On one-relator quotients of the modular group

Marston Conder[*], George Havas[†] and M.F. Newman[§]

[*]Department of Mathematics, University of Auckland,
Private Bag 92019, Auckland, New Zealand
Email: m.conder@auckland.ac.nz

[†]Centre for Discrete Mathematics and Computing,
School of Information Technology and Electrical Engineering,
The University of Queensland, Queensland 4072, Australia
Email: havas@itee.uq.edu.au

[§]Mathematical Sciences Institute,
Australian National University, Canberra 0200, Australia
Email: newman@maths.anu.edu.au

Abstract

We investigate the modular group as a finitely presented group. It has a large collection of interesting quotients. In 1987 Conder substantially identified the one-relator quotients of the modular group which are defined using representatives of the 300 inequivalent extra relators with length up to 24. We study all such quotients where the extra relator has length up to 36. Up to equivalence, there are 8296 more presentations. We confirm Conder's results and we determine the order of all except five of the quotients. Once we find the order of a finite quotient it is easy to determine detailed structural information about the group. The presentations of the groups whose order we have not been able to determine provide interesting challenge problems.

Our study of one-relator quotients of the modular group is 'in the small', that is, with a short extra relator. We briefly compare and contrast our results with generic results.

1 Introduction

The modular group is a much studied object in mathematics. Indeed in the documentation for the award of the 2009 Abel Prize to Mikhail Gromov, this group is described as "one of the most important groups in the modern history of mathematics". It is perhaps best known as the projective special linear group $L_2(\mathbb{Z})$, with a standard representation as a group of linear fractional transformations. It has a large collection of interesting quotients, including most of the nonabelian finite simple groups.

We study the modular group as a finitely presented group. It is isomorphic to the free product of the cyclic groups C_2 and C_3, which gives its natural and shortest presentation: $\{x, y \mid x^2, y^3\}$. We investigate the question: what are the one-relator quotients of this group? In other words, which groups can we obtain by adding one extra relator $w(x, y)$ to the standard presentation?

The theory of Schur multipliers gives a necessary condition for a finite $\{2,3\}$-generated group to be presentable as a one-relator quotient of the modular group. For a finite group G, the group H is said to be a *stem extension* of G if there exists $A \leq Z(H) \cap H'$ with $G \cong H/A$. A stem extension of maximal order is called a *covering group* of G, and the group A in the maximal case is the *Schur multiplier* of G. This depends only on G, and is denoted by $M(G)$. The *deficiency* of a finite presentation $\{X \mid R\}$ of G is $|R| - |X|$. The deficiency of G, denoted by $\operatorname{def}(G)$, is the minimum of the deficiencies of all finite presentations of G. For a good overview of Schur multipliers and related topics see [41], where Corollary 1.2 shows that $\operatorname{rank}(M(G))$ is a lower bound for $\operatorname{def}(G)$. The group G is said to be *efficient* when this lower bound is achieved. It follows that a finite $\{2,3\}$-generated group is not presentable as a one-relator quotient of the modular group unless $M(G)$ has rank 0 or 1.

One-relator quotients of the modular group have been much considered over time. As long ago as 1856 Hamilton [18] produced what we can read as a presentation for A_5 (which he called "Icosian Calculus") via a one-relator quotient of the modular group. In 1901 G.A. Miller [33] identified the triangle groups $\langle x, y \mid x^2, y^3, (xy)^n \rangle$ for $n = 2, 3, 4$ and 5, and in 1902 he showed [34] that they are infinite for $n > 5$.

In 1987 Conder [11] substantially identified all one-relator quotients of the modular group defined using extra relators with length up to 24. There are 71 isomorphism types among those quotients which come from 300 inequivalent presentations. (Subsequently Ulutaş and Cangül wrote a paper on this topic [40], but sadly their work is neither comprehensive nor fully correct.) Importantly, many successful investigations into efficient presentations for simple groups have specifically studied one-relator quotients of the modular group, including [8, 9, 10, 30, 28, 4, 5, 6]. The groups $L_2(p)$ are presentable as one-relator quotients of the modular group for all primes p.

To better understand the nature of one-relator quotients of the modular group, we extend Conder's 1987 work by investigating longer presentations. We describe a canonical form for these presentations. In that context, we study all such quotients with extra relator having length up to 36, and determine the order of almost all of them. When we can determine the order of a finite group, we are able to give detailed structural information about it.

Most of our results are based on computer calculations, which are sometimes substantial. We mainly use Magma [3], which provides excellent facilities for our needs. (Alternatively GAP [17] can be used to do the required computations.) We provide supplementary materials, including some Magma programs on a website [13], together with their outputs. These programs and outputs give further details on our calculations and also provide information on computer resource usage.

2 Conder's approach revisited

In [11] Conder was motivated by a problem about graph embeddings to study what he called at the time "three-relator quotients of the modular group". We now prefer the term *one-relator*, reflecting the count of extra relators, rather than the total relator count.

Following the ideas but not the detail of [11], we define the modular group $\Gamma = \langle x, y \mid x^2, y^3 \rangle$ and consider its one-relator quotient $G = \langle x, y \mid x^2, y^3, w(x, y) \rangle$. Any non-trivial element (other than x, y or y^{-1}) in Γ is conjugate to an element of the form $xy^{\epsilon_1}xy^{\epsilon_2} \dots xy^{\epsilon_n}$ where $\epsilon_i = \pm 1$, which has n syllables and length $2n$.

We consider such elements as candidates for the extra relator. There are 2^n of these, for n syllables. We can reduce the number we look at, however, by utilising automorphisms of the modular group, as described in [11].

We define $u = xy$ and $v = xy^{-1}$. Then $u^{-1}v = y^{-1}x^{-1}xy^{-1} = y^{-2} = y$ and $vu^{-1}v = xy^{-1}y = x$, so Γ has alternative presentation $\{u, v \mid (vu^{-1}v)^2, (u^{-1}v)^3\}$, which we call P. This presentation is more convenient for describing canonical representatives for the extra relator.

There is an automorphism of Γ which inverts each of x and y, and hence interchanges u and v. The resulting extension of Γ is the extended modular group, and is isomorphic to $PGL_2(\mathbb{Z})$. When enumerating inequivalent presentations obtained by adding a relator $r(u, v)$ to P, then r is a positive word and we may assume that u occurs at least as often as v in r. Moreover, by conjugation, we may select the alphabetically earliest rotation of the relator. So our relator begins with u and the number of occurrences of u at the beginning of the relator, before v occurs (if at all), is equal to the maximum length of strings of consecutive appearances of the letter u in any conjugate of the relator. Also, if necessary, we may invert any third relator and then conjugate it by x, noting that $xu^{-1}x = xy^{-1}x^{-1}x = xy^{-1} = v$ (and $xv^{-1}x = xyx^{-1}x = xy = u$), in order to obtain an equivalent choice.

These observations make it quite easy to produce a comprehensive list of presentations. Each relator we need to consider is a reduced word in u and v, and two such words are equivalent if one can be obtained from the other by cyclic permutation, reflection, or complementation (swapping u and v). Hence the number of n-syllable relators is equal to the number of n-bead necklaces, where each bead is one of two colours, turning over is allowed, and complements are equivalent. In particular, for syllable counts from 1 to 18 we obtain (in order) 1, 2, 2, 4, 4, 8, 9, 18, 23, 44, 63, 122, 190, 362, 612, 1162, 2056 and 3914 relators, matching the necklace count in [39]. This also gives a formula for counting the number of n-syllable relators:

$$\left(\sum_{d|n} \left(2^{n/d} \varphi(2d)/(2n) \right) + 2^{[n/2]} \right) /2$$

where ϕ is the Euler phi function. The dominant term is $2^{n-2}/n$.

3 Our methods and the easy cases

We have developed a Magma program [13, `mqEasy.m`] which generates canonical representatives of extra relators with from 3 to 18 syllables, and tries to determine the order of the groups they define, using coset enumeration.

The most common form of proofs of finiteness based on coset enumeration rely on showing that a provably finite subgroup has finite index in the group. Coset enumeration based procedures in Magma have a very rich range of parameters. Selection methods to find good parameters are discussed in [23]. The parameters we choose for most coset enumerations are `Hard:=true` and `Mendelsohn:=true`.

The most common form of proofs of *infiniteness* based on coset enumeration rely on showing that a subgroup (with finite index) has infinite abelianisation.

We start by using coset enumeration over the trivial subgroup, allowing a maximum of 10^6 cosets. If that fails, we look for subgroups with index up to 33 (in principle) and with infinite abelianisation. In fact, because the triangle groups with extra relator $(xy)^n$ and the generalised triangle groups with extra relator $(xyxy^{-1})^n$ have very many subgroups with index up to 33, in those cases we reduce the index limits to lower numbers that suffice.

The three presentations with extra relator having less than three syllables define finite groups. For extra relator with from 3 to 18 syllables, the output `mqEasy.l` shows that 8336 presentations define groups with explicit finite order, while 191 define infinite groups. This leaves 66 groups with order to be determined, out of an initial total count of 8596.

A somewhat modified program, which allows the definition of up to 10^7 cosets and looks at subgroups with index up to 42, reduces the number of outstanding cases to 48; see [13, `mqEasy2.l`]. We find 11 more finite groups, and 7 infinite ones. It is interesting to note that the two largest indexes are found with quite easy coset enumerations, while some small index cases are quite difficult.

4 Commentary on the easy cases

Even though the methodology used thus far is both standard and relatively naive, it has proved to be very successful in determining the group order and even in addressing the isomorphism problem in most cases. We progressively refine the techniques to address the harder problems.

For example, choosing the trivial group as subgroup over which to attempt coset enumeration to prove finiteness is by no means the best way to proceed. It has one implicit advantage, however, namely that when the enumeration succeeds, we get a regular representation for the group. Given a representation for a permutation group of moderate size, it is straightforward to test its isomorphism with any group for which we have a permutation representation. This means we have an implicit solution for the isomorphism problem among these finite quotients. It is also easy to study group structure, as we demonstrate below for the two largest finite groups whose order is revealed above. For the infinite groups, the information revealed about subgroups and sections by the Low Index Subgroups algorithm enables us to divide them into collections of distinct isomorphism types.

Previous work has found infinite families of presentations giving different groups. There are one-parameter families defining an infinite number of different infinite groups, the earliest revealed being the triangle groups [34]. The generalised triangle groups [2], with extra relator w^n for $n > 1$ and w an "interesting" word, are another such family. The simple groups $L_2(p)$ for all prime $p \geq 5$ with extra relator

$$u^2vu^{(p-3)/2}vu^2vu^{(3p-3)/2}v$$

are revealed by [8]. An infinite collection of different finite soluble groups with extra relator

$$xy^{-1}xy(xyxy^{-1})^{n-1}xy^{-1}xy$$

is given by [7].

Analysis of our output thus far reveals (inter alia) that we have the following counts: trivial group, 1856 presentations; C_2, 2183; C_3, 681; C_6, 134; and S_3, 799. The largest two finite groups revealed easily have orders 2 359 296 and 8 491 392. By applying the Magma commands `DegreeReduction` and then `NormalSubgroups` to the regular representations for these two large groups, we can find all normal subgroups, indicating that we can do this for all of the finite groups whose orders are easily found. (The degree reduction step is used to make the normal subgroup construction run much more quickly and use less memory.)

By investigating the quotients with the relevant orders, we observe the following counts for presentations of small simple groups: A_5, 43 presentations; $L_2(7)$, 14; $L_2(8)$, 10; $L_2(11)$, 4; $L_2(13)$, 8; $L_2(17)$, 9; $L_2(19)$, 4; and $L_2(16)$, 3. (In two cases some quotients with the relevant orders are not simple; there are in total 53 presentations defining groups with order 168 and 26 with order 504.)

The smallest $\{2,3\}$-generated simple group which does not occur in our list is $L_3(3)$, which has order 5616. Its shortest presentations as a one-relator quotient of the modular group require (extra relators with) 21 syllables. Also missing is $L_2(29)$, having order 12180, whose shortest presentations require 19 syllables. In contrast, both $L_2(31)$, with order 14880 and three presentations, and $L_2(43)$, with order 39732 and one presentation, do appear, with 17 syllables. Note that the presentation based on [8] listed above for $L_2(43)$ has 91 syllables (the general presentation for $L_2(p)$ uses $2p+5$ syllables).

We have already seen one-parameter infinite families of presentations that define an infinite number of different groups. It is also easy to demonstrate infinite families of distinct presentations for the same group.

Theorem 4.1 *For each $n \geq 0$, the presentation $\{u, v \mid (vu^{-1}v)^2, (u^{-1}v)^3, u^n v^{n+1}\}$ defines the trivial group.*

Proof Since $u^n v^{n+1} = 1$, the element $z = u^n = v^{-(n+1)}$ is central. Conjugating by x gives $u^n = z = z^x = (v^{-(n+1)})^x = u^{n+1}$, so $u = 1$, and the result follows. □

Theorem 4.2 *For each $n > 0$, the presentation $\{u, v \mid (vu^{-1}v)^2, (u^{-1}v)^3, u^n v\}$ defines the cyclic group C_m, where $m = \gcd(n-1, 6)$.*

Proof Since $v = u^{-n}$, the group is cyclic, and hence abelian. The first two relations give $u^2 = v^4$ and $u^3 = v^3$, from which it follows easily that $v = u^{-1}$ and $u^6 = 1$. The third relation implies also $u^{n-1} = 1$, so the group has order $\gcd(n-1, 6)$. □

The two families above are special cases of the more general two-parameter family of groups with presentation $P_{n,k} = \{u, v \mid (vu^{-1}v)^2, (u^{-1}v)^3, u^n v^k\}$. Note that here the element $u^n = v^{-k}$ is central, so $P_{n,k}$ is a central extension of

$$(2,3 \mid n,k) = \langle\, r, s \mid r^2, s^3, (rs)^n, (r^{-1}s)^k \,\rangle,$$

which is a member of the family of groups $(\ell, m \mid n, k)$ studied by Coxeter [14]. Indeed, $(2,3 \mid n,k) \cong \langle\, r,s \mid r^2, s^3, (rs)^d \,\rangle$, which is the $(2,3,d)$ triangle group, for $d = \gcd(n,k)$. By thinking of $P_{n,k}$ defined in terms of x and y we can see that for $d = 1$ (when the triangle group is trivial), the central extension $P_{n,k}$ is perfect and so defines the trivial group if and only if $\gcd(n+k, 6) = 1$. For other $d \leq 5$, $P_{n,k}$ defines a finite nontrivial group; and for $d > 5$ it defines an infinite group. Instances of other infinite families of presentations which define the trivial group can be observed in `mqEasy.l`.

One-relator quotients of the modular group that are trivial lead to balanced presentations of the trivial group, and infinite families give rise to infinite families of balanced presentations. By taking any presentation from one of these families, we can construct central extensions by amalgamating the relators x^2 and y^3.

In the case arising from Theorem 4.1, we may take $\{x, y \mid x^2y^3, (xy)^n(xy^{-1})^{n+1}\}$ and change any selection of $n+1$ instances of x in the second relator into x^{-1}. Then the central extension is perfect, and hence trivial. Each such presentation thus gives $\binom{2n+1}{n+1}$ 'different' presentations of the trivial group. In the case of Theorem 4.2, the group is trivial when $n \equiv 0$ or $2 \bmod 6$, and so we consider $\{x, y \mid x^2y^3, (xy)^n xy^{-1}\}$. Here, if $n \equiv 0 \bmod 6$ then we may change any $n/3$ instances of y to y^{-2} and any $n/2+1$ instances of x into x^{-1}, and obtain $\binom{n+1}{n/3}\binom{n+1}{n/2+1}$ presentations of the trivial group. On the other hand, if $n \equiv 2 \bmod 6$, we may change any $(n-2)/3$ instances of y to y^{-2} and any $n/2$ instances of x to x^{-1}, and obtain $\binom{n+1}{(n-2)/3}\binom{n+1}{n/2}$ presentations. Similar results hold for other one-relator quotients defining the trivial group.

Such one-relator quotients of the modular group can provide balanced presentations of the trivial group in numbers that are exponential in the presentation length. These presentations (and variants based on presentations explicitly in terms of u and v instead of x and y) provide interesting candidates for counterexamples to the Andrews-Curtis conjecture. Indeed, the examples from Theorem 4.1 correspond to variants of a family introduced by Akbulut and Kirby [1]. Other examples, coming from trivial groups with extra relator of the form u^nv^k, seem to be new.

5 Harder presentations

Only 48 presentations remain, as recorded in [13, `last48.m`]. Here we list their extra relators in the order generated by our program, and we number them for convenient reference.

1: $(u^3vuv^2)^2$, 2: $(u^2vuv)^3$, 3: $(u^5vuv)^2$,
4: $(u^5v^3)^2$, 5: $(u^4vu^2v)^2$, 6: $u^3vu^3vu^3v^2uv^2$,
7: $u^3vu^3vu^2v^3u^2v$, 8: $u^3vu^3v^2uv^3uv^2$, 9: $(u^3vu^2v^2)^2$,
10: $(u^3v^2uv^2)^2$, 11: $(u^2vu^2vuv)^2$, 12: $u^{10}uv^2uvuv^2$,
13: $u^8v^2uvuvuv^2$, 14: $u^8vuvuv^2u^2v^2$, 15: $(u^6vuv)^2$,
16: $u^6vuv^6u^2v^2$, 17: $(u^5vu^2v)^2$, 18: $u^5vu^2v^2uv^5uv$,
19: $u^5vuvuvuv^5uv$, 20: u^5vuvuv^5uvuv, 21: $u^5v^2u^2v^5u^2v^2$,
22: $u^4vu^3v^3uv^4uv$, 23: $u^4vu^2vuvuv^2uv^4$, 24: $u^4vu^2vuv^2uv^4uv$,
25: $u^4vu^2vuv^4uv^2uv$, 26: $u^4vu^2v^2uv^4uvuv$, 27: $u^4vuvu^2v^2uvuv^4$,
28: $u^4vuvuvuv^4u^2v^2$, 29: $u^4vuvuv^4u^3v^3$, 30: $u^4vuv^2u^2vuv^4uv$,

31: $u^4vuv^4u^3vuv^3$, 32: $u^4vuv^4uvu^4v^2$, 33: $u^4v^2u^2v^4u^2vuv^2$,
34: $(u^4v^2uv^2)^2$, 35: $u^4v^2uv^2u^2vu^2v^4$, 36: $u^4v^3uvuvu^3v^4$,
37: $u^3vu^2vu^2v^2uv^2uv^3$, 38: $u^3vu^2vuv^2uv^3u^2v^2$, 39: $u^3vu^2vuv^2uv^3uvuv$,
40: $u^3vu^2v^2uv^3u^2vuv^2$, 41: $u^3vu^2v^3u^3v^2uv^3$, 42: $u^3vuvu^3v^3uvuv^3$,
43: $u^3vuvuv^3u^2vuvuv^2$, 44: $u^3vuv^3u^2vuvuvuv^2$, 45: $u^3vuv^3u^2v^3u^3v^2$,
46: $u^3v^2u^2vuvuv^2u^2v^3$, 47: $u^3v^2uvu^2v^3u^2vuv^2$, 48: $(u^2vuvu^2v^2)^2$.

We will use Q_i to refer to the one-relator quotient of the modular group satisfying the i^{th} relator in the above list. A quick perusal of the list reveals that 12 presentations are for generalised triangle groups, namely Q_1 to Q_5, Q_9 to Q_{11}, Q_{15}, Q_{17}, Q_{34} and Q_{48}. The order question has been resolved for all generalised triangle groups; see [2, 27, 32]. Nevertheless, we continue with our computational investigation of all these 48 presentations.

In our first attack on this collection of presentations, we applied our programs to the presentation of the group G on the initial generators x and y. This is good for the Low Index Subgroups implementation, as the presentation includes the order of the generators, but is not so good for standard coset enumeration; the presentation on generators u and v is better for Todd Coxeter enumerations because it is shorter.

We first attempted to prove infiniteness (as our methods of proving finiteness can waste resources if applied to infinite groups), by investigating subgroups and quotients more carefully. Specifically (see `last48.l`), we looked at subgroups with index up to 42, the permutation representations afforded by their coset tables, and the abelian quotient invariants of both the subgroups and their cores (in cases where the core had index less than 2^{16}).

We found 11 more quotients that are infinite because they have subgroups with infinite cores, namely Q_2, Q_4, Q_9, Q_{11}, Q_{13}, Q_{21}, Q_{28}, Q_{30}, Q_{32}, Q_{41} and Q_{48}. In some other cases, we found very large abelianised cores and quotients which suggested that the groups may well be infinite. Also some groups are revealed to have quotients $L_2(p)$ for multiple values of p. They are Q_3, Q_4, Q_5, Q_{11}, Q_{15}, Q_{17}, Q_{20}, Q_{25}, Q_{34}, Q_{42} and Q_{47}, but of these, only Q_4 and Q_{11} were proved infinite using the approach described above.

Various methods have been developed recently for finding homomorphisms from finitely presented groups onto finite groups. Work by Plesken and Fabianska [35] has culminated in an algorithm that finds all quotients of a finitely presented group which are isomorphic to $L_2(p^n)$. We have used an implementation of this algorithm due to Fabianska [16], and applied it to the groups listed above that have multiple $L_2(p)$ quotients. This reveals that all 11 of those groups have L_2-quotients for infinitely many primes, and leaves 28 presentations to consider. Release V2.16 of MAGMA includes an implementation of the Plesken-Fabianska methods, which enables easy verification of infiniteness. Using [13, `PF48.m`] for the last 48 presentations, we can determine whether each group has infinitely many L_2 quotients in less than 5 cpu seconds (and about 9MB of memory for all of them).

Initially we used coset enumerations over the trivial subgroup to prove finiteness, which gives the group order directly and also gives a regular representation for the group. To just prove finiteness, we can do better by using a theorem of Schur on centre-by-finite groups [36, 10.1.4], which leads to the following known result.

Proposition 5.1 *A group is finite if its largest metabelian quotient is finite and it has a cyclic subgroup with finite index.*

This enables us to consider using larger cyclic subgroups in coset enumerations to reduce the hypothetical index, which leads to easier coset enumerations.

For each of our remaining 28 groups, the largest metabelian quotient is finite (since we know that all subgroups with index up to 6 have finite abelianisations). We do not know a priori the orders of u and v (which are equal since $u^x = v^{-1}$), but we can perform coset enumerations over the subgroup generated by either of them. Somewhat arbitrarily, we may choose v and try to enumerate the cosets of $\langle v\rangle$ in G, with the same maximum coset limit, namely 10^7. Using [13, `last28.m`] we thus discovered 13 more finite groups: Q_6 in which $\langle v\rangle$ has index 292032; Q_7 index 78624; Q_8 110592; Q_{10} 3 538 944; Q_{16} 4; Q_{19} 172032; Q_{26} 1; Q_{29} 13; Q_{36} 367416; Q_{39} 1 572 864; Q_{44} 403368; Q_{45} 87500; and Q_{46} 5 308 416.

These groups are all finite and, given this knowledge, it is not too hard to determine their orders. The generalised triangle group Q_{10}, for example, is identified in [31] as a group with order $2^{20}3^4 5 = 424\,673\,280$. The larger indexes here are for groups which are clearly out of range of our previous finiteness proof attempts. By modifying our program to allow the definition of 10^8 cosets [13, `last15.m`], we found three more finite groups: Q_{23}, in which $\langle v\rangle$ has index 746928; Q_{35}, index 31; and Q_{38}, 712500. This leaves 12 presentations (including just one generalised triangle group, namely Q_1) to be resolved.

The standalone coset enumerator ACE3 [24] allows the definition of more than 2×10^9 cosets (avoiding limits in the Magma implementation prior to Release V2.16). Using ACE3 we found that $\langle v\rangle$ has index 63 824 112 in Q_{18} and index 36 in Q_{24}. (Both of these enumerations can now be done via both Magma and GAP.) The best enumeration we have found for $\langle v\rangle$ in Q_{18} uses a maximum of 309 366 526 and a total of 311 338 810 cosets, while the best for Q_{24} uses a maximum of 948 327 123 and a total of 953 684 712. These are very hard enumerations, but note that Q_{24} is handled much more efficiently in Section 7.2.

When the index of $\langle v\rangle$ is moderate we can determine the structure of the group reasonably easily. The index 63 824 112 in Q_{18} is more challenging. We describe the structure of the group in Section 6.

For the 10 remaining presentations, perusal of the subgroup, quotient and section structure (using [13, `last48.m`]) reveals that two of these are certainly very large.

The group Q_1 has sections (indeed cores with abelian quotient invariants) of orders $2^7 \times 6$, $5^6 \times 15$ and $3^7 \times 9$. So far, our computational approach has not succeeded in proving Q_1 to be infinite, but a proof is given in [31], which uses a cleverly constructed 3×3 matrix representation for its derived group.

The group Q_{14} has sections of orders $2^6 \times 8^2$, 3^9 and 2×4^8. Our computational approach has not succeeded in proving Q_{14} to be infinite, but we can give an alternative proof. Conder [12] previously studied a group related to trivalent symmetric graphs, which produced the following two-relator quotient of the modular group as a subgroup of index 8 in a C_2 extension of $L_3(\mathbb{Z})$.

Proposition 5.2 [12, Corollary 2] *The group below is infinite and insoluble:*

$$\langle x, y \mid x^2 = y^3 = (xy)^{12} = (xy^{-1}xy^{-1}xyxyxy^{-1}xy)^2 = 1\rangle.$$

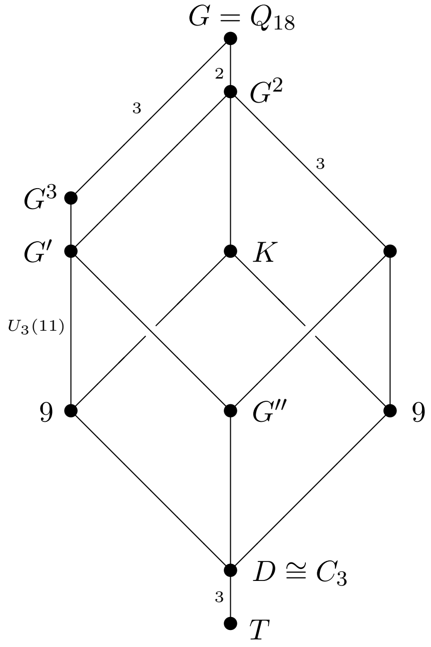
Since $(xy)^8 = (xy)^{-4}$ in this group, it is easy to see that it is a quotient of Q_{14}, and hence Q_{14} is infinite. (Alternatively, information in [12] enables us to build an 8×8 matrix representation for Q_{14}, which directly demonstrates that it is infinite.)

That leaves 8 presentations, which we discuss in Section 7. This was the status of the problem up to June 2009. At that time we had alternative proofs in some cases, but here we have given proofs that so far are primarily based on coset enumeration.

6 A large finite group

In Section 5 we revealed that $\langle v\rangle$ has index 63 824 112 in Q_{18}. This index is so large that it is harder to determine structural information about the group. We do so in some detail here. Let $G = Q_{18}$. It is easy to see that the second derived group G'' has index 18 and is perfect. The quotient G/G'' is $S_3 \times C_3$.

Noting that $63\,824\,112 = 2^4 3^4 11^3 37$ bears much in common with $|U_3(11)| = 2^5.3^2.5.11^3.37$, we investigate whether $U_3(11)$ is a section of Q_{18}. The group of squares G^2 has index 2 and the Magma command `Homomorphisms` reveals that $U_3(11)$ is an image of G^2. We can continue to use Magma to discover more. The figure below shows the part of the normal subgroup lattice of Q_{18} that we reveal.



Let K be the kernel of a homomorphism from G^2 to $U_3(11)$. (There are six homomorphisms but only one kernel.) Let D be $K \cap G''$. The quotient G^2/D is $U_3(11) \times {C_3}^2$. Hence the order of G/D is $1\,276\,482\,240 = 2^6.3^4.5.11^3.37$.

The order of $\langle u \rangle$ modulo D is 60. Let T be $\langle u^{60} \rangle$. Then the index of T in G is $60 \times 63\,824\,112 = 3\,829\,446\,720$.

We now show that T is trivial. We know that T lies in D and has index 3 in D. Let S be the core of T in G. Then S is cyclic and D/S is C_3 or S_3. We can rule out S_3 by contradiction. Assume $D/S \cong S_3$. Then D has a subgroup R with index 2 and D/R is central in G/R. Since the Schur multiplier of $U_3(11)$ has order 3, the quotient G''/R is isomorphic to $U_3(11) \times C_2$. This contradicts the fact that G'' is perfect. Hence $T = S$ and is normal in G. It follows that T is central in G' and so D is abelian. Therefore G''/D^3 is a stem extension of G''/D. Hence D/D^3 is cyclic and D is cyclic. Hence G'' is a stem extension of G''/D and D has order 3. Therefore the order of G is $3\,829\,446\,720 = 2^6.3^5.5.11^3.37$.

Having found that Q_{18} has $U_3(11)$ as a section enables us to construct nice presentations for $U_3(11)$ in various ways. Those will be given in another paper.

7 The last eight

7.1 17 syllables

The group Q_{12} with additional relator $u^{10}v^2uvuv^2$ is the only one with extra relator having less than 18 syllables that was not resolved above. The output `last48.l` shows that the group has quotients $L_2(25)$ and ${C_2}^{12}.L_3(3)$. Holt and Rees [26] revealed these quotients (inter alia) in the group $(2,3,13;4)$, which is a member of another family of groups defined by Coxeter [14], namely

$$(\ell, m, n; q) = \langle r, s \mid r^\ell, s^m, (rs)^n, [r,s]^q \rangle.$$

This observation leads us to note that Q_{12} is isomorphic to

$$H = \langle\, c, d \mid c^2, d^3, (cd)^{13}[c,d]^{-4} \,\rangle$$

which is a central extension of $(2,3,13;4)$. So, to determine the structure of Q_{12}, we need to understand $G = (2,3,13;4)$.

Coxeter's families of groups have been much studied since his paper was published in 1939. A recent paper by Edjvet and Juhàsz [15] provides a good overview of the history of investigations into them. Suffice it to say, the order problem for G was unresolved as at the middle of 2009.

Motivated by our investigation here, Havas and Holt [19] decided to look at G again, and succeeded in proving that it is finite with order 358 848 921 600. The proof relies on coset enumeration, like our finiteness proofs here, but with careful cyclic subgroup selection to take advantage of a generator with as large order as possible. Havas and Holt also comprehensively described the structure of G, went on to show that Q_{12} has order $2|G| = 2^{21}3^4 5^2 13^2$, and described the structure of Q_{12} in [19].

7.2 Knuth-Bendix applications

The output `last48.l` shows that group $G = Q_{22}$ with extra relator $u^4vu^3v^3uv^4uv$ has simplest visible structure of the now seven remaining groups. What we see is consistent with the hypothesis that this group is isomorphic to C_6, and for good reason: it is. It was quite difficult, however, to prove this.

We attempted a large number of coset enumerations, each defining up to 2 billion cosets, in Q_{22} and in its index 2, 3 and 6 subgroups. In no case were we able to discover a cyclic subgroup of finite index.

Another method for proving finiteness for finitely presented groups is Knuth-Bendix rewriting. As a general rule, coset enumeration is much faster than Knuth-Bendix for straightforward examples. Sims [38, Section 5.8], however, points out that Knuth-Bendix was able to find the order of a group defined by a presentation proposed by B.H. Neumann as a challenge for computers, which at that stage no existing Todd-Coxeter implementation had handled. Some other examples where Knuth-Bendix performs well appear in [21, 20], while Neumann's example is resolved by coset enumeration in [22], where there are further performance comparisons of coset enumeration and Knuth-Bendix rewriting.

It is easy using Reidemeister-Schreier rewriting (`Rewrite` in Magma) to obtain a presentation for the derived group of $G = Q_{22}$, namely

$$G' = \langle a, b \mid bbABAbbaBBa, baaBAAABaab, babaBABABababA\rangle$$

(where $A = a^{-1}$ and $B = b^{-1}$ for ease of notation). This was one of the presentations in which we attempted unsuccessful coset enumerations.

Alun Williams has recently released his MAF package [42] which implements various Knuth-Bendix-based applications, and we are grateful to him for his assistance with it and its use. Experiments with MAF told us that G' is trivial. Hence Q_{22} is isomorphic to C_6.

This proof is perhaps not entirely convincing, since one likely consequence of a bug in a Knuth-Bendix program is an incorrect total collapse. So for additional reassurance, we have repeated the calculation using two independently written Knuth-Bendix implementations, RKBP (see the Acknowledgements) and KBMAG [25] (which is available via both GAP and Magma). Both confirm the result. Indeed it can be done quite quickly in Magma [13, Q22I6.l].

In MAF (using the -nowd parameter which expedites calculations for hard finite groups) the cpu time taken was 8076 secs, the maximal number of equations was 2 253 949, and the maximal memory usage was 680MB. Indeed there is no need to go down to the index 6 subgroup. Using MAF with the (x, y)-presentation we obtain a confluent presentation for Q_{22} (having 7 rewrite rules for $x^2, y^3, [x, y]$) in 8674 cpu secs, with maximal number of equations 1 435 516, and with maximal memory usage 1.3GB.

Information in the output `last48.l` shows that the group Q_{27}, with extra relator $u^4vuvu^2v^2uvuv^4$, has order at least 430920. Here also, our coset enumeration methods have (as yet) failed to resolve the finiteness question. However, using MAF with the (x, y)-presentation for Q_{27} we obtain a confluent presentation for it which confirms that the accepted language contains 430920 words, in 13479 cpu secs. (This computation was first done by Alun Williams.)

In this case, the maximal number of equations was 1 198 789, and maximal memory usage was 1.2GB. The reduction FSA has 186144 states and 54538 equations. The word acceptor has 47365 states. The group Q_{27} is one of the largest "complicated" groups that has been proved finite by Knuth-Bendix processes.

In retrospect, we see that Knuth-Bendix can handle 5 other presentationss (Q_{16}, Q_{24}, Q_{26}, Q_{29}, Q_{35}) relatively easily. Using MAF we find that Q_{16} has order 48 in 1.8 cpu seconds; Q_{24}: 648, 241 cpu seconds; Q_{26}: 6, 3.3 cpu seconds; Q_{29}: 78, 32.7 cpu seconds; Q_{35}: 186, 4.1 cpu seconds.

7.3 The five unresolved presentations

This leaves five one-relator quotients of the modular group with extra relator of length 36 for which we are unable to determine finiteness or otherwise, in spite of significant computational attacks via both Todd-Coxeter and Knuth-Bendix based methods. They are:
Q_{31}, $u^4vuv^4u^3vuv^3$; Q_{33}, $u^4v^2u^2v^4u^2vuv^2$; Q_{37}, $u^3vu^2vu^2v^2uv^2uv^3$;
Q_{40}, $u^3vu^2v^2uv^3u^2vuv^2$; and Q_{43}, $u^3vuvuv^3u^2vuvuv^2$.

The output `last48.l` includes much information about all subgroups with index up to 42 in these groups, and about their cores. There is easily enough to reveal that no two of these groups are isomorphic. For example, the counts of the (conjugacy classes of) subgroups with index up to 42 are all different: 23, 14, 12, 27 and 9, respectively.

We know that each of the groups has at least one L_2-section, In `last48.l` we see that: Q_{31} has $L_2(7)$; Q_{33}, $L_2(13)$; Q_{37}, $L_2(13)$; and Q_{40}, $L_2(11)$. Looking more deeply [13, `l6Ile6SimQ.m`] at the subgroups with index up to six in these groups, we see that the index 3 subgroup of Q_{43} maps onto $L_2(64)$ (as does its index 6 subgroup). We know of only one other nonabelian simple section that occurs: the index 2 subgroup of Q_{37} maps onto J_2 (as does its index 6 subgroup).

An easy computation enables us to show that each of the five groups has a largest soluble quotient and to compute its order. We can also compute all normal subgroups with index up to 100000 and their abelian quotient invariants [13, `l6LIN.m`]. By multiplying the index of thus known normal subgroups by the orders of their abelianisations, we can compute lower bounds on the group orders. We can also increase two of those bounds by multiplying them by the orders of independent sections, namely $L_2(64)$ for Q_{43} and J_2 for Q_{37}. We obtain $|Q_{31}| \geq 220\,814\,937\,504$, $|Q_{33}| \geq 124\,488$, $|Q_{37}| \geq 75\,290\,342\,400$, $|Q_{40}| \geq 5\,544\,000$, and $|Q_{43}| \geq 67\,616\,640$.

8 Concluding remarks

We have studied one-relator quotients of the modular group 'in the small', that is, with a short extra relator. It is interesting to compare and contrast our results with recent generic results.

Kapovich and Schupp [29] have produced detailed information on random m-relator quotients of the modular group for all $m \geq 1$. Their paper includes many interesting results, such as the fact that these quotients are generically essentially incompressible — that is, the smallest size of any possible finite presentation of such a group is bounded below by a function which is almost linear in terms of the length of a random presentation for it. They also compute precise asymptotics of the number of isomorphism types of m-relator quotients where all the defining relators are cyclically reduced words of length n; and they obtain other algebraic results and show that such quotients are complete, Hopfian, co-Hopfian, one-ended, word-hyperbolic groups.

Earlier, Schupp [37] proved that the triviality problem restricted to such presentations is undecidable. The isomorphism problem for such presentations is thus certainly undecidable. Indeed, Schupp's proof shows that the isomorphism problem restricted to certain fixed classes of such groups is undecidable. On the other hand, rigidity shows that the isomorphism problem is generically easy.

We have shown that, in the small, most presentations of one-relator quotients of the modular group define finite groups. We know that 220 out of 8596 with up to 18 syllables define infinite groups. The finiteness question remains unresolved for five groups, and the rest are finite. We can solve the isomorphism problem among these finite quotients, and expect that we can do the same for the infinite ones.

One consequence of the Kapovich and Schupp results is that as the relator length tends to infinity, almost all presentations of one-relator quotients of the modular group define infinite groups. This is very different to our results in the small. Their Theorem C (Counting isomorphism types) specialises to give a formula for $I(s)$, the number of isomorphism types of one-relator quotients of the modular group with s syllables. Thus $\lim_{s\to\infty} I(s) = 2^{s-2}/s$, which is the dominant term in our count of inequivalent s-syllable presentations in Section 2. This (possibly surprising) result is consistent with one of Kapovich and Schupp's observations: "the first basic result is that a long random word over a finite alphabet is essentially its own shortest description."

There are five presentations (out of 8596) for which we have not resolved the finiteness question. One clear issue is that current computational methods for proving very large finitely presented groups to be finite are reaching their limits. In particular, our lower bounds on the orders of Q_{31} and Q_{37} lead us to expect that a finiteness proof for either of them would be hard to find.

Acknowledgements

The first author was partially supported by the New Zealand Marsden Fund. The second author was partially supported by the Australian Research Council. We are grateful to Shona Yu who did many experimental investigations on this topic during a research project in 2001/2002. We are grateful to Alun Williams for help with the Monoid Automata Factory, MAF. We are grateful to Charles Sims for making available to us version 1.58 of the Rutgers Knuth-Bendix Package, `RKBP`.

References

[1] Selman Akbulut and Robion Kirby, A potential smooth counterexample in dimension 4 to the Poincaré conjecture, the Schoenflies conjecture and the Andrews-Curtis conjecture, *Topology* **24** (1985), 375–390.

[2] Gilbert Baumslag, John W. Morgan and Peter B. Shalen, Generalized triangle groups, *Math. Proc. Cambridge Philos. Soc.* **102** (1987), no. 1, 25–31.

[3] Wieb Bosma, John Cannon and Catherine 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/`

[4] Colin M. Campbell, George Havas, Alexander Hulpke and Edmund F. Robertson, Efficient simple groups, *Comm. Algebra* **31** (2003), 5191–5197.

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

[6] Colin M. Campbell, George Havas, Colin Ramsay and Edmund F. Robertson, On the efficiency of the simple groups with order less than a million and their covers, *Experiment. Math.* **16** (2007), 347–358.

[7] C.M. Campbell, P.M. Heggie, E.F. Robertson and R.M. Thomas, Finite one-relator products of two cyclic groups with the relator of arbitrary length, *J. Austral. Math. Soc. Ser. A* **53** (1992), no. 3, 352–368.

[8] C.M. Campbell and E.F. Robertson, A deficiency zero presentation for SL(2, p), *Bull. London Math. Soc.* **12** (1980), no. 1, 17–20.

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

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

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

[12] Marston Conder, A surprising isomorphism, *J. Algebra* **129** (1990), no. 2, 494–501.

[13] Marston Conder, George Havas and M.F. Newman, *On one-relator quotients of the modular group; supplementary materials*, (2009), `http://www.itee.uq.edu.au/~havas/orqmg`

[14] H.S.M. Coxeter, The abstract groups $G^{m,n,p}$, *Trans. Amer. Math. Soc.* **45** (1939), no. 1, 73–150.

[15] M. Edjvet and A. Juhàsz, The groups $G^{m,n,p}$, *J. Algebra* **319** (2008), no. 1, 248–266.

[16] Anna Fabianska, *PSL*, (2009), `http://wwwb.math.rwth-aachen.de/~fabianska/PSLHomepage/`

[17] The GAP Group, Aachen, *GAP – Groups, Algorithms, and Programming, Version* 4.4, (2008). See also `http://www.gap-system.org`

[18] William Rowan Hamilton, Memorandum respecting a new system of roots of unity, *Philos. Mag.* **12** (1856), p. 446.

[19] George Havas and Derek F. Holt, On Coxeter's families of group presentations, submitted (2010).

[20] George Havas, M.F. Newman, Alice C. Niemeyer and Charles C. Sims, Groups with exponent six, *Comm. Algebra* **27** (1999), 3619–3638.

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

[22] George Havas and Colin Ramsay, Proving a group trivial made easy: a case study in coset enumeration, *Bull. Austral. Math. Soc.* **62** (2000), no. 1, 105–118.

[23] George Havas and Colin Ramsay, Experiments in coset enumeration, in *Groups and Computation III*, Ohio State University Mathematical Research Institute Publications **8** (de Gruyter, 2001), 183–192.

[24] G. Havas and C. Ramsay. Coset enumeration: ACE version 3.001 (2001). Available as `http://www.itee.uq.edu.au/~havas/ace3001.tar.gz`

[25] Derek F. Holt, The Warwick automatic groups software, *Geometrical and Computational Perspectives on Infinite Groups* (ed. Gilbert Baumslag et al), DIMACS Ser. Discrete Math. Theoret. Comput. Sci. **25** (1996), 69–82.

[26] Derek F. Holt and Sarah Rees, Computing with abelian sections of finitely presented groups, *J. Algebra* **214** (1999), 714–728.

[27] J. Howie, V. Metaftsis and R.M. Thomas, Finite generalized triangle groups. *Trans. Amer. Math. Soc.* **347** (1995), no. 9, 3613–3623.

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

[29] Ilya Kapovich and Paul E. Schupp, Random quotients of the modular group are rigid and essentially incompressible, *J. Reine Angew. Math.* **628** (2009), 91–119.

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

[31] L. Lèvai, G. Rosenberger and B. Souvignier, All finite generalized triangle groups, *Trans. Am. Math. Soc.* **347** (1995), no. 9, 3625–3627.

[32] Vasileios Metaftsis and Izumi Miyamoto, One-relator products of two groups of order three with short relators. *Kyushu J. Math.* **52** (1998), no. 1, 81–97.

[33] G.A. Miller. On the groups generated by two operators. *Bull. Amer. Math. Soc.* **7** (1901), no. 10, 424–426.

[34] G.A. Miller. Groups defined by the orders of two generators and the order of their product. *Amer. J. Math.* **24** (1902), no. 1, 96–100.

[35] W. Plesken and A. Fabianska, An L_2-quotient algorithm for finitely presented groups, *J. Algebra* **322** (2009), no. 3, 914–935.

[36] Derek J.S. Robinson, *A Course in the Theory of Groups, Second Edition*, Graduate Texts Math. **80** (Springer-Verlag, New York 1996).

[37] Paul E. Schupp, Embeddings into simple groups, *J. London Math. Soc.* (2) **13** (1976), no. 1, 90–94.

[38] C.C. Sims, *Computation with finitely presented groups*, Encyclopedia of Mathematics and its Applications **48**, (Cambridge University Press, 1994).

[39] N.J.A. Sloane. The On-Line Encyclopedia of Integer Sequences, (2009),
`http://www.research.att.com/~njas/sequences/A000011`

[40] Yücel Türker Ulutaş and İsmail Naci Cangül, One relator quotients of the modular group, *Bull. Inst. Math. Acad. Sinica* **32** (2004), no. 4, 291–296.

[41] J. Wiegold, The Schur multiplier: an elementary approach, *Groups St Andrews 1981*, London Math. Soc. Lecture Note Ser. **71** (Cambridge University Press, 1982), 137–154.

[42] Alun Williams, *Monoid Automata Factory*, (2009),
`http://www.alunw.freeuk.com/MAF/maf.html`