A computer aided study of a
group defined by fourth powers

M.F. Newman

There is a group defined by fourth powers which did not yield to
attempts to determine its order by coset enumerations. This
group has now been shown to be infinite with the aid of a
computer. An outline of the method is given as well as a simple
direct proof inspired by the results of further computer
calculations.

1.   Introduction

Groups defined by fourth powers have been studied at least since 1902
when Burnside [1] proved (in effect) that the group generated by $\{a, b\}$
with defining relations

$$a^4 = b^4 = (ab)^4 = (a^{-1}b)^4 = (a^{-1}b^2)^4 = (b^{-1}a^2)^4 = (a^2b^2)^4 =$$
$$= (a^{-1}bab)^4 = (b^{-1}aba)^4 = (a^2b^{-1}a^2b)^4 = (b^2a^{-1}b^2a)^4 = e$$

is finite, of order at most 2^{12}. In 1954 Tobin [6] proved there is a
two-generator group of exponent 4 (each element has order dividing 4)
with order 2^{12}. It follows that the freest two-generator gr up of
exponent 4 , $B(2, 4)$, has order 2^{12}. Coxeter and Moser [2, p. 81]
reported in 1957 that $B(2, 4)$ has a presentation

$$\langle a, b;\ a^4 = b^4 = (ab)^4 = (a^{-1}b)^4 = (a^2b)^4 = (ab^2)^4 = (a^2b^2)^4 =$$
$$= (a^{-1}b^{-1}ab)^4 = (a^{-1}bab)^4 = e \rangle .$$

In 1963 Leech [4] reported on attempts to reduce the number of fourth powers needed to define $B(2, 4)$. He said that computer implementations of coset enumeration show that $B(2, 4)$ is fully defined on the generating set $\{a, b\}$ by assigning order 4 to the elements

(1) $a, b, ab, a^{-1}b, ab^2, a^2b$

and any three of the elements

(2) $a^{-1}b^{-1}ab, a^2b^2, a^{-1}bab, ab^{-1}ab$.

Moreover, if only two of the elements (2) are included, groups of order 2^{13} are obtained and, if only one is included, not the commutator $a^{-1}b^{-1}ab$, then the order is 2^{14} . Recently Macdonald [5, p. 112] has shown (using a computer implementation of an algorithm for calculating nilpotent quotients) that the rank of the multiplicator of $B(2, 4)$ is 7 so that every presentation of $B(2, 4)$ on two generators needs at least 9 defining relations.

Leech also reported that a coset enumeration on the presentation

(3) $\langle a, b; a^4 = b^4 = (ab)^4 = (a^{-1}b)^4 = (ab^2)^4 = (a^2b)^4 = (a^{-1}b^{-1}ab)^4 = e \rangle$

exceeded the capacity of his computer. The reason for this is now clear; the group is infinite. A simple proof is given below. This proof arose out of detailed computer aided calculations. It seems worthwhile to give an outline of what actually happened. Before doing so let me make explicit a problem arising out of the discussion above.

What is the least number of fourth powers which define a two-generator finite group?

More generally when the corresponding Burnside problem has a positive solution:

What is the least number of m-th powers which define an n-generator finite group?

As far as I know even the simplest case $m = n = 2$ is open.

2. The computing

An application of the Wamsley implementation of the nilpotent quotient

algorithm [7] to the group G defined by (3) showed (after about three minutes on a Univac 1108) that G has a quotient of nilpotency class 14 and order 2^{30}, and it gave a commutator-power presentation for this quotient. This presentation suggested strongly that G is infinite and that the third term $\gamma_3(G)$ of the lower central series of G might have an infinite commutator quotient group $\gamma_3(G)/\gamma_3'(G)$. An application of an implementation (Havas [3]) of the Reidemeister-Schreier algorithm for obtaining a presentation for subgroups was used to get a presentation for $\gamma_3(G)$ (in about one second on a Cyber 76). From this it could be read off that $\gamma_3(G)/\gamma_3'(G)$ is infinite, in fact is the direct product of a free abelian group of rank 4 and a cyclic group of order 2.

The matter could have rested there. However it seemed worth trying for a "hand" proof. One way would have been to construct $G/\gamma_3'(G)$ from the information available but this seemed somewhat unpleasant. So subgroups of G containing $\gamma_3(G)$ were investigated using an implementation of an abelianized version of the Reidemeister-Schreier algorithm (developed by Leon Sterling, a vacation scholar at ANU). The quotient $G/\gamma_3(G)$ is the freest group of rank 2 which has exponent 4 and is nilpotent of class 2. It has seven normal subgroups of order 2. The commutator quotient groups of the corresponding seven normal subgroups of index 16 in G were computed (in about three seconds on the Univac 1108) and three turned out to be infinite. It follows that at most one of the normal subgroups of index 8 in G containing $\gamma_3(G)$ could have infinite commutator quotient group. Another (half second) run showed this quotient is free abelian of rank 4. From here the construction of an example (described below) was easy.

3. A group

The above calculations show that a suitable extension of a free abelian group of rank at most 4 by a quaternion group of order 8 will be an infinite quotient of the group G presented by (3). This suggested studying groups H generated by a pair $\{a, b\}$ of complex matrices

$$a = \begin{pmatrix} i & 0 & 0 \\ 0 & -i & 0 \\ u & v & 1 \end{pmatrix} \ , \quad b = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ w & x & 1 \end{pmatrix}$$

where u, v, w, x are Gaussian integers. The subgroup T of H consisting of all matrices of the form

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ y & z & 1 \end{pmatrix}$$

is clearly normal and free abelian of rank at most 4 , and the quotient H/T is quaternion. Since

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ s & t & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

every element of H not in T has order 2 or 4 because those not of the form

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ s & t & 1 \end{pmatrix}$$

have their square of this form. It is therefore easy to check that H is a quotient group of G . Now fix H by choosing $u = v = x = 0$ and $w = 1$ then the commutator $[a, b, a]$ is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & 0 & 1 \end{pmatrix}$$

Hence H and therefore G is infinite.

Note added in proof, 9 March 1976. I can now show that the answer to the simplest case of the question posed at the end of Section 1 is, as expected, that the least number of squares needed to define a 2-generator finite group is 3 .

References

[1]   W. Burnside, "On an unsettled problem in the theory of discontinuous
        groups", *Quart. J. Math.* 33 (1902), 230-238.

[2]   H.S.M. Coxeter and W.O.J. Moser, *Generators and relations for discrete
        groups* (Ergebnisse der Mathematik und ihrer Grenzgebiete, 14.
        Springer-Verlag, Berlin, Göttingen, Heidelberg, 1957).

[3]   George Havas, "A Reidemeister-Schreier program", *Proc. Second Internat.
        Conf. Theory of Groups*, Canberra, 1973, 347-356 (Lecture Notes in
        Mathematics, 372. Springer-Verlag, Berlin, Heidelberg, New York,
        1974).

[4]   John Leech, "Coset enumeration on digital computers", *Proc. Cambridge
        Philos. Soc.* 59 (1963), 257-267.

[5]   I.D. Macdonald, "A computer application to finite p-groups", *J.
        Austral. Math. Soc.* 17 (1974), 102-112.

[6]   John Joseph Tobin, "On groups of exponent four" (PhD thesis,
        Manchester University, Manchester, 1954).

[7]   J.W. Wamsley, "Computation in nilpotent groups (theory)", *Proc. Second
        Internat. Conf. Theory of Groups*, Canberra, 1973, 691-700
        (Lecture Notes in Mathematics, 372. Springer-Verlag, Berlin,
        Heidelberg, New York, 1974).

Department of Mathematics,
Institute of Advanced Studies,
Australian National University,
Canberra, ACT.