EFFICIENT SIMPLE GROUPS*

Colin M. Campbell
Mathematical Institute
University of St Andrews
North Haugh, St Andrews, Fife KY16 9SS, SCOTLAND

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

Alexander Hulpke
Department of Mathematics
Colorado State University
Fort Collins, CO 80523, USA

Edmund F. Robertson
Mathematical Institute
University of St Andrews
North Haugh, St Andrews, Fife KY16 9SS, SCOTLAND

Abstract

We prove that the simple group $L_3(5)$ which has order 372000 is efficient by providing an efficient presentation for it. This leaves one simple group with order less than one million, $S_4(4)$ which has order 979200, whose efficiency or otherwise remains to be determined.

1 Introduction

For a finite group G we denote the Schur multiplier by $M(G)$ [16].

Definition 1.1. The *deficiency* of a finite presentation $P := \{X \mid R\}$ of G is $|R|-|X|$. The *deficiency of* G, $\operatorname{def}(G)$, is the minimum of the deficiencies of all finite presentations of G. The group G is said to be *efficient* if $\operatorname{def}(G) = \operatorname{rank}(M(G))$.

In general it seems to be a hard problem to decide whether a given group is efficient. The problems of proving specific finite groups efficient, and of finding

* An early draft of this paper was mistakenly printed in volume 30(2), 971–975 (2002). This is the correct version.

inefficient finite groups, have been studied by several authors. For efficient groups see for example [11, 2, 10], and for inefficient groups [16, 13, 15].

Considerable effort has been put into showing that simple groups of small order are efficient; a survey of results for simple groups of order less than one million is given in [4]. Prior to this work, no further progress on the problem had occurred since that survey, so there remained two simple groups of order less than one million whose deficiency remained to be determined, namely $L_3(5)$ and $S_4(4)$. Since both these groups have trivial multiplier the task of proving efficiency figured to be more difficult than for similar size groups with nontrivial multiplier.

We apply computational methods in an attempt to determine the efficiency of these groups. Our methods have been successful in proving that $L_3(5)$ is efficient and, although the deficiency of $S_4(4)$ is not determined, more progress has been made.

2 Our Approach

As starting points we have presentations on minimal generating pairs for all simple groups of order less than one million [5, 3]. A *minimal generating pair* for G is a pair $x, y \in G$ such that $G = \langle x, y\rangle$, $|x| = 2$ and $|y|$ is minimal among all such y for a given involution x. For many purposes it is sufficient to consider such pairs up to automorphisms.

Definition 2.1. For a word w in the free group generated by a and b, let $e_a(w)$, $e_b(w)$ be the exponent sums of a and b in w.

Lemma 2.2. *Let G be a simple group with trivial Schur multiplier. Suppose G has a presentation of the form*

$$P = \{a, b \mid a^2 = 1, b^p = 1, w(a, b) = 1\} \tag{1}$$

with p prime. Then G has deficiency zero.

Proof. Since G is perfect, p must be odd, $e_a(w)$ is odd and $e_b(w) \not\equiv 0 \pmod p$.

Suppose first that $e_b(w) \equiv \frac{1}{2} \pmod p$. Consider the new word

$$\bar{w}(a, b) = w(a, b)a^{1-e_a(w)}b^{\frac{p+1}{2}-e_b(w)}.$$

Then $P_1 = \{a, b \mid a^2b^p = 1, \bar{w}(a, b) = 1\}$ is a deficiency zero presentation for G. For in $\langle P_1\rangle$ the element a^2 is central, $\langle P_1\rangle / \langle a^2\rangle \cong G$ and, since $\langle P_1\rangle' = \langle P_1\rangle$, then $a^2 \in M(G) = 1$. Hence $a^2 = b^p = 1$ in $\langle P_1\rangle$, so $\langle P_1\rangle \cong \langle P\rangle \cong G$.

Finally, if $e_b(w) \not\equiv \frac{1}{2} \pmod p$, we can perform a Tietze transformation on P, replacing b by $b^{1/(2e_b(w))}$, and apply the same argument. □

The results of [14] show that all finite simple groups have presentations of the form

$$\{a, b \mid a^2 = 1, b^n = 1, w_i(a, b) = 1, i = 1, \ldots, k\}.$$

In particular, for groups of order less than one million, the order n of the second generator can be taken to be a prime. $L_3(5)$ has presentations of this form with $n = 3$ and $S_4(4)$ has presentations of this form with $n = 5$ [3].

3 Computational Methods

Suppose G is a finite simple group with a presentation of the form

$$\{a, b \mid a^2 = 1, b^p = 1, w_i(a, b) = 1, i = 1, \dots, k\}$$

with p prime. A naïve approach is to replace the $w_i(a, b)$ $(i = 1, \dots, k)$ by fewer relators, replacing the pair of relators $w_s(a, b)$ and $w_t(a, b)$ by $g^{-1}w_s(a, b)gw_t^{\pm 1}(a, b)$ for some word $g = g(a, b)$, and iterating the process. Such methods have been used successfully in, for example, [11, 10].

We automated this approach in an attempt to find presentations for $L_3(5)$ and $S_4(4)$ of the form (1). Computing facilities have improved, both in terms of hardware and software, since the earlier work described in [4]. However, we did not find a presentation of the desired form this way, in spite of comprehensive experimentation.

We therefore tried another approach, looking for candidate third relators for a presentation of the form (1) by brute force. Thus we enumerated the short words $w(a, b)$ such that: $w(a, b) = 1$ in $L_3(5)$; $e_a(w)$ is odd; and $e_b(w) \not\equiv 0 \pmod p$. To do this we wrote a reasonably general GAP [6] program `PGRelFind` [7, 8] in order to attempt to find such words in any perfect group with a $(2, p)$ generating pair.

There are some kinds of words we do not need to consider. The word $w(a, b)$ cannot be a proper power (see the classification theorem in [9, p.138]). As $L_3(5)$ does not appear in the classification of [1] we know that $w(a, b)$ cannot be of length ≤ 24. If $p = 3$ we may therefore assume that $w(a, b)$ has a prefix $ababab^{-1}a$, and for $p > 3$ only a prefix aba may be assumed.

Having found a candidate we can attempt to show that it suffices. Our key tool here is coset enumeration. Our first step is to check that the (preimage of a) largest maximal subgroup has correct index. Once this is done, we try to prove the group is correct.

4 An Efficient Presentation for $L_3(5)$

We start off by enumerating candidates in length order. Take the presentation 17.6 of [3] for $L_3(5)$:

$$\begin{aligned}\{a, b \quad | \quad & a^2 = b^3 = (ab)^{31} = (ab)^9 aBab((aB)^3 ab)^3 aB \\ & = (ab)^4 (abaB)^2 (ab)^5 (aB)^4 (abaB)^2 (aB)^3 = 1\}\end{aligned}$$

(writing $B = b^{-1}$). Using the program `PGRelFind` on a faithful permutation representation obtained from this presentation we find that

$$w(a, b) = ababaBaBabaBaBabababaBaBabaBaBababababaBababaBabab$$

of syllable length 50 is such a word (shortest such, in fact).

A coset enumeration (using, for example, the ACE coset enumerator share package [8]) on the resulting presentation

$$\mathcal{L} = \{a, b \mid a^2 = 1, b^3 = 1, w(a, b) = 1\}$$

shows that the index of $\langle b \rangle$ is 124000, proving that $\langle \mathcal{L} \rangle \cong L_3(5)$. Lemma 2.2 now shows that $L_3(5)$ has the efficient presentation

$$\bar{\mathcal{L}} = \left\{a, b \mid a^2b^3 = 1, \bar{w}(a, b) = 1\right\}.$$

In fact, direct coset enumeration shows that the presentation $\{a, b \mid a^2b^3 = AbAbABAbAbABaBaBAbAbABAbAbABaBaBaBabaBaBabaBaBABAB = 1\}$ is an explicit efficient presentation for $L_3(5)$. Using the standard `Hard` style, the ACE enumerator can complete the enumeration over the trivial subgroup defining a maximum of 91457439 cosets and a total of 92162535 cosets.

5 A Deficiency One Presentation for $S_4(4)$

Encouraged by our success with $L_3(5)$, we used the same approach in attempts to find an efficient presentation for $S_4(4)$. The program `PGRelFind` finds various $w(a, b)$ which satisfy $w(a, b) = 1$ in $S_4(4)$; $e_a(w)$ is odd; and $e_b(w) \not\equiv 0 \pmod 5$. Unfortunately, in each case that we have tried the corresponding presentation (1) does not define $S_4(4)$ since we were able to show that it defined a proper extension.

We expanded the search to look at generating pairs for $S_4(4)$ which are not minimal. Despite a major computational effort, again the words found do not lead to efficient presentations of $S_4(4)$.

Finally we took pairs of relators $w_1(a, b)$, $w_2(a, b)$ that we had discovered in the above search. We were able to prove, using coset enumeration, that

$$\left\{a, b \mid a^2, b^{15}, abaBab^7ab^7aB^5abaB^2aB^3ab^2, abaBaBBaBaBBaBab\right\}$$

is a presentation for $S_4(4)$. This leads to a deficiency one presentation using a modification of Lemma 2.2.

The method described in the first paragraph of Section 3 is not applicable to this presentation since any composite relator created that way has even exponent sum on a.

Acknowledgements

The work in this paper was initiated while the second and third authors were in St Andrews. It was supported by EPSRC Grant GL/L21013. The second author was partially supported by the Australian Research Council. We thank Greg Gamble for help with GAP programs. We are grateful to the University of St Andrews for access to the Beowolf cluster and to The University of Queensland's High Performance Computing Unit for access to the Origin 2000 supercomputer where many major computations were performed.

REFERENCES

[1] Conder, M. *Three-relator quotients of the modular group*, Quart. J. Math. Oxford Ser. (2) **38** (1987), no. 152, 427–447.

[2] Campbell, C.M.; Robertson, E.F. *The efficiency of simple groups of order* $< 10^5$, Comm. Algebra **10** (1982), no. 2, 217–225.

[3] Campbell, C.M.; Robertson, E.F. *Presentations for the simple groups* G, $10^5 < |G| < 10^6$, Comm. Algebra **12** (1984), no. 21-22, 2643–2663.

[4] Campbell, C.M.; Robertson, E.F.; Williams, P.D. *Efficient presentations for finite simple groups and related groups*, Proceedings of the Second International Conference on Group Theory held in Pusan, August 15–21, 1988 (Berlin) (Kim, A.C.; Neumann, B.H. Eds.), Springer, 1989, pp. 65–72.

[5] Cannon, J.J.; McKay, J.; Young, K. *The non-abelian simple groups* G, $|G| < 10^5$ *— presentations*, Comm. Algebra **7** (1979), no. 13, 1397–1406.

[6] The GAP Group, Aachen, St Andrews, GAP – *Groups, Algorithms, and Programming, Version* 4.2, 2000.
`http://www-gap.dcs.st-and.ac.uk/~gap/`

[7] Gamble, G.; Havas, G.; Hulpke, A. PGRelFind*: a* GAP *example using the* ACE *share package*, 2000.
`http://www-gap.dcs.st-and.ac.uk/~gap/Intro/pgrelfind.html`

[8] Gamble, G.; Havas, G.; Hulpke, A.; Ramsay, C. ACE*: a* GAP 4 *interface to the Advanced Coset Enumerator of G. Havas and C. Ramsay*, 2000.
`http://www-gap.dcs.st-and.ac.uk/~gap/Share/ace.html`

[9] Howie, J.; Metaftsis, V.; Thomas, R.M. *Triangle groups and their generalisations*, In [12], pp. 135–147.

[10] Jamali, A; Robertson, E.F. *Efficient presentations for certain simple groups*, Comm. Algebra **17** (1989), no. 10, 2521–2528.

[11] Kenne, P.E. *Efficient presentations for three simple groups*, Comm. Algebra **14** (1986), no. 5, 797–800.

[12] Kim, A.C.; Johnson, D.L. (Eds.), *Groups—Korea '94*, Berlin, Walter de Gruyter & Co., 1995.

[13] Kovács, L.G. *Finite groups with trivial multiplicator and large deficiency*, In [12], pp. 211–225.

[14] Malle, G; Saxl, J.; Weigel, T. *Generation of classical groups*, Geom. Dedicata **49** (1994), no. 1, 85–116.

[15] Robertson, E.F; Thomas, R.M.; Wotherspoon, C.I. *A class of inefficient groups with symmetric presentation*, In [12], pp. 277–284.

[16] Wiegold, J. *The Schur Multiplier: An elementary approach*, Groups – St Andrews 1981, (Campbell, C.M; Robertson, E.F. Eds.), LMS Lecture Notes Series, vol. 71, Cambridge University Press, 1982, pp. 137–154.