BULL. AUSTRAL. MATH. SOC. 20D15
VOL. 51 (1995) [353–368]

SOME BOUNDS FOR THE DEGREE OF COMMUTATIVITY OF A p-GROUP OF MAXIMAL CLASS

ANTONIO VERA-LÓPEZ AND GUSTAVO A. FERNÁNDEZ-ALCOBER

In this paper we obtain several lower bounds for the degree of commutativity of a p-group of maximal class of order p^m. All the bounds known up to now involve the prime p and are almost useless for small m. We introduce a new invariant b which is related with the commutator structure of the group G and get a bound depending only on b and m, not on p. As a consequence, we bound the derived length of G and the nilpotency class of a certain maximal subgroup in terms of b. On the other hand, we also generalise some results of Blackburn. Examples are given in order to check the sharpness of the bounds.

For p a prime number and $m \geqslant 4$, a group G of order p^m and nilpotency class $m-1$ is called a p-group of maximal class. Setting $G_i = \gamma_i(G)$ for $i \geqslant 2$, we have $G_{m-1} \neq 1$ and $G_i = 1$ for $i \geqslant m$. We define the characteristic maximal subgroup G_1 by means of

$$G_1/G_4 = C_{G/G_4}(G_2/G_4).$$

The degree of commutativity $c = c(G)$ of G is then given by

$$c(G) = \max\{k \leqslant m-2 \mid [G_i, G_j] \leqslant G_{i+j+k} \text{ for all } i, j \geqslant 1\}.$$

It is clear that $c(G) \geqslant 0$, and that $c(G) = m-2$ if and only if G_1 is Abelian. If we take elements $s \in G - (G_1 \cup C_G(G_{m-2}))$ and $s_1 \in G_1 - G_2$, we define recursively $s_i = [s_{i-1}, s]$ for $i \geqslant 2$. Then $s_i \in G_i - G_{i+1}$ for $1 \leqslant i \leqslant m-1$, so that $G_i = \langle s_i, G_{i+1}\rangle$ and, in particular, $G = \langle s, s_1, \ldots, s_{m-1}\rangle$. Since $[s_i, s_j] \in G_{i+j+c}$, we can define $\alpha(i,j) \in \mathbb{F}_p$ for $i + j \leqslant m - c - 1$ by the relation

$$[s_i, s_j] \equiv s_{i+j+c}^{\alpha(i,j)} \pmod{G_{i+j+c+1}}. \tag{1}$$

We suppose henceforth $p \geqslant 3$, the 2-groups of maximal class being well-known (see [2, III, 11.9]). Then the $\alpha(i,j)$'s satisfy the following conditions (see [8]):

(C1) At least one element $\alpha(1,j)$ is non-zero.

Received 30th May, 1994
This work has been supported by DGICYT grant PB91-0446 and by the University of the Basque Country.

(C2) $\alpha(i,j) = -\alpha(j,i)$ and $\alpha(i,i) = 0$ whenever defined.
(C3) $\alpha(i,j) = \alpha(i+1,j) + \alpha(i,j+1)$ for $i+j \leqslant m-c-2$.
(C4) $\alpha(i,j) = \alpha(i+p-1,j) = \alpha(i,j+p-1)$ for $i+j \leqslant m-c-p$.
(C5) For $i+j+k \leqslant m-2c-1$,

$$\alpha(i,j)\alpha(i+j+c,k) + \alpha(j,k)\alpha(j+k+c,i) + \alpha(k,i)\alpha(k+i+c,j) = 0.$$

We note that (C1) and (C4) together imply that we cannot have $\alpha(1,j) = 0$ for $p-1$ consecutive values of j.

As formula (1) shows, the commutator relations of G derived from the generators s_i are simpler when $c(G)$ is large. For this reason, it is interesting to obtain general lower bounds for $c(G)$, which will allow us to simplify calculations when handling p-groups of maximal class.

In this sense, the first known results are due to Blackburn [1], who can no doubt be considered as the pioneer in the study of this class of groups. He proves that $c(G/Z(G)) \geqslant 1$ always holds and gets the bound $m \leqslant p+1$ for the exponent of $|G|$ when $c(G) = 0$. We generalise this last inequality in the following theorem.

THEOREM 1. *Let $\mathcal{F}$ be the family of the p-groups of maximal class such that $c(G) \neq c(G/Z(G))$. If $G \in \mathcal{F}$ then $c(G) \geqslant m-p-1$.*

PROOF: Set $\overline{G} = G/Z(G)$. If $c(G) = m-2$, the theorem is obvious. Otherwise $c(G) \leqslant m-4$ and $c(\overline{G}) \geqslant c(G)+1$. Thus, for $i+j \leqslant m-c-2$ we have $[\overline{G}_i, \overline{G}_j] \leqslant \overline{G}_{i+j+c+1}$ whence $[G_i, G_j] \leqslant G_{i+j+c+1}$ and $\alpha(i,j) = 0$. If $c \leqslant m-p-2$ then (C4) implies $\alpha(1, m-c-2) = \alpha(1, m-c-p-1) = 0$. Consequently, $\alpha(1,j) = 0$ for all j, which contradicts (C1). □

For example, for any group G with $c(G) = 2$ and $c(\overline{G}) \geqslant 3$ we obtain $|G| \leqslant p^{p+3}$.

Define $a = a(G)$ by the condition that G_a is the maximal normal Abelian subgroup of G. Blackburn shows that $c(G) \geqslant m-p-1$ for $a = 2$ (that is, for G metabelian) and $c(G) \geqslant m-p-2a+4$ for $a \geqslant 3$. He also indicates that this is probably the best possible result for $a < p$. Later, Shepherd [8] and Leedham-Green and McKay [5] obtained independently the bound $c(G) \geqslant [(m-3p+7)/2]$ which depends only on m and p. This bound can be improved to $2c(G) \geqslant m-2p+5$ when G_1 has nilpotency class 2. This was proved by Leedham-Green and McKay [6, Theorem 9.7], as a consequence of their construction of all p-groups of maximal class with G_1 of class 2. They reduce this problem to the calculation of $\mathrm{Hom}_{C_p}\left(\mathcal{O}/\mathfrak{P}^{t-1} \wedge \mathcal{O}/\mathfrak{P}^{t-1}, \mathcal{O}/\mathfrak{P}^{m-t}\right)$ for certain m and t, where $\mathcal{O}$ is the ring of integers in the pth cyclotomic field generated by a primitive complex pth root θ of 1, $\mathfrak{P}$ is the ideal generated by $\kappa = \theta - 1$ and C_p acts via multiplication by θ. Next, we give a direct proof of this result which just involves

the basic properties of the $\alpha(i,j)$'s and the formula [8, Lemma 2.3]

$$(2)\quad \alpha(i,j) = \sum_{\nu=i}^{[(i+j-1)/2]} (-1)^{\nu-i}\binom{j-\nu-1}{\nu-i}\alpha(\nu,\nu+1) \quad \text{for } i+j \leqslant m-c-1,$$

which is easily derived from (C3).

THEOREM 2. *(Leedham-Green, McKay) Let $p \geqslant 5$ and suppose G_1 has nilpotency class 2. Except for the case when $|G| = 5^6$ and $c(G) = 0$, we have $2c(G) \geqslant m - 2p + 5$.*

PROOF: First of all, we observe that once the above-mentioned case is dropped, the result is easily checked for $p \geqslant m-c-1$. So we can suppose $p \leqslant m-c-2$. Since G_1 is of class 2, we have $[G_1, G_1] = G_t$ with $c+3 \leqslant t \leqslant m-1$ and $[G_1, G_t] = 1$. From the values of these commutators we deduce that $\alpha(1,j) = 0$ for $1 \leqslant j \leqslant t-c-2$ and, if $t \leqslant m-c-2$, also for $t \leqslant j \leqslant m-c-2$. (Note that, in this last case, we get $m-c-t-1$ consecutive zero values). Define k as

$$k = \min\{j \mid \alpha(1,j) \neq 0\}.$$

Since we cannot have $\alpha(1,j) = 0$ for $1 \leqslant j \leqslant p-1$, it follows that $t-c-1 \leqslant k \leqslant p-1$. It is clear, by induction on i and using (C3), that $\alpha(i,j) = 0$ for $i+j \leqslant k$.

If $k \leqslant p-5$ then $t \leqslant c+p-4$. On the other hand, $m-c-t-1 \leqslant p-2$ (otherwise we would get $p-1$ consecutive zeros). Combining these inequalities we obtain $2c \geqslant m-2p+5$ in this case.

Suppose now that $p-4 \leqslant k \leqslant p-1$. From (2) we have

$$\alpha(1,k) = \sum_{\nu=1}^{[k/2]} (-1)^{\nu-1}\binom{k-\nu-1}{\nu-1}\alpha(\nu,\nu+1).$$

If k is odd then $\nu + (\nu+1) \leqslant k$ and $\alpha(\nu,\nu+1) = 0$ for $\nu = 1, \ldots, [k/2]$. Hence $\alpha(1,k) = 0$, impossible. Consequently $k = 2l$ is even and $k = p-1$ or $p-3$. Formula (2) then yields

$$\alpha(1,k) = (-1)^{l-1}x, \qquad \alpha(1,k+1) = (-1)^{l-1}lx$$

and, if $k = p-3$,

$$\alpha(1,k+2) = (-1)^{l-1}\binom{l+1}{2}x + (-1)^l y, \quad \alpha(1,k+3) = (-1)^{l-1}\binom{l+2}{3}x + (-1)^l(l+1)y,$$

where we have put $x = \alpha(l,l+1)$ and $y = \alpha(l+1,l+2)$. Observe that $\alpha(1,k) \neq 0$ implies $x \neq 0$.

https://doi.org/10.1017/S0004972700014180 Published online by Cambridge University Press

If $k = p-1$, we derive $\alpha(1,1) = \alpha(1,p) = (-1)^{l-1} lx \neq 0$, a contradiction. If $k = p-3$ we have

$$0 = \alpha(1,p) = (-1)^{l-1}\binom{l+2}{3}x + (-1)^l(l+1)y,$$

whence $y = [(l+2)l/6]\, x$. Thus

$$\alpha(1,p-1) = (-1)^{l-1}\binom{l+1}{2}x + (-1)^l y = (-1)^{l-1}\frac{(2l+1)l}{6}x.$$

In this way, we have proved that $\alpha(1,j) \neq 0$ for $p-3 \leqslant j \leqslant p-1$. According to (C4), there can not exist more than $p-4$ consecutive values of j with $\alpha(1,j) = 0$. Consequently $m-c-t-1 \leqslant p-4$. On the other hand, from $t-c-1 \leqslant k$ we get $t \leqslant c+p-2$ and $2c \geqslant m-2p+5$ follows. □

Our main interest in the theory of p-groups of maximal class is the study of their number of conjugacy classes and the orders of the different centralisers of their elements (see [**9, 10, 11**]). We have focused on solving these problems for groups of small order ($|G| \leqslant p^9$) but p arbitrary. For this purpose, the aforementioned bounds give little information about $c(G)$, since p appears affected by a minus sign in all of them. This fact has led us to search for new lower bounds for $c(G)$ which are independent of p and good enough for small values of m. In the following, we expose the results of our research in this direction.

If G is a p-group of maximal class, we define

$$b = b(G) = \min\{k \mid [G_i, G_j] \leqslant G_{i+j+c+1} \text{ for all } i,j \geqslant k\}.$$

It is clear that $b = 1$ if and only if G_1 is Abelian, that is, $c(G) = m-2$. So we can restrict our attention to the case $b \geqslant 2$. Obviously $b \leqslant a$ and, if $t = [(m-c)/2]$, from $[G_t, G_t] = 1$ we derive $b \leqslant t$, that is, $c(G) \leqslant m-2b$. In particular, $b \leqslant m/2$ always holds and the value of b is controlled by m.

Now we can be precise about what kind of bounds we are looking for: bounds for $c(G)$ of the type

$$c(G) \geqslant \frac{m-\lambda b+\mu}{\nu},$$

where $\lambda, \nu \in \mathbb{N}$ and $\mu \in \mathbb{Z}$, which we shall call (m,b)-type bounds, in contrast with bounds like

$$c(G) \geqslant \frac{m-\lambda p+\mu}{\nu},$$

which we shall refer to as (m,p)-type bounds.

https://doi.org/10.1017/S0004972700014180 Published online by Cambridge University Press

From the definition of b we have $\alpha(i,j) = 0$ for $i,j \geqslant b$ whenever defined. Next, we see that the rest of the $\alpha(i,j)$'s can be expressed in terms of the $\alpha(k,b)$'s with $1 \leqslant k \leqslant b-1$.

In the remainder, we work with generalised binomial coefficients, that is, for $n, k \in \mathbb{Z}$,

$$\binom{n}{k} = \begin{cases} \dfrac{n(n-1)\dots(n-k+1)}{k!}, & \text{if } k \geqslant 1; \\ 1, & \text{if } k = 0; \\ 0, & \text{if } k < 0. \end{cases}$$

LEMMA 3. *Let* $1 \leqslant i \leqslant b-1$.

(i) *If* $b \leqslant j \leqslant m-c-i-1$ *then*

$$\alpha(i,j) = \sum_{k=0}^{b-i-1} (-1)^k \binom{j-b}{k} \alpha(i+k,b). \tag{3}$$

(ii) *If* $i < j \leqslant b-1$ *then*

$$\begin{aligned} \alpha(i,j) = &\sum_{k=0}^{j-i-1} \binom{b-j-1+k}{k} \alpha(i+k,b) \\ &+ \sum_{k=j-i}^{b-i-2} \left\{ \binom{b-j-1+k}{k} - \binom{b-j-1+k}{k+i-j} \right\} \alpha(i+k,b). \end{aligned} \tag{4}$$

PROOF:

(i) We argue by induction on $j \geqslant b$. If $j = b$ (3) trivially holds. Suppose $j > b$. From (C3) we have $\alpha(i,j) = \alpha(i,j-1) - \alpha(i+1,j-1)$. Now the result follows from the inductive hypothesis applied to $\alpha(i,j-1)$ and $\alpha(i+1,j-1)$, except for the case $i = b-1$, when $\alpha(i+1,j-1) = 0$.

(ii) It suffices to prove that, for $i \leqslant j \leqslant b-1$,

$$\alpha(i,j) = \sum_{k=i}^{b-1} \binom{b-i-j+k-1}{k-i} \alpha(k,b) + \sum_{k=j}^{b-1} \binom{b-i-j+k-1}{k-j} \alpha(b,k).$$

This can be done by backwards induction on $j \leqslant b-1$ and, for each fixed value of j, by applying backwards induction on $i \leqslant j$ and using (C3).

□

We note that $\alpha(b-1,j) \neq 0$ for $j = b, \dots, m-c-b$. Otherwise, since (3) yields $\alpha(b-1,j) = \alpha(b-1,b)$ for $b \leqslant j \leqslant m-c-b$, we would have $\alpha(b-1,j) = 0$ for all those j. But then $[G_{b-1}, G_j] \leqslant G_{b+j+c}$ for $j \geqslant b-1$, contradicting the definition of b.

https://doi.org/10.1017/S0004972700014180 Published online by Cambridge University Press

LEMMA 4. *If $G \in \mathcal{F}$, then $b = a$ and $c(G) = m - 2b$.*

PROOF: As shown in the proof of Theorem 1, $\alpha(i,j) = 0$ for $i + j \leqslant m - c - 2$. On the other hand, (3) yields

$$\alpha(1, m-c-2) = \sum_{k=0}^{b-2} (-1)^k \binom{m-c-2-b}{k} \alpha(k+1, b).$$

Suppose $c(G) \leqslant m - 2b - 1$. For $k = 0, \ldots, b-2$ we have $(k+1) + b \leqslant m - c - 2$, whence $\alpha(k+1, b) = 0$ and $\alpha(1, m-c-2) = 0$. Consequently $\alpha(1, j) = 0$ for all j, impossible. Hence $c(G) = m - 2b$. Since [**9**, Lemma 1.6] shows that $c(G) = m - 2a$, we have $b = a$. □

THEOREM 5.

(i) *Let $1 \leqslant i \leqslant b-1$. If $\alpha(i,j) \neq 0$ for $b \leqslant j \leqslant m - c - i - 1$, then $c(G) \geqslant m - p - b - i + 2$.*

(ii) *If $b = 2$ then $c(G) \geqslant m - p - 1$. Also, $c(G) \geqslant 1$ always holds.*

(iii) *If $b \geqslant 3$ then $c(G) \geqslant m - p - 2b + 4$. Hence $c(G) = m - p - 2b + k$ with $4 \leqslant k \leqslant p$.*

PROOF:

(i) If $c \leqslant m - p - b - i + 1$, we have at least $p - 1$ integers in the interval $[b, m-c-i-1]$. Choose $j \equiv i \pmod{p-1}$ such that $b \leqslant j \leqslant m-c-i-1$. Then (C4) implies $\alpha(i,j) = \alpha(i,i) = 0$, a contradiction.

(ii) As observed, $\alpha(b-1, j) \neq 0$ for $b \leqslant j \leqslant m - c - b$. From part (i), $c \geqslant m - p - 2b + 3$ for $b \geqslant 2$. This proves $c \geqslant m - p - 1$ for $b = 2$. Besides, if $c = 0$ then $G \in \mathcal{F}$ and Lemma 4 provides $m = 4$, impossible since $[G_1, G_2] \leqslant G_4$.

(iii) Suppose $c(G) = m - p - 2b + 3$. On the one hand we have

$$\alpha(b-2, m-c-b+1) = \alpha(b-2, m-c-b-p+2) = \alpha(b-2, b-1) = \alpha(b-2, b)$$

and, from (3),

$$\begin{aligned} \alpha(b-2, m-c-b+1) &= \alpha(b-2, b) - (m-c-2b+1)\alpha(b-1, b) \\ &= \alpha(b-2, b) - (p-2)\alpha(b-1, b). \end{aligned}$$

It follows that $\alpha(b-1, b) = 0$ in $\mathbb{F}_p$, impossible.

□

Parts (ii) and (iii) in the last theorem show that we can replace a by b in Blackburn's bounds. We observe that the inequality $c(G) \geqslant m - p - 2b + 3$ for $b \geqslant 2$ is also

proved, arguing in a different way, in [8, Lemma 1.21]. The bound in (ii) can not be improved, since Miech [7] proves that, for $p \geqslant 3$ and $m > p+1$, there exist metabelian p-groups of maximal class of order p^m and degree of commutativity $c(G) = m-p-1$. Nevertheless, the question of whether the bound in (iii) is best possible still remains.

COROLLARY 6. *Suppose $b \geqslant 2$. Then, $a = b = 2$ or $a \in [b, b+(p-5)/2]$, according as $p = 3$ or $p \geqslant 5$.*

PROOF: Suppose $c = m-2a$. If $\alpha(a-1,a) = 0$ then $[G_{a-1}, G_{a-1}] = [G_{a-1}, G_a] \leqslant G_{2a+c} = 1$, impossible. Hence $\alpha(a-1,a) \neq 0$ and $b = a$ in this case. On the other hand, if $c \neq m-2a$, [9, Lemma 1.6] yields $c \leqslant m-2a-1$. Since $c \geqslant m-p-2b+3$ for $b \geqslant 2$, we get $2a \leqslant p+2b-4$ and $a \leqslant b+(p-5)/2$. Thus $p \geqslant 5$ in this last case. So $p = 3$ implies $c = m-2a$ and we deduce that $a = b = 2$ from the bound $c \geqslant m-4$ (see [1, Theorem 3.13]). □

EXAMPLE. Let $p \geqslant 7$ be a prime number and $3 \leqslant a \leqslant (p-1)/2$. Then, for every $m \geqslant 4a-2$ there exists a p-group of maximal class G of order p^m with $b(G) = 2$ and $a(G) = a$. Hence the bounds for a in the previous corollary can not be improved for $b = 2$. (Note that the existence of groups with $b = a = 2$ is assured by Miech's construction of the metabelian p-groups of maximal class.)

The groups of our example can be presented as $G = \langle s, s_i \mid i \geqslant 1 \rangle$, subject to the relations:

(R1) $s^p = 1$;

(R2) $\prod_{k=0}^{p-1} s_{i+k}^{\binom{p}{k+1}} = 1$, for $i \geqslant 1$;

(R3) $s_i = 1$, for $i \geqslant m$;

(R4) $[s_i, s] = s_{i+1}$, for $i \geqslant 1$;

(R5) If $i \geqslant 2$, $[s_i, s_1] = \begin{cases} s_{i+c+1}, & \text{if } i > 2a-3; \\ s_{i+c+1} \prod_{t=0}^{2a-i-3} s_{i+c+t+2}^{\binom{a-2}{t}}, & \text{if } i \leqslant 2a-3; \end{cases}$

(R6) If $2 \leqslant j < i$, $[s_i, s_j] = \begin{cases} s_{m-1}^{(-1)^j \binom{a-j-1}{i-a}}, & \text{if } j \leqslant a-1 \text{ and} \\ & i \geqslant a \geqslant (i+j+1)/2; \\ 1, & \text{otherwise.} \end{cases}$

In (R5) the value of c is taken to be $m-2a-1$. This will be the degree of commutativity of the group in question.

The explicit construction of this group can be performed in the following steps:

(1) Define $G_a = \langle s_i \mid i \geqslant a \rangle$, with the corresponding relations among those above. This group is Abelian and has order p^{m-a}.

(2) Construct $G_2 = \langle s_i \mid i \geqslant 2 \rangle$ as an Abelian extension of G_a (for the theory of

Abelian extensions, see [**12**, III, Section 8]). We have that $|G_2| = p^{m-2}$.

(3) Get $G_1 = \langle s_i \mid i \geqslant 1 \rangle$ as a cyclic extension of G_2. Then $|G_1| = p^{m-1}$.

(4) Finally, consider the automorphism s of G_1 defined by $s_i^s = s_i s_{i+1}$ for $i \geqslant 1$. Then, $o(s) = p$ and $G = \mathrm{Hol}\,(G_1, \langle s \rangle)$ is the group desired.

Shepherd constructs in [**8**, Example 3.26], a metabelian p-group of maximal class of order p^{p+2} with $c(G) = 1$. This shows that, for $b = 2$, there exist no (m,b)-type bounds. But, according to the following theorem, they do exist for $b \geqslant 3$.

THEOREM 7. *If $b \geqslant 3$ then $c(G) \geqslant (m - 3b + 3)/2$.*

PROOF: Assume, on the contrary, that $2c \leqslant m - 3b + 2$. Then $m - 2c - 1 \geqslant 3b - 3$ and we can apply (C5) to the triple $(b-2, b-1, b)$ getting

$$\alpha(b-2,b-1)\alpha(2b+c-3,b) + \alpha(b-1,b)\alpha(2b+c-1,b-2) + \alpha(b,b-2)\alpha(2b+c-2,b-1) = 0.$$

Since $\alpha(2b+c-3,b) = 0$ and $\alpha(b-1,2b+c-2) = \alpha(b-1,b) \neq 0$, we derive

$$\alpha(b-2,b) = \alpha(b-2,2b+c-1) = \alpha(b-2,b) - (b+c-1)\alpha(b-1,b),$$

by making use of (3). Thus $b + c - 1 \equiv 0 \pmod{p}$ and $b + c - 1 \geqslant p$. On the other hand, from Theorem 5 we have $p \geqslant m - c - 2b + 4$. Consequently $2c \geqslant m - 3b + 5$, a contradiction. □

From this (m,b)-type bound we can derive several results about the nilpotency class of G_1 and the derived length of G, similar to those obtained in [**8**] and [**5**] from the (m,p)-type bound $2c \geqslant m - 3p + 6$, but with b playing the role of p.

In the following, we denote the nilpotency class of a nilpotent group K by $\mathrm{cl}\,K$ and its derived length by $\mathrm{dl}\,K$. Also, for $x \in \mathbb{R}$, let $[x]_*$ denote the smallest integer greater than or equal to x.

COROLLARY 8. *Suppose $b \geqslant 3$. The following assertions hold:*

(i) *If $c(G) \neq 1$ then $\mathrm{cl}\,G_1 \leqslant b$. If $c(G) = 1$ then $\mathrm{cl}\,G_1 \leqslant [3(b-1)/2]_*$.*

(ii) *If $m \geqslant 9b - 19$ then $\mathrm{cl}\,G_1 \leqslant 3$.*

PROOF:

(i) If $c(G) = 0$, we have $m = 2b$ from Lemma 4. Now, Corollary 1.15 of [**8**] yields $\mathrm{cl}\,G_1 \leqslant m/2 = b$. Suppose $c(G) \geqslant 1$. An easy induction gives $\gamma_{i+1}(G_1) \leqslant G_{i(c+1)+2}$ for $i \geqslant 1$. So $i(c+1)+2 \geqslant m$ proves that $\mathrm{cl}\,G_1 \leqslant i$. If $c \geqslant 2$ then $(b-2)c \geqslant 2b-5$, that is, $b(c+1)+2 \geqslant 2c+3b-3 \geqslant m$, by using Theorem 7. Consequently $\mathrm{cl}\,G_1 \leqslant b$ in this case. Analogously, for $c = 1$ it suffices to show that $3b-1 \geqslant m$, which is again a consequence of Theorem 7.

https://doi.org/10.1017/S0004972700014180 Published online by Cambridge University Press

(ii) We have $\gamma_4(G_1) \leqslant G_{3c+5}$ and

$$3c+5 \geqslant \frac{3}{2}(m-3b+3)+5 = m + \frac{m-9b+19}{2} \geqslant m,$$

since $m \geqslant 9b-19$.

□

We note that for $b=2$ there is no possible bound for $\operatorname{cl} G_1$ of the kind of the preceding corollary, since the group in the aforementioned example of Shepherd is metabelian and $\operatorname{cl} G_1 = (p+1)/2$.

COROLLARY 9.

(i) $\operatorname{dl} G \leqslant [\log_2(2a+2)]$.

Moreover, if $b \geqslant 3$ we have:

(ii) $\operatorname{dl} G \leqslant [\log_2 3b]$.

(iii) *If $m \geqslant 2a+3b-13$ or $m \geqslant 9b-31$ then* $\operatorname{dl} G \leqslant 3$.

PROOF: First of all, we note that $G^{(i)} \leqslant G_t$ with $t = 3.2^{i-1} + c\left(2^{i-1}-1\right) - 1$ is easily proved by induction on $i \geqslant 1$.

(i) Let $i \geqslant 2$. If $G^{(i)} \neq 1$ then $G_{a-1} \leqslant G^{(i-1)}$. Since $c(G/Z(G)) \geqslant 1$, it follows in any case that $G^{(i-1)} \leqslant G_t$ with $t = 3.2^{i-2} + \left(2^{i-2}-1\right) - 1 = 2^i - 2$. Consequently, $2^{i+1} \leqslant 2a+2$ and $i+1 \leqslant \log_2(2a+2)$. Thus $\operatorname{dl} G \leqslant [\log_2(2a+2)]$, as required.

(ii) If $c(G) = 0$ then $a = b$ and (i) yields $\operatorname{dl} G \leqslant [\log_2(2b+2)]$. Hence we suppose $c(G) \geqslant 1$. If $G^{(i)} \neq 1$ then

$$3.2^{i-1} + c\left(2^{i-1}-1\right) - 1 \leqslant m-1 \leqslant 2c+3b-4,$$

since $b \geqslant 3$. Consequently,

$$2^{i-1} \leqslant \frac{3c+3b-3}{c+3} = 3 + \frac{3b-12}{c+3} \leqslant 3 + \frac{3b-12}{4} = \frac{3b}{4},$$

whence $2^{i+1} \leqslant 3b$ and $i+1 \leqslant \log_2 3b$. Thus $\operatorname{dl} G \leqslant [\log_2 3b]$.

(iii) If $m \geqslant 2a+3b-13$ then

$$c+5 \geqslant \frac{m-3b+3}{2} + 5 = \frac{m-3b+13}{2} \geqslant a,$$

whence $G'' \leqslant G_a$ and $\operatorname{dl} G \leqslant 3$. On the other hand, if $m \geqslant 9b-31$ then

$$3c+11 \geqslant 3\,\frac{m-3b+3}{2} + 11 = m + \frac{m-9b+31}{2} \geqslant m$$

https://doi.org/10.1017/S0004972700014180 Published online by Cambridge University Press

and $G''' = 1$. □

For $p \geqslant 5$ and $3 \leqslant m \leqslant p$, Kovács and Leedham-Green construct a p-group of maximal class of order p^m and derived length $[\log_2(m+1)]$ (see [3]). For these groups we have $a = [(m-1)/2]$ and, consequently, $\mathrm{dl}\, G = [\log_2(2a+2)]$. (Note that $[\log_2(m+1)] = [\log_2 m]$ when m is even.) Hence, for any $a \geqslant 2$ and any prime $p \geqslant 2a+1$, there exists a p-group of maximal class G with $\mathrm{dl}\, G = [\log_2(2a+2)]$.

From Theorem 7 we can also derive that the bound $c \geqslant m-p-2b+4$ in Theorem 5 (iii) can be improved for certain values of m.

COROLLARY 10. *Suppose that $b \geqslant 3$ and let $4 \leqslant k \leqslant p$. If $m \leqslant 2(p-k)+b+4$ then $c \geqslant m-p-2b+k$.*

PROOF: If $c \leqslant m-p-2b+k-1$ then $m-3b+3 \leqslant 2c$ implies $m \geqslant 2(p-k)+b+5$, impossible. □

The bound in Theorem 7 is the best possible for $b = 3$ or 4, as the following examples show.

EXAMPLE. Let $p \geqslant 11$ be a prime number and m an odd integer such that $11 \leqslant m \leqslant p$. Then, there exists a p-group of maximal class G of order p^m with $c(G) = (m-9)/2$ and $b(G) = a(G) = 4$.

This group can be obtained by means of the Campbell-Hausdorff formula (see [4]) from the Lie algebra L over $\mathbb{F}_p$ with basis $(e_0, e_1, \ldots, e_{m-1})$ in which the Lie product is defined as follows:

$$\begin{cases} [e_i, e_i] = 0, & \text{for } i \geqslant 0; \\ [e_i, e_0] = -[e_0, e_i] = e_{i+1}, & \text{for } i \geqslant 1; \\ [e_i, e_j] = -[e_j, e_i] = \left\{ \sum_{k=i}^{j-1} (-1)^{k-i} \binom{j-k-1}{k-i} \lambda_k \right\} e_{i+j+t}, & \text{for } 1 \leqslant i < j. \end{cases}$$

Here, $e_i = 0$ for $i \geqslant m$, $t = (m-9)/2$, $\lambda_i = 0$ for $i \geqslant 4$, $\lambda_3 = 1$, $\lambda_2 = (t+2)/2$ and $\lambda_1 = (3t+4)(t+2)/4(t+1)$. (Note that $t+1 \not\equiv 0 \pmod p$.)

It can be checked, with the help of the theorem given in the Appendix, that these relations indeed yield a Lie algebra.

In the particular case when $m = 11$, we obtain for every $p \geqslant 11$ a p-group of maximal class for which $c(G) = 1$ and $\mathrm{cl}\, G_1 = 5 = [3(b-1)/2]_* > b$.

We can derive in a similar way the group in the next example.

EXAMPLE. Let $p \geqslant 11$ be a prime number and $8 \leqslant m \leqslant p$ an even integer. Then, there exists a p-group of maximal class G of order p^m such that $c(G) = (m-6)/2$ and $b(G) = a(G) = 3$.

Nevertheless, the bound $c \geqslant (m-3b+3)/2$ can be improved for $b \geqslant 5$, as we see in the next theorem.

THEOREM 11. *If $b \geqslant 5$ then $c(G) \geqslant (m-3b+4)/2$. Moreover, unless $b=5$, $c=1$ and $m=p=13$, we have $c(G) \geqslant (m-3b+5)/2$.*

PROOF: First of all, Corollary 6 implies that $p \geqslant 5$. Suppose that $2c \leqslant m-3b+4$. Then $m-2c-1 \geqslant 3b-5$ and from (C5) we have

$$\alpha(b-4,b-3)\alpha(c+2b-7,b)+\alpha(b-3,b)\alpha(c+2b-3,b-4)+\alpha(b,b-4)\alpha(c+2b-4,b-3)=0, \tag{5}$$

$$\alpha(b-4,b-2)\alpha(c+2b-6,b)+\alpha(b-2,b)\alpha(c+2b-2,b-4)+\alpha(b,b-4)\alpha(c+2b-4,b-2)=0, \tag{6}$$

$$\alpha(b-4,b-1)\alpha(c+2b-5,b)+\alpha(b-1,b)\alpha(c+2b-1,b-4)+\alpha(b,b-4)\alpha(c+2b-4,b-1)=0, \tag{7}$$

$$\alpha(b-3,b-2)\alpha(c+2b-5,b)+\alpha(b-2,b)\alpha(c+2b-2,b-3)+\alpha(b,b-3)\alpha(c+2b-3,b-2)=0. \tag{8}$$

If $c=0$ then $m \geqslant 3b-4$. On the other hand, $G \in \mathcal{F}$ and $m=2b$. So $2b \geqslant 3b-4$ and $b \leqslant 4$, impossible. Thus $c \geqslant 1$ and $c+2b-6 \geqslant b$, whence $\alpha(c+2b-6,b) = \alpha(c+2b-5,b)=0$.

Taking into account formula (3), from (8) we derive

$$(c+b-3)\alpha(b-3,b)\alpha(b-1,b)-(c+b-2)\alpha(b-2,b)^2+\binom{c+b-2}{2}\alpha(b-2,b)\alpha(b-1,b)=0, \tag{9}$$

and, from (7),

$$(c+b-1)\alpha(b-3,b)=\binom{c+b-1}{2}\alpha(b-2,b)-\binom{c+b-1}{3}\alpha(b-1,b).$$

If $c+b-1 \equiv 0 \pmod{p}$ then $c+b-1 \geqslant p \geqslant m-c-2b+4$ and $2c \geqslant m-3b+5$, a contradiction. Hence

$$\alpha(b-3,b)=\frac{c+b-2}{2}\alpha(b-2,b)-\frac{(c+b-2)(c+b-3)}{6}\alpha(b-1,b). \tag{10}$$

By substituting this value into (9), we obtain

$$\alpha(b-2,b)^2-(c+b-3)\alpha(b-2,b)\alpha(b-1,b)+\frac{(c+b-3)^2}{6}\alpha(b-1,b)^2=0.$$

Defining $u \in \mathbb{F}_p$ by the condition

$$\alpha(b-2,b)=u(c+b-3)\alpha(b-1,b), \tag{11}$$

https://doi.org/10.1017/S0004972700014180 Published online by Cambridge University Press

it follows that $6u^2-6u+1=0$. (Note that u is well-defined, since $(c+b-3)\alpha(b-1,b)\neq 0$.) Moreover, from (10) we have

$$\alpha(b-3,b)=(3u-1)\frac{(c+b-2)(c+b-3)}{6}\alpha(b-1,b). \tag{12}$$

Now, equation (6) yields

$$\begin{aligned}(c+b-4)\alpha(b-4,b)\alpha(b-1,b)&=(c+b-2)\alpha(b-3,b)\alpha(b-2,b)\\&\quad-\binom{c+b-2}{2}\alpha(b-2,b)^2+\binom{c+b-2}{3}\alpha(b-2,b)\alpha(b-1,b)\end{aligned}$$

and, taking into account (11) and (12),

$$\alpha(b-4,b)=(2u-1)\frac{(c+b-2)(c+b-3)^2}{12(c+b-4)}\alpha(b-1,b). \tag{13}$$

If either $c\geqslant 2$ or $b\geqslant 6$, we have $\alpha(c+2b-7,b)=0$. So (5) reduces to

$$\alpha(b-4,c+2b-3)\alpha(b-3,b)=\alpha(b-4,b)\alpha(b-3,c+2b-4).$$

We can use (3) to express this equality in terms of the $\alpha(i,b)$ with $b-4\leqslant i\leqslant b-1$. Then (11), (12) and (13) give, bearing in mind that $\alpha(b-1,b)\neq 0$,

$$(24u^2-24u+5)c=-(24b-72)u^2+(24b-72)u-(5b-13).$$

Since $6u^2-6u+1=0$, it follows that $c=-(b-1)$ in $\mathbb{F}_p$, that is, $c+b-1\equiv 0 \pmod p$, which is impossible as we know.

So necessarily $b=5$ and $c=1$. Condition (5) is now expressed as

$$\alpha(1,8)\alpha(2,5)=\alpha(1,5)\alpha(2,7)+\alpha(1,2)\alpha(4,5).$$

From (3), (4), (11), (12) and (13) it follows that $72u^2-30u+6=0$. This, together with $6u^2-6u+1=0$, implies $p=13$ and $u=2$. If now $2c=m-3b+3$, we can apply (C5) to the triple $(2,4,5)$ getting

$$\alpha(2,4)\alpha(7,5)+\alpha(4,5)\alpha(10,2)+\alpha(5,2)\alpha(8,4)=0,$$

whence

$$\alpha(2,5)=\alpha(2,10)=\alpha(2,5)-5\alpha(3,5)+10\alpha(4,5)$$

and $\alpha(3,5)=2\alpha(4,5)$. But we also have $\alpha(3,5)=3u\alpha(4,5)=6\alpha(4,5)$ and $\alpha(4,5)\neq 0$, impossible. Hence $2c=m-3b+4$ and $m=13$ in this case.

https://doi.org/10.1017/S0004972700014180 Published online by Cambridge University Press

Consequently, in the rest of the cases we have $2c \geqslant m - 3b + 5$, which completes the proof. □

There is no problem in constructing a p-group of maximal class G of order 13^{13} with $b(G) = 5$ and $c(G) = 1$. To do this, consider the Lie algebra L over $\mathbb{F}_{13}$ with basis $(e_0, e_1, \dots, e_{12})$ and defined by the products

$$\begin{cases} [e_i, e_i] = 0, & \text{for } i \geqslant 0; \\ [e_i, e_0] = -[e_0, e_i] = e_{i+1}, & \text{for } i \geqslant 1; \\ [e_i, e_j] = -[e_j, e_i] = \left\{ \sum_{k=i}^{j-1} (-1)^{k-i} \binom{j-k-1}{k-i} \lambda_k \right\} e_{i+j+1}, & \text{for } 1 \leqslant i < j. \end{cases}$$

Here, $e_i = 0$ for $i \geqslant 13$, $\lambda_i = 0$ for $i \geqslant 5$, $\lambda_4 = 1$, $\lambda_3 = 6$, $\lambda_2 = 3$ and $\lambda_1 = 4$.

It would be desirable to obtain an (m, b)-type bound for $c(G)$ which is attained for all values of b. In order to do this, one should develop a systematic method of handling the equations which arise from applying Shepherd's product formula (C5) to the different triples (i, j, k).

Appendix: The construction of the Lie algebras

The construction of the Lie algebras in the examples after Corollary 10 and Theorem 11 is based on the following result.

Theorem. *Let K be a field and L a finite dimensional algebra over K, with $m = \dim L \geqslant 4$. Let $(e_0, e_1, \dots, e_{m-1})$ be a basis of L and define $e_i = 0$ for $i \geqslant m$. Denote the multiplication in L by $[\ ,\ ]$ and set*

$$\mathcal{J}(i, j, k) = [e_i, e_j, e_k] + [e_j, e_k, e_i] + [e_k, e_i, e_j]$$

for $i, j, k \geqslant 0$. (We are adopting the convention that $[x, y, z] = [[x, y], z]$.) Suppose there exist integers a and c, with $0 \leqslant c \leqslant m - 2$ and $1 \leqslant a \leqslant (m - c)/2$, such that $[\ ,\ ]$ satisfies the following conditions:

(i) $[e_i, e_i] = 0$, *for* $i \geqslant 0$.
(ii) $[e_i, e_j] = -[e_j, e_i]$, *for* $0 \leqslant i < j$.
(iii) $[e_i, e_0] = e_{i+1}$, *for* $i \geqslant 1$.
(iv) $[e_i, e_j] \in \langle e_{i+j+c} \rangle$, *for* $1 \leqslant i \leqslant a - 1$ *and* $i < j$.
(v) $[e_i, e_j] = 0$, *for* $i, j \geqslant a$.
(vi) $\mathcal{J}(0, i, j) = 0$, *for* $1 \leqslant i < j$.
(vii) $\mathcal{J}(i, j, k) = 0$, *for* $1 \leqslant i < j \leqslant a - 1$, $j < k$ *and* $i + j + k = m - 2c - 1$.

Then, L is a nilpotent Lie algebra of maximal class.

Proof: Since (i) and (ii) hold, in order to prove that L is a Lie algebra, it suffices to see that $\mathcal{J}(i, j, k) = 0$ for $i < j < k$.

https://doi.org/10.1017/S0004972700014180 Published online by Cambridge University Press

From (i), (ii) and (vi) it follows that $\mathcal{J}(0,i,j) = 0$ for $i,j \geqslant 0$ and, since $[\ ,\ ]$ is bilinear,

$$[e_0,x,y] + [x,y,e_0] + [y,e_0,x] = 0, \qquad \text{for any } x,y \in L.$$

In particular,

$$[e_0,[e_i,e_j],e_k] + [e_i,e_j,e_k,e_0] + [e_k,e_0,[e_i,e_j]] = 0, \qquad \text{for } i,j,k \geqslant 1.$$

On the other hand, from (i) and (ii) we derive that $[x,y] = -[y,x]$ for all $x,y \in L$. Hence

$$[e_k,e_0,[e_i,e_j]] = [e_{k+1},[e_i,e_j]] = -[e_i,e_j,e_{k+1}].$$

Also,

$$\begin{aligned}[e_0,[e_i,e_j],e_k] &= -[e_i,e_j,e_0,e_k] = [e_j,e_0,e_i,e_k] + [e_0,e_i,e_j,e_k] \\ &= [e_{j+1},e_i,e_k] - [e_{i+1},e_j,e_k] \\ &= -[e_i,e_{j+1},e_k] - [e_{i+1},e_j,e_k].\end{aligned}$$

Consequently,

$$[e_i,e_j,e_k,e_0] = [e_{i+1},e_j,e_k] + [e_i,e_{j+1},e_k] + [e_i,e_j,e_{k+1}].$$

From this relation we deduce that

$$\begin{aligned}[\mathcal{J}(i,j,k),e_0] &= [e_i,e_j,e_k,e_0] + [e_j,e_k,e_i,e_0] + [e_k,e_i,e_j,e_0] \\ &= [e_{i+1},e_j,e_k] + [e_i,e_{j+1},e_k] + [e_i,e_j,e_{k+1}] \\ &\quad + [e_{j+1},e_k,e_i] + [e_j,e_{k+1},e_i] + [e_j,e_k,e_{i+1}] \\ &\quad + [e_{k+1},e_i,e_j] + [e_k,e_{i+1},e_j] + [e_k,e_i,e_{j+1}] \\ &= \mathcal{J}(i+1,j,k) + \mathcal{J}(i,j+1,k) + \mathcal{J}(i,j,k+1).\end{aligned} \tag{14}$$

Let us now prove that $\mathcal{J}(i,j,k) = 0$ for $i < j < k$. According to (vi), we can suppose $i \geqslant 1$. If $j \geqslant a$ then (iv) and (v) directly yield $\mathcal{J}(i,j,k) = 0$. Suppose then $1 \leqslant i < j \leqslant a-1$. If $i+j+k \geqslant m-2c$, the result is again immediate. When $i+j+k \leqslant m-2c-1$ we argue by backwards induction on $i+j+k$. If $i+j+k = m-2c-1$ then $\mathcal{J}(i,j,k) = 0$ by (vii). If $i+j+k < m-2c-1$, the induction hypothesis gives

$$\mathcal{J}(i+1,j,k) = \mathcal{J}(i,j+1,k) = \mathcal{J}(i,j,k+1) = 0$$

and, by (14), $[\mathcal{J}(i,j,k),e_0] = 0$. Now, from (iv) and (v) there exists $\lambda \in K$ such that $\mathcal{J}(i,j,k) = \lambda e_{i+j+k+2c}$, whence $[\mathcal{J}(i,j,k),e_0] = \lambda e_{i+j+k+2c+1}$. Since $i+j+k+2c+1 < m$, it follows that $\lambda = 0$ and $\mathcal{J}(i,j,k) = 0$.

Finally, it is clear from the values of $[\ ,\ ]$ given in the statement that, for $i \geqslant 2$, $L^i = \langle e_k \mid k \geqslant i \rangle$ and, consequently, L is nilpotent of class $m-1$. □

This theorem tells us that, under the special conditions (iii), (iv) and (v) for the basic Lie products, we need not check the Jacobi identity for all the range of values $i < j < k \leqslant m-1$, but only for $i = 0$ and $1 \leqslant j < k$, and for $1 \leqslant i < j \leqslant a-1$, $j < k$ and $i+j+k = m-2c-1$.

References

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

[2] B. Huppert, *Endliche Gruppen I* (Springer-Verlag, Berlin, Heidelberg, New York, 1967).

[3] L.G. Kovács and C.R. Leedham-Green, 'Some normally monomial p-groups of maximal class and large derived length ', *Quart. J. Math. Oxford Ser. (2)* **37** (1986), 49–54.

[4] M. Lazard, 'Sur les groupes nilpotents et les anneaux de Lie', *Ann. Sci. École Norm. Sup. (3)* **71** (1954), 101–190.

[5] C.R. Leedham-Green and S. McKay, 'On p-groups of maximal class, I', *Quart. J. Math. Oxford Ser. (2)* **27** (1976), 297–311.

[6] C.R. Leedham-Green and S. McKay, 'On p-groups of maximal class, III', *Quart. J. Math. Oxford Ser. (2)* **29** (1978), 281–299.

[7] R.J. Miech, 'Metabelian p-groups of maximal class', *Trans. Amer. Math. Soc.* **152** (1970), 331–373.

[8] R. Shepherd, *p-groups of maximal class*, Ph.D. Thesis (University of Chicago, 1970).

[9] A. Vera-López and G.A. Fernández-Alcober, 'On p-groups of maximal class, III', *Math. Proc. Cambridge Philos. Soc.* **109** (1991), 489–507.

[10] A. Vera-López and G.A. Fernández-Alcober, 'The conjugacy vector of a p-group of maximal class', *Israel J. Math.* **86** (1994), 233–252.

[11] A. Vera-López and B. Larrea, 'On p-groups of maximal class', *J. Algebra* **137** (1991), 77–116.

[12] H. Zassenhaus, *The theory of groups* (Chelsea, New York, 1958).

Departamento de Matemáticas
Universidad del País Vasco
Bilbao
Spain
e-mail: mtpveloa@lg.ehu.es
mtpfealg@lg.ehu.es