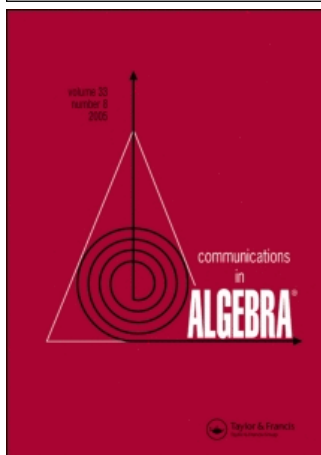


This article was downloaded by:[Australian National University]
On: 11 January 2008
Access Details: [subscription number 788736294]
Publisher: Taylor & Francis
Informa Ltd Registered in England and Wales Registered Number: 1072954
Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



Communications in Algebra

Publication details, including instructions for authors and subscription information:

<http://www.informaworld.com/smpp/title-content=t713597239>

Efficient Simple Groups

Colin M. Campbell ^a, George Havas ^b, Alexander Hulpke ^{cd}, Edmund F. Robertson ^a

^a Mathematical Institute, University of St Andrews, Fife, Scotland

^b Centre for Discrete Mathematics and Computing, School of Information Technology and Electrical Engineering, The University of Queensland, Queensland, Australia

^c Department of Mathematics, Colorado State University, Fort Collins, Colorado, USA

^d Department of Mathematics, Colorado State University, Fort Collins, CO, USA

Online Publication Date: 10 January 2003

To cite this Article: Campbell, Colin M., Havas, George, Hulpke, Alexander and Robertson, Edmund F. (2003) 'Efficient Simple Groups', Communications in

Algebra, 31:10, 5191 - 5197

To link to this article: DOI: 10.1081/AGB-120023154

URL: <http://dx.doi.org/10.1081/AGB-120023154>

PLEASE SCROLL DOWN FOR ARTICLE

Full terms and conditions of use: <http://www.informaworld.com/terms-and-conditions-of-access.pdf>

This article maybe used for research, teaching and private study purposes. Any substantial or systematic reproduction, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.

COMMUNICATIONS IN ALGEBRA®

Vol. 31, No. 10, pp. 5191–5197, 2003

Efficient Simple Groups[#]

Colin M. Campbell,¹ George Havas,² Alexander Hulpke,^{3,*}
and Edmund F. Robertson¹

¹Mathematical Institute, University of St Andrews, North Haugh,
St Andrews, Fife, Scotland

²Centre for Discrete Mathematics and Computing, School of
Information Technology and Electrical Engineering,
The University of Queensland,
Queensland, Australia

³Department of Mathematics, Colorado State University,
Fort Collins, Colorado, USA

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.

[#]A version of this paper with a large number of editorial errors was mistakenly printed in volume 30(9), 4613–4619 (2002). This is the correct version.

*Correspondence: Alexander Hulpke, Department of Mathematics, Colorado State University, Fort Collins, CO 80523, USA; E-mail: hulpke@math.colostate.edu.

5191

DOI: 10.1081/AGB-120023154
Copyright © 2003 by Marcel Dekker, Inc.

0092-7872 (Print); 1532-4125 (Online)
www.dekker.com



Key Words: Efficient presentations; Simple groups.

1. INTRODUCTION

For a finite group G we denote the Schur multiplier by $M(G)$ (Wiegold, 1982).

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

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 inefficient finite groups, have been studied by several authors. For efficient groups see for example Campbell and Robertson (1982), Jamali and Robertson (1989) and Kenne (1986), and for inefficient groups, Kovács (1995), Robertson et al. (1995), and Wiegold (1982).

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 Campbell et al. (1989). 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 (Cannon et al., 1979; Campbell and Robertson, 1984). 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

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

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. $\square$

The results of Malle et al. (1994) show that all finite simple groups have presentations of the form

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

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 $n=5$ (Campbell and Robertson, 1984).

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, Kenne (1986) and Jamali and Robertson (1989).

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 Campbell et al. (1989). 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 (The GAP group, 2000) program PGRelFind (Gamble et al., 2000a,b) 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 Howie et al., 1995, p. 138). As $L_3(5)$ does not appear in the classification of Conder (1987) 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 Campbell and Robertson (1984) for $L_3(5)$:

$$\{a, b \mid a^2 = b^3 = (ab)^{31} = (ab)^9 aBab((aB)^3 ab)^3 aB \\ = (ab)^4 (abaB)^2 (ab)^5 (aB)^4 (abaB)^2 (aB)^3 = 1\}$$

(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 coset enumerator share package (Gamble et al., 2000b) 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

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

In fact, direct coset enumeration shows that the presentation $\{a, b \mid a^2 b^3 = AbAbABAbAbABaBaBaBaBaBaBaBaBaBaBabaBaBABAB = 1\}$ 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 PGRel-Find 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

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

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 Sec. 3 is not applicable to this presentation since any composite relator created that way has even exponent sum on a .



ACKNOWLEDGMENTS

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

- Campbell, C. M., Robertson, E. F. (1982). The efficiency of simple groups of order $< 10^5$. *Comm. Algebra* 10(2):217–225.
- Campbell, C. M., Robertson, E. F. (1984). Presentations for the simple groups G , $10^5 < |G| < 10^6$. *Comm. Algebra* 12(21–22):2643–2663.
- Campbell, C. M., Robertson, E. F., Williams, P. D. (1989). Efficient presentations for finite simple groups and related groups. In: *Proceedings of the Second International Conference on Group Theory held in Pusan, August, 15–21, 1988*; Kim, A. C., Neumann, B. H., eds.; Berlin: Springer, pp. 65–72.
- Cannon, J. J., McKay, J., Young, K. (1979). The non-abelian simple groups G , $|G| < 10^5$ — presentations. *Comm. Algebra* 7(13):1397–1406.
- Conder, M. (1987). Three-relator quotients of the modular group. *Quart. J. Math. Oxford Ser. (2)* 38(152):427–447.
- Gamble, G., Havas, G., Hulpke, A. (2000a). PGRelfind: a GAP example using the share package ACE. <http://www-gap.dcs.st-and.ac.uk/~gap/Intro/pgrelfind.html>.
- Gamble, G., Havas, G., Hulpke, A., Ramsay, C. (2000b). ACE: a GAP 4 interface to the Advanced Coset Enumerator of G. Havas and C. Ramsay. <http://www-gap.dcs.st-and.ac.uk/~gap/Share/ace.html>.
- Howie, J., Metaftsis, V., Thomas, R. M. (1995). Triangle groups and their generalisations. In: Kim, A. C., Johnson, D. L., eds. *Groups-Korea '94*. Berlin: Walter de Gruyter & Co., pp. 135–147.
- Jamali, A., Robertson, E. F. (1989). Efficient presentations for certain simple groups. *Comm. Algebra* 17(10):2521–2528.
- Kenne, P. E. (1986). Efficient presentations for three simple groups. *Comm. Algebra* 14(5):797–800.

- Kovács, L. G. (1995). Finite groups with trivial multiplier and large deficiency. In: Kim, A. C., Johnson, D. L., eds. *Groups-Korea '94*. Berlin: Walter de Gruyter & Co., pp. 211–225.
- Malle, G., Saxl, J., Weigel, T. (1994). Generation of classical groups. *Geom. Dedicata* 49(1):85–116.
- Robertson, E. F., Thomas, R. M., Wotherspoon, C. I. (1995). A class of inefficient groups with symmetric presentation. In: Kim, A. C., Johnson, D. L., eds. *Groups-Korea '94*. Berlin: Walter de Gruyter & Co., pp. 277–284.
- The GAP Group, Aachen, St Andrews, GAP – *Groups, Algorithms, and Programming, Version 4.2*, 2000. <http://www-gap.dcs.st-and.ac.uk/~gap/>.
- Wiegold, J. (1982). The Schur Multiplier: An elementary approach. In: Campbell, C. M., Robertson, E. F., eds. *Groups – St Andrews 1981*. LMS Lecture Notes Series, 71, Cambridge University Press, pp. 137–154.

Received August 2000



