ON THE NUMBER OF p'-DEGREE CHARACTERS IN A FINITE GROUP

GUNTER MALLE AND ATTILA MARÓTI

Abstract. Let p be a prime divisor of the order of a finite group G. Then G has at least $2\sqrt{p-1}$ complex irreducible characters of degrees prime to p. In case p is a prime with $\sqrt{p-1}$ an integer this bound is sharp for infinitely many groups G.

1. Introduction

Let p be a prime and G a finite group. Denote the set of complex irreducible characters of G whose degrees are prime to p by $\mathrm{Irr}_{p'}(G)$. The McKay Conjecture states that $|\mathrm{Irr}_{p'}(G)| = |\mathrm{Irr}_{p'}(N_G(P))|$ where $N_G(P)$ is the normalizer of a Sylow p-subgroup P in G. Some known cases (easy consequence of [5, Thm. 1] and a special case of [7]) of this problem together with a recent result of the second author [11] stating that the number of conjugacy classes in a finite group G is at least $2\sqrt{p-1}$ whenever p is a prime divisor of the order of G allows us to prove the following.

Theorem 1.1. *Let G be a finite group and p a prime divisor of the order of G. Then $|\mathrm{Irr}_{p'}(G)| \geq 2\sqrt{p-1}$.*

Our proof of Theorem 1.1 shows that $|\mathrm{Irr}_{p'}(G)|$ is smallest possible for a finite group G whose order is divisible by a prime p if and only if the normalizer of a Sylow p-subgroup of G has a certain special structure. This may be natural in view of the (unsolved) McKay Conjecture. Our second theorem gives a complete description of finite groups G with the property that $|\mathrm{Irr}_{p'}(G)| = 2\sqrt{p-1}$ for a prime divisor p of the order of G, consistent with the McKay conjecture.

Theorem 1.2. *Let G be a finite group, p a prime divisor of the order of G, and P a Sylow p-subgroup of G. Suppose that $\sqrt{p-1}$ is an integer and set H to be the Frobenius group $C_p \rtimes C_{\sqrt{p-1}}$ (whose subgroup of order p is self centralizing). Then $|\mathrm{Irr}_{p'}(G)| = 2\sqrt{p-1}$ if and only if $N_G(P) \cong H$.*

Moreover this happens if and only if $G \cong H$, or $O_{p'}(G) = F(G)$, the subgroup $F(G)P$ is a Frobenius group, and $G/F(G)$ is either isomorphic to H or is an almost simple group A as described below.

(1) $p = 5$ *and* $A = \mathfrak{A}_5$, $\mathfrak{A}_6$, $\mathrm{L}_2(11)$ *or* $\mathrm{L}_3(4)$;
(2) $p = 17$ *and* $A = \mathrm{S}_4(4)$, $\mathrm{O}_8^-(2)$ *or* $\mathrm{L}_2(16).2$;

Date: January 13, 2015.

2010 *Mathematics Subject Classification.* 20C15, 20C33.

Key words and phrases. height zero characters, McKay conjecture, simple groups.

The first author gratefully acknowledges financial support by ERC Advanced Grant 291512. The second author was supported by an Alexander von Humboldt Fellowship for Experienced Researchers and by OTKA K84233.

(3) *$p = 37$ and $A = {}^2G_2(27)$ or $\mathrm{U}_3(11).2$;*
(4) *$p = 257$ and $A = \mathrm{S}_{16}(2)$, $\mathrm{O}_{18}^-(2)$, $\mathrm{L}_2(256).8$, $\mathrm{S}_4(16).4$, $\mathrm{S}_8(4).2$, $\mathrm{O}_8^-(4).4$, $\mathrm{O}_{16}^-(2).2$ or $F_4(4).2$.*

In Proposition 6.3 we show that for any prime p with $\sqrt{p-1}$ an integer there are in fact infinitely many finite solvable groups G with $|\mathrm{Irr}_{p'}(G)| = 2\sqrt{p-1}$. We remark that it is an open problem first posed by Landau whether there are infinitely many primes p with $\sqrt{p-1}$ an integer (see e.g. [13, Sec. 19]).

2. The McKay Conjecture

Let G be a finite group and p a prime. The McKay Conjecture claims that $|\mathrm{Irr}_{p'}(G)| = |\mathrm{Irr}_{p'}(N_G(P))|$ where $N_G(P)$ is the normalizer of a Sylow p-subgroup P in G. Thus if we wish to bound $|\mathrm{Irr}_{p'}(G)|$ and assume the validity of the McKay Conjecture for G and p, then we may assume that the Sylow p-subgroup P is normal in G. In this case we have $|\mathrm{Irr}_{p'}(G)| \geq |\mathrm{Irr}_{p'}(G/\Phi(P))|$ where $\Phi(P)$ is the Frattini subgroup in P, a normal subgroup of G. Since $P/\Phi(P)$ is an elementary abelian normal subgroup in $G/\Phi(P)$ which is also the Sylow p-subgroup of $G/\Phi(P)$, by Clifford theory we have that all complex irreducible characters of $G/\Phi(P)$ have degrees prime to p. But the number of conjugacy classes of $G/\Phi(P)$ is at least $2\sqrt{p-1}$ by [11, Thm. 1.1] with equality if and only if $\sqrt{p-1}$ is an integer and $G/\Phi(P)$ is the Frobenius group $C_p \rtimes C_{\sqrt{p-1}}$ (whose subgroup of order p is self centralizing).

Now let us suppose that the McKay Conjecture is true for a finite group G and a prime p. Then $|\mathrm{Irr}_{p'}(G)| = 2\sqrt{p-1}$ if and only if the same holds in case G contains a normal Sylow p-subgroup P. By the previous paragraph, $|P/\Phi(P)| = p$ so P is cyclic. But then, by Clifford theory once again, all complex irreducible characters of G have degrees prime to p. Finally, by [11, Thm. 1.1], the number of conjugacy classes of G is equal to $2\sqrt{p-1}$ if and only if G is the Frobenius group $C_p \rtimes C_{\sqrt{p-1}}$.

By the previous two paragraphs we showed Theorem 1.1 and the first half of Theorem 1.2 in case the McKay Conjecture is true for the pair G and p. The McKay Conjecture is known to be true, for example, for groups with a cyclic Sylow p-subgroup, by Dade [5, Thm. 1].

3. Reduction

In this section we prove a reduction of Theorem 1.1 and of the first half of Theorem 1.2 to a question on finite non-abelian simple groups.

Let G be a finite group and p a prime dividing the order of G. By the previous section we can assume that the Sylow p-subgroups of G are not cyclic. So we would like to show $|\mathrm{Irr}_{p'}(G)| > 2\sqrt{p-1}$ in all remaining cases.

From the well-known identity $|G| = \sum_{\chi\in\mathrm{Irr}(G)} \chi(1)^2$ we see that $|\mathrm{Irr}_{p'}(G)| > 2\sqrt{p-1}$ is true for $p = 2$ and $p = 3$. So assume from now on that $p \geq 5$.

3.1. **Reduction to the monolithic case.** Let G be a minimal counterexample to the bound, that is, $|\mathrm{Irr}_{p'}(G)| \leq 2\sqrt{p-1}$ and G does not have a cyclic Sylow p-subgroup.

Let N be a minimal normal subgroup in G. Suppose first that $|G/N|$ is divisible by p. Then $|\mathrm{Irr}_{p'}(G)| \geq |\mathrm{Irr}_{p'}(G/N)| \geq 2\sqrt{p-1}$ by the minimality of G. So both inequalities must be equalities. But then G/N has a Sylow p-subgroup of order p and p^2 divides

$$\sum_{\chi \in \mathrm{Irr}(G)\setminus \mathrm{Irr}(G/N)} \chi(1)^2 = |G| - |G/N|.$$

This implies that p^2 cannot divide $|G|$ (only p). But we excluded the case when G has a cyclic Sylow p-subgroup.

So we must have that $|G/N|$ is not divisible by p, whence $|N|$ is divisible by p. Then N is an elementary abelian p-group or is a direct product of simple groups S having order divisible by p. By this argument it also follows that N is the unique minimal normal subgroup of G. If N is abelian then $\mathrm{Irr}_{p'}(G) = \mathrm{Irr}(G)$ by Clifford theory and so we get the result by [11, Thm. 1.1].

Thus $N = S_1 \times \cdots \times S_t$ where all S_i's are isomorphic to a non-abelian simple group S having order divisible by p. Note that G/N permutes the simple factors transitively (but not necessarily faithfully).

3.2. **Reduction to simple groups.** We continue the investigation of a minimal counterexample G as in the previous subsection. If $\psi \in \mathrm{Irr}_{p'}(N)$ then any irreducible character of G lying above ψ has p'-degree by Clifford theory.

We wish to give a lower bound for the number of G/N-orbits on the set $\mathrm{Irr}_{p'}(N)$. For this we may assume that G/N is as large as possible, subject to our conditions. So we may assume that $G = A \wr T$ where $\mathrm{Inn}(S) \leq A \leq \mathrm{Aut}(S)$ is a group for which $|A/\mathrm{Inn}(S)|$ is prime to p and T is a transitive permutation group on t letters with $|T|$ coprime to p (but we may and will take T to be $\mathfrak{S}_t$). Let A_1 be the stabilizer of S_1 in G. Let K_1 be the normal subgroup of A_1 consisting of those elements which induce inner automorphisms on S_1. Then A_1/K_1 can be considered as a p'-subgroup of $\mathrm{Out}(S_1)$. Let k be the number of A_1-orbits on $\mathrm{Irr}_{p'}(S_1)$. Then $|\mathrm{Irr}_{p'}(G)| \geq \binom{k+t-1}{t}$.

Suppose for a moment that $t \geq 2$. Then $|\mathrm{Irr}_{p'}(G)| \geq \binom{k+1}{2} = k(k+1)/2$. We want this to be larger than $2\sqrt{p-1}$. This is certainly true if $k \geq 2(p-1)^{1/4}$. On the other hand for $t = 1$ we have $G = A$ and so we need $|\mathrm{Irr}_{p'}(G)| > 2\sqrt{p-1}$.

Thus Theorem 1.1 and the first part of Theorem 1.2 is a consequence of the following result.

Theorem 3.1. *Let S be a finite non-abelian simple group whose order is divisible by a prime p at least 5. Suppose that S is not isomorphic to a projective special linear group $\mathrm{L}_2(q)$, a Suzuki group ${}^2B_2(q^2)$ or a Ree group ${}^2G_2(q^2)$. Let $X \leq \mathrm{Aut}(S)$ be a group containing $\mathrm{Inn}(S)$ so that $|X/\mathrm{Inn}(S)|$ is not divisible by p. Furthermore let k be the number of X-orbits on $\mathrm{Irr}_{p'}(S)$. Then*

(a) *$k \geq 2(p-1)^{1/4}$; and*
(b) *if the Sylow p-subgroups of X are not cyclic then $|\mathrm{Irr}_{p'}(X)| > 2\sqrt{p-1}$.*

Note that we may exclude the rank 1 groups $\mathrm{L}_2(q)$, ${}^2B_2(q^2)$ and ${}^2G_2(q^2)$ in Theorem 3.1. Indeed, by Theorems A and B and by the comments in between on page 35 of [7], we see that the McKay Conjecture is true for any corresponding G. So we may as well assume that S is different from these groups.

Note that if X is as in Theorem 3.1 then it is sufficient (but not necessary) to show that $|\mathrm{Irr}_{p'}(X)| > 2\sqrt{p-1} \cdot |X/S|$.

4. Alternating and sporadic simple groups

The aim of this section is to prove Theorem 3.1 for alternating and sporadic groups.

4.1. **The case when $S = \mathfrak{A}_n$.** Let us exclude the case $n = 6$ from the discussion below because in this case the full automorphism group of S is not $\mathfrak{S}_n$.

We begin with a result of Macdonald (the following form of which can be found in a paper by Olsson [12]). For a non-negative integer m let $\pi(m)$ denote the number of partitions of m. An m-split of a non-negative integer s is a sequence of non-negative integers $(s_1, \dots, s_m)$ so that $\sum_{i=1}^{m} s_i = s$. Put $k(m, s) = \sum \pi(s_1)\pi(s_2)\cdots\pi(s_m)$ where the sum is over all m-splits of s. (Notice that $k(m, 0) = 1$.) For a prime divisor p of $|\mathfrak{S}_n|$ let the p-adic expansion of the integer n be $a_0 + a_1 p + \cdots + a_r p^r$. Then Macdonald's result states that

$$|\mathrm{Irr}_{p'}(\mathfrak{S}_n)| = k(1, a_0)k(p, a_1)\cdots k(p^r, a_r).$$

Notice that $m \cdot s \le k(m, s)$ for all m and s. This gives $p - 1 \le n - 1 \le |\mathrm{Irr}_{p'}(\mathfrak{S}_n)|$ since the product of integers each at least 2 is always at least their sum. Thus

$$|\mathrm{Irr}_{p'}(\mathfrak{A}_n)| \ge k \ge (n-1)/2 \ge (p-1)/2.$$

A simple calculation shows that this is larger than $2\sqrt{p-1}$ unless $p \le 17$. So we may assume that $5 \le p \le 17$, otherwise we are done. But the same calculation can be applied using n in place of p. So we may also assume that $n \le 17$.

If $a_0 \ge 3$ or if $a_1 \ge 2$ or if $a_i \ge 1$ for some $i \ge 2$, then $|\mathrm{Irr}_{p'}(\mathfrak{S}_n)| \ge 3p$. Using this bound and the calculation referred to in the previous paragraph we get an affirmative answer to the problem. So only the following cases are to be considered.

(1) $n = p = 5$, 7, 11, 13, 17. In this case $|\mathrm{Irr}_{p'}(\mathfrak{S}_n)| = p$.
(2) $n = p + 1 = 8$, 12, 14. In this case $|\mathrm{Irr}_{p'}(\mathfrak{S}_n)| = p$.
(3) $n = p + 2 = 7$, 9, 13, 15. In this case $|\mathrm{Irr}_{p'}(\mathfrak{S}_n)| = 2p$.

For all the above values of n and p still to be considered (even for $n = 6$) we have that a Sylow p-subgroup of X has order p, that is, is cyclic. So we only have to bound k.

In the exceptional cases (1)–(3) above we certainly have $k \ge (p+1)/2$ since p is odd. But then the bound in (a) of Theorem 3.1 holds for $p \ge 5$.

Now suppose that $n = 6$. It is sufficient to show in this case that $k \ge 2(p-1)^{1/4}$ (where p here is 5). Since the complex irreducible character degrees of $\mathfrak{A}_6$ are 1, 5, 5, 8, 8, 9, 10, we certainly have $k \ge 3$. But 3 is larger than our proposed bound.

4.2. **The case when S is sporadic.** For sporadic groups and ${}^2F_4(2)'$ it is straightforward to check the validity of the conditions in Theorem 3.1 from the known character tables in [4].

5. Groups of Lie type

Here, we prove Theorem 3.1 for groups of Lie type. Let $G = \mathbf{G}^F$ be the group of fixed points under a Steinberg endomorphism F of a simple algebraic group $\mathbf{G}$ of adjoint type over an algebraically closed field of characteristic r. Let p be a prime (which may coincide with r) dividing $|G|$. Let S be the simple socle of G.

5.1. **Two easy observations.** As above, G is a finite reductive group of adjoint type.

Lemma 5.1. *Suppose that p does not divide $|G/S|$. Then the claim of Theorem 3.1 holds for (S,p) if $2\sqrt{p-1}\cdot|\mathrm{Out}(S)|_{p'}<|\mathrm{Irr}_{p'}(G)|$.*

Proof. By the condition on G, by Schreier's conjecture, and by Hall's theorem, we may assume that X contains G. Now $2\sqrt{p-1}\cdot|\mathrm{Out}(S)|_{p'}<|\mathrm{Irr}_{p'}(G)|$ implies that $2\sqrt{p-1}\cdot|X/S|<|\mathrm{Irr}_{p'}(G)|$. From this we have

$$2\sqrt{p-1}<\frac{|G|}{|X|}\cdot\frac{|\mathrm{Irr}_{p'}(G)|}{|G:S|}\leq\frac{|G|}{|X|}\cdot\Big(\frac{1}{|G|}\sum_{g\in G}|\mathrm{fix}(g)|\Big)\leq\frac{1}{|X|}\sum_{g\in X}|\mathrm{fix}(g)|=k$$

where $|\mathrm{fix}(g)|$ denotes the number of fixed points of $g\in X$ on $\mathrm{Irr}_{p'}(S)$. □

Here is a further easy sufficient criterion:

Lemma 5.2. *Let S be non-abelian simple. Assume that there is $I\subseteq\mathrm{Irr}_{p'}(S)$ such that all $\chi\in I$ are $\mathrm{Out}(S)$-invariant and extend to $\mathrm{Aut}(S)$. Then the conclusion of Theorem 3.1 holds for (S,p) if one of the following conditions holds:*

(1) *$p<|I|^2/4+1$, or*
(2) *Sylow p-subgroups of $\mathrm{Aut}(S)$ are cyclic and $p\leq|I|^4/16+1$.*

Proof. By assumption $\mathrm{Out}(S)$ has at least $k:=|I|$ orbits on $\mathrm{Irr}_{p'}(S)$. Since all characters of I extend to $\mathrm{Aut}(S)$, any $S\leq X\leq\mathrm{Aut}(S)$ has $|\mathrm{Irr}_{p'}(X)|\geq k$. Now $k=|I|>2(p-1)^{1/2}\geq2(p-1)^{1/4}$, so (S,p) satisfies the condition in Theorem 3.1(b). If Sylow p-subgroups of $\mathrm{Aut}(S)$ are cyclic, we just need $k>2(p-1)^{1/4}$. □

Note that for invariant characters extendibility to $\mathrm{Aut}(S)$ is automatically satisfied if all Sylow subgroups of $\mathrm{Out}(S)$ are cyclic, for example.

5.2. **The defining characteristic case (for rank $l\geq2$).**

Proposition 5.3. *Theorem 3.1 holds for S of Lie type in characteristic p.*

Proof. As before, let $\mathbf{G}$ be a simple linear algebraic group in characteristic p of adjoint type with a Steinberg endomorphism $F:\mathbf{G}\to\mathbf{G}$ and $G:=\mathbf{G}^F$ such that $S=[G,G]$. All finite simple groups of Lie type are of this form (see [10, Prop. 24.21]). We denote by $(\mathbf{G}^*,F^*)$ the dual pair of $(\mathbf{G},F)$ (see [3, Sec. 4.2]). Here $\mathbf{G}^*$ is a simple algebraic group of simply connected type. We denote the corresponding finite group of Lie type by G^*. By [10, Prop. 24.21], we have $G^*/Z(G^*)\cong[G,G]=S$. Since $p\geq5$, we know by [2, Lemma 5] that the set of p'-degree complex irreducible characters of G is precisely the set of semisimple characters of G, whose elements are labelled by representatives of the conjugacy classes of semisimple elements of G^*. Thus $|\mathrm{Irr}_{p'}(G)|=q^l$ where l is the semisimple rank of $\mathbf{G}^*$, and q is the absolute value of all eigenvalues of F on the character group of an F-stable maximal torus of $\mathbf{G}$, by [3, Thm. 3.7.6(ii)].

By Clifford theory we then have

$$q^l=|\mathrm{Irr}_{p'}(G)|\leq|G:S|\cdot t$$

where t is the number of G/S-orbits on $\mathrm{Irr}_{p'}(S)$. By the orbit-counting lemma,

$$q^l\leq|G:S|\cdot t=\sum_{g\in G/S}|\mathrm{fix}(g)|\leq\sum_{g\in\mathrm{Out}(S)}|\mathrm{fix}(g)|\leq k\cdot|\mathrm{Out}(S)|.$$

So we get $q^l/|\mathrm{Out}(S)| \le k$.

In order to prove Theorem 3.1 for (S, p) it is sufficient to see that $q^l/|\mathrm{Out}(S)| > 2\sqrt{p-1}$, where $q = p^f$. Bounds for $|\mathrm{Out}(S)|$ can be read off from [4, Tab. 5]. If $(f, l, p) \neq (1, 2, 5)$ nor $(1, 2, 7)$, then the bound $|\mathrm{Out}(S)| \le (6l + 3)f$ is sufficient for our purposes (note that $l \ge 2$). On the other hand, if $(f, l, p) = (1, 2, 5)$ or $(1, 2, 7)$ then the bounds $|\mathrm{Out}(S)| \le 6$ and $|\mathrm{Out}(S)| \le 8$ are sufficient, respectively. □

5.3. **Exceptional type groups in non-defining characteristic.**

Proposition 5.4. *Let S be a simple exceptional group of Lie type, not of type ${}^2B_2$ or ${}^2G_2$, and $p \ge 5$ a prime dividing $|S|$ but different from the defining characteristic. Then (S, p) satisfies the conclusion of Theorem 3.1.*

Proof. Let G be a finite reductive group of adjoint type with socle S. We first deal with the primes p for which Sylow p-subgroups of G are non-abelian. These necessarily divide the order of the Weyl group W of G, so $p \le 7$, and G is of type ${}^{(2)}E_6$, E_7 or E_8. Furthermore, $p|(q \pm 1)$ if $p = 7$, or if $p = 5$ and G is not of type E_8. It is then straightforward to check (for example from the tables in [3, §13.9]) that G has at least as many unipotent characters of p'-degree as given in Table 1. Since unipotent characters extend to $\mathrm{Aut}(S)$ by [9, Thm. 2.5], the claim follows from Lemma 5.2 in this case.

TABLE 1. Invariant unipotent characters, $p \in \{5, 7\}$

G	${}^{(2)}E_6$	E_7	E_8
$p = 5$	10	30	20
$p = 7$	–	14	28

We may now assume that Sylow p-subgroups of G are abelian. Then there exists a unique cyclotomic polynomial Φ_d dividing the generic order of G and such that $p|\Phi_d(q)$. Moreover, there exists a maximal torus T_d of G containing a Sylow d-torus of G, and so in particular a Sylow p-subgroup of G (see [10, Thm. 25.14]). Let $\Phi_d^{a_d}$ be the precise power of Φ_d dividing the order polynomial of G. The Sylow p-subgroups of G are cyclic if and only if $a_d = 1$. Let W_d be the relative Weyl group of T_d. Then by generalized Harish-Chandra theory (or alternatively from the formulas in [3, §13.9]) there exist at least $|\mathrm{Irr}(W_d)|$ many unipotent characters of G of p'-degree. By [9, Thms. 2.4 and 2.5] all of these extend to $\mathrm{Aut}(S)$ unless G is of type G_2 and $r = 3$, or of type F_4 and $r = 2$. The various W_d and a_d are explicitly known (see e.g. [1, Tables 1 and 3]), and applying Lemma 5.2 we conclude that our claim holds if p is as in Table 2. Here, the left-most half of the table contains the cases with $a_d > 1$, while in the right-most part we have $a_d = 1$, so Sylow p-subgroups are cyclic.

So from now on we suppose that p is larger than the bound given in the table. Let d, T_d, W_d be as above. Let $s \in T_d$ be semisimple. Then s centralizes a Sylow p-subgroup of G, so the semisimple character in the Lusztig series $\mathcal{E}(G, s)$ has degree prime to p by Lusztig's Jordan decomposition (see e.g. [8, Prop. 7.2]). Since fusion of semisimple elements in maximal tori is controlled by the relative Weyl group, there exist at least

TABLE 2. Aut(S)-invariant unipotent characters

G	d	#	p	d	#	p
G_2	$1,2$	6	$p \leq 10$	$3,6$	6	$p \leq 82$
${}^3D_4$	$1,2$	6	$p \leq 10$	12	4	$p \leq 17$
	$3,6$	7	$p \leq 13$			
${}^2F_4$	$1,4,8',8''$	7	$p \leq 13$	$12,24',24''$	12	$p \leq 1297$
F_4	$1,2$	11	$p \leq 31$	$8,12$	≥ 8	$p \leq 257$
	$3,6$	9	$p \leq 21$			
${}^{(2)}E_6$	$1,2,3,4,6$	≥ 16	$p \leq 65$	$5,8,9,12,(10,18)$	≥ 5	$p \leq 40$
E_7	$1,2,3,4,6$	≥ 48	$p \leq 577$	$5,7,8,9,10,12,14,18$	≥ 14	$p \leq 2402$
E_8	$1,2,3,4,6$	≥ 59	$p \leq 871$	$7,9,14,18$	≥ 28	$p \leq 38417$
	$5,8,10,12$	≥ 32	$p \leq 257$	$15,20,24,30$	≥ 20	$p \leq 10001$

$|T_d|/|W_d|$ semisimple conjugacy classes of G with representatives in T_d, whence $|\mathrm{Irr}_{p'}(G)| \geq |T_d|/|W_d|$. We now go through the various types of groups.

Let first $G = S = G_2(q)$ with $q = r^f > 2$ (as $G_2(2) \cong \mathrm{Aut}(\mathrm{U}_3(3))$). Then $\mathrm{Out}(S)$ is cyclic of order f for $r \neq 3$ respectively $2f$ for $r = 3$, and $d \in \{1,2,3,6\}$, with $a_d = 2$ for $d = 1,2$ and $a_d = 1$ else. Table 2 then shows that $q \geq 11$. It is now straightforward to check that $|T_d|/|W_d| > 2\sqrt{p-1}|\mathrm{Out}(S)|$, so the condition in Lemma 5.1 is satisfied in these cases.

Next consider $G = S = {}^3D_4(q)$, $q = r^f$. As before, $\mathrm{Out}(S)$ is cyclic, of order $3f$. Here, we have $d \in \{1,2,3,6,12\}$, with $a_d = 2$ for $d \leq 6$. By Table 2 we may assume that $q \geq 11$. In all cases the estimate above gives the claim. The same arguments also apply to ${}^2F_4(2^{2f+1})$ and $F_4(q)$.

Now assume that $G = E_6(q)$, $q = r^f$. Here the outer automorphism group is of order $2f\gcd(3, q-1)$, but no longer cyclic. We have $d \in \{1,2,3,4,5,6,8,9,12\}$. First assume that Sylow p-subgroups are cyclic, so $d \in \{5,8,9,12\}$. Then $p \geq 41$ by Table 2, and $|W_d| \leq 12$. The standard estimate now applies. For $d \in \{2,3,4,6\}$ we have $67 \leq p \leq q^2+1$, while $|T_d| \geq (q^2-q)^3$ and $|W_d| \leq 1152$, while for $d = 1$ we have $67 \leq p \leq q-1$ and $|T_d| = (q-1)^6$. In all cases we obtain a contradiction to the standard estimate. The case of ${}^2E_6(q)$ can be handled similarly. For $E_7(q)$ the outer automorphism group has order $f\gcd(2, q-1)$, and the same approach as before applies. Finally, let $G = S = E_8(q)$ with $q = r^f$. Then $|\mathrm{Out}(S)| = f$. We now discuss the various possibilities for d. If $d = 1$, so $p|(q-1)$, then W_d is the Weyl group of G, with $|\mathrm{Irr}(W_d)| = 112$. So we are done whenever $2f\sqrt{p-1} < 112$, which certainly is the case for $q \leq 1000$. For $q \geq 1001$ we have

$$\Phi_d(q)^a/|W_d| = (q-1)^8/696729600 > 2\log_p(q)\sqrt{p-1}.$$

The case $d = 2$ is very similar. For $d = 3$ or $d = 6$, $|W_d| = 155\,520$ (see [1, Table 3]) and $|\mathrm{Irr}(W_d)| = 102$. We may conclude as before. Similarly, for $d = 4$ we have $|W_d| = 46080$ and $|\mathrm{Irr}(W_d)| = 59$; for $d = 5$ or $d = 10$ we have $|W_d| = 600$ and $|\mathrm{Irr}(W_d)| = 45$; for $d = 12$ we have $|W_d| = 288$ and $|\mathrm{Irr}(W_d)| = 48$. Finally, for the cases $d \in \{7,14,9,18,15,20,24,30\}$ with cyclic Sylow p-subgroups the estimates are even easier, using the bounds in Table 2. This achieves the proof. □

5.4. **Groups of classical type in non-defining characteristic.**

Proposition 5.5. *Let S be a simple classical group of Lie type and $p \geq 5$ a prime dividing $|S|$ but different from the defining characteristic. Then (S, p) satisfies the conclusion of Theorem 3.1.*

Proof. Let first $G = \mathrm{SO}_{2n+1}(q)$ or $\mathrm{PCSp}_{2n}(q)$ with $q = r^f$ and $n \geq 2$. Here $\mathrm{Out}(S)$ is cyclic of order $f \gcd(2, q-1)$, respectively of order $2f$ if $n = 2$ and q is even. Let d be minimal such that p divides $q^d \pm 1$. A Sylow d-torus T_d of G has order Φ_d^a when $n = ad+s$ with $0 \leq s < d$. The centralizer of T_d in G has a subgroup of the form $(q^d \pm 1)^a G_s(q)$, where G_s has the same type as G and rank s (see [1, §3A]). The relative Weyl group W_d of T_d is the wreath product $C_{2d} \wr \mathfrak{S}_a$.

If Sylow p-subgroups of G are non-abelian, then $p \leq n$ divides $|W_d|$, whence $p \leq a$ as p cannot divide d. Now the number of unipotent characters of p'-degree of G in the principal p-block is at least the number of p'-characters of W_d, hence of its factor group $\mathfrak{S}_a$, hence at least $p-1$, and all of these are $\mathrm{Out}(S)$-invariant by [9, Thm. 2.5], so we are done in this case.

Else, the centralizer of T_d contains a Sylow p-subgroup of G, whence all semisimple elements of the torus of order $(q^d \pm 1)^a$ give rise to semisimple characters of G in $\mathrm{Irr}_{p'}(G)$, and in addition the unipotent characters in the principal p-block of G, of which there are $|\mathrm{Irr}(W_d)|$ many, have degree coprime to p. Thus by Lemma 5.1 if suffices to show that

$$|\mathrm{Irr}(W_d)| + \frac{(q^d-1)^a}{(2d)^a\, a!} > 2f \gcd(2, q-1)\sqrt{p-1}$$

where $p|(q^d \pm 1)$. If $a = 1$ then Sylow p-subgroups of $\mathrm{Aut}(G)$ are cyclic. Otherwise it is easily seen that this inequality always holds.

Next let $G = \mathrm{PCO}_{2n}^{\pm}(q)$ with $q = r^f$ and $n \geq 4$. Here $\mathrm{Out}(S)$ has order $fg \gcd(4, q^n \pm 1)$, where $g = 6$ for $n = 4$ and $g = 2$ else denotes the number of graph automorphisms. Let again d be minimal such that p divides $q^d \pm 1$. The situation is very similar to the one for groups of types B_n and C_n, except that the relative Weyl group W_d sometimes is a subgroup of index two in the wreath product $C_{2d} \wr \mathfrak{S}_a$. Arguing as before we find that there are no cases with $a > 1$ violating the above inequality. For $a = 1$ Sylow p-subgroups of G are cyclic.

Next let $G = \mathrm{PGL}_n(q)$ with $q = r^f$ and $n \geq 3$. Let d be minimal with p dividing $q^d - 1$ and write $n = ad + s$ with $0 \leq s < d$. A Sylow d-torus T_d of G has order Φ_d^a. The centralizer of T_d in G contains a subgroup of the form $(q^d-1)^a G_s(q)$, where G_s is of type A_{s-1}. The relative Weyl group W_d of T_d is the wreath product $C_d \wr \mathfrak{S}_a$.

If Sylow p-subgroups of G are non-abelian, then $p \leq n$ divides $|W_d|$, and so $p \leq a$. Again, the number of unipotent characters of p'-degree of G in the principal p-block is at least the number of p'-characters of W_d, hence of $\mathfrak{S}_a$, hence at least $p-1$. Since all of these are $\mathrm{Out}(S)$-invariant, we are done in this case.

Otherwise we may assume that $a > 1$. Arguing as in the case of the other classical groups, we arrive at the following inequality

$$|\mathrm{Irr}(W_d)| + \frac{(q^d-1)^a}{d^a\, a!} > 2f \gcd(n, q-1)\sqrt{p-1},$$

which turns out to be satisfied for all relevant values.

The case of $G = \mathrm{PGU}_n(q)$ is entirely similar, which $q^d - 1$ replaced by $q^d - (-1)^d$ throughout. The proof is complete. $\square$

6. Proof of Theorem 1.2

In this section we prove Theorem 1.2.

Lemma 6.1. *Let G be a finite group, p a prime divisor of the order of G, and P a Sylow p-subgroup of G. Suppose that $\sqrt{p-1}$ is an integer and set H to be the Frobenius group $C_p \rtimes C_{\sqrt{p-1}}$ (whose subgroup of order p is self centralizing). Then $|\mathrm{Irr}_{p'}(G)| = 2\sqrt{p-1}$ if and only if $N_G(P) \cong H$. Moreover this happens if and only if $G \cong H$, or $O_{p'}(G) = F(G)$, the subgroup $F(G)P$ is a Frobenius group, and $G/F(G)$ is either isomorphic to H or is an almost simple group A with $N_A(F(G)P/F(G)) \cong H$.*

Proof. We have already proved the first statement of the lemma in the preceding sections.

So now suppose that $N_G(P) \cong H$ holds. Then by Theorem 1.1, we have

$$2\sqrt{p-1} \leq |\mathrm{Irr}_{p'}(G/O_{p'}(G))| \leq |\mathrm{Irr}_{p'}(G)| = 2\sqrt{p-1}$$

and so $N_{G/O_{p'}(G)}(Q) \cong H$ for a Sylow p-subgroup Q of $G/O_{p'}(G)$. Since $O_{p'}(G/O_{p'}(G)) = 1$ and $|Q| = p$, we see that either Q is normal in $G/O_{p'}(G)$ and thus $G/O_{p'}(G) \cong H$, or $G/O_{p'}(G)$ is almost simple. Since P is self centralizing in G, it acts fixed point freely on $O_{p'}(G)$ and so $O_{p'}(G)P$ is a Frobenius group. By Thompson's theorem [14, Thm. 5.1'], $O_{p'}(G) \leq F(G)$. The other containment follows from $P \not\leq F(G)$ whenever $G \not\cong H$.

Now consider the other implication of the second statement of the lemma. Assume that $G \not\cong H$. Since $F(G)P$ is a Frobenius group, we have $N_G(P) \cap F(G) = 1$. Furthermore $N_G(P)$ is isomorphic to $N_{G/F(G)}(F(G)P/F(G)) \cong H$. $\square$

To finish the proof of Theorem 1.2, we need to classify almost simple groups A with the property that the normalizer of a Sylow p-subgroup in A is the Frobenius group $C_p \rtimes C_{\sqrt{p-1}}$ (whose subgroup of order p is self centralizing).

Proposition 6.2. *Let A be a finite almost simple group and p a prime. Then the Sylow p-subgroups of A are as described in Lemma 6.1 if and only if A is as in (1)–(4) of Theorem 1.2.*

Proof. Note that the smallest primes $p > 2$ such that $\sqrt{p-1}$ is an integer are given by $5, 17, 37, 101, 197, 257, ...$ Assume that A is a non-abelian almost simple group with socle S and with a Sylow p-subgroup as in Theorem 1.2. For S a sporadic group, it is readily checked from the Atlas [4] that no example arises (only the primes $p = 5, 17, 37$ are relevant). Now let $S = \mathfrak{A}_n$ with $n \geq 5$. Any element of $\mathfrak{S}_n$ is rational, so any element of order p of $\mathfrak{A}_n$ is conjugate to at least $(p-1)/2$ of its powers. But $(p-1)/2 \leq \sqrt{p-1}$ if and only if $p = 5$, and 5-cycles are non-rational only in $\mathfrak{A}_5$ and in $\mathfrak{A}_6$. This occurs in exception (1).

If S is of Lie type in defining characteristic, its Sylow p-subgroups have order p only when $S = \mathrm{L}_2(p)$, in which case the automizer has order $(p-1)/\gcd(p-1, 2)$. Again, only $p = 5$ and $A = \mathrm{L}_2(5) = \mathfrak{A}_5$ arises.

Now assume that S is of Lie type but p is not the defining characteristic. Note that if p divides $|A|$, then it divides $|S|$, unless A contains a coprime field automorphism. But the latter have non-trivial centralizer in S, so indeed we may suppose that p divides

$|S|$. If p divides the order of the Weyl group of S, then p^2 divides $|S|$, so this is not the case. Otherwise Sylow p-subgroups of S are abelian and contained in some maximal torus T of S. In particular this torus must be of prime order p and self-centralizing. Let $m := |N_A(T)/T|$, then moreover $m^2 + 1 = |T| = p$. So in particular m has to be even. First assume that S is of exceptional Lie type. It is easily seen that under the above restrictions the only example is ${}^2G_2(27)$ with $p = 37$ as in (3), or $F_4(4).2$ with $p = 257$ as in (4). For example, for $A = E_8(q)$, $q = r^f$, the only possible values for m are $m = 15u, 20u, 24u, 30u$ where $u|f$, while $|T| \geq q^8 - q^7 + q^5 - q^4 + q^3 - q + 1$ for cyclic maximal tori, which clearly gives no example.

Finally we handle the case that A is of classical Lie type. If A is of type $B_n(q)$ or $C_n(q)$ with $n \geq 2$ the only cyclic self-centralizing tori have order $(q^n \pm 1)/\gcd(2, q-1)$ and automizer of order $2nf$, where $q = r^f$. But $(q^n \pm 1)/\gcd(2, q-1) = (2n)^2 + 1$ only has the solutions given in cases (2) and (4). For A of type $D_n(q)$ with $n \geq 4$ the cyclic self-centralizing tori are of order $(q^n - 1)/\gcd(4, q^n - 1)$ with automizer of order n, and of order $q^{n-1} - 1$ with $q = 2$ with automizer of order $2(n-1)$. These do not lead to examples. For groups of type ${}^2D_n(q)$ the cyclic self-centralizing tori are of order $(q^n + 1)/\gcd(2, q^n + 1)$ with automizer of order n, and of order $q^{n-1} + 1$ with $q = 2$ with automizer of order $2(n-1)$. The only examples here are those in (2) and (4).

Now assume that $S = \mathrm{L}_n(q)$ with $n \geq 2$. Here, cyclic self-centralizing tori have orders $(q^n-1)/(q-1)/d$ with automizer of order n, and $(q^{n-1}-1)/d$ with automizer of order $n-1$, where $d := \gcd(n, q-1)$. This leads to $\mathrm{L}_2(4) \cong \mathfrak{A}_5$, $\mathrm{L}_2(9) \cong \mathfrak{A}_6$, $\mathrm{L}_2(11)$, $\mathrm{L}_3(4)$, $\mathrm{L}_2(16).2$ and $\mathrm{L}_2(256).8$. Finally, for unitary groups $S = \mathrm{U}_n(q)$ with $n \geq 3$, cyclic self-centralizing tori have orders $(q^n-(-1)^n)/(q+1)/d$ with automizer of order n, and $(q^{n-1}-(-1)^{n-1})/d$ with automizer of order $n-1$, where $d := \gcd(n, q+1)$. This gives $(A, p) = (\mathrm{U}_3(11).2, 37)$ as the only example. □

Finally we prove the last statement of the Introduction.

Proposition 6.3. *For any prime p with $\sqrt{p-1}$ an integer there are infinitely many finite solvable groups G with $|\mathrm{Irr}_{p'}(G)| = 2\sqrt{p-1}$.*

Proof. By Dirichlet's theorem on arithmetic progressions there are infinitely many primes r of the form $pn + 1$ where n is an integer. Pick such an r and set $m := \sqrt{p-1}$. Let V be an m-dimensional vector space over the field with r elements. Then $\Gamma\mathrm{L}(V)$ contains a subgroup $\Gamma\mathrm{L}_1(r^m) \cong C_{r^m-1} \rtimes C_m$. Since p divides $r^m - 1$, this former group contains a (unique) subgroup A of the form $C_p \rtimes C_m$. We claim that $C_A(P) = P$ where P is the Sylow p-subgroup of A. Let x be a generator of P and let y be a generator of a cyclic subgroup of order m in A so that $x^y = x^r$. We have to show that whenever s is an integer with $1 \leq s < m$, then $x^{r^s} \neq x$. But this is clear since $r^m - 1$ does not divide $r^s - 1$.

Now set $G = V \rtimes A$. Then $O_{p'}(G) = F(G) = V$, VP is a Frobenius group, and $G/V = A$ is a Frobenius group of the form $C_p \rtimes C_m$. Now apply Lemma 6.1. □

References

[1] M. Broué, G. Malle, J. Michel, Generic blocks of finite reductive groups. Astérisque No. 212 (1993), 7–92.

[2] O. Brunat, On the inductive McKay condition in the defining characteristic. Math. Z. **263** (2009), 411–424.

[3] R. Carter, *Finite Groups of Lie type: Conjugacy Classes and Complex Characters.* Wiley, Chichester, 1985.
[4] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, *Atlas of Finite Groups.* Clarendon Press, Oxford, 1985.
[5] E. C. Dade, Blocks with cyclic defect groups. Ann. of Math. (2) **84** (1966), 20–48.
[6] I. M. Isaacs, *Character Theory of Finite Groups.* Dover Publications, New York, 1994.
[7] I. M. Isaacs, G. Malle, G. Navarro, A reduction theorem for the McKay conjecture. Invent. Math. **170** (2007), 33–101.
[8] G. Malle, Height 0 characters of finite groups of Lie type. Represent. Theory **11** (2007), 192–220.
[9] G. Malle, Extensions of unipotent characters and the inductive McKay condition. J. Algebra **320** (2008), 2963–2980.
[10] G. Malle, D. Testerman, *Linear Algebraic Groups and Finite Groups of Lie Type.* Cambridge Studies in Advanced Mathematics, 133, Cambridge University Press, Cambridge, 2011.
[11] A. Maróti, A lower bound for the number of conjugacy classes of a finite group. arXiv:1411.0454, 2014.
[12] J. B. Olsson, McKay numbers and heights of characters. Math. Scand. **38** (1976), 25–42.
[13] J. Pintz, Landau's problems on primes. J. Théor. Nombres Bordeaux **21** (2009), 357–404.
[14] H. Wielandt, *Finite Permutation Groups.* Academic Press, New York-London, 1964.

FB Mathematik, TU Kaiserslautern, Postfach 3049, 67653 Kaiserslautern, Germany.
E-mail address: malle@mathematik.uni-kl.de
E-mail address: maroti@mathematik.uni-kl.de