A COMPUTER APPLICATION TO FINITE *p*-GROUPS

Dedicated to the memory of Hanna Neumann

I. D. MACDONALD

(Received 25 July 1972)

Communicated by M. F. Newman

1. Introduction

The first and still the best known computer application to groups exploits coset enumeration and this has been very thoroughly studied; see for instance [2] and [8]. No doubt this is because the algorithm is simple in the sense of programming. The underlying mathematics is far from simple, touching as it does on logical difficulties akin to the word problem for groups, and this is reflected in the facts that random access to large tables is required and that there is no indication at any stage (for example when storage space is exhausted) whether the algorithm would be completed at any later stage. Efficient computation depends on choosing a subgroup of small index m in the group under examination, for group elements will be represented as permutations of degree m, and the larger m is the more tedious it will be to check properties like orders of group elements. Yet in many cases m may have to be fairly large so that the subgroup is "corefree" i.e. the representation is faithful.

These last remarks are very pertinent in the case of finite p-groups. In [5] some properties of a group of order 2^{13} are examined. There happens to be a corefree subgroup of index 2^7 (this index is perhaps smaller than one would expect) and the 2^{13} elements can each be represented as a permutation on 2^7 cosets and examined individually. However 2^{13} is still a relatively small group order and the number of cases in which such methods are feasible is clearly limited.

In some ways the properties of a group of order p^n will depend on n rather than on the prime p. The means of giving precision to this vague remark are to be found in the commutator calculus. So efficient computation in finite p-groups must utilise commutator calculation rather than coset enumeration.

The purpose of this article is to describe a computer programme which,

https://doi.org/10.1017/S1446788700015962 Published online by Cambridge University Press

given a presentation $\mathfrak{P}$ for a group G and a prime p, constructs $G/Z_i(G)$ for $i = 1, 2 \cdots$ where

$$G = Z_0(G) > Z_1(G) > Z_2(G) > \cdots$$

is a descending central series of G obtained by refining the lower central series so that each factor has exponent p. More precisely the terms $\gamma_i(G) > \gamma_{i+1}(G)$ of the lower central series are replaced by

$$\gamma_i(G) > \gamma_i(G)^p\gamma_{i+1}(G) > \cdots > \gamma_i(G)^{p^{e-1}}\gamma_{i+1}(G) > \gamma_{i+1}(G)$$

where $\gamma_i(G)/\gamma_{i+1}(G)$ has exponent p^e but not p^{e-1}. In particular if G is a finite p-group then G itself is constructed. By "constructed" we mean presented by means of relations involving commutators and p-th powers in a manner to be explained; and each $G/Z_i(G)$ will be found after a number of operations to which a bound could be assigned in advance.

2. Group-theoretical preliminaries

Since it is convenient to collect in arrays which are subscripted with positive integers, we collect "to the right"; collection of a in $\cdots ab \cdots$ requires $ab = cba$. Hence the definitions

$$[a, b] = aba^{-1}b^{-1}, \; b^a = aba^{-1},$$

and the consequence

$$b^a = [a,b]b.$$

Collection of first a then b in abc leads to commutators of the form $[b, [a, c]]$, therefore we define $[x_n, x_{n-1}, \cdots, x_1]$ to be $[x_n, [x_{n-1}, \cdots, x_1]]$ inductively for each $n > 2$.

In this notation the usual commutator identities are:

$$[ab, c] = [b, c]^a[a, c], \; [a, cd] = [a, c][a, d]^c,$$

$$[a^{-1}, b] = a^{-1}[a, b]^{-1}a, \; [a, b^{-1}] = b^{-1}[a, b]^{-1}b,$$

$$[ab, cd] = [b, c]^a[a, c][b, d]^{ac}[a, d]^c, \; [a^c, b, c][c^b, a, b][b^a, c, a] = 1,$$

the last of which we call the Jacobi identity. Weights of higher commutators are defined as usual, and $[x_n, \cdots, x_1]$ is said to be simple if each x_i has weight 1. The following well-known result follows from the Jacobi identity:

LEMMA 1. *Every commutator of weight w is the product of simple commutators of weight at least w and their inverses.*

We have to consider presentations of a group G of order p^n. There are elements $\{c_1, \cdots, c_n\}$ in G such that if G_i is defined as $gp\{c_{i+1}, \cdots, c_n\}$ for $0 \leqq i$

$< n$, with $G_n = 1$, then G_i is normal in G, c_iG_i is central in G/G_i, and c_iG_i has order p. Then each element of G has a unique expression of the form $c_n^{\theta(n)} \cdots c_1^{\theta(1)}$ where $0 \leqq \theta(i) < p$ (as an alternative $-p < 2\theta(i) \leqq p$). Further there are numbers $\alpha(i,j)$ and $\beta(i,j,k)$ such that

$$\text{(i)} \qquad c_i^p = c_n^{\alpha(i,n)} \cdots c_{i+1}^{\alpha(i,i+1)} \qquad (1 \leqq i \leqq n), \text{ and}$$

$$\text{(ii)} \qquad [c_i, c_j] = c_n^{\beta(i,j,n)} \cdots c_{j+1}^{\beta(i,j,j+1)} \qquad (1 \leqq i < j \leqq n).$$

We can restrict the α's and β's similarly to the θ's.

Conversely, given α's and β's, and generators $\{c_1 \cdots, c_n\}$ subject to relations (i) and (ii), we have a presentation of a finite p-group, and the question is whether it has order p^n. In fact when a group of order p^n is given there are relations among the α's and β's, and in the light of lemma 2 it is easy to construct examples of presentations with n generators defining a group G of order less than p^n. Though they would in general be difficult to write down explicitly we shall have to know how to obtain the relations in each case.

At this stage some points of notation must be clarified. Given a presentation $\mathfrak{P}$ with relations (i) and (ii), we shall refer to $c_1, \cdots, c_n$ as commutators; this would not be normal usage if for instance the presentation were to define the cyclic group of order p^n. Further, it is easy to see that in the group corresponding to $\mathfrak{P}$ a normal form for elements can be found, such as $c_n^{\theta(n)} \cdots c_1^{\theta(1)}$ where $0 \leqq \theta(i) < p$. We shall refer to the process of expressing an element in such a form, with the aid of (i) and (ii), as commutator collection. This convenient notation admittedly stretches language somewhat.

Lemma 2. *In order that $G = gp\{c_1, \cdots, c_n\}$ subject to the relations* (i) *and* (ii) *shall have order p^n it is necessary and sufficient that the α's and β's satisfy the relations derived from*

$$\text{(iii)} \qquad [c_i, c_j^p] = [c_i, c_n^{\alpha(j,n)} \cdots c_{j+1}^{\alpha(j,j+1)}] \qquad (1 \leqq i, j \leqq n), \textit{ and}$$

$$\text{(iv)} \qquad [c_i, c_j, c_k] = [c_i, c_n^{\beta(j,k\,n)} \cdots c_{k+1}^{\beta(j,k.k+1)}] \qquad (1 \leqq i < j < k \leqq n).$$

Proof. We must say how we derive relations from (iii) and (iv). In the case of (iii) the commutators on both sides are expanded in the form $xyx^{-1}y^{-1}$, collections performed and corresponding exponents equated. For (iv) the left-hand-side is expanded as a word in $\{c_i^{\pm 1}, c_j^{\pm 1}, c_k^{\pm 1}\}$ and the rest of the process is similar.

Proof of necessity is trivial. To prove sufficiency we use induction on n, which allows us to suppose that p^{n-1} is the order of the group G_1 generated by $\{c_2, \cdots, c_n\}$ subject to those relations (iii) and (iv) in which there is no c_1. Now (iii) and (iv) with $i = 1$ indicate that conjugation in G of $gp\{c_2, \cdots, c_n\}$ by c_1 maps that subgroup of G onto itself. Therefore G_1 is a normal subgroup of G and the mapping determined by c_1 is an automorphism, ω say, of G_1. Next ω^p is an automorphism of G_1, namely that induced by conjugation with $c_n^{\alpha(1,n)} \cdots c_2^{\alpha(1,2)}$, because of (iii) with $i > 1$ and $j = 1$; and $c_n^{\alpha(1,n)} \cdots c_2^{\alpha(1,2)}$ is fixed by ω because of (iii) with $i = j = 1$. Therefore theorem 15.3.1 of [1] enables us to conclude that the extension G of G_1 has order p^n.

It does not seem possible to recast (iii) but we have a remarkable fact about (iv):

Lemma 3. *For fixed i, j, k the relation* (iv) *is equivalent to*

$$\text{(v)} \qquad [c_i^{c_k}, c_j, c_k][c_k^{c_j}, c_i, c_j][c_j^{c_i}, c_k, c_i] = 1.$$

This is essentially lemma 2 of [6] so we shall spare the reader a proof of it. We must however make some excuse for the use of the word "equivalent" in the lemma, as some β's appear explicitly in lemma 2 but none in lemma 3. What is intended of course is that the terms $[c_j, c_k]$, $[c_k, c_i]$, $[c_i, c_j]$ appearing in the factors on the left-hand-side of (v) should be replaced by the obvious expressions involving β's, then collection should be undertaken, and corresponding exponents equated. The resulting relations among the β's will be precisely those arising from lemma 2.

A handier form for computation is:

Lemma 4. *For fixed i, j, k the relation* (iv) *is equivalent to*

$$\text{(vi)} \qquad C(i,j,k)C(k,i,j)C(j,k,i) = 1$$

where $C(i,j,k) = [c_i, c_j, c_k][c_j, c_k][c_i, c_k]$.

We are ready to consider the descending central series

$$G = Z_0(G) > Z_1(G) > Z_2(G) > \cdots$$

mentioned earlier. We shall specify G/Z_m for $m = 1, 2, \cdots$ by a set of generators $\{c_1, \cdots, c_n\}$, where $n = n(m)$ and G/Z_m has order p^n, and by relations of the forms (i) and (ii) contained in power and commutator tables respectively. Construction of these tables proceeds by induction on m. When $m = 1$ we put $n(1) = d$ and choose $\{c_1, \cdots, c_d\}$ to be independent elements modulo the Frattini subgroup of G; the c's are of course some subset of the generators in the given presentation $\mathfrak{P}$ of G. Thus when $m = 1$ the tables have the form

$$c_i^p = 1 \ (1 \leqq i \leqq d), \text{ and } [c_i, c_j] = 1 \ (1 \leqq i < j \leqq d).$$

It is important to understand that each generator c_i (where $i > d$) in the presentation for G/Z_m has to come from somewhere, and in fact has been defined in terms of earlier c's as c_k^p or as $[c_j, c_k]$ where $j < k < i$. Thus $c_i (i > d)$ will appear in a definite place in the tables as soon as m is such that the order of G/Z_m is at least p^i, and this particular entry in the tables will not change as m increases. There may of course be other occurrences of this c_i in the tables, but these will usually be subject to alteration as m increases. In effect we need another table to record the definition of each c_i.

https://doi.org/10.1017/S1446788700015962 Published online by Cambridge University Press

It will be convenient to consider two separate cases in the passage from $G/Z_m(m \geqq 1)$ to G/Z_{m+1}, depending on whether or not the class increases. Though the application of the lemmas is the same in the two cases the modification of the tables is different.

First let us suppose that we are attempting to construct G/Z_{m+1} from G/Z_m keeping the class c fixed, so that the exponent of the last non-trivial term of the lower central series increases. As explained above some entries in the power and commutator tables for G/Z_m correspond to definitions of commutators. We list all the places *not* thus associated with definitions; suppose there are t of them with entries $e_1, \cdots, e_t$ respectively. We take further commutators $c_{n+1}, \cdots, c_{n+t}$ and change the entries just mentioned to $c_{n+1}e_1, \cdots c_{n+t}e_t$. (Note that in the commutator table for G/Z_m the entry for $[c_i, c_j]$ where $1 \leqq i < j \leqq n$ will be 1 if the sum of the weights of c_i and c_j exceeds c, and as c is not to increase there is really no point in including this entry in our list of changes.) We also enlarge the tables so as to include the entries

$$c_i^p = 1 \; (n+1 \leqq i \leqq n+t), \quad \text{and}$$

$$[c_i, c_j] = 1, (1 \leqq i < j \leqq n+t \quad \text{and} \quad n+1 \leqq j).$$

Example. Suppose that $\mathfrak{P}$ is some presentation for the quaternion group Q of order 8 and that $p = 2$. From $\mathfrak{P}$ tables for $Q/Z_1(Q)$ are:

$$c_1^2 = 1, c_2^2 = 1; [c_1, c_2] = 1.$$

We define c_3, c_4 as c_1^2, c_2^2 respectively and consider the tables:

$$c_1^2 = c_3, c_2^2 = c_4, c_3^2 = 1, c_4^2 = 1;$$

$$[c_1, c_2] = 1, [c_1, c_3] = 1, [c_1, c_4] = 1,$$

$$[c_2, c_3] = 1, \; [c_2, c_4] = 1,$$

$$[c_3, c_4] = 1.$$

The amended tables which we have at this stage will not in general be the tables for any group, for there will be relations among $c_{n+1}, \cdots, c_{n+t}$. But lemma 2 and its cognates tell us how to use collection to find such relations. Whenever a non-trivial relation appears one of the c's can be expressed in terms of the rest and eliminated from the tables by the obvious substitutions. Eventually tables for a group emerge. However there are also relations in $\mathfrak{P}$ that have to be satisfied, so we have further collection and elimination to perform. If at the end t' of the c's have not been eliminated then we put $n(m+1) = n(m) + t'$, relabel if necessary, and have tables for G/Z_{m+1}. (In the example above the lemmas yield nothing. If the reader will be so good as to give himself a presentation $\mathfrak{P}$ for Q then he will soon find from it that $c_3 = c_4 = 1$.)

https://doi.org/10.1017/S1446788700015962 Published online by Cambridge University Press

It may happen that G/Z_m and G/Z_{m+1} have the same order, in which case we attempt to construct G/Z_{m+1} by increasing the class from c to $c+1$. We take commutators $c_{n+1},\cdots c_{n+t}$ and use them as above, with the difference that the entry for $[c_i\ c_j]$ is to be 1 if and only if the weight sum of c_i and c_j exceeds $c+1$ (not c). The enlargement of the tables is correspondingly greater. We collect and eliminate as before.

Example. Take $\mathfrak{P}$ and Q again, and consider the tables for $Q/Z_1(Q)$. This time we define c_3, c_4, c_5 as $c_1^2, c_2^2\ [c_1, c_2]$ respectively and we contemplate the following tables:

$$c_1^2 = c_3,\ c_2^2 = c_4,\ c_3^2 = 1,\ c_4^2 = 1,\ c_5^2 = 1;$$

$$\begin{aligned}
[c_1,c_2] = c_5,\ [c_1,c_3] = 1,\ [c_1,c_4] = 1,\ [c_1,c_5] &= 1,\\
[c_2,c_3] = 1,\ [c_2,c_4] = 1,\ [c_2,c_5] &= 1,\\
[c_3,c_4] = 1,\ [c_3,c_5] &= 1,\\
[c_4,c_5] &= 1.
\end{aligned}$$

No relations result from the lemmas, but $\mathfrak{P}$ should give $c_3 = c_4 = c_5$. Let us eliminate c_3 and c_4. We thus obtain the following tables:

$$c_1^2 = c_3,\ c_2^2 = c_3,\ c_3^2 = 1;$$

$$[c_1,c_2] = c_3,\ [c_1,c_3] = 1,\ [c_2,c_3] = 1.$$

In either case, if $n(m+1) > n(m)$ then the number of commutators has increased and information has to be recorded in the table of definitions. Lemma 1 applies. In the first case we arrange that each c_i for $n(m) < i \leqq n(m+1)$ is some c_j^p where $n(m-1) < j \leqq n(m)$ and in the second case each c_i is some $[c_j, c_k]$ where $1 \leqq j \leqq d$ and c_k has weight c. Weight means of course weight in $c_1, \cdots, c_d$; this may be defined inductively and recorded at each stage. Thus c_i for $n(m) < i \leqq n(m+1)$ is assigned weight c in the first case above and $c+1$ in the second.

An obviously useful fact in this context is that the exponents of the lower central factors $\gamma_i(G)/\gamma_{i+1}(G)$ of G do not increase as i increases. Thus in the example Q above an attempt to construct $Q/Z_3(Q)$ of class 2 must inevitably be futile, and the reader is urged to show himself that construction with $c = 3$ will also give nothing.

3. The algorithm and its programming

It may be useful to give the bare bones of the algorithm now.

1. Examine $\mathfrak{P}$ and define the integer d. Define the integer MXP so that $G/\gamma_2(G)$ has exponent p^{MXP}. Put EXP and $MW = 1$. Go to 2.

2. If $EXP = MXP$ then put $EXP = 0$ and go to 4, otherwise go to 3.

https://doi.org/10.1017/S1446788700015962 Published online by Cambridge University Press

3. Define new commutators in the first way above (i.e. no increase of c), and collect. If a larger group results put $EXP = 1 + EXP$ and go to 2, otherwise put $MXP = EXP$ then put $EXP = 0$ and finally go to 4.

4. Define new commutators in the second way above (i.e. increase of c), and collect. If a larger group results then put $EXP = 1$, $MW = 1 + MW$ and go to 2, otherwise go to 5.

5. Stop.

We have supposed that $d > 0$ here. Sometimes it is convenient to have for d some number other than the dimension of $G/\phi(G)$ and then the algorithm should be modified. The integer MW refers to the class of the group constructed, and p^{EXP} to the exponent of its γ_{MW}. We note that if G is a finite p-group then the algorithm will terminate and then $\mathfrak{P}$ has been transformed into a presentation involving relations of the forms (i) and (ii) only

Next we elaborate on the mechanics of collection. Suppose that power and commutator tables are ready. Before we can collect arbitrary words we need the values of $[c_i^{\pm 1}, c_j^{\pm 1}]$ for $1 \leqq i < j \leqq n$. The method adopted is to use identities of the form

$$[c_i^{-1}, c_j] = c_i^{-1}[c_i, c_j]^{-1}c_i, \; [c_i, c_j^{-1}] = c_j^{-1}[c_i, c_j]^{-1}c_j$$

to calculate the $[c_i^{\mp 1}, c_j^{\mp 1}]$ inductively. It is clearly feasible to do this first for c_i and c_j with weight sum c (where the group under construction has class c), then weight sum $c - 1$, and so on ending with weight sum 2.

Very long words may arise during the collection process, particularly when the relations of $\mathfrak{P}$ are being collected, for which reason a refinement is introduced. Suppose that during a particular collection all commutators of a fixed weight w have just been collected, then it is possible to collect forthwith every commutator of weight exceeding $c - w$. This saves space by decreasing the length of the word undergoing collection. With this device collection ends as soon as $2w$ exceeds c.

Suppose that all occurrences of c_i in some word have just been collected, giving the result c_i^q. We accept $c_i^{q_o}$ in the collected part of the word where $q = kp + q_o$ and $-p < 2q_o \leqq p$, express c_i^{kp} in terms of $c_n, \cdots, c_{i+1}$ by means of the power tables and put this expression at the end of the uncollected part of the word.

A programme for the algorithm has been written in Elliott ALGOL and is in working order. Tables for powers, commutators, definitions and weights are stored linearly and fast access to these arrays is of course essential, but as they are relatively small there is no storage problem. Collection is carried out in a much larger array. It would be quite feasible to hold this on disc or even magnetic tape and transfer it piece-meal to the fast store for collection because collection proceeds in a "local" fashion. (This refinement has not yet been programmed.) It is clear that the time required for a collection, as a function of the length of the word to be collected, may increase very steeply.

4. Results

(i) It may be worth mentioning that the first stage in the work described above was the writing of a short programme (both in ICL FORTRAN IV and in Elliot ALGOL) for the very much simpler problem of defining and collecting basic commutators. This is of relatively little use in investigations of groups though the following application of it may be of interest. It consists of verifying the identity

$$[a, b;\ c, d] = [a, c;\ b, d][a, d;\ b, c]$$

in $G/\gamma_5(G)$ where G is a group of exponent 4; the identity is given as (4) in the paper [9] of Wright. The programme first defined the basic commutators in a, b, c, d with weight not exceeding 4—there are 90 of them — and then collected the word $(dcba)^4$ as far as weight 4. The result was the product of 1417 basic commutators. Use is then made of the exponent 4 condition. Thus $a^4 = b^4 = c^4 = d^4 = 1$ and $[a, b]^2 \in \gamma_4(G)$ by (1) of [9]. In a relatively free group every relation among the generators determines an identity in the group (see (13.25) in Neumann's book [7]) which means that we can forget about commutators whose entries are a proper subset of $\{a, b, c, d\}$. Now the exponents of $[c, b, a, d]$, $[d, b, a, c]$, $[d, c, a, b]$ were 36, 50, 70 respectively and we recall that $\gamma_4(G)^2 \leqq \gamma_5(G)$ if G has exponent 4; whereas $[a, b;\ c, d]$, $[a, c;\ b, d]$, $[a, d;\ b, c]$ had exponents 11, 11, 25• and Wright's identity follows.

(ii) Since our algorithm for p-groups is constructive it will determine the order and class of a finitely presented p-group as well of course as power and commutator tables. Now in the paper [3] a class of finite nilpotent groups was investigated, presentations being, in the *present* notation,

$$G(\alpha, \beta) = gp\{a, b : a^{[a^{-1}, b^{-1}]} = a^{\alpha}, b^{[a^{-1}, b^{-1}]} = b^{\beta}\}$$

where $\alpha \neq 1$ and $\beta \neq 1$. It was shown that the nilpotent class cannot exceed 8 and there was some speculation that the group $G(34, 7)$ had precise class 8. However Dr J. W. Wamsley pointed out (verbally) some years ago that the relations

$$a^{81} = c^{27} = 1,\ a^{27} = b^{-27}$$

held in $G(34, 7)$ and that the class was less than 8. The problem was therefore given to the computer, which showed that the order of the Sylow 3-subgroup of $G(34, 7)$ is 3^{10} and the class is precisely 7. We give the tables in pages 9 and 10.

(iii) The tables were found for the group of order 2^{13} mentioned in section 1 and described in [5], using the presentation given there. These tables are essentially those given in [4]. As an additional item a further piece of programme was written with a view to finding by collection the order of each of the 2^{13} group elements. It is gratifying to record that the numbers of elements of each order inside and outside the Frattini subgroup are exactly the same as those given in

DEFINITIONS

c_3	$[c_1, c_2]$
c_4	$[c_1, c_3]$
c_5	$[c_2, c_3]$
c_6	$[c_1, c_5]$
c_7	$[c_1, c_6]$
c_8	$[c_2, c_6]$
c_9	$[c_1, c_8]$
c_{10}	$[c_1, c_9]$

WEIGHTS

c_1	1
c_2	1
c_3	2
c_4	3
c_5	3
c_6	4
c_7	5
c_8	5
c_9	6
c_{10}	7

POWER TABLE

c_1^3	$c_{10}c_6c_4^{-1}$
c_2^3	$c_7c_6^{-1}c_5$
c_3^3	$c_7^{-1}c_6$
c_4^3	c_7
c_5^3	$c_{10}c_9^{-1}c_8$
c_6^3	$c_{10}^{-1}c_9$
c_7^3	c_{10}
c_8^3	c_{10}
c_9^3	1
c_{10}^3	1

https://doi.org/10.1017/S1446788700015962 Published online by Cambridge University Press

COMMUTATCR TAELE

	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9
c_1	c_3	c_4	c_7	c_6	c_7	c_{10}	c_9	c_{10}
c_2		c_5	$c_8c_7^{-1}c_6$	$c_{10}c_9^{-1}c_8$	c_8	$c_{10}^{-1}c_9$	c_{10}^{-1}	c_{10}
c_3			c_7	$c_9c_8^{-1}$	c_{10}	c_{10}	c_{10}^{-1}	
c_4				$c_{10}c_9^{-1}$	c_{10}^{-1}			
c_5					c_{10}			

By way of explanation, $c_1^3 = c_{10}c_6c_4^{-1}$ and so on, while $[c_i, c_j]$ is to be found in row c_i column c_j, and any missing entry is 1.

[5]; this provides an interesting check on the accuracy of two quite different computer programmes.

(iv) The final results that we mention here concern the multiplicators of some finite p-groups. The multiplicator of a finite group G may be defined as $H^2(G,\mathbb{C}^*)$ where $\mathbb{C}$ is, say, the complex field, but for computation we use the usual group-theoretic characterisation: it is the largest group M such that there exists an extension H of M by G for which $M \leqq \gamma_2(H) \cap \zeta(H)$, where ζ denotes centre. We recall that if G is a finite p-group then so is M.

The groups G that we consider are the Burnside groups $B(3,3)$ and $B(4,2)$, and what we may denote by $I(4,3)$, the largest group of exponent 4 on 3 generators of order 2. Fortunately Leech has given free presentations for these in [2]. Now an obvious method of finding the multiplicator of a group G whose presentation is $\mathfrak{P}$ is to construct the group H mentioned above. Generators for H correspond to the given generators for G, and there are relations of the form $[x, y] = 1$ where x runs through the generating set of G and y runs through the relators in $\mathfrak{P}$. We still have to arrange that $M \leqq \gamma_2(H)$, and we need more relations in general so that H will be finite. We have after a trivial proof:

LEMMA 5. *If $G = H/M$ where $M \leqq \gamma_2(H)$ and M is normal in H then $G/\gamma_2(G) \cong H/\gamma_2(H)$.*

So for computation of H we find the exponent of $G/\gamma_2(G)$ and put the appropriate value of MXP in among the data, which also include the relations mentioned above. After the machine has done its work a factor group of the group produced

https://doi.org/10.1017/S1446788700015962 Published online by Cambridge University Press

will have to be taken in order that $M \leqq \gamma_2(H)$, and then the structure of M can be seen.

In the cases $B(3,3)$, $B(4,2)$, $I(4,2)$ the multiplicators were found to be abelian of ranks 10, 7, 7 respectively. Now there is a well known relation between the deficiency def G of a group G and the rank of its multiplicator M, namely

$$\operatorname{def} G + \operatorname{rank} M \leqq 0.$$

It is interesting that in the case of each of the three groups G just mentioned the rank of M is the negative of the deficiency of Leech's presentation, so that each of the latter is minimal in a strong sense. It has been conjectured that def G + rank M = 0 for every finite p-group G, which is certainly true in these three cases.

Acknowledgment

The author wishes to thank the referee whose comments led to considerable improvements in the exposition of the paper.

References

[1] M.Hall, *The Theory of Groups* (Macmillan, New York, 1959).

[2] J. Leech, 'Coset enumeration on digital computers', *Proc. Cambridge Philos. Soc.* 59 (1963), 257–267.

[3] I. D. Macdonald, 'On a class of finitely presented groups', *Canad. J. Math.* 14 (1962), 602–613.

[4] I. D. Macdonald, 'Some examples in the theory of groups', *Mathematical Essays dedicated to A. J. Macintyre*, (Ohio University Press, Athens, Ohio, 1970), 263–269.

[5] I. D. Macdonald, 'An application of coset enumeration', to appear in *Austral. Comput. J.*

[6] I. D. Macdonald and B. H. Neumann, 'A third-Engel 5-group', *J. Austral. Math. Soc.* 7 (1967), 555–569.

[7] Hanna Neumann, *Varieties of Groups* (Springer, Berlin, 1967).

[8] H. F. Trotter, 'A machine program for coset enumeration', *Canad. Math. Bull.* 7 (1964), 357–368.

[9] C. R. B. Wright, 'On the nilpotency class of a group of exponent four', *Pacific J. Math.* 11 (1961), 387–394.

Department of Mathematics
University of Stirling, Scotland.

https://doi.org/10.1017/S1446788700015962 Published online by Cambridge University Press