Efficient presentations for the Mathieu simple group M_{22} and its cover

Marston Conder, George Havas and Colin Ramsay

Abstract. Questions about the efficiency of finite simple groups and their covering groups have been the subject of much research. We provide new efficient presentations for the Mathieu simple group M_{22} and its cover, including the shortest known efficient presentation for M_{22} and a somewhat longer presentation which is very suitable for computation.

2000 Mathematics Subject Classification: 20-04, 20D05, 20D06, 20D08, 20F05

1. Introduction

Nice efficient presentations for small simple groups and their covering groups appear in [4]. Here we study the larger simple group M_{22} and its covering group in more detail from a similar point of view. We give new efficient presentations for both of these groups and we describe the computational techniques used in finding them.

For a finite group G the group H is a *stem extension* of G if there is a subgroup $A \leq Z(H) \cap H'$ with $G \cong H/A$. A stem extension of maximal order is called a *covering group* of G and the subgroup A in this case is the *Schur multiplier* of G denoted by $M(G)$. The *deficiency* of a finite presentation $P := \{X \mid R\}$ of G is $|R| - |X|$. The deficiency of G, $\mathrm{def}(G)$, is the minimum of the deficiencies of all finite presentations of G. For a good overview of Schur multipliers and related topics, see [14] — Corollary 1.2 of which shows that $\mathrm{rank}(M(G))$ is a lower bound for $\mathrm{def}(G)$. The group G is said to be *efficient* when this lower bound is achieved.

Deciding whether a given group is efficient may be difficult; indeed the problem is unsolvable in general [1]. Previous work has used a variety of techniques to try to find efficient presentations. In particular, considerable effort has been put into showing that simple groups of small order are efficient. A survey of results as at 1988 for simple groups with order up to one million was given in [5]. Subsequent to this, $L_3(5)$ has been shown to be efficient [3].

Similarly, work has been carried out to show that the covering groups of the small simple groups are efficient. Since, by a result of Kervaire [12], the covering groups of finite simple groups have trivial multiplier, a balanced presentation (that is, one with an equal number of generators and relations) is required to show these groups are efficient. References to balanced presentations for the covering groups of simple groups with order up to one million, as at 1988, are also given in [5].

More recent work on nice efficient presentations for simple groups with order up to 10^5 and their covering groups appears in [4]. Motivated in part by the fact that $\widehat{M}_{22}$ (the covering group of the Mathieu simple group M_{22}) has surprisingly short efficient presentations [9], we investigate efficient presentations for both the simple group M_{22} and its cover. M_{22} has order 443520, its covering group has order 5322240, and its Schur multiplier is cyclic of order 12, so efficient presentations for M_{22} have one more relator than the number of generators.

2. Methodology

We use three distinct techniques in our investigation. We look at short presentations for perfect groups; we consider representatives of all generating pairs for M_{22}; and we look at one-relator quotients of free products $C_m * C_n$ for small m and n. Here we explain the third method after outlining the others which are already described elsewhere.

The first method relies on censuses of short presentations of perfect groups, extending work by Havas and Ramsay [9]. The extension includes 2-generator 2-relator presentations of length up to 24, 2-generator 3-relator presentations of length up to 26, and 3-generator 3-relator presentations of length up to 20 (where *length* is the sum of the lengths of the relators in the presentation). A hardware-independent indication of the resources used is the number of canonical 2-generator 2-relator presentations of length up to 24 which were considered; starting at length 10 the counts are: 1, 4, 7, 68, 78, 600, 694, 6106, 7311, 54844, 66335, 509220, 630052, 4491064 and 5655194.

The second method uses a Magma [2] program developed by Havas, Newman and O'Brien [7], which enables us to find distinct generating sets for moderately-sized permutation groups. (The program uses representatives from appropriately merged orbits of the action of the automorphism group of each permutation group studied.) We use this program to find such distinct generating pairs for groups under consideration, and then use the built-in algorithm of Magma to find a presentation of the group on some of these generating sets.

Presentations found this way tend to have a reasonably small number of relators, but are rarely efficient, even for small groups. Often, however, simply checking all efficient-sized subsets of the relators reveals efficient presentations. These checks are carried out by first quickly checking that a subset presents a perfect group (for otherwise it does not present a group we are seeking). Note that here we might be looking for either the underlying simple group or some stem extension of it. If this test is passed, then we attempt to check by coset enumeration that the presentation defines a group we are seeking; we use the ACE enumerator (Havas and Ramsay [8]), either as available in GAP [6] or MAGMA , or as a stand-alone program for some more difficult cases.

Now we describe the third method in general. We consider one-relator quotients of $C_m * C_n$ (the free product of cyclic groups of orders m and n) for coprime m and n. By a one-relator quotient of a particular group, we mean a group obtained by adding one extra relator to a presentation for the specified group.

The free product $C_m * C_n$ has natural presentation $\{x, y \mid x^m,\ y^n\}$, and we are interested in finding simple or perfect finite quotients of this group that can be obtained by adjoining a single extra relator. Thus we seek quotients of the form $\langle\, x, y \mid x^m,\ y^n,\ w(x,y)\,\rangle$ where $w = w(x,y)$ is a word in the generators x and y and their inverses x^{-1} and y^{-1}, usually of relatively small length. This method requires the enumeration of possibilities for w, with elimination of redundant possibilities that are either equivalent to earlier ones or of a form that will not produce a perfect quotient.

Relators fall into equivalence classes under the obvious operations of cyclic conjugacy and inversion, which together make up a dihedral group of order $2m$ on words of length m: cyclic shift is an operation ρ of order m (taking $g_1g_2g_3...g_m$ to $g_2g_3...g_mg_1$), and inversion is an involutory operation σ (taking $g_1g_2g_3...g_m$ to $g_m^{-1}...g_3^{-1}g_2^{-1}g_1^{-1}$), such that σ inverts ρ under conjugation. Using these observations, it is easy to eliminate cyclic conjugates and inverses of cyclic conjugates of words considered previously in the enumeration of possibilities for w.

Relators which lead to non-perfect quotients are also easily eliminated, using a simple check on the exponent-sum of w for each generator x and y: if $w(x,y) = x^{p_1}y^{q_1}x^{p_2}y^{q_2}...x^{p_s}y^{q_s}$ has exponent-sums $\Sigma_x = p_1+p_2+...+p_s = p$ and $\Sigma_y = q_1+q_2+...+q_s = q$, say, then the abelianisation of the group $\langle\, x, y \mid x^m,\ y^n,\ w(x,y)\,\rangle$ is $\langle\, x, y \mid x^m,\ y^n, x^py^q, [x,y]\,\rangle$, which is non-trivial if $\gcd(m,p) \neq 1$ or $\gcd(n,q) \neq 1$. Hence we require $\gcd(m, \Sigma_x) = \gcd(n, \Sigma_y) = 1$ if we wish to obtain a perfect quotient of $C_m * C_n$.

For each (irredundant) possibility found, we use coset enumeration to attempt to determine the order of the quotient $\langle\, x, y \mid x^m,\ y^n,\ w(x,y)\,\rangle$. In some cases this is already known to be infinite, and those cases are ignored. For example, if $w(x,y) = (xy)^k$ where $1/k + 1/m + 1/n \leq 1$, the quotient is a Euclidean or hyperbolic triangle group, and similarly in many other cases where w is of the form u^k for some subword $u = u(x,y)$, the quotient is a generalised triangle group, and can be eliminated if this is known to be infinite; see [10, 13].

We have implemented MAGMA programs which allow us to specify m, n, allowable lengths for w, and desired quotient groups. We have run such programs seeking presentations which have M_{22} as a homomorphic image.

3. Results

In the following, we adopt the convention of using upper-case letters to denote inverses. Thus, $ABab$ denotes the commutator $[a,b] = a^{-1}b^{-1}ab$, and so on. We assess the presentations produced in terms of their length, their structure, and their behaviour as targets of coset enumeration. By length we mean the total length of the relators (after their free and cyclical reduction, as done by ACE when applicable). We give the total number of cosets used in a successful coset enumeration for this presentation over the trivial subgroup using the `Hard` strategy of the ACE enumerator. (We use this purely as a measure of coset enumeration performance and do not suggest that enumerations over the trivial subgroup are the best way to compute with the presentations to gain other information about the group.)

In 1989 Jamali and Robertson [11] published the first known efficient presentation for M_{22}, namely:

$$\left\{a, b \mid a^2 = (ab)^{11},\ (ababb)^7 = b^4,\ (ab)^2(aB)^2abb(ab)^2aBab(abb)^2 = b^4\right\}.$$

They obtained this by amalgamating relators in a cleverly constructed 5-relator presentation for the group. Our methods (which apply more widely than to just M_{22} and its cover) produce presentations that are much shorter and presentations that have nice forms. Such presentations can be computationally more useful since they lead to efficient straight-line programs which can be used to check group representations.

In 2003 Havas and Ramsay [9] published the first efficient presentation for the covering group $\widehat{M}_{22}$. Surprisingly, the cover has very short efficient presentations: length 17. Indeed, with 'canonical' as defined in [9], the unique shortest canonical presentation for $\widehat{M}_{22}$ is

$$\{a, b \mid aababAAB,\ abbbbaBaB\}.$$

The proof is by coset enumeration. It is also straightforward to use coset enumeration to find coset representatives for central elements having order 12 in this group. (This can be done by simple brute-force: test all of the elements.) A shortest such representative gives

$$\{a, b \mid aababAAB,\ abbbbaBaB,\ aabABBAABBAbbABabbABabbABAb\}$$

as a presentation for M_{22} itself.

Note that this presentation has length 44 compared with length 82 for the Jamali-Robertson presentation. Furthermore, for coset enumeration this presentation is quite easy, requiring a total of only 448968 cosets to enumerate the 443520 cosets of the trivial subgroup. This compares with a total of 907059999 for the Jamali-Robertson presentation and thus it is much superior from a computational perspective.

3.1. Method 1.

Our first method readily reveals the following presentations for the cover with length up to 21 (among others), given in Table 1 (including the shortest canonical 2-generator presentation for $\widehat{M}_{22}$). These presentations from censuses of short presentations arise with relators in a canonic form, as described in [9]. We list the presentations in length order but do not analyze them individually in detail. However we do provide some commentary. We number the presentations for convenience and refer to them as P_n in accord with this numbering. The "Total cosets" column gives total cosets for a successful enumeration over the trivial subgroup. Note that we did not find any 2-generator, 3-relator presentation for M_{22} (as distinct from presentations for the cover) using this method.

Table 1: $\widehat{M}_{22}$ from Method 1

No.	Relators	Length	Total cosets
1	$aababAAB, abbbbaBaB$	17	21611026
2	$aaaaabbb, aababABABab$	19	23024264
3	$aaaaa, bbb, aababABABab$	19	12902711
4	$aaaaabbb, aabABababAB$	19	24442031
5	$aaaaa, bbb, aabABababAB$	19	13063356
6	$aababAAB, aaaaaabbbbb$	19	40304685
7	$aababAAB, aaaaaa, bbbbb$	19	17917189
8	$aaaabAbAb, aabABabbAB$	19	23098382
9	$aababABAB, abbabbaBBB$	19	28017778
10	$aaaaa, ababab, abbAbABB$	19	11181678
11	$abc, aaBcAb, acccBCaC$	19	19102618
12	$abc, aaBcbb, acBcBCCC$	19	19426579
13	$aabAABB, aaabbabAbAbAb$	20	29179041
14	$aabAABB, aabaBABABABab$	20	22226752
15	$aabAABB, ababAbbABBBAb$	20	20068916
16	$aabaabAAB, abababababBB$	20	24018995
17	$aaaaa, ababab, aabABBabAB$	21	13063072
18	$aaaaa, ababab, abaBaBaBBB$	21	38353459
19	$aaaaa, ababab, abbAbAbbbb$	21	37692724

The presentations in Table 1 should be considered in the context of the following three results about relator amalgamation which appear in [4] with proofs and various applications. These results enable us to build efficient presentations for covering groups from deficiency-one presentations for related groups.

Theorem 3.1. *Let G be a finite simple group. Suppose that G, or some stem extension of G, can be presented by*

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

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

Corollary 3.2. *Let G be a finite simple group. Suppose that G, or some stem extension of G, can be presented by*

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

Suppose also that $u(a,b)$ and $v(a,b)$ generate the free group on a and b. Then the covering group of G, all stem extensions of G, and G itself, are efficient.

Theorem 3.3. *Let G be a finite simple group. Suppose that G, or some stem extension of G, can be presented by*

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

In addition, suppose the group $\widetilde{G}$ presented by

$$\left\{a, b \mid u(a,b)^{kp} v(a,b)^{lq} = w(a,b) = 1\right\}$$

is perfect, and is generated by $u(a,b)$ and $v(a,b)$. Then $\widetilde{G}$ is the covering group of G.

Presentation P_1, which is the shortest canonical presentation for $\widehat{M}_{22}$, can be obtained by amalgamating the power relations in a variant of P_{10}. (We use a variant because we have different rules for producing canonical forms for presentations on different generating sets and varying numbers of relators.) Likewise P_2 comes from P_3, while P_4 comes from P_5, and P_6 comes from P_7, and P_8 comes from (a variant of) P_{17}. In a similar way, P_{16} is the result of amalgamating relators in a one-relator quotient of $C_3 * C_5$ with length 22. Notice that relator amalgamation here makes coset enumerations about twice as hard.

The two 3-generator presentations P_{11} and P_{12} can be converted to variants of P_1 by eliminating b from P_{11} and a from P_{12} using the short relator. Applying the reverse operation, by adding a generator to our 2-generator presentation for M_{22} with length 44 (which is a quotient of P_1), yields shorter 3-generator presentations, of length 38. An example is

$$\{a, b, c \mid cba, aaCbAc, abbbCBaB, abcBAcBAbbcabbcabbcAC\}$$

which enumerates quite nicely, using a total of 458114 cosets.

3.2. Method 2.

Our second method revealed 104037 representative generating sets for M_{22}. We investigated about 3000 of these and found the seven 2-generator, 3-relator presentations for M_{22} given in Table 2. These present the simple group itself, and not its cover or any other stem extension. We give the presentations as produced by Magma without modification. We list the presentations in order of discovery (which is somewhat arbitrary) but do not analyze them individually in detail.

3.3. Method 3.

Our third method enables us to look at longer one-relator quotients of $C_m * C_n$ than we can readily handle with the census based approach of Method 1. Indeed

Table 2: M_{22} from Method 2

No.	Relators	Length	Total cosets
1	$BAbABBAABBBABAB, BABBabbaabbabAba,$ $abAbabbaaBAbabAB$	47	13364969
2	$a^{11}, aBaBaaaaBabAAb, AbbAAAAABAbaBaB$	40	21880459
3	$ABBBABABaaBB, AABaBAABABBab,$ $bAAbABAABABabaa$	40	2697010
4	$b^5, AbbAbAAABBABAbb, aBabbAAAbaBBaBB$	35	9346952
5	$AAABaaaBABaB, babaBaaababbab,$ $BAbABAAABBabABA$	41	13205478
6	$(Ba)^5, bAbbaaabbaBA, AAABaaaaBaaaaBA$	37	39388893
7	$BabAbbaababABa, BabaabaaBabAbA,$ $AbabABAABBabAAB$	43	1770844

it revealed variants of presentations found using Method 1. (Again we obtained variants because of different canonical orderings used.)

From the representative sets constructed by Method 2, we determined that a complete list of possible ordered pairs (m, n) for use with Method 3 is: $(2, 5)$, $(2, 7)$, $(2, 11)$, $(3, 5)$, $(3, 7)$, $(3, 8)$, $(3, 11)$, $(4, 5)$, $(4, 7)$, $(4, 11)$, $(5, 6)$, $(5, 7)$, $(5, 8)$, $(5, 11)$, $(6, 7)$, $(6, 11)$, $(7, 8)$, $(7, 11)$, $(8, 11)$. Indeed we applied Method 3 for each of these pairs, hoping to find a one-relator quotient of $C_m * C_n$ which presents M_{22} rather than its cover, but so far without success.

Even though this method has not yet given us what we sought here (the problem to which it was first applied), it has been used elsewhere with excellent outcomes. In [4] efficient presentations for many simple groups have been found as one-relator quotients of $C_m * C_n$, including the smaller Mathieu groups M_{11} and M_{12}.

3.4. Nice central elements.

It has already been observed [4] that many nice deficiency-zero presentations for covering groups of simple groups can be viewed as resulting from Theorem 3.3. Motivated by this and by our first presentation for M_{22}, we continued by investigating such presentations for $\widehat{M}_{22}$ revealed by Methods 1 and 3. In particular, we looked for nice central elements of order 12 in $\widehat{M}_{22}$.

For $\langle P_4 \rangle$ we find that $(aaB)^7$ is a central element of order 12 which gives as a presentation for M_{22} the following:

$$\{a, b \mid a^5 b^3, aabABababAB, (aaB)^7\}.$$

This presentation has nice structure, with orders of a, b and aaB easy to see. Successful coset enumeration over the trivial subgroup uses a modest 777798 cosets. Introducing new generators $x = aaB$ and $y = a$ gives the following shorter presentation:

$$\{x, y \mid x^7, yyXYxyXyyyXYx, y^5(Xyy)^3\}.$$

Its length is 34 (six letters shorter), but coset enumeration over the trivial subgroup is harder, using 1147382 cosets.

Finally, for $\langle P_8 \rangle$ we find that b^{11} is a central element of order 12 which gives the following as a presentation for M_{22}:

$$\{a, b \mid aaaabAbAb, aabABabbAB, b^{11}\}.$$

This presentation too has very nice structure, with orders of a, b and aB easy to see. Successful coset enumeration over the trivial subgroup uses 2104858 cosets. This is the canonical version of the shortest presentation for M_{22} we have found, with length 30.

4. Review

We have shown how to find very many efficient presentations for M_{22}. These include a reasonably short one (simply constructed from the unique shortest canonical presentation for its cover) which has length 44 and which allows quite easy enumeration of cosets. We also have a shorter presentation, with length 30, which has nice structure but which is somewhat worse for coset enumeration. For $\widehat{M}_{22}$ we have various presentations as one-relator quotients of the free product of two cyclic groups; these have appropriate structure to give efficient presentations for M_{22} and all of its stem extensions.

The following questions arise. What is a shortest efficient presentation for M_{22}? (Even though we do not know the answer to this question, we do know the answer for $\widehat{M}_{22}$, a much larger group.) Does M_{22} have efficient presentations that are one-relator quotients of the free product of two cyclic groups? (Again, we do know the answer for $\widehat{M}_{22}$.)

Acknowledgements

The first author was partially supported by the New Zealand Marsden Fund (grant no. UOA124). The second and third authors were partially supported by the Australian Research Council.

References

[1] A.G. bin Ahmad, The unsolvability of efficiency for groups, *Southeast Asian Math. Bull.* **22** (1998), 331–336.

[2] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: the user language, *J. Symbolic Comput.* **24** (1997) 235–265.
See also `http://magma.maths.usyd.edu.au/magma/`

[3] C.M. Campbell, G. Havas, J.A. Hulpke and E.F. Robertson, Efficient simple groups, *Comm. Algebra* **31** (2003) 5191–5197.

[4] C.M. Campbell, G. Havas, C. Ramsay and E.F. Robertson, Nice efficient presentations for all small simple groups and their covers, *LMS J. Comput. Math.* **7** (2004) 266–283.

[5] C.M. Campbell, E.F. Robertson and P.D. Williams, Efficient presentations for finite simple groups and related groups, in *Groups-Korea 1988*, Lecture Notes in Mathematics **1398**, Springer-Verlag, New York (1989), 65–72.

[6] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version* 4.4, 2004; `http://www.gap-system.org/`

[7] G. Havas, M.F. Newman and E.A. O'Brien, On the efficiency of some finite groups, *Comm. Algebra* **32** (2004) 649–656.

[8] G. Havas and C. Ramsay, *Coset enumeration: ACE version 3.001*, 2001; `http://www.itee.uq.edu.au/~havas/ace3001.tar.gz`

[9] G. Havas and C. Ramsay, Short balanced presentations of perfect groups, in *Groups St Andrews 2001 in Oxford, Volume 1*, London Mathematical Society Lecture Note Series **304** (Cambridge University Press, Cambridge, 2003) 238–243.

[10] J. Howie, V. Metaftsis and R.M. Thomas, Finite generalized triangle groups, *Trans. Amer. Math. Soc.* **347** (1995), 3613–3623.

[11] A. Jamali and E.F. Robertson, Efficient presentations for certain simple groups, *Comm. Algebra* **17** (1989) 2521–2528.

[12] M.A. Kervaire, Multiplicateurs de Schur et K-théorie (French), in *Essays on Topology and Related Topics (Mémoires dédiés à Georges de Rham)*, Springer-Verlag, New York (1970), 212–225.

[13] L. Lévai, G. Rosenberger and B. Souvignier, All finite generalized triangle groups, *Trans. Amer. Math. Soc.* **347** (1995), 3625–3627.

[14] J. Wiegold, The Schur multiplier: an elementary approach, in *Groups – St Andrews 1981*, London Mathematical Society Lecture Note Series **71** (Cambridge University Press, Cambridge, 1982) 137–154.

Marston Conder, Department of Mathematics, University of Auckland, Private Bag 92019, Auckland, New Zealand

Email: m.conder@auckland.ac.nz

George Havas, ARC Centre for Complex Systems, School of Information Technology and Electrical Engineering, The University of Queensland, Queensland 4072, Australia

Email: havas@itee.uq.edu.au

Colin Ramsay, ARC Centre for Complex Systems, School of Information Technology and Electrical Engineering, The University of Queensland, Queensland 4072, Australia

Email: cram@itee.uq.edu.au