ISRAEL JOURNAL OF MATHEMATICS **142** (2004), 367–380

GROUPS WITH FEW CLASS SIZES AND THE CENTRALISER EQUALITY SUBGROUP

BY

AVINOAM MANN

Institute of Mathematics, The Hebrew University of Jerusalem
Givat Ram, Jerusalem 91904, Israel
e-mail: mann@math.huji.ac.il

ABSTRACT

Let G be a p-group whose conjugacy classes have at most k sizes. We prove that G is abelian-by- (exponent p^{k-1}) (if $p = 2$, exponent 2^{k-2}). It follows that a 2-group with three class sizes is metabelian. Various other results on class sizes are proved, and some conjectures are formulated.

1. Introduction

In this paper we consider only finite p-groups. Let G be such a group, and let G have conjugacy class sizes $n_1 = 1 < n_2 < \cdots < n_k$. Thus the classes of size n_1 consist of the central elements. We refer to classes of size n_2 as **minimal classes**, and to their elements as **minimal elements**. Recall that if $n_s = p^{b_s}$, and x has n_s conjugates, we say that x has **breadth** $b(x) = b_s$, and that the **breadth** of G is $b(G) = b_k$.

If $k = 2$, i.e. all non-central classes are of the same size, N. Ito [Ito] has shown that G contains a normal abelian subgroup A such that G/A has exponent p. This was sharpened by I. M. Isaacs [Isa] to $\exp(G/Z(G)) = p$. Alternative proofs were given in [M1] and [V] (both [Isa] and [M1] derive their result under somewhat weaker assumptions, see Proposition 11 below). Here we first generalise Ito's result to

THEOREM 1: *A p-group G with just k conjugacy class sizes is an extension of an abelian group by a group of exponent p^{k-1}. If $p = 2$ and $k \geq 3$, the exponent can be taken to be 2^{k-2}.*

Received September 16, 2003 and in revised form January 27, 2004

COROLLARY 2: *A 2-group with just three conjugacy class sizes is metabelian.*

K. Ishikawa [Ish] has recently proved that if $k = 2$, then the nilpotency class of G satisfies $cl(G) \leq 3$. No such result is possible if $k \geq 3$: for each order p^n there exist groups of that order of maximal class, i.e. of class $n-1$, with an abelian maximal subgroup, and then the class sizes are 1, p, and p^{n-2}. But it is natural to ask if there is a bound for the derived length of G. More precisely, we make the following

CONJECTURE: *There exist functions $f(s)$ and $g(p)$ such that, with the above notations, the subgroup of G generated by the classes of sizes $n_1, \dots, n_s$ has derived length at most $f(s)$, and the subgroup generated by the minimal elements has class at most $g(p)$.*

Indeed, in view of known results and conjectures about the analogous problem where the number of irreducible character degrees is given, one may surmise that $f(s)$ would be about s, or even $\log s$. For $g(p)$ a likely value may be p. Our modest contribution towards a proof of the conjecture consists of Corollary 2 and the following three results.

THEOREM 3: *A p-group G that is generated by its minimal classes satisfies $cl(G) \leq 3$.*

The proof, which is a minor modification of Ishikawa's argument, is indicated below. Moreover, a simplification of Ishikawa's argument was given by I. M. Isaacs, and his proof, which implies Theorem 3 immediately, is presented in [BI]. The argument in [BI] also shows that if $cl(G) = c \geq 4$, then the minimal elements generate a subgroup of class less than c.

Before stating the next results we recall that G^n denotes the subgroup of G generated by the nth powers, $\{\gamma_i(G)\}$ is the lower central series, and $\{\mathbf{Z}_i(G)\}$ is the upper central series. The commutator subgroup $\gamma_2(G)$ is also denoted by G'.

THEOREM 4: *The subgroup generated by the minimal classes of a 2-group G is of class 2 at most. This subgroup centralizes G^2.*

THEOREM 5: *The subgroup generated by the minimal classes of a metabelian p-group G is of class 3 at most. This subgroup centralizes $\gamma_3(G)$.*

Theorem 4, and the case $p = 2$ of Theorem 1, depend on the following

PROPOSITION 6: *If G is a 2-group, the minimal elements x satisfying $x^2 \in \mathbf{Z}(G)$ lie in $\mathbf{Z}_2(G)$.*

Other proofs employ the following characteristic subgroup of p-groups:

Definition: Let G be a p-group. The **centraliser equality subgroup $\mathbf{D}(G)$** of G is the subgroup generated by all elements of G satisfying $\mathbf{C}_G(x) = \mathbf{C}_G(x^p)$.

Obviously $\mathbf{D}(G) \geq \mathbf{Z}(G)$, and easy examples show that both equality and inequality of these two subgroups occur. The applicability of this subgroup in our context follows from the obvious fact that if x is a minimal element, then either $x^p \in \mathbf{Z}(G)$, or x is one of the generating elements of $\mathbf{D}(G)$. The next result shows, among other things, that $\mathbf{D}(G)$ always has a large centraliser. For its statement, recall that a **left n-Engel element** is an element x such that $[y, x, \ldots, x] = 1$ for all $y \in G$, where x occurs in the commutator n times.

THEOREM 7: *Let G be a p-group.*

(a) *$\mathbf{D}(G)$ is abelian.*
(b) *If $\mathbf{D}(G) \leq H \leq G$, and $cl(H) \leq p$, then $\mathbf{D}(G) \leq \mathbf{Z}(H)$.*
(c) *$\mathbf{C}_G(\mathbf{D}(G))$ contains $\mathbf{Z}_p(G)$, as well as all normal subgroups of G of class less than p, all elements of breadth less than p, and all left p-Engel elements.*
(d) *Let $c < p$. If N is maximal among the normal subgroups of G of class c, then $\mathbf{D}(G) \leq N$.*
(e) *$\mathbf{D}(G) \leq \mathbf{ZJ}(G)$.*

Here we recall that $\mathbf{J}(G)$ is the **Thompson subgroup** of G, the subgroup generated by all abelian subgroups of maximal order, and $\mathbf{ZJ}(G)$ is its centre, which is equal to the intersection of all these abelian subgroups. Recall also that various subgroups with properties similar to those of $\mathbf{J}(G)$ were defined; we have in mind the two $\mathbf{K}$-subgroups of Glauberman [BH, section X.8] and the Puig subgroup $\mathbf{L}(G)$ [BG, Appendix B]. It is not difficult to see that $\mathbf{D}(G)$ lies in the centre of all three of these subgroups.

The proof of (e) depends on a slight extension of a result of J. D. Gillam [G]:

PROPOSITION 8: *Let G be a metabelian p-group, and let B be an abelian subgroup of G of maximal order. Then G contains a normal abelian subgroup $C \leq B^G$ such that $|C| = |B|$.*

[G] does not have the claim that $C \leq B^G$, but it is easy to see that it follows from the proof. However, we prefer to give an independent proof of the full proposition.

These results are proved in the next section, starting with Theorem 7, then deriving Theorems 1 to 5 in order, interspersing this with Propositions 6 and 8 and other necessary intermediate results. In Section 3 we state and prove some further results. Most of these involve the quantitative invariant $b(x)$.

ACKNOWLEDGEMENT: I am very grateful to Gustavo Fernández-Alcober, and to the referee, for various suggestions regarding both the presentation of this paper and its proofs. Some of the results in Section 3 are due to the referee. I am also grateful to K. Ishikawa, Y. Barnea, A. Jaikin-Zapirain and I. M. Isaacs for communicating their results prior to publication.

2. Proofs

The following lemma is included for completeness.

LEMMA 9: *Let G be a p-group of class $c \leq p$, and let $x, y \in G$. Then x^p commutes with y if and only if x commutes with y^p.*

Proof: The claim of the lemma can be written as: $[x^p, y] = 1$ iff $[x, y^p] = 1$. We will show that both equalities are equivalent to $[x, y]^p = 1$. Note that $G' \leq Z_{c-1}(G)$, therefore $cl(\langle x, G'\rangle) \leq c - 1 \leq p - 1$, and in particular $\langle x, x^y\rangle = \langle x, [x, y]\rangle$ has class less than p, and is therefore a so-called **regular** p-group (see [Hu], III.10). In such groups $a^p = b^p$ is equivalent to $(a^{-1}b)^p = 1$, therefore $[x^p, y] = 1$, which is the same as $x^p = (y^{-1}xy)^p$, is equivalent to $[x, y]^p = 1$, and by symmetry the last equality is equivalent also to $[x, y^p] = 1$.

Proof of Theorem 7: (a) Write $D = \mathbf{D}(G)$, suppose that this subgroup is not abelian, and let $z \in \mathbf{Z}_2(D) - \mathbf{Z}(D)$, with $z^p \in \mathbf{Z}(D)$. Let x be one of the generating elements of D. Then $cl(\langle x, z\rangle) \leq 2$, therefore $[z, x^p] = [z^p, x] = 1$, and thus $z \in \mathbf{C}_G(x^p) = \mathbf{C}_G(x)$. Letting x range over all generators of D, we obtain $z \in \mathbf{Z}(D)$, a contradiction.

Note: This proof was suggested by the proof of Proposition 3 in [Isa].

(b) Let a be one of the generating elements of $\mathbf{D}(G)$, and $x \in H$. We prove that a commutes with x by induction on the order $o(x)$ of x. By the induction hypothesis a commutes with x^p, and by Lemma 9 this is equivalent to x commuting with a^p, i.e. $x \in \mathbf{C}(a^p) = \mathbf{C}(a)$.

(c) and (d) Since D is abelian, $cl(D\mathbf{Z}_p(G)) \leq p$. Similarly, if $N \triangleleft G$ and $cl(N) \leq p - 1$, then $cl(DN) \leq p$, by Fitting's Theorem. Thus the first two claims of (c) follow from (b). From this part of (c) it follows in turn that

$cl(DN) = cl(N)$, so if N is maximal of its class, we see that $DN = N$, i.e. $D \leq N$. This proves (d). For the next claim of (c) note that an element of breadth b is contained in a normal subgroup of class at most b, by [M3], Corollary 11 (an alternative proof is given in Proposition 17 below). Finally, if x is a left p-Engel element, and $y \in \mathbf{D}(G)$, then all commutators of weight $p+1$ in x and y either involve y at least twice, or x occurs p times. In either case the commutator is the identity, because $\mathbf{D}(G)$ is abelian and x is p-Engel, so $cl(\langle x, y\rangle) \leq p$, and we can quote (b).

We remark that once we have proved the last claim of (c), we can use it to prove in a similar manner that in (b) we can weaken the assumption on $cl(H)$ to H being a p-Engel group (i.e. all elements of H are left p-Engel).

Proof of Proposition 8: Let B be an abelian subgroup of maximal order in the metabelian p-group G. We choose B so that among the abelian subgroups of order $|B|$ in B^G it has a maximal intersection with G', and we may assume that it is not normal. Choose an element $x \in \mathbf{N}_G(\mathbf{N}_G(B)) - \mathbf{N}_G(B)$. Then $B \neq B^x$, and B and B^x normalise each other, so $A = BB^x = B[B,x]$ is of class 2, and since both B and B^x are maximal abelian subgroups, the equality $\mathbf{Z}(A) = B \cap B^x$ holds. We have $A \neq B$, therefore $[B,x] \not\leq B$. Now let $E = \mathbf{Z}(A)(B \cap G')[B,x] \leq A$; then $E \leq B^G$. Since G' is abelian, so are $(B \cap G')[B,x]$ and E. Moreover $A = BE$, and $B \cap E \geq \mathbf{Z}(A) = B \cap B^x$, so $|E| \geq |B|$, and the maximality implies $|E| = |B|$. But $E \cap G' > B \cap G'$, a contradiction.

Proof of Theorem 7(e): Let B be an abelian subgroup of maximal order of G. Then $K = DB$ is a metabelian group, so, by Proposition 8, K contains a normal abelian subgroup C such that $|C| = |B|$ and $C \leq B^K$. By part (d) applied to K, we have $D \leq C$, so that $K = DB \leq CB \leq B^K$, which implies $K = B$, i.e. $D \leq B$.

Proof of Proposition 6 (The present proof is due to the referee): Write $Z = \mathbf{Z}(G)$, let x be a minimal element satisfying $x^2 \in \mathbf{Z}(G)$, and first assume that $b := b(x) = 1$ and let $C = \mathbf{C}_G(x)$. Then $|G : C| = 2$, and x has a unique conjugate, say y. Then x and y lie in $\mathbf{Z}(C)$, so they commute, and $xy \in Z$. Therefore $N := Z\langle x\rangle^G = Z\langle x, y\rangle = Z\langle x\rangle$, so that $|N : Z| = 2$ and $N \leq \mathbf{Z}_2(G)$.

Next assume that $b > 1$, and let H be a maximal subgroup containing C. Then x has breadth $b-1$ in H, and this is the minimal breadth in H. Since G contains no elements of breadth 1, we have $\mathbf{Z}(H) = Z$. By induction $x \in \mathbf{Z}_2(H)$. Choose $h \in H - C$, and write $z = [x,h]$. Then $1 \neq z \in Z$. Therefore $\langle x, h\rangle$ is of class 2, so $z^2 = [x,h]^2 = [x^2,h] = 1$. Thus $U = \langle z\rangle$ is a central subgroup of order

2, and in G/U the coset xU is a minimal element of breadth $b-1$. Moreover, the elements of G that are central in G/U have at most two conjugates in G, and since $b > 1$, we get $\mathbf{Z}(G/U) = Z/U$, and also $\mathbf{Z}_2(G/U) = \mathbf{Z}_2(G)/U$. But by induction $xU \in \mathbf{Z}_2(G/U)$, and so $x \in \mathbf{Z}_2(G)$.

Proof of Theorem 1: The first part states that if G has k class sizes, then G is an extension of a normal abelian subgroup by a group of exponent p^{k-1}. To see this, just note that if $x \in G$ has order p^e $(\mathrm{mod}\, \mathbf{D}(G))$, then $x, x^p, \ldots, x^{p^e}$ have strictly increasing centralisers, so $e + 1 \leq k$, and thus $G/D(G)$ has exponent at most p^{k-1}.

Now assume that $p = 2$. We first note that then $\mathbf{D}(G)$ centralises all the minimal elements. Indeed, if x is minimal, then by Proposition 6, x lies either in $\mathbf{D}(G)$ or in $\mathbf{Z}_2(G)$, so our claim follows from parts (a) and (c) of Theorem 7. It follows that if we write N for the subgroup generated by all minimal elements, and $K = \mathbf{D}(G)N$, then $\mathbf{D}(G) \leq \mathbf{Z}(K)$.

Now let $z \notin K$. Then $\mathbf{C}_G(z) \neq \mathbf{C}_G(z^2)$, and if $z^2 \notin K$, then also $\mathbf{C}_G(z^2) \neq \mathbf{C}_G(z^4)$, etc. Therefore either $z^{2^{k-2}} \in K$, or that element is either central or minimal, so $z^{2^{k-2}} \in K$ in any case, and $G^{2^{k-2}} \leq K$. Moreover, for x a minimal element, if $x^2 \in \mathbf{Z}(G)$, we have $cl(\langle x, z\rangle) \leq 2$, so again $[z^2, x] = [z, x^2] = 1$, and G^2 centralises such elements x. But $G^{2^{k-2}}$ centralises also $\mathbf{D}(G)$, since $\mathbf{D}(G) \leq \mathbf{Z}(K)$. Thus $G^{2^{k-2}}$ is contained in the abelian subgroup $\mathbf{Z}(K)$.

Corollary 2 follows immediately from Theorem 1.

Proof of Theorem 3: As mentioned, this is given in [BI]. Alternatively, one can follow the proof of the main theorem of [Ish], with the following modifications (using the notations of [Ish]). First, the element z has to be chosen so that $z^p \in \gamma_{c-1}(G)$. This ensures that $[y, z]^p \in \mathbf{Z}(G)$. The element y can be chosen to lie in any given set of generators of G, so we take it to be in a minimal class. Finally, the elements $x_1, \ldots, x_m$ generate, not $\gamma_{c-1}(G)\mathbf{Z}(G)/\mathbf{Z}(G)$, but the socle of that group. With these changes the proof carries through.

Proof of Theorem 4: As pointed out in the introduction, an element of a minimal class is either in $\mathbf{D}(G)$ or satisfies $x^p \in \mathbf{Z}(G)$. Thus Proposition 6 implies that all minimal elements lie in the class 2 subgroup $\mathbf{D}(G)\mathbf{Z}_2(G)$. Moreover, if x is as in Proposition 6, and $y \in G$, then $cl\langle x, y\rangle \leq 2$, therefore $[x, y^2] = [x^2, y] = 1$. If x is any minimal element, then some power x^q of it satisfies $\mathbf{C}_G(x^q) = \mathbf{C}_G(x)$ and $(x^q)^2 \in \mathbf{Z}(G)$, and thus all minimal elements centralize all squares. This proves Theorem 4.

Theorem 5 also needs an auxiliary result.

PROPOSITION 10: *Let G be a p-group, let N be the subgroup generated by all minimal elements, and write $C = \mathbf{C}_G([N,G])$. Then $[C,N] \leq \mathbf{Z}(G)$ and $[C,G]$ centralises N.*

Proof: Let x be a minimal element, let $H = \mathbf{C}_G(x)$ and $Z = \mathbf{Z}(H)$, and let $y \in \mathbf{N}_G(H) - H$ satisfy $y^p \in H$. Then $1 \neq [x,y] \in Z$, therefore $[x,y]$ is either minimal or central, and in the first case $\mathbf{C}_G([x,y]) = \mathbf{C}_G(x)$, and in particular $C = \mathbf{C}_G([N,G]) \leq \mathbf{C}_G([x,y]) = \mathbf{C}_G(x)$, so $[C,x] = 1$. We thus may assume that $[x,y]$ is central, for each y as above. In that case we employ induction on $b = b(x)$. First, if $b = 1$, then $|G : \mathbf{C}_G(x)| = p$, and all elements outside $\mathbf{C}_G(x)$ can be taken as y above. Since these elements generate G, the assumption that $[x,y]$ is always central means that $x \in \mathbf{Z}_2(G)$, and $[x,G] \leq \mathbf{Z}(G)$. So let $b > 1$. Since $[x,y]$ is central, $\langle x,y \rangle$ has class 2, and as before we have $[x,y]^p = 1$. Write $K = \langle [x,y] \rangle$. Then in G/K the image of x is a minimal element, and has breadth $b-1$. All minimal elements in G/K are images of minimal elements in G, so if M/K is the subgroup generated by the minimal elements of G/K, then $M \leq N$ so $C/K \leq \mathbf{C}_{G/K}([M/K, G/K])$, and by induction on b we have $[C,x] \leq \mathbf{Z}(G \bmod K)$. However, since $b > 1$, we have, similarly to the proof of Proposition 6, $\mathbf{Z}(G \bmod K) = \mathbf{Z}(G)$, ending the proof that $[C,x] \leq \mathbf{Z}(G)$ for all minimal elements x. The last claim $[G,C] \leq \mathbf{C}(N)$ follows from the three subgroups lemma.

Proof of Theorem 5: In the notation of the last proposition, $G' \leq C$, so that $\gamma_3(G) \leq [C,G]$, and the same proposition implies that N centralizes $\gamma_3(G)$. In particular, $\gamma_3(N) \leq \mathbf{Z}(N)$, so $cl(N) \leq 3$.

3. Further results

As mentioned in the introduction, both [Isa] and [M1] prove that $exp(G/\mathbf{Z}(G) = p$ under weaker assumptions than that G has just two class sizes. In [Isa] it is assumed that there exists a normal subgroup N such that all classes outside N have the same size, and in [M1] it is assumed, as in [Ito], that of two distinct proper centralisers, none contains the other (but they may have different indices). We now combine these two assumptions.

PROPOSITION 11: *Let the p-group G contain a normal subgroup N, such that if two elements outside N have different centralizers, then neither of these centralizers contains the other. Then either G/N has exponent p, or G contains an abelian maximal subgroup (which contains N).*

Proof: Suppose that G/N has an element, say xN, of order greater than p. Then both x and x^p lie outside N, therefore they have the same centraliser. Thus all elements of G which do not have order $p \pmod N$ lie in the abelian subgroup $D := \mathbf{D}(G)$. Moreover, if $n \in N$, then xn also does not have order $p \pmod N$, so $xn \in D$, implying $n \in D$, i.e. $N \leq D$. If $|G : D| \geq p^2$, let $D \leq H \leq G$, with $|H : D| = p^2$. Then H/N is metabelian, has exponent greater than p, and all elements of H/N of order not p lie in D/N. But according to [HK], in a metabelian group of exponent greater than p, all elements of order not p generate a subgroup of index at most p. This is a contradiction.

The next two results are due to the referee. We denote by N the normal closure of some element $x \in G$, by $C = \mathbf{C}_G(x)$ its centraliser, and write $b = b(x)$, and $Z = \mathbf{Z}(G)$.

LEMMA 12: *If x has order p, then $|N| \leq p^{p^b}$. If equality holds, then N is elementary abelian.*

Proof: By induction on b. The case $b = 0$ is obvious. Let $b > 0$, let H be a maximal subgroup containing C, and let $M = \langle x \rangle^H$. By induction, $|M| \leq p^{p^{b-1}}$, and M has at most p conjugates in G, and these are all contained in H and normalise each other, so their product N has order at most p^{p^b}. Moreover, if equality holds, then N is a direct product of these conjugates, and M is elementary abelian by induction, hence so is N.

LEMMA 13: *If $x^p \in Z$, then $|N : N \cap Z| < p^{p^b}$.*

Proof: By the previous lemma, $|N : N \cap Z| \leq |N : \langle x^p \rangle| \leq p^{p^b}$. Suppose that equality holds; then again Lemma 12 implies that $N/\langle x^p \rangle$ is elementary abelian, with the p^b conjugates of x as a basis. Moreover, x must have the same breadth b (and not smaller) also modulo $\langle x^p \rangle$, which means that x has the same centraliser in G and in $G/\langle x^p \rangle$, in particular N is abelian. Then the product of the conjugates of x is central, so these conjugates are not independent modulo Z, hence $|N : N \cap Z| < p^{p^b}$.

PROPOSITION 14: *Let G be a p-group, and let $x \in G$ have breadth b and order $p^e \pmod{\mathbf{Z}(G)}$. Then $x \in \mathbf{Z}_r(G)$, where $r = 1 + e(p^b - 1)$, and $|N : N \cap Z| < p^{ep^b}$.*

Proof: The case $e = 1$ of the inequality is Lemma 13, and this inequality implies the inclusion in $Z_r(G)$. If $e > 1$, write $M = \langle x^p \rangle^G$; induction shows that $|M : M \cap Z| < p^{(e-1)p^b}$, and Lemma 12 shows that $|N : M| \leq p^{p^b}$, establishing the inequality. The inductive hypothesis yields also $x^p \in \mathbf{Z}_{1+(e-1)(p^b-1)}(G)$.

Letting $G^* := G/\mathbf{Z}_{(e-1)(p^b-1)}(G)$, the previous case shows that $x^* \in \mathbf{Z}_{p^b}(G^*)$, so $x \in \mathbf{Z}_{1+e(p^b-1)}(G)$.

A variation on this is:

PROPOSITION 15: *An element of breadth b lies in $\mathbf{Z}_{p^b}(\operatorname{mod}\mathbf{D}(G))$.*

Proof: We keep the notations b and C as above. We certainly may assume that $x \notin \mathbf{D}(G)$, so $b(x^p) \leq b-1$, and by induction $x^p \in K := \mathbf{Z}_{p^{b-1}}(G \operatorname{mod}\mathbf{D}(G))$. We can find a subgroup H such that $C \leq H \leq \mathbf{C}_G(x^p)$ and $|H : C| = p$. Then $x \in \mathbf{Z}(C) \triangleleft H$ and $x^p \in \mathbf{Z}(H)$. Let $y \in H - C$, and write $[x, y; n] = [x, y, y, \dots, y]$, where y occurs n times. Since $x \in \mathbf{Z}(C) \triangleleft H$, we have $[x, y; n] \in \mathbf{Z}(C)$. By the previous proposition, $x \in \mathbf{Z}_p(H)$, implying $[x, y; p] = 1$. Thus $[x, y; p-1] \in \mathbf{Z}(H)$. Induction on b implies that $[x, y; p-1] \in K$. That means that in G/K, the coset $[x, y; p-2]K$ is centralized by HK/K, so Proposition 14 yields $[x, y; p-2] \in \mathbf{Z}_{2p^{b-1}}(\operatorname{mod}\mathbf{D}(G))$. Working now modulo the last subgroup in the same way, etc., we get $[x, y; p-i] \in \mathbf{Z}_{ip^{b-1}}(\operatorname{mod}\mathbf{D}(G))$. The case $i = p$ is our claim.

We next verify a special case of a conjecture of Y. Barnea and I. M. Isaacs. Write $n_2 = p^r$, $n_k = p^s$. It is conjectured in [BI] that $cl(G)$ is bounded in terms of $s - r$.† We first recall some concepts from [M2]. A non-central element $x \in G$ is **extreme**, if for all elements $y_1, \dots, y_t \in G$, either $[x, y_1, \dots, y_t] \in \mathbf{Z}(G)$ or $\mathbf{C}_G([x, y_1, \dots, y_t]) = \mathbf{C}_G(x)$. Elements of $\mathbf{Z}_2(G)$ are trivially extreme; other extreme elements are termed **properly extreme**. We quote the following two results:

R1. Minimal elements centralising G' are extreme ([M2], p. 46).

R2. Let $x, y \in G$. If x is extreme, does not lie in $\mathbf{Z}_{i+1}(G)$, and does not commute with y, then $b(y) > ib(x)$ ([M2], statement P8).

PROPOSITION 16: *In a 2-group G, all minimal elements are extreme and lie in $\mathbf{Z}_{s-r+2}(G)$. If $k = 3$, then $cl(G) \leq s - r + 3$.*

Proof: By Theorem 4, all minimal elements centralise G^2, so R1 implies that all minimal elements are extreme. If $\mathbf{Z}_{i+2}(G)$ is the first term of the upper central series containing the minimal element x, R2 shows that $s > ir \geq i + r - 1$, so $x \in \mathbf{Z}_{s-r+2}(G)$. If $k = 3$, then all elements outside $\mathbf{Z}_{s-r+2}(G)$ have p^s conjugates, so $G/\mathbf{Z}_{s-r+2}(G)$ has exponent 2, by [Isa], implying $cl(G) \leq s-r+3$.

† This conjecture has now been proved by A. Jaikin-Zapirain.

Next we give an alternative proof to a result of [M3] that was quoted in the proof of Theorem 7(c)

PROPOSITION 17: *If x is not central, then $cl(N) \leq b$.*

Proof: If $b = 1$, then C is maximal in G, hence normal, and $N \leq \mathbf{Z}(C) \lhd G$, so N is abelian. For $b > 1$, let K be the core of C, i.e. the maximal normal subgroup contained in C. Then $K = \mathbf{C}_G(N)$, and $\mathbf{Z}(N) = N \cap K$. Since C/K contains no normal subgroup of G/K, and $\mathbf{C}_{G/K}(xK) \geq \mathbf{Z}(G/K) \neq 1$, we see that $C/K \neq \mathbf{C}_{G/K}(xK)$, and thus $b(xK) < b$. By induction: $cl(N) = cl(N/N \cap K) + 1 = cl(NK/K) + 1 \leq (b-1) + 1$, and we are done.

Let us elaborate this argument. Define the **breadth sequence** of x as follows: for $x = 1$ the sequence is empty. For $x \neq 1$, the sequence consists of $b(x)$ followed by the breadth sequence of xK in G/K. For instance, if x is central then the sequence is $\{0\}$, and if $b = 1$ then the sequence is $\{1\}$. The above proof shows that the sequence is strictly decreasing. The **length** of the sequence is the number of elements in it.

COROLLARY 18: *If $x \neq 1$, then $cl(N)$ equals the length of the breadth sequence.*

This is seen by the proof of Proposition 17.

We end this paper with a couple of results on a special class of p-groups that was discussed by I. D. Macdonald [Mc]. If x has order p^n, then $p^{n-1}(p-1)$ powers of x generate $\langle x \rangle$. If two of these are conjugate, they are conjugate under $\mathbf{N}_G(\langle x \rangle)$, and the number of them in each conjugacy class is $|\mathbf{N}_G(\langle x \rangle) : \mathbf{C}_G(\langle x \rangle)|$, so the number of classes represented by these powers is $p^d(p-1)$, for some d. Since all these elements have the same breadth, it follows that the number of non-identity classes of a given breadth is divisible by $p-1$. In [LMM] groups having exactly $p-1$ minimal classes were discussed, while in [Mc] groups having exactly $p-1$ classes of maximal size are investigated. The main results there are: *Let G be a group of order p^n having just $p-1$ classes of size p^b, for $b = b(G)$. Then $cl(G) \geq 3$, $b(G) \geq 4$, and $n \leq b^2 + b$.* There exists such a group of order 2^7, class 3, and breadth 4, direct powers of this group yield other examples, and the acknowledgement in [Mc] indicates that there exist still other such 2-groups (the claim made in [M4], that the 2-groups constructed in [VLW] yield more examples, is wrong). Still other examples, of arbitrarily high class, were constructed by G. A. Fernández-Alcober and E. A. O'Brien. However, no example of odd order is known.

Here we indicate an alternative proof to the inequality $b \geq 4$, by showing that $b = 3$ is possible only for $p = 2$. We also show that $b = 4$ implies that $p \leq 3$. Thus the inequality for n shows that there are only finitely many such groups of breadth 4, and it becomes of interest to improve that inequality. In [LMM, p. 94] the improvement $n \leq b^2$ was remarked. We give the further improvement $n \leq b^2 - 1$. Even though this improvement is minute, the difference between the number of groups of order, say, 3^{16}, to the number of groups of order 3^{15}, is vast, so we feel justified in including this result here.

PROPOSITION 19: *Let $|G| = p^n$, and let G contain exactly $p-1$ classes of elements of breadth $b = b(G)$. If $b = 3$ then $p = 2$, and if $b = 4$ then $p \leq 3$. Moreover, $n \leq b^2 - 1$.*

Proof: First let $b = 3$. There are $p^3(p-1)$ elements of breadth 3. Let N be a normal subgroup of order p^2. Then either N is central and contains p^2 classes, or N contains p central elements and $p-1$ classes of size p. There are $p^n - p^2 - p^3(p-1)$ elements outside N and not of breadth 3, and these have breadth at most 2, so we obtain that the class number $k(G)$ of G is at least $p^{n-2} - 1 - p(p-1) + 2p - 1 + p - 1 = p^{n-2} - (p-3)(p-1)$.

If p is odd, then $k(G) \geq 3p^{n-3}$, so [GMMPS, Theorem 1] shows that one of the following holds: either $|G'| \leq p^2$, or $|G : \mathbf{Z}(G)| \leq p^3$, or G contains an abelian maximal subgroup M. In the first two cases $b(G) \leq 2$. In the third case, for any $x \notin M$, we have $\mathbf{Z}(G) = \mathbf{C}_M(x)$, $G' = [M, x]$ and $p^{b(x)} = |M : \mathbf{Z}(G)| = |G'|$. Thus all elements outside M have the same breadth, contradicting our assumptions.

The last statement of our proposition shows that to eliminate the breadth 3 case we have only to check 2-groups of orders up to 2^8.

Now assume that $b = 4$. A similar estimate, taking this time N of order p^3, yields the lower bound $k(G) \geq p^{n-3} - (p-4)(p-1)$. If $p > 5$, this is more than $5p^{n-4}$. For $p = 5$ the same inequality holds unless $k(G) = p^{n-3} - r$, where $0 < r \leq p-1$. Recall the result of P. Hall, that $k(G) \equiv |G| \bmod((p^2-1)(p-1))$ (see, e.g., [M1]), and note that $p^n \equiv p^{n-3} - r \bmod((p^2-1)(p-1))$ is impossible for these values of r and $p \geq 5$.

Thus $k(G) \geq 5p^{n-4}$ if $p \geq 5$, so Theorem 2 of [GMMPS] shows that one of four possibilities occur: either $|G'| \leq p^3$, or $|G : \mathbf{Z}(G)| \leq p^4$, or there exists a normal subgroup N of order p such that $|G/N : \mathbf{Z}(G/N)| \leq p^3$, or G contains a maximal subgroup M with $b(M) \leq 1$. The first two possibilities imply $b \leq 3$. In the third case $b(G/N) \leq 2$, implying again $b \leq 3$. Thus we have the last case.

Here if M is abelian, then as above we get the contradiction that all elements outside M have the same breadth. Thus $b(M) = 1$, meaning that $|M'| = p$ [Kn]. Then G/M' contains the maximal abelian subgroup M/M', so again all elements outside M/M' have the same breadth in G/M'. Since some of the elements of G outside M have breadth 4, and the others a smaller breadth, the elements of G/M' outside M/M' all have breadth 3, and the same centraliser in M/M', say C/M', where $|G : C| = p^4$. Let X be the set of elements of G of breadth 3. These lie outside M, since the elements of M have breadth at most 2, and there are $p^n - p^{n-1} - p^4(p-1) > p^{n-1}$ of them (note that $b = 4$ implies $n \geq 6$). Thus X generates G. If $x \in X$, then $\mathbf{C}_M(x) \leq C$, and because $b(x) = 3$, we have $\mathbf{C}_M(x) = C$. This implies $C \leq \mathbf{Z}(G)$, so again $b(G) \leq 3$, the final contradiction.

It remains to prove the inequality for n. Let x have the maximal breadth b, and let $1 < i < p$. The automorphism of $\langle x \rangle$ mapping x to x^i does not have a p-power order, therefore x and x^i are not conjugate in G. It follows that the $p-1$ classes of breadth b are the classes of $x, x^2, \ldots, x^{p-1}$, so all elements of breadth b are contained in the proper subgroup $\langle x \rangle^G$, and in particular they are contained in each maximal subgroup containing x. Connect $C = \mathbf{C}_G(x)$ to G by a maximal chain of subgroups H_i, with $C = H_0$, for each i choose an element x_i in $H_i - H_{i-1}$, and let $y_b = x_b$ and $y_i = y_b x_i$ for $i < b$. Write $L = \langle y_1, \ldots, y_b \rangle$; then $G = CL$, and the generators of L lie outside the maximal subgroup H_{b-1}, therefore they have breadth less than b. Let $D = \mathbf{C}_G(L)$. Since $|G : \mathbf{C}_G(y_i)| \leq p^{b-1}$, we have $|G : D| \leq p^{b(b-1)}$. All conjugates of x are conjugate to it by an element of L, so if $d \in D$ we have $(xd)^L = x^L d$, a set of size p^b. Thus xd has breadth b, and is one of the $(p-1)p^b$ elements of this breadth, so $|D| \leq (p-1)p^b$ implying $|D| \leq p^b$ and $|G| \leq p^{b^2}$.

So far this was the argument of [Mc], as modified in [LMM]. Now assume that the equality $n = b^2$ holds. Then the proof above shows that $|D| = p^b$. Let A be the set of elements of breadth b, and define a subgroup E by $E = \{w \in G \mid Aw = A\}$. Then $AE = A$, so A is a union of cosets of E, and $|E| \leq |A|$, implying $|E| \leq p^b$. On the other hand, we saw that $D \leq E$, therefore $D = E$ and E has order p^b. Change the definition of L and D by changing x_b to any other element of $G - H_{b-1}$. We still have $D = E$, so D remains unchanged, and in particular it centralises all such elements x_b, i.e. all elements outside H_{b-1}, which means that $D \leq Z := \mathbf{Z}(G)$. Since the reverse inclusion is obvious, we have $D = Z$. Let $d \in Z$. We saw that xd has breadth b, and so is conjugate to a power x^i, where $1 \leq i \leq p-1$. But in G/Z the cosets xZ and x^iZ are conjugate only if $i = 1$. Thus all elements in xZ are conjugate to x, which means that this coset is the conjugacy class of x. Then all commutators involving x lie in Z, so $x \in \mathbf{Z}_2(G)$.

Next, write $L_i = \langle y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_b \rangle$ and $D_i = \mathbf{C}_G(L_i)$. Again the equality $n = b^2$ implies that $|G : D_i| = p^{(b-1)^2}$ and $|D_i : Z| = p^{b-1}$. For $d \in D_i$ we have $(xd)^{L_i} = x^{L_i} d$, a set of size p^{b-1}. Assume also that $d \notin Z$; then $xd \notin xZ$, so xd is not conjugate to x. If xd is conjugate to x^i, $1 < i < p$, then $x \in \mathbf{Z}_2(G)$ implies that $x^i Z = xdZ$, and thus $x \in D_i$, a contradiction since x does not centralise any y_j. Therefore xd is not of maximal breadth, and thus $b(xd) = b - 1$, and all conjugates of xd have the form $x^y d$, $y \in L_i$. Taking any $w \in G$ we obtain $[xd, w] = (xd)^{-1}(xd)^w = (xd)^{-1} x^y d = d^{-1}[x, y]d = [x, y] \in Z$. Therefore $xd \in \mathbf{Z}_2(G)$ and $d \in \mathbf{Z}_2(G)$ and $D_i \leq \mathbf{Z}_2(G)$.

But the subgroups $D_1, \ldots, D_b$ generate their direct sum in G/Z, because, e.g., $D_1 \cap D_2 \cdots D_b = Z$, and this implies $|D_1 D_2 \cdots D_b : Z| = p^{b(b-1)}$, which in turn shows $D_1 \cdots D_b = G$ and thus G is of class 2, contradicting [Mc].

References

[BG] H. Bender and G. Glauberman, *Local Analysis for the Odd Order Theorem*, Cambridge University Press, Cambridge, 1994.

[BH] N. Blackburn and B. Huppert, *Finite Groups III*, Springer-Verlag, Berlin, 1982.

[BI] Y. Barnea and I. M. Isaacs, *Lie algebras with few centralizer dimensions*, Journal of Algebra **259** (2003), 284–299.

[C] M. Cartwright, *Class and breadth of a finite p-group*, The Bulletin of the London Mathematical Society **19** (1987), 425–430.

[G] J. D. Gillam, *A note on finite metabelian p-groups*, Proceedings of the American Mathematical Society **25** (1970), 189–190.

[GMMPS] N. Gavioli, A. Mann, V. Monti, A. Previtali and C. M. Scoppola, *Groups of prime power order with many conjugacy classes*, Journal of Algebra **202** (1998), 129–141.

[HK] G. T. Hogan and W. P. Kappe, *On the H_p-problem for finite p-groups*, Proceedings of the American Mathematical Society **20** (1969), 450–454.

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

[Isa] I. M. Isaacs, *Groups with many equal classes*, Duke Mathematical Journal **37** (1970), 501–506.

[Ish] K. Ishikawa, *On finite p-groups which have only two conjugacy lengths*, Israel Journal of Mathematics **129** (2002), 119–123.

[Ito] N. Ito, *On finite groups with given conjugate types I*, Nagoya Mathematical Journal **8** (1953), 17–28.

[Kn] H. G. Knoche, *Über den Frobeniusschen Klassbegriff in nilpotenten Gruppen*, Mathematische Zeitschrift **55** (1951), 71–83.

[LMM] P. Longobardi, M. Maj and A. Mann, *Minimal classes and maximal class in p-groups*, Israel Journal of Mathematics **110** (1999), 93 102.

[M1] A. Mann, *Conjugacy classes in finite groups*, Israel Journal of Mathematics **31** (1978), 78 84.

[M2] A. Mann, *Extreme elements of finite p-groups*, Rendiconti del Seminario Matematico della Università di Padova **83** (1990), 45–54.

[M3] A. Mann, *Space groups and groups of prime power order VII. Powerful p-groups and uncovered p-groups*, The Bulletin of the London Mathematical Society **24** (1992), 271–276.

[M4] A. Mann, *Review of [VLW]*, MR 85i 20023.

[Mc] I. D. Macdonald, *Finite p-groups with unique maximal classes*, Proceedings of the Edinburgh Mathematical Society **26** (1983), 233-239.

[V] L. Verardi, *On groups whose noncentral elements have the same finite number of conjugates*, Unione Matematica Italiana. Bollettino. A. Serie VII **2-A** (1988), 391–400.

[VLW] M. R. Vaughan-Lee and J. Wiegold, *Generation of p-groups by elements of bounded breadth*, Proceedings of the Royal Society of Edinburgh. Section A **95A** (1983), 215 221.