ISRAEL JOURNAL OF MATHEMATICS **142** (2004), 163–187

ON THE NUMBER OF CONJUGACY CLASSES OF ZEROS OF CHARACTERS*

BY

ALEXANDER MORETÓ

Departament d'Àlgebra, Universitat de València
46100 Burjassot, València, Spain
e-mail: mtbmoqua@lg.ehu.es

AND

JOSU SANGRONIZ

Departamento de Matemáticas, Facultad de Ciencias
Universidad del País Vasco, 48080 Bilbao, Spain
e-mail: mtpsagoj@lg.ehu.es

ABSTRACT

Let m be a fixed non-negative integer. In this work we try to answer the following question: What can be said about a (finite) group G if all of its irreducible (complex) characters vanish on at most m conjugacy classes? The classical result of Burnside about zeros of characters says that G is abelian if $m = 0$, so it is reasonable to expect that the structure of G will somehow reflect the fact that the irreducible characters vanish on a bounded number of classes. The same question can also be posed under the weaker hypothesis that *some* irreducible character of G has m classes of zeros. For nilpotent groups we shall prove that the order is bounded by a function of m in the first case but only the derived length can be bounded in general under the weaker condition. For solvable groups the situation is not so well understood although we shall prove that the Fitting height can be bounded by a double logarithmic function of m, improving a recent result by G. Qian.

* Both authors research is partially supported by the Feder, the Spanish Ministerio de Ciencia y Tecnología, grant BFM2001-0180, and the University of the Basque Country, grant 1/UPV00127.310-E-13817/2001. The first author is also supported by the Basque Government.
Received February 2, 2003

1. Introduction

Let G be a non-abelian finite group. For every $\chi \in \mathrm{Irr}(G)$ we put

$$m(\chi) = |\{C \in \mathrm{cl}(G) \mid \chi(x) = 0 \text{ for } x \in C\}|,$$

where $\mathrm{cl}(G)$ denotes the set of conjugacy classes of G.

Let $m(G) = \max_{\chi \in \mathrm{Irr}(G)} m(\chi)$ and $n(G) = \min_{\chi \in \mathrm{Irr}_1(G)} m(\chi)$, where $\mathrm{Irr}_1(G)$ stands for the set of non-linear irreducible characters of G. A number of papers have been devoted to the study of the zeros of the characters of a finite group. In particular, in a very recent paper G. Qian [24] proves that the Fitting height $h(G)$ of a solvable group G is bounded by a linear function of $m(G)$. In this work our aim is twofold: trying to improve Qian's result both quantitatively (giving a more realistic bound for the Fitting height) and qualitatively (substituting the Fitting height by some other group invariant like the derived length or the order or replacing $m(G)$ by $n(G)$). In the first direction, using information from [20], we obtain the following result.

THEOREM A: *Let G be a solvable group and write $F_i(G)$ (simply $F(G)$ for $i = 1$) to denote the ith term in the Fitting series of G. Then*

(i) *There exist real numbers C_1 and C_2 such that $h(G) \leq C_1 \log\log m(G) + C_2$ whenever $m(G) > 1$.*

(ii) *$|G : F_{10}(G)|$ is bounded in terms of $m(G)$.*

(iii) *If $|F_{10}(G)|$ is odd, then $|G : F(G)|$ is bounded in terms of $m(G)$.*

Parts (ii) and (iii) of this theorem are actually examples of our second goal. We believe that it is possible to improve Qian's result also qualitatively, however our results in this direction refer mostly to nilpotent groups. (Actually, we will just state these results for p-groups and it will always be clear how to extend them to nilpotent groups.) For instance, we have the following.

THEOREM B: *Let P be a finite non-abelian p-group. Then $|P|$ is bounded by some function that depends only on $m(P)$.*

As dihedral groups of order $2m$ show, the order of a non-abelian supersolvable group cannot be bounded in terms of $m(G)$, so this result cannot be pushed further.

Much effort has been devoted to finding good lower bounds for the number of conjugacy classes of a finite group in terms of the order of the group (see [23], for instance). This result shows that for nilpotent groups it is possible to bound the group order by the number of certain conjugacy classes. While we do not give explicit bounds, it is possible to obtain them just by following the proofs.

A classical theorem of W. Burnside asserts that any non-linear character of a finite group vanishes at some element. Our next result shows that for p-groups there always exists more than one conjugacy class of zeros of any non-linear character.

THEOREM C: *Let χ be a non-linear irreducible character of a finite p-group P of degree p^n. Then $m(\chi)$ is a multiple of $p-1$ bigger than or equal to $(p+n)(p-1)$. In particular, $m(\chi) \geq p^2 - 1$.*

The last inequality is best possible, as extraspecial p-groups of order p^3 show. We will see that there are 2-groups and 3-groups of arbitrarily large order with faithful characters that vanish on exactly 3 and 8 conjugacy classes, respectively, so it is not possible to bound the order of a p-group P in terms of $n(P)$ for $p \leq 3$. Rather surprisingly, the order of a p-group with an irreducible character vanishing on exactly $p^2 - 1$ conjugacy classes is bounded (by a function depending on p only) if $p \geq 5$.

THEOREM D: *Let $p \geq 5$ be a prime number and P a p-group. Suppose that there exists $\chi \in \mathrm{Irr}(P)$ such that $m(\chi) = p^2 - 1$. Let r be the smallest prime that does not divide $p-1$. Then $|P| \leq p^{2r-1}$ and, moreover, this bound can be improved to $|P| \leq p^{r+1}$ if χ is faithful.*

We will see that the bound that we have obtained in the faithful case is best possible for all but finitely many primes. In order to check this we will need some results on the so-called permutation polynomials. These results are proved in Section 2.

In view of this result it is tempting to conjecture that for $p \geq 5$ the order of a p-group P is bounded in terms of $n(P)$. However, we shall show that there are p-groups with arbitrarily large order and an irreducible character vanishing on exactly $(p-1)! + p^2 - p$ classes. These groups also have unbounded nilpotence class (they are of maximal class) though they are metabelian. The next theorem shows that it is not possible to find p-groups P with arbitrarily large derived length and fixed $n(P)$.

THEOREM E: *Let P be a finite p-group. Then the derived length of P is bounded by some function that depends only on $n(P)$.*

We will show in Section 6 that it is not possible to bound the derived length of a solvable group G in terms of $n(G)$. We conjecture the following.

CONJECTURE F: *If G is solvable, then $\mathrm{dl}(G)$ and $|G : F(G)|$ are bounded in terms of $m(G)$.*

Note that the second statement of this conjecture has been proved for odd order groups in Theorem A. We will also see that it is not possible to bound the index $|G : F(G)|$ in terms of $n(G)$. However, we conjecture the following.

CONJECTURE G: *The Fitting height of a solvable group G is bounded in terms of $n(G)$.*

We shall prove this conjecture when $n(G) = 1$.

As proved by D. Chillag in [4] and independently by Y. Berkovich and L. Kazarin in [1], $m(G) = 1$ if and only if G is a Frobenius group with complement of order 2 and abelian kernel of odd order. In particular, Conjecture F holds if $m(G) = 1$. Groups G with $m(G) = 2$ were studied in [2] and it follows from Theorem 1.1 of that paper that Conjecture F also holds in this case. We have taken the study of these groups further and, with the help of the detailed information of these groups given in Theorem 1.1 of [2], we have obtained a complete classification of them.

THEOREM H: *Let G be a finite group. Then $m(G) = 2$ if and only if G is isomorphic to one of the following groups:*

(i) *The symmetric group S_4.*
(ii) *The alternating group A_5.*
(ii) *The projective special linear group* $\mathrm{PSL}(2, 7)$.
(iv) *An extension of a group of order 2 by a Frobenius group with complement of order 2 and abelian kernel of odd order.*
(v) *A Frobenius group with complement of order 3 and abelian kernel.*

We have also been able to prove Conjecture F for supersolvable groups. It might be true that the derived length of a solvable group is bounded by some function of $m(\chi)$ for any faithful irreducible character χ. An easy subdirect product argument shows that this would imply Conjecture F.

Next, we explain the way our results are distributed in the paper. In Section 2 we review some results on permutation polynomials that will be useful in Section 4, where we prove Theorem D. Section 3 is devoted to the proof of Theorem C. We prove Theorem B in Section 5. Finally, we present some results on bounding the derived length by the number of classes of zeros in Section 6 and those on the Fitting height in Section 7.

ACKNOWLEDGEMENT: We thank G. A. Fernández-Alcober, R. Guralnick, M. Isaacs, A. Mann and M. Zieve for helpful comments. The results of Section 2 have been proved by Guralnick and Zieve and are included here with their kind permission. Some of this work was done while both of us were visiting the

University of Wisconsin, Madison. We thank the Mathematics Department for its hospitality.

2. Permutation polynomials

Let F be the finite field with q elements, where q is a power of a prime p. A polynomial with coefficients in F is called a **permutation polynomial** if it is a bijection from F onto itself. We write $\mathrm{md}(q)$ to denote the minimal degree of a non-linear permutation polynomial over the field with q elements. Our proof of Theorem D yields that $|P| \leq p^{\mathrm{md}(p)+1}$ if χ is faithful and $|P| \leq p^{2\,\mathrm{md}(p)-1}$ in general and that the bound in the faithful case is best possible. The goal of this section is to obtain a precise estimation of $\mathrm{md}(p)$ that allows us to claim that the bound in Theorem D is best possible in the faithful case for all but finitely many primes, i.e., we need to compute the exact value of $\mathrm{md}(p)$ for almost all primes.

We remark that if r does not divide $p-1$ then the polynomial $f(x) = x^r \in \mathbb{F}_p[x]$ is a bijection, so it is clear that Theorem D follows from the bounds mentioned in the previous paragraph. It is a consequence of a theorem of Dickson, that appears as Theorem 84 of [9] (which actually goes back to Hermite for fields of prime order), that the degree of a non-linear permutation polynomial over the field with q elements does not divide $q-1$, so $\mathrm{md}(p)$ is at least the smallest number not dividing $p-1$. In particular, $\mathrm{md}(p)$ can be arbitrarily large.

The goal of this section is to prove that $\mathrm{md}(p) = r$, where r is the smallest prime that does not divide $p-1$, for almost all primes. First, we need a lemma, whose proof seems to have been known for a long time but for which there doesn't seem to be a reference. An **exceptional polynomial** over $\mathbb{F}_q$ is a polynomial $f \in \mathbb{F}_q[x]$ for which the only factors of $f(x) - f(y) \in \mathbb{F}_q[x,y]$ which are irreducible in $K[x,y]$ are the scalar multiples of $x-y$, where K is an algebraic closure of $\mathbb{F}_q$. It was proved by Cohen [6] that every exceptional polynomial is a permutation polynomial, but we will not need this fact.

LEMMA 2.1: *If $f(x) \in \mathbb{F}_q[x]$ is a non-exceptional permutation polynomial of degree d, then*

$$q + 3 - 2d \leq [2q^{1/2}](d-2)(d-3)/2.$$

In particular, $q < d^4$.

Proof: Since $f(x)$ is non-exceptional, there is a polynomial $R(x,y) \in \mathbb{F}_q[x,y]$ such that $R(x,y)$ divides $f(x) - f(y)$, $R(x,y)$ is not a multiple of $x-y$ and

$R(x,y)$ is irreducible in $K[x,y]$, where K is an algebraic closure of $\mathbb{F}_q$. Let D be the degree of R and N the number of pairs $(a,b) \in (\mathbb{F}_q)^2$ such that $R(a,b) = 0$. Notice that $D \leq d-1$, so by Corollary 2(b) of [17] we have that

$$N \geq q+1-D-[2q^{1/2}](D-1)(D-2)/2 \geq q+2-d-[2q^{1/2}](d-2)(d-3)/2.$$

On the other hand, $R(a,b) = 0$ can only occur if $a = b$ (because f is a permutation polynomial), so the number N is the number of roots of the polynomial $R(x,x) \in \mathbb{F}_q[x]$. This polynomial is non-zero (otherwise $x-y$ would be a divisor of $R(x,y)$) and its degree is at most $d-1$, so $N \leq d-1$ and the result follows. ∎

THEOREM 2.2: *The minimal degree of a permutation polynomial over the field with p elements is the smallest prime that does not divide $p-1$ unless $p \in \mathcal{S} = \{7, 211, 421, 631, 1051, 1471, 2311\}$.*

Proof: If r is the least prime not dividing $p-1$, then as we have pointed out before, $\mathrm{md}(p) \leq r$. Let's suppose that this inequality is strict and show that $p \in \mathcal{S}$ in this case. It is proved in [10] (see also Chapter 6 of [18]) that r is the lowest degree of any non-linear exceptional polynomial over $\mathbb{F}_p$, so it follows that, under our assumption $\mathrm{md}(p) < r$, a permutation polynomial of minimal degree is not exceptional and, by Lemma 2.1, $\mathrm{md}(p) > p^{1/4}$. Therefore, any prime less than $p^{1/4}$ must divide $p-1$. For $p \geq 17^4$, the number of primes less that $p^{1/4}$ is at least $4p^{1/4}/\log p$ (see Corollary 1 in [25], for instance). Trivial estimates yield that $p \leq 23^4$. Now, using a computer, it is easy to determine for which of these primes p, $p-1$ is divisible by all the primes that do not exceed $p^{1/4}$. The list of primes thus obtained can be further reduced taking into account the stronger inequality in Lemma 2.1 and the result of Dickson and Hermite. After these reductions only the primes in $\mathcal{S}$ remain. ∎

The polynomial $x^4 + 3x$ is a permutation polynomial over $\mathbb{F}_7$, so $p = 7$ is a genuine exception to this theorem. It seems likely that for the remaining primes p in $\mathcal{S}$ the minimal degree is also the smallest prime that does not divide $p-1$.

3. Proof of Theorem C

The goal of this section is to prove Theorem C. We introduce first some notation that will be maintained throughout this paper.

Given a group G and $g \in G$, we write $\mathrm{cl}_G(g)$ to denote the conjugacy class of g in G. If N is a normal subgroup of G, then the preimage in G of $\mathrm{cl}_{G/N}(gN)$ is

the union of some conjugacy classes $C_1, \ldots, C_n$ of G. If $\overline{\chi} \in \mathrm{Irr}(G/N)$ vanishes at gN and we view $\overline{\chi}$ as a character χ of G, then we have that χ vanishes on all the conjugacy classes $C_1, \ldots, C_n$. In particular, $m(\overline{\chi}) \leq m(\chi)$ with an equality if and only if the classes of zeros of $\overline{\chi}$ lift to unique classes in G. It follows that, in general, $m(G/N) \leq m(G)$. It is also clear that if N is a normal subgroup of a group G and x_1N and x_2N are not conjugate in G/N, then x_1 and x_2 are not conjugate in G. We will use these facts without further explicit mention. If S is a normal subset of G, we write $k_G(S)$ to denote the number of conjugacy classes of G contained in S. We simply write $k(G)$ for the number of conjugacy classes of G.

We need the following easy lemma.

LEMMA 3.1: *Let M be a normal subgroup of a p-group P and H a subgroup of M with $|M : H| = p^n$. Then*

$$k_P(M - \bigcup_{g \in P} H^g) \geq n(p-1).$$

Proof: Argue by induction on $|M|$, the case $M = 1$ being trivial. Take a minimal normal subgroup N of P inside M and apply the inductive hypothesis to the group P/N and the subgroups M/N and HN/N. The result is then clear if $N \leq H$. Otherwise $N \cap H = 1$ and we obtain $(n-1)(p-1)$ classes inside $M - \bigcup_{g \in P} H^g N$. Since N is central, the non-trivial elements in N provide us with $p-1$ extra classes in $M - \bigcup_{g \in P} H^g$, so the result follows. ∎

Proof of Theorem C: The fact that $m(\chi)$ is a multiple of $p-1$ can be proved by standard methods, noting that if the exponent of P is p^e then the Hall p'-subgroup of the group of units of $\mathbb{Z}/p^e\mathbb{Z}$ acts fixed point freely on the set of conjugacy classes of zeros of χ.

Now we want to see that $m(\chi) \geq (p+n)(p-1)$. Of course we can suppose from the outset that χ is a faithful character. Let $H \leq P$ be a subgroup of index p^n such that $\chi = \lambda^P$ for some linear character λ of H and M a maximal subgroup containing H. Then χ vanishes on $P - \bigcup_{g \in P} H^g$, so by the previous lemma we have

$$m(\chi) \geq k_P(P - M) + k_P(M - \bigcup_{g \in P} H^g) \geq k_P(P - M) + (n-1)(p-1).$$

If all the centralizers of the elements in $P - M$ have order greater than p^2, then $P - M$ has at least $p^3 - p^2$ classes and the result is clear. Otherwise, the centralizer of some element, say g, has order p^2 so, by a well-known result of

M. Suzuki (see Satz III.14.23 in [11]), P is a p-group of maximal class. The case $|P| = p^3$ is obvious (all the non-linear characters have degree p and vanish on exactly $p^2 - 1$ classes), so in the sequel we suppose that $|P| \geq p^4$. Then the second centre Z_2 is abelian and, by Problem 6.11 of [13], χ is a relative M-character with respect to Z_2. This means that the subgroup H can be taken to contain Z_2. Note that $k_P(P-M) \geq p^2 - p$, so we only need to produce $p-1$ classes of zeros inside $\bigcup_{g \in P} H^g$. We shall do this by proving that χ vanishes on $Z_2 - Z$ (Z denotes the centre of P). Let $z \in Z_2 - Z$. Since $C_P(g) = \langle g \rangle Z$, it is clear that $[z, g] \neq 1$. On the other hand the restriction of λ to Z is not the principal character (because $\chi = \lambda^P$ is faithful), so $\varepsilon = \lambda([z, g])$ is a primitive pth root of unity. Finally, we compute $\chi(z)$. We have

$$\chi(z) = \chi(z^g) = \chi(z[z, g]) = \chi(z)\lambda([z, g]) = \chi(z)\varepsilon,$$

and it follows that $\chi(z) = 0$. ∎

Note that a consequence of the last theorem is that the number of classes of zeros of any non-linear character χ of a p-group P is at least $p^2 - 1$ and the equality can only hold if the p-group has maximal class and the degree of the character is p. It also follows from the proof that if we assume in addition that χ is faithful (and $|P| \geq p^4$), then χ vanishes on the $p^2 - p$ conjugacy classes outside a certain maximal subgroup and on the $p-1$ conjugacy classes that are contained in $Z_2(P) - Z(P)$. If χ is not faithful and its kernel is K then, as a character of P/K, χ also vanishes on $p^2 - 1$ classes, which lift to unique classes in P. This simply means that for any zero x of χ, all the elements in the coset xK are conjugate. We will make use of these ideas later on. It was pointed out by Berkovich (see [4]) that the number of zeros for p-groups that are not of maximal class is at least $p^3 - p^2$ (this is also clear from the preceding proof).

4. Characters of p-groups with few classes of zeros

First, we present examples that show that it is possible to have $m(\chi) = p^2 - 1$ for characters of 2-groups and 3-groups of arbitrarily large order.

Take first any 2-group of maximal class P (of order at least 8) and a faithful irreducible character χ. If C is the maximal cyclic subgroup of P, then χ can be induced from a linear character λ of C and λ has order $|C| = 2^n$ (otherwise, χ would not be faithful). For $x \in C$ we have that $\chi(x) = \lambda(x) + \lambda(x^i) = \varepsilon + \varepsilon^i$, where ε is a primitive $o(x)$-th root of unity and i depends on the group P. In any case it happens that ε^i is the opposite of ε if and only if $o(x) = 4$, so the

zeros of χ are exactly the elements of $P - C$ and the two elements of C of order 4, a set that is the union of three conjugacy classes.

Now, instead of just constructing the promised family of 3-groups, we shall show that for any odd prime p there are p-groups (of maximal class) of arbitrarily large order having an irreducible character with exactly $(p-1)! + p^2 - p$ classes of zeros (8, for $p = 3$). This will show that in general the order of a p-group P (or even the nilpotence class) cannot be bounded by a function of $n(P)$. This example will also play a key role in the proof of Theorem D.

Example 4.1: Let p be an odd prime and suppose P is a p-group with a maximal subgroup which is homocyclic of rank $p-1$ and has exponent p^e, say $A = \langle x_1, \ldots, x_{p-1} \rangle$. Assume also that there exists an element $g \in P - A$ such that $x_i^g = x_{i+1}$ for $1 \leq i < p-1$ and $x_{p-1}^g = x_1^{-1} \cdots x_{p-1}^{-1}$. We claim that any irreducible faithful character of P vanishes on exactly $(p-1)! + p^2 - p$ conjugacy classes. Checking this requires some computations which we now sketch below.

LEMMA 4.2: *Let $\varepsilon_1, \ldots, \varepsilon_{p-1}$ be p^nth roots of unity adding up to -1. Then they are the different $p-1$ primitive pth roots of unity.*

Proof: Apply to the relation $1 + \varepsilon_1 + \cdots + \varepsilon_{p-1} = 0$ the automorphisms in the Galois group of the field extension $\mathbb{Q}(\varepsilon_1, \ldots, \varepsilon_{p-1})/\mathbb{Q}$. One gets that for any integer j coprime with p, $1 + \varepsilon_1^j + \cdots + \varepsilon_{p-1}^j = 0$. Now the coefficients of the polynomial $l(x) = (x - \varepsilon_1) \cdots (x - \varepsilon_{p-1})$ can be computed by using Newton's formulas (see, for instance, p. 179 of [7]) and it turns out that $l(x) = x^{p-1} + \cdots + x + 1$, so the result is clear. ∎

LEMMA 4.3: *Let p be an odd prime number and define the following matrix in the indeterminates $x_1, \ldots, x_{p-1}$:*

$$\Delta(x_1, \ldots, x_{p-1}) = \begin{pmatrix} x_2 & x_3 & \ldots & x_{p-1} & d \\ x_3 & x_4 & \ldots & d & x_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ d & x_1 & \ldots & x_{p-3} & x_{p-2} \end{pmatrix},$$

where $d = -x_1 - \cdots - x_{p-1}$. The determinant of this matrix defines a polynomial $f(x_1, \ldots, x_{p-1})$ with integer coefficients. Then

(1)

$$f(x_1, \ldots, x_{p-1}) = (-1)^{p(p-1)/2} \prod_{\substack{\zeta^p = 1 \\ \zeta \neq 1}} (x_1 + (1+\zeta)x_2 + \cdots + (1+\zeta+\cdots+\zeta^{p-2})x_{p-1}).$$

In particular, if $c_1, \ldots, c_{p-1}$ are integers, then

$$f(c_1, \ldots, c_{p-1}) \equiv (-1)^{p(p-1)/2}(c_1 + 2c_2 + \cdots + (p-1)c_{p-1})^{p-1} \pmod{p}.$$

Proof: Take any primitive pth root of unity ζ. To calculate the determinant of Δ, note that if we multiply the jth column by $\zeta+\zeta^2+\cdots+\zeta^j$ and then sum these columns for $j = 1, \ldots, p-1$, we obtain a column whose entries are polynomials which are proportional to $x_1 + (1+\zeta)x_2 + \cdots + (1+\zeta+\cdots+\zeta^{p-2})x_{p-1}$. We conclude that all these linear polynomials for the various ζ divide f and so, except for a constant, their product is f. To compute the constant simply evaluate in $x_1 = 1$, $x_2 = \cdots = x_{p-1} = 0$.

The congruence can be obtained by reducing the coefficients on both sides of (1) modulo a maximal ideal of the ring of integers of $\mathbb{Q}(\zeta)$ (ζ is a primitive pth root of unity) containing $p\mathbb{Z}$. The point is that, modulo this ideal, ζ becomes 1. ∎

Suppose now that χ is a faithful irreducible character of the group P in the example. Then $\chi = \lambda^P$ for some linear character λ of A and, since χ is faithful and $(x_1x_2^2\cdots x_{p-1}^{p-1})^{p^{e-1}}$ is in the centre of P, we have that $\lambda((x_1x_2^2\cdots x_{p-1}^{p-1})^{p^{e-1}}) \neq 1$. Now fix once and for all a primitive p^eth root of unity ε and take integers $c_1, \ldots, c_{p-1}$ such that $\lambda(x_1^{i_1}\cdots x_{p-1}^{i_{p-1}}) = \varepsilon^{c_1i_1+\cdots+c_{p-1}i_{p-1}}$. Note that the preceding remark simply says that $c_1 + 2c_2 + \cdots + (p-1)c_{p-1} \not\equiv 0 \pmod{p}$.

To simplify the expressions, we put $C = (c_1, \ldots, c_{p-1})$, $X = (i_1, \ldots, i_{p-1})$ and denote by M the $(p-1)\times(p-1)$ matrix with 1's in the second upper diagonal, -1's in the last row and zeros elsewhere. Then

$$\chi(x_1^{i_1}\cdots x_{p-1}^{i_{p-1}}) = \varepsilon^{XC^t}(1+\varepsilon^{X(M-I)C^t}+\cdots+\varepsilon^{X(M^{p-1}-I)C^t}).$$

(Here I is the $(p-1)\times(p-1)$ identity matrix and C^t denotes the transpose matrix of C.) Lemma 4.2 implies that $x_1^{i_1}\cdots x_{p-1}^{i_{p-1}}$ is a zero of χ if and only if

$$(2)\qquad \begin{cases} X(M-I)C^t & \equiv & k_1p^{e-1} & \pmod{p^e}, \\ & \vdots & & \\ X(M^{p-1}-I)C^t & \equiv & k_{p-1}p^{e-1} & \pmod{p^e}, \end{cases}$$

where $k_1, \ldots, k_{p-1}$ is a permutation of the numbers $1, \ldots, p-1$. We can write this system more compactly as

$$(3)\qquad XR - XC^t(1,\ldots,1) \equiv (k_1,\ldots,k_{p-1})p^{e-1} \pmod{p^e},$$

where $R = \Delta(c_1, \ldots, c_{p-1})$. Note that $C = -(1,\ldots,1)R$, so (3) simplifies to

$$(4)\qquad XR + XRJ \equiv (k_1,\ldots,k_{p-1})p^{e-1} \pmod{p^e},$$

where J is the $(p-1)\times(p-1)$ matrix all of whose entries are 1. By the last lemma, the determinant of R is coprime with p (remember that $c_1 + 2c_2 + \cdots +$

$(p-1)c_{p-1} \not\equiv 0 \pmod{p}$), so the number of solutions of (4) is the same as for

$$Y(I+J) \equiv (k_1, \ldots, k_{p-1})p^{e-1} \pmod{p^e}. \tag{5}$$

The solutions of this system are $y_1 \equiv 0 \pmod{p^{e-1}}$, $y_i \equiv y_1 + (k_i - k_1)p^{e-1} \pmod{p^e}$ for $2 \leq i \leq p-1$ (we notice that at some point it is necessary to make use of the fact that $k_1 + \cdots + k_{p-1} \equiv 1 + \cdots + (p-1) \equiv 0 \pmod{p}$). We conclude that the number of solutions of any of the systems (2) to (5) is p, which means that the number of zeros of χ in A is $p(p-1)!$. So χ vanishes on $(p-1)!$ classes inside A and also on the $p^2 - p$ classes that make up $P - A$. We find that the total number of classes of zeros of χ is $(p-1)! + p^2 - p$.

We work now toward a proof of Theorem D where we show that the behaviour of the primes 2 and 3 is exceptional in the sense that a p-group with an irreducible character vanishing on exactly $p^2 - 1$ conjugacy classes has bounded order for $p \geq 5$. In the proof of the next lemma we make use of the fact that the exponent of the derived subgroup of a p-group of maximal class and order at most p^{p+1} is p (see [3]). We have made the rest of the proof self-contained although it could be simplified by using some additional results from the theory of p-groups of maximal class.

LEMMA 4.4: *Let M be an abelian p-group of order at most p^p with a subgroup M_0 such that M/M_0 is cyclic. Suppose that M has an automorphism α of order p which fixes exactly p elements in M, none of which, except for the identity, lies in M_0. Then there exist elements $x_1, \ldots, x_r$ in M such that M is the direct product of the subgroups $\langle x_i \rangle$ and one of the following happens:*

(i) *M is elementary abelian, $M_0 = \langle x_1, \ldots, x_{r-1} \rangle$ and $x_i^\alpha = x_i x_{i+1}$ for $1 \leq i \leq r$ (put $x_{r+1} = 1$).*

(ii) *All the elements x_i have order p, except for x_1, which has order p^2, $M_0 = \langle x_2, \ldots, x_r \rangle$, $x_i^\alpha = x_i x_{i+1}$ for $1 \leq i \leq r-1$ and $x_r^\alpha = x_r x_1^{lp}$ for some $(l, p) = 1$.*

Proof: The semidirect product $P = \langle \alpha \rangle \ltimes M$ is a p-group of maximal class of order at most p^{p+1}, so the exponent of P' is p and, since $P' \leq M$, P' is elementary abelian. We have $P' \leq \Omega_1(M) \leq M \leq P$, where

$$\Omega_1(M) = \{x \in M \mid x^p = 1\}.$$

Since $|P : M| = p$ and $|P : P'| = p^2$, either $P' = \Omega_1(M)$ or else, $\Omega_1(M) = M$. We deal first with the latter case, that is, when M is elementary abelian. Then $M = M_0 \times Z(P)$, whence $P' = [M, \alpha] = [M_0, \alpha]$. Of course we can assume that

$|M| = p^r > p$, so that $P' \neq 1$ and $Z(P) \leq P' = [M_0, \alpha]$. Fix a generator x_r of $Z(P)$ and take $x_{r-1} \in M_0$ such that $x_r = [x_{r-1}, \alpha]$. The subgroup generated by x_{r-1} and x_r is normal in P so, unless its order is greater than p^{r-1}, it is contained in P' and we can pick $x_{r-2} \in M_0$ such that $x_{r-2} = [x_{r-1}, \alpha]$. Arguing this way we can find elements $x_1, \ldots, x_r$ such that $x_i^\alpha = x_i x_{i+1}$ ($x_{r+1} = 1$, as usual). Now we only need to prove that M is generated by the x_i, but this is clear because otherwise there would exist a largest $1 \leq i < r$ such that $x_i \in \langle x_{i+1}, \ldots, x_r \rangle$ and then

$$x_{i+1} = [x_i, \alpha] \in [\langle x_{i+1}, \ldots, x_r \rangle, \alpha] = \langle x_{i+2}, \ldots, x_r \rangle,$$

against the choice of i.

We deal finally with the second case $P' = \Omega_1(M)$. Then M is not elementary abelian but does have a maximal subgroup which is elementary abelian, namely P', so M is the direct product of a cyclic subgroup of order p^2 and subgroups of order p. It follows that M^p has order p and $M^p = Z(P)$. We apply the previous case with $\Omega_1(M)$ and $\Omega_1(M) \cap M_0$ playing the role of M and M_0, respectively (note that $M_0 \neq \Omega_1(M)$ because $Z(P)$ is contained in $\Omega_1(M)$ but not in M_0). We conclude that there exists a minimal set of generators of $\Omega_1(M)$, $x_2, \ldots, x_r, \omega$ such that $\Omega_1(M) \cap M_0 = \langle x_2, \ldots, x_r \rangle$ and $x_i^\alpha = x_i x_{i+1}$ for $2 \leq i \leq r-1$, $x_r^\alpha = x_r \omega$ and $\omega^\alpha = \omega$. Since $x_2 \in \Omega_1(M) = P' = [M, \alpha]$, there exists $x_1 \in M$ such that $x_1^\alpha = x_1 x_2$ and $x_1 \notin \Omega_1(M)$ (otherwise, $x_2 = [x_1, \alpha] \in \langle x_3, \ldots, x_r, \omega \rangle$, which is impossible). Thus the order of x_1 is p^2 and $x_1^p \in Z(P) = \langle \omega \rangle$ (because x_1^p is fixed by α), whence $\omega = x_1^{lp}$ with $(l, p) = 1$. ∎

We are now ready to prove the faithful case in Theorem D.

Proof of Theorem D, faithful case: We know that P is a p-group of maximal class, that the degree of χ is p and that $\chi = \lambda^P$ for λ a linear character of a maximal subgroup M, which is abelian (M' is contained in the kernel of χ and so is trivial). We split the proof in two cases. First we suppose that $|P| \geq p^{p+1}$. As is usual when dealing with p-groups of maximal class, we shall denote by P_i, $i \geq 2$, the ith term of the lower central series. Then P_2/P_{p+1} has order p^{p-1} and exponent p (by [3]) and, being inside M/P_{p+1}, is abelian. We conclude that the rank of M is at least $p-1$. Now we take an elementary abelian subgroup $A \leq M$ of rank $p-1$ and normal in P and set $L = \langle g \rangle A$, where g is an element outside M. Since L is not abelian, χ restricts irreducibly to it, so it follows from Example 4.1 (the particular case when A is elementary abelian) that χ_L vanishes on $(p-1)!$ classes in A (at this point, the distinction between L-classes and P-classes is immaterial). Taking into account the classes in $P - M$, we

conclude that χ vanishes on at least $(p-1)!+p^2-p$ classes, which is impossible because this number is greater than p^2-1 for $p \geq 5$.

We consider now the case $|P| \leq p^p$. We apply the previous lemma to the group M, the subgroup $M_0 = \operatorname{Ker}\lambda$ and the automorphism α induced by conjugation by an element $g \in P - M$. According to the lemma two cases can occur. In the first one M is elementary abelian and there exists a minimal set of generators $x_1, \ldots, x_r$ such that $x_i^g = x_i x_{i+1}$ ($x_{r+1} = 1$) and $M_0 = \operatorname{Ker}\lambda = \langle x_1, \ldots, x_{r-1}\rangle$, that is $\lambda(x_i) = 1$ for $1 \leq i < r$ and $\lambda(x_r) = \varepsilon$, a primitive pth root of unity. Since χ only vanishes on p^2-1 classes, the only zeros in M are the elements in $Z_2(P) - Z(P) = \langle x_{r-1}, x_r\rangle - \langle x_r\rangle$ (we can suppose of course that $|P| \geq p^4$).

Routine computations show that

$$\lambda^{g^{-j}}(x_1^{i_1}\cdots x_r^{i_r}) = \varepsilon^{i_r + i_{r-1}\binom{j}{1} + i_{r-2}\binom{j}{2} + \cdots + i_1\binom{j}{r-1}}$$

(we adhere to the usual convention of setting $\binom{j}{k} = 0$ if $k > j$).

For $i_1, \ldots, i_r$ fixed elements in $\mathbb{F}_p$, we define the polynomial

$$\varphi(x) = i_1\binom{x}{r-1} + \cdots + i_{r-1}\binom{x}{1} + i_r,$$

where $\binom{x}{i}$, $1 \leq i < p$, is the polynomial $x(x-1)\cdots(x-i+1)/i! \in \mathbb{F}_p[x]$. We note that

$$\chi(x_1^{i_1}\cdots x_r^{i_r}) = \varepsilon^{\varphi(0)} + \varepsilon^{\varphi(1)} + \cdots + \varepsilon^{\varphi(p-1)},$$

so $x_1^{i_1}\cdots x_r^{i_r}$ is a zero of χ if and only if φ is a permutation polynomial on $\mathbb{F}_p$ (by Lemma 4.2). It is clear that the map assigning to each element $x_1^{i_1}\cdots x_r^{i_r}$ the corresponding polynomial φ is a bijection between M and the set of polynomials of degree at most $r-1$. Under this map linear polynomials correspond to the elements in the difference $\langle x_{r-1}, x_r\rangle - \langle x_r\rangle$, that is, to the zeros of χ in M. We conclude that, apart from linear polynomials, permutation polynomials must have degree at least r, so $r \leq \operatorname{md}(p)$ and $|P| = p^{r+1} \leq p^{\operatorname{md}(p)+1}$.

We consider now the second possibility in Lemma 4.4 and maintain the notation there. This time $\lambda(x_1^{i_1}\cdots x_r^{i_r}) = \varepsilon^{i_1}$, where ε is a primitive p^2th root of unity and

$$\lambda^{g^{-j}}(x_1^{i_1}\cdots x_r^{i_r}) = \varepsilon^{i_1 + pl(i_r\binom{j}{1} + i_{r-1}\binom{j}{2} + \cdots + i_1\binom{j}{r})},$$

so $x_1^{i_1}\cdots x_r^{i_r}$ is a zero of χ if and only if the polynomial

$$\psi(x) = i_1\binom{x}{r} + i_{r-1}\binom{x}{r-1} + \cdots + i_r\binom{x}{1}$$

is a permutation polynomial. Since χ has no more zeros in M than those in $\langle x_r, \omega\rangle - \langle\omega\rangle$, we conclude that non-linear permutation polynomials must have degree at least $r+1$, so $r \leq \mathrm{md}(p) - 1$ and $|P| = p^{r+2} \leq p^{\mathrm{md}(p)+1}$. ∎

It is clear from the above proof that the bound obtained is best possible. Actually, with some routine extra work one could classify the p-groups with a faithful character vanishing exactly on $p^2 - 1$ conjugacy classes.

To prove the general bound in Theorem D we need to recall some results from the theory of p-groups of maximal class. If P is such a p-group and $|P| = p^n \geq p^4$, we define the maximal subgroup P_1 as the centralizer in P of P_2/P_4. Then P is called **exceptional** if there exist $i, j \geq 1$ with $i + j \leq n - 1$ and $[P_i, P_j] = P_{i+j}$. Otherwise P is called **non-exceptional**, i.e., when $[P_i, P_j] \leq P_{i+j+1}$ for all $i, j \geq 1$. In the former case, P has exactly $(p-1)^2$ conjugacy classes of size p^{n-2} whereas, in the latter, the number of such classes is $p^2 - p$ (see [3]).

LEMMA 4.5: *Let P be a non-exceptional p-group of maximal class of order $p^n \geq p^4$ and $x \in P_j - P_{j+1}$ for some $1 \leq j \leq n-2$. Then the elements in the coset xP_{j+2} are all conjugate if and only if $C_P(x) = P_{n-j-1}$. Moreover, in that case $n \leq 2j+1$.*

Proof: Let us denote by C the conjugacy class of x. We begin noting that $C \subseteq xP_{j+1}$ but $C \not\subseteq xP_{j+2}$ (because x is central modulo P_{j+1} but not modulo P_{j+2}). The cosets xP_{j+1} and xP_{j+2} have sizes p^{n-j-1} and p^{n-j-2}, respectively and the size of C is also a power of p. Then it is clear that the inclusion $xP_{j+2} \subseteq C$ amounts to the equality $xP_{j+1} = C$. Since one of the inclusions here is always true, we conclude that this equality holds if and only if $|C| = |P_{j+1}|$ or, in terms of centralizers, $|C_P(x)| = p^{j+1}$.

On the other hand, P is non-exceptional so $[x, P_{n-j-1}] \leq [P_j, P_{n-j-1}] \leq P_n = 1$, that is $P_{n-j-1} \leq C_P(x)$ and $|P_{n-j-1}| = p^{j+1}$, so the first part of the lemma follows directly. In particular, under the hypothesis of the lemma, $x \in C_P(x) = P_{n-j-1}$. But $x \in P_j - P_{j+1}$, so $n - j - 1 \leq j$, that is $n \leq 2j+1$. ∎

Proof of Theorem D, general case: Set $K = \mathrm{Ker}\,\chi$, which can be supposed to be non-trivial so that $|P| = p^n \geq p^4$. By the faithful case of this theorem we know that $p^s = |P/K| \leq p^{\mathrm{md}(p)+1}$. The character χ vanishes outside a maximal subgroup M of P and also on at least $p-1$ classes inside M. But the number of classes in $P - M$ is at least $p^2 - p$, so no more classes can exist here and,

in addition, the size of all of them must be p^{n-2}. As indicated before, this can only happen if P is a non-exceptional p-group of maximal class. Viewed as a character of P/K, χ also vanishes on p^2-1 classes so each of them must lift to a single conjugacy class of P, which simply means that all the elements in the coset xK are conjugate if x is a zero of χ. Now we take $x \in P_{s-2} - P_{s-1}$, which modulo K is in $Z_2(P/K) - Z(P/K)$ and so is a zero of χ. Then by the previous lemma we conclude that $|P| \leq p^{2s-3}$ and therefore, $|P| \leq p^{2\,\mathrm{md}(p)-1}$ because $s \leq \mathrm{md}(p)+1$. ∎

In the next example we construct p-groups for $p \geq 5$ which possess non-faithful irreducible characters vanishing on p^2-1 conjugacy classes. However, they do not prove that the general bound in Theorem D is best possible.

Example 4.6: Let r be an odd number with $r \leq \mathrm{md}(p)$. We claim that there exists a p-group P of order p^{r+2} with an irreducible character χ such that its kernel has order p and it vanishes on p^2-1 classes. We start with the group $H = \langle g \rangle \ltimes A$, the semidirect product between the elementary abelian group $A = \langle x_1, \ldots, x_r \rangle$ of rank r and the cyclic group $\langle g \rangle$ of order p, where the action is given by $x_i^g = x_i x_{i+1}$ ($x_{r+1} = 1$). Then all we need is a non-exceptional group of maximal class P of order p^{r+2} such that P/P_{r+1} is isomorphic to H and $[P_{r-1}, P_1] = P_{r+1}$ (this is simply a reformulation of the condition that all the classes in $Z_2(P/P_{r+1}) - Z(P/P_{r+1})$ lift to unique classes in P). Instead of trying to find such a group it is easier to construct a Lie algebra over $\mathbb{F}_p$ of maximal class $\mathcal{L}$ of dimension $r+2$ such that $[\mathcal{L}_i, \mathcal{L}_j] \leq \mathcal{L}_{i+j+1}$ for all $i, j \geq 1$, $[\mathcal{L}_{r-1}, \mathcal{L}_1] = \mathcal{L}_{r+1}$ and $\mathcal{L}/\mathcal{L}_{r+1}$ has a basis $e_1, \ldots, e_r, f$ satisfying the relations $[e_i, e_j] = 0$ and $[e_i, f] = e_{i+1}$ ($e_{r+1} = 0$). Of course, the ideals $\mathcal{L}_i$ are defined similarly to the subgroups P_i but in the context of Lie algebras. Then the p-group P corresponding to $\mathcal{L}$ under the Lazard correspondence satisfies all the conditions required. Note that Lazard's correspondence can be used since the nilpotence class of $\mathcal{L}$ should be $r+1 \leq \mathrm{md}(p)+1 \leq p-1$.

To construct our Lie algebra $\mathcal{L}$ we consider a vector space with a basis $e_1, \ldots, e_r, \omega, f$ and define a Lie product by setting $[e_i, e_{r-i}] = (-1)^i \omega$, $[e_i, f] = e_{i+1}$ for $1 \leq i < r$ and $[e_r, f] = \omega$ (the rest of the products among the generators are defined to be zero). To check that this actually defines a Lie algebra structure, notice first that the relations for $e_1, \ldots, e_r, \omega$ define a Lie algebra structure of nilpotence class 2 (the relations are consistent because r is odd) and f acts on it as a derivation.

Since we have proved that $\mathrm{md}(p)$ is the smallest prime that does not divide $p-1$ for almost all p, this example shows for almost all primes we cannot

remove the hypothesis that the character is faithful if we want to obtain the bound $|P| \leq p^{\mathrm{md}(p)+1}$.

Unfortunately, we have been unable to settle the following question for $p \geq 5$.

QUESTION 4.7: *What is the smallest integer $n = n(p)$ such that there are p-groups of arbitrarily large order with an irreducible character with n conjugacy classes of zeros?*

Our results show that $p^2 - 1 < n(p) \leq (p-1)! + p^2 - p$.

5. Bounding the order of a p-group P in terms of $m(P)$

In this section we show that the order of a p-group can be bounded if **all** its irreducible characters vanish on at most a fixed number of classes. We need one lemma. Recall that if P is a p-group, the **cobreadth** of P is defined as $\mathrm{cb}(P) = \min_{x \in P} |C_P(x)|$.

LEMMA 5.1: *The cobreadth of a p-group P cannot exceed $2n(P)$.*

Proof: Write $|P| = p^n$ and let $\chi \in \mathrm{Irr}(P)$ be non-linear. As before, there exists a (normal) subgroup M of index p in P such that χ is induced from some character of M. In particular, χ vanishes on the $p^n - p^{n-1}$ elements of $P - M$. Since χ vanishes on $m(\chi)$ conjugacy classes, we deduce that the number of conjugacy classes of $P - M$ cannot exceed $m(\chi)$. Thus, the average size of the conjugacy classes of P contained in $P - M$ is at least $(p^n - p^{n-1})/m(\chi)$ and the same thing must happen for the size of one of these classes. This means that for some element in $P - M$ the order of the centralizer is at most $\frac{p}{p-1} m(\chi) \leq 2m(\chi)$ and the result follows directly. ∎

Finally, we show that the order of a non-abelian p-group P can be bounded in terms of $m(P)$.

Proof of Theorem B: Let φ be an irreducible character of P of maximal degree among all the irreducible characters. By Theorem 12.26 of [13], there exists an abelian subgroup B of P of index at most $\varphi(1)^4$. By Theorem 5.1 of [22], we have that P has a normal abelian subgroup of index at most $\varphi(1)^8$. By Theorem C the degree of φ is bounded by a function of $m(\varphi)$, so P has an abelian normal subgroup with index bounded by a function of the number of classes of zeros of an irreducible character of maximal degree and consequently also by a function of $m(P)$.

Let A be an abelian normal subgroup of P of maximal order and notice that, by the preceding discussion, the index of A is bounded by a function of $m(P)$.

Put $K = [A, P]$. Since A is not central, we have that $K > 1$ and we can take a maximal subgroup L of K such that $L \trianglelefteq P$. Set $Z/L = Z(P/L)$. Since $K > L$, we have that $A \cap Z < A$. Also, since K/L has order p, $K \leq A \cap Z$. We write $\overline{P} = P/L$ and use the bar convention. Note that $\overline{A} \leq Z_2(\overline{P})$. Thus

$$[\overline{A}^p, \overline{P}] = [\overline{A}, \overline{P}]^p = \overline{K}^p = \overline{1}$$

and we deduce that $A/(A \cap Z)$ has exponent p.

By Lemma 5.1 there exists $x \in P$ such that $|C_P(x)|$ is bounded by some function of $m(P)$. We can view x as an automorphism of A, and viewed as such an automorphism its order cannot exceed $|P : A|$, which is bounded in terms of $m(P)$. It follows that the rank of A is bounded by some function that depends only on $m(P)$ (by Corollary 2.7 of [16], for instance). Since $A/(A \cap Z)$ has exponent p, this means that the order of $A/(A \cap Z)$ is similarly bounded and the same thing happens for the index $|P : A \cap Z|$.

Let N be a normal subgroup of P such that $N \leq A$ and $|N/A \cap Z| = p$. Note that $|P : N|$ is bounded in terms of $m(P)$. Pick $x \in N - (A \cap Z)$ and put $C/L = C_{\overline{P}}(\overline{x})$. Since x is not central modulo L, we have that $\overline{1} \neq [\overline{x}, \overline{P}] \leq \overline{K}$, whence $[\overline{x}, \overline{P}] = \overline{K}$ has order p.

Since N is not contained in Z, P does not act trivially on N/L and does not act trivially on $\mathrm{Irr}(N/L)$ either. Let λ be an irreducible character of N/L that is not P-invariant. Since N/K is central in P/K, we deduce that $\mu = \lambda_{K/L} \neq 1_{K/L}$.

Now, let $\chi \in \mathrm{Irr}(P|\lambda), y \in N - (A \cap Z)$ and $g \in P$ such that $[g, y] \notin L$. Then

$$\chi(y) = \chi(y^g) = \chi(y)\mu([g, y])$$

and it follows that $\chi(y) = 0$.

Write $|N| = p^k$. Since A is abelian the size of any conjugacy class contained in N cannot exceed $|P : A|$. We have then that

$$\frac{p^k - p^{k-1}}{|P : A|} \leq k_P(N - (A \cap P)) \leq m(\chi) \leq m(P),$$

and we deduce that $p^k - p^{k-1}$ is bounded in terms of $m(P)$. This implies that k is bounded in terms of $m(P)$. Since p and $|P : N|$ are also bounded in terms of $m(P)$, the result follows. ∎

6. Bounding the derived length

First, we prove Theorem E. This is an immediate consequence of the following theorem of A. Shalev.

THEOREM 6.1: *The derived length of a p-group is bounded in terms of the cobreadth.*

Proof: This is Theorem A′ of [26]. The proof there also gives an explicit bound. ∎

Proof of Theorem E: This follows from Lemma 5.1 and Shalev's Theorem. ∎

Our next result shows that it is not possible to extend Theorem E to solvable groups. It also shows that it is not possible to bound $|G : F(G)|$ in terms of $n(G)$.

THEOREM 6.2: *For any integers m and l, there exists a monomial group G with a Sylow tower and $\chi \in \mathrm{Irr}(G)$ such that $\mathrm{dl}(G) > m$, $|G : F(G)| > l$ and χ vanishes just on one conjugacy class of G.*

Proof: Let n be an integer such that the derived length of the group $U = U_n(q)$ of upper unitriangular matrices of size n over the finite field with q elements is greater than m (n doesn't actually depend on q). Let $r \geq \max\{l, n\}$ be a prime number and $\overline{a}$ a generator of the group of units $\mathcal{U}(\mathbb{Z}/r\mathbb{Z})$. By Dirichlet's Theorem, there exists a prime of the form $p = a + kr$ for some positive integer k. Thus we have $\mathcal{U}(\mathbb{Z}/r\mathbb{Z}) = \langle \overline{p} \rangle$. Let $q = p^{r-1}$. Since $q \equiv 1 \pmod{r}$, $F = \mathbb{F}_q$ contains r different rth roots of unity. We choose n such roots $\zeta_1 = 1, \zeta_2 = \zeta, \zeta_3, \ldots, \zeta_n$. Let σ be the diagonal matrix $\mathrm{diag}(\zeta_1, \ldots, \zeta_n)$. Note that the order of σ is r and that σ acts fixed point freely on U by conjugation. Of course, we can view the semidirect product $L = \langle \sigma \rangle \ltimes U$ as a subgroup of the group of invertible upper triangular matrices $T_n(q)$. The Frobenius automorphism of F induces an automorphism ψ of L of order $r - 1$. Put $G = \langle \psi \rangle \ltimes L$.

It is clear that G has a Sylow tower. Now we want to see that G is an M-group. First, we define certain subgroups of U. For every $1 \leq i < j \leq n$, let $H_{i,j}$ be the subgroup of U formed by the matrices whose non-diagonal entries in the first $j - 1$ columns and in the last $n - i$ rows of the jth column are zero, the rest of the entries above the diagonal being arbitrary. (Note that $H_{1,2} = U$.) Conveniently ordered, the subgroups $H_{i,j}$ form an increasing sequence of F-algebra groups (see [14] for the definition of an algebra group) and adding the

subgroups 1, L and G we obtain a series of normal subgroups of G. By Theorem A of [14], the restriction of a character of some subgroup $H_{i,j}$ to the preceding one in the normal series is either irreducible or splits as the sum of q different irreducible characters. Since G/L is cyclic and L/U has prime order, we can refine our normal series to a normal series where all the consecutive quotients between U and G have prime order. In particular, it also holds for these terms that the restriction of a character to the preceding subgroup is either irreducible or the sum of different irreducible characters. Now we can apply Lemma 1.2 of [27] to deduce that G is an M-group.

Write $C = \langle \psi \rangle$ and $S = \langle \sigma \rangle$, so that $G = CSU$. Since C acts Frobenius on S and S acts Frobenius on U, there exists a unique conjugacy class of elements of order r and all other elements of G are r'-elements. Thus, it suffices to show that there exists a non-linear character $\chi \in \mathrm{Irr}(G)$ such that $\chi(x) \neq 0$ for any r'-element x. Actually, we shall find χ as a character of the group $J = G/H_{2,3}$. Note that all we need to worry about is that χ does not vanish on the r'-elements of J, since then this condition will be automatically satisfied by the r'-elements of G.

We can identify J with CSF, where the action of σ on F is given by multiplication by $\zeta_2 = \zeta$. Let $H = CF$ and $N = SF$. Write $F = P \times Q$, where P is the prime subfield of F and let $\lambda = \delta \times 1_Q$, where δ is a non-principal linear character of P. Since S acts Frobenius on F and C fixes P, we deduce that $I_J(\lambda) = H$. Now, λ extends to H and then induces to an irreducible character χ of J. By Lemma 2.1 of [21], for instance, we know that $\chi(x) \neq 0$ for all $x \in F$. Also, either by an easy calculation or by Theorem 13.6 of [13], one can see that χ does not vanish on any of the elements of $H - F$. This means that χ does not vanish on any element of the Hall r'-subgroup H and so it does not vanish on any r'-element at all, which is what we needed. ∎

Now we show that Conjecture F holds for supersolvable groups. Since in a supersolvable group G the quotient $G/F(G)$ is abelian, there is an irreducible character that is induced from some character of $F(G)$ (by Proposition 19.17 of [12]). In particular, it vanishes on $G - F(G)$. Now, it is clear that $G - F(G)$ has at least $|G : F(G)| - 1$ conjugacy classes of G and it follows that $|G : F(G)| \leq m(G) + 1$. So we just need to bound the derived length. In order to achieve this, we need the following result. Given an integer n, $\omega(n)$ is the number of prime divisors (counting multiplicities) of n and for any group G, we define $\omega(G) = \max\{\omega(\chi(1)) \mid \chi \in \mathrm{Irr}(G)\}$.

THEOREM 6.3: *Let G be a supersolvable group. There exist constants E_1 and*

E_2 such that $\mathrm{dl}(G) \leq E_1 \log \omega(G) + E_2$.

Proof: Since G is supersolvable, we have that $G' \leq F(G)$. There exist a prime p and $P \in \mathrm{Syl}_p(F(G))$ such that $\mathrm{dl}(P) = \mathrm{dl}(F(G))$. Let p^n be the largest degree of the irreducible characters of P. As we have done already in the proof of Theorem B, P has a normal abelian subgroup A of index at most p^{8n}. Thus the derived length of P/A is logarithmically bounded in terms of n (using a well-known theorem of P. Hall). Since $n \leq \omega(G)$ and $\mathrm{dl}(G) \leq \mathrm{dl}(P) + 1$, the result follows. ∎

PROPOSITION 6.4: *Let G be a supersolvable group. There exist constants C_1 and C_2 such that*

$$\mathrm{dl}(G) \leq C_1 \log m(G) + C_2.$$

Proof: First note that the argument in Lemma 3.1 proves that if G is a supersolvable group and $H \leq G$ has index n, then $k_G(G - \bigcup_{g \in G} H^g) \geq \omega(n)$. Now, using the fact that supersolvable groups are M-groups, we have that $m(\chi) \geq \omega(\chi(1))$ for any $\chi \in \mathrm{Irr}(G)$, so $m(G) \geq \omega(G)$ and the result follows from the previous theorem. ∎

In view of this proof, it would suffice to obtain a lower bound for $k_G(G - \bigcup_{g \in G} H^g)$ in terms of $\omega(|G : H|)$ in order to obtain a bound for the derived length of an M-group G by $m(G)$. However, this is not possible. One can take the semilinear group $G = \Gamma(q)$ for any power q of a prime p and H a Hall p'-subgroup of G. Since G is a Frobenius group there is only one conjugacy class of non-identity elements disjoint with H. However, it might be true that such a bound exists if we assume in addition that a (linear) character of H induces irreducibly to G, but we have been unable to prove this.

Next we prove Theorem H. Note that a consequence of Theorem H is that if $m(G) = 2$ and G is solvable then $\mathrm{dl}(G) \leq 3$.

Proof of Theorem H: It is not difficult to check that if G belongs to one of the families (i)–(v), then $m(G) = 2$. Conversely, suppose that $m(G) = 2$. By Theorem 1.1 of [2], we may assume that there exist A and Z both of them of order at most 2 such that $G/Z = A \ltimes F$, where F is a Frobenius group with complement of order 3 and nilpotent kernel of class ≤ 2. We want to see that G is the symmetric group S_4 or a Frobenius group with complement of order 3 and abelian kernel.

First, suppose that the Fitting height of G is greater than 2. Then Lemma 5 of [24] yields that $G \cong S_4$, so we may assume that G is metanilpotent.

Write $F = C \ltimes K$, with $C = \langle x \rangle$ cyclic of order 3 and K nilpotent of class ≤ 2. Put $J = AF = ACK$. Note that A acts trivially on C. We want to prove that $A = 1$ and K is abelian.

Suppose first that K is not abelian. Let H be a maximal subgroup of K' normal in K and let $\mu \in \mathrm{Irr}(K/H)$ with $\mu(1) > 1$. Write $Y/H = Z(K/H)$. It is clear that $|K : Y| \geq 4$. By Theorem 7.5 of [12], μ vanishes on $K - Y$. Since F is a Frobenius group, $\varphi = \mu^F \in \mathrm{Irr}(F)$. Assume first that φ extends to an irreducible character χ of J. Then $\chi_K = \mu + \mu^x + \mu^{x^2}$ vanishes on $K - \bigcup_{i=0}^{2} Y^{x^i}$, which is a non-empty set. Since χ also vanishes on the two conjugacy classes that make up $F - K$, we deduce that $m(\chi) > 2$, a contradiction.

Thus, we may assume that $A > 1$ and $\varphi^J \in \mathrm{Irr}(J)$. But now we have that $m(\varphi^J) \geq k_J(J - K) > 2$, another contradiction. We deduce that K is abelian.

Next, we prove that A acts trivially on K. Otherwise, there exists a linear character μ of K whose inertia group in AK is K. Since CK is Frobenius, we have that the inertia group of μ in CK is K too. We conclude that $\mu^J \in \mathrm{Irr}(J)$ and vanishes on $J - K$. Since this normal subset has more than two conjugacy classes, we have reached another contradiction. This means that $J = A \times F$. Now, $m(J) = 2$ implies that $A = 1$.

We have that G/Z is a Frobenius group with complement of order 3 and abelian kernel. Take a non-linear irreducible character ψ of G/Z and gZ an element of any of the two conjugacy classes of zeros of ψ. Then gZ splits into $|Z|$ conjugacy classes of zeros of ψ when viewed as a character of G. Hence, we have that $Z = 1$ and G belongs to the family (v), as desired. ∎

7. Bounding the Fitting height

We begin with the proof of Theorem A. We need the following results.

THEOREM 7.1: *Let G be a solvable group. Then there exists $\mu \in \mathrm{Irr}(F_{10}(G))$ such that $\mu^G \in \mathrm{Irr}(G)$. Furthermore, if $|G|$ is odd, then there exists $\tau \in \mathrm{Irr}(F_3(G))$ such that $\tau^G \in \mathrm{Irr}(G)$ and if $\lambda \in \mathrm{Irr}(F(G))$ lies under τ, then $\lambda^{F_2(G)} \in \mathrm{Irr}(F_2(G))$.*

Proof: These are Theorems C and D of [20]. ∎

If a group G acts on a module V, we write $r(G, V)$ to denote the number of orbits of the action of G on V.

THEOREM 7.2: *Assume that a solvable group G acts faithfully and completely reducibly on a finite module V. Then $\mathrm{dl}(G) \leq D_1 \log\log r(G,V) + D_2$ for some constants D_1 and D_2.*

Proof: If G acts irreducibly on V, then this is Theorem 2.4 of [15]. Thus, we may assume that $V = V_1 \oplus V_2$ for non-trivial G-modules V_1 and V_2. Arguing by induction on $|GV|$, we deduce that

$$\begin{aligned}\mathrm{dl}(G) &= \max\{\mathrm{dl}(G/C_G(V_1)), \mathrm{dl}(G/C_G(V_2))\}\\ &\leq \max\{D_1 \log\log r(G/C_G(V_1), V_1) + D_2,\\ &\qquad D_1 \log\log r(G/C_G(V_2), V_2) + D_2\}\\ &\leq D_1 \log\log r(G,V) + D_2,\end{aligned}$$

as desired. ∎

The following result is Theorem A.

THEOREM 7.3: *Let G be a solvable group. Then $|G : F_{10}(G)|$ is bounded in terms of $m(G)$ and there exist real numbers C_1 and C_2 such that*

$$h(G) \leq C_1 \log\log m(G) + C_2.$$

Furthermore, if $|F_{10}(G)|$ is odd then $|G : F(G)|$ is bounded in terms of $m(G)$.

Proof: First, we assume that G is an arbitrary solvable group. Certainly, we may assume that $F_{10}(G) < G$. By Theorem 7.1, there exists $\chi \in \mathrm{Irr}(G)$ such that $\chi(x) = 0$ for all $x \in G - F_{10}(G)$. Hence, we have that

$$m(G) \geq k_G(G - F_{10}(G)) \geq k(G/F_{10}(G)) - 1$$

and the first assertion follows from [23].

Now, we write $\overline{G} = G/F_{10}(G)$. By Gaschutz's Theorem (see [11]),

$$H = \overline{G}/F(\overline{G}) \cong G/F_{11}(G)$$

acts faithfully and completely reducibly on $V = F(\overline{G})/\Phi(\overline{G})$. It is clear that

$$k(\overline{G}) \geq k(\overline{G}/\Phi(\overline{G})) \geq r(H,V).$$

We deduce that $m(G) \geq r(H,V) - 1$. Using Theorem 7.2, we have that

$$\begin{aligned}h(G) &= h(G/F_{11}(G)) + 11 \leq \mathrm{dl}(H) + 11 \leq D_1 \log\log r(H,V) + D_2 + 11\\ &\leq D_1 \log\log(m(G)+1) + D_2 + 11 \leq D_1 \log\log m(G) + D_2'.\end{aligned}$$

Finally, we assume that $|F_{10}(G)|$ is odd and we want to bound $|G : F(G)|$. By Theorem 7.1, there exists $\chi_1 \in \mathrm{Irr}(G)$ such that $\chi_1(x) = 0$ for all $x \in G - F_{10}(G)$. Applying Theorem 7.1 to $F_{10}(G)$ and $F_{10}(G)/F(G)$, we can find characters $\varphi_2, \varphi_3 \in \mathrm{Irr}(F_{10}(G))$ such that $\varphi_2(x) = 0$ for all

$$x \in (F_{10}(G) - F_3(G)) \cup (F_2(G) - F(G))$$

and $\varphi_3(x) = 0$ for all $x \in F_3(G) - F_2(G)$. If we take $\chi_2 \in \mathrm{Irr}(G|\varphi_2)$ and $\chi_3 \in \mathrm{Irr}(G|\varphi_3)$, we can conclude that for all $x \in G - F(G)$ at least one of the three characters χ_1, χ_2 or χ_3 vanishes at x. Now, it suffices to argue as in the first paragraph to complete the proof of the theorem. ∎

We conclude with the proof of the following special case of Conjecture G.

THEOREM 7.4: *Let χ be an irreducible character of a solvable group G with exactly one conjugacy class of zeros. Then the Fitting height of G does not exceed* 5.

Proof: Let N be the normal subgroup of G generated by the conjugacy class of zeros of χ. By [28], we know that G/N' is a doubly transitive Frobenius group whose kernel is N/N'. Also, N/N' is an elementary abelian group and N is a Camina group with respect to N'. E. M. Zhmud also proved that the Sylow p-subgroups of N are Camina groups. By [28], their nilpotence class does not exceed 3. Now, we can use Theorem 3 of [5] to deduce that the Fitting height of N is at most 2.

We have that G/N acts transitively on the non-trivial elements of N/N' and using Theorem 6.8 of [19], we deduce that the Fitting height of G/N is at most 3. Thus, $h(G) \leq 5$, as desired. ∎

References

[1] Y. Berkovich and L. Kazarin, *Finite groups in which the zeros of every non-linear irreducible character are conjugate modulo its kernel,* Houston Journal of Mathematics **24** (1998), 619–630.

[2] M. Bianchi, D. Chillag and A. Gillio, *Finite groups in which every irreducible character vanishes on at most two conjugacy classes,* Houston Journal of Mathematics **26** (2000), 451–461.

[3] N. Blackburn, *On a special class of p-groups,* Acta Mathematica **100** (1958), 45–92.

[4] D. Chillag, *On zeroes of characters of finite groups*, Proceedings of the American Mathematical Society **127** (1999), 977–983.

[5] D. Chillag, A. Mann and C. M. Scoppola, *Generalized Frobenius groups II*, Israel Journal of Mathematics **62** (1988), 269–282.

[6] S. D. Cohen, *The distribution of polynomials over finite fields*, Acta Arithmetica **17** (1970), 255–271.

[7] P. M. Cohn, *Algebra*, Vol. 1, Wiley, New York, 1982.

[8] R. Dark and C. M. Scoppola, *On Camina groups of prime power order*, Journal of Algebra **181** (1996), 787–802.

[9] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Dover, New York, 1958.

[10] M. D. Fried, *On a conjecture of Schur*, The Michigan Mathematical Journal **17** (1970), 41–55.

[11] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, 1967.

[12] B. Huppert, *Character Theory of Finite Groups*, deGruyter, Berlin, 1998.

[13] I. M. Isaacs, *Character Theory of Finite Groups*, Dover, New York, 1994.

[14] I. M. Isaacs, *Characters of groups associated with finite algebras*, Journal of Algebra **177** (1995), 708–730.

[15] T. M. Keller, *Orbits in finite group actions*, in *Groups St. Andrews 2001 in Oxford*, Cambridge University Press, Cambridge, 2003.

[16] E. I. Khukhro, *p-Automorphisms of Finite p-Groups*, Cambridge University Press, Cambridge, 1998.

[17] D. B. Leep and C. C. Yeomans, *The number of points on a singular curve over a finite field*, Archiv der Mathematik **63** (1994), 420–426.

[18] R. Lidl, G. L. Mullen and G. Turnwald, *Dickson Polynomials*, Wiley, New York, 1993.

[19] O. Manz and T. R. Wolf, *Representations of Solvable Groups*, Cambridge University Press, Cambridge, 1993.

[20] A. Moretó and T. R. Wolf, *Orbit sizes, character degrees and Sylow subgroups*, Advances in Mathematics, to appear.

[21] G. Navarro, *Zeros of primitive characters in solvable groups*, Journal of Algebra **221** (1999), 644–650.

[22] K. Podoski and B. Szegedy, *Bounds in groups with finite abelian coverings or with finite derived groups*, Journal of Group Theory **5** (2002), 443–452.

[23] L. Pyber, *Finite groups have many conjugacy classes*, Journal of the London Mathematical Society **46** (1992), 239–249.

[24] G. Qian, *Bounding the Fitting height of a solvable group by the number of zeros in a character table*, Proceedings of the American Mathematical Society **130** (2002), 3171–3176.

[25] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois Journal of Mathematics **6** (1962), 64–94.

[26] A. Shalev, *On almost fixed point free automorphisms*, Journal of Algebra **157** (1993), 271–282.

[27] B. Szegedy, *On the characters of the group of upper-triangular matrices*, Journal of Algebra **186** (1996), 113–119.

[28] E. M. Zhmud, *On finite groups having an irreducible character with one class of zeros*, Soviet Mathematics Doklady **20** (1979), 795–797.