third, and fourth authors thank the Mathematical Science Research Institute in Berkeley, CA, and its generous staff for providing a collaborative and productive work environment during their residency in the summer of 2019. The authors would like to extend their gratitude to Gunter Malle for carefully reading, and especially spotting some incomplete arguments in, an earlier draft of this manuscript. Last but not least, the authors are obliged to the anonymous referee for their useful suggestions and comments.

2. Preliminaries

Our notation for characters follows [17] and [30]. Our notation for blocks follows [27]. Sometimes we denote by $B_0(G)$ the principal p-block of G, where p is a fixed prime in the context. If p is our fixed prime, let $\sigma_k \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ be the automorphism that fixes p'-roots of unity and sends p-power roots of unity ξ to ξ^{1+p^k}. (So the automorphism σ defined in the introduction is σ_1 here, whenever $p = 2$.) By elementary number theory, we have that σ_k restricted to any cyclotomic field has order a power of p. Notice that a linear character λ of a finite group is fixed by σ_k if and only if the p-part of the order of λ divides p^k.

In the next results, we work with slightly more generality than is required. The following is a well-known result by J. G. Thompson.

Lemma 2.1. *Let G be a finite group, p be a prime and $P \in \mathrm{Syl}_p(G)$. If every linear character of P of order p extends to G, then G has a normal p-complement.*

Proof. Let M be the minimal normal subgroup of G such that G/M is a p-elementary abelian group. Clearly, $\Phi(P) \subseteq M \cap P$. If $\lambda \in \mathrm{Irr}(P)$ has order p and $\nu_P = \lambda$, where $\nu \in \mathrm{Irr}(G)$, notice that $(\nu_{p'})_P = 1$, so we may assume that ν has p-power order. Also, since $(\nu_P)^p = \lambda^p = 1$, we have that $\nu^p = 1$. Hence $M \subseteq \mathrm{Ker}(\nu)$ and $M \cap P \subseteq \mathrm{Ker}(\lambda)$. We deduce that $M \cap P \subseteq \Phi(P)$. By a theorem of Thompson (see Problem 6.20 of [17])

$$1 = \mathbf{O}^p(P) = \mathbf{O}^p(G) \cap P\,.$$

Hence G has a normal p-complement. □

Recall that if G is a finite group, $P \in \mathrm{Syl}_p(G)$ and $N \lhd G$, then $\Phi(PN/N) = \Phi(P)N/N$. We will frequently use the following fact.

Lemma 2.2. *Suppose that G is a finite group, and let $P \in \mathrm{Syl}_p(G)$. Let $N \lhd G$ be such that G/N has order divisible by p. Assume that $P/\Phi(P)$ has order p^2. Then either $PN/\Phi(P)N$ has order p and G/N has a cyclic Sylow p-subgroup, or $PN/\Phi(P)N$ has order p^2 and N has a normal p-complement.*

Proof. Let $\bar{G} = G/N$ and use the bar notation. Now, $1 < \bar{P}/\Phi(\bar{P})$ has order a divisor of p^2. If $\bar{P}/\Phi(\bar{P})$ has order p, then $\bar{P}$ is cyclic.

Suppose that $\bar{P}/\Phi(\bar{P})$ has order p^2. Let $Q = P \cap N$. Then $Q \subseteq \Phi(P)$ and therefore $N \cap \Phi(P) = Q \in \mathrm{Syl}_p(N)$. By Lemma 2.1 applied in the group NP, we obtain that NP has a normal p-complement, and so does N. □

Lemma 2.3. *Let G b a finite group. Write $K = \mathbf{O}^p(G)$, $P \in \mathrm{Syl}_p(G)$, and $Q = P \cap K$. Assume that $\lambda \in \mathrm{Irr}(Q)$ is linear of order p^k and is P-invariant. Then there exists $\rho \in \mathrm{Irr}(P)$ of order p^k that extends λ.*

Proof. Let τ be the restriction of σ_k to $\mathbb{Q}_{|G|} = \mathbb{Q}(\xi)$, where $\xi \in \mathbb{C}$ has order $|G|$. Consider $A = \langle \tau \rangle \times P$, so that A is a p-group and λ is A-invariant. By Lemma 2.1 (ii) of [32], λ^K has a p'-degree irreducible A-invariant constituent θ with p'-multiplicity. Let $\chi \in \mathrm{Irr}(G)$ be the canonical extension of θ (using Corollary 6.28 of [17]), which is $\langle \tau \rangle$-invariant (by uniqueness). Let $\psi = \chi_P$. We have that $[\chi_Q, \lambda] = [\theta_Q, \lambda] \not\equiv 0 \bmod p$. By Lemma 2.1(ii) of [32], there is some τ-invariant constituent $\rho \in \mathrm{Irr}(P)$ of ψ such that $[\rho_Q, \lambda]$ is not divisible by p. Since λ is P-invariant, $Q \lhd P$, and P is a p-group, it follows that $\rho_Q = \lambda$ (using Corollary 11.29 of [17]). Since $o(\lambda) = p^k$ and $o(\rho)$ divides p^k (because ρ is τ-invariant), we have that $o(\rho) = p^k$. This proves the lemma. □

Lemma 2.4. *Suppose that G is a finite group, $P \in \mathrm{Syl}_p(G)$ and $P\mathbf{C}_G(P) \leqslant H \leqslant G$. Suppose that $\theta \in \mathrm{Irr}(b)$ has p'-degree and it is σ_k-invariant, where b is the principal block of H. Then there exists a σ_k-invariant $\chi \in \mathrm{Irr}(G)$ of p'-degree in the principal block of G such that $[\chi_H, \theta]$ is not divisible by p.*

Proof. By the comments before Theorem 9.24 of [27], we know that b^G is defined. By Brauer's third main theorem (Theorem 6.7 of [27]), we have that $b^G = B$ is the principal block of G. Now, if

$$\Psi = \sum_{\chi \in \mathrm{Irr}(B)} [\theta^G, \chi]\chi\,,$$

we have that $\Psi(1)_p = \theta^G(1)_p = 1$ by Corollary 6.4 of [27]. Let $A = \langle\tau\rangle$, where here τ is the restriction of σ_k to the $|G|$-th cyclotomic field extension $\mathbb{Q}_{|G|}$ of $\mathbb{Q}$, as above. Since B is τ-invariant and θ is τ-invariant, we have that Ψ is τ-invariant. By Lemma 2.1 (ii) of [32], there is a p'-degree A-invariant constituent χ of Ψ with p'-multiplicity. □

If a group A acts by automorphisms on G and $\tau \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$, we shall denote by $\mathrm{Irr}_{p',A,\tau}(B_0(G))$ the set of $A \times \langle\tau\rangle$-invariant characters in the principal block of G which have degree not divisible by p. If A or τ are trivial, we choose not to write A or τ. In the next three results, we want to relate $\mathrm{Irr}_{p',\sigma}(B_0(G))$ with $\mathrm{Irr}_{p',\sigma}(B_0(H))$ for certain subgroups H in some special situations.

Lemma 2.5. *Let G be a finite group, p be a prime and $P \in \mathrm{Syl}_p(G)$. Write $N = \mathbf{O}^p(G)$, and suppose that G/N is cyclic and non-trivial. Then*

$$|\mathrm{Irr}_{p',\sigma_1}(B_0(G))| = p|\mathrm{Irr}_{p',P,\sigma_1}(B_0(N))|\,.$$

Proof. If $\chi \in \mathrm{Irr}_{p'}(G)$, we have that $\chi_N = \theta$ is irreducible by Corollary 11.29 of [17]. Also θ is P-invariant. Furthermore, if χ is σ_1-invariant, then θ is σ_1-invariant. Moreover, since G/N is a p-group, χ lies in the principal p-block of G if and only if θ lies in the principal p-block of N, using [27, Corollary 9.6]. Conversely, if $\theta \in \mathrm{Irr}_{p',P}(N)$, then θ is G-invariant. We claim that the determinantal order $o(\theta) = |N : \mathrm{Ker}(\det\theta)|$ of θ is coprime to p (here $\det\theta$ is defined as in [18, Problem 2.3]). Write $K = \mathrm{Ker}(\det\theta) \lhd G$ as θ (and hence $\det\theta$) is G-invariant. Take $O/K = \mathbf{O}^p(N/K)$, so that $O \lhd G$ and G/O is a p-group. By definition $O = N$ and hence N/K is a p'-group (recall N/K is cyclic). As $(\theta(1)o(\theta), |G : N|) = 1$, by [18, Corollary 6.28], θ has a canonical extension γ to G. In particular, γ is σ_1-invariant if and only if θ is. By [27, Corollary 9.6], if $\theta \in B_0(N)$, then $\mathrm{Irr}(G|\theta) \subseteq \mathrm{Irr}(B_0(G))$. In this case, there is a canonical bijection $\mathrm{Irr}(G/N) \to \mathrm{Irr}(G|\theta)$ given by $\lambda \mapsto \lambda\gamma$ (by the Gallagher correspondence Corollary 1.23 of [30]), where linear characters of G/N correspond to p'-degree characters of G over θ. Notice that if γ is σ_1-invariant and λ is linear, then $\lambda\gamma$ is σ_1-invariant if and only if λ is σ_1-invariant, which happens if and only if $\lambda^p = 1$. Recall that since $G/N > 1$ is a cyclic p-group, there are exactly p linear characters $\lambda \in \mathrm{Irr}(G/N)$ satisfying $\lambda^p = 1$. The proof of the lemma easily follows from these considerations. □

The following is elementary.

Lemma 2.6. *If G is a finite group of even order, then $|\mathrm{Irr}_{2',\sigma}(B_0(G))|$ is even.*

Proof. See Lemma 1.4 of [39]. □

Next is a well-known result of J. Alperin and E. C. Dade.

Theorem 2.7. *Suppose that N is a normal subgroup of G, with G/N a p'-group. Let $P \in \mathrm{Syl}_p(G)$ and assume that $G = N\mathbf{C}_G(P)$. Then restriction of characters defines a natural bijection between the irreducible characters of the principal blocks of G and N. In particular, $|\mathrm{Irr}_{p',\tau}(B_0(G))| = |\mathrm{Irr}_{p',\tau}(B_0(N))|$, for any $\tau \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$.*

Proof. The case where G/N is solvable was proved in [1] and the general case in [8]. The last part of the statement follows immediately since τ acts on $\mathrm{Irr}(B_0)$ (preserving character degrees). □

Finally, we shall need the following.

Theorem 2.8. *Suppose that G is a finite group, and N is a normal subgroup of G with $N = \mathbf{O}^p(N)$. Suppose that G/N has a normal p-complement K/N, and that $P \in \mathrm{Syl}_p(G)$. Let $L = N\mathbf{N}_G(P)$. Then there is a natural bijection*

$$\mathrm{Irr}_{p'}(B_0(G)) \to \mathrm{Irr}_{p'}(B_0(L))$$

which commutes with $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$-action.

Proof. Let $C = K \cap L$, and notice that $C/N = \mathbf{C}_{K/N}(P)$. By Theorem E of [37], there is natural bijection $^*\colon \mathrm{Irr}_{p',P}(B_0(K)) \to \mathrm{Irr}_{p',P}(B_0(C))$ that commutes with $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$-action. Since $N = \mathbf{O}^p(N)$ and K/N is a p'-group, notice that $K = \mathbf{O}^p(K)$ and $C = \mathbf{O}^p(C)$. Every $\theta \in \mathrm{Irr}_{p',P}(B_0(K))$ has a canonical extension $\hat{\theta}$ to G, and every $\eta \in \mathrm{Irr}_{p',P}(B_0(C))$ has a canonical extension $\hat{\eta}$ to L. Using the Gallagher correspondence, and the fact that G/K is a p-group, we have that each $\chi \in \mathrm{Irr}_{2'}(B_0(G))$ can be uniquely written as $\chi = \lambda\hat{\theta}$ for some $\lambda \in \mathrm{Irr}(G/K)$ linear, where $\theta = \chi_K$. Similarly, every $\psi \in \mathrm{Irr}_{2'}(B_0(L))$ can be uniquely written as $\psi = \lambda\hat{\eta}$ for some $\lambda \in \mathrm{Irr}(L/C) = \mathrm{Irr}(G/K)$ linear, where $\eta = \psi_C$. Hence $\lambda\hat{\theta} \mapsto \lambda\widehat{\theta^*}$ yields a natural bijection

$$\mathrm{Irr}_{2'}(B_0(G)) \to \mathrm{Irr}_{2'}(B_0(L))$$

that commutes with $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$-action. □

3. Proof of Theorem A

In this section, we prove that Theorem A is true it if holds for certain almost simple groups. We shall prove the following in Section 4.

Theorem 3.1. *Suppose that G is a finite almost simple group, with socle S. Assume that G/S is a cyclic 2-group or a group of odd order. Let $P \in \mathrm{Syl}_2(G)$. Then $P/\Phi(P)$ has order 4 if and only if $|\mathrm{Irr}_{2',\sigma_1}(B_0(G))| = 4$.*

Although in some of the following we could work in slightly more generality, let us fix now our prime $p = 2$, and let $\sigma = \sigma_1$ for the rest of the section. We recall that $\mathbf{O}_{2'}(G)$ lies in the kernel of every character in the principal block by [27, Theorem 6.10].

We shall need to use one of the main results of [39].

Theorem 3.2. *Suppose that G is a finite group. Then G has a cyclic Sylow 2-subgroup if and only if $|\mathrm{Irr}_{2',\sigma}(B)| = 2$, where B is the principal 2-block of G.*

Also, we need a different (and much easier version) of the previous result.

Lemma 3.3. *Suppose that G is a finite group and B is the principal 2-block of G. Then G has a normal 2-complement if and only if $\mathrm{Irr}_{2',\sigma}(B)$ consists of linear characters. Also, G has a cyclic Sylow 2-subgroup if and only if $\mathrm{Irr}_{2',\sigma}(B)$ consists of two linear characters.*

Proof. Let P be a Sylow 2-subgroup of G. We prove the first statement. First suppose that $\mathrm{Irr}_{2',\sigma}(B)$ consists of linear characters. Let $\lambda \in \mathrm{Irr}(P/\Phi(P))$. Write $P\mathbf{C}_G(P) = P \times U$, and consider $\hat{\lambda} = \lambda \times 1_U$. By Lemma 2.4 and the hypothesis, we have that λ extends to a σ-invariant character of G. By Lemma 2.1, we have that G has a normal 2-complement K. If furthermore $\mathrm{Irr}_{2',\sigma}(B)$ consists of two linear characters, then $P/\Phi(P)$ is cyclic, and P is cyclic.

Suppose that G has a normal 2-complement M. Then $\mathrm{Irr}(B) = \mathrm{Irr}(G/M)$ can be identified with $\mathrm{Irr}(P)$, by [27, Theorem 9.9.(c)]. Hence the converse follows trivially.

The second statement is a direct consequence of the first one, since groups with a cyclic Sylow 2-subgroup have a normal 2-complement by a well-known result proved independently by Frobenius and Burnside. □

In the final step of the proof of Theorem A, we shall arrive at a particular minimal situation. To solve that step takes longer than one would have expected.

Lemma 3.4. *Suppose that $G = NP$, where N is a nonabelian nonsimple minimal normal subgroup of G, $\mathbf{C}_G(N) = 1$, G/N is cyclic and $P \in \mathrm{Syl}_2(G)$. Let $S \lhd N$ be simple, $H = \mathbf{N}_G(S)$, $C = \mathbf{C}_G(S)$ and let $V \in \mathrm{Syl}_2(H/C)$. Then the following hold.*

(a) $|\mathrm{Irr}_{2',\sigma}(B_0(G))| = 4$ *if and only if* $H > SC$ *and* $|\mathrm{Irr}_{2',\sigma}(B_0(H/C))| = 4$.

(b) $|P : \Phi(P)| = 4$ *if and only if* $H > SC$ *and* $|V : \Phi(V)| = 4$.

Proof. Write $G/N = \langle Nx \rangle$ for some $x \in P$. Notice that $H \lhd G$ and $G/H = \langle Hx \rangle$. Suppose that G/H has order k. Then N is the direct product of the subgroups $\{S^{x^j}\}$, $j = 0, \ldots, k-1$ (where $x^j \in P$ are representatives of the right cosets of H in G). Write $Q = H \cap P = \mathbf{N}_P(S) \in \mathrm{Syl}_2(H)$. Let $R = N \cap P = N \cap Q \in \mathrm{Syl}_2(N)$, and let $R_1 = S \cap Q = S \cap P = S \cap R \in \mathrm{Syl}_2(S)$. By a standard argument, see for instance, the next to the last paragraph of the proof of Theorem 2.4 of [32], we have that $Q = \mathbf{N}_P(R_1)$. Also, $R = R_1 \times R_1^x \times \cdots \times R_1^{x^{k-1}}$. Use the bar convention so that $\bar{R}_1 = R_1C/C$ is a Sylow 2-subgroup of $\bar{S} = SC/C$ and $\bar{Q} = QC/C$ is a Sylow 2-subgroup of $\bar{H} = H/C$. Furthermore, $\bar{Q} \cap \bar{S} = \bar{R}_1$, and $\bar{Q}/\bar{R}_1$ is cyclic, and by hypothesis, nontrivial. Since $SC = S \times C$, we have that $\bar{R}_1$ is isomorphic to R_1. Notice too that H/SC is isomorphic to $\bar{Q}/\bar{R}_1$.

By hypothesis $S < N$. In particular, G/N is non-trivial, $H < G$ and $Q < P$. Since $P/R \cong G/N$ is cyclic, we have that $|P : R\Phi(P)| = 2$. Hence $Q \subseteq R\Phi(P)$ (otherwise $QR\Phi(P) = Q\Phi(P) = P$ would yield $Q = P$). If $R_1 \subseteq \Phi(P)$ then $R_1^x \subseteq \Phi(P)$ (hence for every x^j with $j \in \{0, \ldots k-1\}$), and thus $R \subseteq \Phi(P)$. Then $|P : \Phi(P)| = 2$ and P is cyclic. In particular R would be cyclic, a contradiction. Hence, $\Phi(P) < R_1\Phi(P) \leqslant R\Phi(P)$.

First we prove the 'only if' implication of (b). Assume that $|P : \Phi(P)| = 4$. Then $|R\Phi(P) : \Phi(P)| = 2$ and $R_1\Phi(P) = R\Phi(P)$. Let $\tau \in \mathrm{Irr}_Q(R_1)$ be linear of order 2. (Such character exists: for example, let $\lambda \in \mathrm{Irr}(R_1\Phi(P)/\Phi(P))$ be the only nontrivial, then $\lambda|_{R_1}$ is nontrivial linear of order 2 and $R_1 \cap \Phi(P) \subseteq \mathrm{Ker}(\lambda|_{R_1})$. Since $Q \subseteq R\Phi(P) = R_1\Phi(P)$, we also have that $\lambda|_{R_1}$ is Q-invariant. Moreover $\lambda|_{R_1}$ is the unique linear Q-invariant character of order 2 of R_1 with $R_1 \cap \Phi(P)$ in its kernel.) Write $\gamma = \tau \times \tau^x \times \cdots \times \tau^{x^{k-1}} \in \mathrm{Irr}(R)$. Then γ is linear of order 2 and, by Lemma 4.1(ii) of [35], is P-invariant. By Lemma 2.3, there exists $\nu \in \mathrm{Irr}(P/\Phi(P))$ that extends γ, and therefore τ. In particular, $\Phi(P) \cap R_1$ is contained in the kernel of τ (so $\tau = \lambda|_{R_1}$). Hence, we see that $\mathrm{Irr}_Q(R_1)$ contains a unique linear character of order 2. We claim that $H > SC$. Otherwise, $QC = (P \cap H)C = PC \cap SC = (P \cap S)C = R_1C$. Thus $\bar{Q} = \bar{R}_1$, and $\mathrm{Irr}_Q(R_1) = \mathrm{Irr}(R_1)$ has a unique linear character of order 2. Hence R_1 is cyclic, but this is impossible as S is nonabelian simple, and the claim follows.

Note that also $\bar{R}_1 \cong R_1$ has a unique $\bar{Q}$-invariant linear character of order 2 (as $Q \cap C = \mathbf{C}_P(S)$ acts trivially on $\mathrm{Irr}(R_1)$). Since every nontrivial character of $\bar{R}_1\Phi(\bar{Q})/\Phi(\bar{Q})$ corresponds to a $\bar{Q}$-invariant linear character of order 2 of $\bar{R}_1$ (note $\bar{R}_1\Phi(\bar{Q}) \leqslant \bar{Q}$), this implies that, $|\bar{R}_1 : \Phi(\bar{Q}) \cap \bar{R}_1| = |\bar{R}_1\Phi(\bar{Q}) : \Phi(\bar{Q})| = 2$. Note that $R \leqslant R_1C$. Then $\bar{Q}/\bar{R}_1$ is cyclic, because P/R is cyclic, and nontrivial, since otherwise R_1 would be cyclic, as in the paragraph above (a contradiction). We conclude that $|\bar{Q} : \Phi(\bar{Q})| = |\bar{Q} : \bar{R}_1\Phi(\bar{Q})||\bar{R}_1\Phi(\bar{Q}) : \Phi(\bar{Q})| = 4$.

We now prove the 'if' implication of (b). Assume that $|\bar{Q} : \Phi(\bar{Q})| = 4$ and that $H > SC$ (that is, $\bar{Q} > \bar{R}_1$). Since $|P : R\Phi(P)| = 2$ it suffices to show that $|R\Phi(P) : \Phi(P)| = 2$. By Lemma 2.3, every $\bar{Q}$-invariant linear character of $\lambda \in \mathrm{Irr}(\bar{R}_1)$ of order 2 extends to a linear character of $\bar{Q}$ of order 2, and hence $\bar{R}_1 \cap \Phi(\bar{Q}) \subseteq \mathrm{Ker}(\lambda)$. Using that $|\bar{Q} : \Phi(\bar{Q})| = 4$, so that $|\bar{R}_1\Phi(\bar{Q}) : \Phi(\bar{Q})| = 2$ we deduce that λ is unique.

We work to show that $|R\Phi(P) : \Phi(P)| = 2$. Note that $R\Phi(P)/\Phi(P) \cong R/R \cap \Phi(P)$. If $\gamma \in \mathrm{Irr}(R/R \cap \Phi(P))$ has order 2, then γ is P-invariant (because it may be identified with a character of $R\Phi(P)/\Phi(P) \leqslant P/\Phi(P)$). Therefore $\gamma = \tau \times \tau^x \times \cdots \times \tau^{x^{k-1}} \in \mathrm{Irr}(R)$ for some $\tau \in \mathrm{Irr}_Q(R_1)$ linear of order 2 (by Lemma 4.1(ii) of [35]). In particular τ seen as a character of $\bar{R}_1 \cong R_1$ is $\bar{Q}$-invariant of order 2, hence $\tau = \lambda$. We deduce that there is only one choice for γ, and $|R : R \cap \Phi(P)| = 2$, as wanted.

Finally, we show (a). By Lemma 4.1(ii) of [35], there is a natural bijection $\mathrm{Irr}_{2',Q}(S) \to \mathrm{Irr}_{2',P}(N)$ given by $\psi \mapsto \psi \times \psi^x \times \cdots \times \psi^{x^{k-1}}$ that respects σ-action and principal 2-blocks. (The last part follows from the definition of principal block as in [27, Definition 3.1]). In particular, $|\mathrm{Irr}_{2',P,\sigma}(B_0(N))| = |\mathrm{Irr}_{2',Q,\sigma}(B_0(S))|$. Of course, this equals $|\mathrm{Irr}_{2',QC/C,\sigma}(B_0(SC/C))|$, since S and SC/C are naturally isomorphic.

By Lemma 2.5 applied in G, we have that $|\mathrm{Irr}_{2',\sigma}(B_0(G))| = 2|\mathrm{Irr}_{2',P,\sigma}(B_0(N))|$. If $H > SC$, by the same lemma we also have that $|\mathrm{Irr}_{2',\sigma}(B_0(H/C))| = 2|\mathrm{Irr}_{2',Q,\sigma}(B_0(S))|$.

Suppose that $|\mathrm{Irr}_{2',\sigma}(B_0(G))| = 4$. Then we have that $|\mathrm{Irr}_{2',P,\sigma}(B_0(N))| = 2$. Thus $|\mathrm{Irr}_{2',Q,\sigma}(B_0(S))| = 2$. If $H = SC$, then $Q = (Q \cap S)\mathbf{C}_Q(S)$ fixes all irreducible characters of S. Then $|\mathrm{Irr}_{2',\sigma}(B_0(S))| = 2$. By Theorem 3.2, we have that S has a cyclic Sylow 2-subgroup, but this is not possible since S is nonabelian simple. Therefore we have that $H > SC$ in both directions, and $|\mathrm{Irr}_{2',\sigma}(B_0(G))| = |\mathrm{Irr}_{2',\sigma}(B_0(H/C))|$. ☐

Notice that in Lemma 3.4, we need that $H > SC$, otherwise the wreath product of A_5 with C_2 is a counterexample to both of its statements.

We are finally ready to prove Theorem A (assuming Theorem 3.1 on almost simple groups), which we restate now.

Theorem 3.5. *Suppose that G is a finite group, and let $P \in \mathrm{Syl}_2(G)$. Assume that Theorem 3.1 is true. Then $|P : \Phi(P)| = 4$ if and only if $|\mathrm{Irr}_{2',\sigma}(B_0(G))| = 4$.*

Proof. For both directions, we may assume that $\mathbf{O}_{2'}(G) = 1$.

Assume first that $|P : \Phi(P)| = 4$. We prove that $|\mathrm{Irr}_{2',\sigma}(B_0(G))| = 4$ by induction on $|G|$. First note that if U is a complement of P in $\mathbf{N}_G(P)$ and we write $V = \mathbf{O}_{p'}(\mathbf{N}_G(P))$, then U/V acts faithfully on $P/\Phi(P) \cong \mathsf{C}_2 \times \mathsf{C}_2$ by [18, Corollary 3.30]. Thus either $U = V$ or $U/V \cong \mathsf{C}_3$.

Let N be a minimal normal subgroup of G. Since $\Phi(P)N/N = \Phi(PN/N)$, we have that $|PN : \Phi(P)N|$ is 1, 2 or 4.

Assume that $|PN : \Phi(P)N| = 1$, then G/N has odd order. Thus $P \subseteq N$. If N is a 2-group, then we have that $P = N \lhd G$, and either $G = N$ or $G = \mathsf{A}_4$ (using that $\mathbf{O}_{2'}(G) = 1$ and U/V has order 1 or 3). In both cases, the result is clear. If N is nonabelian, then N is the direct product of k copies of a nonabelian simple group S. Also, P is the direct product of k copies of the Sylow 2-subgroup of S, which is not cyclic (as groups with cyclic Sylow 2-sugroups have a normal 2-complement). Since $P/\Phi(P)$ has order 4, necessarily $k = 1$, and N is simple. Since $\mathbf{O}_{2'}(G) = 1$ and $\mathbf{Z}(N) = 1$, we have that $\mathbf{C}_G(N) = 1$. It follows that G is almost simple in this case, and the result follows by Theorem 3.1.

Assume now that $|PN : \Phi(P)N| = 4$. By Lemma 2.2, we have that N has a normal 2-complement. Since $\mathbf{O}_{2'}(G) = 1$, we have in this case that N is a 2-group and $N \subseteq \Phi(P)$. By induction, we have that $|\mathrm{Irr}_{2',\sigma}(B_0(G/N))| = 4$. Hence, we only need to prove that if $\chi \in \mathrm{Irr}_{2',\sigma}(B_0(G))$, then N is in the kernel of χ and χ belongs to the principal block of G/N when viewed as a character of G/N. If τ is the restriction of σ to the $|G|$-th cyclotomic field, we know that τ has 2-power order. By Lemma 2.1(ii) of [32], we have that χ_P contains a linear τ-invariant constituent $\lambda \in \mathrm{Irr}(P)$. Since λ is τ-invariant, it follows that $\lambda^2 = 1$. Thus $N \subseteq \Phi(P) \subseteq \mathrm{Ker}(\lambda)$ and hence $N \subseteq \mathrm{Ker}(\chi)$. It remains to show that if $\bar{\chi} \in \mathrm{Irr}(G/N)$ is the character given by $\bar{\chi}(Nx) = \chi(x)$ for $x \in G$, then $\bar{\chi} \in \mathrm{Irr}(B_0(G/N))$. Since $\bar{\chi}$ has odd degree, it follows that $\bar{\chi}$ lies in a block of G/N of maximal defect P/N. By Problem 4.5 of [27], we only need to prove that if $Nx \in G/N$, with $x \in G$, is 2-regular with $P/N \subseteq \mathbf{C}_{G/N}(Nx)$, then

$$\left(\frac{|G/N : \mathbf{C}_{G/N}(Nx)|\bar{\chi}(Nx)}{\bar{\chi}(1)}\right) \equiv |G/N : \mathbf{C}_{G/N}(Nx)|$$

modulo any maximal ideal of the ring of algebraic integers in $\mathbb{C}$ containing 2. First notice that $Nx \in \mathbf{N}_{G/N}(P/N) = \mathbf{N}_G(P)/N$. Also, we may assume that x is a 2-regular element, using that $Nx = (Nx)_{2'} = Nx_{2'}$. Notice that

$$\mathbf{C}_{G/N}(Nx) = \mathbf{C}_G(x)N/N\,,$$

using that $(|N|, o(x)) = 1$ (and [18, Corollary 3.28]). We have shown that x is a 2-regular element of $\mathbf{N}_G(P)$ centralizing P/N. Therefore x centralizes $P/\Phi(P)$, and by [18, Corollary 3.29] we have that x centralizes P. In particular, $N \subseteq \mathbf{C}_G(x)$. Then $|G/N : \mathbf{C}_{G/N}(Nx)| = |G : \mathbf{C}_G(x)|$. Since χ is in the principal block of G, we have that

$$\left(\frac{|G/N : \mathbf{C}_{G/N}(Nx)|\bar{\chi}(Nx)}{\bar{\chi}(1)}\right) = \left(\frac{|G : \mathbf{C}_G(x)|\chi(x)}{\chi(1)}\right) \equiv |G : \mathbf{C}_G(x)|\,,$$

modulo any maximal ideal of the ring of algebraic integers in $\mathbb{C}$ containing 2, as desired.

Assume finally that $|PN : \Phi(P)N| = 2$. Then G/N has a cyclic Sylow 2-subgroup and therefore, a normal 2-complement K/N. Let $Q = P \cap N \in \mathrm{Syl}_2(N)$. Then $P/\Phi(P)Q$ and $\Phi(P)Q/\Phi(P)$ have order 2. Notice that U acts (trivially) on $P/\Phi(P)Q$ and $\Phi(P)Q/\Phi(P)$, and hence U acts trivially on $P/\Phi(P)$ by [18, Problem 3E.3]. In particular, $U \subseteq \mathbf{C}_G(P)$ by [18, Corollary 3.29] and hence $V = U$, so $\mathbf{N}_G(P) = P \times U$.

If N is a 2-group, then G is (2-)solvable. Hence $U \subseteq \mathbf{O}_{2'}(G) = 1$, by [18, Theorem 4.33]. In this case, $\mathbf{N}_G(P) = P$, and there is a natural bijection $\mathrm{Irr}_{2'}(G) \to \mathrm{Irr}_{2'}(P)$ that commutes with Galois action (see Theorem F of [28], the Galois equivariance follows immediately from the description of the natural bijection). Since G has only one 2-block (by Theorem 10.20 of [27]), the theorem is proven in this case. Thus we may assume that $\mathbf{O}_2(G) = 1$. In particular, N is a direct product of nonabelian simple groups. (Thus $\mathbf{O}^2(N) = 1$). By Theorem 2.8, and by induction, we may assume $M = PN \lhd G$. Since $\mathbf{N}_G(P) = P \times U = P\mathbf{C}_G(P)$, we have that $G = N\mathbf{N}_G(P) = M\mathbf{C}_G(P)$. By Theorem 2.7 and induction, we may assume that $G = M$. If $N = G$, then G is nonabelian simple and the statement follows by Theorem 3.1. Therefore we may assume that $N < G$. Recall that G/N is a cyclic 2-group. Notice that $\mathbf{C}_G(N) = 1$. Otherwise, since $N \cap \mathbf{C}_G(N) = 1$ and G/N is a 2-group, we will conclude that $\mathbf{O}_2(G) > 1$. Let $S \lhd N$ be (nonabelian) simple, and write $H = \mathbf{N}_G(S)$, $C = \mathbf{C}_G(S)$. We have that H/C is almost simple. Then $|\mathrm{Irr}_{2',\sigma}(B_0(G))| = 4$ now follows from Lemma 3.4 and Theorem 3.1.

Assume now that $|\mathrm{Irr}_{2',\sigma}(B_0(G))| = 4$, and we prove that $|P : \Phi(P)| = 4$ by induction on $|G|$. We divide the proof of this direction in several steps.

Step 1. If $N \lhd G$ and $\gamma \in \mathrm{Irr}_{2',\sigma}(B_0(NP))$, then there is $\eta \in \mathrm{Irr}_{2',\sigma}(B_0(G))$ lying over γ.

Proof. By Theorem 2.7 (applied to $NP \lhd NP\mathbf{C}_G(P)$), there is an extension $\hat{\gamma} \in \mathrm{Irr}_{2',\sigma}(B_0(NP\mathbf{C}_G(P)))$ of γ. By Lemma 2.4, the claim follows.

Step 2. We may assume that G has no proper normal subgroup M of odd index such that $\mathbf{C}_G(P) \subseteq M$.

Proof. Assume the contrary and let $M \lhd G$ be a proper normal subgroup of odd index in G with $\mathbf{C}_G(P) \subseteq M$.

By [33, Lemma 3.1], all irreducible characters of G that lie over characters in the principal block of M are in the principal block of G. In particular, $\mathrm{Irr}(G/M) \subseteq \mathrm{Irr}_{2',\sigma}(B_0(G))$ (for G/M has odd order) and hence $|\mathrm{Irr}(G/M)| \leqslant 4$ by hypothesis. Then $G/M \cong \mathsf{C}_3$ ([3], Note A). Since $|\mathrm{Irr}(G/M)| = 3$, we deduce that there is a unique $\eta \in \mathrm{Irr}(B_0(G))$ of odd degree, σ-invariant which does not contain M in the kernel. By Step 1, every $1 \neq \gamma \in \mathrm{Irr}_{2',\sigma}(B_0(M))$ lies under η. In particular, all such γ are G-conjugate, by Clifford's theorem, and there are exactly three of them (otherwise γ would give rise to three extensions in $\mathrm{Irr}_{2',\sigma}(B_0(G))$ by [32, Lemma 5.1]). Hence $|\mathrm{Irr}_{2',\sigma}(B_0(M))| = 4$ and we are done by induction.

Let N be a minimal normal subgroup of G. By Lemma 2.6 and using that $\mathrm{Irr}(B_0(G/N)) \subseteq \mathrm{Irr}(B_0(G))$, we have $|\mathrm{Irr}_{2',\sigma}(B_0(G/N))| = 2$ or 4, unless G/N has odd order.

Step 3. G/N does not have odd order.

Proof. Suppose first that N is semisimple. If G/N has odd order, then $\mathbf{C}_G(N) = 1$, using that $\mathbf{O}_{2'}(G) = 1$. Notice that $N\mathbf{C}_G(P) \lhd G$ since $G = N\mathbf{N}_G(P)$ by the Frattini argument. If $N\mathbf{C}_G(P) = G$, then by Theorem 2.7 and induction, we may assume that $G = N$. In this case, G is simple and the statement is true by Theorem 3.1. So we assume that $N\mathbf{C}_G(P) < G$, but this contradicts Step 2.

So we are left with the case where N is an elementary abelian 2-group. In this case $N = P$ and, since $\mathbf{O}_{2'}(G) = 1$, we have that $\mathbf{C}_G(N) = N$. By Step 2 we conclude that $G = N$, and hence $G \cong \mathsf{C}_2$, a contradiction.

Step 4. If $1 < K$ is any normal subgroup of G, then $|\mathrm{Irr}_{2',\sigma}(B_0(G/K))| \neq 4$.

Suppose now that $|\mathrm{Irr}_{2',\sigma}(B_0(G/K))| = 4$. By induction, we have that $|PK : \Phi(P)K| = 4$. Also, every odd-degree σ-invariant irreducible character of G in the principal block has K in its kernel. Hence, if $\theta \in \mathrm{Irr}_{2',\sigma}(B_0(KP))$, then K is in the kernel of θ, by Step 1. Assume that K is a 2-group. If $\theta \in \mathrm{Irr}(P/\Phi(P))$, then $K \subseteq \mathrm{Ker}(\theta)$. Hence $K \subseteq \Phi(P)$ and we have that $|P : \Phi(P)| = |PK : \Phi(P)K| = 4$. Assume that KP has a normal 2-complement, then K has normal 2-complement. Since $\mathbf{O}_{2'}(G) = 1$, then K is a 2-group, then $K \subseteq \Phi(P)$ as before and we are also done in this case. Hence, we may assume that KP does not have a normal 2-complement. By Lemma 3.3, there is some $\gamma \in \mathrm{Irr}_{2',\sigma}(B_0(KP))$ which is nonlinear. In particular, K is not contained in the kernel of γ, a contradiction.

Final Step. By Steps 3 and 4, it remains to deal with the case where $|\mathrm{Irr}_{2',\sigma}(B_0(G/N))| = 2$. By Theorem 3.2, we have that G/N has a normal 2-complement K/N and a nontrivial cyclic Sylow 2-subgroup PN/N. Since N is minimal normal and $\mathbf{O}_{2'}(G) = 1$, we deduce that $\mathbf{O}^2(K) = K$. By Lemma 2.5, we have that $|\mathrm{Irr}_{2',P,\sigma}(B_0(K))| = 2$.

Suppose that N is a 2-group. Then G is (2-)solvable, so G and K have only one 2-block (by Theorem 10.20 of [27]) namely the principal one. In particular, $|\mathrm{Irr}_{2',P,\sigma}(K)| = 2$. Since the Sylow 2-subgroup of K is normal and 2-elementary abelian, by [39, Lemma 2.2(a)] we conclude that $|\mathrm{Irr}_P(K)| = |\mathrm{Irr}_{2',P,\sigma}(K)| = 2$. If $1 \neq \lambda \in \mathrm{Irr}_P(N)$, then λ lies under some P-invariant irreducible character of K because λ^K has odd-degree. We see therefore that $|\mathrm{Irr}_P(K/N)| = 1$ and by the Glauberman correspondence, $\mathbf{C}_{K/N}(P) = 1$. This implies that $P = \mathbf{N}_G(P)$. By [28, Theorem F], there is a natural bijection $\mathrm{Irr}_{2'}(G) \to \mathrm{Irr}_{2'}(P)$ that commutes with Galois action (this easily follows from the description of the bijection). In particular $4 = |\mathrm{Irr}_{2',\sigma}(G)| = |\mathrm{Irr}_{2',\sigma}(P)| = |P : \Phi(P)|$ and we are done in this case.

So we may assume that N is semisimple. By Theorem 2.8 and induction, we may assume that $PN \lhd G$. Assume that $M = PN < G$, and write $H = \mathbf{C}_G(P)M \lhd G$. By Step 2, we have that $H = G$. By Theorem 2.7 (applied with respect to $M \lhd H = G$) and induction, we may assume that $G = M = PN$. Assume that $D = \mathbf{C}_G(N) > 1$. Then D is a 2-group since $D \cap N = 1$, and also $D < P$. By Lemma 2.6 and the hypothesis $|\mathrm{Irr}_{2',\sigma}(B_0(G/D))| = 2$ or 4. Step 4 forces $|\mathrm{Irr}_{2',\sigma}(B_0(G/D))| = 2$. Thus by Theorem 3.2, the subgroup $P/D \in \mathrm{Syl}_2(G/D)$ is cyclic. Let $Q = P \cap N \in \mathrm{Syl}_2(N)$. In particular $Q \cong QD/D \leqslant P/D$ is cyclic, a contradiction (as N is nonsolvable). We conclude that $D = 1$. If N is simple, then we are done by Theorem 3.1. So we may assume that N is nonabelian nonsimple. Then the theorem follows from Lemma 3.4 and Theorem 3.1 on almost simple groups. $\square$

4. Almost Simple Groups

The goal in this section is to prove Theorem 3.1.

4.1. **Alternating and Sporadic Groups.** Here we consider the cases of alternating groups, sporadic groups, and some small groups of Lie type. The following may be well-known, but we record it in part to illustrate the types of computations with semidirect products that are also required for the details of some of the results throughout Section 4.3 below.

Lemma 4.1. *Let n be a positive integer. Let $P \in \mathrm{Syl}_2(\mathsf{S}_n)$ and let $Q \in \mathrm{Syl}_2(\mathsf{A}_n)$. Then P/P' and Q/Q' are elementary abelian. If $n = 2^k$ or $2^k + 1$ with $k > 1$, then $|P : P'| = |Q : Q'|$. Otherwise, $|P : P'| = 2|Q : Q'|$.*

Proof. If $n = 2$ or 3, then the respective Sylow 2-subgroups are cyclic of order 2, so we may assume $n \geqslant 4$.

Suppose that $n = 2^k$ or $2^k + 1$, so $k > 1$. We proceed by induction on k to see that P/P' and Q/Q' are isomorphic to C_2^k.

If $k = 2$, then $P/P' \cong \mathsf{C}_2 \times \mathsf{C}_2 \cong Q/Q'$. Write P_j for a Sylow 2-subgroup of S_{2^j} and Q_j for a Sylow 2-subgroup of A_{2^j} with $Q_j \subseteq P_j$. With the notation of [38, Lemma 4.14] we can write $P_k = \{(x, y; z^\alpha) \mid x, y \in P_{k-1},\ \alpha \in \{0, 1\}\} \cong P_{k-1} \wr \langle z\rangle$, where z is an involution of signature 1 that permutes the two copies of P_{k-1}. Then $Q_k = \{(x, y; z^\alpha) \mid x, y \in P_{k-1}, \mathrm{sgn}(x) = \mathrm{sgn}(y),\ \alpha \in \{0, 1\}\}$. Hence, we can write $Q_k = H \rtimes \langle z\rangle$, where $H = \{(x, y; 1) \mid x, y \in P_{k-1}, \mathrm{sgn}(x) = \mathrm{sgn}(y)\}$. Since $P_k' = (P_{k-1}' \times P_{k-1}')\Delta P_{k-1}$, where $\Delta P_{k-1} = \{(x^{-1}, x; 1) \mid x \in P_{k-1}\} \leqslant P_k$, we have that $P_k/P_k' \cong P_{k-1}/P_{k-1}' \times \mathsf{C}_2$ (by $(x, y, z^\alpha)P_k' \mapsto (xy, z^\alpha)$). By induction $P_k/P_k' \cong \mathsf{C}_2^k$. Similarly, one can see that $Q_k' = (H \rtimes \langle z\rangle)' = H'\Delta H$, where $\Delta H = \{(h^{-1}, h; 1) \mid h \in P_{k-1}\}$. In particular, $Q_k/Q_k' \cong H/H'\Delta H \times \mathsf{C}_2$ and $H/H'\Delta H \cong Q_{k-1}/Q_{k-1}'$. As before, the conclusion holds by induction.

Now suppose that $n = 2^{k_1} + \cdots + 2^{k_t}$, with $k_1 > \ldots > k_t \geqslant 0$, is not of the form 2^k nor $2^k + 1$. We can write $P = P_{k_1} \times \cdots \times P_{k_t}$, with the notation for P_j as above. It follows from the first part of the proof that P/P' is elementary abelian. Note that $Q = \{(x_1, \ldots, x_t) \mid x_j \in P_{k_j}, \prod_j \mathrm{sgn}(x_j) = 1\}$. Of course, $Q' \subseteq P'$. Since P is the direct product of at least two nontrivial wreath products, then each of the projections of Q into P_{k_j} is surjective. Given $[x_j, y_j] \in P_{k_j}'$, we want to see that $(1, \ldots, [x_j, y_j], \ldots, 1) \in P'$ is a commutator in Q. This can be done using auxiliary elements $z_\ell \in P_\ell$ with $\mathrm{sgn}(z_\ell) = -1$ (for example z_ℓ of cycle type $(2, 1^{2^\ell - 2})$) whenever $P_\ell > 1$. In particular, $P' \subseteq Q'$ and so $P' = Q'$. Hence Q/Q' is elementary abelian as it is a subgroup of P/P' and $|P : P'| = 2|Q : Q'|$ as wanted. □

Lemma 4.2. *Theorem 3.1 holds when S is an alternating group A_n with $n \geqslant 5$.*

Proof. If $n \leqslant 9$, the statement can be checked using GAP, so we assume that $n > 9$. Since $\mathrm{Aut}(S) = \mathsf{S}_n$, the only possibilities for A are $A = \mathsf{A}_n$ or $A = \mathsf{S}_n$. Let $P \in \mathrm{Syl}_2(\mathsf{S}_n)$. If $n = 2^{k_1} + \cdots + 2^{k_t}$ where $0 \leqslant k_t < \cdots < k_1$, then using Lemma 4.1, $|P/P'| = |P/\Phi(P)| = 2^{k_1 + \cdots + k_t} > 8$, since $n > 9$. Similarly, since the characters of $\mathsf{S_n}$ are rational-valued, [23, Theorem 1.3] yields that $|\mathrm{Irr}_{2',\sigma_1}(B_0(\mathsf{S}_n))| = 2^{k_1 + \cdots + k_t} > 8$, and therefore $|\mathrm{Irr}_{2',\sigma_1}(B_0(\mathsf{A}_n))|$ and $|Q/Q'|$ are at least 8, using Lemma 4.1 and the fact that every odd-degree character of $\mathsf{S_n}$ restricts irreducibly to $\mathsf{A_n}$. □

The next lemma reduces us to the case of simple groups of Lie type. Throughout, we will let $\mathrm{PSL}_n^{\pm}(q)$ denote the group $\mathrm{PSL}_n(q)$ in the case $+$ and $\mathrm{PSU}_n(q)$ in the case $-$, and similar for $\mathrm{SL}_n^{\pm}(q)$, $\mathrm{GL}_n^{\pm}(q)$, and $\mathrm{PGL}_n^{\pm}(q)$.

Lemma 4.3. *Let S be a simple sporadic group or one of the simple groups $\mathrm{PSL}_3(2)$, $\mathrm{PSL}_3(4)$, $\mathrm{PSU}_4(2)$, $\mathrm{PSU}_4(3)$, $\mathrm{PSL}_5^{\pm}(2)$, $\mathrm{PSL}_6^{\pm}(2)$, ${}^2B_2(8)$, $B_3(2)$, $B_3(3)$, $D_4(2)$, $F_4(2)$, ${}^2F_4(2)'$, $E_6(2)$, ${}^2E_6(2)$, $G_2(2)'$, or $G_2(4)$. Then Theorem 3.1 holds for S.*

Proof. In these cases, the statement can be seen using [11] and the GAP Character Table Library, together with some computation with semidirect products along the lines of the groups of Lie type below. □

4.2. **General Preliminaries.** Due to the nature of their automorphism groups, the following lemmas will often be helpful in the case of groups of Lie type.

Lemma 4.4. *Let A be a finite group such that $A = G \rtimes C$ is the semidirect product of a subgroup G with a nontrivial cyclic 2-group C. Let $\mathcal{K} \leqslant \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ be a subgroup and let $\chi \in \mathrm{Irr}_{2'}(G)$ be invariant under C and $\mathcal{K}$. Then there exist at least two $\mathcal{K}$-invariant elements of $\mathrm{Irr}_{2'}(A)$ extending χ. In particular, for $\mathcal{K} = \langle \sigma_1 \rangle$, there are* exactly *two $\mathcal{K}$-invariant extensions.*

Proof. If χ is linear, then we may view χ as a character of G/G'. Since χ is invariant under the cyclic group $C \cong A/G$, we know that there are (linear) extensions to A, which we may view as characters of $A/\mathrm{Ker}(\chi) = G/\mathrm{Ker}(\chi) \times C$. Hence the characters $\chi \times 1_C$ and $\chi \times \eta$ give the desired extensions, where η denotes the unique member of $\mathrm{Irr}(C)$ of order 2. The general case follows using [17, Lemma 6.24], and the last statement follows from the fact that $\{1, \eta\}$ are the only characters of a cyclic 2-group fixed by σ_1. □

Lemma 4.5. *Let A be a finite group and let $G \lhd A$ with $|A/G|$ odd. If $\chi \in \mathrm{Irr}(G)$ is fixed by σ_1, then every element of $\mathrm{Irr}(A|\chi)$ is fixed by σ_1.*

Proof. This is a direct application of [32, Lemma 5.1]. □

The following lemma can be found, e.g., as [5, Lemma 17.2].

Lemma 4.6. *Let G be a finite group. Two characters of $S = G/\mathbf{Z}(G)$ are in the same block if and only if they are in the same block as a character of G.*

We also record the following:

Lemma 4.7. *Let $G \lhd A$ and $\chi \in \mathrm{Irr}_{2'}(B_0(G))$. Then:*

(1) There exists $\tilde{\chi} \in \mathrm{Irr}(B_0(A)|\chi)$;
(2) If $|A/G|$ is odd, then there exists $\tilde{\chi} \in \mathrm{Irr}_{2'}(B_0(A)|\chi)$; and
(3) If $|A/G|$ is a power of 2, then $B_0(A)$ is the unique block of A above $B_0(G)$.

Proof. Parts (1) and (3) are Theorem 9.4 and Corollary 9.6 of [27] in the case of the principal block, and part (2) follows from Clifford theory. □

4.3. **Groups of Lie type.** By a group of Lie type, we will mean a finite group $G = \mathbf{G}^F$ that is the set of fixed points of a connected reductive algebraic group $\mathbf{G}$ defined over $\overline{\mathbb{F}}_q$ with q a power of a prime p, under a Steinberg map F. We also keep the general set-up of [39, Section 3.1]. In particular, we fix a regular embedding $\mathbf{G} \hookrightarrow \widetilde{\mathbf{G}}$ as in [5, Chapter 15], and write $\widetilde{G} = \widetilde{\mathbf{G}}^F$. Here $\mathbf{Z}(\widetilde{\mathbf{G}})$ is connected and by [21] (see also [5, Theorem 15.11]), restrictions of characters from $\widetilde{G}$ to G are multiplicity-free. By a simple group of Lie type S, we mean $S = G/\mathbf{Z}(G)$ with $G = \mathbf{G}^F$ and $\mathbf{G}$ simple of simply connected type. In this situation, we will also write $\widetilde{S} = \widetilde{G}/\mathbf{Z}(\widetilde{G})$, so that $\mathrm{Aut}(S) = \widetilde{S} \rtimes D$ with D generated by certain so-called graph and field automorphisms of S. We also remark that $|\widetilde{S}/S|$ is relatively prime to q.

The set $\mathrm{Irr}(\widetilde{G})$ is partitioned into Lusztig series $\mathcal{E}(\widetilde{G}, s)$, where s ranges over semisimple elements of the dual group $\widetilde{G}^*$, up to $\widetilde{G}^*$-conjugacy. The characters $\mathcal{E}(\widetilde{G}, 1)$ are called *unipotent* characters, and there is a bijection between $\mathcal{E}(\widetilde{G}, s)$ and $\mathcal{E}(\mathbf{C}_{\widetilde{G}^*}(s), 1)$ such that if $\chi \in \mathrm{Irr}(\widetilde{G})$ corresponds to $\psi \in \mathcal{E}(\mathbf{C}_{\widetilde{G}^*}(s), 1)$, then $\chi(1) = [\widetilde{G}^* : \mathbf{C}_{\widetilde{G}^*}(s)]_{p'}\psi(1)$.

A similar statement holds for G (see [21]), where now we denote by $\mathcal{E}(\mathbf{C}_{G^*}(s), 1)$ the set of characters lying above those in $\mathcal{E}(\mathbf{C}_{G^*}(s)^\circ, 1)$. (Here as an abuse of notation, we define $\mathbf{C}_{G^*}(s)^\circ := (\mathbf{C}_{\mathbf{G}^*}(s)^\circ)^{F^*}$ where $(\mathbf{G}^*, F^*)$ is dual to $(\mathbf{G}, F)$ and $G^* = (\mathbf{G}^*)^{F^*}$.) We may therefore parametrize $\mathrm{Irr}(G)$ by (s, ψ) for $s \in G^*$ semisimple, up to conjugacy, and $\psi \in \mathcal{E}(\mathbf{C}_{G^*}(s), 1)$.

We will call any character in Lusztig correspondence with a character lying over one parametrized by $(s, 1_{\mathbf{C}_{G^*}(s)^\circ})$ a *semisimple* character of G. Note that a semisimple character has degree $[G^* : \mathbf{C}_{G^*}(s)]_{p'}$. In particular, for a semisimple element $s \in G^*$, we will often write χ_s for a choice of semisimple character of G corresponding to s.

It will be useful to recall that in our situation, a semisimple character χ_s of $\widetilde{G}$ is trivial on the center as long as $s \in \widetilde{G}^*$ lies in $[\widetilde{G}^*, \widetilde{G}^*]$, using [34, Lemma 4.4], and restricts irreducibly to G as long as s is not conjugate to sz for any $1 \neq z \in \mathbf{Z}(\widetilde{G}^*)$. Further, from [36, Corollary 2.5], $\chi_s^\varphi = \chi_{s^{\varphi^*}}$ for $\varphi \in D$, where φ^* is an automorphism of $\widetilde{G}^*$ dual to φ.

We begin with the following, which is a direct consequence of [41, Lemma 3.4 and Proposition 3.8].

Lemma 4.8. *Let G be a group of Lie type and let $\chi \in \mathrm{Irr}(G)$ be a semisimple character. Assume that one of the following holds:*

- *G is defined in characteristic 2; or*
- *G is defined in odd characteristic and χ is in a series indexed by $s \in G^*$ with $s^2 = 1$.*

Then χ is fixed by σ_1.

Proof. Let G be defined over $\mathbb{F}_q$. If $s \in G^*$ is semisimple with $s^2 = 1$ or with q a power of 2, then [41, Lemma 3.4] yields that $\mathcal{E}(G, s)$ is fixed by σ_1, since either $s^2 = 1$ or $|s|$ is odd, and σ_1 fixes odd roots of unity. Further, the Gelfand-Graev characters are fixed by σ_1 since they are induced from characters obtained from linear characters of $(\mathbb{F}_q, +)$, which is an elementary abelian 2-group or p-group with p odd. Hence [41, Proposition 3.8] yields every semisimple character in $\mathcal{E}(G, s)$ is fixed by σ_1. □

4.3.1. *Defining Characteristic.* Here we consider the case that $\mathbf{G}$ is defined in characteristic 2.

Proposition 4.9. *Let S be a simple group of Lie type defined in characteristic 2 and assume S is not isomorphic to an alternating group or one of the groups listed in Proposition 4.3. Let A be an almost simple group with socle S such that A/S is odd or a cyclic 2-group. Then $|\mathrm{Irr}_{2',\sigma_1}(B_0(A))| > 4$ and $|P/\Phi(P)| > 4$ for $P \in \mathrm{Syl}_2(A)$, unless $S = \mathrm{SL}_2(2^{2^b})$ or $\mathrm{PSU}_3(2^{2^{b-1}})$ with $b \geqslant 2$ and $A/S \cong C_{2^b}$ a 2-group of field automorphisms. In the latter cases, $|\mathrm{Irr}_{2',\sigma_1}(B_0(A))| = 4 = |P/\Phi(P)|$.*

Proof. We have $S = G/\mathbf{Z}(G)$, where $G = \mathbf{G}^F$ is a (perfect) group of Lie type of simply connected type over $\mathbb{F}_q$ with q a power of 2. Recall that $\widetilde{S}/S$ and $\mathbf{Z}(G)$ are trivial unless $\mathbf{G} = \mathrm{SL}_n$ or E_6, in which cases $\widetilde{S}/S \cong \mathbf{Z}(G)$ is odd and cyclic.

Let Φ and Π be the set of roots and simple roots, respectively, for $\widetilde{\mathbf{G}}$, with respect to a fixed F-stable Borel subgroup $\mathbf{B}$ and maximal torus $\mathbf{T}$ for $\widetilde{\mathbf{G}}$. Then we may write $\mathbf{B} = \mathbf{UT}$ where $\mathbf{U}$ is the unipotent radical.

1. The Character Side. We have $\mathrm{Irr}_{2'}(B_0(S)) = \mathrm{Irr}_{2'}(S)$ using [5, 6.14, 6.15, and 6.18]. Let $\mathcal{X}$ denote the set of semisimple characters of G trivial on $\mathbf{Z}(G)$. Then $\mathcal{X} \subseteq \mathrm{Irr}_{2',\sigma_1}(B_0(S))$, using Lemmas 4.6 and 4.8. Recall that if A/S is a cyclic 2-group, we may identify $A = S \rtimes C$, where $C \leqslant D$ is a cyclic 2-subgroup. We aim to show that:

(i) $\mathcal{X}$ contains at least five pairwise non-$\mathrm{Aut}(S)$-conjugate members; and
(ii) $\mathcal{X}$ contains at least three C-invariant members for any cyclic 2-subgroup $C \leqslant D$.

Note that (i) and (ii) will yield the result in the cases A/S is odd and A/S is a cyclic 2-group, respectively, using Lemmas 4.5, and 4.4, together with Lemma 4.7. Throughout the proof, let $\delta \in \mathbb{F}_{q^2}^\times$ denote an element of order 3 and when $q \geqslant 4$, let $\xi \in \mathbb{F}_{q^2}^\times$ with $|\xi| \notin \{1, 3\}$.

1.a. First assume S is not one of $G_2(q), F_4(q), {}^3D_4(q), {}^2B_2(q)$, ${}^2F_4(q)$, or $\mathrm{PSL}_n^\pm(q)$. In paragraphs 5 - 9 of [14, Proposition 4.3], two nontrivial semisimple elements of $\widetilde{G}^*$ are constructed in the case of defining characteristic larger than 3, using certain products of elements $h_\alpha(\delta)$, where h_α denotes a coroot corresponding to a simple root α for fixed root system for $\widetilde{\mathbf{G}}$ and δ is a certain element of $\mathbb{F}_{q^2}^\times$. The exact same arguments work here, replacing the δ used there with our δ of order 3, yielding two semisimple elements s_1 and s_2 of $\widetilde{G}^*$ whose corresponding characters χ_{s_1} and χ_{s_2} of $\widetilde{G}$ are trivial on $\mathbf{Z}(\widetilde{G})$, invariant under D, and have different degrees. In the case Φ is not of type E_6, we have $\widetilde{G} = G$, so we see (ii) holds. In the case Φ is type E_6, note that $\widetilde{S}/S$ has size dividing 3. Then if A/S is a cyclic 2-group, at least one of the constituents of each restriction χ_S is A-invariant for each of $\chi = \chi_{s_1}, \chi_{s_2}$, so (ii) still holds. (Here we identify χ_{s_i} with the corresponding character of $S = G/\mathbf{Z}(G)$.)

If $q \geqslant 4$, then in all cases, taking two additional characters $\chi_{s_1'}$ and $\chi_{s_2'}$ of $\widetilde{G}$ constructed in the same way as [14, Proposition 4.3], but with δ replaced with ξ will ensure two more non-Aut (S)-conjugate members of $\mathcal{X}$. Indeed, we see as before that $\chi_{s_1'}$ and $\chi_{s_2'}$ have different degrees. Further, the orders of the semisimple elements ensure that χ_{s_i} and $\chi_{s_i'}$ are not Aut (S)-conjugate for $i = 1, 2$, completing the argument for (i).

Now assume $q = 2$ and S is not as in Lemma 4.3. If S is ${}^2D_4(2)$, $E_7(2)$ or $E_8(2)$, then the list of character degrees available at [20] yields at least 5 odd-degree characters with multiplicity 1, completing the proof for these groups. If S is $B_n(2)$ or $C_n(2)$ with $n \geqslant 3$, then there are 5 odd-degree unipotent characters (see [24, Theorem 6.8]), completing the proof in this case since $\mathrm{Out}(S) = 1$ and unipotent characters of classical groups are rational-valued by [22, Corollary 1.12]. If S is $D_n(2)$ or ${}^2D_n(2)$ with $n \geqslant 5$, then we see that (i) holds since $G^* \cong G$ has at least 5 distinct centralizer structures of semisimple elements.

1.b. If $S = G_2(q)$ or $F_4(q)$, the list of character degrees available at [20] shows that there are at least five distinct odd character degrees, which must come from semisimple characters using [24, Theorem 6.8], accomplishing (i). (Recall that here we have excluded the case $q = 2$.) For $G_2(q)$, the character table is also available in CHEVIE [12]. To see that (ii) holds for $G_2(q)$, we may consider the trivial character, together with the unique character of degree $q^3 + \eta$, where $q \equiv \eta \pmod 3$, and the character $\chi_{14}(k)$ or $\chi_{18}(k)$ in CHEVIE notation with $\zeta_1^k = \delta$ or $\xi_1^k = \delta$, respectively, in the cases $\eta = 1$ or -1. Here ζ_1 and ξ_1 are primitive $q - 1$ and $q + 1$ roots of unity, respectively.

To see that (ii) holds for $S = F_4(q)$ in the case $q \equiv 1 \pmod 3$ (so q is an even power of 2), we want three members of $\mathcal{X}$ invariant under any 2-group of field automorphisms. This is achieved by considering the trivial character, the unique character of degree $\Phi_2^2\Phi_3^2\Phi_4^2\Phi_8\Phi_{12}$ (here Φ_m is the mth cyclotomic polynomial in q), and a semisimple character χ_s with $s = h_2 = (1, 1, z, z)$ in the notation of [43], taking $z = \delta$. Indeed, the generating field automorphism maps such an element to its inverse, which defines the same conjugacy class as s. When $S = F_4(q)$ with $q \equiv -1 \pmod 3$, we need three members of $\mathcal{X}$ invariant under the order-two graph automorphism. The trivial character, the unique character of degree $\Phi_1^2\Phi_3^2\Phi_4^2\Phi_8\Phi_{12}$, and the character guaranteed by [41, Lemma 5.7 and Proposition 6.4] yields (ii) in this case.

1.c. Let $S = {}^3D_4(q)$. If $3 \mid (q - 1)$, then taking the trivial character together with the characters $\chi_9(k_1), \chi_9(k_2), \chi_{11}(\ell_1)$, and $\chi_{11}(\ell_2)$ such that $|\zeta_1^{k_1}| = |\varphi_3^{\ell_1}| = 3$ and $|\zeta_1^{k_2}| \neq 3 \neq |\varphi_3^{\ell_2}|$ in CHEVIE notation show that (i) and (ii) are satisfied. If $3 \mid (q+1)$, we may instead use $\chi_{17}(k_i)$ and $\chi_{20}(\ell_i)$ with the roles of (ζ_1, φ_3) replaced by (ξ_1, φ_6). (Here ζ_1 is a $q - 1$ root of unity, ξ_1 is a $q + 1$ root of unity, and φ_3 and φ_6 are $q^2 + q + 1$ and $q^2 - q + 1$ roots of unity, respectively.)

1.d. If $S = {}^2B_2(2^{2n+1})$ or ${}^2F_4(2^{2n+1})$, then $\mathrm{Out}(S)$ is cyclic with odd order, so it suffices to know that (i) holds. For ${}^2F_4(2^{2n+1})$ with $n \geqslant 1$, this is clear just from the list of character degrees, found at [20]. For ${}^2B_2(2^{2n+1})$ with $n \geqslant 2$, there are four distinct odd character degrees, but using the character table in CHEVIE, we see there are at least two of the same degree that are not conjugate under field automorphisms, which generate $\mathrm{Out}(S)$.

1.e. For the remainder of part 1 of the proof, let $S = \mathrm{PSL}_n^{\pm}(q)$, $\widetilde{G} = \mathrm{GL}_n^{\pm}(q) \cong \widetilde{G}^*$, $G = \mathrm{SL}_n^{\pm}(q) = [\widetilde{G}, \widetilde{G}]$, and $\widetilde{S} = \mathrm{PGL}_n^{\pm}(q) \cong G^*$ for an appropriate value of n. Further, recall that in this situation, semisimple classes of $\widetilde{G}^*$ are determined by eigenvalues.

If $n \geqslant 4$ and $q \geqslant 4$, the characters of $\widetilde{G}$ of the form χ_s for $s \in [\widetilde{G}^*, \widetilde{G}^*]$ with eigenvalues $\{\delta, \delta^{-1}, 1, \dots, 1\}$, $\{\delta, \delta^{-1}, \delta, \delta^{-1}, 1, \dots, 1\}$, $\{\xi, \xi^{-1}, 1, \dots, 1\}$, and $\{\xi, \xi^{-1}, \xi, \xi^{-1}, 1, \dots, 1\}$ are irreducible on G and trivial on $\mathbf{Z}(\widetilde{G})$, since each s is non-conjugate to sz for any $1 \neq z \in$

$\mathbf{Z}(\widetilde{G})$. Since these semisimple elements are pairwise not $\mathrm{Aut}(S)$-conjugate and the same is true for their images in G^*, we see that the same is also true for the corresponding characters of S. Further, those involving δ are invariant under the field automorphisms, and in case $+$, all of these characters are also invariant under the inverse-transpose map, which induces the graph automorphism. This yields that (i) and (ii) hold for $\mathrm{PSL}_n^{\pm}(q)$ with $n \geqslant 4$ and $q \geqslant 4$.

If $n \geqslant 7$ and $q = 2$, the characters of $\widetilde{G}$ of the form χ_s for $s \in [\widetilde{G}^*, \widetilde{G}^*]$ with eigenvalues $\{\delta, \delta^{-1}, 1, \ldots, 1\}$ and $\{\delta, \delta^{-1}, \delta, \delta^{-1}, 1, \ldots, 1\}$ satisfy the same properties as above, showing that (ii) holds. To obtain (i), we note that there are at least two more semisimple elements of G whose centralizers in $\widetilde{G}$ have distinct structures, yielding at least two more non-Aut (S)-conjugate characters in $\mathcal{X}$ when the corresponding semisimple characters are restricted to G and viewed as characters of S.

1.f. Let $S = \mathrm{SL}_2(q)$ with $q \geqslant 8$ a power of 2. Then we obtain at least five $\mathrm{Aut}(S)$-orbits in $\mathcal{X}$ by taking semisimple characters of $\widetilde{S} = \widetilde{G} = \mathrm{GL}_2(q)$ corresponding to semisimple elements $s \in \widetilde{G}^* \cong \widetilde{G}$ with eigenvalues $\{\xi, \xi^{-1}\}$, where ξ ranges over elements $\xi \in \mathbb{F}_{q^2}^{\times}$, since they must restrict irreducibly to S. Write $q = 2^{2^b \cdot m}$ with m odd. If A/S is a cyclic 2-group, we may view A as $A = S \rtimes C$ with $C \leqslant \langle F_2^m \rangle$, where F_2 is the generating field automorphism induced by $x \mapsto x^2$. Then if $m > 1$, we may construct characters as above with $\xi = \xi_1$ and ξ_2, $2^m - 1$ and $2^m + 1$ roots of unity, respectively, to obtain two nontrivial semisimple characters invariant under C and yielding the desired three C-invariant members of $\mathcal{X}$. If $m = 1$ but C does not contain F_2, then C is contained in $\langle F_2^2 \rangle$. In this case, taking ξ_1 and ξ_2 to instead be 3rd and 5th roots of unity yields the result. Finally, if $m = 1$ and $C = \langle F_2 \rangle$, then the only nontrivial C-invariant character in $\mathrm{Irr}_{2'}(S)$ is of the form χ_s where s has eigenvalues $\{\delta, \delta^{-1}\}$ with $|\delta| = 3$. This yields $|\mathrm{Irr}_{2',\sigma_1}(B_0(A))| = 4$ in this case, using Lemma 4.4.

1.g. When $S = \mathrm{PSL}_3^{\pm}(q)$, we may consider the same semisimple elements of $\widetilde{G}^*$ as in case *1.f* above, adding an eigenvalue of 1. The corresponding semisimple characters of $\widetilde{S} = \mathrm{PGL}_3^{\pm}(q)$ are in this case also fixed by τ. However, in the case $3 \mid (q \mp 1)$, a semisimple element s of $\widetilde{G}^*$ with eigenvalues $\{\delta, \delta^{-1}, 1\}$, where $|\delta| = 3$, is conjugate to sz with $z = \delta \cdot I_3 \in \mathbf{Z}(\widetilde{G}^*)$. This yields that the corresponding character χ_s of $\widetilde{G}$ (or of $\widetilde{S}$) restricts to the sum of three irreducible characters of G (or S). The character χ_s is invariant under graph and field automorphisms, and hence for any 2-group of automorphisms C, at least one of these constituents must be fixed by C. Then with this in mind, the same arguments as for $\mathrm{SL}_2(q)$ above yield that (i) holds, and further (ii) holds except possibly if $q = 2^{2^b}$ and $C = \langle \tau F_2 \rangle$ in the case $+$ or $C = \langle F_2 \rangle$ in either case $\pm$.

So, let $S = \mathrm{PSL}_3(q)$, where $q = 2^{2^b}$ with $b \geqslant 2$ and let $A = S \rtimes C$ with C cyclic of size 2^b. Note that these conditions force $3 \mid (q-1)$ and $7 \mid (q^2+q+1)$. The semisimple character χ_s of $\widetilde{G}$, where s has eigenvalues $\{\delta, \delta^{-1}, 1\}$, restricts to the sum of three irreducible characters of G (or S) of degree $\frac{1}{3}(q + 1)(q^2 + q + 1)$. Since χ_s is A-invariant and $|C|$ is a power of 2, it follows that at least one of these three irreducible characters of S must also be C-invariant. Further, from [25, Lemma 3.5], we see that that all three of these characters are invariant under $\langle \tau F_2 \rangle$, completing (ii) when $C = \langle \tau F_2 \rangle$. In the case $C = \langle F_2 \rangle$, we may let $\mu \in \mathbb{F}_{q^3}^{\times}$ with $|\mu| = 7$ and consider the character χ_s of $\widetilde{G}$ with $s \in \widetilde{G}^*$ having eigenvalues

(μ, μ^2, μ^4), or equivalently, (μ, μ^q, μ^{q^2}). Then χ_s is trivial on $\mathbf{Z}(\widetilde{G})$, restricts irreducibly to G, and is invariant under C, completing the proof of (ii) in this case.

Finally, suppose $S = \mathrm{PSU}_3(q)$ with $q = 2^{2^{b-1}}$ and $b \geqslant 2$ and let $A = S \rtimes C$ with $C = \langle F_2 \rangle \cong C_{2^b}$. Note that $S = G$ in this case, since $3 \mid (q-1)$. The only nontrivial C-invariant odd-degree character of G comes from the character χ_s of $\widetilde{G}$, where $s \in \widetilde{G}^*$ has eigenvalues $\{\delta, \delta^{-1}, 1\}$, which is trivial on $\mathbf{Z}(\widetilde{G})$ and restricts irreducibly to G. Hence using Lemmas 4.4 and 4.7, we see that $|\mathrm{Irr}_{2',\sigma_1}(B_0(A))| = 4$ in this case.

2. The Sylow Side. Note that $|\mathbf{Z}(G)|$ and $|\widetilde{G}/G|$ are odd, so a Sylow 2-subgroup of S may be identified with one of G or $\widetilde{G}$, which is the unipotent radical $U = \mathbf{U}^F$. Now, by [10, Lemma 2.2], we have U/U' is isomorphic to the direct product $\prod_{\omega\in\Omega}(\mathbb{F}_{q^{|\omega|}}, +)$, where the product is taken over the orbits Ω of the action induced by F on the fundamental roots Π for $\widetilde{\mathbf{G}}$. In particular, from this we see that U/U' is not 2-generated, since we are assuming $q \geqslant 8$ in the case of $\mathrm{PSL}_2(q)$ and ${}^2B_2(q)$. Then $|P/\Phi(P)| > 4$ if A/S is odd.

Now, if $A = S \rtimes C$ with C induced by an order-two graph automorphism stabilizing U, then $U/\langle U', [U, C]\rangle$ is of the form $(\mathbb{F}_q, +)^k$, where k is the number of orbits of C on the simple roots Π. Note that in the cases with nontrivial graph automorphisms being considered, we have $q \geqslant 4$ or $k \geqslant 2$, and hence this is at least 2-generated. Then a generating set for $P/P' = U/\langle U', [U, C]\rangle \times C$ contains more than 2 elements.

Finally, if $A = S \rtimes C$ with C a cyclic 2-group generated by a field or graph-field automorphism φ, then $U/\langle U', [U, C]\rangle \cong (U/U')^{\varphi}$, the fixed points under φ. Hence this is at least 2-generated, yielding a generating set for $P/P' \cong U/\langle U', [U, C]\rangle \times C$ with more than two elements, except in the case $\varphi = F_2$ and $\mathbf{G} = \mathrm{SL}_2$ or $\mathbf{G} = \mathrm{SL}_3$ with F twisted. In the latter cases, we see $U/\langle U', [U, C]\rangle \cong (\mathbb{F}_2, +)$ is cyclic, so P/P' is 2-generated. □

4.3.2. *Non-Defining Characteristic.* Now we consider the case that $\mathbf{G}$ is defined in characteristic $p \neq 2$.

Lemma 4.10. *Let q be odd and let S be a simple group of type $G_2(q)$, $F_4(q)$, $E_7(q)$, or ${}^3D_4(q)$. Then every odd-degree character of S is rational-valued, and hence lies in the principal block. Further, the following hold:*

- $|\mathrm{Irr}_{2'}(S)| > 4$*;*
- *for $S \neq G_2(q)$, there are more than 4 odd degrees with multiplicity one; and*
- *for $S = G_2(q)$, exactly 4 of the odd degrees have multiplicity one.*

Proof. By [31, Lemma 3.1], we have all odd-degree real-valued characters lie in the principal block. Observing the character tables for $G_2(q)$ and ${}^3D_4(q)$ in CHEVIE, we see that odd-degree characters are rational and that the statements about multiplicities holds. We see from the list of character degrees in [20] that the odd character degrees of $F_4(q)$ and $E_7(q)_{sc}$ have multiplicity one. In all cases, there are more than five odd-degree characters. In the case of E_7, since $|\mathbf{Z}(E_7(q)_{sc})| = 2$, these characters are also trivial on the center and hence are characters of S. This completes the proof. □

Before stating the next lemma, we recall that the unipotent characters of $\widetilde{G}$ are irreducible when restricted to G and trivial on $\mathbf{Z}(\widetilde{G})$, by the work of Lusztig [21]. Hence we may view these characters as characters of $S, \widetilde{S}, G$, or $\widetilde{G}$, as needed.

Lemma 4.11. *Let G be a group of Lie type defined in odd characteristic such that $\mathbf{G}$ is of simply connected type A_{n-1} with $n \geqslant 6$, B_n or C_n with $n \geqslant 3$, D_n with $n \geqslant 5$, or E_n with $n \geqslant 6$, or such that G is of type ${}^2D_4$. Then there exist more than four odd-degree unipotent characters of G. Further, these characters are rational-valued as characters of $\widetilde{G}$, lie in the principal 2-blocks of $\widetilde{G}$ and G, and at least five of them extend to* $\mathrm{Aut}(S)$ *when viewed as characters of $S = G/\mathbf{Z}(G)$.*

Proof. By [26, Proposition 7.4], all unipotent characters of G with odd degree lie in the principal series, and hence are in bijection with $\mathrm{Irr}_{2'}(W)$, where W is the Weyl group of G. Further, by the work of Lusztig [22], every unipotent character is realizable over $\mathbb{Q}$ in the case of classical groups, and by [40, Proposition 4.4], all odd-degree unipotent characters (of G or $\widetilde{G}$) are realizable over $\mathbb{Q}$, and hence lie in the principal block using [31, Lemma 3.1]. For classical groups, W has a quotient isomorphic to $\mathsf{S_n}$, which has at least 8 odd-degree characters for $n \geqslant 6$, using [23, Corollary 1.3]. We also see, for example using GAP, that there are at least 8 odd-degree characters of W in the cases G is of type B_n or C_n with $3 \leqslant n \leqslant 5$, D_5, ${}^2D_4$, or ${}^2D_5$. In the case $\mathbf{G}$ is of type E_6, E_7, or E_8, the explicit list of unipotent character degrees in [6, Section 13.9] yields more than 4 odd-degree unipotent characters. The last assertion follows using [25, Proposition 2.3 and Theorem 2.5], noting that there are at least five unipotent characters in the case $D_n(q)$ with $n > 4$ even that are labeled by nondegenerate symbols. □

Proposition 4.12. *Let S be a simple group of Lie type defined in odd characteristic and such that S is not isomorphic to an alternating group or one of the groups listed in Lemma 4.3. Let A be an almost simple group with socle S such that A/S has odd order or is a cyclic 2-group, and let $P \in \mathrm{Syl}_2(A)$. Then $|\mathrm{Irr}_{2',\sigma_1}(B_0(A))| > 4$ and $|P/\Phi(P)| > 4$, unless one of the following holds:*

- *$S = \mathrm{PSL}_2(q)$ and A/S is not a cyclic 2-group generated by field automorphisms; or*
- *$S = \mathrm{PSL}_3^{\pm}(q)$ and $|A/S|$ is odd.*

In the latter cases, $|\mathrm{Irr}_{2',\sigma_1}(B_0(A))| = 4 = |P/\Phi(P)|$.

Proof. Recall that A may be viewed as a subgroup of a semidirect product $\widetilde{S} \rtimes C$, where $C \leqslant D$ has odd order or is a cyclic 2-group.

1. The Character Side. Similar to Proposition 4.9, except for the listed exceptional cases and some cases that must be treated slightly differently, our strategy is to show that there are at least 5 pairwise non-Aut (S)-conjugate members of $\mathrm{Irr}_{2',\sigma_1}(B_0(S))$ that restrict irreducibly from $B_0(\widetilde{S})$, which will give the result when $A \leqslant \widetilde{S}$ or $|A/S|$ is odd using Lemmas 4.5 and 4.7. We also aim to show that there are three members of $\mathrm{Irr}_{2',\sigma_1}(B_0(S))$ that are invariant under 2-elements in D, which will complete the proof using Lemma 4.4 in the remaining cases that A/S is a cyclic 2-group.

1.i. If $S = G/\mathbf{Z}(G)$ with G as in Lemmas 4.10 or 4.11, then we are done by combining those with Lemmas 4.4, 4.5, and 4.7. For $S = {}^2G_2(3^{2r+1})$, we see from the character table in CHEVIE [12] that there are exactly eight odd-degree characters and they are all fixed by σ_1, and from [44] that they all also lie in the principal block. Further, four of these character degrees have multiplicity one, yielding at least 5 pairwise non-Aut(S)-conjugate members of $\mathrm{Irr}_{2',\sigma_1}(B_0(S))$, which completes the proof in this case since $|\mathrm{Out}(S)|$ is odd.

In the remaining cases, G is of classical type, and using [5, 21.14], $B_0(G)$ is comprised of those series $\mathcal{E}(G,s)$ with $|s|$ a power of 2, and similar for $B_0(\widetilde{G})$.

1.ii. Now let $S = D_4(q) = \mathrm{P}\Omega_8^+(q)$ or $S = C_2(q) = \mathrm{PSp}_4(q)$. Here $\widetilde{S}/S$ is a 2-group. Using [25, Proposition 2.4 and Theorem 2.5], we see that there are four A-invariant unipotent characters of odd degree if A does not contain the graph automorphism of order 3 in the case $D_4(q)$, which are also rational-valued (even as characters of $\widetilde{S}$) by the work of Lusztig [22, Corollary 1.12]. This is enough if A/S is a nontrivial cyclic 2-group, using Lemma 4.4. Even if A contains the triality graph automorphism, note that four unipotent characters of odd degree may still be chosen to be pairwise non-A-conjugate.

Let $s \in G^*$ lie in the center of a Sylow 2-subgroup of G^* and have order 2. Then χ_s has odd degree and is σ_1-invariant by Lemma 4.8. Since G is perfect and $\mathbf{Z}(G)$ is a 2-group, we see that χ_s may be viewed as a character of $\mathrm{Irr}_{2'}(B_0(S))$, using Lemma 4.6. Since χ_s is not $\mathrm{Aut}(S)$-conjugate to any unipotent character, this takes care of the case $|A/S|$ is odd.

It remains to deal with the cases $S = \mathrm{PSL}_n^{\pm}(q)$ with $2 \leqslant n \leqslant 5$. Let $S = \mathrm{PSL}_n^{\pm}(q)$, $G = \mathrm{SL}_n^{\pm}(q)$, and $\widetilde{G} \cong \widetilde{G}^* = \mathrm{GL}_n^{\pm}(q)$ for the appropriate value of n. Note that again in these cases, unipotent characters lie in the principal block and are rational-valued and extend to $\mathrm{Aut}(S)$, for the same reason as in Lemma 4.11.

1.iii. First let $n = 4$ or 5. Then we have four unipotent characters of odd degree, which may be viewed as characters of $\widetilde{S}$ that restrict irreducibly to S. Note that in the case $n = 4$, there is one more σ_1-invariant extension to $\widetilde{S}$ for each of these unipotent characters, which also must lie in the principal block since $\widetilde{S}/S$ is a 2-group. This yields eight members of $|\mathrm{Irr}_{2',\sigma_1}(B_0(A))|$ if $\mathrm{PSL}_4^{\pm}(q) < A \leqslant \widetilde{S}$. Hence if A/S is a nontrivial cyclic 2-group, we are done by also using Lemma 4.4.

Now, let $s \in \widetilde{G}^*$ be semisimple with eigenvalues $\{-1,-1,1,1\}$ in case $n = 4$ or $\{-1,-1,-1,-1,1\}$ in case $n = 5$. Note that $s \in [\widetilde{G}^*, \widetilde{G}^*] \cong G$, and hence the corresponding semisimple character χ_s of $\widetilde{G}$ is trivial on $\mathbf{Z}(\widetilde{G})$. Further, since $|s| = 2$, χ_s lies in $B_0(\widetilde{G})$, and is fixed by σ_1 by Lemma 4.8. In the case $n = 5$, χ_s has odd degree and s is not $\widetilde{G}^*$-conjugate to any sz for $1 \neq z \in \mathbf{Z}(\widetilde{G}^*)$, and hence χ_s restricts irreducibly to G. In the case $n = 4$, the degree of the character χ_s of $\widetilde{G}$ is $2 \pmod 4$, and it restricts to the sum of two irreducible odd-degree characters in G, since s is conjugate to $-s$. These restricted characters are also semisimple, indexed by semisimple elements of G^* of order 2, and hence are still fixed by σ_1 using Lemma 4.8. This yields a fifth member of $\mathrm{Irr}_{2',\sigma_1}(B_0(S))$ that is non-$\mathrm{Aut}(S)$-conjugate to the unipotent characters discussed above, completing the proof for the cases $\mathrm{PSL}_4^{\pm}(q)$ or $\mathrm{PSL}_5^{\pm}(q)$.

1.iv. If $S = \mathrm{PSL}_2(q)$, then there are four odd-degree characters of S. These come from the two unipotent characters and the two odd-degree restrictions of the character χ_s of $\widetilde{G}$ where s has eigenvalues $\{\varepsilon_4, \varepsilon_4^{-1}\}$ with $|\varepsilon_4| = 4$. Here as in the case of $\mathrm{PSL}_4(q)$ in 1.iii above, the degree of χ_s is $2 \pmod 4$. For the same reasons as there, these characters lie in $B_0(S)$ and are fixed by σ_1. Also, note that $\widetilde{S} = \mathrm{PGL}_2(q)$ also has exactly four odd-degree characters, coming from the two extensions of each unipotent character of S, which are also in $\mathrm{Irr}_{2',\sigma_1}(B_0(\widetilde{S}))$ following the same reasoning as in 1.iii.

We can see from the character table of S that the four members of $\mathrm{Irr}_{2',\sigma_1}(B_0(S))$ are fixed by field automorphisms. Hence, if A is the semidirect product $S \rtimes C$ with C a 2-group of field automorphisms, then these extend to give 8 members of $\mathrm{Irr}_{2',\sigma_1}(B_0(A))$, using Lemma 4.4.

If q is square and $A \neq \widetilde{S}$ is an extension of S by a cyclic 2-group not comprised of field automorphisms, then we may write $A = S\langle \alpha\varphi\rangle$, where α is a diagonal automorphism and φ is a field automorphism. Since the four members of $\mathrm{Irr}_{2',\sigma_1}(B_0(S))$ are fixed by field automorphisms but only the two unipotent characters are fixed by a nontrivial diagonal automorphism, we see that the odd-degree characters of A are again the extensions of the two unipotent characters (namely, the trivial and Steinberg characters) of S. As A/S is a 2-group, each such extension lies in $\mathrm{Irr}_{2'}(B_0(A))$. Further, the trivial and Steinberg characters each extend to a rational-valued character of $\mathrm{Aut}\,(S)$ (see [42] for extensions of the Steinberg character) and we therefore again obtain exactly two σ_1-invariant extensions of each of these two characters, yielding $|\mathrm{Irr}_{2',\sigma_1}(B_0(A))| = 4$.

This leaves the case A is the semidirect product $A = S \rtimes C$ with C a group of field automorphisms of odd order. In this case, we claim that each $\chi \in \mathrm{Irr}_{2'}(B_0(S)) = \mathrm{Irr}_{2',\sigma_1}(B_0(S))$ has a unique extension that lies in $B_0(A)$. By Theorem 2.7 and Lemma 4.5, it suffices to know that α centralizes a Sylow 2-subgroup of S for any $\alpha \in C$. Write $q = p^{2^b m}$ with m odd and let F_p be the generating field automorphism for S induced by the map $x \mapsto x^p$. By considering the construction of a Sylow 2-subgroup of $\mathrm{GL}_2(q)$ in [4], we see that there is a $P_2 \in \mathrm{Syl}_2(\mathrm{GL}_2(q))$ centralized by $F_p^{2^b}$, and hence centralized by C. To be more precise, if $q \equiv 1 \pmod 4$, we have P_2 is generated by matrices with entries $1, 0$, and ϵ with ϵ a $(q-1)_2$-root of unity in $\mathbb{F}_q^\times$. Since 2 divides $\Phi_d(p)$ if and only if d is a power of 2, we see $(q-1)_2 = (p^{2^b} - 1)_2$, and hence $F_p^{2^b}$ fixes ϵ. If $q \equiv 3 \pmod 4$, note that q is an odd power of p. Here P_2 instead is generated by matrices with entries $\pm 1, 0, \epsilon' + \epsilon'^q$, where ϵ' is a $(q^2-1)_2$-root of unity in $\mathbb{F}_{q^2}^\times$. Using the same argument as above, but using instead the generator F_p^2, shows that again P_2 is centralized by C. Then we are done, taking a Sylow 2-subgroup of $\mathrm{SL}_2(q)$ as a subgroup of P_2.

1.v. If $S = \mathrm{PSL}_3^\pm(q)$, there are two unipotent characters of odd degree. We may also consider the two odd-degree characters that come from the series $\mathcal{E}(\widetilde{G}, s)$ of $\widetilde{G}$, where we define s to have eigenvalues $\{-1, -1, 1\}$. These correspond to the trivial character and Steinberg character of $\mathbf{C}_{\widetilde{G}^*}(s) \cong \mathrm{GL}_2^\pm(q) \times \mathrm{GL}_1^\pm(q)$ under the Jordan decomposition of characters. Note that these characters are irreducible on G and trivial on $\mathbf{Z}(\widetilde{G})$ since $s \in [\widetilde{G}^*, \widetilde{G}^*] \cong G$ and s is not $\widetilde{G}^*$-conjugate to sz for $1 \neq z \in \mathbf{Z}(\widetilde{G}^*)$. Further, since $|s| = 2$, these characters lie in $B_0(\widetilde{G})$, and the corresponding characters of G, $\widetilde{S}$, and S are then also in the principal block, since $B_0(\widetilde{G})$ covers a unique block of G and using Lemma 4.6. Lemma 4.8 implies χ_s is fixed by σ_1, and hence so is the character corresponding to the Steinberg character of $\mathbf{C}_{\widetilde{G}^*}(s)$, since it is the unique character in the series with that degree. Similarly, since the class of s is invariant under $\mathrm{Aut}(S)$, we know that so are these two characters. Note that these two characters and the two unipotent characters are the only members of $\mathrm{Irr}_{2',\sigma_1}(B_0(S))$. If A/S is a nontrivial cyclic 2-group, this yields 8 members of $\mathrm{Irr}_{2',\sigma_1}(B_0(A))$, using Lemmas 4.4 and 4.7.

If $|A/S|$ is odd, we claim that for each member of $\mathrm{Irr}_{2',\sigma_1}(B_0(S))$, exactly one character of A above it lies in $B_0(A)$, yielding exactly four characters of $\mathrm{Irr}_{2',\sigma_1}(B_0(A))$ using Lemma

4.5 and 4.7(2). For $A = \widetilde{S}$, the characters of $\widetilde{G}$ lying above the series $\mathcal{E}(G,1)$ and $\mathcal{E}(G,s)$ must lie in the series $\mathcal{E}(G,z)$ and $\mathcal{E}(G,sz)$ for $z \in \mathbf{Z}(\widetilde{G}^*)$, by [5, Proposition 15.6]. To be trivial on $\mathbf{Z}(\widetilde{G})$, we further require $z \in [\widetilde{G}^*, \widetilde{G}^*] \cap \mathbf{Z}(\widetilde{G}^*)$, which has size dividing 3. Recalling that only series indexed by 2-elements are in the principal block of $\widetilde{G}$, this shows the claim when $A = \widetilde{S}$. To complete the proof, as in the case 1.iv above, it suffices to know that $F_p^{2^b}$ centralizes a Sylow 2-subgroup of $\widetilde{G} = \mathrm{GL}_3^{\pm}(q)$. Here, we write $\bar{q} = p^{2^b m}$ with m odd, where $\bar{q} = q$ in the case $\mathrm{PSL}_3(q)$ and $\bar{q} = q^2$ in the case $\mathrm{PSU}_3(q)$. Since such a Sylow 2-subgroup is the direct product of $P_2 \times P_1$, by [4], where $P_i \in \mathrm{Syl}_2(\mathrm{GL}_i^{\pm}(q))$ for $i = 1, 2$, we are done by the same arguments as 1.iv, since P_1 is cyclic generated by a $(q \mp 1)_2$ root of unity in $\mathbb{F}_{\bar{q}}^{\times}$.

2. The Sylow Side. If $S = {}^2G_2(3^{2r+1})$, then $|\mathrm{Out}(S)|$ is odd, so P is a Sylow 2-subgroup of S, which is elementary abelian of order 8. We therefore assume that S is not ${}^2G_2(q)$.

Let W be the Weyl group $\mathbf{N_G}(\mathbf{T})/\mathbf{T}$ of $\mathbf{G}$ and write $w = 1$ if $q \equiv 1 \pmod 4$ and $w = w_0$, the longest element of W, if $q \equiv 3 \pmod 4$. By [16, Theorem 4.10.2], a Sylow 2-subgroup P_0 of either G or $\widetilde{G}/\mathbf{Z}(\widetilde{G})$ contains an abelian normal subgroup P_T containing the 2-part of $\mathbf{Z}(G)$, such that P_0/P_T is isomorphic to a Sylow 2-subgroup of $C_W(Fw)$. We remark (see [13, Exercise 1.13]) that w_0 is central in W unless W is type A_n with $n \geqslant 2$, D_n with n odd, or E_6. In any case, P_0/P_T is isomorphic to a Sylow 2-subgroup of an irreducible Weyl group. Now, the structure of these groups is well-known, and we see that a Sylow 2-subgroup of such a Weyl group is at least three-generated, except for the Weyl groups $W(G_2)$, $W(B_2)$, and $W(A_n)$ with $n < 5$.

2.i. Assume first that $C_W(Fw)$ is not one of these groups. That is, we assume S is not one of $G_2(q)$, ${}^3D_4(q)$, $B_2(q) = \mathrm{PSp}_4(q)$, or $\mathrm{PSL}_n^{\pm}(q)$ with $n \leqslant 5$. In this case, it remains to show that the statement holds in the case A/S is a cyclic 2-group generated by graph and field automorphisms, and hence may be taken to be of the form $A = S \rtimes C$ with $C \leqslant D$. Now, from the construction in [16, Theorem 4.10.2], P_0 may be chosen so that P_0 and P_T are normalized by C and such that the action of C on $Q_0 := P_0/P_T \leqslant C_W(Fw)$ is compatible with that on W, and hence there is a Sylow 2-subgroup P of A that has a quotient of the form $Q := Q_0 \rtimes C$. Since field automorphisms act trivially on W (and hence on Q_0), and graph automorphisms permute the generators of W and hence act trivially on the abelianization of Q_0, we see that Q is again at least three-generated.

2.ii. Although the Sylow 2-subgroups of $W(G_2)$ are 2-generated, the Sylow 2-subgroups of $S = G_2(q)$, which are the same for ${}^3D_4(q)$, are well-studied (see, e.g. [15]) and not 2-generated. Since $\mathrm{Out}(S)$ is generated by field automorphisms unless q is a power of 3 in the case of G_2, which act trivially on W, we see a Sylow 2-subgroup of A is also not 2-generated in this case. If A has socle $G_2(q)$ with q a power of 3 and contains a graph or graph-field automorphism, we may argue as in the case of $B_2(q)$ in 2.i. For $S = \mathrm{PSL}_n^{\pm}(q)$ with $n = 4, 5$ or $\mathrm{PSp}_4(q)$, we have Q_0 is 2-generated. Similarly, we see $Q_0 \rtimes C$ is more than 2-generated when C is a nontrivial cyclic 2-group of field automorphisms. A Sylow 2-subgroup of $\mathrm{PSL}_5^{\pm}(q)$ is the same as that of $\mathrm{SL}_5^{\pm}(q)$, which is isomorphic to a Sylow 2-subgroup of $\mathrm{GL}_4^{\pm}(q)$. So, it suffices to note that we can deduce that the Sylow 2-subgroups of $\mathrm{PSL}_4(q)^{\pm}$, $\mathrm{GL}_4^{\pm}(q)$, $\mathrm{PGL}_4^{\pm}(q)$, $\mathrm{PSp}_4(q)$, and PCSp$_4$(q) are at least 3-generated by the construction in [4] of Sylow 2-subgroups of classical groups.

2.iii. The Sylow 2-subgroups of $\mathrm{PSL}_2(q)$ and $\mathrm{PGL}_2(q)$ are either Klein-4 or dihedral, and hence 2-generated. When q is square and A/S is a cyclic 2-group with A of the form $\mathrm{PSL}_2(q)\langle\alpha\varphi\rangle$, where φ is a field automorphism and α is a diagonal automorphism, α can be induced by the diagonal matrix in $\mathrm{GL}_2(q)$ with diagonal $(\omega, 1)$, where ω is a $(q-1)_2$-root of unity in $\mathbb{F}_q^\times$. Then, modulo $\mathbf{Z}(\mathrm{SL}_2(q))$, a Sylow 2-subgroup of A can be generated by $\alpha\varphi$ and the anti-diagonal matrix with anti-diagonal $(1, -1)$.

Now, the group $P_2 \times P_1$, where $P_i \in \mathrm{Syl}_2(\mathrm{GL}_i^\pm(q))$ for $i = 1, 2$, is a Sylow 2-subgroup of $\mathrm{GL}_3^\pm(q)$. Then there is a Sylow 2-subgroup of $\mathrm{SL}_3^\pm(q)$, which is isomorphic to that of $\mathrm{PSL}_3^\pm(q)$, comprised of the set of $(x, y) \in P_2 \times P_1$ with $y = \det x^{-1}$, which is isomorphic to P_2. By [4], we see P_2 is either semidihedral or $C_{2^s} \wr C_2$, both of which are 2-generated. If $A = S \rtimes C$ with $S = \mathrm{PSL}_2(q)$ or $\mathrm{PSL}_3^\pm(q)$ and $C \leqslant D$ a nontrivial cyclic 2-group, and $\bar{P}$ is a Sylow 2-subgroup of S, then we can see using the constructions in [4] that $\bar{P}$ can be chosen so that the order-2 generators of $\bar{P}/\Phi(\bar{P})$ are C-invariant, and hence $P = \bar{P} \rtimes C$ is three-generated in this case. □

Propositions 4.9 and 4.12, together with Lemmas 4.2 and 4.3, complete the proof of Theorem 3.1.

References

[1] J. L. Alperin, Isomorphic blocks, *J. Algebra* **43** (1976), 694–698.

[2] R. Brauer, Representations of finite groups, in: '*Lectures on Modern Mathematics*', vol. I, ed. by T. Saaty, John Wiley & Sons, 1963.

[3] W. Burnside, Theory of Groups of Finite Order, Dover, 1955.

[4] R. W. Carter, P. Fong, The Sylow 2-subgroups of the finite classical groups, *J. Algebra.* **1**:2 (1964), 139–151.

[5] M. Cabanes, M. Enguehard, *Representation Theory of Finite Reductive Groups*, New Mathematical Monographs, Cambridge University Press. 2004.

[6] R. W. Carter, *Finite groups of Lie type, Conjugacy classes and complex characters*, Pure and Applied Mathematics (New York), John Wiley & Sons, Inc., New York, 1985.

[7] D. A. Craven, *Representation Theory of Finite Groups: a Guidebook*, Springer, 2019.

[8] E. C. Dade, *Remarks on isomorphic blocks, J. Algebra* **45** (1977), 254–258.

[9] E. C. Dade, Blocks with cyclic defect groups, *Ann. of Math.* **84** (1966), 20–48.

[10] F. Digne, G. I. Lehrer, J. Michel, On Gelfand-Graev characters of reductive groups with disconnected centre, *J. Reine Angew. Math.* **491** (1997), 131–147.

[11] The GAP Group, GAP Groups, Algorithms, and Programming, Version 4.4; 2004, `http://www.gap-system.org`.

[12] M. Geck, G. Hiss, F. Lübeck, G. Malle, G. Pfeiffer, CHEVIE – A system for computing and processing generic character tables for finite groups of Lie type, Weyl groups and Hecke algebras. *Appl. Algebra Engrg. Comm. Comput.*, 7:175–210, 1996.

[13] M. Geck, G. Pfeiffer, *Characters of finite Coxeter groups and Iwahori-Hecke algebras*, London Mathematical Society Monographs. New Series, vol. 21, The Clarendon Press, Oxford University Press, New York, 2000.

[14] E. Giannelli, N. Rizo, A. A. Schaeffer Fry, Groups with few p'-character degrees, *J. Pure Appl. Algebra.* **224** (2020) no 8.

[15] D. Gorenstein, K. Harada, Finite simple groups of low 2-rank and the families $G_2(q)$, $D_4^2(q)$, q odd, *Bull. Amer. Math. Soc.*, **77**:6 (1971), 829–862.

[16] D. Gorenstein, R. Lyons, R. Solomon, *The classification of the finite simple groups. Number 5. Part III. Chapters 1–6*, volume 40 of *Mathematical Surveys and Monographs.* American Mathematical Society, Providence, RI, 2002.

[17] I. M. Isaacs, *Character Theory of Finite Groups*, AMS Chelsea Publishing, Providence, RI, 2006.

[18] I. M. Isaacs, *Finite group theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.

[19] A. Jaikin-Zapirain, The number of finite p-groups with bounded number of generators, in Finite groups 2003 (eds Ho, Sin, Tiep and Turull; Walter de Gruyter GmbH & Co. KG, Berlin, 2004) 209–217.

[20] F. Lübeck, Character degrees and their multiplicities for some groups of Lie type of rank < 9 (webpage, 2007). `http://www.math.rwth-aachen.de/ Frank.Luebeck/chev/DegMult/index.html`.

[21] G. Lusztig, On the representations of reductive groups with disconnected centre, *Orbites Unipotentes et Représentations, I. Astérisque* **168** (1988), 157–166.

[22] G. Lusztig, Rationality properties of unipotent representations, *J. Algebra* **258** (2002), 1–22.

[23] I. G. MacDonald, On the degrees of the irreducible representations of symmetric groups, *Bull. London Math. Soc.* **3** (1971), 189–192.

[24] G. Malle, Height 0 characters of finite groups of Lie type, *Represent. Theory,* **11** (2007),192–220.

[25] G. Malle, Extensions of unipotent characters and the inductive McKay condition, *J. Algebra* **320** (2008) (7), 2963–2980.

[26] G. Malle, B. Späth, Characters of odd degree, *Ann. of Math.* (2) **184** 3 (2016), 869–908.

[27] G. Navarro, *Characters and Blocks of Finite Groups*, Cambridge University Press, 1998.

[28] G. Navarro, Linear characters of Sylow subgroups. *J. Algebra* **269** (2003), no. 2, 589–598.

[29] G. Navarro, The McKay conjecture and Galois automorphisms, *Ann. of Math.* **160** (2004), 1129–1140.

[30] G. Navarro, *Character Theory and the McKay Conjecture*, Cambridge University Press, 2018.

[31] G. Navarro, B. Sambale, P. H. Tiep, Characters and Sylow 2-subgroups of maximal class revisited, *J. Pure Appl. Algebra* **222** (2018), 3721–3732.

[32] G. Navarro, P. H. Tiep, Sylow subgroups, exponents, and character values, *Trans. Amer. Math. Soc.* **372** (2019), 4263–4291.

[33] G. Navarro, P. H. Tiep, Brauer's height zero conjecture for the 2-blocks of maximal defect, *J. Reine Angew. Math.* **669** (2012), 225–247.

[34] G. Navarro, P. H. Tiep, Characters of relative p'-degree over normal subgroups, *Ann. Math.* **2**:178 (2013), 1135–1171.

[35] G. Navarro, P. H. Tiep, A. Turull, p-rational characters and self-normalizing Sylow p-subgroups, *Represent. Theory* **11** (2007), 84–94.

[36] G. Navarro, P. H. Tiep, A. Turull, Brauer characters with cyclotomic field of values, *J. Pure Appl. Algebra* **212** (2008), 628–635.

[37] G. Navarro, P. H. Tiep, C. Vallejo, Brauer correspondent blocks with one simple module, *Trans. Amer. Math. Soc.* **371** (2019), no. 2, 903–922.

[38] J. B. Olsson, On the p-blocks of symmetric and alternating groups and their coverings, *J. Algebra* **128** (1990), 188–213.

[39] N. Rizo, A. A. Schaeffer Fry, C. Vallejo, Galois action on the principal blocks and cyclic Sylow subgroups, *Algebra Number Theory* **14** (2020), no. 7, 1953–1979..

[40] A. A. Schaeffer Fry, Action of Galois automorphisms on Harish-Chandra series and Navarro's self-normalizing Sylow 2-subgroup conjecture, *Trans. Amer. Math. Soc.* **372** no. 1 (2019), 457–483.

[41] A. A. Schaeffer Fry, J. Taylor, On self-normalizing Sylow 2-subgroups in type A, *J. Lie Theory* (2018), 28:1, 139–168.

[42] P. Schmid, Extending the Steinberg representation, *J. Algebra* **150** (1992), 254–256.

[43] K. Shinoda, The conjugacy classes of Chevalley groups of type F_4 over finite fields of characteristic 2, *J. Fac. Sci. Univ. Tokyo* **21** (1974), 133–159.

[44] H. N. Ward, On Ree's series of simple groups, *Bull. Amer. Math. Soc.* **69**, No. 1 (1963), 113–114.

Departament de Matemàtiques, Universitat de València, 46100 Burjassot, València, Spain.
Email address: gabriel@uv.es

Departament de Matemàtiques, Universitat de València, 46100 Burjassot, València, Spain.
Email address: noelia.rizo@uv.es

Dept. Mathematical and Computer Sciences, MSU Denver, Denver, CO 80217, USA
Email address: aschaef6@msudenver.edu

Departamento de Matemáticas, Edificio Sabatini, Universidad Carlos III de Madrid, Av. Universidad 30, 28911, Leganés. Madrid, Spain
Email address: carolina.vallejo@uc3m.es