ISRAEL JOURNAL OF MATHEMATICS **TBD** (2024), 1–32
DOI: 10.1007/s11856-024-2613-1

BOUNDING p-BRAUER CHARACTERS IN FINITE GROUPS WITH TWO CONJUGACY CLASSES OF p-ELEMENTS

BY

Nguyen Ngoc Hung

Department of Mathematics, The University of Akron, Akron, OH 44325, USA
e-mail: hungnguyen@uakron.edu

AND

Benjamin Sambale*

Institut für Algebra, Zahlentheorie und Diskrete Mathematik
Leibniz Universität Hannover
Welfengarten 1, 30167 Hannover, Germany
e-mail: sambale@math.uni-hannover.de

AND

Pham Huu Tiep**

Department of Mathematics, Rutgers University, Piscataway, NJ 08854, USA
e-mail: tiep@math.rutgers.edu

Dedicated to Burkhard Külshammer on the occasion of his retirement

* The second author is supported by the German Research Foundation (SA 2864/1-2 and SA 2864/3-1).
** The third author gratefully acknowledges the support of the NSF (grants DMS-1840702 and DMS-2200850), the Joshua Barlaz Chair in Mathematics, and the Charles Simonyi Endowment at the Institute for Advanced Study (Princeton).
Received December 9, 2021 and in revised form April 25, 2022

ABSTRACT

Let $k(B_0)$ and $l(B_0)$ respectively denote the number of ordinary and p-Brauer irreducible characters in the principal block B_0 of a finite group G. We prove that, if $k(B_0)-l(B_0)=1$, then $l(B_0)\geq p-1$ or else $p=11$ and $l(B_0)=9$. This follows from a more general result that for every finite group G in which all non-trivial p-elements are conjugate, $l(B_0)\geq p-1$ or else $p=11$ and $G/\mathbf{O}_{p'}(G)\cong C_{11}^2\rtimes \mathrm{SL}(2,5)$. These results are useful in the study of principal blocks with few characters.

We propose that, in every finite group G of order divisible by p, the number of irreducible Brauer characters in the principal p-block of G is always at least $2\sqrt{p-1}+1-k_p(G)$, where $k_p(G)$ is the number of conjugacy classes of p-elements of G. This indeed is a consequence of the celebrated Alperin weight conjecture and known results on bounding the number of p-regular classes in finite groups.

1. Introduction

Let G be a finite group and p a prime. Bounding the number $k(G)$ of conjugacy classes of G and the number $k_{p'}(G)$ of p-regular conjugacy classes of G is a classical problem in group representation theory, one important reason being that $k(G)$ is the same as the number of non-similar irreducible complex representations of G and $k_{p'}(G)$ is the same as the number of non-similar irreducible representations of G over an algebraically closed field $\mathbb{F}$ of characteristic p. It was shown recently in [HM, Theorem 1.1] that if G has order divisible by p, then

$$k_{p'}(G)\geq 2\sqrt{p-1}+1-k_p(G),$$

where $k_p(G)$ denotes the number of conjugacy classes of p-elements of G. As it is obvious from the bound itself that equality could occur only when $p-1$ is a perfect square, a "correct" bound remains to be found.

Motivated by the study of blocks which contain a small number of characters, in this paper we are interested in the situation where all the non-trivial p-elements of the group are conjugate.

Theorem 1.1: *Let p be a prime and G a finite group in which all non-trivial p-elements are conjugate. Then one of the following holds:*

(i) $k_{p'}(G)\geq p$.
(ii) $k_{p'}(G)=p-1$ *and* $G\cong C_p\rtimes C_{p-1}$ *(Frobenius group).*
(iii) $p=11$, $G\cong C_{11}^2\rtimes \mathrm{SL}(2,5)$ *(Frobenius group) and* $k_{p'}(G)=9$.

Finite groups with a unique non-trivial conjugacy class of p-elements arise naturally from block theory. For a p-block B of a group G, as usual let $\mathrm{Irr}(B)$ and $\mathrm{IBr}(B)$ respectively denote the set of irreducible ordinary characters of G associated to B and the set of irreducible Brauer characters of G associated to B, and set $k(B) := |\mathrm{Irr}(B)|$ and $l(B) := |\mathrm{IBr}(B)|$. The difference $k(B) - l(B)$ is one of the important invariants of the block B as it somewhat measures the complexity of B, and in fact, the study of blocks with small $k(B) - l(B)$ has attracted considerable interest; see [KNST, KS, RSV] and references therein.

It is well-known that $k(B)-l(B) = 0$ if and only if $k(B) = l(B) = 1$, in which case the defect group of B is trivial. What happens when $k(B) - l(B) = 1$? Brauer's formula for $k(B)$ (see [KNST, p. 311]) then implies that all non-trivial B-subsections are conjugate. (Recall that a B-subsection is a pair (u, b_u) consisting of a p-element $u \in G$ and a p-block b_u of the centralizer $\mathbf{C}_G(u)$ such that the induced block b_u^G is exactly B.) Therefore, if B_0 is the principal p-block of G and $k(B_0) - l(B_0) = 1$, then all the non-trivial p-elements of G are conjugate.

Given a p-block B of G, the well-known blockwise Alperin weight conjecture (BAW) claims that $l(B)$ is equal to the number of G-conjugacy classes of p-weights of B (for details see Section 3). The conjecture implies $l(B_0) \geq l(b_0)$, where B_0 and b_0 are respectively the principal blocks of G and $\mathbf{N}_G(P)$, and P is a Sylow p-subgroup of G. It is easy to see that

$$l(b_0) = k_{p'}(\mathbf{N}_G(P)/\mathbf{O}_{p'}(\mathbf{N}_G(P))).$$

Now suppose that $k_p(G) = 2$. Then the main result of [KNST] asserts that, aside from very few exceptions, the Sylow p-subgroups of G are (elementary) abelian, and so let us assume for a moment that $P \in \mathrm{Syl}_p(G)$ is abelian. It follows that $\mathbf{N}_G(P)$ controls G-fusion in P, and thus $\mathbf{N}_G(P)/\mathbf{O}_{p'}(\mathbf{N}_G(P))$ has a unique non-trivial conjugacy class of p-elements as G does. Therefore, the BAW conjecture and (the p-solvable case of) Theorem 1.1 imply the following, which we are able to prove using only the known cyclic Sylow case of the conjecture.

Theorem 1.2: *Let p be a prime and G a finite group in which all non-trivial p-elements are conjugate. Let B_0 denote the principal p-block of G. Then one of the following holds:*

(i) $l(B_0) \geq p$.
(ii) $l(B_0) = p-1$ *and* $\mathbf{N}_G(P)/\mathbf{O}_{p'}(\mathbf{N}_G(P)) \cong C_p \rtimes C_{p-1}$ *(Frobenius group).*
(iii) $p = 11$, $G/\mathbf{O}_{p'}(G) \cong C_{11}^2 \rtimes \mathrm{SL}(2,5)$ *(Frobenius group) and* $l(B_0) = 9$.

Theorem 1.2 implies that if G is a finite group with $k_p(G) = 2$ then $k(B_0) \geq p$ or $p = 11$ and $k(B_0) = 10$. Indeed, we obtain the following. Here, $k_0(B)$ denotes the number of irreducible ordinary characters of height 0 in B.

THEOREM 1.3: *Let p be a prime and G a finite group in which all non-trivial p-elements are conjugate. Let B_0 denote the principal p-block of G. Then $k_0(B_0) \geq p$ or $p = 11$ and $k_0(B_0) = 10$.*

We mention another consequence, which is useful in the study of principal blocks with few characters, in particular the case $k(B_0) - l(B_0) = 1$. Note that by [KNST, Theorem 3.6], the Sylow p-subgroups of G then must be (elementary) abelian, and hence by [KM1], $k_0(B_0) = k(B_0)$.

COROLLARY 1.4: *Let p be a prime and G a finite group with principal p-block B_0. If $k(B_0) - l(B_0) = 1$ then $k_0(B_0) = k(B_0) \geq p$ or $p = 11$ and $k_0(B_0) = k(B_0) = 10$.*

For a quick example, let us assume that $k(B_0) = 4$ and $l(B_0) = 3$. Then Corollary 1.4 implies that $p \leq 4$, and since the case $p = 3$ is eliminated by [Lan, Corollary 1.6], one ends up with $p = 2$, implying that the defect group of B_0 must be of order 4 by [Lan, Corollary 1.3], and thus is the Klein four group. This result was recently proved in [KS, §5]. (See Section 7 for more examples with $k(B_0) = l(B_0) + 1 = 5$ or 7.)

In Section 6 we go one step further and prove that $k_{p'}(G) \geq (p-1)/2$ for finite groups G with at most three classes of p-elements. As explained in Section 3, this and the BAW conjecture then imply that $l(B_0) \geq (p-1)/2$ for principal blocks B_0 of groups with $1 < k_p(G) \leq 3$. In general, we propose that

$$l(B_0) \geq 2\sqrt{p-1} + 1 - k_p(G)$$

for arbitrary groups of order divisible by p, and this follows from [HM, Theorem 1.1] and again the BAW conjecture. We should mention that our proposed bound complements the conjectural upper bound for the number $l(B)$ proposed by Malle and Robinson [MR], namely $l(B) \leq p^{r(B)}$, where $r(B)$ is the sectional p-rank of a defect group of B.

The paper is organized as follows. In the next Section 2, we prove Theorem 1.1 for p-solvable groups. In Section 3 we make a connection between Theorem 1.2 and other bounds on $l(B_0)$ with the BAW conjecture. In Section 4 we prove a key result on principal blocks of almost simple groups of Lie type, Theorem 4.1.

This result will then be used in Section 5 to prove Theorems 1.1 and 1.2. In Section 6 we prove a general bound for the number of p-regular conjugacy classes in almost simple groups without any assumption on the number of p-classes, and this will be used to achieve a right bound for $k_{p'}(G)$ for finite groups G with at most three classes of p-elements. Finally, the proof of Theorem 1.3 and more examples of applications of Theorem 1.2 are presented in Section 7.

2. p-Solvable groups

We begin by proving Theorem 1.1 for p-solvable groups.

THEOREM 2.1: *Let G be a p-solvable group with $k_p(G) = 2$. Then one of the following holds:*

(i) $k_{p'}(G) \geq p$.
(ii) $k_{p'}(G) = p - 1$ *and* $G \cong C_p \rtimes C_{p-1}$ *(Frobenius group).*
(iii) $p = 11$, $G \cong C_{11}^2 \rtimes \mathrm{SL}(2,5)$ *(Frobenius group) and* $k_{p'}(G) = 9$.

Proof. We assume first that $\mathbf{O}_{p'}(G) = 1$. Then $P := \mathbf{O}_p(G) \neq 1$ since G is p-solvable. Since every p-element is conjugate to an element of P, P must be a Sylow p-subgroup. Since $\mathbf{Z}(P) \trianglelefteq G$, it follows that $P = \mathbf{Z}(P)$ is elementary abelian. Moreover, $\mathbf{C}_G(P) = P$ and $\overline{G} := G/P$ is a transitive linear group (on P). We need to show that $k_{p'}(G) = k_{p'}(\overline{G}) = k(\overline{G}) \geq p - 1$ excluding the exceptional case. By Passman's classification [Pas, Theorem I], $\overline{G}$ is a subgroup of the semilinear group

$$\Gamma\mathrm{L}(1, p^n) \cong \mathbb{F}_{p^n}^{\times} \rtimes \mathrm{Aut}(\mathbb{F}_{p^n}) \cong C_{p^n-1} \rtimes C_n$$

where $P \cong \mathbb{F}_{p^n}$, or one of finitely many exceptions. We start with the first case. Suppose that $\mathbb{F}_{p^n}^{\times}$ does not fully lie inside $\overline{G}$. Then $\overline{G} \cap \mathbb{F}_{p^n}^{\times} \trianglelefteq \overline{G}$ is intransitive on $P \setminus \{1\}$ and $\overline{G}/\overline{G} \cap \mathbb{F}_{p^n}^{\times} \cong \overline{G}\mathbb{F}_{p^n}^{\times}/\mathbb{F}_{p^n}^{\times} \leq \mathrm{Aut}(\mathbb{F}_{p^n})$ permutes the orbits of $\overline{G} \cap \mathbb{F}_{p^n}^{\times}$. However, $\mathrm{Aut}(\mathbb{F}_{p^n})$ fixes some $x \in P \setminus \{1\}$ in the base field $\mathbb{F}_p$. Hence, $\overline{G}$ cannot act transitively on $P \setminus \{1\}$. This shows that $\mathbb{F}_{p^n}^{\times} \leq \overline{G}$. Now $\overline{G}$ has at least $(p^n - 1)/n \geq p - 1$ conjugacy classes lying inside $\mathbb{F}_{p^n}^{\times}$. The equality here occurs if and only if $n = 1$, in which case G is the Frobenius group $C_p \rtimes C_{p-1}$.

Now suppose that $\overline{G}$ is one of the exceptions in Passman's list (see [Sam1, Theorem 15.1] for detailed information). For $p = 3$ the claim reduces to $|\overline{G}| \geq 3$ which is obviously true. The remaining cases can be checked by computer. It turns out that $G \cong C_{11}^2 \rtimes \mathrm{SL}(2,5)$ with $p = 11$ is the only exception.

Finally, suppose that $N := \mathbf{O}_{p'}(G) \neq 1$. Since $k_p(G) = k_p(G/N)$, the above arguments apply to G/N. Since at least one p-regular element lies in $N \setminus \{1\}$, we obtain

$$k_{p'}(G) \geq 1 + k_{p'}(G/N) \geq p$$

unless $p = 11$ and $G/N \cong C_{11}^2 \rtimes \mathrm{SL}(2,5)$. Suppose in this case that $k_{11'}(G) = 10$. Then all non-trivial elements of N are conjugate in G. As before, N must be an elementary abelian q-group for some prime $q \neq 11$. Let $N \leq M \trianglelefteq G$ such that $M/N \cong C_{11}^2$. Then G/M acts transitively on the M-orbits of $N \setminus \{1\}$. In particular, these M-orbits have the same size. Since the non-cyclic group M/N cannot act fixed point freely on N, all M-orbits have size 1 or 11. In the second case, $(|N| - 1)/11$ divides $|G/M| = 120$. This leaves only the possibility that N is cyclic of order $q \geq 23$. But then $G/\mathbf{C}_G(N)$ is cyclic and we derive the contradiction $G = G'N \leq \mathbf{C}_G(N)$.

It remains to deal with the case where M acts trivially on N. Here we may go over to $\overline{G} := G/\mathbf{O}_{11}(G)$ such that $k(\overline{G}) = k_{11'}(G) = 10$. Since $\overline{G}$ acts transitively on $\overline{N} \setminus \{1\}$, we obtain that $|\overline{N}| - 1$ divides $|\overline{G}/\overline{N}| = |G/M| = 120$. Since $\overline{G}/\mathbf{C}_{\overline{G}}(\overline{N}) \in \{\mathrm{SL}(2,5), A_5\}$, this leaves the possibilities $|\overline{N}| \in \{2^4, 5^2\}$. Now it can be checked by computer that there is no (perfect) group with these properties. ∎

Apart from finitely many exceptions, the proof actually shows that

$$k_{p'}(G) \geq \frac{p^n - 1}{n}$$

where $|G|_p = p^n$.

The following result provides a bound for $k_{p'}(G)$ in p-solvable groups with three conjugacy classes of p-elements.

Theorem 2.2: *Let G be a p-solvable group with $k_p(G) = 3$. Then*

$$k_{p'}(G) \geq \frac{p-1}{2}$$

with equality if and only if $p > 2$ and G is the Frobenius group $C_p \rtimes C_{(p-1)/2}$.

Proof. As in the proof of Theorem 2.1 we start by assuming $\mathbf{O}_{p'}(G) = 1$. Since the claim is easy to show for $p \leq 5$, we may assume that $p \geq 7$ in the following.

Let $P := \mathbf{O}_p(G) \neq 1$ and $H := G/P$. Suppose first that $|H|$ is divisible by p. Then $k_p(H) = 2$ and

$$k_{p'}(G) = k_{p'}(H) \geq p - 2 > \frac{p-1}{2}$$

by Theorem 2.1. Now let H be a p'-group. Suppose that P possesses a characteristic subgroup $1 < Q < P$. Then $P \setminus Q$ must be an H-orbit and therefore $|P \setminus Q|$ is not divisible by p. This is clearly impossible. Hence, P is elementary abelian and $G \cong P \rtimes H$ is an affine primitive permutation group of rank 3 (i.e., a point stabilizer has three orbits on P). These groups were classified by Liebeck [Lie].

Let $|P| = p^n$. Suppose first that $H \leq \Gamma\mathrm{L}(1, p^n)$. Then $C := H \cap \mathbb{F}_{p^n}^\times$ is a semiregular normal subgroup of H and $H/C \leq \mathbb{F}_{p^n}$. Clearly, C has exactly $\frac{p^n-1}{|C|}$ orbits on $P \setminus \{1\}$ each of length $|C|$. Moreover, $\mathrm{Aut}(\mathbb{F}_{p^n})$ fixes one of these orbits and can merge at most n of the remaining (same argument as in the previous proof). Hence, $|C| + n|C| \geq p^n - 1$ and $|C| \geq \frac{p^n-1}{1+n}$. Now there are at least $\frac{p^n-1}{n+n^2}$ conjugacy classes of H lying inside C. Since

$$\frac{p^n-1}{p-1} = 1 + p + \cdots + p^{n-1} \geq 1 + 2 + \cdots + 2^{n-1} = 2^n - 1 \geq \frac{n(n+1)}{2},$$

we obtain $k_{p'}(H) \geq \frac{p-1}{2}$ with equality if and only if $n = 1$ and $G \cong C_p \rtimes C_{(p-1)/2}$.

Now assume that H acts imprimitively on $P = P_1 \times P_2$ interchanging P_1 and P_2. Then

$$K := \mathbf{N}_H(P_1) = \mathbf{N}_H(P_2) \trianglelefteq H$$

and $K/\mathbf{C}_H(P_1)$ is a transitive linear group on P_1. Theorem 2.1 yields

$$k(K) \geq k(K/\mathbf{C}_H(P_1)) \geq p - 2.$$

Since $|H : K| = 2$, the conjugacy classes of K can only fuse in pairs in H. This leaves at least $1 + \frac{p-3}{2} = \frac{p-1}{2}$ conjugacy classes of H inside K and there is at least one more class outside K. Altogether, $k(H) \geq \frac{p+1}{2}$.

Next suppose that $P = P_1 \otimes P_2$ considered as $\mathbb{F}_q$-spaces where $q^a = p^n$ and H stabilizes P_1 and P_2. Here $|P_1| = q^2$ and $|P_2| = q^d \geq q^2$. By [Lie, Lemma 1.1], H has an orbit of length $(q^d - 1)(q^d - q)$, but this is impossible since H is a p'-group.

The cases (A4)–(A11) in Liebeck [Lie] are not p-solvable. Cases (B) and (C) are finitely many exceptions. Suppose that $p = 7$ and $k(H) \leq 3$. It is well-known that then $H \leq S_3$ and therefore $|P| \leq 1 + 6 + 6$. It follows that

$n = 1$ and $G \cong C_7 \rtimes C_3$. Hence, let $p \geq 11$. From [Lie] we obtain $|P| \leq 89^2$. Since the primitive permutation groups of degree at most $2^{12} - 1$ are available in GAP [GAP], we may assume that $p \geq 67$. There are only three cases left, namely $p \in \{71, 79, 89\}$ and $n = 2$. Here $A_5 \leq H/\mathbf{Z}(H)$. Since A_5 is a maximal subgroup of $\mathrm{PSL}(2, p)$ (see [Hup, Hauptsatz II.8.27]), it follows that $H \cap \mathrm{SL}(2, p) = \mathrm{SL}(2, 5)$. Consequently,

$$C := H/\mathrm{SL}(2,5) \leq \mathrm{GL}(2,p)/\mathrm{SL}(2,p) \cong C_{p-1}.$$

Since H has an orbit of length at least $(p^2 - 1)/2$, we obtain

$$120|C| = |H| \geq (p^2 - 1)/2.$$

This yields $k(H) \geq 1 + |C| > (p - 1)/2$ unless $p = 79$ and $|C| = 26$. In this exception, $H = \mathrm{SL}(2, 5).2 \times C_{13}$ and obviously $k(H) \geq 3 \cdot 13 = (p - 1)/2$.

Finally, suppose that $N := \mathbf{O}_{p'}(G) \neq 1$. Then the above arguments apply to G/N and we obtain

$$k_{p'}(G) \geq 1 + k_{p'}(G/N) > \frac{p-1}{2}$$

since at least one non-trivial p-regular element lies in N. ∎

We remark that the p-solvability assumption in Theorem 2.2 will be removed in Section 6.

3. The blockwise Alperin weight conjecture

In this section, we will explain that, when the Sylow p-subgroups of G are cyclic, the main result Theorem 1.2 (and also Theorem 6.1) is a consequence of the known cyclic Sylow case of the blockwise Alperin weight (BAW) conjecture and the p-solvable results proved in the previous section.

Let B be a p-block of G. Recall that $l(B)$ denotes the number of irreducible Brauer characters of B. A p-weight for B is a pair (Q, λ) of a p-subgroup Q of G and an irreducible p-defect zero character λ of $\mathbf{N}_G(Q)/Q$ such that the lift of λ to $\mathbf{N}_G(Q)$ belongs to a block which induces the block B. The BAW conjecture claims that $l(B)$ is equal to the number of G-conjugacy classes of p-weights of B. In particular, the conjecture implies that $l(B) \geq l(b)$, where b is the Brauer correspondent of B (see [Alp, Consequence 1]). In fact, when a defect group of B is abelian, the conjecture is equivalent to $l(B) = l(b)$ (see [Alp, Consequence 2]).

Let $P \in \mathrm{Syl}_p(G)$, and let B_0 and b_0 be respectively the principal blocks of G and $\mathbf{N}_G(P)$. Assume that the BAW conjecture holds for (G,p). Since $\mathbf{N}_G(P)$ is p-solvable, [Nav1, Theorems 9.9 and 10.20] show that

$$l(B_0) \geq l(b_0) = k_{p'}(\mathbf{N}_G(P)/\mathbf{O}_{p'}(\mathbf{N}_G(P))) = k(\mathbf{N}_G(P)/P\mathbf{C}_G(P)).$$

Let $H := \mathbf{N}_G(P)/P\mathbf{C}_G(P)$ and $Z := \mathbf{Z}(P)$. We then have $k(H) = k_{p'}(Z \rtimes H)$, and it follows that

$$l(B_0) \geq k_{p'}(Z \rtimes H).$$

By Burnside's fusion argument (see [Isa, Lemma 5.12]), H controls fusion in Z. In particular, $k_p(Z \rtimes H) \leq k_p(G)$. (We note that it also follows from the BAW conjecture that $k(B_0) \geq k(Z \rtimes H)$ by [Nav2, Theorem D]. We thank G. Navarro for pointing out this fact to us.)

Combining the above analysis with the results of the previous section, we deduce that, if $k_p(G) = 2$ then $k_p(Z \rtimes H) = 2$ and $l(B_0) \geq p-1$ or $p = 11$ and $\mathbf{N}_G(P)/\mathbf{O}_{p'}(\mathbf{N}_G(P)) \cong C_{11}^2 \rtimes \mathrm{SL}(2,5)$. Similarly, if $k_p(G) = 3$ then $k_p(Z \rtimes H) = 2$ or 3, and thus $l(B_0) \geq (p-1)/2$, by Theorems 2.1 and 2.2. Also, when $k_p(G) = 2$, $l(B_0) = p-1$ if and only if $k_{p'}(\mathbf{N}_G(P)/\mathbf{O}_{p'}(\mathbf{N}_G(P))) = p-1$, which occurs if and only if $\mathbf{N}_G(P)/\mathbf{O}_{p'}(\mathbf{N}_G(P))$ is isomorphic to the Frobenius group $C_p \rtimes C_{p-1}$, by Theorem 2.1.

We have seen that Theorem 1.2 holds for (G,p) if the BAW conjecture holds for (G,p). In particular, by Dade's results [Dad] on blocks with cyclic defect groups, we have proved Theorem 1.2 for groups with cyclic Sylow p-subgroups.

We also have the following, which was already mentioned in the introduction.

Proposition 3.1: *Let p be a prime and G a finite group with $k_p(G) = 3$. Let B_0 be the principal block of G. Then the blockwise Alperin weight Conjecture (for B_0) implies that $l(B_0) \geq (p-1)/2$.*

Proposition 3.2: *Let p be a prime and G a finite group of order divisible by p. Let B_0 be the principal block of G. Then the blockwise Alperin weight Conjecture (for B_0) implies that $l(B_0) \geq 2\sqrt{p-1} + 1 - k_p(G)$.*

Proof. This follows from the above analysis and [HM, Theorem 1.1]. ∎

We end this section with another consequence of the BAW conjecture on possible values of $k(B)$ and $l(B)$ in blocks with $k(B) - l(B) = 1$. In the following theorem we make use of Jordan's totient function $J_2 : \mathbb{N} \to \mathbb{N}$ defined by

$$J_2(n) := n^2 \prod_{p|n} \frac{p^2-1}{p^2}$$

where p runs through the prime divisors of n (compare with the definition of Euler's function ϕ).

Theorem 3.3: *Let B be a p-block of a finite group G with defect d such that $k(B)-l(B)=1$. Suppose that B satisfies the Alperin weight Conjecture. Then one of the following holds:*

(i) *$d = nk$ such that all prime divisors of n divide p^k-1. Moreover, if 4 divides n, then 4 divides p^k-1. Here*

$$l(B) = \sum_{e|n} \frac{p^{ek}-1}{ne} J_2(n/e).$$

In particular, $l(B) = p^d - 1$ if $n = 1$ and $l(B) > (p^k-1)\phi(n) + \frac{p^d-1}{n^2}$ if $n > 1$.

(ii)

p^d	5^2	7^2	11^2	11^2	23^2	29^2	59^2
$l(B)$	7	8	9	35	88	63	261

Conversely, all values for $l(B)$ given in (i) *and* (ii) *do occur in examples.*

Proof. By [HKKS, Theorem 7.1], B has an elementary abelian defect group D. The equation $k(B)-l(B)=1$ implies further that the inertial quotient E of B acts regularly on $D \setminus \{1\}$. It follows that all Sylow subgroups of E are cyclic or quaternion groups (see [Hup, Hauptsatz V.8.7]). In particular, E has trivial Schur multiplier. Hence, the Alperin weight conjecture asserts that $l(B) = k(E)$ (see [Sam1, Conjecture 2.6] for instance). Note that $D \rtimes E$ is a sharply 2-transitive group on D and those were classified by Zassenhaus [Zas] (see also [DiMo, Section 7.6]). Apart from the seven exceptions described in (ii), $D \rtimes E$ arises from a Dickson near-field F where $(F,+) \cong D$ and $F^\times \cong E$. More precisely, there exists a factorization $d = nk$ as in (i) such that F can be identified with $\mathbb{F}_{q^n}$ where $q = p^k$ and the multiplication is modified as follows. Let $\mathbb{F}_{q^n}^\times = \langle \zeta \rangle$. Let $\gamma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, $x \mapsto x^q$ be the Frobenius automorphism of $\mathbb{F}_{q^n}$ with respect to $\mathbb{F}_q$. According to Zassenhaus, q has multiplicative order n modulo $(q-1)n$, and for every integer a there exists a unique integer a^* such that $0 \le a^* < n$ and

$$q^{a^*} \equiv 1 + a(q-1) \pmod{(q-1)n}.$$

One can check that the pairs (ζ^a, γ^{a^*}) with $0 \le a < q^n - 1$ form a subgroup of $\Gamma\mathrm{L}(1, q^n)$. We identify the elements of $F^\times$ with those pairs, so that the multiplication in F agrees with the multiplication in $\Gamma\mathrm{L}(1, q^n)$. Note that $F^\times$ is just the Singer cycle $\mathbb{F}_q^\times$ if $n = 1$. Although different choices for ζ may lead to non-isomorphic near-fields, the group $F^\times$ is certainly uniquely defined (as a subgroup of $(\mathbb{Z}/(q^n-1)\mathbb{Z}) \rtimes (\mathbb{Z}/n\mathbb{Z})$ for instance).

It is easy to check that $A := \langle (\zeta^n, 1) \rangle \trianglelefteq F^\times$ and $F^\times/A \cong C_n$. This makes it possible to compute $k(E) = k(F^\times)$ via Clifford theory with respect to A. The natural actions of $F^\times$ on A and on $\mathrm{Irr}(A)$ are permutation isomorphic, by Brauer's permutation lemma. Thus, instead of counting characters of A with a specific order we may just count elements. For a divisor $e \mid n$, let $\alpha(e)$ be the number of elements in $F^\times \cap \mathbb{F}_{q^e} := \{(\zeta^a, \gamma^{a^*}) : \zeta^a \in \mathbb{F}_{q^e}\}$ which do not lie in any proper subfield of $\mathbb{F}_{q^e}$. Then

$$\beta(e) := |F^\times \cap \mathbb{F}_{q^e}| = \frac{q^e - 1}{e} = \sum_{f \mid e} \alpha(f).$$

By Möbius inversion we obtain

$$\alpha(e) = \sum_{f \mid e} \mu(e/f) \frac{q^f - 1}{f}.$$

This is also the number of characters in $\mathrm{Irr}(A)$ with inertial index e. These characters distribute into $\alpha(e)/e$ orbits under $F^\times$. Each such character has n/e distinct extensions to its inertial group and each such extension induces to an irreducible character of $F^\times$. The number of characters of $F^\times$ obtained in this way is therefore $\alpha(e)n/e^2$. In total,

$$l(B) = k(E) = k(F^\times) = \sum_{e \mid n} \frac{n}{e^2} \sum_{f \mid e} \mu(e/f) \frac{q^f - 1}{f}.$$

Now observe that $n^2 = \sum_{d \mid n} J_2(d)$ for all $n \ge 1$. Hence, another Möbius inversion yields

$$\sum_{e \mid n} \frac{n}{e^2} \sum_{f \mid e} \mu(e/f) \frac{q^f - 1}{f} = \sum_{f \mid n} \frac{q^f - 1}{fn} \sum_{e' \mid \frac{n}{f}} \Big(\frac{n}{e'f}\Big)^2 \mu(e') = \sum_{f \mid n} \frac{q^f - 1}{fn} J_2(n/f).$$

If $n > 1$, then $n\phi(n) = n^2 \prod_{p \mid n} \frac{p-1}{p} < J_2(n)$ and the second claim follows.

Conversely, if $d = nk$ satisfies the condition in (i), then a corresponding near-field F can be constructed as above. This in turn leads to a sharply 2-transitive group $G = F \rtimes F^\times$. Now G has only one block B, namely the principal block, and $l(B) = k(F^\times)$ is given as above. ∎

4. Principal blocks of almost simple groups of Lie type

This section is devoted to the proof of the following result:

THEOREM 4.1: *Let $p \geq 3$ be a prime and $S \neq {}^2F_4(2)'$ a simple group of Lie type in characteristic different from p. Assume that the Sylow p-subgroups of S are abelian but not cyclic. Let $S \trianglelefteq G \leq \mathrm{Aut}(S)$ such that $p \nmid |G/S|$. Let $B_0(G)$ be the principal p-block of G. Then either $l(B_0(G)) \geq p$ or $k_p(G) \geq 3$.*

We will work with the following setup. Let $\mathcal{G}$ be a simple algebraic group of simply connected type defined over $\mathbb{F}_q$ and F a Frobenius endomorphism on $\mathcal{G}$ such that $S = \mathbb{G}/\mathbf{Z}(\mathbb{G})$, where $\mathbb{G} := \mathcal{G}^F$ is the set of fixed points of $\mathcal{G}$ under F. Let $\mathcal{G}^*$ be an algebraic group with a Frobenius endomorphism which, for simplicity, we denote by the same F, such that $(\mathcal{G}, F)$ is in duality to $(\mathcal{G}^*, F)$. Set $\mathbb{G}^* := \mathcal{G}^{*F}$. As we will see below, the Brauer characters in the principal blocks of S and $\mathbb{G}$ arise from the so-called unipotent characters of $\mathbb{G}$. These are the irreducible characters of $\mathbb{G}$ occurring in a Deligne–Lusztig character $R^{\mathcal{G}}_{\mathcal{T}}(1)$, where $\mathcal{T}$ runs over the F-stable maximal tori of $\mathcal{G}$; see [DiMi, Definition 13.19]. It is well-known that the unipotent characters of $\mathbb{G}$ all have $\mathbf{Z}(\mathbb{G})$ in their kernel, and so they are viewed as (unipotent) characters of S.

With the hypothesis of Theorem 4.1 on $P \in \mathrm{Syl}_p(S)$ and p, we may assume that S is not one of the types A_1, ${}^2G_2$, and ${}^2B_2$. Assume for a moment that S is also not a Ree group of type ${}^2F_4$, so that F defines an $\mathbb{F}_q$-rational structure on $\mathcal{G}$. Let d be the multiplicative order of q modulo p.

By [KM2, Theorem A], which includes earlier results of Broué–Malle–Michel [BMM] and of Cabanes–Enguehard [CE], the p-blocks of $\mathbb{G}$ are parameterized by d-cuspidal pairs $(\mathcal{L}, \lambda)$ of a d-split Levi subgroup $\mathcal{L}$ of $\mathcal{G}$ and a d-cuspidal unipotent character λ of $\mathcal{L}^F$. In particular, the principal block of $\mathbb{G}$ corresponds to the pair consisting of the centralizer $\mathcal{L}_d := \mathbf{C}_{\mathcal{G}}(\mathcal{S}_d)$ of a Sylow d-torus $\mathcal{S}_d$ of $\mathcal{G}$ and the trivial character of $\mathcal{L}_d^F$. Moreover, the number of unipotent characters in $B_0(\mathbb{G})$ is the same as the number of characters in the d-Harish-Chandra series associated to the pair $(\mathcal{L}_d, 1)$. By [BMM, Theorem 3.2], characters in each d-Harish-Chandra series are in one-to-one correspondence with the irreducible characters of the relative Weyl group of the d-cuspidal pair defining the series. Therefore, the number of unipotent characters in $B_0(\mathbb{G})$ is precisely the number of irreducible characters of the relative Weyl group $W(\mathcal{L}_d)$ of $\mathcal{L}_d$.

Assume that $p \nmid |\mathbf{Z}(\mathbb{G})|$. Then, as the Sylow p-subgroups of S are abelian, those of $\mathbb{G}$ are abelian as well. In such situation, we follow [MM, §5.3] to control the number of conjugacy classes of p-elements in $\mathbb{G}$. In particular, by [Mal3, Proposition 2.2], we know that the order d of q modulo p defined above is the unique positive integer such that $p \mid \Phi_d(q)$ and Φ_d divides the generic order of $\mathbb{G}$, where Φ_d denotes the dth cyclotomic polynomial. Furthermore, p is indeed a good prime for $\mathcal{G}$ (see [Mal3, Lemma 2.1]). Let $\Phi_d^{m_d}$ be the precise power of Φ_d dividing the generic order of $\mathbb{G}$.

Assume furthermore that G has a unique class of nontrivial p-elements. By the main result of [KNST], a $P \in \mathrm{Syl}_p(S)$ must be elementary abelian, and thus $\Phi_d(q)$ is divisible by p but not p^2. Therefore, P is isomorphic to the direct product of m_d copies of C_p. Since P is non-cyclic, $m_d > 1$.

It is well-known that fusion of semisimple elements in a maximal torus is controlled by its relative Weyl group (see [MT, Exercise 20.12] or [MM, p. 6123]). By choosing P to be inside the Sylow d-torus $\mathcal{S}_d$ and letting $\mathcal{T}_d$ be an F-stable maximal torus of $\mathcal{G}$ containing $\mathcal{S}_d$, we deduce that the fusion of p-elements in P is controlled by the relative Weyl group $W(\mathcal{T}_d)$ of $\mathcal{T}_d$. Therefore, the number of conjugacy classes of (non-trivial) p-elements of $\mathbb{G}$, and hence of S, is at least

$$\frac{|P|-1}{|W(\mathcal{T}_d)|} = \frac{p^{m_d}-1}{|W(\mathcal{T}_d)|}.$$

Note that when d is regular for $\mathcal{G}$, which means that $\mathbf{C}_{\mathcal{G}}(\mathcal{S}_d)$ is a maximal torus of $\mathcal{G}$, the maximal torus $\mathcal{T}_d$ can be chosen to be the same as $\mathcal{L}_d = \mathbf{C}_{\mathcal{G}}(\mathcal{S}_d)$, and this indeed happens for all exceptional types and all d, except the single case of type E_7 and $d = 4$ (see also [HSF, p. 19]).

Recall that $p \nmid |\mathbf{Z}(\mathbb{G})|$, and thus $B_0(\mathbb{G})$ and $B_0(S)$ are isomorphic, and, moreover, p is a good prime for $\mathcal{G}$. By a result of Geck [Gec2, Theorem A], the restrictions of unipotent characters of $\mathbb{G}$ in $B_0(\mathbb{G})$ to p-regular elements form a basic set of Brauer characters of $B_0(\mathbb{G})$. In particular, $l(B_0(S)) = l(B_0(\mathbb{G}))$ is precisely the number of unipotent (ordinary) characters in $B_0(\mathbb{G})$, which in turn is the number $k(W(\mathcal{L}_d))$ of irreducible characters of $W(\mathcal{L}_d)$, as mentioned above.

Proposition 4.2: *Theorem 4.1 holds for groups of exceptional Lie types.*

Proof. We will keep the notation above. In particular, $\mathbb{G}$ and $\mathbb{G}^*$ are finite reductive groups of respectively simply-connected and adjoint type with

$$S = \mathbb{G}/\mathbf{Z}(\mathbb{G}) \cong [\mathbb{G}^*, \mathbb{G}^*].$$

First we note that the Sylow 3-subgroups of simple groups of type E_6 or ${}^2E_6$ are not abelian since their Weyl group $(\mathrm{SO}(5,3))$ has a non-abelian Sylow 3-subgroup. So we have $p \nmid |\mathbf{Z}(\mathbb{G})|$ in all cases.

We will follow the following strategy to prove the theorem for exceptional types. Let $\mathbb{G}_1$ be the extension of $\mathbb{G}^*$ to include field automorphisms. We will view both $\mathbb{G}_1$ and $\mathbb{G}^*$ as subgroups of $\mathrm{Aut}(S)$. Let

$$H := \langle G \cap \mathbb{G}^*, \mathbf{C}_{G\cap\mathbb{G}_1}(P)\rangle,$$

where $P \in \mathrm{Syl}_p(S)$. Note that every unipotent character of S is $\mathbb{G}_1$-invariant and extendible to its inertial subgroup in $\mathrm{Aut}(S)$, by results of Lusztig and Malle (see [Mal2, Theorems 2.4 and 2.5]). In particular, every unipotent character in $B_0(S)$ extends to a character in $B_0(\mathbb{G}_1)$. By [Gec2, Theorem A], it follows that each $\theta \in \mathrm{IBr}(B_0(S))$ extends to some $\mu \in \mathrm{IBr}(B_0(G\cap\mathbb{G}_1))$. Now $\mu_H \in \mathrm{IBr}(B_0(H))$. Moreover, as $P\mathbf{C}_{G\cap\mathbb{G}_1}(P) \subseteq H$, $B_0(G\cap\mathbb{G}_1)$ is the only block of $G\cap\mathbb{G}_1$ covering $B_0(H)$ (see [RSV, Lemma 1.3]). It follows that

$$\mu\eta \in \mathrm{IBr}(B_0(G\cap\mathbb{G}_1)) \quad \text{for every } \eta \in \mathrm{IBr}((G\cap\mathbb{G}_1)/H)$$

by [Nav1, Corollary 8.20 and Theorem 9.2]. (Here we remark that $(G\cap\mathbb{G}_1)/H$ is a quotient of $(G\cap\mathbb{G}_1)/(G\cap\mathbb{G}^*)$ and thus cyclic, implying that $|\mathrm{IBr}((G\cap\mathbb{G}_1)/H)| = |(G\cap\mathbb{G}_1)/H|$.) Note that each character $\mu\eta \in \mathrm{IBr}(B_0(G\cap\mathbb{G}_1))$ lies under a character of $\mathrm{IBr}(B_0(G))$ and two of them $\mu\eta$ and $\mu'\eta'$ are fused under G only possibly when the unipotent characters μ_S and μ'_S are fused under graph automorphisms of S. Let n denote the number of orbits of unipotent characters in $B_0(S)$ under $\mathrm{Aut}(S)$. We now have

$$l(B_0(G)) \geq n|(G\cap\mathbb{G}_1)/H|. \tag{4.1}$$

We recall here that the number of unipotent characters in $B_0(S)$ is exactly

$$k(W(\mathcal{L}_d)).$$

How these unipotent characters are fused under graph automorphisms will be examined below in a case by case analysis.

Assume for now that d is regular for $\mathcal{G}$ (which means $(\mathcal{G}, d) \neq (E_7, 4)$), we then choose $\mathcal{T}_d := \mathcal{L}_d$ as mentioned above. Recall that $|P| = p^{m_d}$ and S then has at least $(p^{m_d} - 1)/|W(\mathcal{L}_d)|$ conjugacy classes of non-trivial p-elements. Assume that G has a unique class of non-trivial p-elements, and therefore we aim to prove that $l(B_0(G)) \geq p$. Since $\mathbf{C}_G(P)$ fixes every class of p-elements of S, we deduce that

$$\frac{p^{m_d} - 1}{|W(\mathcal{L}_d)|} \leq \frac{|G|}{|\langle S, \mathbf{C}_G(P)\rangle|} \leq \mathbf{d}\frac{|G|}{|H|} \leq \mathbf{dg}\frac{|G \cap \mathbb{G}_1|}{|H|}, \tag{4.2}$$

where $\mathbf{d} = |\mathbb{G}^* : S|$ and $\mathbf{g} = |\mathrm{Out}(S) : \mathbb{G}_1|$ are respectively the orders of the groups of diagonal and graph automorphisms of S.

We now go through various types of S to reach the conclusion, with the help of (4.1) and (4.2). For simplicity, set

$$x := |(G \cap \mathbb{G}_1)/H|.$$

The relative Weyl groups $W(\mathcal{L}_d)$ for various types of $\mathcal{G}$ and d are available in [BMM, Table 3]. These relative Weyl groups are always complex reflection groups and we will follow their notation in [BMM] as well as [Ben]. Recall that as the Sylow p-subgroups of S are non-cyclic, we may exclude the types ${}^2B_2$ and ${}^2G_2$.

Let $S = G_2(q)$ with $q > 2$. Then $d \in \{1, 2\}$, $m_1 = m_2 = 2$, and $W(\mathcal{L}_d)$ is the dihedral group D_{12}. Here all unipotent characters of S are $\mathrm{Aut}(S)$-invariant unless $q = 3^f$ for some odd f, in which case the graph automorphism fuses two certain unipotent characters in the principal series, by a result of Lusztig (see [Mal2, Theorem 2.5]). In any case, the bound (4.1) yields $l(B_0(G)) \geq (k(D_{12}) - 1)x = 5x$. Together with (4.2), we have

$$l(B_0(G)) \geq 5x > \sqrt{24x} \geq \sqrt{p^2 - 1} > p - 1,$$

as desired.

For $S = F_4(q)$ we have $d \in \{1, 2, 3, 4, 6\}$ with $m_1 = m_2 = 4$ and $m_3 = m_4 = m_6 = 2$. Here all unipotent characters of S are $\mathrm{Aut}(S)$-invariant unless $q = 2^f$ for some odd f, in which case the graph automorphism fuses eight pairs of certain unipotent characters. Also,

$$W(\mathcal{L}_{1,2}) = G_{28}, \quad W(\mathcal{L}_{3,6}) = G_5 \quad \text{and} \quad W(\mathcal{L}_4) = G_8.$$

In all cases we have

$$l(B_0) \geq (k(W(\mathcal{L}_d)) - 8)x > (2|W(\mathcal{L}_d)|x)^{1/m_d} \geq (p^{m_d} - 1)^{1/m_d} > p - 1.$$

For all other exceptional types every unipotent character of S is $\mathrm{Aut}(S)$-invariant, again by [Mal2, Theorem 2.5]. The bound (4.1) then implies that $l(B_0(G)) \geq k(W(\mathcal{L}_d))x$. On the other hand, the bound (4.2) yields

$$\mathbf{dg}x|W(\mathcal{L}_d)| \geq p^{m_d} - 1.$$

The routine estimates are then indeed sufficient to achieve the desired bound.

As the arguments for ${}^3D_4$, E_6, ${}^2E_6$, E_7 with $d\neq 4$, and E_8 are fairly similar, we provide details only for $S=E_8(q)$ as an example. Then $d\in\{1,2,3,4,6,5,8,10,12\}$ with $m_{1,2} = 8$, $m_{3,4,6} = 4$, and $m_{5,8,10,12} = 2$. Going through various values of d, we observe that $k(W(\mathcal{L}_d))^{m_d} > |W(\mathcal{L}_d)|$ for all relevant d. The above estimates then imply that

$$l(B_0(G))^{m_d} \geq k(W(\mathcal{L}_d))^{m_d}x > |W(\mathcal{L}_d)|x \geq p^{m_d} - 1,$$

which in turns implies that $l(B_0(G)) \geq p$.

Assume that $S = E_7(q)$ and $d = 4$. (Recall that $d = 4$ is not regular for type E_7.) Then $m_d = 2$. By [BMM, Table 1], $\mathcal{L}_d = \mathcal{S}_d.A_1^3$, $W(\mathcal{L}_d) = G_8$ and $W(\mathcal{T}_d)$ is an extension of G_8 by C_2^3 for any maximal torus $\mathcal{T}_d$ containing $\mathcal{S}_d$. Note that here $\mathrm{Out}(S)$ is the direct product of $C_{\gcd(2,q-1)}$ and C_f where $q = \ell^f$ for some prime ℓ, and thus is abelian. Let

$$y := |G/\langle S, \mathbf{C}_G(P)\rangle|$$

and arguing similarly as above, we have $l(B_0(G)) \geq k(W(\mathcal{L}_d))y = 16y$ and $p^2 - 1 \leq y|W(\mathcal{T}_d)| = 768y$. If $y \geq 3$ then $l(B_0(G))^2 \geq 16^2y^2 \geq 768y \geq p^2-1$, as desired. If $y = 1$ then $p \leq 23$, and since we are done if $p \leq 16$, we may assume that $p = 17, 19$, or 23, but for these primes, $p^2 - 1$ does not divide $|W(\mathcal{T}_d)| = 768$, implying that S, and hence G, has more than one class of p-elements. Lastly, if $y = 2$ then the only prime we need to take care of is $p = 37$, but as $37^2 - 1 = 1368$ cannot be a sum of two divisors of $|W(\mathcal{T}_d)|$, S now has at least three classes of p-elements, implying that G has more than one class of p-elements, as desired.

Finally, let $S = {}^2F_4(q)$ with $q = 2^{2n+1} \geq 8$. Here the prime p divides exactly one of $\Phi_1(q)$, $\Phi_2(q)$, $\Phi_{4^+}(q) = q + \sqrt{2q} + 1$, and $\Phi_{4^-}(q) = q - \sqrt{2q} + 1$, and $m_d = 2$ in all cases. All the Sylow d-tori are maximal and their relative Weyl groups are D_{16} for $d = 1$, G_{12} for $d = 2$, and G_8 for $d = 4^{\pm}$. With these modifications, the estimates (4.1) and (4.2) are still applied to arrive at the desired bound $l(B_0(G)) \geq p$. ∎

PROPOSITION 4.3: *Theorem 4.1 holds for groups of classical types. More precisely, if S is a classical group and $p \geq 3$ as in Theorem 4.1, then either $k_p(G) \geq 3$, or $p = 3|(q-\epsilon)$, $S = \mathrm{PSL}^\epsilon(3,q)$, and $l(B_0(G)) \geq 3$.*

Proof. First consider $S = \mathrm{PSL}^\epsilon(n,q)$ with $\epsilon = \pm$ and $n \geq 3$. Here, as usual, $\mathrm{PSL}^+(n,q) := \mathrm{PSL}(n,q)$ and $\mathrm{PSL}^-(n,q) := \mathrm{PSU}(n,q)$. Let e be the smallest positive integer such that $p \mid (q^e - \epsilon^e)$.

Assume that $p \nmid |\mathbf{Z}(\mathrm{SL}^\epsilon(n,q))|$, and thus we may view P as a (Sylow) p-subgroup of $\mathrm{SL}^\epsilon(n,q)$. Since P is not cyclic, we have $2e \leq n$. (If $2e > n$ then P would be contained in a torus of order $q^e - \epsilon^e$, and hence cyclic.) Let α be an element of $\overline{\mathbb{F}}_q^\times$ of order p. We then can find an element $x_0 \in \mathrm{SL}^\epsilon(e,q)$ of order p that is conjugate to $\mathrm{diag}(\alpha, \alpha^{\epsilon q}, \ldots, \alpha^{(\epsilon q)^{e-1}})$ over $\overline{\mathbb{F}}_q$. Now we observe that the two elements $x := \mathrm{diag}(x_0, I_{n-e})$ and $y := \mathrm{diag}(x_0, x_0, I_{n-2e})$ of $\mathrm{SL}^\epsilon(n,q)$ produce two corresponding elements of order p in S that cannot be conjugate in G, as desired.

Now assume $p \mid |\mathbf{Z}(\mathrm{SL}^\epsilon(n,q))|$. As $P \in \mathrm{Syl}_p(S)$ is abelian, this happens only when $p = 3$ (see [KS, Lemma 2.8]). The proof of [KNST, Lemma 2.5] shows that, in this case, $S = \mathrm{PSL}^\epsilon(3,q)$ with $3 \mid (q-\epsilon)$ but $9 \nmid (q-\epsilon)$. Moreover, $q = \ell^f$ for some prime ℓ with $3 \nmid f$, so the Sylow 3-subgroups of S (and G) are elementary abelian of order 9. Suppose that $l(B_0(G)) \leq 2$. Then the irreducible Brauer characters in $B_0(G)$ are 1_G, and possibly another character qγ. On the other hand, it is known from [Gec1, Theorem 4.5] and [Kun, Table 1] that $B_0(S)$ then contains precisely 5 distinct irreducible 3-Brauer characters, two of which, 1_S and α, are linear combinations of the restrictions of the two unipotent characters of degrees 1 and $q^2 - \epsilon q$ to 3-regular elements, and thus are G-invariant; and three more $\beta_1, \beta_2, \beta_3$. It follows that γ lies above α, but then none of the Brauer characters of $B_0(G)$ can lie above β_i, a contradiction. Hence $l(B_0(G)) \geq 3$, as required. (In fact, Broué's abelian defect group conjecture, and hence the blockwise Alperin weight conjecture, holds for principal 3-blocks with elementary abelian defect groups of order 9, see [KK], and thus the bound $l(B_0(G)) \geq 3$ also follows by Section 3.)

For symplectic and orthogonal types, note that as p is odd, we may view $P \in \mathrm{Syl}_p(S)$ as a Sylow p-subgroup of Sp, SO, and GO. Let e be the smallest positive integer such that $p \mid (q^{2e} - 1)$. As above we have $2e \leq n$ by the non-cyclicity of P.

Consider $S = \mathrm{PSp}(2n,q)$ with $n \geq 2$. Since $\mathrm{SL}(2,q^e) < \mathrm{Sp}(2e,q)$, we may find an element x_0 in $\mathrm{Sp}(2e,q)$ of order p with spectrum

$$\{\alpha, \alpha^q, \ldots, \alpha^{q^{e-1}}, \alpha^{-1}, \alpha^q, \ldots, \alpha^{-q^{e-1}}\}$$

(see the proof of [NT, Proposition 2.6]). Note that

$$\mathrm{Sp}(2e,q) \times \mathrm{Sp}(2e,q) \times \mathrm{Sp}(2n-4e,q) < \mathrm{Sp}(2e,q) \times \mathrm{Sp}(2n-2e,q) < \mathrm{Sp}(2n,q).$$

Now one sees that the images of

$$x := \mathrm{diag}(x_0, I_{2n-2e}) \quad \text{and} \quad y := \mathrm{diag}(x_0, x_0, I_{2n-4e})$$

in S are not conjugate in G.

Consider $S = \Omega(2n+1,q)$ with q odd and $n \geq 3$. Since $p \mid (q^{2e}-1)$, there is a (unique) $\lambda \in \{\pm 1\}$ such that $p \mid (q^e - \lambda)$. Using the embedding

$$C_{q^e-\lambda} \cong \mathrm{SO}^\lambda(2,q^e) < \mathrm{GO}^\lambda(2e,q),$$

we may find $x_0 \in \mathrm{GO}^\lambda(2e,q)$ of order p and with the spectrum

$$\{\alpha^{\pm 1}, \alpha^{\pm q}, \ldots, \alpha^{\pm q^{e-1}}\}.$$

This x_0 then must be inside $\mathrm{SO}^\lambda(2e,q)$ since it has order p. Note that

$$\mathrm{SO}^\lambda(2e,q) \times \mathrm{SO}^\lambda(2e,q) \times \mathrm{SO}(2n-4e+1,q) < \mathrm{SO}(2n+1,q).$$

It follows that the images of

$$x := \mathrm{diag}(x_0, I_{2n-2e+1}) \quad \text{and} \quad y := \mathrm{diag}(x_0, x_0, I_{2n-4e+1})$$

in S are of order p, and are not conjugate in G.

For $S = \mathrm{P}\Omega^+(2n,q)$ with $n \geq 4$, using the same element $x_0 \in \mathrm{SO}^\lambda(2e,q)$ as in the case of odd-dimensional orthogonal groups and the embedding

$$\mathrm{SO}^\lambda(2e,q) \times \mathrm{SO}^\lambda(2e,q) \times \mathrm{SO}^+(2n-4e,q) < \mathrm{SO}^+(2n,q),$$

we arrive at the same conclusion.

Finally, consider $S = \mathrm{P}\Omega^-(2n,q)$ with $n \geq 4$. If $n = 2e$, then we have $p \mid (q^n - 1)$ and it follows that the Sylow p-subgroups of S are in fact cyclic, which is not the case. So $n \geq 2e+1$. As in the case of split orthogonal groups, but using the embedding

$$\mathrm{SO}^\lambda(2e,q) \times \mathrm{SO}^\lambda(2e,q) \times \mathrm{SO}^-(2n-4e,q) < \mathrm{SO}^-(2n,q),$$

we have that G has at least two classes of non-trivial p-elements as well. This finishes the proof. ∎

5. Proofs of Theorem 1.1 and Theorem 1.2

In this section we prove Theorem 1.2, relying on Theorem 4.1. After that we deduce Theorem 1.1.

We restate Theorem 1.2 for the convenience of the reader.

Theorem 5.1: *Let p be a prime and let G be a finite group with $k_p(G) = 2$. Let B_0 be the principal p-block of G. Then either $l(B_0) \geq p - 1$, or $p = 11$ and $G/\mathbf{O}_{p'}(G) \cong C_{11}^2 \rtimes \mathrm{SL}(2, 5)$. Furthermore, $l(B_0) = p - 1$ if and only if $\mathbf{N}_G(P)/\mathbf{O}_{p'}(\mathbf{N}_G(P))$ is isomorphic to the Frobenius group $C_p \rtimes C_{p-1}$.*

Proof. Recall that B_0 is isomorphic to the principal p-block of $G/\mathbf{O}_{p'}(G)$. We may assume that $\mathbf{O}_{p'}(G) = 1$. Moreover, as the theorem is obvious for $p = 2$, we will assume $p \geq 3$. Also, since the case of cyclic Sylow follows from the blockwise Alperin weight conjecture, as explained in Section 3, we assume furthermore that $P \in \mathrm{Syl}_p(G)$ is not cyclic. We aim to prove that $l(B_0) > p - 1$ or $p = 11$ and $G \cong C_{11}^2 \rtimes \mathrm{SL}(2, 5)$.

Assume first that P is non-abelian. Then $p \leq 5$ by the main result of [KNST]. Moreover, when $p = 5$, G is isomorphic to the sporadic simple Thompson group Th, and from the Atlas [Atl] we get $l(B_0) = l(B_0(Th)) = 20 > 4$, as desired. Let $p = 3$. Then $S := \mathbf{O}^{p'}(G)$ is isomorphic to the Rudvalis group Ru, the Janko group J_4, the Tits group ${}^2F_4(2)'$, or the Ree groups ${}^2F_4(q)$ with $q = 2^{6b\pm1}$ for $b \in \mathbb{Z}^+$, by [KNST] again. Since

$$\mathbf{C}_G(S) \cong \mathbf{C}_G(S)/\mathbf{C}_G(S) \cap S \cong G/S = G/\mathbf{O}^{p'}(G),$$

we have

$$\mathbf{C}_G(S) \leq \mathbf{O}_{p'}(G) = 1$$

and G is almost simple. We now check with [GAP] that

$$l(B_0(Ru)) = l(B_0(J_4)) = l(B_0({}^2F_4(2)')) = l(B_0({}^2F_4(2))) = 9 > 2.$$

Therefore we may assume that $S = {}^2F_4(q)$ with $q = 2^{6b\pm1}$ for some $b \in \mathbb{Z}^+$ and $S \trianglelefteq G \leq \mathrm{Aut}(S)$. By [Mal1, §6 and §7] (see also [Him, Table C5]), the principal 3-block of ${}^2F_4(q)$ $(q \geq 8)$ contains three irreducible Brauer characters (denoted by ϕ_{21}, $\phi_{5,1}$, and of course the trivial character) that are $\mathrm{Aut}(S)$-invariant (since their degrees are unique in $B_0(S)$), and thus we have $l(B_0) \geq 3$, as wanted.

We may now assume that P is abelian. By Burnside's fusion argument, all non-trivial p-elements of $\mathbf{N}_G(P)$ are conjugate, i.e., $\mathbf{N}_G(P)$ satisfies the hypothesis of Theorem 2.1. Let N be a minimal normal subgroup of G. If N is elementary abelian, then $N = P$ since every element of P is conjugate to some element of N. From $\mathbf{O}_{p'}(G) = 1$ it then follows that B_0 is the only block of G. Hence, the theorem follows from Theorem 2.1. Now let $N = T_1 \times \cdots \times T_n$ with non-abelian simple groups $T_1 \cong \cdots \cong T_n$. Since $\mathbf{O}_{p'}(G) = 1$, $|T_i|$ is divisible by p. Since non-trivial p-elements of the form $(x, 1, \ldots, 1)$ and $(x, x, 1, \ldots, 1)$ in N cannot be conjugate in G, we conclude that $n = 1$, i.e., N is simple. Since $\mathbf{C}_G(N) \cap N = \mathbf{Z}(N) = 1$ we have $\mathbf{C}_G(N) \leq \mathbf{O}_{p'}(G) = 1$. Altogether,

$$G \leq \mathrm{Aut}(N),$$

i.e., G is an almost simple group. Moreover, $p \nmid |G/N|$.

Let $N = \mathsf{A}_n$ be an alternating group. Recall that the Sylow p-subgroups of G (and N) are not cyclic. Therefore, $n \geq 2p$. But then the p-elements of cycle type (p) and (p, p) are not conjugate in G.

The sporadic and the Tits groups can be checked with [GAP] (or one appeals to the Alperin weight conjecture proved in [Sam2]).

Next let N be a simple group of Lie type in characteristic p. Then P can only be abelian if $N \cong \mathrm{PSL}(2, p^n)$ for some $n \geq 1$ (see [SW, Proposition 5.1] for instance). In this case, the Alperin weight conjecture is known to hold for B_0, i.e., $l(B_0) = l(b_0)$ where b_0 is the principal block of $\mathbf{N}_G(P)$. Now $l(b_0)$ is the number of p-regular conjugacy classes of the p-solvable group $H := \mathbf{N}_G(P)/\mathbf{O}_{p'}(\mathbf{N}_G(P))$. Hence, the claim follows from Theorem 2.1 unless possibly $p = 11$ and $H = C_{11}^2 \rtimes \mathrm{SL}(2, 5)$. Then however

$$N \cong \mathrm{PSL}(2, 11^2)$$

and $\mathrm{SL}(2, 5)$ is not involved in $\mathbf{N}_G(P)$.

The final case, where N is a simple group of Lie type in characteristic different from p, follows from Theorem 4.1. ∎

The following is Theorem 1.1 in the introduction.

Theorem 5.2: *Let p be a prime and G a finite group in which all non-trivial p-elements are conjugate. Then either $k_{p'}(G) \geq p-1$, or $p=11$ and $G \cong C_{11}^2 \rtimes \mathrm{SL}(2, 5)$ (in which case $k_{p'}(G) = 9$). Furthermore, $k_{p'}(G) = p - 1$ if and only if $G \cong C_p \rtimes C_{p-1}$ (Frobenius group).*

Proof. By Theorem 1.2 there are three cases to consider.

If $l(B_0) \geq p$, then clearly $k_{p'}(G) \geq p$.

Next assume that $l(B_0) = p - 1$ and $\mathbf{N}_G(P)/\mathbf{O}_{p'}(\mathbf{N}_G(P)) \cong C_p \rtimes C_{p-1}$ for a Sylow p-subgroup P. If there exists another block $B_1 \neq B_0$, then again $k_{p'}(G) \geq l(B_0) + l(B_1) \geq p$. Hence, we may assume that B_0 is the only block of G. Since $|P| = p$, all characters in G have p'-degree. It follows from the Ito–Michler theorem that $P \trianglelefteq G$. In particular, G is p-solvable and $\mathbf{O}_{p'}(\mathbf{N}_G(P)) = 1$ by [Nav1, Theorem 10.20].

Finally, let $p = 11$ and $G/\mathbf{O}_{p'}(G) \cong C_{11}^2 \rtimes \mathrm{SL}(2,5)$. Then G is p-solvable and Theorem 1.1 follows from Theorem 2.1. ∎

6. Groups with three p-classes

In this section we prove the following result, which provides a bound for $k_{p'}(G)$ for groups G with 3 conjugacy classes of p-elements.

Theorem 6.1: *Let G be a finite group with $k_p(G) = 3$. Then $k_{p'}(G) \geq (p-1)/2$ with equality if and only if $p > 2$ and G is the Frobenius group $C_p \rtimes C_{(p-1)/2}$.*

We will prove that Theorem 6.1 follows from Theorem 2.2, [HM, Theorem 2.1] on bounding the number of orbits of p-regular classes of simple groups under their automorphism groups, the known cyclic Sylow case of the blockwise Alperin weight Conjecture, and the following result.

Theorem 6.2: *Let p be a prime and S a finite simple group with non-cyclic Sylow p-subgroups. Let $S \trianglelefteq G \leq \mathrm{Aut}(S)$. Then $k_{p'}(G) \geq p$.*

Proof. The theorem is clear when $p = 2, 3$ as $|G|$ has at least 3 prime divisors. Therefore we may assume that $p \geq 5$. We also may assume that S is not a sporadic simple group or the Tits group, as these could be checked directly using the character table library in [GAP].

Let $S = \mathsf{A}_n$. Since the Sylow p-subgroups of S are not cyclic, we have $n \geq 2p \geq 10$. It follows that A_n has at least $p-1$ cycles of odd length not divisible by p. These cycles together with an involution of S produce at least p p-regular classes of G, as desired.

Next we assume that S is a simple group of Lie type in characteristic p. As before, one then can find a simple algebraic group $\mathcal{G}$ of simply connected type defined in characteristic p and a Frobenius endomorphism F such that

$S = \mathbb{G}/\mathbf{Z}(\mathbb{G})$, where $\mathbb{G} = \mathcal{G}^F$. According to [Car, Theorem 3.7.6], the number of semisimple classes of $\mathbb{G}$ is q^r, where q is the size of the underlying field of $\mathcal{G}$ and r is the rank of $\mathcal{G}$. Therefore,

$$k_{p'}(S) \geq \frac{k_{p'}(\mathbb{G})}{k_{p'}(\mathbf{Z}(\mathbb{G}))} \geq \frac{q^r}{|\mathbf{Z}(\mathbb{G})|}.$$

To prove the theorem in this case, it suffices to prove that $q^r \geq p|\mathbf{Z}(\mathbb{G})||\mathrm{Out}(S)|$. Using the known values of $|\mathbf{Z}(\mathbb{G})|$ and $|\mathrm{Out}(S)|$ available in [Atl, p. xvi] for instance, it is straightforward to check the inequality for all S and relevant values of q, r and p, unless (S, p) is one of the following pairs

$$\{(\mathrm{PSL}(2{,}5^2), 5), (\mathrm{PSL}(3,7){,}7), (\mathrm{PSL}(3,13), 13), (\mathrm{PSU}(3,5), 5), (\mathrm{PSU}(3,11), 11)\}.$$

Again the character tables of the corresponding almost simple groups are available in [GAP] unless $S = \mathrm{PSL}(3,13)$. For this exception we used the computer to find 13 distinct pairs $(|\langle x\rangle|, |\mathbf{C}_S(x)|)$ where $x \in S$ is p-regular. Of course these elements cannot be conjugate in G.

For the rest of the proof, we will assume that S is a simple group of Lie type in characteristic $\ell \neq p$ and let $\mathbb{G} \leq \mathrm{Out}(S)$ be a finite reductive group of adjoint type with socle S. (Note that $\mathbb{G}$ from now on is different from before where it denotes the finite reductive group of simply-connected type.)

Lemma 6.3: *Let S, G and $\mathbb{G}$ as above. If $k_{p'}(\mathbb{G}) \geq p|\mathrm{Out}(S)|$, then*

$$k_{p'}(G) \geq p.$$

Proof. Let $\mathrm{IBr}(S)$ denote the set of p-Brauer irreducible characters of S and $n(H, \mathrm{IBr}(S))$ the number of orbits of the action of a group H on $\mathrm{IBr}(S)$. Let

$$G_1 := \langle G \cup \mathbb{G}\rangle.$$

Then

$$\begin{aligned} k_{p'}(G) \geq n(G, \mathrm{IBr}(S)) \geq n(G_1, \mathrm{IBr}(S)) &= \frac{1}{|G_1|}\Bigg(\sum_{\theta\in\mathrm{IBr}(S)} |\mathrm{Stab}_{G_1}(\theta)|\Bigg) \\ &\geq \frac{1}{|G_1|}\Bigg(\sum_{\theta\in\mathrm{IBr}(S)} |\mathrm{Stab}_{\mathbb{G}}(\theta)|\Bigg) = \frac{|\mathbb{G}|}{|G_1|} n(\mathbb{G}, \mathrm{IBr}(S)) \\ &\geq \frac{|\mathbb{G}|}{|G_1|}\frac{k_{p'}(\mathbb{G})}{|\mathbb{G}/S|} \geq \frac{k_{p'}(\mathbb{G})}{|\mathrm{Out}(S)|} \geq p, \end{aligned}$$

as claimed. ∎

Recall that $p \geq 5$. As the Sylow p-subgroups of S, where p is not the defining characteristic of S, are non-cyclic, S is not one of the types A_1, ${}^2B_2$ and ${}^2G_2$.

1. Let $\mathbb{G} = \mathrm{PGL}^\epsilon(n,q)$ with $\epsilon = \pm$, $q = \ell^f$ and $n \geq 3$. Here as usual we use $\epsilon = +$ for linear groups and $\epsilon = -$ for unitary groups. Consider tori T_i ($i \in \{n-1, n\}$) of $\mathbb{G}$ of size $(q^i - (\epsilon 1)^i)/(q - \epsilon 1)$. Since $\gcd(|T_{n-1}|, |T_n|) = 1$, there exists $t \in \{n-1, n\}$ such that $p \nmid |T_t|$. Note that the fusion of semisimple elements in T_t is controlled by the relative Weyl group, say W_t, of T_t, which is the cyclic group of order t (see [MM, Proposition 5.5] and its proof, for instance). Therefore, the number of p-regular (semisimple) classes of $\mathbb{G}$ with representatives in T_t is at least

$$\frac{q^t - (\epsilon 1)^t}{t(q - \epsilon 1)}.$$

Let $k \in \mathbb{N}$ be the order of q modulo p. Since the Sylow p-subgroups of S are not cyclic, we must have $n \geq 2k$, implying that $p \leq q^{\lfloor n/2 \rfloor} - 1$. Now one can check that

$$\frac{q^t - (\epsilon 1)^t}{t(q - \epsilon 1)} \geq 2f \gcd(n, q - \epsilon 1)p = |\mathrm{Out}(S)|p$$

for all possible values of q, n and p. It follows that

$$k_{p'}(\mathbb{G}) \geq |\mathrm{Out}(S)|p,$$

and therefore we are done in this case by Lemma 6.3.

2. Let $\mathbb{G} = \mathrm{SO}(2n+1, q)$ or $\mathrm{PCSp}(2n, q)$ for $n \geq 2$ and $q = \ell^f$. Since p is odd, it does not divide both $q^n - 1$ and $q^n + 1$. Let T be a maximal torus of G of order either $q^n - 1$ or $q^n + 1$ such that $p \nmid |T|$. The fusion of (semisimple) elements in T is controlled by its relative Weyl group, which is cyclic of order $2n$ in this case. Therefore, the number of conjugacy classes with representatives in T is at least $1 + (q^n - 2)/(2n)$, and it follows that

$$k_{p'}(\mathbb{G}) \geq 2 + \frac{q^n - 2}{2n},$$

since S has at least one non-trivial unipotent class.

Let $k \in \mathbb{N}$ be minimal such that p divides $q^{2k} - 1$. Since the Sylow p-subgroups of S are non-cyclic, we must have $n \geq 2k$. Let $n = 2$. It then follows that $k = 1$ and, as $p \geq 5$, we have $q \geq 8$, and thus the desired inequality $2 + (q^2 - 2)/4 \geq 2fp = p|\mathrm{Out}(S)|$ follows easily. So let $n \geq 3$, and hence $\mathrm{Out}(S)$

is cyclic of order $f\gcd(2,q-1)$. We now easily check that

$$k_{p'}(\mathbb{G}) \geq 2 + \frac{q^n-2}{2n} \geq f\gcd(2,q-1)p$$

for all the relevant values of p,q and n, unless $(n,p,q)=(4,5,2)$, and indeed in all cases we have

$$k_{p'}(\mathbb{G}) \geq p|\mathrm{Out}(S)|,$$

and the theorem follows by Lemma 6.3.

3. Let $\mathbb{G} = \mathrm{PCO}^{\epsilon}(2n,q)$ with $\epsilon = \pm$, $q=\ell^f$ and $n \geq 4$. Here

$$|\mathrm{Out}(S)| = 2f\gcd(4,q^n-\epsilon 1)$$

unless $(n,\epsilon)=(4,+)$, in which case $|\mathrm{Out}(S)| = 6f\gcd(4,q^n-\epsilon 1)$. Similar to other classical groups we have $n \geq 2k$ where k is minimal such that $p \mid (q^{2k}-1)$. First assume that $k \nmid n$. A maximal torus of $\mathbb{G}$ of size $q^n-\epsilon 1$ will then produce at least

$$1 + \frac{q^n-\epsilon 1}{2n}$$

p-regular classes, which are sufficient for the desired bound of $p|\mathrm{Out}(S)|$ unless $(n,\epsilon,q,p) = (4,+,4,5)$, $(5,\pm,2,5)$. The bound still holds for these exceptions since S has elements of at least 5 different orders coprime to 5, which makes $k_{p'}(G) \geq 5 = p$.

Now we may assume $k \mid n$. The case $\epsilon = -$ and $p \mid (q^k-1)$ can be treated as above using a torus of size q^n+1, with a note that $\gcd(q^n+1,q^k-1) \mid 2$ and thus every element in that torus has order coprime to p. So we assume that $\epsilon = +$ or $\epsilon = -$ and $p \mid (q^k+1)$.

Observe that now $\mathbb{G}$ has tori of size $q^{n-1} \pm 1$ which consists of p-regular elements. Also, the non-trivial conjugacy classes with representatives in these two tori have only one possible common class, which is an involution class. Therefore,

$$k_{p'}(\mathbb{G}) \geq 2 + \frac{q^{n-1}-3}{2(n-1)} + \frac{q^{n-1}-1}{2(n-1)} = 2 + \frac{q^{n-1}-2}{n-1} := h(q,n).$$

It turns out that the desired bound $h(q,n) \geq p|\mathrm{Out}(S)|$ is satisfied unless $(S,p) = (P\Omega^-_{12}(2),5)$, $(P\Omega^+_{12}(2),7)$, $(P\Omega^+_{12}(3),13)$, $(P\Omega^+_{16}(2),17)$, $(P\Omega^+_{16}(3),41)$, $(P\Omega^+_8(4),5)$, or $(P\Omega^+_8(q),p)$ with $q \leq 29$ and $p \mid (q^2+1)$ but $p \nmid (q^2-1)$.

For the pairs $(S,p) = (P\Omega^-_{12}(2),5)$, $(P\Omega^+_{12}(2),7)$, or $(P\Omega^+_8(4),5)$, one can confirm the bound by just counting the prime divisors of $|S|$. For $(S,p) = (P\Omega^+_{16}(2),17)$, by counting elements of certain order in the two tori of sizes $2^7 \pm 1$, we observe that $\mathbb{G} = S$ has at least $126/14 = 9$ classes of 127-elements, $42/14 = 3$ classes of 43-elements, and $84/14 = 6$ classes of 129-elements, which implies that G has at least 10 classes of $\{127, 43, 129\}$-elements, and hence, by also including classes of elements of order 1, 2, 3, 5, 7, 9, 13, we have the claimed bound. The same strategy also works for $(P\Omega^+_{12}(3), 13)$ and $(P\Omega^+_{16}(3), 41)$.

We are now left with the case $(S, p) = (P\Omega^+_8(q), p)$ with $q \leq 29$ and $p \mid (q^2+1)$ but $p \nmid (q^2 - 1)$. Using the lower bound for the number of $\mathrm{Aut}(S)$-orbits on p-regular classes of S in the proof of [HM, Lemma 4.6], we end up with the open cases

$$(q, p) \in \{(4, 17), (5, 13), (8, 13), (9, 41), (11, 61)\}.$$

These groups can be realized as permutation groups (of degree 21,435,888 in the last case) in [GAP]. In each case we constructed enough random p-regular elements in S and computed their centralizer orders to make sure that these elements are not conjugate in G.

4. Now we turn to the case where S is of exceptional type different from ${}^2B_2$ and ${}^2G_2$. To conveniently write the order $|S|$ and its factors, we use Φ_d to denote the dth cyclotomic polynomial over the rational numbers.

As above let $\mathbb{G}$ be a finite reductive group (over a field of size q) of adjoint type with socle S, and assume that $|\mathbb{G}| = q^N \prod_i \Phi_i(q)^{a(i)}$ for suitable positive integers $a(i)$ and N. (Indeed, N is the number of positive roots in the root system corresponding to S.) First we assume that the Sylow p-subgroups of $\mathbb{G}$ are not abelian. Then p must divide the order of the Weyl group of $\mathbb{G}$, and thus $\mathbb{G}$ is one of the types E_6, ${}^2E_6$, E_7, and E_8 and $p \leq 7$. Using elementary number theory, one now easily observes that $|S|$ has at least 8 different prime divisors, and hence $k_{p'}(G) \geq 7 \geq p$. So we may and will assume that the Sylow p-subgroups of $\mathbb{G}$ (and S) are abelian (but not cyclic). It follows that there exists a unique $d \in \mathbb{N}$ such that $p \mid \Phi_d(q)$ and $a(d) \geq 2$; see [MT, Lemma 25.14].

Let $\mathbb{G} = G_2(q)$ with $q = \ell^f \geq 3$. We then have $p \mid (q^2 - 1)$. Note that $\mathbb{G} = S$ has maximal tori of coprime orders $\Phi_3(q)$ and $\Phi_6(q)$, which are furthermore coprime to p since $p \geq 5$. The relative Weyl groups of these tori have order 6 (see [BMM, Tables 1 and 3] for sizes of Weyl groups of various maximal tori). Therefore,

$$k_{p'}(\mathbb{G}) \geq 1 + \frac{\Phi_3(q) - 1}{6} + \frac{\Phi_6(q) - 1}{6} = 1 + \frac{q^2}{3}.$$

It is now sufficient to check that $1 + q^2/3 \geq fp$, but this is straightforward. The case $S = F_4(q)$ is handled similarly by considering two maximal tori of orders $\Phi_8(q)$ and $\Phi_{12}(q)$.

Let $S = {}^2F_4(q)$ with $q = 2^{2m+1} \geq 8$. Then we have $p \mid \Phi_1(q)\Phi_2(q)\Phi_4(q)$. Using maximal tori of orders $\Phi_{12}^{\pm}(q) := q^2 \pm \sqrt{2q^3} + q \pm \sqrt{2q} + 1$ with the relative Weyl group of order 12, we end up with

$$k_{p'}(G) \geq 1 + \frac{\Phi_{12}^{+}(q) - 1}{12} + \frac{\Phi_{12}^{-}(q) - 1}{12} = 1 + \frac{q^2 + q}{6}.$$

Certainly $1 + (q^2 + q)/6 \geq (2m + 1)p$ for all possible values of p and m except $(p, m) = (13, 1)$, but this exception can be checked directly using [GAP].

Let $S = {}^3D_4(q)$. We then have $p \mid \Phi_1(q)\Phi_2(q)\Phi_3(q)\Phi_6(q)$. The relative Weyl group of a maximal torus of order $\Phi_{12}(q)$ has order 4, and thus the number of classes with representatives in this torus is at least $1 + (q^4 - q^2)/4$, which in turn is at least $3fp$, as we wanted, unless $(q, p) = (2, 7)$, $(3, 13)$, or $(4, 13)$. The first exception can be handled easily using [Atl]. Let $(S, p) = ({}^3D_4(4), 13)$. We already know that S has at least $(4^4 - 4^2)/4 = 60$ classes of elements of order $\Phi_{12}(4) = 241$ and thus, as $\mathrm{Out}(S)$ is cyclic of order 6, we are done unless $G = \mathrm{Aut}(S)$. In fact, even for $G = \mathrm{Aut}(S)$, one just notices that G has at least $60/6 = 10$ classes of elements of order 241, and therefore, together with classes of elements of order 1, 2 and 3, the desired bound follows. Finally let $(S, p) = ({}^3D_4(3), 13)$. Then S has at least 18 classes of elements of order $\Phi_{12}(3) = 73$, which produces at least 6 classes for G. Now note that $\mathrm{SL}(2, 27) \leq S$, and by using [Atl], we then observe that $\mathrm{SL}(2, 27)$, and hence S, has elements of orders 1, 2, 3, 4, 6, 7, 14, which produce 7 more 13-regular classes, as wanted.

For $\mathbb{G} = E_6(q)_{ad}$, we have $p \mid \Phi_d(q)$ for some $d \in \{1, 2, 3, 4, 6\}$. Consider the (semisimple) classes with representatives in a maximal torus of size $\Phi_9(q)$. Notice that this torus has the relative Weyl group of order 9, so we obtain

$$k_{p'}(\mathbb{G}) \geq 1 + \frac{q^6 + q^3}{9},$$

which is certainly at least $|\mathrm{Out}(S)|p$ for every relevant q and p. Similar arguments also work for $\mathbb{G} = {}^2E_6(q)_{ad}$ and $E_7(q)_{ad}$, but using a maximal torus of respectively size $\Phi_{18}(q)$ and $\Phi_1(q)\Phi_9(q)$ or $\Phi_2(q)\Phi_9(q)$, depending on which size is coprime to p. For $\mathbb{G} = E_8(q)$ with $q = \ell^f$ we have $p \mid \Phi_d(q)$ for some $d \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$ and $\mathbb{G}$ has a maximal torus of size $\Phi_{30}(q)$ with the relative Weyl group of order 30, and it follows that

$$k_{p'}(\mathbb{G}) \geq 1 + \frac{\Phi_{30}(q) - 1}{30} \geq fp,$$

as desired. This concludes the proof of Theorem 6.2. ∎

We are now in the position to prove the main result of this section.

Proof of Theorem 6.1. Assume that the theorem is false and let G be a minimal counterexample. In particular, G is not isomorphic to the Frobenius group $F_p := C_p \rtimes C_{(p-1)/2}$ and $k_{p'}(G) \leq (p-1)/2$. Since $k_p(G/\mathbf{O}_{p'}(G)) = k_p(G) = 3$ and $k_{p'}(G/\mathbf{O}_{p'}(G)) \leq k_{p'}(G)$, we have $\mathbf{O}_{p'}(G) = 1$ or $G/\mathbf{O}_{p'}(G) \cong F_p$. In the latter case G has a cyclic Sylow p-subgroup and hence cannot be a counterexample, as shown in Section 3, and thus we have $\mathbf{O}_{p'}(G) = 1$. Let N be a minimal normal subgroup of G. It follows that $p \mid |N|$, and hence $k_p(G/N) < k_p(G)$. Now since $k_p(G/N)$ cannot be 2 by Theorem 1.2, we must have $p \nmid |G/N|$ and moreover, N is the unique minimal normal subgroup of G.

We are done if N is abelian by Theorem 2.2. So we may assume that N is a direct product of, say n, copies of a non-abelian simple group, say S. Note that $p \mid |S|$ since $p \mid |N|$. Therefore, the assumption $k_p(G) = 3$ implies that $n \leq 2$.

Assume that $n = 2$. Let $m(S,p)$ be the number of $\mathrm{Aut}(S)$-orbits on p-regular classes of S. We then have

$$k_{p'}(G) \geq \frac{1}{2} m(S,p)(m(S,p)+1).$$

It was shown in [HM, Theorem 2.1] that either $m(S,p) > 2\sqrt{p-1}$ or (S,p) belongs to a list of possible exceptions described in [HM, Table 1]. For the former case, we have

$$k_{p'}(G) > \frac{2\sqrt{p-1}(2\sqrt{p-1}+1)}{2} > \frac{p-1}{2},$$

which is a contradiction. For the latter case, going through the list of exceptions, we in fact still have

$$\frac{m(S,p)(m(S,p)+1)}{2} > \frac{p-1}{2},$$

which again leads to a contradiction.

Finally we may assume that $n = 1$, which means that G is an almost simple group with socle S. Furthermore, $p \nmid |G/S|$. The theorem now follows from Section 3 when Sylow p-subgroups of S are cyclic and from Theorem 6.2 otherwise. This completes the proof. ∎

7. Theorem 1.3 and further applications

We now derive Theorem 1.3, which is restated, from Theorem 1.2.

Theorem 7.1: *Let p be a prime and G a finite group in which all non-trivial p-elements are conjugate. Let B_0 denote the principal p-block of G. Then $k_0(B_0) \geq p$ or $p = 11$ and $k_0(B_0) = 10$.*

Proof. The theorem follows from Theorem 1.2 and [KM1] when the Sylow p-subgroups of G are abelian. Assume otherwise. Then, as mentioned before, by [KNST, Theorem 1.1], either

(a) $p = 3$ and $\mathbf{O}^{p'}(G/\mathbf{O}_{p'}(G))$ is isomorphic to Ru, J_4 or ${}^2F_4(q)'$ with $q = 2^{6b\pm1}$ for a nonnegative integer b, or

(b) $p = 5$ and $G/\mathbf{O}_{p'}(G)$ is isomorphic to Th.

We now just proceed as in the proof of Theorem 5.1, but with height 0 characters instead of Brauer characters. For (b) we have $k_0(B_0) = k_0(B_0(Th)) = 20 > 5$, and we are done. For (a) we may assume that G is almost simple. As

$$k_0(B_0(Ru)) = k_0(B_0(J_4)) = k_0(B_0({}^2F_4(2)')) = k_0(B_0({}^2F_4(2))) = 9$$

by [GAP], we may now assume that $S = {}^2F_4(q)'$ with $q = 2^{6b\pm1}$ for some $b \in \mathbb{Z}^+$ and $S \trianglelefteq G \leq \mathrm{Aut}(S)$. According to [Mal1, §6 and §7], the principal 3-block of S contains the Steinberg character denoted by χ_{21} (of degree q), the semisimple character denoted by $\chi_{5,1}$ (of degree $(q-1)(q^2+1)^2(q^4-q^2+1)$), and the trivial character, all of which are $3'$-degree and $\mathrm{Aut}(S)$-invariant, implying that $k_0(B_0) \geq 3$. The theorem is fully proved. ∎

Finally, we provide some more examples of applications of Theorem 1.2 in the study of principal blocks with few characters.

Theorem 7.2: *Let G be a finite group with a Sylow p-subgroup P and the principal p-block B_0. Assume that $k(B_0) = 5$ and $l(B_0) = 4$. Then $P \cong C_5$.*

Proof. By Theorem 1.2, we have $p \leq 5$. By [KNST, Theorem 3.6], P is (elementary) abelian. It then follows by [KM1] that the ordinary irreducible characters in B_0 all have p'-degree, and thus $k_0(B_0) = 5$. However, by [Lan, Corollaries 1.3 and 1.6], $5 = k_0(B_0)$ is divisible by p if $p = 2$ or 3, which cannot happen.

So we are left with $p = 5$. The equality part of Theorem 1.2 then implies that $\mathbf{N}_G(P)/\mathbf{O}_{p'}(\mathbf{N}_G(P))$ is isomorphic to the Frobenius group $C_p \rtimes C_{p-1}$. In particular, $P \cong C_5$, as wanted. ∎

THEOREM 7.3: *Let G be a finite group with a Sylow p-subgroup P and the principal p-block B_0. Assume that $k(B_0) = l(B_0) + 1 = 7$. Then $P \cong C_7$.*

Proof. Again by Theorem 1.2, we have $p \leq 7$ and as above, the cases $p = 2$ or 3 do not occur by [Lan, Corollaries 1.3 and 1.6]. If $p = 7$ then the equality part of Theorem 1.2 implies that $\mathbf{N}_G(P)/\mathbf{O}_{p'}(\mathbf{N}_G(P)) \cong C_7 \rtimes C_6$, yielding that $P \cong C_7$, as claimed.

We now eliminate the possibility $p = 5$. As the Alperin weight conjecture has been known for p-solvable groups and groups with cyclic p-Sylow (see [Spa] for instance), it follows from Theorem 3.3 that G is not p-solvable and has a non-cyclic Sylow p-subgroup. Arguing as in the proof of Theorem 5.1, we may assume that G is an almost simple group with a socle S of Lie type in characteristic not equal to p and $p \nmid |G/S|$. Moreover, P is abelian but non-cyclic. The proof of Proposition 4.3 then shows that, when S is of classical type, G has more than one class of non-trivial p-elements, contradicting the assumption that $k(B_0) - l(B_0) = 1$ and Brauer's formula mentioned in the introduction. Also, the proof of Proposition 4.2 shows that $l(B_0) \geq 7$ when S is of exceptional types except possibly type G_2. (Indeed, the principal block of $G_2(q)$ has exactly 6 irreducible modular characters when $p \mid \Phi_{1,2}(q) = q \pm 1$, since $k(W(\mathcal{L}_{1,2})) = k(D_{12}) = 6$.) So assume $S = G_2(q)$. Note that, since P is not cyclic, $5 = p \mid (q \pm 1)$ and hence q is not an odd power of 3, implying that every unipotent character of S (including 6 in $B_0(S)$) is $\mathrm{Aut}(S)$-invariant, by [Mal2, Theorem 2.5]. However, a quick inspection of the principal block of $G_2(q)$ (see [His, Theorems A and B]) reveals that it contains two (families of) non-unipotent characters of different degrees, implying that $B_0(G)$ contains at least 2 irreducible ordinary characters lying over non-unipotent characters of S. It follows that $k(B_0(G)) \geq 6 + 2 = 8$. This final contradiction completes the proof. ∎

We conclude by noting that, while Theorem 7.2 can also be deduced from the main result of [RSV] on principal blocks with exactly 5 irreducible ordinary characters, Theorem 7.3 is new.

ACKNOWLEDGMENTS. The authors are grateful to Gunter Malle for the careful reading of an earlier version of the paper and providing helpful suggestions that led to a clearer exposition. We thank Attila Maróti for several fruitful discussions on p-regular classes. We also thank the referee for helpful comments on the paper.

References

[Alp] J. L. Alperin, *Weights for finite groups*, in *The Arcata Conference on Representations of Finite Groups (Arcata, Calif., 1986)*, Proceedings of Symposia in Pure Mathematics, Vol. 47, American Mathematical Society, Providence, RI, 1987, pp. 369–379.

[Ben] M. Benard, *Schur indices and splitting fields of the unitary reflection groups*, Journal of Algebra **38** (1976), 318–342.

[BMM] M. Broué, G. Malle and J. Michel, *Generic blocks of finite reductive groups*, Astérisque **212** (1993), 7–92.

[CE] M. Cabanes and M. Enguehard, *On unipotent blocks and their ordinary characters*, Inventiones Mathematicae **117** (1994), 149–164.

[Car] R. W. Carter, *Finite Groups of Lie Type*, Pure and Applied Mathematics (NY), Wiley and Sons, New York, 1985.

[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.

[Dad] E. C. Dade, *Blocks with cyclic defect groups*, Annals of Mathematics **84** (1966), 20–48.

[DiMi] F. Digne and J. Michel, *Representations of Finite Groups of Lie Type*, London Mathematical Society Student Texts, Vol. 21, Cambridge University Press, Cambridge, 1991.

[DiMo] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics, Vol. 163, Springer, New York, 1996.

[GAP] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.11.0*, 2020, http://www.gap-system.org

[Gec1] M. Geck, *Irreducible Brauer characters of the* 3*-dimensional special unitary groups in non-defining characteristic*, Communications in Algebra **18** (2000), 563–584.

[Gec2] M. Geck, *Basic sets of Brauer characters of finite groups of Lie type. II*, Journal of the London Mathematical Society **47** (1993), 255–268.

[HKKS] L. Héthelyi, R. Kessar, B. Külshammer and B. Sambale, *Blocks with transitive fusion systems*, Journal of Algebra **424** (2015), 190–207.

[Him] F. Himstedt, *On the decomposition numbers of the Ree groups* ${}^2F_4(q^2)$ *in non-defining characteristic*, Journal of Algebra **325** (2011), 364–403.

[His] G. Hiss, *On the decomposition numbers of* $G_2(q)$, Journal of Algebra **120** (1989), 339–360.

[HM] N. N. Hung and A. Maróti, *p-Regular conjugacy classes and p-rational irreducible characters*, Journal of Algebra **607** (2022), 387–425.

[HSF] N. N. Hung and A. A. Shaeffer Fry, *On Héthelyi–Külshammer's conjecture for principal blocks*, Algebra & Number Theory **17** (2023), 1127–1151.

[Hup] B. Huppert, *Endliche Gruppen. I*, Grundlehren der Mathematischen Wissenschaften, Vol. 134, Springer, Berlin, 1967.

[Isa] I. M. Isaacs, *Finite Group Theory*, Graduate studies in Mathematics, Vol. 92, American Mathematical Society, Providence, RI, 2008.

[KM1] R. Kessar and G. Malle, *Quasi-isolated blocks and Brauer's height zero conjecture*, Annals of Mathematics **178** (2013), 321–384.

[KM2] R. Kessar and G. Malle, *Lusztig induction and l-blocks of finite reductive groups*, Pacific Journal of Mathematics **279** (2015), 267–296.

[KK] S. Koshitani and N. Kunugi, *Broué's conjecture holds for principal* 3*-blocks with elementary abelian defect group of order 9*, Journal of Algebra **248** (2002), 575–604.

[KS] S. Koshitani and T. Sakurai, *The principal p-blocks with four irreducible characters*, Bulletin of the London Mathematical Society **53** (2021), 1124–1138.

[KNST] B. Külshammer, G. Navarro, B. Sambale and P. H. Tiep, *Finite groups with two conjugacy classes of p-elements and related questions for p-blocks*, Bulletin of the London Mathematical Society **46** (2014), 305–314.

[Kun] N. Kunugi, *Morita equivalent* 3*-blocks of the* 3*-dimensional projective special linear groups*, Proceedings of the London Mathematical Society **80** (2000), 575–589.

[Lan] P. Landrock, *On the number of irreducible characters in a 2-block*, Journal of Algebra **68** (1981), 426–442.

[Lie] M. W. Liebeck, *The affine permutation groups of rank three*, Proceedings of the London Mathematical Society **54** (1987), 477–516.

[Mal1] G. Malle, *Die unipotenten Charaktere von* ${}^2F_4(q^2)$, Communications in Algebra **18** (1990), 2361–2381.

[Mal2] G. Malle, *Extensions of unipotent characters and the inductive McKay condition*, Journal of Algebra **320** (2008), 2963–2980.

[Mal3] G. Malle, *On the inductive Alperin–McKay and Alperin weight conjecture for groups with abelian Sylow subgroups*, Journal of Algebra **397** (2014), 190–208.

[MM] G. Malle and A. Maróti, *On the number of p'-degree characters in a finite group*, International Mathematics Research Notices **20** (2016), 6118–6132.

[MR] G. Malle and G. R. Robinson, *On the number of simple modules in a block of a finite group*, Journal of Algebra **475** (2017), 423–438.

[MT] G. Malle and D. Testerman, *Linear Algebraic Groups and Finite Groups of Lie Type*, Cambridge Studies in Advanced Mathematics, Vol. 133, Cambridge University Press, Cambridge, 2011.

[Nav1] G. Navarro, *Characters and Blocks of Finite Groups*, London Mathematical Society Lecture Note Series, Vol. 250, Cambridge University Press, Cambridge, 1998.

[Nav2] G. Navarro, *Some remarks on global/local conjectures*, in *Finite Simple Groups: Thirty Years of the Atlas and Beyond*, Contemporary Mathematics, Vol. 694, American Mathematical Society, Providence, RI, 2017, pp. 151–158.

[NT] G. Navarro and P. H. Tiep, *Abelian Sylow subgroups in a finite group*, Journal of Algebra **398** (2014), 519–526.

[Pas] D. S. Passman, *p-Solvable doubly transitive permutation groups*, Pacific Journal of Mathematics **26** (1968), 555–577.

[RSV] N. Rizo, A. A. Schaeffer Fry and C. Vallejo, *Principal blocks with 5 irreducible characters*, Journal of Algebra **585** (2021), 316–337.

[Sam1] B. Sambale, *Blocks of Finite Groups and Their Invariants*, Lecture Notes in Mathematics, Vol. 2127, Springer, Cham, 2014.

[Sam2] B. Sambale, *Broué's isotypy conjecture for the sporadic groups and their covers and automorphism groups*, International Journal of Algebra and Computation **25** (2015), 951–976.

[SW] M. Sawabe and A. Watanabe, *On the principal blocks of finite groups with abelian Sylow p-subgroups*, Journal of Algebra **237** (2001), 719–734.

[Spa] B. Späth, *A reduction theorem for the blockwise Alperin weight conjecture*, Journal of Group Theory **16** (2013), 159–220.

[Zas] H. Zassenhaus, *Über endliche Fastkörper*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **11** (1935), 187–220.