ZEROS OF CHARACTERS OF FINITE GROUPS

Gunter Malle, Gabriel Navarro and Jørn B. Olsson

Universität Kassel, Universitat de València, University of Copenhagen

1. Introduction

Let G be a finite group and let $\chi \in \mathrm{Irr}(G)$ be an irreducible complex character of G. W. Burnside proved that if χ is nonlinear, then there exists $g \in G$ such that $\chi(g) = 0$.

Theorem A. *Let G be a finite group and let $\chi \in \mathrm{Irr}(G)$ be nonlinear. If $\chi(1)$ is a π-number, then there exists a π-element $g \in G$ such that $\chi(g) = 0$.*

In the special case when $\chi(1)$ is a power of a prime p, we will prove that χ vanishes on some p-element of G by using some elementary argument. To prove the general result, however, we will need the Classification of Finite Simple Groups.

What we really prove in this paper is the following stronger result.

Theorem B. *Let G be a finite group and let $\chi \in \mathrm{Irr}(G)$ be nonlinear. Then there exists $g \in G$ of prime power order such that $\chi(g) = 0$.*

Since characters of degree not divisible by some prime number p never vanish on p-elements, it is then clear that Theorem B implies Theorem A.

There are some variations of theorems A and B which are simply not true. For instance, if χ in $\mathrm{Irr}(G)$ has degree divisible by p, then there does not necessarily exist a p-element on which χ vanishes. It is enough to consider $\mathrm{L}_2(11)$ with any character of degree 10 and $p = 2$. It is also not true that if χ vanishes on some element x, then χ has to vanish on some p-part of x. For instance, if G is M_{11}, then χ has an irreducible character of degree 11, vanishing on an element of order 6 and which is nonzero on 2- and 3-elements. Thirdly, it is not true that a nonlinear character has to vanish on some element of prime order, as shown by any quaternion group. Interestingly enough, this seems to be the case for simple groups (and we do prove this for the groups of Lie type and the sporadic groups).

Part of this work was done while the authors were visiting the Mathematisches Forschungsinstitut Oberwolfach. We would like to thank the Institute for its hospitality.

2. The case where $\chi(1)$ is a prime power

We start with an elementary lemma.

(2.1) Lemma. *Let $\chi \in \mathrm{Irr}(G)$ and let $Z \leq \mathbf{Z}(G)$ such that $\chi|_Z = \chi(1)\lambda$ for a faithful character $\lambda \in \mathrm{Irr}(Z)$. Then $\chi(x) = 0$ for all $x \in G$ with $\mathbf{C}_G(x)/Z \neq \mathbf{C}_{G/Z}(xZ)$.*

Proof. Let $y \in \mathbf{C}_{G/Z}(xZ) \setminus \mathbf{C}_G(x)/Z$ and write $z := [x, y]$ so that $xz = x^y$. Then $1 \neq z \in Z$ and hence

$$\chi(x) = \chi(x^y) = \chi(xz) = \chi(x)\lambda(z)\,.$$

Since $\lambda(z) \neq 1$, the result follows. □

For inductive purposes we will need the following statement:

(2.2) Lemma. *Assume that $\chi \in \mathrm{Irr}(G)$ vanishes on some p-element of $G/\ker\chi$. Then χ vanishes on some p-element of G.*

Proof. Let $K = \ker\chi > 1$ and $xK \in G/K$ a p-element such that $\chi(xK) = 0$. In this case, we have that $xK = x_pK$,

$$\chi(x_p) = \chi(x_pK) = \chi(xK) = 0$$

and the result follows.

(2.3) Theorem. *Let $\chi \in \mathrm{Irr}(G)$ with $\chi(1) > 1$. If $\chi(1)$ is a power of a prime number p, then $\chi(x) = 0$ for some p-element x of G.*

Proof. We argue by induction on $|G|$. We may assume that $\ker\chi = 1$ for otherwise the theorem follows by induction from Lemma (2.2).

Let $Z = \mathbf{Z}(G)$ and write

$$\chi|_Z = \chi(1)\lambda\,,$$

where $\lambda \in \mathrm{Irr}(Z)$ is faithful.

If G/Z is a p'-group, then $\chi(1) = 1$ since $\chi(1)$ divides $|G : Z|$ by Ito's theorem (Theorem (6.15) of [5]). This contradiction shows that $|G/Z|_p > 1$.

Let $Z \neq xZ \in \mathbf{Z}(PZ/Z)$, where x is a p-element and P is a Sylow p-subgroup of G. Let $H/Z = \mathbf{C}_{G/Z}(xZ)$; then it follows by Lemma (2.1) that $H = \mathbf{C}_G(x)$. Since $|G : H|$ is prime to p we conclude that

$$(\chi(1), |G : \mathbf{C}_G(x)|) = 1\,.$$

By Burnside's theorem (Theorem (3.8) of [5]), we deduce that $\chi(x) = 0$ or $|\chi(x)| = \chi(1)$. In the latter case, since χ is faithful we will have that $x \in \mathbf{Z}(G)$ (by Lemma (2.27) of [5]) and this is not possible. Hence, we have that $\chi(x) = 0$, proving the theorem. □

3. Reducing to simple groups

To reduce Theorem B to a question on finite simple groups, we will need the following two results (which also depend on the Classification). We state them for the reader's convenience.

(3.1) Theorem (B. Fein, W. M. Kantor, M. Schacher). *Suppose that $H < G$. Then there exists an element $x \in G$ of prime power order such that x lies in no G-conjugate of H.*

Proof. See [3]. $\square$

(3.2) Theorem (H. Blau). *Assume that G is a quasisimple group and let $z \in \mathbf{Z}(G)$. Then one of the following holds:*

(i) $\mathrm{order}(z) = 6$ *and* $G/\mathbf{Z}(G) \cong \mathfrak{A}_6, \mathfrak{A}_7, \mathrm{Fi}_{22}, \mathrm{U}_6(2)$, *or* ${}^2E_6(2)$*;*
(ii) $\mathrm{order}(z) = 6$ *or* 12 *and* $G/\mathbf{Z}(G) \cong \mathrm{L}_3(4), \mathrm{U}_4(3)$ *or* M_{22}*;*
(iii) $\mathrm{order}(z) = 2$ *or* 4*,* $G/\mathbf{Z}(G) \cong \mathrm{L}_3(4)$*, and* $\mathbf{Z}(G)$ *is noncyclic;*
(iv) z *is a commutator.*

Proof. See [1]. $\square$

(3.3) Theorem. *Theorem B is true if it holds for the non-abelian finite simple groups.*

Proof. Let G be a minimal counterexample to Theorem B. We prove that G is a nonabelian simple group.

Write $Z = \mathbf{Z}(G)$ and $\chi_Z = \chi(1)\lambda$, where $\lambda \in \mathrm{Irr}(Z)$.

Step 1. *The character χ is primitive.*

Suppose that $\gamma^G = \chi$, where $\gamma \in \mathrm{Irr}(H)$ and $H < G$. By the Theorem (3.1), there exists an element $x \in G$ of prime power order lying in no G-conjugate of H. Then

$$\chi(x) = \gamma^G(x) = 0$$

by the character induction formula.

Step 2. *The character χ is faithful. Hence, every abelian normal subgroup of G is cyclic and central.*

The first assertion is Lemma (2.2), and then the second part follows from Lemma (2.27) and Corollary (6.13) of [5].

Step 3. *The group G/Z is simple nonabelian. Furthermore, Z contains every normal subgroup of G.*

Let $N \triangleleft G$ and let $\theta \in \mathrm{Irr}(N)$ be an irreducible constituent of χ_N. By the Clifford correspondence (Theorem (6.11) of [5]), we will have that χ is induced from some irreducible character of T, where T is the stabilizer of θ in G. By Step 1, we deduce that θ is G-invariant. Then $\chi_N = e\theta$ for some integer e, by Clifford's theorem. Now, if $\theta(1) > 1$, since the zeros of θ are zeros of χ, the theorem would be true for χ. So we may assume that $\theta(1) = 1$. Hence

$$N' \subseteq \ker\theta \subseteq \ker\chi = 1$$

and we deduce that $N \subseteq Z$ by Step 2. Hence G/Z is simple. If G is solvable, we conclude that G is abelian and we are done.

Step 4. *We have that*

$$\mathbf{C}_{G/Z}(gZ) = \mathbf{C}_G(g)/Z$$

for every $g \in G$.

Let $g \in G$. Write $H/Z = \mathbf{C}_{G/Z}(gZ)$. We have that $\mathbf{C}_G(g)/Z \subseteq H/Z$ and we want equality. If $g \in Z$, there is nothing to prove. So we may assume that $g \in G \setminus Z$. Suppose that $\mathbf{C}_G(g) < H$. Then there exists a Sylow p-subgroup of H which is not contained in $\mathbf{C}_G(g)$. Hence, there exists a p-element $x \in H \setminus \mathbf{C}_G(g)$, and $\chi(x) = 0$ by Lemma (2.1).

Step 5. *G is a simple group.*

If $1 \neq z \in Z$, we claim that z is not a commutator. Otherwise, $z = x^{-1}y^{-1}xy$ and we deduce that $xZ \in \mathbf{C}_{G/Z}(yZ)$. Hence $y \in \mathbf{C}_G(x)$ and $z = 1$, a contradiction.

Now, we use Theorem (3.2). Assume that $Z > 1$ and let $1 \neq z \in Z$. Since z is not a commutator, we should be in cases (i), (ii) or (iii) of Theorem (3.2). Also, since Z is cyclic (by Step 2), we may rule out the case (iii). Hence, by Theorem (3.2), there exists $y \in \langle z \rangle$ of order 3. Now, y is not a commutator and by applying Theorem (3.2) to y, we get a contradiction. $\square$

For the 26 sporadic simple groups, the Atlas [2] allows to easily verify the following:

(3.4) Theorem. *Let G be a sporadic simple group. Then there exist four conjugacy classes of elements of prime order in G such that every non-trivial irreducible character of G vanishes on at least one of them.*

Here, four cannot be replaced by three since in the Thompson group Th there do not exist three conjugacy classes of prime power elements such that any nontrivial character vanishes on at least one of them.

We will consider the validity of the principal results for the remaining two families of non-abelian simple groups, that is, the alternating groups, and the simple groups of Lie type, in the next two sections.

4. Alternating groups

The irreducible characters χ_λ of the symmetric group of degree n are labelled by the partitions λ of n.

If p is a prime number let

$$n = a_0 + a_1 p + \cdots + a_k p^k$$

be the p-adic decomposition of n, $(0 \leq a_i \leq p-1, a_k \neq 0)$. We let $\pi_{np} \in \mathfrak{S}_n$ be an element, which is a product of a_1 p-cycles with a_2 p^2-cycles $\cdots$ and a_k p^k-cycles. We prove

(4.1) Theorem. *If $p|\chi_\lambda(1)$ then $\chi_\lambda(\pi_{np}) = 0$.*

(4.2) Theorem. *Let ρ be a nonlinear irreducible character of the alternating group $\mathfrak{A}_n$. Then there exists a prime p and a p-element $g \in \mathfrak{A}_n$ such that $\rho(g) = 0$.*

Remark. If ρ is as in Theorem (4.2) and $p|\rho(1)$ then we show in fact that $\rho(\pi_{np}) = 0$ whenever $\pi_{np} \in \mathfrak{A}_n$. This is always the case when p is odd. When $p = 2$, π_{np} need not be in $\mathfrak{A}_n$. This happens for instance when n is a power of 2. It is not known whether ρ will necessarily vanish on some 2-element in this case.

The proof of Theorem (4.2) depends on Theorem (4.1) with an additional argument for $p = 2$. The essential ingredient in the proof of Theorem (4.1) is a new combinatorial result (Proposition (4.5)) about the connection between certain p-invariants of a partition. We also need a combinatorial description of the power of p dividing $\chi_\lambda(1)$, essentially due to Macdonald [9].

Remark. It is an easy consequence of the Murnaghan-Nakayama formula ([6], 2.4.7), that any non-linear character of $\mathfrak{S}_n$ vanishes on either an n-cycle or on an $(n-1)$-cycle and thus the corresponding conjugacy classes are *strongly orthogonal* as defined in the next section. Most likely it is also true, that any nonlinear character of $\mathfrak{A}_n$ vanishes on some element of prime order, but the method used here is not sufficient to prove this.

For the following calculations *p need not be a prime.* To each partition λ of n is associated a *p-core* $C_p(\lambda)$ and a *p-quotient* $Q_p(\lambda) = (\lambda_0, \cdots, \lambda_{p-1})$. See [6], [14]. The p-core is a partition without p-hooks obtained by removing a sequence of p-hooks from λ. The p-quotient is a p-tuple of partitions. We may recover λ from $C_p(\lambda)$ and $Q_p(\lambda)$. The following important fact is needed:

(4.3) Lemma. *Let $H_p(\lambda)$ be the (multi-)set of hooks of λ of length divisible by p. (Thus $H_1(\lambda) =: H(\lambda)$ is the set of all hooks of λ). There is a canonical bijection between $H_p(\lambda)$ and $\dot{\bigcup}_{t=0}^{p-1} H(\lambda_t)$ such that a hook of length ℓp is mapped onto a hook of length ℓ. This bijection is compatible with hook removals.*

Proof. See for example Theorem (3.3) in [14]. $\square$

If $Q_p(\lambda) = (\lambda_0, \cdots, \lambda_{p-1})$ we call

$$w_p(\lambda) = |\lambda_0| + \cdots + |\lambda_{p-1}|$$

the *p-weight* of λ. Then Lemma (4.3) implies that

$$|H_p(\lambda)| = w_p(\lambda) \tag{1}$$

and the compatibility of hook removals implies

(4.4) Lemma. *If μ is obtained from λ by removing an ℓp-hook then*

$$w_p(\mu) = w_p(\lambda) - \ell\ .$$

In particular, $w_p(\lambda)$ is the maximal number of p-hooks which may subsequently be removed from λ.

We have generally

$$n = |\lambda| = |C_p(\lambda)| + pw_p(\lambda)\ . \tag{2}$$

As described in [13], [14] we may repeat the process of taking cores and quotients to obtain the *p-core tower* of λ. It has rows numbered by $i = 0, 1, 2, \cdots$. The i'th row contains p^i p-cores. The 0'th row is $C_p(\lambda)$, the p-core of λ. If $Q_p(\lambda) = (\lambda_0, \cdots, \lambda_{p-1})$ then the 1st row is $C_p(\lambda_0), \cdots, C_p(\lambda_{p-1})$. The 2nd row contains the p-cores of the partitions occurring in $Q_p(\lambda_0), \cdots, Q_p(\lambda_{p-1})$, and so on. A partition may be recovered from its p-core tower. We let $\alpha_i(\lambda)$ be the sum of the cardinalities of the partitions in the ith row of the p-core tower. By iteration of (2) we get

$$n = \sum_{i\geq 0} \alpha_i(\lambda)p^i\ . \tag{3}$$

We need also the integers $v_i(\lambda)$ defined by

$$v_i(\lambda) = w_{p^i}(\lambda)\ ,$$

the p^i-weight of λ, so that $v_0(\lambda) = |\lambda| = n$, $v_1(\lambda)$ is the p-weight of λ and so on. The relation between the $\alpha_i(\lambda)$'s and $v_i(\lambda)$'s is given by

(4.5) Proposition. *For $j \geq 0$*

(i) $v_j(\lambda) = \sum_{i\geq j} \alpha_i(\lambda)p^{i-j}$

and

(ii) $\alpha_j(\lambda) = v_j(\lambda) - pv_{j+1}(\lambda)$.

Proof. It is clear that (ii) is a consequence of (i). We prove (i) by induction on $j \geq 0$. For $j = 0$ (i) is just the formula (3) above. Assume $j > 0$.

Let $Q_p(\lambda) = (\lambda_0, \lambda_1, \cdots, \lambda_{p-1})$. From the definition of the p-core tower it is clear that for all $j \geq 1$

$$\alpha_j(\lambda) = \sum_{t=0}^{p-1} \alpha_{j-1}(\lambda_t)\ .$$

Moreover the bijection of Lemma (4.3) between $H_p(\lambda)$ and $\bigcup_{t=0}^{p-1} H(\lambda_t)$ shows that for all $j \geq 1$

$$v_j(\lambda) = \sum_{t=0}^{p-1} v_{j-1}(\lambda_t)\ .$$

If we apply the induction hypothesis to each λ_t we get

$$v_{j-1}(\lambda_t) = \sum_{i'\geq j-1} \alpha_{i'}(\lambda_t)p^{i'-j+1}\ .$$

Summing over t we get in view of the above equations

$$v_j(\lambda) = \sum_{i' \geq j-1} \alpha_{i'+1}(\lambda) p^{i'-j+1}$$

and if we substitute $i' = i - 1$ we get

$$v_j(\lambda) = \sum_{i \geq j} \alpha_i(\lambda) p^{i-j} ,$$

as desired. □

(4.6) Proposition. *Let $n = \sum_{i=0}^{k} a_i p^i$ be the p-adic decomposition of n, $a_k \neq 0$. Consider the decomposition of n according to the p-core tower of λ*

$$n = \sum_{i=0}^{k} \alpha_i(\lambda) p^i .$$

(i) If $\alpha_k(\lambda) \neq a_k$ then it is not possible to remove subsequently a_k hooks of length p^k from λ.

(ii) If $\alpha_k(\lambda) = a_k$ then it is possible to subsequently remove a_k hooks of length p^k from λ. The resulting partition μ is unique and satisfies $\alpha_i(\mu) = \alpha_i(\lambda)$ for $1 \leq i \leq k-1$ and $\alpha_k(\mu) = 0$.

Proof. Since $p^{k+1} > n$ we have $v_{k+1}(\lambda) = 0$. Hence by Lemma (4.5) (ii) $\alpha_k(\lambda) = v_k(\lambda)$.

(i) If $\alpha_k(\lambda) \neq a_k$ then in fact $\alpha_k(\lambda) < a_k$ since otherwise

$$\begin{aligned}(\alpha_k(\lambda) - a_k)p^k \geq p^k &> (p-1)p^{k-1} + (p-1)p^{k-2} + \cdots + (p-1) \\ &\geq a_{k-1}p^{k-1} + a_{k-2}p^{k-2} + \cdots + a_0\end{aligned}$$

or

$$\alpha_k(\lambda) p^k > n = \sum_{i=0}^{k} a_i p^i .$$

Thus the p^k-weight $v_k(\lambda)$ of λ is strictly less than a_k, so (i) follows from Lemma (4.4).

(ii) If $\alpha_k(\lambda) = a_k$, then a_k is the exact p^k-weight of λ, whence $\mu = C_{p^k}(\lambda)$ is the p^k-core of λ. We use Lemma (4.4) (with appropriate values for p and ℓ in that lemma) to get

$$\begin{aligned}v_k(\mu) &= v_k(\lambda) - v_k(\lambda) = 0 \\ v_{k-1}(\mu) &= v_{k-1}(\lambda) - p v_k(\lambda) \\ v_{k-2}(\mu) &= v_{k-2}(\lambda) - p^2 v_k(\lambda)\end{aligned}$$

etc.

For $1 \leq i \leq k-1$ we get from Proposition (4.5) (ii) that

$$\begin{aligned}\alpha_i(\mu) &= v_i(\mu) - pv_{i+1}(\mu)\\ &= v_i(\lambda) - p^{k-i}v_k(\lambda) - pv_{i+1}(\lambda) + p\cdot p^{k-i-1}v_k(\lambda)\\ &= v_i(\lambda) - pv_{i+1}(\lambda)\\ &= \alpha_i(\lambda)\ ,\end{aligned}$$

as desired. □

Proof of Theorem (4.1). We are now assuming that p is a prime. Let λ be a partition of n and let the integers a_i and $\alpha_i(\lambda)$ be as above. By Proposition (6.4) in [14] (see also [9], [13]), the exponent to which p divides $\chi_\lambda(1)$ is

$$\left(\sum_{i=1}^{k}\alpha_i(\lambda) - \sum_{i=1}^{k} a_i\right)\Big/(p-1)\ .$$

Thus if $p|\chi_\lambda(1)$, then this number is nonzero.

Assume that j is the maximal number, $0 \leq j \leq k$ such that $\alpha_j(\lambda) \neq a_j$. Note that $j \neq 0$: If $\alpha_i(\lambda) = a_i$ for all $i \geq 1$ then also $\alpha_0(\lambda) = a_0$. By repeated use of Proposition (4.6) (ii) we see that it is possible to remove a_k cycles of length p^k from λ followed by a_{k-1} cycles of length p^{k-1} ... followed by a_{j+1} cycles of length p^{j+1}. The resulting partition μ satisfies

$$\alpha_i(\mu) = \alpha_i(\lambda) \quad \text{for} \quad 1 \leq i \leq j\ .$$

By Proposition (4.6) (i) it is not possible to remove $\alpha_j(\lambda) = \alpha_j(\mu)$ cycles of length p^j from μ.

Assume now that $\chi_\lambda(\pi_{np}) \neq 0$. Then by repeated use of the Murnaghan-Nakayama formula for the character values of $\mathfrak{S}_n$ ([6], 2.4.7) it should be possible to remove a_k cycles of length p^k-cycles from λ followed by a_{k-1} cycles of length p^{k-1} ... followed by a_1 cycles of length p. But this contradicts the above. Thus $\chi_\lambda(\pi_{np}) = 0$. □

Proof of Theorem (4.2). We need the description of the irreducible character values in $\mathfrak{A}_n$, as given in [6], Section 2.5. The character χ_λ of $\mathfrak{S}_n$ remains irreducible when restricted to $\mathfrak{A}_n$ exactly when the partition λ is different from its associate partition. This means that the Young diagram of λ is non-symmetric.

Suppose that p is odd. Then $\pi_{np} \in \mathfrak{A}_n$. Moreover if ρ_λ is a constituent of $\chi_\lambda|_{\mathfrak{A}_n}$ then $p|\chi_\lambda(1)$ if and only if $p|\rho_\lambda(1)$. By [6], Theorem, 2.5.13 and Theorem (4.1) $\rho_\lambda(\pi_{np}) = 0$ *except* in the case where λ is self-associate and the cycle lengths of π_{np} are exactly the diagonal hooklengths of λ. Thus

$$n = p^{d_1} + p^{d_2} + \cdots + p^{d_t}$$

is a sum of different powers of p, say $d_1 > \cdots > d_t \geq 0$, where p^{d_i}, $i = 1, \cdots, t$ are the diagonal hooklengths of λ. By repeated use of Proposition (4.5) (ii) we see that

$$\alpha_j(\lambda) = \begin{cases} 1 & \text{if} \quad j = d_i \quad \text{for some } i\\ 0 & \text{otherwise}\ .\end{cases}$$

From Proposition (6.4) in [14] we conclude that $p \nmid \chi_\lambda(1)$, a contradiction.

For $p = 2$ the problem arises that π_{np} may not be an element of $\mathfrak{A}_n$. (This occurs if the even part of n is a sum of an odd number of different powers of 2). If $\pi_{n2} \in \mathfrak{A}_n$, then the argument for p odd also works for $p = 2$. Indeed, if $2|\rho_\lambda(1)$ then $2|\chi_\lambda(1)$, whence $\chi_\lambda(\pi_{n2}) = 0$. But $\rho_\lambda(\pi_{n2}) = \delta\, \chi_\lambda(\pi_{n2})$, where $\delta = \frac{1}{2}$ or 1 according to whether λ is self-associate or not.

It is not clear at the moment how the argument should be modified when $\pi_{n2} \notin \mathfrak{A}_n$. But in any case the following argument may be used:

Suppose $2|\rho_\lambda(1)$. If $\rho_\lambda(1)$ is a power of 2 then ρ_λ vanishes on a 2-element by Theorem (2.3). Otherwise some prime $r \neq 2$ divides $\rho_\lambda(1)$ and then $\rho_\lambda(\pi_{nr}) = 0$. $\square$

5. Groups of Lie type

In order to prove Theorem B for simple groups of Lie type we will use Lusztig's classification of the irreducible complex characters of these groups (see [8]). In fact our methods allow to prove a result which is stronger in two aspects:

1) we are able to choose elements of prime order,
2) the number of elements can be bounded above (four elements suffice).

Thus we will show:

(5.1) Theorem. *Let G be a finite simple group of Lie type. Then there exist four conjugacy classes of elements of prime order in G such that every non-trivial irreducible character of G vanishes on at least one of them.*

The proof will be given in the subsequent sections. By going through these proofs it is possible to recover the right choice for the four classes in each group.

The assertion about prime order already fails for covering groups of simple groups: $\mathrm{SL}_2(5)$ has faithful irreducible characters which only vanish on an element of order 4. As for the number of classes, we shall prove in many cases that three elements suffice. It is clear that for any given two conjugacy classes of G, there will always be at least two irreducible characters taking nonzero values on both of them. Thus a result with three classes would be optimal.

The underlying reason why Theorem 5.1 (and the related results in [12, 7, 11]) holds and can be proved is that, in a sense, most characters of groups of Lie type are of defect zero for most primes dividing the group order.

This statement can be made more precise as follows. By the results of Lusztig, for any given series $\{G(q) \mid q \text{ a prime power}\}$ of groups of Lie type the proportion of irreducible characters which are not irreducible Deligne-Lusztig characters $\pm R_{T,\theta}$ tends to zero like c/q for some constant c depending only on the type of G. But $\pm R_{T,\theta}$ is of defect zero for any prime not dividing the order of the torus T (and different from the defining characteristic). Since $|T|$ is very small compared to $|G|$, this gives a concrete form to our above claim.

If there exist two maximal tori T_1, T_2 of G of coprime order, then the above considerations imply that asymptotically all but c/q of the irreducible of G vanish on regular elements of at least one of the two tori. In fact, we will show in many cases that then the corresponding classes are strongly orthogonal. Here we say that a pair of conjugacy classes C_1, C_2 of a finite group G is *strongly orthogonal* if all but two irreducible complex characters of G vanish either on C_1 or on C_2.

The existence of pairs of strongly orthogonal classes for simple groups of Lie type was already established in [12] and [7], but unfortunately the classes given there cannot always be chosen to contain elements of prime power order.

5.1 The strategy.

We introduce the following notation. The n-th cyclotomic polynomial over $\mathbb{Q}$ is denoted by $\Phi_n(x)$. For fixed q we denote by $l(n)$ a Zsigmondy prime divisor of $\Phi_n(q)$. By Zsigmondy's theorem (see [4], IX, Theorem 8.3) $l(n)$ exists whenever $n \geq 3$, $(n,q) \neq (6,2)$, or $n=2$ and $q+1$ is not a power of 2

Let $\tilde{G}$ be the group of fixed points under a Frobenius morphism of a simple algebraic group of simply-connected type over the algebraic closure of a finite field. Thus we have $\tilde{G} = \tilde{G}(q)$ for some prime power $q = p^f$. We let $G = \tilde{G}/\mathbf{Z}(\tilde{G})$. Then any finite simple group of Lie type occurs among the groups G, except for the Tits group ${}^2F_4(2)'$.

Our strategy for the proof of Theorem 5.1 is as follows. For each of the sixteen families of groups of Lie type, we choose two or three maximal tori T_i such that the Sylow ℓ_i-subgroups of G are cyclic for suitable Zsigmondy prime divisors ℓ_i of $|T_i|$. It then follows that all elements of order ℓ_i of G are regular. Then we apply Lusztig's classification of the irreducible complex characters of G to prove that only few irreducible characters do not vanish on regular elements of all T_i, and all of these are unipotent characters. This was basically already done in [12,7,11]. We then show that the remaining nontrivial unipotent characters different from the Steinberg character are of defect zero for some other suitably chosen prime, thus vanish on all elements of that order. Finally, the Steinberg character is of defect 0 for the defining characteristic p, thus it vanishes on all p-elements.

This approach works at least if the group order is divisible by enough Zsigmondy prime divisors. The remaining cases can be handled by ad hoc arguments and by using the tables in the Atlas [2].

5.2 Classical groups.

Here we consider the case that $\tilde{G}$ is of simple, simply connected classical type.

Table 5.2: Tori and Zsigmondy primes for classical groups.

	$\lvert T_1\rvert$	$\lvert T_2\rvert$	ℓ_1	ℓ_2
A_n	$(q^{n+1}-1)/(q-1)$	q^n-1	$l(n+1)$	$l(n)$
${}^2A_n$ $(n \geq 3$ odd$)$	$(q^{n+1}-1)/(q+1)$	q^n+1	$l(n+1)$	$l(2n)$
${}^2A_n$ $(n \geq 2$ even$)$	$(q^{n+1}+1)/(q+1)$	q^n-1	$l(2n+2)$	$l(n)$
B_n, C_n $(n \geq 3$ odd$)$	q^n+1	q^n-1	$l(2n)$	$l(n)$
B_n, C_n $(n \geq 2$ even$)$	q^n+1	$(q^{n-1}+1)(q+1)$	$l(2n)$	$l(2n-2)$
D_n $(n \geq 5$ odd$)$	q^n-1	$(q^{n-1}+1)(q+1)$	$l(n)$	$l(2n-2)$
D_n $(n \geq 4$ even$)$	$(q^{n-1}-1)(q-1)$	$(q^{n-1}+1)(q+1)$	$l(n-1)$	$l(2n-2)$
${}^2D_n(n \geq 4)$	q^n+1	$(q^{n-1}+1)(q-1)$	$l(2n)$	$l(2n-2)$

In Table 5.2 we have defined two maximal tori T_1, T_2 for each type of $\tilde{G}$ (by giving their orders, which determines them uniquely). Except for types B_n, C_n with n even this is Table 2.1 in [12]. Furthermore, in each case we have indicated the Zsigmondy prime ℓ_i for the order of T_i.

Most of the following result is already contained in loc. cit., §2.

(5.3) Lemma. *Let $\tilde{G}$ be of classical simply-connected type as in Table 5.2, not of type B_n, C_n or D_n with n even. Assume that the Zsigmondy primes indicated in the table exist. Then there exist three conjugacy classes of elements of prime order in G such that each nontrivial irreducible character of G vanishes on at least one of them.*

Proof. We first claim that the tori T_1, T_2 contain regular elements of prime order. It can be checked from the known formulas for the order of maximal tori of $\tilde{G}$ that whenever T is a maximal torus of order divisible by the Zsigmondy prime ℓ_i then it must be conjugate to T_i. Thus the centralizer of any ℓ_i-singular element of G contains just one type of torus, hence must be a torus itself. In particular, any ℓ_i-singular element is regular semisimple (see [12], §2).

It was shown in (the proofs of) Theorems 2.1–2.6 in loc. cit. that any irreducible character of G different from the trivial and the Steinberg character vanishes on the regular elements of T_1 or of T_2. The Steinberg character vanishes on all p-singular elements, where $p|q$ is the defining characteristic of G. Thus we may choose elements of order ℓ_i in T_i and an arbitrary element of order p to obtain the desired conclusion. □

(5.4) Lemma. *Let $\tilde{G}$ be of classical simply-connected type as in Table 5.2, not of type B_n, C_n or D_n with n even. Then there exist four conjugacy classes of elements of prime order in G such that each nontrivial irreducible character of G vanishes on at least one of them.*

Proof. By Lemma 5.3, it remains to deal with the cases where not both Zsigmondy primes ℓ_1, ℓ_2 exist. By the results in [12], §2, it still remains true that all irreducible characters of G different from the trivial and the Steinberg character vanish on the regular elements of either T_1 of T_2. Thus if we can find regular elements of prime order in both tori, we are done by the same argument as in the generic case, with three classes.

For $G = \mathrm{L}_2(q)$ all non-trivial elements in T_1 and in T_2 are regular. Hence we may choose any elements of prime order in T_1, T_2. For $G = \mathrm{L}_3(q)$ Zsigmondy primes exist in T_1. The image of T_2 in G has order $(q^2 - 1)/\gcd(q - 1, 3)$. Unless $q + 1$ is a power of 2, there exist regular elements of prime order in this torus and we are done. If $q+1$ is a power of 2, then it can be checked from the known character table of $\mathrm{L}_3(q)$ that we may take the Zsigmondy class in T_1, the involution class, and a class of regular unipotent elements. Note that all p-elements in G have order p since here $p \neq 2$.

For $\mathrm{L}_6(2)$ we may take elements of order 2, 5, 7, and 31, for $\mathrm{L}_7(2)$ we choose elements of order 2, 3, 7, and 127.

For $G = \mathrm{U}_3(q)$, $q \geq 3$, there always exist Zsigmondy primes in T_1. In T_2 there exist regular elements of prime order unless $q - 1$ is a power of 2. If $q - 1$ is a power of 2, then it can be checked from the known character table of $\mathrm{U}_3(q)$ that we may take the Zsigmondy class in T_1, the involution class, and a class of regular unipotent elements.

For $\mathrm{U}_6(2)$ the prime ℓ_1 does not exist, but the torus T_1 contains a regular element of order 7, and similarly ℓ_2 does not exist for $\mathrm{U}_7(2)$ but the torus T_2 contains a regular element of order 7.

For $\mathrm{S}_6(2)$ we take elements of orders 2, 3, 5, and 7.

Finally, if $G = \mathrm{O}_8^-(2)$, there exists no Zsigmondy prime ℓ_2. Here the result holds with elements of orders 2, 7, and 17. □

(5.5) Lemma. *Let $\tilde G$ be of simply-connected type B_n or C_n with n even. Then there exist four conjugacy classes of elements of prime order in G such that each nontrivial irreducible character of G vanishes on at least one of them.*

Proof. Let C_1, C_2 be conjugacy classes of regular elements in T_1, T_2 respectively. It was shown in the proof of [11], 3D and 3E, that the only characters apart from the trivial and the Steinberg character not vanishing on either C_1 or C_2 are the two unipotent characters (respectively one if $n = 4$) indexed by the symbols

$$\begin{pmatrix} 0 & 1 & n \\ & - & \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 0 & 1 & \dots & n-2 & n-1 & n \\ & 1 & \dots & n-2 & & \end{pmatrix}.$$

Since these symbols possess no $(n-1)$-hooks the degrees of the corresponding unipotent characters are of ℓ_3-defect zero for any Zsigmondy prime $l(n-1)$. Let ℓ_1, ℓ_2 denote Zsigmondy primes as in Table 5.2. If ℓ_1, ℓ_2, ℓ_3 exist, we choose C_i to contain elements of order ℓ_i, $1 \le i \le 3$, and C_4 to contain elements of order p. Then by the above all non-trivial characters vanish on one of $C_1, \dots, C_4$.

We now deal with the cases where not all Zsigmondy primes exist, that is, $n = 4$ or $(n, q) = (8, 2)$. In both cases, the groups of type B_n and C_n are isomorphic.

For $G = \mathrm{S}_4(q)$ with q odd, we take C_1 to contain elements of order ℓ_1 and C_2 to contain elements of odd prime order dividing $q^2 - 1$. Then all but three (unipotent) characters vanish on these two classes. There exists a subregular unipotent class C_3 of elements of order p on which both the Steinberg character and the third remaining unipotent character vanish. For $G = \mathrm{S}_4(q)$ with $q > 2$ even, both ℓ_1 and ℓ_2 exist (note that $\mathrm{S}_4(2)' \cong \mathfrak{A}_6$). The unipotent character indexed by the above symbol is of defect zero for any prime ℓ_3 dividing $q^2 - 1$, the Steinberg character is of p-defect zero.

For $\mathrm{S}_8(2)$ we take elements of orders 2, 5, 7, and 17. $\square$

(5.6) Lemma. *Let $\tilde G$ be of simply-connected type D_n with n even. Then there exist four conjugacy classes of elements of prime order in G such that each nontrivial irreducible character of G vanishes on at least one of them.*

Proof. Let C_1, C_2 be conjugacy classes of regular elements in T_1, T_2 respectively. It was shown in [11], 3G, that the only characters apart from the trivial and the Steinberg character not vanishing on either C_1 or C_2 are the two unipotent characters indexed by the symbols

$$\begin{pmatrix} n-1 \\ 1 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 0 & \dots & n-3 & n-1 \\ 1 & \dots & n-2 & n-1 \end{pmatrix}.$$

and furthermore the latter two have degree divisible by $l(2n-4)$. For $n \ge 4$ there exists a Zsigmondy prime $\ell_3 = l(2n-4)$ and moreover for $n \ge 6$ the ℓ_3-Sylow subgroup of G is cyclic. So in this case the unipotent characters indexed by the above two symbols are of ℓ_3-defect zero. Let ℓ_1, ℓ_2 denote Zsigmondy primes for G as in Table 5.2. These exist unless $(n, q) = (4, 2)$. We may then choose C_i to contain elements of order ℓ_i, $1 \le i \le 3$, and C_4 to contain elements of order p. By the above all non-trivial characters vanish on one of $C_1, \dots, C_4$.

It remains to consider the case $n = 4$. For $G = \mathrm{O}_8^+(q)$ with $q > 2$, ℓ_1, ℓ_2 and ℓ_3 exist. Since $\ell_3 \ge 5$ there exist regular semisimple elements of order ℓ_3 in the maximal torus of order $(q^2+1)^2$. As the degrees of the unipotent characters indexed by the above two symbols are divisible by ℓ_3, both characters vanish on such a regular element.

Finally, the Steinberg character vanishes on all elements of order p. For $\mathrm{O}_8^+(2)$ we may choose elements of orders 2, 3, 5, and 7. $\square$

Lemmas 5.3–5.6 prove Theorem 5.1 for simple groups of classical Lie type.

5.3 Exceptional groups.

We now investigate the exceptional groups of Lie type. We make use of the exceptional isomorphisms ${}^2G_2(3)' = \mathrm{L}_2(8)$ and $G_2(2)' = \mathrm{U}_3(3)$, and of the fact that ${}^2B_2(2)$ is solvable to exclude these groups from consideration.

It has been proved in [7], Theorem 10.1, that pairs of strongly orthogonal classes exist for all exceptional simple groups of Lie type. Nevertheless, it is not true that the classes in loc. cit. can always be taken to contain elements of prime power order. We will hence rather make use of the approach in [11], §4. For the Suzuki- and Ree-groups explicit character tables are known, and an easy check shows:

(5.7) Lemma. *Let G be a simple exceptional group of type ${}^2B_2$, ${}^2G_2$ or ${}^2F_4$. Then Theorem 5.1 holds for G.*

Proof. Let first $G = {}^2B_2(q^2)$, $q^2 = 2^{2n+1} > 2$. Then it follows from the known character table that any non-trivial irreducible character of G vanishes on either an involution, an element of prime order dividing $q^2 - 1$ or an element of prime order dividing $q^4 + 1$.

Similarly, for $G = {}^2G_2(q^2)$, $q^2 = 3^{2n+1} > 3$, any non-trivial character vanishes on either an element of order 3, or elements of odd prime order dividing either $q^2 - 1$ or $q^6 + 1$.

For $G = {}^2F_4(q^2)$, $q^2 = 2^{2n+1} > 2$, we let C_1, C_2 be classes of elements of prime order dividing $q^4 + \sqrt{2}q^3 + q^2 + \sqrt{2}q + 1$, $(q^4 - q^2 + 1)/3$ respectively. Then by the results of [10] only four irreducible characters of G vanish on neither class, all of them unipotent. Furthermore, two of these unipotent characters of degree $q^4(q^8 - 1)^2/3$ vanish on elements of prime order dividing $q^4 + 1$, while the Steinberg character vanishes on all p-elements.

For ${}^2F_4(2)'$ we may take elements of orders 2, 3, 5, and 13. $\square$

For the seven remaining families, we choose two or three classes of maximal tori as in Table 4.2 of [11], which is reproduced here in Table 5.8.

Table 5.8: Tori T_1, T_2 and T_3.

G	$\lvert T_1\rvert$	$\lvert T_2\rvert$	$\lvert T_3\rvert$	ℓ_1	ℓ_2	ℓ_3
$G_2(q)$	Φ_6	Φ_3		$l(6)$	$l(3)$	
${}^3D_4(q)$	Φ_{12}	Φ_3^2		$l(12)$	$l(3)$	
$F_4(q)$	Φ_{12}	Φ_8		$l(12)$	$l(8)$	
$E_6(q)$	$\Phi_{12}\Phi_3$	Φ_9	$\Phi_8\Phi_2\Phi_1$	$l(12)$	$l(9)$	$l(8)$
${}^2E_6(q)$	Φ_{18}	$\Phi_{12}\Phi_6$	$\Phi_8\Phi_2\Phi_1$	$l(18)$	$l(12)$	$l(8)$
$E_7(q)$	$\Phi_{18}\Phi_2$	$\Phi_{14}\Phi_2$	$\Phi_{12}\Phi_3\Phi_1$	$l(18)$	$l(14)$	$l(12)$
$E_8(q)$	Φ_{30}	Φ_{24}	Φ_{20}	$l(30)$	$l(24)$	$l(20)$

(5.9) Lemma. *Let $\tilde{G}$ be a simple simply-connected group of exceptional Lie type as in Table 5.8. Then Theorem 5.1 holds for G.*

Proof. Let T_i be maximal tori of $\tilde{G}$ with orders as given in Table 5.8. Let C_1, C_2 be conjugacy classes of regular elements in T_1, T_2 respectively. The irreducible characters of G not vanishing on either of T_1, T_2 were determined in [11], §4. In particular they are all unipotent.

For $G_2(q)$, Zsigmondy primes ℓ_1, ℓ_2 exist unless $q = 2$, which is excluded because $G_2(2)' = \mathrm{U}_3(3)$. Since the Sylow ℓ_i-subgroups are cyclic, any element of order ℓ_i in T_i is regular, so we choose C_i to contain elements of order ℓ_i. If q is not a power of 3, let C_3 be the class of elements of order 3 which are not central in a Sylow 3-subgroup. Then from the known character table one can check that two of the unipotent characters not vanishing on C_1 and C_2 take value 0 on C_3. If $q = 3^f > 3$ then there exists an odd prime $\ell_3 \neq 3$ dividing $q^2 - 1$. Here, the two unipotent characters are of ℓ_3-defect 0. In both cases, the Steinberg character is of p-defect 0. For $G_2(3)$ we may take elements of orders 2, 3, 7, and 13.

For $G = {}^3D_4(q)$ both Zsigmondy primes exist. Let C_i be classes of elements of order ℓ_i in T_i. The elements in C_1 are necessarily regular. The characters of G not vanishing on C_1 were listed in [11]. Among those, only three are not of ℓ_2-defect 0. One of them is of defect zero for Zsigmondy primes $l(6)$ (which exist for $q \neq 2$), the other is the Steinberg character. In the case of $q = 2$, we may take elements of orders 2, 3, 7, and 13.

For $G = F_4(q)$ both Zsigmondy primes exist. By loc. cit. the characters of G not vanishing on regular elements of either torus are the trivial character, the Steinberg character, and two unipotent characters of ℓ_3-defect zero, for the Zsigmondy prime $\ell_3 = l(3)$.

For $G = E_6(q), {}^2E_6(q)$, $E_7(q)$ or $E_8(q)$ all three Zsigmondy primes always exist. Let C_i be conjugacy classes of elements of order ℓ_i, $i = 1, 2, 3$. By loc. cit. only the trivial and the Steinberg character do not vanish on at least one of the C_i, $i = 1, 2, 3$. Thus taking for C_4 any class of p-elements we obtain the assertion for G. □

This completes the proof of Theorem 5.1 and hence of Theorem B.

References

[1] H. Blau, *A fixed-point theorem for central elements in quasisimple groups*, Proc. Amer. Math. Soc. **122** (1994), 79–84.

[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[3] B. Fein, W. M. Kantor, M. Schacher, *Relative Brauer groups, II*, J. reine angew Math. **328** (1981), 39–57.

[4] B. Huppert, N. Blackburn, *Finite Groups II*, Springer, Berlin Heidelberg New York, 1982.

[5] I. M. Isaacs, *Character theory of finite groups*, Dover, New York, 1994.

[6] G. James, A. Kerber, *The representation theory of the symmetric group*, Addison-Wesley Publishing Co., Reading, Mass., 1981.

[7] F. Lübeck, G. Malle, $(2,3)$-*generation of exceptional groups*, J. London Math. Soc. **59** (1999), 109–122.

[8] G. Lusztig, *Characters of reductive groups over a finite field*, Annals of Math. Studies, vol. 107, Princeton University Press, Princeton, 1984.

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

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

[11] G. Malle, *Almost irreducible tensor squares*, Comm. Algebra **27** (1999), 1033–1051.
[12] G. Malle, J. Saxl, T. Weigel, *Generation of classical groups*, Geom. Dedicata **49** (1994), 85–116.
[13] J.B. Olsson, *McKay numbers and heights of characters*, Math. Scand. **38, no. 1** (1976), 25–42.
[14] J.B. Olsson, *Combinatorics and representations of finite groups*, Lecture Notes in Mathematics, vol. 20, Universität Essen, Essen, 1993.

Fachbereich Mathematik/Informatik, Universität Kassel, Heinrich-Plett-Str. 40, D–34132 Kassel, Germany
E-mail address: malle@mathematik.uni-kassel.de

Departament d'Algebra, Facultat de Matemátiques, Universitat de València, 46100 Burjassot. València, Spain
E-mail address: gabriel@uv.es

Matematisk Afdeling, Universitetsparken 5, DK-2100 Copenhagen, Denmark
E-mail address: olsson@math.ku.dk