ON THE EFFICIENCY OF SOME FINITE GROUPS

George Havas
Centre for Discrete Mathematics and Computing
School of Information Technology and Electrical Engineering
The University of Queensland, Queensland 4072, AUSTRALIA

M.F. Newman
Mathematical Sciences Institute
Australian National University
Canberra 0200, AUSTRALIA

E.A. O'Brien
Department of Mathematics
University of Auckland
Private Bag 92019, Auckland, NEW ZEALAND

Abstract

We describe a new technique for finding efficient presentations for finite groups. We use it to answer three previously unresolved questions about the efficiency of group and semigroup presentations.

1 Introduction

In this paper we report on a new practical technique for studying finite presentations for finite groups. This technique has allowed us to answer three previously unresolved questions about the efficiency of some finite groups. The questions relate to some groups with order 3^8 (see [9]), the group PSU(3,3) (see [3]) and some groups with order 2^{14} (see [8]).

The new technique is based on the observation that presentations for a group built on different generating sets with the same size can have quite different properties. We expect that the most significant property in the context of the questions we have been considering is the length of the presentation; that is, the sum of the lengths of the relators or relations. The length of the shortest presentation on a generating set varies considerably over all generating sets with the same size of a fixed group. A simple example illustrates the extent of this length variation. Consider the alternating group

A_5. For the generating set $\{a = (2,5,4),\ b = (1,2,3,4,5)\}$ a shortest presentation is $\{a, b \mid a^3, b^5, (ab)^2\}$ which has length 12. On the other hand for the generating set $\{a = (3,4,5),\ b = (1,2,3)\}$ a shortest presentation is $\{a, b \mid a^3, (aba^{-1}b)^2, abab^2abab^{-1}\}$ which has length 20. (The proof that it is shortest requires some work.) Note that the smallest number of relations relative to a generating set need not be the same for all minimal generating sets. The group of the trefoil knot is an example [5]. It is not known whether this can happen for finite groups.

The successful method for finding groups with deficiency zero in [9] involved looking at certain presentations with deficiency zero and observing the groups which are defined by them. This showed, for example, that 10 of the 14 groups with order 3^8 and trivial multiplicator have deficiency zero. We also found presentations (#11, #12, #13 and #14 [9, Section 3.4]) with deficiency zero which were 'close' to defining the other 4 groups in that the groups defined have a largest soluble quotient which has order 3^8. Since then two of these presentations have been shown to define infinite groups: #14 is settled in [7] and Derek Holt (private communication) has settled #13 using the same method.

The new technique involves taking many generating sets for a given group. On each generating set we build a presentation and then discard relations. Informally we regard two generating sets for a group as *equivalent* if the shortest presentations on them have the same length. For a generating set X of a group G, all the generating sets obtained from X by applying an automorphism of G to it are equivalent to X. So is the generating set obtained by inverting a generator. See Section 2 for details.

The first question we consider is whether the remaining 4 groups with order 3^8 and trivial multiplicator have deficiency zero. We introduce the name $3^8\#x$ for the group which is the largest 3-quotient of the group defined by the presentation $\#x$ in Section 3.4 of [9]. The new technique produces a number of efficient presentations for $3^8\#11$. These presentations are not restricted to the type guaranteed by Theorem 2 of [9]. This observation leads to other purely relator-based searches which found shorter presentations with deficiency zero for some of the groups settled in [9]. The searches did not produce an efficient presentation for any of the groups $3^8\#12$, $3^8\#13$ or $3^8\#14$. However, we produced more presentations which define groups whose largest soluble quotient is the group in question. Further details are in Section 3. We also applied a related technique to the groups with order 5^8 and trivial multiplicator.

Another question we consider arises from a paper of Campbell, Mitchell and Ruškuc [3]. They are interested in finding efficient semigroup presentations for finite groups. A finite semigroup presentation for a semigroup S is efficient if the number of relations minus the number of generators is the rank of the second homology group of S. They showed that every efficient group presentation for a finite group can be turned into an efficient semigroup presentation by adding at most one more generator and, if so, one more relation and then suitably modifying the existing relations. Further they showed that if the group presentation has a special form then the extra generator and relation are not needed. They give, as an example where an extra generator is used, a 3-generator, 3-relation semigroup presentation for PSU(3,3). Our technique enables us to find a special group presentation for PSU(3,3), so there is an efficient semigroup presentation for PSU(3,3) with 2 generators and 2 relations. See Section 4 for details.

Finally, we consider a question which arises out of the paper of Havas and Newman [8] in which it was shown that there are finite groups which cannot be generated by 3 elements and have a presentation with 4 generators and 5 relations. The method used in that paper was essentially a random search over presentations with 4 generators and 5 relations of a certain type. It produced groups of this kind with orders $2^{16}, 2^{17}, 2^{18}$ and 2^{19}. It is a well-known consequence of the Golod-Shafarevich Theorem that a finite p-group which has a minimal generating set with four elements needs at least five relations to define it. As was remarked in [8] the smallest order for a group of this kind is at least 2^{14}. Here we exhibit a 4-generator, 5-relator group with order 2^{14}. See Section 5 for details.

All computations reported in this paper were carried out using MAGMA [1] on a variety of platforms.

2 Presenting a group on different generating sets

Recall that in our study of groups with deficiency zero in [9] we constructed candidate groups. However, we made little use of the groups, instead concentrating on all short presentations of a certain kind. Here we focus on the groups.

We use the following technique to investigate whether a given group G has a presentation on k generators and r relators.

1. We determine a set of k-element subsets of G which generate G; the set is representative in the sense that every k-element generating set is equivalent to at least one member of it.

2. For each such generating set X of G, we obtain a finite presentation $\{X \mid \mathcal{R}\}$ for G on X.

3. Finally, we consider all r-element subsets $\mathcal{S}$ of $\mathcal{R}$ and investigate whether $\{X \mid \mathcal{S}\}$ presents G.

We now describe how to construct the representative k-element generating sets for G in more detail. The initial stage of the procedure is as follows.

a. Construct $\mathrm{Aut}(G)$, the automorphism group of G.

b. Construct a list $\mathcal{L}_1$ of representatives of orbits under $\mathrm{Aut}(G)$ of those elements of G not in the Frattini subgroup $\Phi(G)$.

c. Let x_1, the first element of a putative generating set, range over the elements of $\mathcal{L}_1$.

Assume $[x_1, x_2, \ldots, x_i]$ has been constructed. The inductive stage is as follows.

a. Let $S_{x_1,\ldots,x_i}$ be the stabiliser of $[x_1, \ldots, x_i]$ in $\mathrm{Aut}(G)$.

b. Construct a list $\mathcal{L}_{i+1}$ of representatives of orbits under $S_{x_1,\ldots,x_i}$ of those elements of G not in the subgroup $\langle \Phi(G), x_1, \ldots, x_i \rangle$.

c. Let x_{i+1} range over the elements of $\mathcal{L}_{i+1}$.

As described, the procedure chooses representatives of orbits under $\mathrm{Aut}(G)$ of elements of G. We can reduce the number of representatives by using length-preserving automorphisms of the corresponding free group. In practice, we merge the existing orbits under the mapping $g \longmapsto g^{-1}$. This usually gives a substantial reduction.

The procedure produces a representative list of generating sets for G. Then, given as input $G = \langle X \rangle$, the relation-finding algorithm of [4] is used to construct a finite presentation $\{X \mid \mathcal{R}\}$ for G.

The final stage of our technique is to attempt to find an r-element subset $\mathcal{S}$ of $\mathcal{R}$ which presents G. We do this by running through all r-element subsets of $\mathcal{R}$.

A verification that $\{X \mid \mathcal{S}\}$ presents G relies on a successful coset enumeration [11]. A successful enumeration over the trivial subgroup gives a direct proof. In more difficult cases, we enumerate cosets over a cyclic subgroup. If a cyclic subgroup is shown to have finite index, then the Reidemeister-Schreier algorithm can be used to find a presentation for it, and its order can be calculated by computing abelian quotient invariants.

It is possible to enumerate billions of cosets [10], but such enumerations are computationally expensive. Hence, we use cheap filters to remove presentations which cannot define the desired group. In particular, if G is a p-group, we check whether the group $\langle X \mid \mathcal{S} \rangle$ has a larger p- or metabelian quotient than G and, if so, discard the presentation. Such filters are discussed in Section 3.3 of [9]. If G is perfect we check that the group defined by a presentation has trivial abelian quotient invariants.

As a further heuristic filter for hard cases, we first carry out restricted coset enumerations over some larger subgroups. If these succeed we attempt enumerations over cyclic subgroups, now allowing many more cosets to be defined.

Our technique has random components: the orbit representatives are selected randomly and the implementation of the relation-finding algorithm has some random aspects. Therefore different runs may produce different output presentations.

3 Groups with order p^8

For brevity in the following sections we use the case inverse convention in which A and B denote a^{-1} and b^{-1}, etc.

Theorem 3.1. *The group defined by the presentation*

$$\{a, b, c \mid BcABACAB, acBABBC, CCBBACBa\}$$

is $3^8\#11$*.*

Its order can be verified by coset enumeration. That it is $3^8\#11$ can be proved by the standard presentation algorithm [14].

We obtained presentations for $3^8\#11$ by using the procedure described in Section 2 to produce about 75000 different generating sets. Among the subsets of relators for one of these generating sets we found the presentation of the theorem. This presentation does not conform to Theorem 2 of [9]:

Proposition 3.2. *If a group of order p^8 has a 3-generator 3-relator presentation, then it has a presentation $\{a, b, c \mid u, v, w\}$ where the length of each relator is at least $p + 2$ and the exponent sum matrix is diagonal with entries p, p, p.*

It is easy to convert our presentation to a conforming presentation with length 27: multiply a cyclic permutation of the first relator by a cyclic permutation of the inverse of the second relator, and do the same with the third relator.

In [9] we investigated conforming presentations with total relator length up to 21. The discovery of this presentation led us to investigate longer and nonconforming presentations involving relators with lengths up to 9. In a search through about 8 million presentations we found 30 nonconforming presentations with various lengths, none shorter than 23, for $3^8\#11$. Even though we applied both the new technique and these extra relator based searches, we did not find a 3-relator presentation for $3^8\#12$, $3^8\#13$ or $3^8\#14$.

We discovered nonconforming presentations shorter than our published presentations for other groups with order 3^8. Thus:

$$\begin{aligned} \{a,b,c \mid bbcbC, ccacA, abaabb\} &\quad \text{presents} \quad 3^8\#2;\\ \{a,b,c \mid bbcbC, ccAca, abaabb\} &\quad \text{presents} \quad 3^8\#3;\\ \{a,b,c \mid abaabb, bCbbCC, cacBcbA\} &\quad \text{presents} \quad 3^8\#6;\\ \{a,b,c \mid abaabb, bcbbcc, accbAcB\} &\quad \text{presents} \quad 3^8\#7. \end{aligned}$$

We also found a shorter conforming presentation for $3^8\#9$, namely

$$\{a,b,c \mid aaBab, bbCacbA, ccBcAba\}.$$

This was revealed by doing more comprehensive coset enumerations than when we first considered the presentation.

In [9] we proposed a candidate efficient presentation for a group with order 5^8, however it presents an infinite group [7]. The approach used successfully for $3^8\#11$ is not readily applicable to groups with order 5^8 since each group has too many representative generating sets. Instead we investigated a random selection of generating sets for each of the 32 groups with order 5^8 and trivial multiplicator. We found many presentations with deficiency one for these groups, but none with deficiency zero.

4 PSU(3,3) as an efficient semigroup

Campbell, Mitchell and Ruškuc [3] ask whether, given a group presentation for G, one can always find a semigroup presentation for G on the same generating set and with the same deficiency. They have the following result.

Proposition 4.1. *Let G be the group defined by the finite group presentation $\mathcal{P} = \{A \mid R\}$ where $|R| \geq |A|$ and let A be a semigroup generating set for G. In addition, assume that R contains a relation of the form $E = 1$, where E is a word which contains no inverses of generators, but which contains every generator at least once, and also contains the square of at least one generator. Then G has a semigroup presentation $\{A \mid Q\}$ with $|Q| = |R|$.*

Using another proposition, they obtain an efficient semigroup presentation for PSU(3,3) with 3 generators and 3 relations. They start from the efficient group presentation for PSU(3,3) due to Kenne [12], which does not contain a relation which allows application of Proposition 4.1. We show that PSU(3,3) has a 2-generator, 2-relation semigroup presentation by producing a suitable group presentation for PSU(3,3).

An application of our technique produces efficient presentations for PSU(3,3). Some are shorter than that of Kenne, for example:

$$\{a,b \mid B^2ABa^3BA, b^2AB^2Ab^2aBa\}.$$

However none of these are suitable for applying Proposition 4.1.

Instead, we obtained the following result by a variation of our methods.

Theorem 4.2. *The group* PSU(3,3) *has the efficient presentation*

$$\{a, b \mid a^3b^7, ABabbaabbbABB\}.$$

This can be proved by coset enumeration. We constructed the presentation by using our technique to find a 3-relator presentation which satisfies the following proposition due to Campbell, Havas and Robertson [2].

Proposition 4.3. *Let G be a finite simple group. Suppose that G, or some stem extension of G, can be presented as*

$$\{a, b \mid a^p = b^q = w(a, b) = 1\}.$$

Then G, the covering group of G, and all stem extensions of G, are efficient.

Since G is perfect, p and q are coprime. Campbell *et al.* [2] show how to convert such a presentation to an efficient presentation involving two relators: a^pb^q and $\bar{w}(a, b)$ depending on $w(a, b)$.

The relation-finding algorithm as implemented in Magma is well-suited for this task, since it usually includes relators giving the order of the group generators. Application of our procedure to PSU(3,3) gives 1442 representative generating sets. Among the resulting 3-relator subsets we found a presentation including the relators a^3 and b^7 plus a third relator $w(a, b)$ which leads to $\bar{w}(a, b) = ABabbaabbbABB$. We found several suitable group presentations on generating pairs with orders $\{3, 4\}$ and $\{3, 8\}$, as well as others with orders $\{3, 7\}$. However, we found no suitable presentation on a generating pair with orders $\{2, 7\}$. (An earlier attempt at finding one on generators with orders $\{2, 7\}$ is described in [6].)

5 An efficient group with order 2^{14}

Recall from [8] that the smallest p-group with a 4-generator, 5-relator presentation has order at least 2^{14}. However, no 4-generator 5-relator group with order 2^{14} was known. An argument similar to that of Theorem 1 of [9] shows that such a group has Frattini rank 4; its largest class 2 quotient has order 2^9 and nuclear rank 5; further its largest class 3 quotient has order precisely 2^{14} and is terminal. Such groups are *candidates*.

We used the p-group generation algorithm (see [13]) to construct a complete and irredundant list of candidates. A total of 3217 of the 6709 groups with order 2^9 and class 2 have nuclear rank equal to 5. Of these 14 have terminal immediate descendants with order 2^{14}: one has 104; each of the remaining 13 has 512. Hence there are 6760 candidates.

We constructed a presentation on a minimal generating set for each candidate. For each presentation and for each resulting 5-relator subset, we checked whether the group presented by this subset had largest 2-quotient with order 2^{14}. If so, we sought to prove finiteness by coset enumeration. This approach succeeded in exactly one instance.

Theorem 5.1. *The presentation*

$$\{a, b, c, d \mid caCAdd, CDCaaBDB, CDcBaBDA, BCDaaBDc, cbABaBcb\}$$

defines a group with order 2^{14}.

A moderately hard coset enumeration shows that the subgroup $\langle a \rangle$ has index 2048 in the group and the order, 8, of a can be found by computing the abelian quotient invariants of $\langle a \rangle$. A difficult coset enumeration over the trivial subgroup gives the result directly.

We expect that by looking at many generating sets as described in Section 2 efficient presentations for other groups with order 2^{14} could be found, but we have not attempted to do so.

Acknowledgements

This work was supported in part by the Marsden Fund of New Zealand via grant #9144/3600776. The second author was partially supported by the Australian Research Council.

REFERENCES

[1] Bosma, Wieb; Cannon, John; Playoust, Catherine. The Magma algebra system I: the user language. In *Computational algebra and number theory*, London, 1993; J. Symbolic Comput. **1997**, *24* (3-4), 235–265.

[2] Campbell, Colin M.; Havas, George; Robertson, Edmund F. Nice efficient presentations for small simple groups and their covers. Preprint.

[3] Campbell, C. M.; Mitchell, J. D.; Ruškuc, N. On defining groups efficiently without using inverses. Math. Proc. Cambridge Philos. Soc. **2002**, *133* (1), 31–36.

[4] Cannon, John J. Construction of defining relators for finite groups. Discrete Math. **1973**, *5*, 105–129.

[5] Dunwoody, M. J.; Pietrowski, A. Presentations of the trefoil group. Canad. Math. Bull. **1973**, *16*, 517–520.

[6] Gamble, Greg; Havas, George; Hulpke, Alexander. `PGRelFind`: a GAP example using the ACE share package, **2002**.
`http://www.gap-system.org/~gap/Intro/pgrelfind.html`
(accessed September 2002).

[7] Havas, George; Holt, Derek F.; Kenne, P. E.; Rees, Sarah. Some challenging group presentations. J. Austral. Math. Soc. Ser. A **1999**, *67* (2), 206–213.

[8] Havas, George; Newman, M. F. Minimal presentations for finite groups of prime-power order. Comm. Algebra **1983**, *11* (20), 2267–2275.

[9] Havas, George; Newman, M. F.; O'Brien, E. A. Groups of deficiency zero. In *Geometric and computational perspectives on infinite groups*, Minneapolis, MN and New Brunswick, NJ, 1994; DIMACS Ser. Discrete Math. Theoret. Comput. Sci. **1996**, *25*, Amer. Math. Soc., Providence, RI, 53–67.

[10] Havas, George; Ramsay, Colin. Proving a group trivial made easy: a case study in coset enumeration. Bull. Austral. Math. Soc. **2000**, *62* (1), 105–118.

[11] Havas, George; Ramsay, Colin. Experiments in coset enumeration. In *Groups and computation, III*, Columbus, OH, 1999; Ohio State Univ. Math. Res. Inst. Publ. **2001**, *8*, de Gruyter, Berlin, 183–192.

[12] Kenne, P. E. Efficient presentations for three simple groups. Comm. Algebra **1986**, *14* (5), 797–800.

[13] O'Brien, E. A. The p-group generation algorithm. In *Computational group theory, Part 1*; J. Symbolic Comput. **1990**, *9* (5-6), 677–698.

[14] O'Brien, E. A. Isomorphism testing for p-groups. J. Symbolic Comput. **1994**, *17* (2), 133–147.