THE CHARACTER DEGREES AND NILPOTENCE CLASS OF A p-GROUP

by
I. M. Isaacs

Mathematics Department
University of Wisconsin
480 Lincoln Drive
Madison WI 53706
USA

E-mail: isaacs@math.wisc.edu

and

Alexander Moretó
Departamento de Matematicas
Universidad del País Vasco
Apartado 644
48080 Bilbao
SPAIN
E-mail: mtbmoqua@lg.ehu.es

Research support:

First author: The United States National Security Agency.
Second author: The Basque Government and the University of the Basque Country.

1. Introduction.

Let P be a finite p-group, where p is some prime number. As usual, we write $\mathrm{cd}(P)$ to denote the set of degrees of the irreducible complex characters of P and we note that $\mathrm{cd}(P)$ is a set of powers of p that contains the number 1. The converse of this statement is also true: If $\mathcal{S}$ is an arbitrary set of powers of the prime number p, subject only to the condition that $1 \in \mathcal{S}$, then there is some finite p-group P such that $\mathrm{cd}(P)$ is exactly the set $\mathcal{S}$. In fact, it is always possible to choose P so that its nilpotence class $c(P)$ does not exceed 2. This theorem of the first author is the main result of [**1**].

A more subtle question is whether or not the given set $\mathcal{S}$ of powers of p can occur as $\mathrm{cd}(P)$ for some p-group P having *large* nilpotence class. It is known, for example, that for each prime p, there exist p-groups P of unboundedly large nilpotence class such that $\mathrm{cd}(P) = \{1, p\}$. On the other hand, if $\mathrm{cd}(P) = \{1, p^2\}$, then the nilpotence class of P is bounded, and in fact, $c(P) \leq p$. More generally, if $\mathrm{cd}(P) = \{1, p^e\}$, where $e > 1$ is arbitrary, then also $c(P) \leq p$. (These results appear in [**5**].)

Now suppose that $\mathcal{S}$ is an arbitrary set of powers of p such that $1 \in \mathcal{S}$. We shall say that $\mathcal{S}$ is a **class-bounding set** if there is some integer n (depending on $\mathcal{S}$) such that $c(P) \leq n$ for every p-group P with $\mathrm{cd}(P) = \mathcal{S}$. For example, by the results mentioned in the previous paragraph, we see that if $|\mathcal{S}| = 2$, then $\mathcal{S}$ is class bounding precisely when $p \notin \mathcal{S}$ and, of course, if $|\mathcal{S}| = 1$, then $\mathcal{S} = \{1\}$ and $\mathcal{S}$ is trivially class bounding because $\mathrm{cd}(P) = \mathcal{S}$ only when P is abelian.

It is easy to construct large sets that can be proved to be *not* class bounding. For example, if e is any positive integer, then the set $\mathcal{S}_e = \{1, p, p^2, p^3, \ldots, p^e\}$ is never class bounding. This is because this set is $\mathrm{cd}(P)$ for every p-group P that is a direct product of e groups, each having degree set $\{1, p\}$. As we mentioned previously, however, such groups can have arbitrarily large nilpotence class, and this shows that $\mathcal{S}_e$ is not class bounding, as we claimed.

But sets that can be proved to be class bounding are harder to find. In fact, we believe that up to now, the only known class-bounding sets are those of cardinality at most two. The main results of this paper, however, allow us to construct degree-bounding sets with arbitrarily large cardinality.

THEOREM A. *Fix a prime p and an integer $a > 1$ and let P be a p-group such that p^a is the smallest member of $\mathrm{cd}(P)$ exceeding 1. If the largest member of $\mathrm{cd}(P)$ does not exceed p^{2a}, then the nilpotence class of P is bounded above by some function of p and a.*

Thus, for example, the sets $\{1, p^2, p^3\}$, $\{1, p^2, p^4\}$ and $\{1, p^2, p^3, p^4\}$ are class bounding, as is any set of the form $\mathcal{S} = \{1, p^a\} \cup \mathcal{T}$, where $a > 1$ and $\mathcal{T}$ is any subset of $\{p^{a+1}, p^{a+2}, \ldots, p^{2a}\}$.

Another way to build class-bounding sets of large cardinality is to use the following result.

THEOREM B. *Let $\mathcal{S}$ be a class-bounding set and let b be a power of p exceeding the square of the largest member of $\mathcal{S}$. Then $\mathcal{S} \cup \{b\}$ is also class bounding provided that this set does not contain p.*

In particular, Theorem B provides an alternative proof that the set $\{1, p^e\}$ is class bounding if $e > 1$.

Our proofs of Theorems A and B rely on special properties enjoyed by p-groups P such that $p \notin \mathrm{cd}(P)$. In particular, the following result shows that to bound the nilpotence class of such a group in terms of its irreducible character degrees, it suffices to bound the nilpotence class of its derived subgroup P'.

THEOREM C. *Let P be a p-group such that $p \notin \mathrm{cd}(P)$. Then $c(P) < Kc(P') + M$, where K and M are integers depending only on $b(P)$, the largest irreducible character degree of P.*

Our results are motivated by the paper **[6]**, in which M. C. Slattery considered p-groups satisfying a condition on character degrees similar to (but slightly stronger than) the hypothesis in our Theorem A. Under the additional assumption that the derived subgroup is abelian, he showed that the nilpotence class of such a group is bounded. Although in our Theorem A, we obtain a bound on the nilpotence class without any assumption on the derived subgroup, our Theorem C is consistent with Slattery's idea that the structure of the derived subgroup of a p-group is relevant to the problem of bounding its nilpotence class in terms of its character degrees.

It is tempting to conjecture that a set $\mathcal{S}$ of powers of p is class bounding if and only if it does not contain p, and as we have seen, this is indeed true if $|\mathcal{S}| \leq 2$. We can now push this a bit further.

THEOREM D. *Let $\mathcal{S}$ be a set of three powers of the prime p, where $1 \in \mathcal{S}$. Then $\mathcal{S}$ is class bounding if and only if $p \notin \mathcal{S}$.*

We mention that in contrast with the situation for the nilpotence class, the derived length $\mathrm{dl}(P)$ of a p-group P is always bounded in terms of the set $\mathrm{cd}(P)$ of its irreducible character degrees. In fact, since all p-groups are monomial groups, it follows from Taketa's theorem that $\mathrm{dl}(P) \leq |\mathrm{cd}(P)|$. (See Theorem 5.12 of **[2]**.) Unlike the situation with derived length, however, there definitely does not exist a function $f(n)$, independent of the prime p, such that if P is a p-group and $p \notin \mathrm{cd}(P)$, then $c(P) \leq f(|\mathrm{cd}(P)|)$. (By Example 3.9 of **[5]**, there exists for each prime p a p-group P such that $c(P) = p$ and $\mathrm{cd}(P) = \{1, p^e\}$ for every integer $e > 1$.) It may be true, however, that $c(P)$ is bounded by some function of p and $|\mathrm{cd}(P)|$ whenever $p \notin \mathrm{cd}(P)$, but there is very little evidence for this.

The condition that $p \notin \mathrm{cd}(P)$ seems very strong, and so one might ask if in that case there is an upper bound for the nilpotence class $c(P)$ that depends only on p and is otherwise independent of $\mathrm{cd}(P)$. In fact, for each prime p, the nilpotence class of such a group can be unboundedly large. To see this, let F be a field of order $q = p^e$ and let P be the full Sylow p-subgroup of $GL(n, q)$. Then by the main result of **[3]**, we know that $\mathrm{cd}(P)$ consists of powers of q, and so $p \notin \mathrm{cd}(P)$ if $e > 1$. It is well known, however, that $c(P)$ is unboundedly large for large n.

We close this introduction by thanking the institutions where each of us was a visitor while doing some of his work on this paper. The first author was at the Institute for Experimental Mathematics in Essen, Germany and the second author was at the Mathematics Department of the University of Wisconsin, Madison. The hospitality of both hosts is much appreciated.

2. Theorem C.

In this section, we consider p-groups that lack an irreducible character of degree p, and we work toward a proof of Theorem C. The key is the following easy observation.

(2.1) LEMMA. *Suppose that P is a p-group and that $p \notin \mathrm{cd}(P)$. Let $L \lhd P$ with P/L cyclic. Then $L' = P'$.*

Proof. Of course, $L' \subseteq P'$, and so we work to prove the reverse containment. By replacing P with P/L', we can assume that L is abelian, and our goal is to prove that P is abelian. Otherwise, choose $K \lhd P$, maximal with the property that P/K is nonabelian. Then $(P/K)'$ is the unique minimal normal subgroup of P/K and it follows that $|(P/K)'| = p$. We deduce from this that P/Z is elementary abelian, where $Z/K = \mathbf{Z}(P/K)$.

Since L/K is abelian and Z/K is central in P/K, we see that LZ/K is abelian. Also, P/LZ is both cyclic and elementary abelian, and hence $|P : LZ| \leq p$. Since P/K is nonabelian and has an abelian subgroup of index at most p, it follows that P/K has an irreducible character of degree p. This is a contradiction, and we conclude that P is abelian, as required. ∎

We use the notation $P^1 = P$, $P^2 = [P, P]$ and in general, $P^{i+1} = [P^i, P]$ for $i \geq 1$. The subgroups P^i are thus the terms of the lower central series of P and it is well known that $[P^n, P^m] \subseteq P^{n+m}$ for all integers $m, n \geq 1$. The nilpotence class $c(P)$ is the unique integer k such that $P^k > 1$ but $P^{k+1} = 1$.

The following general fact appears as Lemma 2.1 of **[6]**, but we provide the (short) proof here for the convenience of the reader.

(2.2) LEMMA. *Let P be any group and suppose that $L \lhd P$ and $L' = P'$. Then $P^n = L^n$ for all integers $n \geq 2$.*

Proof. By hypothesis, we have $P^2 = P' = L' = L^2$, and so working by induction on n, we can assume that $n \geq 3$. Clearly, $L^n \subseteq P^n$, and so it suffices to prove the reverse containment. We have

$$P^n = [P^{n-1}, P] = [L^{n-1}, P] = [L^{n-2}, L, P]\,,$$

where the second equality follows by the inductive hypothesis. We want to show that $P^n \subseteq L^n$, and so since $L^n \lhd P$, it suffices by the three subgroups lemma to show that $[P, L^{n-2}, L] \subseteq L^n$ and that $[L, P, L^{n-2}] \subseteq L^n$.

We have

$$[P, L^{n-2}, L] \subseteq [P, P^{n-2}, L] = [P^{n-1}, L] = [L^{n-1}, L] = L^n\,,$$

as desired. Also,

$$[L, P, L^{n-2}] \subseteq [P', L^{n-2}] = [L', L^{n-2}] = [L^2, L^{n-2}] \subseteq L^n\,,$$

and this completes the proof. ∎

Next, we work in the group ring $\mathbb{Z}F$, where F is an arbitrary finite p-group. If $X \subseteq F$, we write $\hat{X}$ to denote the element of $\mathbb{Z}F$ obtained by adding the elements of X.

(2.3) LEMMA. *Let F be a p-group and let S be the additive subgroup of the group ring $\mathbb{Z}F$ generated by all elements of the form $\hat{E}$, where E runs over the subgroups of F such that F/E is cyclic. If $X \subseteq F$ is any subgroup such that F/X is abelian, then $|F:X|\hat{X} \in S$. In fact, if X is proper in F, then $(|F:X|/p)\hat{X} \in S$.*

Proof. We proceed by induction on the index $|F:X|$. If F/X is cyclic, then $\hat{X}$ is one of the generating elements of S and there is nothing further to prove. We can assume, therefore, that F/X is not cyclic, and hence there exists a subgroup $A \subseteq F$ such that $X \subseteq A$ and A/X is elementary of order p^2. If Y/X is any one of the $p+1$ subgroups of order p in A/X, then $|F:Y| < |F:X|$ and the inductive hypothesis applies. Since $Y < F$, we conclude that $n\hat{Y} \in S$, where $n = |F:Y|/p = |F:A|$. Now $\hat{A} = t - p\hat{X}$, where t is the sum of the elements $\hat{Y}$ as Y/X runs over the subgroups of order p in A/X. It follows that that $nt \in S$ and by the inductive hypothesis applied to the subgroup A, we also have $n\hat{A} = |F:A|\hat{A} \in S$. We conclude that $np\hat{X} \in S$, and since $np = |F:X|/p$, the proof is complete. ∎

In certain cases, our next result can be used to establish a connection between the exponent and the nilpotence class of a p-group.

(2.4) LEMMA. *Suppose that P acts on A, where P is a p-group and A is abelian of exponent p^e. Then $[A,P,P,\ldots,P] = 1$, where the number of commutations with P is $e|P|$.*

Proof. Proceeding by induction on e, we consider first the case where $e = 1$ so that A is elementary. We must show in this case that $[A,P,P,\ldots,P] = 1$, where there are $|P|$ commutations by P, and we prove this by induction on $|P|$. If $P = 1$, then, of course, $[A,P] = 1$, and there is nothing further to prove. We can assume, therefore, that $P > 1$, and we let Q be a subgroup of index p in P. Write $A_0 = A$, $A_1 = [A,Q]$ and in general $A_i = [A_{i-1},Q]$ if $i > 0$. By the inductive hypothesis, we have $A_{|Q|} = 1$, and since $|P| = p|Q|$, it suffices to show that $[A_i,P,P,\ldots,P] \subseteq A_{i+1}$ for $i \geq 0$, where there are p commutations by P. But Q acts trivially on A_i/A_{i+1}, and so P/Q is a group of order p that acts on A_i/A_{i+1}. It therefore suffices to prove the lemma in the situation where $|P| = p$ (and where we continue to assume that $e = 1$). To do this, we view A as a vector space over a field of order p and we let T be the linear operator on A induced by a generator of P. We see that $[A,P,\ldots,P] = A(T-1)^i$, where there are i commutations by P and $i \geq 0$. Since $(T-1)^p = T^p - 1 = 0$, this completes the proof in the case where $e = 1$.

We can now assume that $e > 1$ and we consider the action of P on $\overline{A} = A/\Phi(A)$. Since $\overline{A}$ has exponent p, it follows by what we have already proved that $[\overline{A},P,P,\ldots,P] = 1$, where there are $|P|$ commutations by P, and thus $[A,P,\ldots,P] \subseteq \Phi(A)$, where again there are $|P|$ commutations by P. But $\Phi(A)$ has exponent p^{e-1}, and so by the inductive hypothesis, $(e-1)|P|$ commutations by P will annihilate $\Phi(A)$. It follows that $e|P|$ commutations by P will annihilate A, and the proof is complete. ∎

(2.5) COROLLARY. *In the situation of Lemma 2.4, we have $[A,P,P,\ldots,P] = 1$, where the number of commutations is $e|P:\mathbf{C}_P(A)|$.*

Proof. Apply Lemma 2.4 to the natural action of $P/\mathbf{C}_P(A)$ on A. ∎

Next, we recall that for any finite group G, there exists an abelian subgroup $A \subseteq G$ with index bounded above by some function of $b = b(G)$, the largest irreducible character

degree of G. (See Theorem 12.23 of [**2**] for this result of the first author and D. S. Passman.) It follows that $\mathrm{core}_G(A)$ is a normal abelian subgroup of G whose index is bounded in terms of b.

At this point, we can prove that $c(P)$ is bounded in terms of $b(P)$ and the maximum of the exponents of abelian normal subgroups of P'. To obtain this easy result, it is not even necessary to assume that $p \notin \mathrm{cd}(P)$.

(2.6) COROLLARY. *Let p^e be the maximum of the exponents of all abelian normal subgroups of P', where P is a p-group. Then the nilpotence class $c(P)$ is bounded in terms of e and $b = b(P)$.*

Proof. Choose an abelian normal subgroup A of P of index bounded by some function of b. Since the order of P/A is bounded in terms of b, so too is its nilpotence class, and it follows that there is some integer M depending only on b such that $P^M \subseteq A$. Since we can certainly assume that $M \geq 2$, it follows that P^M is an abelian normal subgroup of P', and thus its exponent does not exceed p^e. Also, $A \subseteq \mathbf{C}_P(P^M)$, and hence by Corollary 2.5, we know that $1 = [P^M, P, P, \ldots, P] = P^{N+M}$, where there are $N = e|P : A|$ commutations by P. It follows that $c(P) < N + M$, and the result follows. ∎

Finally, we are ready to prove Theorem C.

Proof of Theorem C. As in the proof of Corollary 2.6, we can choose an abelian normal subgroup A of P with index bounded in terms of $b = b(P)$. It follows that there is an integer M depending only on b such that $(P/A)^M = 1$, and for convenience, we assume that $M \geq 2$. We thus have $P^m \subseteq A \cap P'$ for all integers $m \geq M$.

Let $Q = AP'$ and note that if $m \geq M$, then $[P^m, Q] = [P^m, P']$ since A centralizes P^m. (Recall that A is abelian and that $P^m \subseteq A$.) We will show that there exists an integer K, depending only on b, such that $P^{m+K} \subseteq [P^m, Q]$ for all integers $m \geq M$. It follows that $P^{m+2K} \subseteq [P^{m+K}, Q] \subseteq [P^m, Q, Q]$ for integers $m \geq M$ and continuing like this, we deduce that for each positive integer n, we have

$$P^{M+nK} \subseteq [P^M, Q, Q, \ldots, Q] = [P^M, P', P', \ldots, P'] \subseteq (P')^{n+1},$$

where there are n commutations by Q and by P'. (Note that the final containment holds because $P^M \subseteq P'$ since $M \geq 2$.) If we write $N = c(P')$, it follows that $P^{M+NK} = 1$, and thus the nilpotence class $c(P) < M + NK$, as required.

Let $V = P^m/[P^m, Q]$, where $m \geq M$. Then P acts on V and our goal is to find some integer K, depending only on b, such that $[V, P, P, \ldots, P] = 1$, where there are K commutations by P. Since Q acts trivially on V, however, we see that P/Q acts on V and our goal is to show that $[V, P/Q, P/Q, \ldots, P/Q] = 1$, where there are K commutations and K is some integer depending only on b. But $|P/Q| \leq |P/A|$, which is bounded above by some function of b. Since V is abelian, it would suffice by Lemma 2.4 to show that the exponent of V is bounded in terms of b. In fact, it suffices to show that the exponent of $[V, P/Q] = [V, P]$ is bounded in terms of b, and this we proceed to prove.

If $L \lhd P$ with P/L cyclic, then since we are assuming that $p \notin \mathrm{cd}(P)$, we know by Lemmas 2.1 and 2.2 that $P^n = L^n$ for all integers $n \geq 2$. In particular, we have

$$[P^m, L] = [L^m, L] = L^{m+1} = P^{m+1} = [P^m, P].$$

If $\lambda \in \mathrm{Irr}(P^m)$ is fixed by L, then $[P^m, P] = [P^m, L] \subseteq \ker(\lambda)$, and it follows that λ is fixed by all of P.

Write $F = P/A$ and $U = \mathrm{Irr}(P^m)$ and observe that F acts on U since A acts trivially because A is abelian and contains P^m. We view U (written additively) as a $\mathbb{Z}F$-module. If $u \in U$ is arbitrary and $E \subseteq F$, then $u{\cdot}\hat{E}$ is E-invariant, and thus if E is normal in F with a cyclic factor group, it follows from the preceding paragraph that $u{\cdot}\hat{E}$ is F-invariant. This shows that $US \subseteq \mathbf{C}_U(F)$, where S is the additive subgroup of the group ring $\mathbb{Z}F$ generated by elements of the form $\hat{E}$ for normal subgroups E of F with cyclic factors.

Now write $X = Q/A \subseteq F$ and observe that F/X is abelian since $P' \subseteq Q$. By Lemma 2.3, it follows that $|F : X|\hat{X}$ lies in S. If $u \in U$ is X-invariant, then $u{\cdot}\hat{X} = |X|u$, and it follows that

$$|F|u = |F : X||X|u = u{\cdot}|F : X|\hat{X} \in US\,,$$

and so $|F|u$ is F-invariant. Translating this back into the language of the action of P on the linear characters of P^m, we see that if $\lambda \in \mathrm{Irr}(P^m)$ is Q-invariant, then $\lambda^{|P:A|}$ is P-invariant.

Recall that our goal is to show that the abelian group $[V, P]$ has exponent that is bounded in terms of b. We will show, in fact, that this exponent is a divisor of $|P : A|$, which we know is bounded in terms of b. (For notational convenience, we write $|P : A| = e$.) It suffices to show that $[v, g]^e = 1$ for all elements $v \in V$ and $g \in P$. Let λ be an arbitrary linear character of V. Since $V = P^m/[P^m, Q]$, we see that we can view λ as a Q-invariant linear character of P^m, and thus we know that λ^e is P-invariant. Hence $\lambda^e(v) = \lambda^e(v^g)$, and we have $1 = \lambda^e([v, g]) = \lambda([v, g]^e)$. Since λ was arbitrary, it follows that $[v, g]^e = 1$, and thus $[V, P]$ has exponent dividing e, as desired. ∎

In particular, Theorem C tells us that if P is a metabelian p-group and $p \notin \mathrm{cd}(P)$, then the nilpotence class of P is bounded in terms of $b = b(P)$. This improves on the result in **[6]**, where Slattery obtained a bound on the class of a metabelian p-group under much stronger hypotheses on the character degrees. In fact, in this metabelian case, we can sharpen our arguments somewhat to obtain an explicit and relatively small bound. (But it seems probable that this is still far from the best possible result of this type.)

(2.7) THEOREM. *Let P be a metabelian p-group and suppose that $p \notin \mathrm{cd}(P)$. If $b(P) = p^e$, then $c(P) \leq 2 + (e-1)p^e$.*

Proof. We work by induction on $|P|$ and we observe that the hypotheses on P are inherited by homomorphic images P/N, where $N \lhd P$. Since $b(P/N) \leq b(P)$ and the function $2 + (e-1)p^e$ is monotonic in e, it follows that $c(P/N) \leq 2 + (e-1)p^e$ for every nonidentity normal subgroup N. We can assume, therefore, that P has a unique minimal normal subgroup, and thus $\mathbf{Z}(P)$ is cyclic and P has a faithful irreducible character χ. Because P is metabelian, it follows that χ is induced from a linear character of a subgroup $A \supseteq P'$, and since $A \lhd P$, we see that all irreducible constituents of χ_A are linear. But χ is faithful, and so A is abelian and therefore no irreducible character of P has degree larger than $|P : A| = \chi(1)$. In particular, it follows that $|P : A| = b(P)$.

Now we argue as we did in the proof of Theorem C. We observe that if $L \lhd P$ and P/L is cyclic, then $[P', P] = P^3 = L^3 = [L', L] = [P', L]$, and thus P fixes every L-invariant linear character of P'. We let $U = \mathrm{Irr}(P')$, and we view U as a module for the group ring

$\mathbb{Z}F$, where $F = P/A$. Observe that F is abelian since we chose A to contain P'. Also, since we can assume that P is nonabelian, we have $A < P$, and so $F > 1$. If $E \subseteq F$ and F/E is cyclic, then $u\cdot\hat{E}$ is E-invariant, and hence is F-invariant, and thus all members of US are F-invariant, where S is as in Lemma 2.3. We apply Lemma 2.3 to the identity subgroup of F, and we deduce that $|F|u$ is F-invariant for all $u \in U$. In fact, since $1 < F$, we can use the slightly stronger statement in the conclusion of Lemma 2.3 to conclude that $(|F|/p)U$ consists of F-invariant elements.

Write $m = |F|/p$ and recall that $|F| = p^e$ so that $m = p^{e-1}$. From the result of the previous paragraph, we see that if $\lambda \in \mathrm{Irr}(P')$ is arbitrary, then λ^m is P-invariant, and thus $\lambda^m(x) = \lambda^m(x^g)$ for $x \in P'$ and $g \in P$. Thus $1 = \lambda^m([x,g]) = \lambda([x,g]^m)$, and since λ was arbitrary, it follows that $[x,g]^m = 1$, and thus $P^3 = [P', P]$ has exponent dividing $m = p^{e-1}$.

Since A is in the kernel of the action of P on P^3 and $|P/A| = p^e$, it follows by Corollary 2.5 that $[P^3, P, P, \ldots, P] = 1$, where the number of commutations by P is $(e-1)|P : A| = (e-1)p^e$. Thus $P^n = 1$, where $n = 3 + (e-1)p^e$, and it follows that $c(P) \leq 2 + (e-1)p^e$, as required. ∎

3. Theorem A.

The following three results give information about the subgroups of an arbitrary finite group G in terms of the parameter $b(G)$. The first two of these are essentially Lemma 12.10 and Problem 12.12(a) of **[2]**, but since they are crucial ingredients of our proof of Theorem A, we present them here, along with their short proofs.

(3.1) LEMMA. *Let $A \subseteq G$, where A is abelian and $b(G) = b$. Then the number of orbits in the conjugation action of A on G is at least $|G|/b$.*

Proof. By the basic orbit counting formula (often attributed to Burnside), the number of orbits is

$$\begin{aligned}\frac{1}{|A|}\sum_{a\in A}|\mathbf{C}_G(a)| &= \frac{1}{|A|}\sum_{a\in A}\sum_{\chi\in\mathrm{Irr}(G)}|\chi(a)|^2\\ &= \sum_{\chi\in\mathrm{Irr}(G)}[\chi_A,\chi_A]\\ &\geq \sum_{\chi\in\mathrm{Irr}(G)}\chi(1)\,,\end{aligned}$$

where the inequality holds because A is abelian, and so χ_A is a sum of $\chi(1)$ linear characters.

Now $|G| = \sum \chi(1)^2 \leq b\sum\chi(1)$, and thus $\sum\chi(1) \geq |G|/b$, where all of these sums run over $\chi \in \mathrm{Irr}(G)$. The result now follows. ∎

(3.2) LEMMA. *Let $Z \subseteq \mathbf{Z}(H)$, where $H \subseteq G$ and $b(G) = b$. If $|G : H| > b$, then there exists $g \in G - H$ such that $|Z : \mathbf{C}_Z(g)| \leq b^2$.*

Proof. Let Z act on G by conjugation and observe that $|Z : \mathbf{C}_Z(g)|$ is the size of the orbit containing the element g. We can assume, therefore, that every Z-orbit containing an element of $G - H$ has size exceeding b^2, and we work to obtain a contradiction. Note

that since $H < G$, there actually are orbits of size exceeding b^2, and hence G is nonabelian and $b > 1$.

The elements of H all lie in orbits of size 1 under the conjugation action of Z on G, and so these elements account for $|H|$ orbits of this action. By Lemma 3.1, the total number of orbits is at least $|G|/b$, and so the $|G| - |H|$ elements outside of H are divided into at least $|G|/b - |H|$ orbits. Since we are assuming that each of these orbits has size exceeding b^2, we obtain the inequality $(g/b - h)b^2 < g - h$, where we have written $g = |G|$ and $h = |H|$. Thus $bg - b^2h < g - h$, or equivalently, $g(b-1) < h(b^2-1)$. Since $b - 1 > 0$, we deduce that $g < h(b+1)$, and thus $|G : H| = g/h < b + 1$. But $|G : H|$ is an integer, and so we have $|G : H| \leq b$, and this is contrary to hypothesis. ∎

(3.3) THEOREM. *Let $b(G) = b$. Then there exists $N \lhd G$ such that $|G : N| \leq b$ and $|N : \mathbf{Z}(N)|$ is bounded by some function of b.*

Proof. Suppose $N \lhd G$ and $|G : N| > b$, and write $Z = \mathbf{Z}(N)$. We show that there exists a normal subgroup $M > N$ such that $|Z : Z \cap \mathbf{Z}(M)|$ is bounded above by some function of b and $|G : N|$. To see this, observe that by Lemma 3.2, there exists an element $g \in G - N$ such that $|Z : \mathbf{C}_Z(g)| \leq b^2$. Write $A = \mathbf{C}_Z(g)$ and note that $A \lhd N$ and $Z \lhd G$, and thus the G-conjugacy class of A consists of at most $|G : N|$ subgroups of Z, each of index at most b^2 in Z. Writing $B = \mathrm{core}_G(A)$, we deduce that $|Z : B| \leq (b^2)^{|G:N|}$, and we see that $B \lhd G$ and the index $|Z : B|$ is bounded in terms of b and $|G : N|$. We set $M = \mathbf{C}_G(B)$, and we observe that $M \lhd G$ and $M \supseteq N$. Finally, we observe that this containment is strict since $g \in M$ and $g \notin N$.

Now as we observed earlier, there exists a subgroup $A \lhd G$, where A is abelian and $|G : A|$ is bounded in terms of b. We start to define a strictly increasing series of subgroups $N_i \lhd G$ by setting $N_0 = A$. Now if we are given N_i and it happens that $|G : N_i| > b$, we apply the result of the previous paragraph to the subgroup N_i. We construct $N_{i+1} \lhd G$ with $N_{i+1} > N_i$, and where there is a central subgroup of N_{i+1} whose index in the center of N_i is bounded above in terms of b and $|G : N_i|$. In fact, $|G : N_i| \leq |G : A|$, which is bounded in terms of b alone, and also $|N_{i+1} : N_i| \leq |G : A|$ is bounded in terms of b. It follows that there is some integer m depending only on b and such that

$$|N_{i+1} : \mathbf{Z}(N_{i+1})| \leq m|N_i : \mathbf{Z}(N_i)|$$

whenever N_{i+1} is defined. Since $N_0 = A$ is abelian, we conclude that $|N_i : \mathbf{Z}(N_i)| \leq m^i$ for all subscripts i for which N_i is defined.

Our strictly increasing chain of normal subgroups eventually terminates when we reach a subgroup $N = N_k$ with $|G : N| \leq b$. Since $|N : \mathbf{Z}(N)| \leq m^k$, where m is bounded in terms of b, we see that to complete the proof, it suffices to show that k is also bounded in terms of b. But this is clear since $A = N_0 < N_1 < \cdots < N_k \subseteq G$, and we see that $k \leq \log_2(|G : A|)$. Thus k is indeed bounded in terms of b since we selected A such that $|G : A|$ is bounded. ∎

Finally, we are ready to prove Theorem A.

Proof of Theorem A. We are given a p-group P whose irreducible character degrees other than 1 all lie in the set $\{p^a, p^{a+1}, \ldots, p^{2a}\}$, where $a > 1$. We want to show that there is an upper bound for the nilpotence class $c(P)$ in terms of p and a. Since $p \notin \mathrm{cd}(P)$, we know by Theorem C that $c(P)$ is bounded in terms of $b = b(P)$ and the class $c(P')$ of the derived subgroup. Since $b \leq p^{2a}$, we see that it suffices to bound $c(P')$ in terms of b.

By Theorem 3.3, choose a subgroup $N \lhd P$ such that $|P : N| \leq b$ and $|N : \mathbf{Z}(N)|$ is bounded in terms of b. If P/N is nonabelian, it would have a nonlinear irreducible character of some degree f. Then $f \in \mathrm{cd}(P)$, and since $f > 1$, we see that $f \geq p^a$. Also, $f^2 < |P/N| \leq b$, and we have $p^{2a} < b$, which is not the case. This shows that P/N is abelian, and thus $P' \subseteq N$ and $c(P') \leq c(N)$. But $|N : \mathbf{Z}(N)|$ is bounded in terms of b, and since it is clear that $c(N) \leq |N : \mathbf{Z}(N)|$, the proof is complete. ∎

4. Theorem B.

In this section, after a few preliminary results, we prove Theorem B. In the following, when we refer to the 'order' of a linear character of some group, we mean, of course, its order as an element of the group of linear characters. Also, we shall use the notation of [**4**]: If $N \lhd G$, then $\mathrm{Irr}(G|N)$ denotes the set $\{\chi \in \mathrm{Irr}(G) \mid N \not\subseteq \ker(\chi)\}$ and $\mathrm{cd}(G|N)$ is defined to be the set of degrees of the members of $\mathrm{Irr}(G|N)$. The one result from [**4**] that we shall need is Corollary 3.2, which asserts that if $|\mathrm{cd}(G|N)| = 1$, then N is abelian.

(4.1) LEMMA. *Let $A \lhd P$ where P is a p-group and A is abelian, and suppose $\mathrm{cd}(P|A) = \{m\}$. If λ is a linear character of A of order exceeding p and T is its stabilizer in P, then all of the following hold.*

(a) $|P : T| = m$.

(b) T/A *is abelian.*

(c) $\mathbf{N}_P(T)/T$ *has no elementary abelian subgroup of order* p^2.

Proof. Let $\chi \in \mathrm{Irr}(P|\lambda)$. Then $\chi \in \mathrm{Irr}(P|A)$ since λ is not principal, and thus $\chi(1) = m$. Since P/A is nilpotent, there exists a subgroup U with $A \subseteq U \subseteq P$ and a character μ of U such that $\mu_A = \lambda$ and $\mu^P = \chi$. (This follows from Theorem 6.22 of [**2**], for example.) Since $\mu_A = \lambda$, we see that μ is linear, and thus $|P : U| = \chi(1) = m$. Also, λ is invariant in U, and hence $U \subseteq T$. We need to prove equality here.

Suppose that $U < T$ and let $U \lhd V \subseteq T$ with $|V/U| = p$. Let ν be the product of the p (not necessarily distinct) conjugates of μ under the action of V/U. Then ν is invariant in V and since $U < V$, it follows that ν cannot induce irreducibly to V. We conclude that ν^P is reducible, and so the degrees of its irreducible constituents are all less than $|P : U| = m$, and hence they do not lie in $\mathrm{Irr}(P|A)$. It follows that $A \subseteq \ker(\nu)$, and so $\nu_A = 1_A$. But ν is a product of p linear characters conjugate in V to μ, and thus ν_A is a product of p conjugates of $\mu_A = \lambda$ in V. Since V is contained in the stabilizer of λ, however, we see that $1_A = \nu_A = \lambda^p$, and this is a contradiction since we are assuming that the order of λ exceeds p. This proves that $T = U$, and so $|P : T| = m$, proving (a).

Now if $\beta \in \mathrm{Irr}(T/A)$, then $\beta\mu$ is an irreducible character of T that lies over λ, and thus $(\beta\mu)^P$ is irreducible since T is the stabilizer of λ in P. Therefore $(\beta\mu)^P \in \mathrm{Irr}(P|A)$, and so this character has degree $m = |P : T|$. It follows that $\beta(1) = 1$, and since β was arbitrary, we conclude that T/A is abelian, proving (b).

Now we use reasoning similar to that in the proof of (a) to derive a contradiction if there exists a subgroup $V \subseteq P$ such that $T \lhd V$ and V/T is elementary abelian of order p^2. Suppose X/T is any nonidentity subgroup of V/T and write $\tau^{(X)}$ to denote the product of all of the $|X/T|$ (not necessarily distinct) conjugates of μ under the action of X/T. Then $\tau^{(X)}$ is invariant in $X > T$, and thus it cannot induce irreducibly to P. The irreducible constituents of $(\tau^{(X)})^P$ thus have degree less than m, and so they do not lie in $\mathrm{Irr}(P|A)$. We deduce that $A \subseteq \ker(\tau^{(X)})$ for every nonidentity subgroup X/T of V/T.

Let σ be the product of the $p+1$ linear characters $\tau^{(X)}$, as X/T runs over the subgroups of order p in V/T. Then $A \subseteq \ker(\sigma)$ and we see that $\sigma = \mu^p \tau^{(V)}$. Since also $A \subseteq \ker(\tau^{(V)})$, it follows that $A \subseteq \ker(\mu^p)$, and thus $1_A = (\mu^p)_A = \lambda^p$. This is the desired contradiction since λ has order exceeding p, and this proves (c). ∎

(4.2) LEMMA. *Let G be arbitrary and act on an abelian p-group V of exponent at least p^4. Assume that all G-orbits in V consisting of elements of order exceeding p have the same size n. Then $|G : \mathbf{C}_G(V)| = n$.*

Proof. Build a graph on the set of elements of V of order exceeding p by linking x and y if either x is a power of y or y is a power of x. If x and y are linked, then one of $\mathbf{C}_G(x)$ and $\mathbf{C}_G(y)$ contains the other, but since these subgroups both have index n in G, we deduce that $\mathbf{C}_G(x) = \mathbf{C}_G(y)$. It follows that all of the elements in each connected component of our graph have the same stabilizer in G.

Now fix an element $a \in V$ of order p^4. Let $H = \mathbf{C}_G(a)$, and note that $|G : H| = n$. We will complete the proof by showing that $H = \mathbf{C}_G(V)$. We show first that $H \subseteq \mathbf{C}_G(b)$ for every element $b \in V$ of order p^2. To see this, note that since V is abelian, we have $(ab)^{p^2} = a^{p^2}$. This is an element of order p^2 joined to both a and ab in the graph, and so a and ab lie in the same connected component and have the same stabilizer H in G. Thus $a, ab \in \mathbf{C}_V(H)$, and it follows that $b \in \mathbf{C}_V(H)$ and $H \subseteq \mathbf{C}_G(b)$, as claimed.

Since every connected component of our graph contains an element of order p^2 and all the elements in each component have the same stabilizer in G, it follows that H stabilizes every element of V of order exceeding p. We conclude that $V = \Omega_1(V) \cup \mathbf{C}_V(H)$. Now $\Omega_1(V) < V$ since V is abelian of exponent exceeding p. Since V cannot be a union of two proper subgroups, we deduce that $\mathbf{C}_V(H) = V$, and so $H \subseteq \mathbf{C}_G(V) \subseteq \mathbf{C}_G(a) = H$. Thus $H = \mathbf{C}_G(V)$ and the proof is complete. ∎

Proof of Theorem B. We are given a class-bounding set $\mathcal{S}$ and a p-group P such that $\mathrm{cd}(P) = \mathcal{S} \cup \{p^b\}$. Assuming that p^b exceeds the square of the largest member of $\mathcal{S}$ and that $p \notin \mathrm{cd}(P)$, we need to show that $c(P)$ is bounded in terms of $b(P) = p^b$.

Let Ξ be the sum of all irreducible characters of P with degrees in the set $\mathcal{S}$ and write $K = \ker(\Xi)$. We proceed to show that $\mathrm{cd}(P/K) = \mathcal{S}$ and that $\mathrm{cd}(P|K) = \{p^b\}$. (And in thus, in particular, K is abelian by Corollary 3.2 of [**4**].) First, observe that K is contained in the kernels of all irreducible characters of P with degrees different from p^b, and thus $\mathrm{cd}(P|K) \subseteq \{p^b\}$. Also, since every member of $\mathcal{S}$ is the degree of some irreducible constituent of Ξ, which is a character of P/K, we see that $\mathcal{S} \subseteq \mathrm{cd}(P/K)$.

If α and β are any two irreducible characters of P with degrees in $\mathcal{S}$, we see that $\alpha(1)\beta(1) < p^b$, and thus the irreducible constituents of $\alpha\beta$ must also have degrees in $\mathcal{S}$. It follows that all irreducible constituents of all powers of Ξ have degrees in $\mathcal{S}$. But Ξ

is a faithful character of the group P/K, and so every irreducible character of P/K is a constituent of some power of Ξ. (See Theorem 4.3 of **[2]**.) It follows that the degree of every irreducible character of P/K lies in $\mathcal{S}$, and since we already knew that $\mathcal{S} \subseteq \mathrm{cd}(P/K)$, we must have equality here, as claimed. Also, P has some irreducible character χ of degree p^b and we now know that $K \not\subseteq \ker(\chi)$. Thus $\chi \in \mathrm{Irr}(P|K)$, and since we already knew that $\mathrm{cd}(P|K) \subseteq \{p^b\}$, we must have equality here too.

Suppose first that the exponent of K is at least p^4. By Lemma 4.1(a), we see that the stabilizer in P of every linear character of K of order exceeding p has index exactly p^b in P. We can therefore apply Lemma 4.2 to the action of P on the abelian group $\mathrm{Irr}(K)$, which also has exponent at least p^4. We deduce that the kernel of this action has index p^b in P. But an element of P that acts trivially on $\mathrm{Irr}(K)$ must also act trivially on K, and so we see that if we write $C = \mathbf{C}_P(K)$, we have $|P : C| = p^b$ and C is the full stabilizer in P of every linear character of K of order exceeding p. By Lemma 4.1(b), we know that C/K is abelian, and since $K \subseteq \mathbf{Z}(C)$, we see that the nilpotence class of C is at most 2. By Lemma 4.1(c), we also know that P/C has no elementary abelian subgroup of order p^2, and it follows that P/C is either cyclic or generalized quaternion. But the latter alternative is impossible since P has no irreducible character of prime degree, and thus P/C is cyclic and $P' \subseteq C$. But then $c(P') \leq 2$, and it follows by Theorem C that $c(P)$ is bounded in terms of $b(P)$, as desired.

We can now assume that the exponent of K is less than p^4. Since $\mathrm{cd}(P/K) = \mathcal{S}$ and $\mathcal{S}$ is class bounding, we know that the nilpotence class of P/K is bounded in terms of $\mathcal{S}$. We also know that P has an abelian normal subgroup A of index bounded in terms of $b(P)$, and thus the nilpotence class of P/A is bounded in terms of $b(P)$. It follows that there exists an integer N depending only on $b(P)$ such that $P^N \subseteq A \cap K$. Since A is abelian, it acts trivially on P^N, which has exponent at most p^4 since it is contained in K. It follows from Corollary 2.5 that $1 = [P^N, P, P, \ldots, P]$, where there are $4|P : A|$ commutations by P. Since both N and $|P : A|$ are bounded in terms of $b(P)$, this yields the desired bound on $c(P)$. ∎

5. Theorem D.

In this section we prove Theorem D, which asserts that if $\mathcal{S}$ is a set of powers of p containing 1 and $|\mathcal{S}| = 3$, then $\mathcal{S}$ is class bounding if and only if $p \notin \mathcal{S}$. One direction of this is an immediate corollary of Theorems A and B.

(5.1) COROLLARY. *Suppose that P is a p-group and that $\mathrm{cd}(P) = \{1, p^a, p^b\}$, where $1 < a < b$. Then $c(P)$ is bounded in terms of b.*

Proof. If $b \leq 2a$, the result follows from Theorem A and if $b > 2a$, it follows from Theorem B. ∎

The following result completes the proof of Theorem D.

(5.2) THEOREM. *Given integers $b > 1$ and N and a prime p, there exists a p-group P such that $c(P) > N$ and $\mathrm{cd}(P) = \{1, p, p^b\}$.*

Proof. Since we know that the set $\{1, p\}$ is not class bounding, we can choose a p-group D of class exceeding N and such that $\mathrm{cd}(D) = \{1, p\}$. In fact, the construction of such groups in [**5**] shows that we can assume that D has an abelian subgroup A of index p. Let $U = D \times V$, where V is elementary abelian of order p^{2b-1}, and note that $A \lhd U$ and U/A is elementary abelian of order p^{2b}. Also, we let E be an extraspecial p-group of order p^{2b+1}, and we write $Z = \mathbf{Z}(E)$ so that E/Z is elementary abelian of order p^{2b}, and in particular, $E/Z \cong U/A$.

Working in the direct product $U \times E$, we can construct a subgroup P having normal subgroups K and L such that $K \cap L = 1$, where $P/K \cong U$ and $P/L \cong E$, and where under these isomorphisms, $KL/K \subseteq P/K$ corresponds to the subgroup A of U and $KL/L \subseteq P/L$ corresponds to the subgroup Z of E.

Let T be the unique subgroup of P (containing K) such that T/K corresponds to the subgroup D of U under the given isomorphism between P/K and U and note that since KL/K corresponds to $A \subseteq D$, we have $KL \subseteq T$. Also, let S be the unique subgroup of P containing K such that S/K corresponds to the subgroup V of U. Since $U = D \times V$, we see that both S and T are normal in P, that $ST = P$ and that $S \cap T = K$. Observe also that $S \cap L = S \cap (T \cap L) = K \cap L = 1$, and thus $SL = S \times L$ is a direct product. Finally, we note that $SL/K = (S/K)(KL/K)$ corresponds to the subgroup VA of U, and thus $|P : SL| = |U : VA| = p$.

Since $D \cong T/K \cong P/S$, it follows that the nilpotence class of P cannot be less than that of D, and so it suffices to show that $\mathrm{cd}(P) = \{1, p, p^b\}$. Since $\mathrm{cd}(P/S) = \mathrm{cd}(D) = \{1, p\}$ and $\mathrm{cd}(P/L) = \mathrm{cd}(E) = \{1, p^b\}$, all that is required is to show that every irreducible character of P with degree exceeding p has degree p^b. For this purpose, it suffices to show that every nonlinear irreducible character of the index p subgroup $SL \subseteq P$ has degree p^{b-1} and that no such character can be invariant in P.

Recall that $SL = S \times L$ and that both S and L are normal in P. It follows that every irreducible character θ of SL has the form $\theta = \alpha \times \beta$, where $\alpha \in \mathrm{Irr}(S)$ and $\beta \in \mathrm{Irr}(L)$. Also, θ is invariant in P if and only if both α and β are invariant in P.

Let $\theta \in \mathrm{Irr}(SL)$ be nonlinear and write $\theta = \alpha \times \beta$, where $\alpha \in \mathrm{Irr}(S)$ and $\beta \in \mathrm{Irr}(L)$. Since $L \cong KL/K \cong A$ is abelian, we see that β is linear, and therefore α is nonlinear. But $S \cong SL/L$, which has index p in $P/L \cong E$. Since E is an extraspecial p-group of order p^{2b+1}, it follows that α has degree p^{b-1}, and thus θ has degree p^{b-1}, as required. Also, the character $\alpha \times 1_L$ of SL corresponds to a nonlinear character of SL/L, which has index p in the extraspecial group P/L. It follows that $\alpha \times 1_L$ cannot be invariant in P/L, and thus α is not invariant in P. We conclude that $\theta = \alpha \times \beta$ is not invariant in P. This completes the proof. ∎

REFERENCES

1. I. M. Isaacs, Sets of p-powers as irreducible character degrees, Proc. Amer. Math. Soc. **96** (1986) 551–552.

2. I. M. Isaacs, *Character Theory of Finite Groups*, Dover, New York, 1994.

3. I. M. Isaacs, Characters of groups associated with finite algebras, J. of Algebra **177** (1995) 708–730.

4. I. M. Isaacs and G. Knutson, Irreducible character degrees and normal subgroups, J. of Algebra **199** (1998) 302–326.

5. I. M. Isaacs and D. S. Passman, A characterization of groups in terms of the degrees of their characters II, Pacific J. of Math. **24** (1968) 467–510.

6. M. C. Slattery, Character degrees and nilpotence class in p-groups, J. of Austral. Math. Soc., Ser A, **57** (1994) 76–80.