Computing with abelian sections of finitely presented groups.

Derek F. Holt and Sarah Rees

Derek F. Holt
Mathematics Institute
University of Warwick
UK
E-mail: dfh@maths.warwick.ac.uk

Sarah Rees
Department of Mathematics
University of Newcastle
UK
Sarah.Rees@ncl.ac.uk

Address for correspondence:

Derek F. Holt
Mathematics Institute
University of Warwick
Coventry CV4 7AL
Great Britain

Proposed running head: Computing with abelian sections

Abstract

Let G be a finitely presented group. This paper describes the theory and practice of a method for obtaining information about the finite and abelian-by-finite quotients of G, which often allows computation further down into the group than has been possible by more traditional methods. The paper also describes the authors' software package **quotpic**, which provides a user-friendly implementation of the algorithms involved in this method, as part of a complete range of facilities for computing various types of quotients of finitely presented groups.

1 Introduction

When attempting to compute finite quotients of a finitely presented group G, it is generally the case that the larger the quotient, the more difficult is the computation. In particular, if a finite quotient G/N is known already, then the difficulty of finding abelian-by-finite quotients G/N' with $N' \subset N$ and N/N' abelian increases with the order of G/N.

We have recently developed a method of computing such quotients, which appears to increase the range of values of $|G/N|$ for which such computations are practical. It works when G/N has a non-cyclic abelian normal subgroup M/N and the idea, roughly, is to divide-and-conquer the problem by performing the required calculations with the smaller factor groups G/K, where $N \subset K \subset M$ and G/K is cyclic.

This method is described in detail in the final section of the paper. Our other objective is to discuss some of the functionality of the software package **quotpic**, which was designed and written by the authors for computing various types of quotients of finitely presented groups G. In particular, it now includes a convenient implementation of the new abelian-by-finite quotient algorithm. There is an earlier paper ([Holt & Rees 1991]) on **quotpic**, which is now somewhat out-of-date, so this a convenient opportunity to rectify that anomaly, and to indicate the directions in which the program has developed.

quotpic is an interactive graphics display program which takes a finite presentation of a fixed group G as input. Its basic function is to construct quotients of G and to display the output graphically as a lattice on a screen. Each vertex of the lattice corresponds to a normal subgroup of finite index in G. A click on a vertex opens a menu from which the user can select functions to build the lattice downwards below the selected normal subgroup. The article [Holt & Rees 1991] still gives a reasonable account of the basic principles of the program. A number of changes were already proposed in Section 5 of that paper, and all of those were implemented; in addition there are other new features.

The reader who wants more technical details about the graphical interface to **quotpic** should refer either to [Holt & Rees 1991] or (better) to **quotpic** itself, since it is the sort of program that is most easily learnt by practice. We shall concentrate here on its mathematical capabilities, particularly on the more recent developments. In Section 2 we give an overview of these capabilities, and indicate the directions in which the program has developed. Sections 3 and 4 then describe two new facilities that can be applied whenever normal subgroups N and M of G have been found such that M/N is an abelian p-group for some prime p. Section 3 explains in some theoretical detail an algorithm to find the conjugacy classes of complements of M/N in G/N (if any), in the case when M/N is elementary. The theory and practice of the method mentioned above of finding abelian quotients of N using the cyclic quotients of M/N is discussed in detail in Section 4. Sections 3 and 4 also contain examples of applications of these new features to actual group theoretical problems.

The program is available by anonymous `ftp` from `ftp.maths.warwick.ac.uk` in the directory `people/dfh/isom_quotpic` or `ftp.ncl.ac.uk` in the directory `pub/local/nser`, or from `http://www.maths.warwick.ac.uk/~dfh`. We are very happy to receive bug reports, suggestions for improvements, and other enquiries.

2 An updated overview of quotpic

The underlying idea in **quotpic** is to apply algorithms to the input group G that compute subgroups of finite index in G, and then to find presentations of these subgroups using the Reidemeister-Schreier method, so that the same algorithms can be applied to the subgroups, thereby calculating further subgroups of larger index. These algorithms include searching for epimorphisms onto fixed finite groups, and searching for all subgroups up to a given index, together with abelian, nilpotent, soluble and p-group quotient algorithms. The code for some of them has been imported from elsewhere (see below for references).

Such computations can be done equally efficiently (and no doubt more efficiently in some cases) in a number of group theory packages, including GAP ([Schönert et. al. 1992]) and MAGMA ([Bosma & Cannon 1993]). There are however two big advantages in using **quotpic**. The first is its graphical interface, which enables the user to have an immediate overview of the current state of the calculations; this alone often makes **quotpic** faster and easier to use in practice than a command-line based package. The second is that **quotpic** maintains information internally about the embedding of the subgroups H in G (for example the conjugation action of G on H when H is normal), which enables it to perform some calculations that would be very cumbersome to do in a different system. An example of this is the use of the Aachen implementation of the Meataxe algorithm ([Lux, Müller and Ringe 1994]) to find all normal subgroups of G that lie within a maximal elementary abelian layer M/N of G.

quotpic is designed as a program which functions at two levels. The graphics are organised at one level; the algorithms are run by UNIX system calls to `C` programs, and information is passed between those programs using files. Since the beginning of **quotpic**, this design has made it easy for us to incorporate implementations from elsewhere; thus **quotpic** provides convenient access to some of the best implementations of group theory algorithms currently available in the world. Since [Holt & Rees 1991], the number of imported algorithms has increased; as planned at that time (and listed in Section 5 of that paper), we have included Schönert's implementation of the low index subgroup algorithm, O'Brien's implementation of the ANU p-quotient algorithm and Nickel's implementation of the nilpotent quotient algorithm. In addition we have added access to Havas' Todd-Coxeter coset enumerator ([Cannon et. al. 1973]) and Brückner's implementation of Plesken's modular soluble quotient algorithm ([Brückner 1997, Plesken 1987]). Each of these facilities can be applied to any subgroup H of G for which a presentation has been calculated. We are very grateful to the authors of these imported programs for their cooperation in helping us to integrate their programs into **quotpic**.

The original version of **quotpic**, as the name suggests, concentrated very much on the construction of the lattice of normal subgroups. Although the displayed vertices continue to correspond to normal subgroups of the input group G, the available functions can now be applied, in principal, to any subgroup H that has been found. Each such H is associated with a displayed vertex corresponding to its core K in G, and H is accessed via that vertex.

As it has always done, **quotpic** stores its information on subgroups by the construction of finite permutation representations of G. Each such representation is associated with one specific vertex, which corresponds to the kernel K of this permutation representation in G. The representation may be transitive or intransitive, but a transitive one should be thought of as representing the subgroup which is the stabiliser H in G of a fixed point (i.e. the point numbered 1) in the representation. Thus $K \subseteq H$, and K is indeed the core of H in G. This permutation representation is precisely the input that is required for the Reidemeister-Schreier algorithm to compute a presentation of H. Most of the available functions can only be applied to H after this presentation has been computed, and **quotpic** does this automatically as soon as it is required.

The permutation representation corresponding to K itself is the regular permutation representation of G/K. This is calculated routinely whenever $|G/K|$ is sufficiently small, and its presence is indicated to the user by the corresponding displayed vertex being green and circular. A yellow triangular vertex indicates that this regular representation is not stored, but there are some permutation representations associated with this vertex. The main menu obtained by clicking on the vertex lists the operations available that can be applied to K. The non-regular transitive permutation representations associated with the vertex represent non-normal subgroups H of G for which K is the core of H in G. To perform operations on H, the user clicks on the vertex corresponding to K and then selects the 'non-normal subgroups' option. The required subgroup

H can then be selected by scrolling through the list of all such subgroups, and then (finally) a menu displaying the available operations on H appears.

Any transitive permutation representation of H that is computed as a result of computations on H is automatically lifted to the transitive representation of G with the same stabiliser, provided that its degree is not too large. This may result in the display of a new (circular or triangular) vertex corresponding to the core of this stabiliser in G. Of course, the core may already have been computed earlier as a result of some other calculation. If the index is not too large, then **quotpic** automatically checks to see if this is the case, by comparing the new core with all other known normal subgroups of the same index. If the index is large, then this is not done routinely, but the user can force the comparison of two apparently distinct normal subgroups of the same index by computing their intersection; if they turn out to be equal, then their corresponding vertices will be identified, and all known information about them amalgamated.

In Sections 3 and 4 below, we describe in some detail two particular new features of **quotpic**, together with some examples of their application. These depend on the use of the Reidemeister-Schreier subgroup presentation algorithm applied to a normal subgroup M of G. From this presentation, it is possible to compute various quotients of M and, in particular, for a given prime p, the largest elementary abelian p-quotient M/N of M. We can regard M/N as a vector space, with some fixed basis B, over $GF(p)$, and use the Reidemeister-Schreier rewriting process to express any word in the generators of G that lies in M as a vector in M/N with respect to B. This enables us, for example, to calculate matrices for the conjugation action of the generators of G on M/N.

3 Finding complements of elementary abelian sections

3.1 Theory

Let $G = \langle x_1, \ldots, x_m | r_1, \ldots, r_n \rangle$ be our group, and suppose that G has normal subgroups M and N with $N \subset M$ and M/N an elementary abelian p-group of order p^d, with p prime. In this section, we consider the problem of deciding whether or not M/N has a complement in G/N and, if so, finding representatives of the conjugacy classes of such complements. For each such representative C/N, the permutation representation of G on the cosets of C can be computed if desired, and if its degree p^d is not too large. The kernel of this representation (that is, the core of C in G) will contain N.

We can regard M/N as a vector space V of dimension d over $GF(p)$, and let $B = \{b_1, \ldots b_d\}$ be a generating set for M/N or, equivalently, a basis for V. (We use additive notation for V whenever we are treating it as a vector space.)

In order to perform the required calculations, we need three other items of data:

1. Words $r_{n+1}, \ldots, r_{n'}$ in x_i such that $\langle x_1, \ldots, x_m | r_1, \ldots, r_{n'} \rangle$ is a presentation of G/M.
2. $d \times d$ matrices M_i $(1 \le i \le m)$ over $GF(p)$, giving the conjugation action of the generators x_i of G on $M/N = V$, relative to the fixed basis B.
3. The values u_i of the elements $r_{n+1}, \ldots, r_{n'}$ modulo N, calculated as vectors in $M/N = V$, using the basis B.

To find extra relators for the quotient, we use the standard algorithm based on guessing relators and eventually using Todd-Coxeter coset enumeration to verify that we have enough to define G/M as an abstract group. This was first described in [Cannon 1973]. As mentioned at the end of the previous section, the Reidemeister-Schreier process for the subgroup M of G can be used to calculate the required matrices M_i. The values u_j in M/N of the extra relators r_j $(n+1 \le j \le n')$ for G/M can also be calculated by Reidemeister-Schreier rewriting. Since the r_j for $j \le n$ are relators of G, we put u_j to be the zero element of V for $1 \le j \le n$. From now on, we do not need to distinguish between the two sets of relators.

A complement of M/N in G/N, as a transversal for M/N in G/N, must be generated by elements $x_i v_i$ $(1 \le i \le m)$ for suitable $v_i \in M/N$. For any choice of words v_i, the group $H/N = \langle x_i v_i \rangle$ has the property that $H/N.M/N = G/N$, and hence $|H/N| \ge |G/N|/|M/N|$. Now H/N is a complement provided that $|H/N| = |G/N|/|M/N| = |G/M|$; so it is enough to check that $|H/N|$ is a homomorphic image of (and hence no larger than) $|G/M|$.

Suppose that, for $1 \le j \le n'$, the word r_j has length l_j and is equal to $x_{j,1}^{\varepsilon_{j,1}} x_{j,2}^{\varepsilon_{j,2}} \ldots x_{j,l_j}^{\varepsilon_{j,l_j}}$, where each $\varepsilon_{j,k}$ is equal to ± 1. Then the above discussion shows that the elements $x_i v_i$ generate a complement if and only if the elements

$$y_j := (x_{j,1} v_{j,1})^{\varepsilon_{j,1}} (x_{j,2} v_{j,2})^{\varepsilon_{j,2}} \ldots (x_{j,l_j} v_{j,l_j})^{\varepsilon_{j,l_j}}$$

lie in N for all $1 \le j \le n'$. By collecting the generators x_i to the left, we find that $y_j = u_j w_j$, where

$$w_j = v_{j,1}^{y_{j,1}} v_{j,2}^{y_{j,2}} \ldots v_{j,l_j}^{y_{j,l_j}}$$

and, for $1 \le k \le l_j$, the conjugating element $y_{j,k}$ is equal to $x_{j,k+1}^{\varepsilon_{j,k+1}} x_{j,k+2}^{\varepsilon_{j,k+2}} \ldots x_{j,l_j}^{\varepsilon_{j,l_j}}$ if $\varepsilon_{j,k} = 1$ and $-x_{j,k}^{\varepsilon_{j,k}} x_{j,k+1}^{\varepsilon_{j,k+1}} \ldots x_{j,l_j}^{\varepsilon_{j,l_j}}$ if $\varepsilon_{j,k} = -1$. (Here we are using g^h to denote $h^{-1}gh$ and g^{-h} to denote its inverse $h^{-1}g^{-1}h$.) See also page 103 of [Holt & Plesken 1989] for an alternative notation using Fox derivatives.

For a complement, we therefore need (using additive notation) $w_j = -u_j$ as elements of V, for $1 \le j \le n'$. Since we know the elements u_j as vectors in V and the matrices $M(i)$ for the conjugation action of the x_i on V, this reduces to an explicit system of dn' equations in dm unknowns in V, where the unknowns are the components of the vectors v_i $(1 \le i \le m)$. The equations can be solved by echelonising their matrix in the standard way.

If they have no solution, then the extension is non-split, and there are no complements. Assume therefore that solutions exist, and that $v_i = c_i$ $(1 \le i \le m)$ is one such solution. Then, a general solution has the form $c_i + z_i$, where z_i $(1 \le i \le m)$ is a solution of the corresponding homogeneous system of equations $w_j = 0$. These solutions z_i form a vector space which is essentially equal to the space of 1-cocyles $Z^1(G/M, V)$. We are only interested in finding the complements up to conjugacy, so we need to find the subspace of coboundaries $B^1(G/M, V)$ and select complements $c_i + z_i$, where we take one solution z_i for each coset of $B^1(G/M, V)$ in $Z^1(G/M, V)$. Since $B^1(G/M, V)$ is generated by the d solutions $y(k)_i$ $(1 \le k \le d)$, where $y(k)_i = b_k^{x_i} - b_k$, these calculations are routine.

Suppose now that the elements v_i $(1 \le i \le m) \in M$ are such that the elements $x_i v_i$ do generate a complement C/N, and we wish to calculate the permutation representation of G on the right cosets of C. The index $|G : C|$ is equal to p^d, and for coset representatives, we can take coset representatives v of N in M. We need to calculate the permutation action of the x_i on these cosets, but this is straightforward, since $v x_i = x_i v^{x_i} = (x_i v_i)(v_i^{-1} v^{x_i})$, where $x_i v_i \in C$, and so x_i maps the coset $C v_i$ to $C v_i^{-1} v^{x_i}$.

3.2 Example

In [Bray 1995], Bray carried out a systematic investigation of finite groups that could be presented as quotients of various (infinite) groups with symmetric presentations, by adding extra relators. One example was

$$G = \langle x, y, t | x^3, y^2, (xy)^2, t^3, (yt)^2, (xt)^{17}, (x^2t)^9, (yxt)^{16}, (yt^x t)^3 \rangle.$$

He identified G as an extension of a group of order 2^9 by $L_2(17)$ having a quotient isomorphic to a split extension of an elementary abelian group of order 2^8 by $L_2(17)$, but was unable to determine the precise structure of the full group. Using **quotpic**, we found that it is in fact a split extension of an elementary abelian group of order 2^9 by $L_2(17)$, having two conjugacy classes of complements.

4 Using maximal subgroups of elementary abelian sections

4.1 Theory

The facility to be described in this section is quite a simple one, but when combined with some theoretical results, it can be used to obtain information about larger quotients of G than would be possible by direct computation. Several examples of its application will be described in the second subsection below. For a finitely generated group H and a prime p, we shall use $O^{\mathrm{el(p)}}(H)$ to denote the smallest normal subgroup of H such that $H/O^{\mathrm{el(p)}}(H)$ is an elementary abelian p-group. One of the basic facilities of **quotpic** is to compute $O^{\mathrm{el(p)}}(H)$ for subgroups H of G for which the permutation representation of G on the cosets of H has been stored.

Suppose that the normal subgroup L of G has been computed together with the regular representation of G/L, that $M = O^{\mathrm{el(p)}}(L)$ has also been computed for some prime p, and that $|L/M| = p^d$. Then, as mentioned earlier, **quotpic** can compute the action of G on L/M, as $d \times d$ matrices over $GF(p)$. Assuming that p^d is not too large (perhaps up to about a million), **quotpic** can then use these matrices to calculate representatives K_i/M of the orbits of the action of G on the maximal subgroups of L/M. Provided that $|G : K_i| = p|G : L|$ is not too large, it can then compute the permutation representations of G on the cosets of the subgroups K_i. As usual, the kernels of these representations (which are the cores of the K_i in G) will be plotted, either as triangular or circular vertices, depending on their index in G. These will lie between M and L, and some of them may be equal to M. (Note that the vertices corresponding to normal subgroups between M and L can also be obtained by **quotpic** using the Meataxe option, but in that case, when their index is too large, they will have no associated stored permutation representation.)

The point of the above is to enable us to obtain information about the abelian quotients of M, by carrying out calculations on the subgroups K_i rather than on M itself. Since the index $|G : K_i| = p|G/L|$ is in general smaller than $|G : M| = p^d|G/L|$, this has the effect of extending the effective range of **quotpic**. We shall now describe the related theory which enables us to obtain this information.

Proposition 4.1 *Let X be a finite group having a normal subgroup Y, such that X/Y is an abelian p-group and Y is an elementary abelian q-group, for distinct primes p and q. Then the intersection W in X of the groups $O^{\mathrm{el(q)}}(Z)$, where Z ranges over all subgroups of X with $Y \subseteq Z$ and X/Z cyclic, is trivial.*

PROOF: Since X/Y is finite abelian it is a direct product of cyclic groups, so $W \subseteq Y$. Suppose $W \neq 1$. Clearly $W \trianglelefteq X$, so we can choose a nontrivial minimal normal subgroup V of X with $V \subseteq W$. Now V corresponds to an irreducible representation over $GF(q)$ of the the abelian group X/Y, and so by the standard representation theory of abelian groups, $X/C_X(V)$ must be cyclic. Thus $C_X(V)$ is one of the subgroups Z defined in the lemma, and so $V \subseteq O^{\mathrm{el(q)}}(C_X(V))$. By Maschke's Theorem, V has a complementary submodule U in Y, and by the Schur-Zassenhaus theorem Y has a complement C in $C_X(V)$. Then $C_X(V) = V \times CU$, so the quotient $C_X(V)/CU$ of $C_X(V)$ is an elementary abelian q-group, and hence $CU \supseteq O^{\mathrm{el(q)}}(C_X(V))$. But this contradicts $V \subseteq O^{\mathrm{el(q)}}(C_X(V))$, because $V \cap CU = 1$. $\square$

Corollary 4.2 *With X and Y as in the lemma, if $O^{\mathrm{el(q)}}(Z) = Z$ for all subgroups Z with $Y \subseteq Z$ and X/Z cyclic, then $Y = 1$.*

The most straightforward applications of these results using **quotpic** arise when X/Y is elementary abelian, in which case the subgroups Z are just those of index p in X.

Let G be a finitely presented group, and let L, M, N be normal subgroups of G with $N \subseteq M \subseteq L$, where L/M is an elementary abelian p-group and M/N an elementary abelian q-group, for distinct primes p and q. Let K be a subgroup of index p in L. Then the kernel of the permutation representation of G on the right cosets of $O^{\mathrm{el(q)}}(K)$ is the intersection of the subgroups $O^{\mathrm{el(q)}}(K^g)$, for all $g \in G$. We therefore have the following immediate consequences of Proposition 4.1 and its corollary, by putting $X = L/N$ and $Y = M/N$.

Proposition 4.3 *Let G, L, M, N, p and q be as above, and let $K_1, \ldots, K_n$ be representatives of the the orbits of the action of G by conjugation on the subgroups of index p in L. Then, where ρ_i is the permutation representation of G on the right cosets of $O^{\mathrm{el(q)}}(K_i)$, the intersection of the kernels of the ρ_i is equal to N.*

Corollary 4.4 *With the same notation, if $O^{\mathrm{el(q)}}(K_i) = K_i$ for each i, then $N = M$.*

These results are most useful in cases where **quotpic** would have difficulty in computing G/N directly, because the index $|G : M|$ is too large. Assuming that the index $|G : K_i|$ is not too large, then by using the facility described at the beginning of this section, **quotpic** can compute the subgroups K_i and the orders of the quotients $K_i/O^{\mathrm{el(q)}}(K_i)$. If these should happen to be all trivial, then we can immediately conclude from the corollary that $N = M$.

If the quotients themselves are not too large, then we can also compute the permutation representations of G on the cosets of the subgroups $O^{\mathrm{el(q)}}(K_i)$. The kernels of these representations will then be plotted by **quotpic**. By the lemma, N can then be found as the intersection of these kernels, and an (intransitive) faithful permutation representation of G/N will be stored, so the order of G/N can also be calculated.

By allowing the prime q to vary, we get the following useful result about infinite abelian quotients of M.

Corollary 4.5 *Let G, L, M, p and K_i be as in Proposition 4.3.*
(i) If none of the K_i/N has an infinite abelian quotient, then neither does M/N.
(ii) Let $q \neq p$ be a prime. If none of the K_i has a finite abelian invariant divisible by q, then neither does M.

Proof: (i) If M has an infinite abelian quotient, then it has a nontrivial elementary abelian q-quotient for all primes q. It follows from Corollary 4.4 that at least one of the subgroups K_i has nontrivial elementary abelian q-quotients for infinitely many primes q, which implies that it has an infinite abelian quotient.
(ii) Suppose that M has a finite abelian invariant divisible by the prime q, and let $Y[M,M]/[M,M]$ be a cyclic direct factor of $M/[M,M]$ of order a power of q. Then $YO^{\mathrm{el}(q)}(M)/O^{\mathrm{el}(q)}(M)$ has order q, so by Proposition 4.3, we have $Y \not\subseteq O^{\mathrm{el}(q)}(K_i)$ for some i, at least after replacing Y by a conjugate. Thus $Y[K_i,K_i]/[K_i,K_i]$ is a non-trivial finite q-group, and so K_i must have a finite abelian invariant of order divisible by q. $\square$

4.2 Examples

4.2.1 An example of Seidel

Several years ago, we were asked to investigate the structure of the following group, by J.J. Seidel.

$$\begin{aligned} G = \langle\, a,b,c,d,e,f \quad | \quad & a^3, b^3, c^3, d^3, e^3, f^3, (ac)^2, (ad)^2, (ae)^2, (bd)^2, \\ & (be)^2, (bf)^2, (ce)^2, (cf)^2, (df)^2, (ab^{-1})^2, \\ & (af^{-1})^2, (bc^{-1})^2, (cd^{-1})^2, (de^{-1})^2, (ef^{-1})^2 \,\rangle. \end{aligned}$$

We find, using **quotpic**, that G maps onto A_5, and that the kernel L of this map has L/M of order 2^{12}, where $M = O^{\mathrm{el}(2)}(L)$. It is difficult to investigate the abelian quotients of M directly, although V. Felsch in Aachen did eventually succeed, after an overnight computation, in finding a presentation of M, simplifying it, and calculating its abelian quotient as a free abelian group of rank 25.

By using the methods described above, we can obtain similar information much more quickly. We found that there are 105 orbits of G in its action on the subgroups of index 2 in L. Although this seems a lot, they only have index 120 in G, and it took less than 2 seconds cpu-time to calculate the maximal abelian quotients of each of these. It turned out that these were 2-groups except for four of the 105 orbit representatives; there was an additional infinite cyclic factor in three of the cases and two infinite cyclic factors in the fourth. We then calculated $K/O^{\mathrm{el}(3)}(K)$ for these four maximal subgroups K, which gave us four new vertices, corresponding to cores of the subgroups $O^{\mathrm{el}(3)}(K)$; the indices were 360 for three of them, and 1080 for the fourth. By taking the intersection of these four cores, and computing the order of the resulting permutation group, we were able to calculate very easily the order of $M/O^{\mathrm{el}(3)}(M)$, which turned out to be 3^{25}. Since none of the abelian quotients of the maximal subgroups K has finite cyclic factors of orders divisible by primes other than 2, Corollary 4.5(ii) implies that $M/[M,M]$ is a direct product of a free abelian group of rank 25, and possibly a 2-group.

4.2.2 An example going back to Coxeter

The family of groups

$$(m, n, p; q) = \langle\, x, y \mid x^m, y^n, (xy)^p, [x, y]^q \,\rangle,$$

introduced by Coxeter in [Coxeter 1939] has been intensively investigated, the most frequent problem being to determine which are finite. Thanks to the work of Coxeter, Howie, Edjvet, Thomas and others, together with various computer calculations (see, for example, [Thomas 1995] for further details and references), there are now only six outstanding cases. Of these, five have $m = 3$ and $q = 2$. The other one, $(2, 3, 13; 4)$ is in some ways the most frustrating, since fairly large finite quotients are known. (In fact the largest finite quotient currently known has order 358 848 921 600, and composition factors $L_2(25), L_3(3)$ and C_2 13 times.)

In particular, there is an epimorphism from $G = (2, 3, 13; 4)$ onto $L_3(3)$, with kernel L, for which L/M has order 2^{12} where $M = O^{\mathrm{el}(2)}(L)$. Using **quotpic**, we find that L/M has two conjugacy classes of complements in G/M. We can also use the action of G on maximal subgroups of L/M to help us prove reasonably quickly that M is perfect. It turns out that there are 14 orbits of G on these maximal subgroups, and for each orbit representative K_i we find that $K_i/[K_i, K_i]$ has order 2^{11}, which means of course that $[K_i, K_i] = M$. By Corollaries 4.4 and 4.5(i) above, this implies that $M/[M, M]$ is a 2-group. However, by applying the p-quotient algorithm to L, we find that L/M is the maximal 2-quotient of L, and so M is in fact perfect. (In fact, this result was first computed by the second author and Mike Newman, but they did the calculation for all 4095 maximal subgroups of L/M, rather than just the 14 orbit representatives.)

The index in G of the subgroups K_i is 11 232, which is moderately large for an abelian quotient computation, but this turns out to be a very straightforward example, and in fact the computation of $K_i/[K_i, K_i]$ took only about 10 seconds cpu-time for each K_i.

4.2.3 The Heineken group

We carried out a somewhat similar, but much longer computation starting with the example

$$G = \langle\, x, y, z \mid [x, [x, y]] = z, [y, [y, z]] = x, [z, [z, x]] = y \,\rangle,$$

proposed by Heineken several years ago as a possible candidate for a finite group with a balanced cyclic presentation. In fact, we were able to show recently that it is infinite by proving it automatic, and explicitly computing its word acceptor [Holt & Hurt 1997], but investigating its finite quotients remains a challenging problem. The largest known such quotient is an extension of a 2-group of order 2^{24} by A_5.

We took L to be a normal subgroup with G/L an extension of a group of order 2^6 by A_5, and found that L/M has order 2^{14}, where $M = O^{\mathrm{el}(2)}(L)$. (Hence G/M is an extension of 2^{20} by A_5, and is not quite the largest known finite quotient of G.) We then calculated that G has 23 orbits on the maximal subgroups of L/M. The index of these maximal subgroups K_i in G is 7680, which is smaller than in the previous example, but it turns out that this example is much more difficult to compute with, and we were unable to calculate $K_i/[K_i, K_i]$. However, we can calculate $K_i/O^{\mathrm{el(p)}}(K_i)$ for specific primes p, and so far we have used this to establish (using the above corollaries, as before), that M has no infinite abelian quotients, and no nontrivial 3-groups or 5-groups as quotients.

4.2.4 The Havas-Newman-O'Brien deficiency zero 3-groups

In [Havas, Newman & O'Brien 1996], the authors defined presentations of fourteen groups with three generators and three relators that they believed to be finite of order 3^8; they were able to verify this property for the first ten of them using coset enumeration. The remaining four presentations are

1. $\langle a, b, c \mid cac^{-1}b^{-1}aba,\ bacba^{-1}c^{-1}b,\ cb^{-1}acbca^{-1} \rangle$,
2. $\langle a, b, c \mid acab^{-1}c^{-1}ab,\ b^2a^{-1}c^{-1}acb,\ ca^{-1}b^{-1}cabc \rangle$,
3. $\langle a, b, c \mid acab^{-1}c^{-1}ab,\ acbc^{-1}ba^{-1}b,\ b^{-1}abc^2a^{-1}c \rangle$,
4. $\langle a, b, c \mid a^3 = [c^{-1}, b],\ b^3 = a^{-1}cabc^{-1}b^{-1},\ c^3 = [a^{-1}, b^{-1}][a^{-1}, c][b, c] \rangle$.

For these, they were unable to prove finiteness, but could show easily, using the nilpotent quotient algorithm, that the largest nilpotent quotients of all four groups have order 3^8. We have been able to prove, using the methods of this section, that the largest soluble quotient of each of these groups also has order 3^8. The direct calculation, using Reidemeister-Schreier and integral matrix diagonalisation on the kernels of the maps onto the quotients of order 3^8, seems too difficult. However, H. Brückner was also able to carry out this computation using his implementation of the Plesken soluble quotient algorithm [Brückner 1997, Plesken 1987]; as we have already mentioned, this implementation is now available within **quotpic**. That the computation is possible using Plesken's algortihm is not really surprising, because our method could be regarded as a cruder version of Plesken's method that works in a more general situation (not just for soluble greoups).

By using Corollary 4.4 as in the previous examples, it is possible to reduce the computation to the calculation of the abelian quotients of a number of subgroups of index 3^6. However, even that is very difficult for integral matrix diagonalisation, and we were unable to complete the calculation in the fourth example. By using Proposition 4.1 in a situation where X/Y is abelian but not elementary abelian, we were able to reduce the problem to the calculation of abelian quotients of 12 subgroups of index 3^5 and 9 subgroups of index 3^4 in each group. These calculations were carried out successfully for all groups. As expected, all such abelian quotients were 3-groups, thereby proving the desired result.

To be more precise, in each of the four examples, we take X to be the commutator subgroup $[G, G]$ of the group G defined by the presentation, and Y to be $[X, X]$. Then Y has index 3^8 in G (and is therefore the kernel onto the largest nilpotent quotient of G), and X/Y is abelian, with invariants $3, 9, 9$. So it suffices to compute the abelian invariants of all subgroups Z of X for which X/Z is a maximal cyclic quotient of order 3 or 9. To locate the appropriate subgroups Z, we start by calculating the largest elementary abelian 3-quotients of each of the 13 subgroups W of index 3 in X. Then four of these quotients have order 3^3, and the remaining nine have order 3^2. Those with order 3^2 are precisely those for which W/Y is a direct product of two cyclic groups of order 9, and so they are the ones for which X/W is a maximal cyclic quotient of X of order 3. We therefore need to calculate their abelian invariants, which is easy. On the other hand, the subgroups Z for which X/Z is cyclic of order 9 are all contained as subgroups of index 3 in one of the four groups W for which $W/O^{\mathrm{el}(3)}(W)$ has order 3^3. We can therefore use **quotpic** to calculate the orbit representatives of the conjugation action of G on the subgroups of index 3 in W, and for each W we find that there are three orbit representatives of subgroups Z for which X/Z is cyclic. This produces a total of 12 subgroups Z of index 3^5 in G for which we need to calculate the abelian invariants.

References

[Bosma & Cannon 1993] W. Bosma and J. Cannon, MAGMA *Handbook*, Sydney, 1993.

[Bray 1995] J.N. Bray, *Symmetric Presentations of Finite Groups*, M.Phil. Thesis, University of Birmingham, UK, 1995.

[Brückner 1997] H. Brückner, Doctoral Thesis, RWTH Aachen.

[Cannon 1973] J. Cannon, "Construction of Defining Relators for Finite Groups", *Discrete Mathematics* **5** (1960), 105–129.

[Coxeter 1939] H.S.M. Coxeter, "The abstract groups $G^{m,n,p}$", *Trans. Amer. Math. Soc.* **45** (1939), 73–150.

[Cannon et. al. 1973] John J. Cannon, Lucien A. Dimino, George Havas, Jane M. Watson, "Implementation and analysis of the Todd-Coxeter algorithm", *Math. Comp.* **27** (1973), 463–490.

[Havas, Newman & O'Brien 1996] George Havas, M.F. Newman and E.A. O'Brien, "Groups of deficiency zero", in G. Baumslag et al. (eds.), *Geometric and Computational Perspectives on Infinite Groups*, DIMACS series in Discrete Mathematics and Theoretical Computer Science **25** (1996) 53–67.

[Holt & Hurt 1997] D.F. Holt and D.F. Hurt, "Automatic coset systems and subgroup presentations", submitted to *J. Symbolic Computation.*

[Holt & Plesken 1989] D. Holt and W. Plesken, *Perfect groups*, Oxford University Press, 1989.

[Holt & Rees 1991] D.F. Holt and Sarah Rees, "A graphics system for displaying finite quotients of finitely presented groups", in L. Finkelstein and W.M. Kantor (eds.), *Groups and Computation*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science **11** (1993) 113 – 126.

[Lux, Müller and Ringe 1994] K. Lux, J. Müller and M. Ringe, "Peakword condensation and submodule lattices: an application of the MEAT-AXE", *J. Symbolic Computation* **17** (1994), 529–544.

[Plesken 1987] W. Plesken, "Towards a soluble quotient algorithm", *J. Symbolic Computation* **4**, 111–122.

[Schönert et. al. 1992] M. Schönert et. al., GAP – *Groups, Algorithms, and Programming*, Lehrstuhl D für Mathematik, RWTH Aachen, Germany, first edition, 1992.

[Thomas 1995] R.M. Thomas, "Group presentations where the relators are proper powers", in C. M. Campbell et al. (eds.), *Groups '93 - Galway / St Andrews, Volume 2*, London Math. Soc. Lecture Notes **212**, Cambridge University Press (1995), 549 – 560.