

FINITE p -GROUPS WITH UNIQUE MAXIMAL CLASSES

by I. D. MACDONALD

(Received 9th October 1981, revised 7th July 1982)

Is it possible for a finite p -group to have only one conjugacy class of maximal size? This question was opened to public consideration in a paper [2] of John Meldrum dealing with the breadth of the wreath product of finite p -groups. His Theorem 21 gives a formula for the breadth of $A \wr B$ in terms of various constants including the breadths of A and B , a formula which differs according to whether or not A has a unique largest class. Hence the question.

There are certainly p -groups (dihedral and such like) with just two maximal classes, but the general opinion seems to be that the answer to the question above is “no”, i.e. that a finite p -group with more than one element must have more than one maximal class. In this connection, see Theorem 4 below.

Note that in a finite p -group containing the element $a \neq 1$, distinct conjugacy classes are represented by a, a^2, \dots, a^{p-1} . (For if $a^x = a^\alpha$ with $1 \leq \alpha < p$ then $\alpha = 1$, because x has p -power order.) This shows that a finite p -group with unique maximal class has $p = 2$, and further suggests:

Problem. Is there a prime p and a finite p -group G which has precisely $p - 1$ conjugacy classes of maximal size?

Theorem 1. *If p is a prime and G is a finite p -group such that G has breadth n and has precisely $p - 1$ conjugacy classes of size p^n then $|G| \leq p^{n^2 + n}$.*

Proof. Suppose that a, a^2, \dots, a^{p-1} represent the $p - 1$ classes of size p^n . Then G contains elements b_1, b_2, \dots, b_n such that $B = \langle b_1, \dots, b_n \rangle$ and $G = C(a)B$ where $C(a)$ denotes the centraliser of a in G . Consider $U = C(B)$. Since $|G : C(b_i)| \leq p^n$ for $1 \leq i \leq n$ we have $|G : U| \leq p^{n^2}$.

Take an arbitrary element $u \in U$, and consider au . This element has breadth n , because $\{(au)^b : b \in B\}$ contains precisely p^n elements. So au is conjugate to one of a, a^2, \dots, a^{p-1} , i.e. equals one of $(p - 1)p^n$ elements. That is, u has at most $(p - 1)p^n$ values; $|U| \leq (p - 1)p^n < p^{n+1}$.

It follows that $|G| = |G : U| |U| \leq p^{n^2 + n}$.

Theorem 1 gives an upper bound of roughly n^2 on the nilpotency class of the group G which features in it, whereas the next result shows that the class must exceed 2. (A group G is said to have class 2 iff the commutator subgroup $\delta(G)$ lies in the centre $\zeta(G)$.)

Theorem 2. *If p is a prime and G is a non-trivial finite p -group of class 2 and breadth n then G has at least p conjugacy classes of size p^n .*

Proof. Suppose by way of contradiction that G is a finite p -group, for some prime p , with class 2 and breadth n , containing an element $a \neq 1$ such that every element of breadth n is conjugate to one of $\{a^i: 1 \leq i < p\}$. As in Theorem 1, $G = C(a)B$ and $B = \langle b_1, \dots, b_n \rangle$. Without loss of generality we suppose that $G = \langle a, b_1, \dots, b_n \rangle$.

Put $c_i = [a, b_i]$ for $1 \leq i \leq n$. Observe that if $z \in \zeta(G)$ then az has breadth n and $z = [a, x]$ for some $x \in G$. But $\delta(G) \leq \zeta(G)$. Therefore $\delta(G) \leq \langle [a, x]: x \in G \rangle = \langle c_1, \dots, c_n \rangle$. Indeed

$$\delta(G) = \langle c_1, \dots, c_n \rangle.$$

Next we remark that a and a^{1+p} are elements of the same breadth. It follows that a^{1+p} is conjugate in G to one of $\{a^i: 1 \leq i < p\}$. This suffices to show that $a^p \in \delta(G)$. Therefore $a^p \in \zeta(G)$. We infer that $c_i^p = 1$ for $1 \leq i \leq n$, and that $G/\zeta(G)$ has exponent p .

Let g be a general element of G :

$$g = a^\lambda b_1^{\phi_1} \dots b_n^{\phi_n} z$$

where $0 \leq \lambda < p$, $0 \leq \phi_i < p$ for $1 \leq i \leq n$, and $z \in \zeta(G)$. The hypothesis on G is that g has breadth n if $\lambda \neq 0$ and $\Phi = \mathbf{0}$, and breadth $< n$ otherwise; here

$$\Phi^t = (\phi_1, \dots, \phi_n).$$

To assist in calculation of the conjugates of g we put

$$[b_i, b_j] = c_1^{\alpha_{1ij}} c_2^{\alpha_{2ij}} \dots c_n^{\alpha_{nij}}$$

where $0 \leq \alpha_{kij} < p$ for $1 \leq k, i, j \leq n$.

We have, for $1 \leq i \leq n$,

$$\begin{aligned} [g, b_i] &= [a, b_i]^\lambda [b_1, b_i]^{\phi_1} \dots [b_n, b_i]^{\phi_n} \\ &= c_i^\lambda (c_1^{\alpha_{11i}} \dots c_n^{\alpha_{n1i}})^{\phi_1} \dots (c_1^{\alpha_{1ni}} \dots c_n^{\alpha_{nni}})^{\phi_n} \\ &= c_i^\lambda c_1^{\beta_{1i}} c_2^{\beta_{2i}} \dots c_n^{\beta_{ni}} \end{aligned}$$

where we put

$$\beta_{ji} = \alpha_{j1i} \phi_1 + \alpha_{j2i} \phi_2 + \dots + \alpha_{jni} \phi_n.$$

If g has breadth $< n$ then the matrix $\lambda I + B$ has rank $< n$, where $B = [\beta_{ji}]$. Note that

$$B = [A_1 \Phi, A_2 \Phi, \dots, A_n \Phi]$$

with $A_k = [\alpha_{kji}]$ an $n \times n$ skew-symmetric matrix over \mathbb{Z}_p (with 0's on the diagonal).

Consider g with $\lambda \neq 0$. Let $\Phi \neq \mathbf{0}$. Then $\lambda I + B$ has rank $< n$. That is to say, if $\lambda \neq 0$ then $-\lambda$ is an eigenvalue of B , for all $\Phi \neq \mathbf{0}$. (Observe that if $p-1 > n$ then we have already reached the required contradiction.) In particular B has eigenvalue 1, for all $\Phi \neq \mathbf{0}$.

We now derive a contradiction in view of the following result.

Lemma. Let p be a prime and n a positive integer. If A_1, A_2, \dots, A_n are $n \times n$ skew-symmetric matrices over \mathbb{Z}_p (with 0's on the diagonal), if Φ is an $n \times 1$ vector and if $B = [A_1\Phi, A_2\Phi, \dots, A_n\Phi]$ then there is a non-zero value of Φ for which 1 is not an eigenvalue of B .

Proof. Fix $\Phi \neq 0$. Let $q(\lambda)$ be the characteristic polynomial of B .

$$q(\lambda) = \lambda^n + c_1\lambda^{n-1} + \dots + c_{n-1}\lambda + c_n.$$

Because each A_k is skew-symmetric $\Phi^t A_k \Phi = 0$ and so $\Phi^t B = 0$, i.e. B is singular. Hence $c_n = 0$.

By well-known properties of the characteristic equation, each c_i is a homogeneous polynomial of degree $\leq i$ in $\phi_1, \phi_2, \dots, \phi_n$. It follows that $c_1 + c_2 + \dots + c_{n-1}$ is a polynomial of degree $\leq n-1$ in $\phi_1, \phi_2, \dots, \phi_n$, with constant term 0. So by the Theorem of Chevalley and Warning the equation

$$c_1 + c_2 + \dots + c_{n-1} = 0$$

in \mathbb{Z}_p has at least p solutions Φ , and in particular has a non-zero solution. With this Φ we have $q(1) = 1$. That is to say, 1 is not an eigenvalue of B with this non-zero value of Φ .

This completes the proof of the Lemma and of Theorem 2.

Corollary. If p is a prime and G is a finite p -group of breadth 2 then G has at least p conjugacy classes of size p^2 .

Proof. Suppose otherwise. Then there is a prime p and a finite p -group G with an element a of breadth 2, and every element of G is either conjugate to a, a^2, \dots or a^{p-1} or has breadth < 2 . If $x \in G$ has breadth 1 then $|G:C(x)| = p$. So $C(x)$ is normal in G , $G/C(x)$ is abelian, and $C(x)$ contains $\delta(G)$. But G is generated by all its elements of breadth 1. It follows that $\delta(G)$ is central in G , and application of Theorem 2 concludes the proof.

The next result, though its proof is far from elegant, justifies its inclusion in view of Theorem 4.

Theorem 3. If p is a prime and G is a finite p -group of breadth 3 then G has at least p conjugacy classes of size p^3 .

Proof. Suppose by way of contradiction that G contains an element a such that every element of breadth 3 is conjugate to one of $\{a^i: 1 \leq i < p\}$. Clearly G is generated by the (non-empty) set of those elements outside the normal closure $\langle a \rangle^G$ of $\langle a \rangle$, and such elements have breadth ≤ 2 . By Satz 2 of Knoche [1] the class of G is ≤ 3 . In view of Theorem 2 we take the class to be precisely 3.

Let $\{b_1^i b_2^j b_3^k: 0 \leq i, j, k < p\}$ be a right transversal of $C(a)$ in G . We lose no generality in supposing that $G = \langle a, b_1, b_2, b_3 \rangle$. Put $c_i = [a, b_i]$ for $1 \leq i \leq 3$. Since $\zeta(G) \leq \{[a, x]: x \in G\}$ we have $|\zeta(G)| \leq p^3$. We distinguish three cases.

Case 1: $|\zeta(G)| = p$.

Let $\zeta(G) = \langle c_3 \rangle$ and note that $c_3^p = 1$. We have $\gamma_3(G) = \langle c_3 \rangle$, and in particular $[c_i, a] \in \langle c_3 \rangle$. We choose b_1, b_2 in such a way that

$$[c_2, a] = 1. \tag{1}$$

We put

$$[c_2, b_i] = c_3^{\omega_i} (0 \leq \omega_i < p) \tag{2}$$

for $1 \leq i \leq 2$.

Suppose by way of contradiction that there exists $j (1 \leq j \leq 2)$ with $\omega_j \neq 0$. Then b_j cannot be conjugate to $a^\lambda (1 \leq \lambda < p)$ for otherwise

$$c_3^{\omega_j} = [c_2, b_j] = [c_2, a^\lambda] = 1.$$

Similarly ab_j is not conjugate to a^λ ; so both b_j and ab_j have breadth ≤ 2 .

We shall need the well-known commutator identities

$$[x, yz] = [x, z][x, y]^z, \tag{3}$$

$$[xy, z] = [x, z]^y[y, z]. \tag{4}$$

Consider $C(b_j)$. We assert that $\{c_2^\alpha a^\beta : 0 \leq \alpha, \beta < p\}$ is a right transversal of $C(b_j)$ in G . This may be seen directly or with the help of the following calculation:

$$[b_j, c_2^\alpha a^\beta] = [a^\beta, b_j]^{-1} c_3^{-\alpha \omega_j}. \tag{5}$$

Note that $c_j^p \in \langle c_3 \rangle$. Similarly we have $\{c_2^\alpha b_j^\beta : 0 \leq \alpha, \beta < p\}$ for a right transversal of $C(ab_j)$ in G and

$$[ab_j, c_2^\alpha b_j^\beta] = [a, b_j^\beta]^{b_j} c_3^{-\alpha \omega_j}. \tag{6}$$

Now (5) and (6) show that both $[b_j, x]$ and $[ab_j, x]$ lie in $\langle c_j, c_3 \rangle$ for all x in G . By (4) $[a, x] \in \langle c_j, c_3 \rangle$, and so $\langle c_1, c_2, c_3 \rangle = \langle c_j, c_3 \rangle$ of order p^2 . This is a contradiction.

Case 2: $|\zeta(G)| = p^2$ and $\langle a \rangle^G$ is non-abelian.

We put $\zeta(G) = \langle c_2, c_3 \rangle$. Then $[c_1, a] \neq 1$, and we lose no generality in supposing

$$[c_1, a] = c_3. \tag{7}$$

Note that if b_2 were conjugate to $a^\lambda (1 \leq \lambda < p)$ then $b_2 \equiv a^\lambda c_1^\mu$ modulo $\zeta(G)$ with $0 \leq \mu < p$, and

$$c_2 = [a, b_2] = [a, c_1^\mu] = c_3^{-\mu},$$

a contradiction. So b_2 is not conjugate to a^λ . Neither is ab_2 , by a very similar proof.

We shall need the Jacobi-Witt identity, which in groups of class 3 takes the form

$$[x, y, z] [y, z, x] [z, x, y] = 1 \tag{8}$$

where $[x, y, z] = [[x, y], z]$. If we put $x = a, y = b_1, z = b_2$ then we obtain

$$[c_1, b_2] = [b_1, b_2, a]^{-1}. \tag{9}$$

This allows us to put

$$[c_1, b_2] = c_2^\theta c_3^\phi \tag{10}$$

with $0 \leq \theta, \phi < p$.

Consider $C(b_2)$. We have $\{c_1^\alpha a^\beta : 0 \leq \alpha, \beta < p\}$ for a right transversal of $C(b_2)$ in G if $\phi \neq 0$, and

$$[b_2, c_1^\alpha a^\beta] = c_2^{-\alpha\theta - \beta} c_3^{-\alpha\phi}. \tag{11}$$

So we have $[b_2, b_1] \in \langle c_2, c_3 \rangle$ if $\phi \neq 0$, and then by (9) $[c_1, b_2] = 1$, so $\phi = 0$. Thus (10) becomes

$$[c_1, b_2] = c_2^\theta. \tag{10'}$$

Consider $C(ab_2)$. We have $\{c_1^\alpha b_2^\beta : 0 \leq \alpha, \beta < p\}$ for a right transversal of $C(ab_2)$ in G , and

$$[ab_2, c_1^\alpha b_2^\beta] = c_2^{-\alpha\theta + \beta} c_3^{-\alpha}. \tag{12}$$

Therefore $[ab_2, b_1] \in \langle c_2, c_3 \rangle$. By (4)

$$c_1 \equiv [b_1, b_2] \text{ modulo } \zeta(G),$$

and (9) gives

$$[c_1, b_2] = [a, c_1]^{-1} = c_3^{-1},$$

which contradicts (10').

Case 3: $|\zeta(G)| = p^2$ or p^3 and $\langle a \rangle^G$ is abelian.

Since $C(a)$ does not contain b_i or ab_i for any i , these elements cannot be conjugate to $a^\lambda (1 \leq \lambda < p)$. Suppose by way of contradiction that $[b_1, b_2] \notin \langle c_1, c_2, c_3 \rangle$. Consider $C(b_2)$. We have $\{a^\alpha b_1^\beta : 0 \leq \alpha, \beta < p\}$ as a right transversal of $C(b_2)$ in G , and

$$[b_2, a^\alpha b_1^\beta] = c_2^{-\alpha} [b_1^\beta, b_2]^{-1}. \tag{13}$$

Consider $C(ab_2)$. We have $\{a^\alpha b_1^\beta : 0 \leq \alpha, \beta < p\}$ as a right transversal of $C(ab_2)$ in G , and

$$[ab_2, a^\alpha b_1^\beta] = c_1^{\beta b_2} c_2^{-\alpha} [b_1^\beta, b_2]^{-1}. \tag{14}$$

We use (13) and (14) to calculate $[a, x]$ for arbitrary x in G , obtaining

$$[a, x]^{b_2} = [ab_2, x][b_2, x]^{-1} \\ = c_1^{\delta b_2} c_2^{-\gamma + \alpha} [b_1^\beta, b_2][b_1^\delta, b_2]^{-1}$$

for certain $\alpha, \beta, \gamma, \delta$ such that $0 \leq \alpha, \beta, \gamma, \delta < p$. Clearly $\beta = \delta$. If we take $x = b_3$ then we obtain $c_3 = c_2^{-\alpha + \gamma}$, a contradiction. This shows that $[b_1, b_2] \in \langle c_1, c_2, c_3 \rangle$.

If $\zeta(G) = \langle c_1, c_2, c_3 \rangle$ then we conclude that G must have class 2, a contradiction.

In the final case $\zeta(G) = \langle c_2, c_3 \rangle$ of order p^2 and $[c_1, a] = 1$. We still have (9). Therefore $[c_1, b_2] = 1$. Similarly $[c_1, b_3] = 1$. But since $c_1 \notin \zeta(G)$ we must have $[c_1, b_1] \neq 1$, and we might as well suppose that

$$[c_1, b_1] = c_3. \tag{15}$$

Consider $C(b_1)$. We have $\{c_1^\alpha a^\beta : 0 \leq \alpha, \beta < p\}$ for a right transversal of $C(b_1)$ in G , and

$$[b_1, c_1^\alpha a^\beta] = c_1^{-\beta} c_3^{-\alpha}. \tag{16}$$

Consider $C(ab_1)$. We have $\{c_1^\alpha a^\beta : 0 \leq \alpha, \beta < p\}$ for a right transversal of $C(ab_1)$ in G , and

$$[ab_1, c_1^\alpha a^\beta] = c_1^{-\beta} c_3^{-\alpha}. \tag{17}$$

As usual we can now calculate that

$$[a, x]^{b_2} = c_1^{\beta - \delta} c_3^{\alpha - \gamma} \tag{18}$$

for certain $\alpha, \beta, \gamma, \delta$ such that $0 \leq \alpha, \beta, \gamma, \delta < p$. Taking $x = b_2$ gives a final contradiction.

This completes the proof of Theorem 3.

In contrast to Theorems 2 and 3 we have:

Theorem 4. *There is a group of order 2^7 and breadth 4 which has one and only one conjugacy class of 2^4 elements.*

Proof. Consider the group $G = \langle a, b_1, b_2 \rangle$ with power relations

$$a^2 = b_1^2 = b_2^2 = 1, c_1^4 = c_2^4 = 1,$$

where the c_i are defined as part of the commutator relations:

	b_1	b_2	c_1	c_2
a	c_1	c_2	c_1^2	c_2^2
b_1	\cdot	1	c_1^2	c_1^2
b_2	\cdot	\cdot	c_1^2	c_2^2

In this table the entry in row x column y is $[x, y] = x^{-1}y^{-1}xy$.

The first part of the proof is to show that G has order 2^7 . This may be done by one of the machine processes. Alternatively G can be constructed as an extension of $\mathbb{Z}_4 \times \mathbb{Z}_4$ (corresponding to $\langle c_1, c_2 \rangle$) by $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (corresponding to $G/\langle c_1, c_2 \rangle$). The details are left for the reader to supply.

The second thing is to establish the breadth properties of G . It is clear that the breadth of a and of G is 4. It remains to prove that every class not containing a has size $\leq 2^3$. This follows if every $x \in \delta(G)$ except $a \in \delta(G)$ splits into at least 2 classes, which is true if $|C(x)| \geq 2^4$ for every x of the form $a^\lambda b_1^{\phi_1} b_2^{\phi_2}$ with $(\phi_1, \phi_2) \neq (0, 0)$. Note that $C(x) \geq \langle x, c_1^2, c_2^2 \rangle$, and that

$$c_1 \in C(ab_1) \cap C(ab_2),$$

$$c_1 c_2 \in C(b_1) \cap C(ab_1 b_2),$$

$$b_1 \in C(b_2) \cap C(b_1 b_2).$$

This essentially completes the proof of Theorem 4.

Open questions.

1. Is there a finite p -group, for every odd prime p , which has precisely $p-1$ maximal classes?
2. Is there a finite p -group, for every prime p , which has precisely $p-1$ classes of size p^{α_1} and p^{α_2} respectively, where α_1 is the largest element breadth and α_2 the second largest?
3. Is it true that if G is a finite p -group with precisely $p-1$ maximal classes, and if a lies in one such class, then $\delta(G) = \langle [a, x] : x \in G \rangle$?
4. Is it true that every finite p -group is isomorphic to a factor group of a finite p -group with precisely $p-1$ maximal classes?

Acknowledgements. This work was started after discussions with Dr. A. R. Prince. I am indebted to him for stimulation and improvements. In particular I thank him for the remark about the maximal classes of the dihedral groups, for the proof given here of the Corollary to Theorem 2, and for pointing out that my original example for Theorem 4 contained the example given above as a subgroup.

I also thank Dr. E. F. Robertson for nilpotent quotient calculations using the computer facility in the University of St. Andrews.

REFERENCES

1. H.-G. KNOCHÉ, Über den Frobeniusschen Klassenbegriff in Nilpotenten Gruppen. II, *Math. Z.* **59** (1953), 8–16.
2. J. D. P. MELDRUM, Centralisers in wreath products, *Proc. Edinburgh Math. Soc.* **22** (1979), 161–168.

UNIVERSITY OF STIRLING