CHARACTER DEGREES AND NILPOTENCE CLASS OF FINITE p-GROUPS: AN APPROACH VIA PRO-p GROUPS

A. JAIKIN-ZAPIRAIN AND ALEXANDER MORETÓ

Abstract. Let $\mathcal{S}$ be a finite set of powers of p containing 1. It is known that for some choices of $\mathcal{S}$, if P is a finite p-group whose set of character degrees is $\mathcal{S}$, then the nilpotence class of P is bounded by some integer that depends on $\mathcal{S}$, while for some other choices of $\mathcal{S}$ such an integer does not exist. The sets of the first type are called class bounding sets. The problem of determining the class bounding sets has been studied in several papers (see [9, 10, 11, 22]). The results obtained in these papers made tempting to conjecture that a set $\mathcal{S}$ is class bounding if and only if $p \notin \mathcal{S}$. In this article we provide a new approach to this problem. Our main result shows the relevance of certain p-adic space groups in this problem. With its help, we are able to prove some results that provide new class bounding sets. We also show that there exist non class bounding sets $\mathcal{S}$ such that $p \notin \mathcal{S}$.

1. Introduction

It is known that any finite set of powers of a prime number p containing 1 can occur as the set of character degrees of some p-group of class ≤ 2 (see [5]). (A new proof of this result has been found in [11], where it has also been shown that any finite set of powers of p containing 1 and cardinality greater than 1 occurs as the set of character degrees of some p-group of class n for any $1 < n \leq p$.) Following [9] and [11], we say that a finite set $\mathcal{S}$ of powers of p containing 1 is **class bounding** if there is some integer n (depending on $\mathcal{S}$) such that $c(P) \leq n$ for every p-group P with $\mathrm{cd}(P) = \mathcal{S}$. (As usual, $\mathrm{cd}(P)$ denotes the set of degrees of the complex irreducible characters of P). The question we are interested in is the following: which are the class bounding sets? This question has been object of study in recent years, and it seems to be far from being solved.

Throughout this article $\mathcal{S}$ will denote a finite set of powers of p containing 1. In 1968 I. M. Isaacs and D. S. Passman proved that if $|\mathcal{S}| = 2$ then $\mathcal{S}$ is class bounding if and only if p does not belong to $\mathcal{S}$. The analog result for sets of size 3 has been proved in [9], where Isaacs and the second author also found class bounding sets of arbitrarily large size. These class bounding sets share the property that p is not a member of any of them. These results made tempting to conjecture that $\mathcal{S}$ is class bounding if and only if p does not belong to $\mathcal{S}$. The proof of the "only if" part of this "conjecture" is the main theorem of [11].

We say that $\mathcal{S}$ is **strongly class bounding** if there is some integer n (depending on $\mathcal{S}$) such that $c(P) \leq n$ for every p-group P with $\mathrm{cd}(P) \subseteq \mathcal{S}$, that is, if every subset of $\mathcal{S}$ is class bounding. This concept is closely related to that of being class

1991 *Mathematics Subject Classification.* Primary 20C15, Secondary 20E18.

Research of the first author partially supported by DGICYT. Research of the second author supported by the Basque Government and the University of the Basque Country.

bounding. Of course, every strongly class bounding set is class bounding. Also, every known class bounding set is strongly class bounding. It seems likely that every class bounding set is strongly class bounding, but we have been unable to prove this.

In this work we provide a new approach to the problem of determining the (strongly) class bounding sets, which will allow us to make some progress toward a solution. Our main result characterizes the strongly class bounding sets in terms of certain pro-p groups. (We refer the reader to Section 3 for some basic facts about these groups and for more detailed references.) More precisely, we obtain a characterization in terms of certain p-adic space groups. The p-adic space groups were already known to be useful for some other problems related to the classification of finite p-groups, like in the coclass conjectures (see, for instance, [16]).

Since the p-adic space groups are infinite groups, we need to refer to characters of infinite groups. We will do this in the following way. Given an arbitrary group G, we say that χ is an irreducible character of G if it is an irreducible character of some finite quotient of G and the set of character degrees of G, $\mathrm{cd}(G)$, is the set of degrees of its irreducible characters.

Theorem A. *A set $\mathcal{S}$ is not strongly class bounding if and only if there exists a non-nilpotent just infinite p-adic space group R whose point group is a p-group and such that $\mathrm{cd}(R) \subseteq \mathcal{S}$.*

Using this theorem we can obtain results that provide both class bounding sets and non class bounding sets. First, we show some new class bounding sets. These results present some slight differences according to whether $p = 2$ or p is odd. We define

$$\epsilon(p) = \begin{cases} 0 & \text{if } p > 2; \\ 1 & \text{if } p = 2. \end{cases}$$

Theorem B. *Let $p^j = \min(\mathcal{S} - \{1\})$ and assume that $j > 1$. If the cardinality of $\mathcal{S}$ is less than or equal to $j + 2 - \epsilon(p)$ then $\mathcal{S}$ is (strongly) class bounding.*

Observe that, in particular, this result gives a new proof of the fact that if p does not belong to $\mathcal{S}$ and $|\mathcal{S}| = 3$ then $\mathcal{S}$ is class bounding. But it proves more. For instance, it proves that if p is odd then any set $\mathcal{S}$ of cardinality 4 such that $p \notin \mathcal{S}$ is class bounding. It also provides a new proof of Theorem A of [9], except for the case when $p = 2$ and $\mathcal{S} = \{1, 2^j, \dots, 2^{2j}\}$ for some $j > 1$. Unfortunately, we have been unable to decide whether or not the stronger hypothesis in the case $p = 2$ is really necessary.

As an immediate corollary of this theorem we obtain the answer to Questions 2 and 3 of [11]. Following [11], given a class bounding set $\mathcal{S}$, we write $b(\mathcal{S})$ to denote the maximum of the nilpotence classes of the p-groups P such that $\mathrm{cd}(P) = \mathcal{S}$.

Corollary C. *Given any positive integer n, there exists a p-group P such that $\mathrm{cd}(P)$ is class bounding and $\mathrm{dl}(P) = n$. In particular, the maximum of the numbers $b(\mathcal{S})$ as $\mathcal{S}$ runs over the class bounding sets cannot be bounded in terms of p.*

Proof. Let $P_{m,j}$ be the Sylow p-subgroup of $\mathrm{GL}(m, p^j)$. It is well-known (see Satz III.16.3 of [3], for instance) that there exists m such that $\mathrm{dl}(P_{m,j}) = n$. We fix this value m. It is also known (see [4] and [7]) that $\mathrm{cd}(P_{m,j})$ is a set of powers of p^j whose cardinality does not depend on j. Thus, choosing j large enough, $|\mathrm{cd}(P_{m,j})| \leq j$ and therefore $\mathrm{cd}(P_{m,j})$ is class bounding. □

This corollary shows that there exist "complicated" p-groups whose set of character degrees is class bounding.

If every class bounding set were strongly class bounding, then the next result would generalize Theorem B of [9]. Anyway, it provides many new class bounding sets.

Theorem D. *Assume that $\mathcal{S} = \{1\} \cup \mathcal{R} \cup \mathcal{T}$, where $\mathcal{R}$ and $\mathcal{T}$ are non-empty sets of powers of p, $p < p^j = \min(\mathcal{R})$, $\{1\} \cup \mathcal{R}$ is strongly class bounding and $\min(\mathcal{T}) > \max(\mathcal{R})^2$. If $|\mathcal{T}| \leq j - \epsilon(p)$ then $\mathcal{S}$ is (strongly) class bounding.*

Isaacs and Slattery [11] have proved that if p belongs to $\mathcal{S}$ then $\mathcal{S}$ is not class bounding. It has been asked (see Question 1 of [11]) whether or not those are all the non class bounding sets. Our next theorem shows that the answer is "no".

Theorem E. *If $\max(\mathcal{S}) < p^j$ for some $j > 1$, then the set $\mathcal{S} \cup \{p^j, \dots, p^{2j+1}\}$ is not class bounding.*

This theorem also shows that, at least when p is odd, the result obtained in Theorem B is best possible, i.e., there exist non class bounding sets $\mathcal{S}$ of cardinality $j+3$, where $p^j = \min(\mathcal{S} - \{1\})$.

In our way toward a proof of these theorems we obtain several results that, we hope, will be useful for other purposes. Some of these results are related to the minimum degree of the non-linear irreducible characters of a finite p-group. Other results refer to the number of orbit sizes in the action of groups on modules. We think that the following result is specially noteworthy (even though the proof is easy), and this is the reason why we state it here. It refers to arbitrary finite groups. Given a finite group G and a module V for G, we write $\mathrm{os}(G, V)$ to denote the set of orbit sizes in the action of G on V excluding the number 1. We also write $d(G)$ to denote the minimal number of generators of G. We recall that the rank of a finite group G (we denote it by $\mathrm{rk}(G)$) is the maximum of the numbers $d(H)$, as H runs over the subgroups of G.

Theorem F. *Let G be any finite group and V a faithful FG-module, where F is a field of characteristic 0 or characteristic coprime to the order of G and order larger than the number of subgroups of G. Then the rank of G is bounded by a quadratic function of $|\mathrm{os}(G, V)|$.*

We have been unable to find any reference to results of this type when the field is infinite. T. M. Keller has obtained results of this flavor for finite fields (see, for instance, Theorem 2.1 of [12]). We do not know whether a linear bound for the number of generators (or, perhaps, even for the rank) exists.

We have tried to make this paper as comprehensible as possible, giving references to most of the results required about character theory and pro-p groups. In Section 2 we give the proof of Theorem F, which does not require either character theory or the theory of pro-p groups. Next, in Section 3 we present the basic facts about pro-p groups required in the remaining of this work. We devote Section 4 to the proof of Theorem A. In Section 5, which can be read independently of the rest of the paper, we study the relation between the minimal degree of the non-linear irreducible characters of a finite p-group and the rank of the abelian subgroups of the p-group and obtain results that will possibly be useful for other questions. We obtain more results referring to the minimal degree in Section 6, but these are more focused on our problem and allow us to present the proofs of Theorems B and D in Section 7. Finally, we construct the example that proves Theorem E in Section 8 and we conclude with some observations and questions in Section 9.

We thank Y. Barnea for helpful comments about the writing of this paper. This work was done while the second author was visiting the University of Wisconsin, Madison. He thanks the Mathematics Department for its hospitality.

2. Orbit sizes and number of generators

Throughout this section G denotes an arbitrary finite group. Our aim is to prove Theorem F. We begin with an easy (but important) lemma.

Lemma 2.1. *Let V be an FG-module, where F is a field of order greater than the number of subgroups of G, and $\mathcal{C} = \{C_G(v) \mid v \in V\}$. If $C_1, C_2 \in \mathcal{C}$, then $C_1 \cap C_2 \in \mathcal{C}$.*

Proof. There exist $v_1, v_2 \in V$ such that $C_1 = C_G(v_1)$ and $C_2 = C_G(v_2)$. We consider the centralizers $C_\gamma = C_G(v_1 + \gamma v_2)$, as γ runs over F. Since the order of the field F is greater than the number of subgroups of G, there exist two different elements of F, α and β, so that $C_\alpha = C_\beta = C$. Hence C centralizes v_1 and v_2. Conversely, every element that centralizes v_1 and v_2 belongs to C. Therefore $C_1 \cap C_2 = C \in \mathcal{C}$. □

The next proposition includes what we need to prove our results on the nilpotence class and character degrees of finite p-groups.

Proposition 2.2. *Let V be a faithful FG-module and A an abelian subgroup of G. If $|F|$ is greater than the number of subgroups of G and the characteristic of F does not divide $|A|$, then $d(A) \le |\operatorname{os}(G, V)|$.*

Proof. Let $d = d(A)$. By Lemma 3.6 of [21], there exist $m \ge d$ and $v_1, \ldots, v_m \in V$ such that $A = A_0 > A_1 > \cdots > A_m = 1$, where $A_i = C_{A_{i-1}}(v_i)$ for $i \ge 1$. Now,

$$G > C_G(v_1) > C_G(v_1) \cap C_G(v_2) > \cdots > C_G(v_1) \cap \cdots \cap C_G(v_m),$$

and the result follows since, by the previous lemma, the intersection of centralizers is a centralizer. □

Theorem 2.3. *Let d be the maximum rank of the abelian subgroups of a finite p-group P. Then*

$$d(P) \le \begin{cases} d(d+1)/2 & \textit{if } p > 2; \\ d(d+1)/2 + d^2 & \textit{if } p = 2. \end{cases}$$

Proof. This is a theorem of J. G. Thompson (see Satz III.12.3 of [3]) for odd primes and A. Mann [18] for $p = 2$. □

Theorem 2.4. *The number of generators of a finite group G cannot exceed $1 + \max d(P)$, as P runs over the Sylow subgroups of G.*

Proof. This theorem has been obtained independently by R. M. Guralnick [2] and A. Lucchini [17], using the classification of finite simple groups. The result had been previously obtained by L. Kovacs [14] for solvable groups. □

Now, we can prove Theorem F.

Theorem 2.5. *Let G be any finite group and V a faithful FG-module, where F is a field of characteristic* 0 *or characteristic coprime to the order of G and order larger than the number of subgroups of G. Let $n = |\operatorname{os}(G, V)|$. Then*

$$\operatorname{rk}(G) \leq n(n+1)/2 + n^2 + 1.$$

Proof. Let $H \leq G$ and let d be the maximum rank of the abelian p-subgroups of H, as p runs over the set of prime divisors of $|G|$. By Theorem 2.3, the maximum rank of the Sylow p-subgroups of H is bounded by $d(d+1)/2$ for $p > 2$ and $d^2 + d(d+1)/2$ for $p = 2$. Now, the result follows from the previous theorem and Proposition 2.2. □

The best bound that one can expect for the number of generators of the group G in terms of n is $d(G) \leq 2n$, as the action of the central product of $n-1$ copies of the dihedral group of order 8 and the quaternion group on a faithful irreducible complex module V of dimension 2^n shows. (It is easy to see that $\operatorname{os}(G, V) \subseteq \{2^{n+2}, \ldots, 2^{2n+1}\}$.) It would be interesting to decide whether a linear bound exists. We have not attempted to do this, however.

3. Some basic facts about pro-p groups

In this section we review some elementary results about pro-p groups that will be necessary in the remainder of this article. We refer the reader to [1, 13] or [23] for background and more advanced results on pro-p groups.

We begin with the definition of a pro-p group which is based on the notion of inverse limit. We recall that a **directed set** is a non-empty partially ordered set $(X, \leq)$ such that if $x, y \in X$ then there exists $z \in X$ such that $z \geq x$ and $z \geq y$. An **inverse system** of finite p-groups over X is a family of finite p-groups $(G_x)_{x \in X}$ with homomorphisms $\alpha_{x,y} \colon G_x \to G_y$ (defined when $x \geq y$) such that $\alpha_{x,x}$ is the identity and $\alpha_{x,y}\alpha_{y,z} = \alpha_{x,z}$ whenever $x \geq y \geq z$. We say that the inverse system is **surjective** if all the homomorphisms $\alpha_{x,y}$ are surjective. The **inverse limit** of a surjective inverse system of finite p-groups is the subgroup of the cartesian product $\prod_{x \in X} G_x$ consisting of all the elements of the form $(g_x)_{x \in X}$ such that $g_x \alpha_{x,y} = g_y$ whenever $x \geq y$. We give the discrete topology to each of the G_x and the product topology to $\prod_{x \in X} G_x$. In this way, the inverse limit G with the induced topology is a topological group. This topological group is called a **pro-p group**. We say that G is **finitely generated** if it is finitely generated as a topological group. (This is equivalent to the existence of a number d such that $d(G_x) \leq d$ for every $x \in X$. See Proposition 4.2.1 of [23].)

An example of a pro-p group is the additive group of the ring of p-adic integers $\mathbb{Z}_p$, which arises as the inverse limit of the cyclic groups of p-power order. Its role in the theory of pro-p groups is similar to that of the cyclic groups of prime order within the theory of finite groups.

One standard fact that we will use is that a non-nilpotent pro-p group has finite quotients of arbitrarily large nilpotence class. To see this, observe that a pro-p group G is a subgroup of a direct product of finite nilpotent groups (those forming the surjective inverse system). Since G is not nilpotent, there exist finite p-groups of arbitrarily large nilpotence class among those that belong to the inverse system. Now, it is enough to note that each of these finite p-groups is a quotient of G (this follows from the fact that the inverse system is surjective).

Let $\mathcal{C}$ be a class of finite p-groups. We call a group G a **pro-$\mathcal{C}$ group** if it is a pro-p group proceeding from an inverse limit of groups in the class $\mathcal{C}$.

We need the following fact about pro-$\mathcal{C}$ groups.

Lemma 3.1. *Let $\mathcal{C}$ be a class of finite p-groups closed under quotients and G a finitely generated pro-$\mathcal{C}$ group. Then every finite quotient of G belongs to $\mathcal{C}$.*

Proof. Let N be a normal subgroup of G of finite index. By Theorem 4.3.5 of [23], N is open. There exists a family of finite p-groups $(G_x)_{x\in X} \subseteq \mathcal{C}$ such that G is the inverse limit of (G_x). Now, by Proposition 1.2.1 of [23], G/N is isomorphic to a quotient of some G_x. Hence $G/N \in \mathcal{C}$. □

Next, we recall the concept of p-adic space group. We write $\mathbb{Z}_p$ to denote the ring of p-adic integers and $\mathbb{Q}_p$ to denote its field of quotients. An l-dimensional ($l > 0$) **p-adic space group** R can be defined as an extension of a free $\mathbb{Z}_p$-module $T(R)$ of rank l by a finite group $P(R)$ acting faithfully on $T(R)$. The subgroup $T = T(R)$ is called the **translation subgroup** of R and $P = P(R)$ is its **point group**. In this paper, we will also assume that $P(R)$ is a p-group. In this case, R is a pro-p group (it is the inverse limit of the groups $(R/p^kT)_{k\in\mathbb{N}}$, where the homomorphisms are the canonical projections). We say that R is **just infinite** if every non-trivial closed normal subgroup of R has finite index in R. By p. 2 of [13], this means that $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T$ is an irreducible $\mathbb{Q}_pP$-module.

We need the next result about just infinite p-adic space groups. We use the notation above.

Lemma 3.2. *Let R be a just infinite p-adic space group, $P = P(R)$ and $T = T(R)$. Then there exists a $\mathbb{Z}_pP$-module M, which is $\mathbb{Z}_p$-free, such that R is a subgroup of finite index of PM and $R \cap M = T$.*

Proof. See p. 76 of [15]. □

4. A characterization of strongly class bounding sets

In this section we prove Theorem A. This result will be the key to our results on class bounding and non class bounding sets.

We need two easy and known lemmas. We include their short proofs for the convenience of the reader. The first one is a ring theoretic fact.

Lemma 4.1. *In the quotient polynomial ring $D = \mathbb{Z}_p[T]/(T^p - 1)$, the following hold:*

(i) $pD \subseteq (T-1)D + (T^{p-1} + \cdots + T + 1)D$.
(ii) $(T-1)^pD = p(T-1)D$.

Proof. (i) Notice that for all i, $T^i - 1 \in (T-1)D$. Since

$$p = (T^{p-1} + \cdots + T + 1) - \sum_{i=1}^{p-1}(T^i - 1),$$

the result follows.

(ii) Consider the homomorphism of D-modules $\varphi : D \longrightarrow (T-1)D$ defined by $\varphi(f(T) + (T^p - 1)) = (T-1)f(T) + (T^p - 1)$ for any $f(T) \in \mathbb{Z}_p[T]$. It is clear that $\operatorname{Ker}\varphi = (1 + T + \cdots + T^{p-1})D$ and that φ determines an isomorphism between $B = \mathbb{Z}_p[T]/(1 + T + \cdots + T^{p-1})$ and $(T-1)D$ as D-modules. Under this isomorphism, the ideals $p(T-1)D$ and $(T-1)^pD$ of D correspond to the ideals pB and $(T-1)^{p-1}B$ of B, respectively. Our task is to show that these last two ideals coincide. To prove that $(T-1)^{p-1}B \subseteq pB$ it is enough to use the binomial formula,

$$(T-1)^{p-1} = T^{p-1} - (p-1)T^{p-2} + \cdots + (-1)^{p-1},$$

and the fact that $\binom{p-1}{n} \equiv (-1)^n \pmod p$ for $1 \le n \le p-1$.

It is clear that $|B/pB| = p^{p-1}$. As in the first part, $p \in (T-1)B$. Therefore

$$|(T-1)^iB/(T-1)^{i+1}B| \le |B/(T-1)B| = p.$$

for every $i \ge 0$. Hence $|B/(T-1)^{p-1}B| \le p^{p-1}$. Since $(T-1)^{p-1}B \subseteq pB$ and $|B/pB| = p^{p-1}$, we obtain that $(T-1)^{p-1}B = pB$, as desired. □

Lemma 4.2. *Let A be a finite abelian subgroup of* $\mathrm{GL}(n,F)$*, where F is a field of characteristic coprime to $|A|$ or 0. Then the number of generators of A is at most n.*

Proof. We may view A as a subgroup of $\mathrm{GL}(n,\overline{F})$, where $\overline{F}$ is an algebraically closed field containing F. Thus A is diagonalizable and we conclude that A has rank $\le n$. □

We recall some notation from [8]: given a normal subgroup N of a group G, we write $\mathrm{Irr}(G|N)$ to denote the set of irreducible characters of G whose kernel does not contain N and $\mathrm{cd}(G|N)$ to denote the set of degrees of the characters of $\mathrm{Irr}(G|N)$.

Theorem 4.3. *Let $\mathcal{S}$ be a finite set of powers of p containing 1. Then $\mathcal{S}$ is not strongly class bounding if and only if there exists a non-nilpotent just infinite p-adic space group R such that* $\mathrm{cd}(R) \subseteq \mathcal{S}$*.*

Proof. First, assume that there exists such a p-adic space group. As observed in the previous section, R has finite quotients of arbitrarily large nilpotence class. Furthermore, all the character degrees of any of these quotients belong to $\mathcal{S}$. We conclude that $\mathcal{S}$ is not strongly class bounding.

Conversely, suppose that $\mathcal{S}$ is not strongly class bounding. We want to prove that there exists a non-nilpotent just infinite p-adic space group R such that $\mathrm{cd}(R) \subseteq \mathcal{S}$. For every $a \ge 0$, we consider a set S_a of finite p-groups defined by: P belongs to S_a if and only if $\mathrm{cd}(P) \subseteq \mathcal{S}$, $Z(P)$ is cyclic and P has an abelian normal subgroup A of index at most p^a. Write $p^m = \max(\mathcal{S})$. By Theorem 12.26 of [6], every finite p-group whose set of character degrees is contained in $\mathcal{S}$ has an abelian normal subgroup of index bounded by some function of p^m. Hence, there exists an integer b (which is bounded by some function of p^m) such that for every $a \ge b$, $S_a = S_b$. It is clear that if a given set $\mathcal{S}$ is not strongly class bounding, then there exist finite p-groups with cyclic center and character degrees contained in $\mathcal{S}$ of arbitrarily large nilpotence class. (Given a finite p-group P of nilpotence class n, there exists $\chi \in \mathrm{Irr}(P|\gamma_n(P))$. Hence $c(P/\operatorname{Ker}\chi) = n$, $P/\operatorname{Ker}\chi$ has cyclic center and $\mathrm{cd}(P/\operatorname{Ker}\chi) \subseteq \mathrm{cd}(P)$). Thus there is not an absolute bound for the nilpotence class of the groups of $\cup_r S_r$. Let s be the integer such that the nilpotence class of all groups in S_{s-1} is bounded by some number (say c) but there is not any bound for the groups in S_s. It is clear that $s \le b$.

Let n be any integer greater than c. Let $P \in S_s$ of nilpotence class greater than $n + p^m$. Then P has an abelian normal subgroup A of index p^s. Put $\overline{P} = P/A$

and let $z \in Z(\overline{P})$ be an element of order p. We view A as a left $\mathbb{Z}_p\overline{P}$-module and write $A_1 = (z-1)A$ and $A_2 = (1+z+\cdots+z^{p-1})A$. (Using group-theoretic notation $A_1 = [A,z]$.) Note that A_1 and A_2 are normal subgroups of P. Since P/A_1 has an abelian subgroup of index less than p^s, $c(P/A_1) \leq c < n$. Observe that $1+z+\cdots+z^{p-1}$ annihilates A_1 and $z-1$ annihilates A_2. Now, by part (i) of Lemma 4.1, the intersection of A_1 and A_2 is annihilated by p. This means that $A_1 \cap A_2$ has exponent p. By Theorem 2.32 of [6], P has a faithful irreducible character whose degree cannot exceed p^m (because $\mathrm{cd}(P) \subseteq \mathcal{S}$). In particular, A is isomorphic to a subgroup of $\mathrm{GL}(p^m, \mathbb{C})$. By the previous lemma, the rank of A is $\leq p^m$. Hence the order of $A_1 \cap A_2$ is $\leq p^{p^m}$ and therefore $c(P/(A_1 \cap A_2)) \geq n$. Since $n > c(P/A_1)$, we deduce that $c(P/A_2) \geq n$.

Let $Q = P/A_2$. By the definition of A_2, $1+z+\cdots+z^{p-1}$ annihilates A/A_2 and by Lemma 4.1, $p \in \mathbb{Z}_p(z-1)+\mathbb{Z}_p(1+z+\cdots+z^{p-1})$. Hence $p(A/A_2) \leq (z-1)(A/A_2)$. Thus

$$p^i(A/A_2) \leq (z-1)^i(A/A_2) \leq \gamma_{i+1}(Q)$$

for every i, since $(z-1)^i(A/A_2) = [A/A_2, z, \ldots, z]$ where in the right hand side of this equality there are i commutations with z. Since A has rank $\leq p^m$, we have that $|Q : \gamma_{i+1}(Q)| \leq p^{s+ip^m}$. We conclude that there is no absolute bound for the nilpotence class of the following finite p-groups:

$$\mathcal{W} = \{P \mid \mathrm{cd}(P) \subseteq \mathcal{S}, P \text{ has an abelian normal subgroup of index at most } p^s \text{ and } |P/\gamma_{i+1}(P)| \leq p^{s+ip^m} \text{ for every } i\}.$$

Note that if $P \in \mathcal{W}$, then every quotient of P also belongs to $\mathcal{W}$. Now, we construct an infinite pro-p group G such that $G/\gamma_k(G)$ belongs to $\mathcal{W}$ for every k and G has an abelian normal subgroup B of index p^s. Consider the pairs (P, A), where $P \in \mathcal{W}$ and A is an abelian normal subgroup of P of index at most p^s. We say that two pairs (P_1, A_1) and (P_2, A_2) are equivalent if there exists an isomorphism of groups $\phi\colon P_1 \to P_2$ such that $\phi(A_1) = A_2$. We shall identify two such pairs. If we fix the order of P then there exists a finite number of inequivalent pairs.

Let $R_1 = (\{1\}, \{1\})$ and $W_1 = \{(P, A) \mid P \in \mathcal{W}\}$. Suppose that we have constructed a pair $R_j = (P_j, A_j)$ and an infinite subset W_j of W_1 such that if $(P, A) \in W_j$, then $(P/\gamma_j(P), A\gamma_j(P)/\gamma_j(P))$ is equivalent to R_j. The number of possibilities for $(P/\gamma_{j+1}(P), A\gamma_{j+1}(P)/\gamma_{j+1}(P))$ when $(P, A) \in W_j$ is finite. Then there exists R_{j+1} such that the set W_{j+1} consisting of the pairs $(P, A) \in W_j$ with $(P/\gamma_{j+1}(P), A\gamma_{j+1}(P)/\gamma_{j+1}(P))$ equivalent to R_{j+1} is infinite. Let (G, B) be the inverse limit of R_j (the maps are the canonical projections). Since the number of generators of the groups P_j remains bounded for $j \geq 2$ (this is because, by the definition of $\mathcal{W}$, the number of generators of any of the groups P_j cannot exceed $\log_p |P_j/\gamma_2(P_j)| \leq s + p^m$), G is finitely generated and by Lemma 3.1, $\mathrm{cd}(G) \subseteq \mathcal{S}$.

Let $t(B)$ be the torsion subgroup of B. Note that $t(B)$ is a finite normal subgroup of G. Replacing G by $G/t(B)$ we can suppose that B is torsion free. Decompose $V = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} B = \oplus V_i$ as a sum of irreducible $\mathbb{Q}_p(G/B)$-modules (this is possible by Maschke's Theorem). Suppose that V_1 is a non-trivial submodule. With a slight abuse of notation, we write $N = B \cap \oplus_{i \geq 2} V_i$ and view it as a normal subgroup of G. We also write $T = B/N$ and $R = G/N$. By the definition of N, T is a $\mathbb{Z}_p$-free module. Also, R/T acts irreducibly and non-trivially on $V_1 \cong \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T$ and, in particular, R is not nilpotent. Put $K = C_R(T)$. By the choice of s, T is a maximal abelian normal subgroup of R. Thus $K = T$, so the action of R/T on T is faithful.

This means that R is a non-nilpotent p-adic space group and, by p. 2 of [13], it is also just infinite. $\square$

The same argument as in the proof of this theorem allows to prove analog results for classes of groups closed under quotients. For instance, for the class of metabelian groups.

Theorem 4.4. *Let $\mathcal{S}$ be a set of powers of p containing 1. Then $\mathcal{S}$ is not strongly class bounding within the class of finite metabelian p-groups if and only if there exists a metabelian non-nilpotent just infinite p-adic space group R such that* $\mathrm{cd}(R) \subseteq \mathcal{S}$.

With the help of this theorem it is not difficult to obtain a new proof of part of Theorem 2.7 of [9]. (We remark that our methods do not allow us to find any bounds.)

Theorem 4.5. *Assume that $p \notin \mathcal{S}$. Then $\mathcal{S}$ is class bounding within the class of finite metabelian p-groups.*

Proof. We argue by way of contradiction. By Theorem 4.4 there exists a metabelian non-nilpotent just infinite p-adic space group R such that $\mathrm{cd}(R) \subseteq \mathcal{S}$. Thus the point group P is abelian and, since it acts irreducibly on $\mathbb{Q}_p \otimes T$, we conclude that P is cyclic. Now, using Lemma 2.1 of [9], we conclude that $\mathrm{cd}(R) = \{1\}$, a contradiction. $\square$

5. The minimum degree of the non-linear irreducible characters

It is known that the minimum degree of the non-linear characters of a finite non-abelian p-group P has a strong influence on the structure of the group (see, for example, Problem 5.14 of [6] or [19]). In this section we obtain new results in this direction. We write $m(P)$ to denote the minimum of the degrees of the non-linear irreducible characters of P. Our results relate $m(P)$ and the rank of the abelian subgroups of P.

The first part of the next lemma is well-known (see Theorem 6 of [19]), but we include the proof for the sake of completeness.

Lemma 5.1. *Let P be a finite p-group and p^j the minimum degree of the non-linear irreducible characters of P. Then the following hold.*

(i) $d(P) \geq 2j$.
(ii) *If $\gamma_{n+1}(P) \neq 1$, then $|\gamma_n(P)/\gamma_{n+1}(P)\gamma_n(P)^p| \geq p^j$.*

Proof. (i) Let M be a normal subgroup of P such that $|P' : M| = p$ and write $\overline{P} = P/M$. Since $d(\overline{P}) \leq d(P)$ and $m(\overline{P}) \geq m(P)$, we may assume that P' has order p. By Problem 2.13 of [6], for instance, $p^{2j} = |P : Z(P)|$ and, since $P/Z(P)$ is elementary abelian, it follows that $d(P) \geq 2j$.

(ii) Let M be a normal subgroup of P of index p in $\gamma_{n+1}(P)$. Let $V = P/\Phi(P)$ and $U = \gamma_n(P)/\gamma_{n+1}(P)\gamma_n(P)^p$. Write $\overline{P} = P/M$. We have a bilinear pairing $V \times U \to \gamma_{n+1}(\overline{P})$ determined by commutation. Assume that $|U| < p^j$. Then, there exist $u_1, \ldots, u_{j-1} \in U$ such that $U = \langle u_1, \ldots, u_{j-1}\rangle$. Also, $|V : C_V(u_i)| \leq p$ for all i. Write $W = \cap_{i=1}^{j-1} C_V(u_i)$. We have that $|V : W| \leq p^{j-1}$ and W commutes with U. Let W_1 be the preimage in P of W. Hence $[W_1, \gamma_n(P)] < \gamma_{n+1}(P)$. Using Lemma 2.1 of [22], this implies that $W_1' < P'$. This contradicts Theorem 1 of [19]. $\square$

Corollary 5.2. *Let P be a p-group of class ≥ 3 and $m(P) = p^j$. Then P has an abelian subgroup of rank at least j. Furthermore, if $p > 2$ and $Z(P)$ is cyclic then P has an abelian subgroup of rank $\geq j + 1$.*

Proof. Let $c = c(P)$. Then $[\gamma_{c-1}(P), \gamma_{c-1}(P)] \leq \gamma_{2(c-1)}(P) = 1$, so $\gamma_{c-1}(P)$ is abelian. By the previous lemma, its rank is at least j.

Assume now that $p > 2$ and $Z(P)$ is cyclic. We may assume that the rank of all abelian subgroups of P is $\leq j$ and we want to obtain a contradiction. Let $A = \Omega_1(\gamma_{c-1}(P))$. Then $\Omega_1(\gamma_c(P)) \leq A$. Hence, there exist $a_1, \ldots, a_{j-1} \in A$ such that

$$A = \langle \Omega_1(\gamma_c(P)), a_1, \ldots, a_{j-1} \rangle.$$

Also, $C_P(a_i)$ has index $\leq p$ in P, since $[a_i, P]$ has order $\leq p$ (we are using that $[a_i, P] \leq \Omega_1(\gamma_c(P)) \leq Z(P)$). Thus $|P : C_P(A)| \leq p^{j-1}$. Now, since the number of generators of $\gamma_{c-1}(P)$ is j, the number of generators of A is also j. Thus A is a maximal normal abelian subgroup of exponent p of P. By a theorem of J. Alperin (see Satz III.12.1 of [3]), every element of order p of $C_P(A)$ belongs to A and therefore is central in $C_P(A)$. Now, by a theorem of Thompson (see Hilfssatz III.12.2 of [3]), $d(C_P(A)) \leq d(A) = j$. Hence

$$d(P) \leq d(P/C_P(A)) + d(C_P(A)) \leq 2j - 1,$$

a contradiction with Lemma 5.1. □

If the nilpotence class of P is 2 and $Z(P)$ is cyclic, we can obtain a similar result.

Lemma 5.3. *Let P be a p-group of class 2 and assume that $Z(P)$ is cyclic. If $m(P) = p^j$ then there exists an abelian subgroup of rank at least j. Furthermore, if p is odd then P has an abelian subgroup of rank $\geq j + 1$.*

Proof. Let $V = H/P' = \Omega_1(P/P')$. By Lemma 5.1, $d(V) = d(P) \geq 2j$. Since $Z(P)$ is cyclic and P has class 2, $|H'| = p$. As before, commutation determines an alternating form $\alpha \colon V \times V \to H'$.

Since the dimension of V is at least $2j$, there exists an isotropic subspace W of V of dimension at least j. Then the preimage of W in H is abelian and has rank $\geq j$, as desired.

Assume now that $p > 2$. We define a group homomorphism $\varphi \colon H/P' \to P'/(P')^p$ by $\varphi(hP') = h^p(P')^p$. Let $V_1 = \operatorname{Ker} \varphi$. The dimension of V_1 is at least $2j - 1$, so there exists an isotropic subspace W_1 of V_1 of dimension $\geq j$. Let K be the preimage of W_1 in H. Then $d(K) \geq d(W_1) \geq j$ and K is abelian.

Finally,

$$d(K) = \log_p |K/K^p| = \log_p |K/(P')^p| = \log_p(|K/P'||P'/(P')^p|) \geq j + 1,$$

where the second equality holds because $P' \leq K$ and $W_1 \leq \operatorname{Ker} \varphi$. This concludes the proof. □

The results obtained in this lemma are best possible, as any extraspecial p-group when p is odd and central products of a quaternion group and dihedral groups of order 8 if $p = 2$ show.

6. Orbit sizes and $m(P)$

We have just studied the influence of $m(P)$ on the structure of a p-group P. Now, we shall show that this invariant is also important in our problem.

We need a series of lemmas. Let R be a non-nilpotent just infinite p-adic space group. By Lemma 3.2, R is a subgroup of finite index of a semidirect product $S = M \rtimes P$, where M is a free $\mathbb{Z}_p$-module and P is a finite p-group that acts faithfully on M. We will assume this notation in the remaining. We will also keep the notation of the proof of the following lemma throughout this section.

Lemma 6.1. *Let M be a free $\mathbb{Z}_p$-module and let P act on M. Then there exists a $\mathbb{Z}_pP$-module U, which is $\mathbb{Z}_p$-free, such that $\mathrm{Irr}(M/p^nM) \cong U/p^nU$ as $\mathbb{Z}_pP$-modules for every n. Furthermore, if the action of P on M is faithful then P also acts faithfully on U.*

Proof. Let $k \geq s$. Since $M/p^{k-s}M$ is canonically isomorphic to p^sM/p^kM, there exist canonical isomorphisms of $\mathbb{Z}_pP$-modules

$$\tau_{k,k-s} \colon \mathrm{Irr}(p^sM/p^kM) \to \mathrm{Irr}(M/p^{k-s}M).$$

Now, we write $\alpha_{k,k-s}$ to denote the composition of the restriction homomorphism from $\mathrm{Irr}(M/p^kM)$ onto $\mathrm{Irr}(p^sM/p^kM)$ and $\tau_{k,k-s}$. Note that $\alpha_{k,k-s}(\chi) = \chi^{p^s}$. It is easy to check that the P-modules $(\mathrm{Irr}(M/p^kM))_{k\in\mathbb{N}}$ with the surjective P-homomorphisms $(\alpha_{k,n})_{k\geq n}$ form an inverse system. Let U be the inverse limit of this system. Of course, for every n, $\mathrm{Irr}(M/p^nM)$ and U/p^nU are isomorphic $\mathbb{Z}_pP$-modules.

Assume now that P acts faithfully on M. By way of contradiction, suppose that there exists $1 \neq g \in P$ that acts trivially on U. Then g acts trivially on $U/p^nU \cong \mathrm{Irr}(M/p^nM)$ for every n. Hence g acts trivially on M/p^nM for every n. It follows that g acts trivially on M, a contradiction. □

Lemma 6.2. *With the notation above, let $u \in U$. For any positive integer k, we write u_k to denote the image of u in U/p^kU. Then there exists an integer $k_0 = k_0(u)$ such that for every $k \geq k_0$, $C_P(u) = C_P(u_k)$.*

Proof. Let $C = \cap_{k=1}^{\infty} C_P(u_k)$. It is clear that $C_P(u) \leq C$. We want to prove the reverse inequality. Assume that $g \in P$ does not act trivially on u, so that $u^gu^{-1} \notin p^kU$ for some integer k. Therefore $g \notin C$ and $C = C_P(u)$. Since

$$C_P(u_1) \geq C_P(u_2) \geq C_P(u_3) \geq \cdots$$

and P is finite, there exists k_0 such that if $k \geq k_0$ then $C = C_P(u_k)$. Thus $C_P(u) = C_P(u_k)$ for $k \geq k_0$, as desired. □

We write $\phi_k \colon U/p^kU \to \mathrm{Irr}(M/p^kM)$ to denote the group isomorphisms whose existence was proved in Lemma 6.1. By Problem 6.18 of [6], for instance, $\phi_k(u_k)$ extends to its stabilizer in S. Write $\psi_k(u_k)$ to denote any of these extensions. Now, by Clifford's correspondence (Theorem 6.11 of [6]), $\chi_{u_k} = \psi_k(u_k)^S$ is an irreducible character of S. Observe that if $k \geq k_0$

$$\chi_{u_k}(1) = |S : I_S(\phi_k(u_k))| = |P : I_P(\phi_k(u_k))| = |P : C_P(u_k)| = |P : C_P(u)|.$$

This way we can obtain information about the character degrees of S. However, we are interested in the character degrees of R. Our next result shows that all the degrees of S constructed in this way are indeed members of $\mathrm{cd}(R)$.

Lemma 6.3. *With the notation above, there exists a positive integer $k_1 = k_1(u)$ such that for every $k \geq k_1$, $(\chi_{u_k})_R \in \mathrm{Irr}(R)$.*

Proof. By Lemma 3.2, we know that $S = MR$ and $M \cap R = T(R)$. By Problem 5.2 of [6],

$$(\chi_{u_k})_R = ((\psi_k(u_k))^S)_R = \left((\psi_k(u_k))_{R\cap I_S(\phi_k(u_k))}\right)^R.$$

We need to show that when k is large enough this last character is irreducible. It is clear that $(\phi_k(u_k))_T$ is invariant in $R \cap I_S(\phi_k(u_k))$. We need to show that indeed $R \cap I_S(\phi_k(u_k))$ is the inertia subgroup of $(\phi_k(u_k))_T$ in R. If we prove this, then the result will follow using Clifford's correspondence.

Since M/T is finite, there exists s such that $p^s M \leq T$. By the construction of Lemma 6.1, U is the inverse limit of $(\mathrm{Irr}(M/p^k M), \alpha_{k,n})$. For $k > s$ we have the following commutative diagram, where the maps are homomorphisms of $\mathbb{Z}_p P$-modules, the left vertical arrow denotes the canonical projection and the right vertical arrow is the homomorphism $\alpha_{k,k-s}$:

$$\begin{array}{ccc} U/p^k U & \xrightarrow{\phi_k} & \mathrm{Irr}(M/p^k M) \\ \downarrow & & \downarrow \\ U/p^{k-s} U & \xrightarrow{\phi_{k-s}} & \mathrm{Irr}(M/p^{k-s} M) \end{array}$$

Now, suppose that $k \geq k_0 + s = k_1$. Then $C_P(u_k) = C_P(u_{k-s})$, by Lemma 6.2. Since the vertical arrows of the diagram are P-isomorphisms, we conclude that $I_P(\phi_k(u_k)) = I_P(\phi_{k-s}(u_{k-s}))$. Using the notation of the proof of Lemma 6.1, we observe that $\phi_k(u_k)_{p^s M} = \tau^{-1}_{k,k-s}(\phi_{k-s}(u_{k-s}))$. Thus $\phi_k(u_k)$ is invariant under a given element of P if and only if $\phi_k(u_k)_{p^s M}$ is invariant under that element. In particular, we deduce that the inertia groups in S of $\phi_k(u_k)$ and $\phi_k(u_k)_T$ coincide. Hence $R \cap I_S(\phi_k(u_k))$ is the inertia subgroup of $(\phi_k(u_k))_T$ in R, as desired. □

Lemma 6.4. *With the notation above, let K be a normal subgroup of finite index of R. Then*

$$\mathrm{os}(P, U) \subseteq \mathrm{cd}(R|K).$$

Proof. Let $n \in \mathrm{os}(P, U)$ and $u \in U$ such that $|P : C_P(u)| = n$. There exist m such that $u \in p^m U - p^{m+1} U$ and s such that $p^s M \subseteq K$. Now, if $k - m > s$ then the order of u_k is greater that p^s. Thus the order of the character $\phi_k(u_k)$ is greater than p^s. Therefore $K \not\leq \mathrm{Ker}\,\phi_k(u_k)$ and we conclude that $K \not\leq \mathrm{Ker}\,\chi_{u_k}$.

Since, by Lemma 6.2, $C_P(u) = C_P(u_k)$ for large k, we obtain that

$$n = |P : C_P(u_k)| = |P : I_P(\phi_k(u_k))| = \chi_{u_k}(1) \in \mathrm{cd}(S).$$

By Lemma 6.3, if k is large enough, $(\chi_{u_k})_R \in \mathrm{Irr}(R)$. We deduce that $n \in \mathrm{cd}(R|K)$. □

Next we prove the main result of this section, whose proof is now immediate.

Theorem 6.5. *Let R be a non-metabelian (non-nilpotent) just infinite p-adic space group and K a normal subgroup of finite index. Write $m(R) = p^j$. Then*

$$|\,\mathrm{cd}(R|K)| \geq j + 1 - \epsilon(p).$$

Proof. Since P is not abelian, $m(P) \geq m(R)$. By extending scalars we may view U as a faithful $\mathbb{Q}_p P$-module. By the previous lemma and Proposition 2.2

$$|\operatorname{cd}(R|K)| \geq |\operatorname{os}(P, U)| \geq d(A)$$

for every abelian subgroup A of P. Since P acts faithfully and irreducibly on T, $Z(P)$ is cyclic. Now, the result follows from Corollary 5.2 and Lemma 5.3. □

7. Class bounding sets

Now, with the help of Theorem 6.5 and Theorem A, we can present the proofs of Theorem B and Theorem D, which provide new class bounding sets.

Theorem 7.1. *Let $p^j = \min(\mathcal{S} - \{1\})$ and assume that $j > 1$. If the cardinality of $\mathcal{S}$ is less than or equal to $j + 2 - \epsilon(p)$ then $\mathcal{S}$ is (strongly) class bounding.*

Proof. Assume that $\mathcal{S}$ has cardinality $\leq j + 2 - \epsilon(p)$ and $\min(\mathcal{S} - \{1\}) = p^j > p$. Suppose that $\mathcal{S}$ is not strongly class bounding. Then, by Theorem A, there exists a non-nilpotent just infinite p-adic space group R such that $\operatorname{cd}(R) \subseteq \mathcal{S}$. Since R is not nilpotent, it has finite quotients of arbitrarily large nilpotence class. By Theorem 2.7 of [9] we have that R is not metabelian. Hence $P(R)$ is not abelian. Since R is just infinite and is not metabelian, then $K = R''$ is a normal subgroup of finite index of P (observe that by Proposition 1.19 of [1] K is closed). By Theorem 5.12 of [6], 1 and p^j do not belong to $\operatorname{cd}(R|K)$. Now, we can apply Theorem 6.5 to obtain that

$$|\mathcal{S}| \geq |\operatorname{cd}(R)| \geq 2 + j + 1 - \epsilon(p) = j + 3 - \epsilon(p),$$

a contradiction with the hypothesis. □

Theorem 7.2. *Assume that $\mathcal{S} = \{1\} \cup \mathcal{R} \cup \mathcal{T}$, where $\mathcal{R}$ and $\mathcal{T}$ are non-empty sets of powers of p, $p < p^j = \min(\mathcal{R})$, $\{1\} \cup \mathcal{R}$ is strongly class bounding and $\min(\mathcal{T}) > \max(\mathcal{R})^2$. If $|\mathcal{T}| \leq j - \epsilon(p)$ then $\mathcal{S}$ is (strongly) class bounding.*

Proof. By way of contradiction, suppose that $\mathcal{S}$ is not strongly class bounding. As before, there exists a non-metabelian non-nilpotent just infinite p-adic space group R such that $\operatorname{cd}(R) \subseteq \mathcal{S}$.

Since $\{1\} \cup \mathcal{R}$ is strongly class bounding there exists an integer n such that for every finite p-group P with character degrees contained in $\{1\} \cup \mathcal{R}$, $c(P) \leq n$. Let $K = \gamma_{n+1}(R)$ and let χ be an arbitrary element of $\operatorname{Irr}(R)$ such that $\chi(1) \in \{1\} \cup \mathcal{R}$. The finite group $R/\operatorname{Ker}\chi$ has a faithful character whose degree belongs to $\mathcal{R}$ and, by the fact that $\min(\mathcal{T}) > \max(\mathcal{R})^2$ and Theorem 4.3 of [6], $\operatorname{cd}(R/\operatorname{Ker}\chi) \subseteq \{1\} \cup \mathcal{R}$. We conclude that $K \leq \operatorname{Ker}\chi$. Hence, $\operatorname{cd}(R|K) \subseteq \mathcal{T}$. This contradicts Theorem 6.5. The theorem follows. □

8. Sets that do not bound the class

In this section we prove Theorem E. Before proceeding with the details of the construction that provides the non class bounding sets, we will explain briefly the way the group looks like. We work in the group ring of an extraspecial p-group E of order p^{2j+1} for $j > 1$ over the p-adic integers. Within this group ring we find an appropriate infinite abelian subgroup A on which E acts by left multiplication. The semidirect product $G = A \rtimes E$ has finite quotients which are p-groups of arbitrarily large nilpotence class. Most of the work is to prove that $m(G) \geq p^j$. For this we need to show that if the inertia subgroup of a character of A is "large" then it must be equal to G. Corollary 8.2 is a key step toward the proof that this is the case. Once this is established in Theorem 8.4, we obtain that the sets $\{1, p^j, \dots, p^{2j+1}\}$ are not class bounding for any $j > 1$ by using ideas from the rest of the article. Finally, using techniques of Isaacs and Slattery [11], we obtain the full strength of Theorem E in Theorem 8.5.

We begin with the following technical lemma, which is essential for the proof of Corollary 8.2.

Lemma 8.1. *Let P be a finite p-group such that $|P'| = p$. Assume that the exponent of P is $p > 2$ or that $p = 2$ and the exponent of P/P' is 2. Suppose that $\{x_1, \dots, x_n\} \subseteq P - P'$ is a (minimal) set of generators of P and that z is a generator of P'. Let $\Delta(P)$ the augmentation ideal of $\mathbb{Z}_pP$. Then for every $k \geq 1$, the ideal $(z-1)\Delta(P)^k$ of $\mathbb{Z}_pP$ is generated as a $\mathbb{Z}_p[z]$-module by the set J_k consisting of the elements of the form*

$$(z-1)^{\alpha+1}(x_1-1)^{\beta_1}(x_2-1)^{\beta_2}\dots(x_n-1)^{\beta_n}$$

where $0 \leq \alpha \leq (k+1)/2$, $0 \leq \beta_i \leq p-1$ for all $1 \leq i \leq n$ and $2\alpha+\beta_1+\beta_2+\dots+\beta_n \geq k$.

Proof. There exist $g, h \in P$ such that $z = [g, h]$. Then

$$\begin{aligned} z-1 = [g,h]-1 &= g^{-1}h^{-1}gh - 1 = (g^{-1}h^{-1} - h^{-1}g^{-1})gh \\ &= \big((g^{-1}-1)(h^{-1}-1) - (h^{-1}-1)(g^{-1}-1)\big)\, gh \in \Delta(P)^2. \end{aligned}$$

This implies that

$$(z-1)^{\alpha}(x_1-1)^{\beta_1}\dots(x_n-1)^{\beta_n} \in \Delta(P)^{2\alpha}\Delta(P)^{\beta_1}\dots\Delta(P)^{\beta_n} \subseteq \Delta(P)^k,$$

since $2\alpha+\beta_1+\beta_2+\dots+\beta_n \geq k$. Now it is clear that J_k is contained in $(z-1)\Delta(P)^k$ for every k.

We work to prove that any element of $(z-1)\Delta(P)^k$ can be obtained from elements in J_k. First, we assume that $p > 2$. We argue by induction on k. The result is clear for $k = 1$. We assume that it holds for $k-1$ and that $k > 1$. First, we claim that for every $i \leq n$, $(z-1)(x_i-1)^p$ belongs to the $\mathbb{Z}_p[z]$-module generated by the elements $(z-1)^p(x_i-1)^s$, where $1 \leq s \leq p-1$. By the binomial theorem,

$$(x_i-1)^p = x_i^p - 1 + p(x_i-1)h = p(x_i-1)h,$$

where h is a polynomial in (x_i-1) of degree $\leq p-2$. Now,

$$(z-1)(x_i-1)^p = (z-1)p(x_i-1)h = f(z)(z-1)^p(x_i-1)h, \tag{1}$$

where we have applied Lemma 4.1 in the last equality. The claim follows.

Let $[x_i, x_j] = z^{a_{ij}}$ for $1 \leq i, j \leq n$. Observe that

$$\begin{aligned} [x_i, x_j] - 1 &= x_i^{-1}x_j^{-1}x_ix_j - 1 = x_i^{-1}x_j^{-1}(x_ix_j - x_jx_i) \\ &= x_i^{-1}x_j^{-1}((x_i-1)(x_j-1) - (x_j-1)(x_i-1)), \end{aligned}$$

and therefore

$$\begin{aligned} (x_i-1)(x_j-1) &= (x_j-1)(x_i-1) + x_jx_i(z^{a_{ij}}-1) \\ &= (x_j-1)(x_i-1) + (z^{a_{ij}}-1)(x_j-1)(x_i-1) \\ &\quad + (z^{a_{ij}}-1)(x_j-1) + (z^{a_{ij}}-1)(x_i-1) + (z^{a_{ij}}-1). \end{aligned} \tag{2}$$

Now, we want to see that the set $(x_i-1)J_{k-1}$ is contained in the $\mathbb{Z}_p[z]$-module generated by J_k. This is a routine calculation using equations (1) and (2). We will just sketch the proof. Let $y = (z-1)^{\alpha+1}(x_1-1)^{\beta_1}(x_2-1)^{\beta_2}\dots(x_n-1)^{\beta_n} \in J_{k-1}$. If x_i commutes with x_j for all $j < i$, then

$$(x_i-1)y = (z-1)^{\alpha+1}(x_1-1)^{\beta_1}\dots(x_{i-1}-1)^{\beta_{i-1}}(x_i-1)^{\beta_i+1}(x_{i+1}-1)^{\beta_{i+1}}\dots(x_n-1)^{\beta_n}.$$

If $\beta_i < p-1$ then it is clear that this element belongs to J_k, so we may assume that $\beta_i = p-1$. Now, we have that

$$\begin{aligned}(x_i-1)y =& (z-1)^{\alpha}(x_1-1)^{\beta_1}\dots(x_{i-1}-1)^{\beta_{i-1}}\left\{(z-1)(x_i-1)^p\right\}\cdot\\ &\cdot(x_{i+1}-1)^{\beta_{i+1}}\dots(x_n-1)^{\beta_n}.\end{aligned}$$

But we have proved that $(z-1)(x_i-1)^p$ is a sum of "monomials" of the form $g_s(z)(z-1)^p(x_i-1)^s$, where $g_s(z) \in \mathbb{Z}_p[z]$ and $1 \le s \le p-1$. Therefore $(x_i-1)y$ is a sum of "monomials" on $z-1, x_1-1, \dots, x_n-1$ where the exponent of x_j-1 is β_j for $j \neq i$, the exponent of x_i-1 is at least 1 (and at most $p-1$) and the exponent of $z-1$ is $\beta+p$. All we have to do is to check that the last condition on the exponent that defines J_k holds. But this is easy.

Hence, we may assume that x_i does not commute with x_j for some $j < i$. Observe that $z-1$ divides all the monomials but the first of the right hand side on the last equality obtained in the penultimate paragraph. Using this fact and arguing as in the previous paragraph, we conclude that in this case $(x_i-1)y$ also belongs to the $\mathbb{Z}_p[z]$-module generated by J_k.

Assume now that $p = 2$. We want to prove that if $y \in J_{k-1}$ then $(x_i-1)y$ belongs to the $\mathbb{Z}_p[z]$-module generated by J_k for every i. The same argument as in the case $p > 2$ works except for when $x_i^2 = z$ and

$$y = (z-1)^{\alpha+1}(x_1-1)^{\beta_1}\dots(x_{i-1}-1)^{\beta_{i-1}}(x_i-1)(x_{i+1}-1)^{\beta_{i+1}}\dots(x_n-1)^{\beta_n}$$

for some $0 \le \alpha \le k/2$, $0 \le \beta_j \le 1$ and $2\alpha + \sum\beta_j \ge k-1$. In this case,

$$\begin{aligned}(z-1)(x_i-1)^2 &= (z-1)(z-2x_i+1)\\ &= (z-1)((z-1)-2(x_i-1))\\ &= (z-1)((z-1)(1+(x_i-1))\\ &= (z-1)^2x_i\\ &= (z-1)^2(x_i-1)+(z-1)^2,\end{aligned}$$

where the third equality follows from the fact that $(z-1)^2 = -2(z-1)$. Now, it is easy to check that $(x_i-1)y$ belongs to the module generated by J_k, as desired.

Since $\Delta(P) = \sum_i (x_i-1)\mathbb{Z}_pP$,

$$(z-1)\Delta(P)^k = (z-1)\sum_{i=1}^{n}(x_i-1)\Delta(P)^{k-1} = \sum_{i=1}^{n}(x_i-1)(z-1)\Delta(P)^{k-1}.$$

Now, by the inductive hypothesis and the fact that $(x_i-1)J_{k-1}$ is contained in the $\mathbb{Z}_p[z]$-module generated by J_k, we conclude that $(z-1)\Delta(P)^k$ is contained in the $\mathbb{Z}_p[z]$-module generated by J_k, as desired. □

Corollary 8.2. *Under the hypotheses of the previous lemma, assume that X is a non-abelian subgroup of P and let $A_k = (z-1)\Delta(P)^k$ for $k \ge n(p-1)$. Then $\Delta(P)A_k = \Delta(X)A_k$.*

Proof. We may assume that a minimal system of generators of X is $\{x_1, \ldots, x_m\}$ for some m. Applying the previous lemma to both P and X, we obtain that

$$A_k = \sum_{i_{m+1},\ldots,i_n=0}^{p-1} (z-1)\Delta(X)^{k-(i_{m+1}+\cdots+i_n)}(x_{m+1}-1)^{i_{m+1}} \ldots (x_n-1)^{i_n}.$$

In particular,

$$\begin{aligned}
\Delta(P)A_k &= A_{k+1} \\
&= \sum_{i_{m+1},\ldots,i_n=0}^{p-1} (z-1)\Delta(X)^{k+1-(i_{m+1}+\cdots+i_n)}(x_{m+1}-1)^{i_{m+1}} \ldots (x_n-1)^{i_n} \\
&= \Delta(X) \sum_{i_{m+1},\ldots,i_n=0}^{p-1} (z-1)\Delta(X)^{k-(i_{m+1}+\cdots+i_n)}(x_{m+1}-1)^{i_{m+1}} \ldots (x_n-1)^{i_n} \\
&= \Delta(X)A_k,
\end{aligned}$$

as desired. □

Finally, we need the next lemma to estimate the character degrees of the group that we will build to prove Theorem E.

Lemma 8.3. *Let G be the semidirect product of the finite groups H and A, where H acts on A and A is abelian. Then* $\operatorname{cd}(G)$ *is the set of numbers $|H : I_H(\lambda)|\beta(1)$ where λ runs over* $\operatorname{Irr}(A)$ *and $\beta \in \operatorname{Irr}(I_G(\lambda)/A)$.*

Proof. This is Lemma 2.3 of [20], for instance. □

Now, we are ready to prove Theorem E. The next result includes the main part of it.

Theorem 8.4. *Let $n, j > 1$ be integers. Then there exists a group of derived length 3 with set of character degrees $\{1, p^j, \ldots, p^{2j+1}\}$ and nilpotence class greater than n.*

Proof. Let E be the extraspecial p-group of exponent p and order p^{2j+1} (or the central product of j dihedral groups of order 8 if $p = 2$). Let z be a generator of E' and $\{x_1, \ldots, x_{2j}\}$ a system of generators of E. It is well known that any subgroup of E of index less than p^j is not abelian. We work in the group ring $\mathbb{Z}_pE$. Consider the ideal $A = (z-1)\Delta(E)^{2j(p-1)}$ as an infinite additive group. The group E acts on A via left multiplication. Let G be the semidirect product defined by these groups and this action. For any $g \in E$ and $a \in A$, $[a, g] = (g-1)a$. Since A is abelian, G has derived length three.

Since G has an abelian subgroup of index p^{2j+1}, all the character degrees of G are $\leq p^{2j+1}$. Now, assume that the stabilizer in E of some linear character of A is a subgroup T of index less than p^j. Hence T is not abelian. By Corollary 8.2

$$[A, E] = \Delta(E)A = \Delta(T)A = [A, T].$$

This means that every T-invariant character of A is E-invariant. Thus $T = E$. Using Lemma 8.3, we conclude that $m(G) = p^j$.

The group E has an elementary abelian subgroup of order p^{j+1}. Arguing as in the proof of Theorem B, we obtain that G has at least $j+3$ character degrees. Hence $\operatorname{cd}(G) = \{1, p^j, \ldots, p^{2j+1}\}$.

The group G is the inverse limit of $(G/p^kA)_{k\in\mathbb{N}}$. As remarked in Section 3, there exist groups among the members of this family of arbitrarily large nilpotence class. Also, since any normal subgroup of G of finite index contains some of the subgroups p^kA, we deduce that if k is large enough $\mathrm{cd}(G/p^kA) = \{1, p^j, \ldots, p^{2j+1}\}$. $\square$

Theorem 8.5. *Let n be an integer and $j > 1$. Assume that $\max(\mathcal{S}) < p^j$. Then there exists a p-group P of derived length 3 and class greater than n such that $\mathrm{cd}(P) = \mathcal{S} \cup \{p^j, \ldots, p^{2j+1}\}$.*

Proof. We will use the notation of the previous proof. By the proof of Theorem 2.3 and Corollary 2.4 of [11] there exists a p-group Q of nilpotence class 2 with a normal abelian subgroup Q_1 of index p^j such that Q/Q_1 is elementary abelian and $\mathrm{cd}(Q) = \mathcal{S}$.

Let E_1 be a normal abelian subgroup of E of index p^j. By Lemma 2.1 of [11] there exists a p-group H with normal subgroups X and Y such that $X \cap Y = 1$ and there exist isomorphisms $\alpha\colon H/X \to E$ and $\beta\colon H/Y \to Q$ mapping XY/X onto E_1 and XY/Y onto Q_1, respectively. By the proof of Theorem 2.3 of [11] $\mathrm{cd}(H) = \mathcal{S} \cup \{p^j\}$. Observe also that the class of H is 2.

We define an action of H on A in the following way: H/X acts on A as E acts on A and X acts trivially on A. The proof of the previous theorem shows that the inertia subgroup of any irreducible character of A has index $\geq p^j$ in H. Also, by the definition of the action, X fixes any character of A so this index cannot be greater than p^{2j+1}. Assume that T is the stabilizer in H of some character of A and let $\beta \in \mathrm{Irr}(T)$. Since X is abelian, $\beta(1) \leq |T : X|$. Using Lemma 8.3 we conclude that $\mathrm{cd}(HA) = \mathcal{S} \cup \{p^j, \ldots, p^{2j+1}\}$. We conclude the result as in the proof of the previous theorem. $\square$

9. Further remarks and questions

We hope that the techniques introduced in this paper will be useful to make further progress on the problem of determining the class bounding sets. However, we cannot even guess what sets may be expected to be class bounding. In this section we intend to show that there is still much work to be done before a complete answer can be found. Our first question is directly related to the results of this article.

Question 9.1. *Are the differences for the prime $p = 2$ in the statements of Theorems B and D really necessary?*

In particular, it would be interesting to decide the answer to the following question

Question 9.2. *Is $\{1, 2^2, 2^4, 2^5\}$ class bounding?*

As we have seen, any set of powers of an odd prime number p of cardinality 4 not containing p is class bounding. This seems the most likely counterexample for $p = 2$.

We think that the next question should have an affirmative answer.

Question 9.3. *Is every class bounding set strongly class bounding?*

A particular case is the following question.

Question 9.4. *Is it true that if $\mathcal{S} \supseteq \{1, p^j, \ldots, p^{2j+1}\}$ for some $j > 1$ then $\mathcal{S}$ is not class bounding?*

Our approach to the problem is not effective, in the sense that it does not give us any hint about the bounds for the class bounding sets. We have shown however that these bounds do not depend only on p.

Question 9.5. *Is it true that $b(\mathcal{S})$ is bounded by some function of p and n as $\mathcal{S}$ runs over the class bounding sets of cardinality n? This holds when $n = 2$ by a theorem of Isaacs and Passman* [10].

Question 9.6. *Find some bound for the class bounding sets obtained in this paper.*

References

[1] J. D. Dixon, M. P. F. du Sautoy, A. Mann, D. Segal, "Analytic Pro-p Groups", Second edition. Cambridge Studies in Advanced Mathematics, **61**. Cambridge University Press, Cambridge, 1999.

[2] R. M. Guralnick, *On the number of generators of a finite group*, Arch. Math. **53** (1989), 521–523.

[3] B. Huppert, "Endliche Gruppen", Springer-Verlag, Berlin-New York, 1967.

[4] B. Huppert, *A remark on the character-degrees of some p-groups*, Arch. Math. **59** (1992), 313–318.

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

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

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

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

[9] I. M. Isaacs, A. Moretó, *The character degrees and nilpotence class of a p-group*, J. Algebra **238** (2001), 827–842.

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

[11] I. M. Isaacs, M. C. Slattery, *Character degree sets that do not bound the class of a p-group*, to appear in Proc. Amer. Math. Soc.

[12] T. M. Keller, *Orbit sizes and character degrees*, Pacific J. Math. **187** (1999), 317–332.

[13] G. Klaas, C. R. Leedham-Green, W. Plesken, "Linear Pro-p Groups of Finite Width", Lecture Notes in Mathematics **1674**, Springer-Verlag, Berlin, 1997.

[14] L. Kovacs, *On finite soluble groups*, Math. Z. **103** (1968), 37–39.

[15] C. R. Leedham-Green, S. McKay, W. Plesken, *Space groups and groups of prime-power order. V. A bound to the dimension of space groups with fixed coclass*, Proc. London Math. Soc(3) **52** (1986), 73–94

[16] C. R. Leedham-Green, M. F. Newman, *Space groups and groups of prime-power order. I.,* Arch. Math. **35** (1980), 193–202.

[17] A. Lucchini, *A bound on the number of generators of a finite group*, Arch. Math. **53** (1989), 313–317.

[18] A. Mann, *Generators of* 2*-groups*, Israel J. Math. **10** (1971), 158–159.

[19] A. Mann, *Minimal characters of p-groups*, J. Group Theory **2** (1999), 225–250.

[20] A. Previtali, *Orbit lengths and character degrees in p-Sylow subgroups of some classical Lie groups*, J. Algebra **177** (1995), 658–675.

[21] J. M. Riedl, *Fitting heights of solvable groups with few character degrees*, J. Algebra **233** (2000), 287–308.

[22] M. C. Slattery, *Character degrees and nilpotence class in p-groups*, J. Austral Math. Soc. (Series A) **57** (1994), 76–80.

[23] J. S. Wilson, "Profinite Groups", LMS Monographs, New Series, **19**, The Clarendon Press, Oxford University Press, 1998.

Departamento de Matemáticas, Facultad de Ciencias, Universidad Autónoma de Madrid, Cantoblanco Ciudad Universitaria, 28049 Madrid (Spain)
E-mail address: ajaikin@uam.es

Departamento de Matemáticas, Universidad del País Vasco, Apartado 644, 48080 Bilbao (Spain)
E-mail address: mtbmoqua@lg.ehu.es