J. Aust. Math. Soc. **85** (2008), 323–332
doi:10.1017/S1446788708000852

BEHIND AND BEYOND A THEOREM ON GROUPS RELATED TO TRIVALENT GRAPHS

GEORGE HAVAS✉, EDMUND F. ROBERTSON and DALE C. SUTHERLAND

(Received 17 December 2007; accepted 4 May 2008)

Communicated by Peter M. Neumann

Dedicated to Cheryl Praeger for her sixtieth birthday

Abstract

In 2006 we completed the proof of a five-part conjecture that was made in 1977 about a family of groups related to trivalent graphs. This family covers all 2-generator, 2-relator groups where one relator specifies that a generator is an involution and the other relator has three syllables. Our proof relies upon detailed but general computations in the groups under question. The proof is theoretical, but based upon explicit proofs produced by machine for individual cases. Here we explain how we derived the general proofs from specific cases. The conjecture essentially addressed only the finite groups in the family. Here we extend the results to infinite groups, effectively determining when members of this family of finitely presented groups are simply isomorphic to a specific quotient.

2000 *Mathematics subject classification*: 20F05, 20-04.

Keywords and phrases: finitely presented groups, proofs, Todd–Coxeter coset enumeration, trivalent graphs.

1. Introduction

The groups $F^{a,b,c}$ are defined by

$$F^{a,b,c} = \langle r, s \mid r^2, rs^a rs^b rs^c \rangle.$$

Campbell, Coxeter and Robertson studied the groups in [2]. After determining the structure of various subclasses, they made 'the $F^{a,b,c}$ conjecture', which we state after some preliminaries. Combined with some results in [2], this conjecture completely describes the structure of all finite groups in the $F^{a,b,c}$ family in terms of a specific finite quotient that is fully understood.

This research was partially supported by the Australian Research Council and by the Engineering and Physical Sciences Research Council grant EP/C523229/01, 'Multidisciplinary Critical Mass in Computational Algebra and Applications'.

Define $n = a + b + c$ and $d = \gcd(a - b, b - c)$. The structure of the groups

$$H^{a,b,c} = \langle r, s \mid r^2, s^{2n}, rs^a rs^b rs^c \rangle$$

is completely determined in [2, Section 3]. If $n = 0$ then $F^{a,b,c}$ is clearly infinite. In [2] the groups $F^{a,b,c}$ are shown to be infinite when $t = \gcd(a, b, c) \neq 1$ except when $H^{a/t,b/t,c/t}$ is abelian, in which case $F^{a,b,c} \cong H^{a,b,c} \cong C_{2n}$. The conjecture addresses the remaining cases. Provided $\gcd(a, b, c) = 1$, $n \neq 0$ and $\gcd(d, 6) \neq 6$, the groups $H^{a,b,c}$ are finite metabelian groups. If $\gcd(a, b, c) = 1$ and $d \geq 6$ the groups $F^{a,b,c}$ are infinite [2].

The now proved $F^{a,b,c}$ conjecture is as follows. Suppose that $\gcd(a, b, c) = 1$ and $n \neq 0$. Let $\theta : F^{a,b,c} \to H^{a,b,c}$ be the natural homomorphism. Let $N = \ker \theta$. Then: $N = 1$ if $d = 1$ or 2; $N \cong C_2$ if $d = 3$; $N \cong Q_8$ if $d = 4$; and $N \cong \mathrm{SL}(2, 5)$ if $d = 5$.

The $d = 5$ case is resolved in [7] with the steps comprising the general proof first being observed to hold in specific small cases investigated by coset enumeration. Then in [8] we complete the proof of the conjecture by resolving the last three cases, $d = 2$, 3 and 4. (We also give an alternative proof for the case $d = 1$, which had been earlier proved in [3] and also, by a different technique, in [4].) Our proofs were found by using computer-generated proofs [6] for specific instances, which enabled us to observe the crucial role played by certain involutions.

In this paper we do two things. First, we explain how the proof came about. To do this, we outline the background material on computer-generated proofs, and then demonstrate how specific proofs led to the proof of the conjecture. We already generalized the result in [8, Section 3] for all $\gcd(a, b, c) \neq 1$ with $1 < d \leq 5$. Our second contribution is the extension of the result to its full generalization for $\gcd(a, b, c) = 1$, which proves when the map θ is an isomorphism, regardless of whether $F^{a,b,c}$ is finite or infinite.

2. Proof extraction after coset enumeration

The proofs of theorems that include machine computations may be opaque. This is especially true for proofs that rely on the collapse of a coset enumeration to one coset. Havas and Ramsay address this issue in [6] where they introduce the notions of proof words and proof certificates. Brief details follow.

Implicit in the underlying working of a coset enumeration are formal proofs that words ω in the group generators are actually in the subgroup, as shown by Leech [9]. The utility PEACE [10] (Proof Extraction After Coset Enumeration) has been developed to automate the production of such proofs. Thus PEACE produces *proofwords*, which can be regarded as certificates attesting to subgroup membership.

A fully expanded proofword consists of a product of subgroup generators and of conjugates of group relators (by group generators). The subgroup generators appear in the proofword as given in the input to the coset enumeration or as the formal inverses thereof. Relators (as given in the input) and their formal inverses may be cycled in proofwords. The final proofword consists simply of a string of group generators

or their inverses, with some substrings 'highlighted' by parentheses (group relators or their inverses, perhaps cycled) or square brackets (subgroup generators or their inverses).

By construction, ω and the proofword are equivalent and, since conjugates of relators are trivial in the group, the proofword is also equivalent to a product of subgroup generators. Thus, free reduction of the proofword produces ω, while reduction after cancelling the conjugates of relators gives a product of subgroup generators. The length of proofwords that can be found to show a given word is in a given subgroup exhibit great variability, depending on coset enumeration details. Further information and examples are provided in [6].

3. Lemma-based PEACE proofs

Once PEACE produces a proofword for an element h of the group, it has proved that h is also an element of the subgroup. The proofword is a product of subgroup generators and (possibly conjugated) relators, and, removing all brackets, freely reduces to h. Producing a step-by-step proof from this PEACE proof certificate is a matter of recursively dividing the proofword into disjoint products.

If p is the proofword, and q is obtained from p by removing the relators and reducing, then clearly p and q represent the same element and $pq^{-1} = 1$. Thus q is merely h written as a product of the subgroup generators.

Let us consider the word w that is obtained from pq^{-1}, where we have removed the square brackets indicating subgroup generators and reduced. This word w is a valid proofword itself: a proofword for the identity. For each subgroup generator that appeared in p, the inverse is found in q^{-1}, so in w the generator acts as a conjugator for the subword between itself and its inverse. The subword must be equivalent to the identity, so this conjugated subword is also trivial. Proving $w = 1$ is thus equivalent to providing a proof of $p = q$.

The word w can be broken up into disjoint products, such that

$$w = w_1^{x_1} w_2^{x_2} \cdots w_n^{x_n},$$

where x_i is a word over the group generators and conjugates w_i. Each w_i is either a relator, the inverse of a relator, or, like w, can be broken down further into disjoint products. Thus, the proofword w can be recursively broken down until the disjoint products are conjugates of relators.

A rooted tree can be created with w as the root and each vertex a subword. For a vertex v (where we would write $v = v_1^{x_{i_1}} v_2^{x_{i_2}} \cdots v_k^{x_{i_k}}$, each x_{i_j} being a word over the group generators), the children of v are the words $v_1, v_2, \ldots, v_k$ such that v_1 is the left-most child of v. The leaves of the tree are then relators or their inverses, each vertex in the tree is equivalent to the group identity, and we are in a position to build up our step-by-step proof.

A subtree can be seen as a proof for the word r at the root, where the last line of this proof is $1 = r$. Beginning with one branch in the tree, consider the leaf vertex v_j

and its parent,

$$v = v_1^{x_{i_1}} \cdots v_{j-1}^{x_{i_{j-1}}} v_j^{x_{i_j}} v_{j+1}^{x_{i_{j+1}}} \cdots v_k^{x_{i_k}}.$$

Our proof begins with the lines

$$\begin{aligned} 1 &= v_j \\ &= x_{i_j}^{-1} v_j x_{i_j}, \end{aligned}$$

where each line has been reduced.

Using the subtrees rooted at each v_n for $n \in \{1, \ldots, j-1\} \cup \{j+1, \ldots, k\}$, we can form the proofs for each of $1 = v_n$ and extend them to obtain $1 = x_{i_n}^{-1} v_n x_{i_n}$. Now, to obtain $1 = v$ in our proof, we need to successively apply each of the proofs of $1 = v_n^{x_{i_n}}$ for integers n from $j-1$ down to 1 and then for integers n from $j+1$ to k.

When considering the word $v_n^{x_{i_n}}$ for $n < j$, from the proof $1 = x_{i_n}^{-1} v_n x_{i_n}$, we form the lemma $a = b$ where b^{-1} is the subword of maximal length such that

$$x_{i_n}^{-1} v_n x_{i_n} = a b^{-1},$$

and the last line of our main proof is $1 = bw'$. Thus, by substituting a for b, the next line of our proof would be

$$1 = aw'.$$

For $n > j$, from the proof $1 = x_{i_n}^{-1} v_n x_{i_n}$, we form the lemma $c = d$ where c^{-1} is the subword of maximal length such that

$$x_{i_n}^{-1} v_n x_{i_n} = c^{-1} d,$$

and the last line of our main proof is $1 = w'c$. Thus, by substituting d for c, the next line of our proof is

$$1 = w'd.$$

Each substitution is equivalent to multiplying on either the right or the left by $x_{i_n}^{-1} v_n x_{i_n}$. Thus, iteratively applying the substitutions obtained from these lemmas for n from $j-1$ down to 1 and then for n from $j+1$ to k, we end up with a proof for

$$1 = v_1^{x_{i_1}} \cdots v_{j-1}^{x_{i_{j-1}}} v_j^{x_{i_j}} v_{j+1}^{x_{i_{j+1}}} \cdots v_k^{x_{i_k}} = v.$$

For a simple example, consider the group $F^{-1,1,3}$ presented by

$$F^{-1,1,3} = \langle r, s \mid r^2, rs^{-1}rs^1rs^3 \rangle,$$

and the subgroup $\langle rsr \rangle$. For the element s^6, PEACE produces the proofword

$$[r^{-1}s^{-1}r^{-1}](r^{-2})[rsr](r^{-2})(rs^{-1}rsrs^3)s^{-3}(r^{-2})(rs^{-1}rsrs^3)s^3,$$

which shows that $s^6 = 1$,

Removing the square brackets, we can divide the proofword up into disjoint products

$$\begin{aligned} a &= r^{-1}s^{-1}r^{-1}(r^{-2})rsr, \\ b &= (r^{-2})(rs^{-1}rsrs^3), \\ c &= s^{-3}(r^{-2})(rs^{-1}rsrs^3)s^3. \end{aligned}$$

We break these down further, giving

$$\begin{aligned} a_1 &= (r^{-2}), \\ b_1 &= (r^{-2}), \\ b_2 &= (rs^{-1}rsrs^3), \\ c_1 &= (r^{-2}), \\ c_2 &= (rs^{-1}rsrs^3). \end{aligned}$$

Then, the proofword is $(a_1)^{rsr}(b_1b_2)(c_1c_2)^{s^3}$. The necessary lemmas are the following.

LEMMA 3.1. *We have* $r^{-1} = s^{-1}rsrs^3$.

PROOF.

$$\begin{aligned} 1 &= rs^{-1}rsrs^3 \quad \text{(from } b_2 \text{ and } c_2\text{)} \\ r^{-1} &= s^{-1}rsrs^3. \end{aligned}$$

□

LEMMA 3.2. *We have* $r^{-1}sr = srs^3$.

PROOF.

$$\begin{aligned} 1 &= r^{-1}.r^{-1} \quad \text{(from } b_1\text{)} \\ &= r^{-1}s^{-1}rsrs^3 \quad \text{(from Lemma 3.1)} \\ r^{-1}sr &= srs^3. \end{aligned}$$

□

LEMMA 3.3. *We have* $r^{-1}s^{-1}r^{-1}srs^3 = s^6$.

PROOF.

$$\begin{aligned} 1 &= r^{-1}.r^{-1} \quad \text{(from } c_1\text{)} \\ &= r^{-1}s^{-1}rsrs^3 \quad \text{(from Lemma 3.1)} \\ &= s^{-3}(r^{-1}s^{-1}rsrs^3)s^3 \\ &= s^{-3}r^{-1}s^{-1}rsrs^6 \\ r^{-1}s^{-1}r^{-1}srs^3 &= s^6. \end{aligned}$$

□

Based on these lemmas our proof is thus:

$$\begin{aligned} 1 &= (r^{-2}) \quad (\text{from } a_1) \\ &= r^{-1}s^{-1}r^{-1}(r^{-2})rsr \quad (\text{from } a) \\ &= r^{-1}s^{-1}r^{-1}.r^{-1}sr \\ &= r^{-1}s^{-1}r^{-1}srs^3 \quad (\text{from Lemma 3.2}) \\ &= s^6 \quad (\text{from Lemma 3.3}). \end{aligned}$$

We count this proof as having four steps, comprising the three lemmas plus the segment above. We developed computer tools that produce such lemma-based proofs from proofwords. Further details are given in [11].

4. Applications to the groups $F^{a,b,c}$

In order to test the usefulness of PEACE and of our lemma-based proofs, we decided to apply them to a problem that had been attempted unsuccessfully by conventional methods. We studied the groups $F^{a,b,c}$. We conducted many experiments to find short proofwords for relevant relations, then converted shorter proofwords to lemma-based proofs.

For $d = 2$ the conjecture is proved if the relation $s^{2n} = 1$ can be deduced. We describe how we applied our tools to obtain a proof for this case. First we make a number of observations regarding PEACE-based proofs.

(1) Even starting with a short PEACE proofword, the lemma-based proofs obtained as described in Section 3 are long. In an instance with moderate length proofword, for $F^{3,5,7}$ the proof that $s^{30} = 1$ contains 270 steps, starting from a proofword with 1160 symbols (generators or inverses) comprising 67 relator applications, 30 subgroup generators and the rest being conjugating symbols.

(2) There is no use taking proofs such as that for $s^{30} = 1$ in $F^{3,5,7}$ and hoping to generalize them. Rather, we must seek to find significant ideas within such a proof.

(3) Most of the steps in the proofs found by PEACE are trivial. For example in the proof of $s^{30} = 1$ in $F^{3,5,7}$ considered above, the first few lemmas are

$$rs^7rs^3rs^5 = 1, \quad s^3rs^5 = s^{-2}r^{-1}s^{-3}r^{-1}s^{-2},$$
$$r^{-1}s^{-3}r^{-1}s^{-7}r^{-1}s^{-5} = 1, \quad s^2r^{-2}s^{-2} = 1.$$

These are all obvious. We therefore need to search for nontrivial facts in the computer-generated proofs. We looked at the PEACE-generated proofs of $s^{2k+8} = 1$ in $F^{1,3,k}$ for $k = 3, 5, 7, 11$. We made several observations.

(a) The difficulty (measured by proof length) did not seem to increase with increasing k.

(b) No expression longer than four syllables appeared in the proof that $s^{2k+8} = 1$, so, after using $r^2 = 1$, all words in the proof were essentially of the form $rs^\alpha rs^\beta rs^\gamma rs^\delta = 1$.

(c) The proofs seemed to use the fact that in this particular case $b - a = 2a$.

Using these observations, we were able to find a proof that $s^{2k+8} = 1$ with seven steps. We then tried to find a proof for the groups $F^{3,5,k}$. We observed that the proofs found by PEACE for the first few values of k did increase in difficulty with increasing k. Also, more than four syllables were involved, and the proof we had obtained for $F^{1,3,k}$ did not generalize.

However, we did observe a significant type of four-syllable relation in these PEACE proofs. For $F^{3,5,7}$ we observed relations of the form

$$(rs^{10}rs^5)^2 = 1, \quad (rs^{12}rs^3)^2 = 1, \quad (rs^{14}rs)^2 = 1.$$

They specify involutions in the group. They are part of a sequence. Proving that all relations in this sequence hold is enough to yield our desired result (since $(rs^0rs^{15})^2 = 1$ is in it and reduces to $s^{30} = 1$, as required). Examining different proofs for small k led us to observe that for $F^{3,5,k}$ relations of the form $(rs^{2m+3}rs^{k-2m+5})^2 = 1$ hold. Having discovered what we should try to prove in general, we used induction to obtain a proof. Since k is odd, $k + 5$ is even. Put $m = (k + 5)/2$ to obtain $s^{2k+16} = 1$ in $F^{3,5,k}$, as required.

We decided next to look at the groups $F^{a-2,a,a+2}$ for small odd a. The presentation here exhibited more symmetry, which helped us to recognize significant lemmas in the PEACE proofs. Again we observed that the proofs involved certain squares. This time the relations were of the form $(rs^{2m}rs^{3a-2m})^2 = 1$. Now $m = 0$ gives $s^{6a} = 1$ as required.

We proceeded to examine the groups $F^{a-2,a,a+4}$ followed by $F^{a-2,a,a+2m}$, again finding that we could construct a proof from a sequence of squares, although a harder induction was involved at each stage. Finally, generalizing to $F^{a-2j,a,a+2m}$, where $\gcd(j, m) = 1$, led to a proof of the conjecture for $d = 2$.

A similar investigation in the cases $d = 3$ and $d = 4$ eventually led to us completing the proof of the $F^{a,b,c}$ conjecture. We present the proof of the cases $d = 2, 3, 4$ in [8], where we also present an alternative proof for the case $d = 1$. These proofs are all based on use of our computer tools and the methods described in this section. (The conjecture had been earlier proved true when $d = 1$ in [3] and also, by a different technique, in [4].)

5. When is $F^{a,b,c} \cong H^{a,b,c}$?

The key question addressed by the $F^{a,b,c}$ conjecture is whether $F^{a,b,c} \cong H^{a,b,c}$ when $\gcd(a, b, c) = 1$. The proved conjecture answers this question for finite $F^{a,b,c}$, when $n \neq 0$ and $1 \leq d \leq 5$. If $n = 0$ then $F^{a,b,c}$ is infinite but the s^{2n} relation collapses so $F^{a,b,c} \cong H^{a,b,c}$. If $n \neq 0$, $d > 6$ and $\gcd(d, 6) \neq 6$ then $F^{a,b,c}$ is infinite but $H^{a,b,c}$ is finite, so $F^{a,b,c} \ncong H^{a,b,c}$. This leaves only $n \neq 0$ and $\gcd(d, 6) = 6$ unresolved. We show that in this case $F^{a,b,c} \ncong H^{a,b,c}$, which leads to the following theorem.

THEOREM 5.1. *Suppose* $\gcd(a, b, c) = 1$. *Then* $F^{a,b,c} \cong H^{a,b,c}$ *if and only if* $n = 0$, *or* $d = 1$ *or* $d = 2$.

Before proving the theorem, we briefly indicate how we came to the conclusion for $\gcd(a, b, c) = 1$, $n \neq 0$ and $\gcd(d, 6) = 6$. We investigated a large number of instances by writing straightforward GAP [5] and MAGMA [1] programs that tried to distinguish $F^{a,b,c}$ and $H^{a,b,c}$ for many explicit values of a, b, c (without insisting that $\gcd(a, b, c) = 1$). Typical distinguishing features came from studies of corresponding low-index subgroups and from studies of epimorphisms onto $\mathrm{PSL}(2, p)$ for various p. We discovered that, for every triple of values with $\gcd(a, b, c) = 1$, $n \neq 0$ and $\gcd(d, 6) = 6$ that we tried, we could prove the groups to be different. In the end we concluded that index-three subgroups suffice for this case.

PROOF. When $n = 0$ the s^{2n} relation collapses and $F^{a,b,c} \cong H^{a,b,c}$, so in the remainder of this proof we assume $n \neq 0$.

If $d = 1$ or $d = 2$ then $F^{a,b,c} \cong H^{a,b,c}$ by [8]. Also by [8], we see that $F^{a,b,c} \ncong H^{a,b,c}$ when $d = 3, 4$. By [7] $F^{a,b,c} \ncong H^{a,b,c}$ when $d = 5$, but we can show this last case directly.

Since $\gcd(a, b, c) = 1$, adding the relation $s^d = 1$ to $F^{a,b,c}$ gives the triangle group $(2, 3, d)$. Hence, when $d = 5$, $F^{a,b,c}$ has A_5 as a homomorphic image, so cannot be $H^{a,b,c}$ since when $\gcd(d, 6) \neq 6$, $H^{a,b,c}$ is metabelian by [2]. To complete the proof we must show that $F^{a,b,c} \ncong H^{a,b,c}$ when $\gcd(d, 6) = 6$. We note that in this case adding $s^6 = 1$ to both $F^{a,b,c}$ and $H^{a,b,c}$ only shows that both are infinite with the triangle group $(2, 3, 6)$ as a homomorphic image.

Let $a = b - 6p$ and $c = b + 6q$ where p, q are not necessarily coprime. Since $\gcd(a, b, c) = 1$, $(b, 6) = 1$. We consider separately the two cases $b = 1 + 6t$ and $b = 5 + 6t$. In the first of these cases we have $a = 1 + 6(t - p)$, $b = 1 + 6t$ and $c = 1 + 6(t + q)$.

Consider the subgroup K of index three in $F^{1+6(t-p),1+6t,1+6(t+q)}$ where r and s act on the cosets of K as the permutations (2 3) and (1 2) respectively, where $K = 1$, $K.s = 2$, and $K.sr = 3$. We obtain a presentation for K using Reidemeister–Schreier on generators x, y, z, where $1.r = x.1$, $2.s = y.1$ and $3.s = z.3$. Note that the relation $r^2 = 1$ gives $3.r = 2$. The presentation has the following four relators:

$$x^2, \quad xy^{3(t-p)}z^{1+6t}y^{1+3(t+q)}, \quad z^{1+6(t-p)}y^{1+3t}xy^{3(t+q)}, \quad y^{1+3(t-p)}xy^{3t}z^{1+6(t+q)}.$$

Eliminating x from the second of these gives the following relation matrix for the quotient K/K':

$$\begin{pmatrix} 2 + 12t + 6q & 2 + 12t - 12p \\ 2 + 12t + 6q - 3p & 2 + 12t - 6p \\ 2 + 12t + 3q - 3p & 2 + 12t + 6q - 6p \end{pmatrix}.$$

Moving the second row to the top and subtracting it from the other two rows reduces this matrix to

$$\begin{pmatrix} 2 + 12t + 6q - 3p & 2 + 12t - 6p \\ 3p & -6p \\ -3q & 6q \end{pmatrix}.$$

Taking the factor 2 out of the second column and then adding it to the first gives

$$2\begin{pmatrix} 3+18t+6q-6p & 1+6t-3p \\ 0 & -3p \\ 0 & 3q \end{pmatrix},$$

showing that $|K/K'| = 18(1+6t+2q-2p)\gcd(p,q)$.

To complete the proof in this case we must examine the extra relations that arise from adding the relation $s^{2n}=1$ to $F^{a,b,c}$ giving $H^{a,b,c}$, which, in this case, is $s^{6+12(3t-p+q)}=1$. We obtain two extra relations for the corresponding subgroup (L, say) of index three in $H^{a,b,c}$, namely

$$y^{3+6(3t-p-q)}=1, \quad z^{6+12(3t-p+q)}=1.$$

The relation matrix for the quotient L/L' has two extra rows and the reduction proceeds as before to give

$$\begin{pmatrix} 2+12t+6q-3p & 2+12t-6p \\ 3p & -6p \\ -3q & 6q \\ 3+18t-6p+6q & 0 \\ 0 & 6+36t-12q+12p \end{pmatrix}.$$

Again, divide the second column by 2 and add to the first column to obtain

$$2\begin{pmatrix} 3+18t+6q-6p & 1+6t-3p \\ 0 & -3p \\ 0 & 3q \\ 3+18t-6p+6q & 0 \\ 0 & 3+18t-6p+6q \end{pmatrix}.$$

It is now easy to see that the order of L/L' reduces to

$$6(1+6t+2q-2p)\gcd(1+6t,3p,3q),$$

showing that, in this case, $F^{a,b,c} \ncong H^{a,b,c}$ since $\gcd(1+6t,3p,3q)$ cannot be divisible by 3 so that

$$\begin{aligned} |L/L'| &= 6(1+6t+2q-2p)\gcd(1+6t,3p,3q) \\ \neq |K/K'| &= 18(1+6t+2q-2p)\gcd(p,q). \end{aligned}$$

The case $b=5+6t$ is similar. □

We have resolved the question as to when $F^{a,b,c} \cong H^{a,b,c}$ for $\gcd(a,b,c)=1$. It is interesting to consider the same question for $\gcd(a,b,c)\neq 1$, where various cases remain to be answered.

References

[1] 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://www.maths.usyd.edu.au:8000/u/magma/.

[2] C. M. Campbell, H. S. M. Coxeter and E. F. Robertson, 'Some families of finite groups having two generators and two relations', *Proc. Roy. Soc. Lond. Ser.* A **357** (1977), 423–438.

[3] C. M. Campbell and E. F. Robertson, 'On 2-generator 2-relation soluble groups', *Proc. Edinb. Math. Soc.* (2) **23** (1980), 269–273.

[4] ———, 'Groups related to $F^{a,b,c}$ involving Fibonacci numbers', in: *The Geometric Vein* (Springer, New York, 1981), pp. 569–576.

[5] The GAP Group, *GAP — Groups, Algorithms, and Programming*, Version 4.4, 2004. See also http://www.gap-system.org/.

[6] G. Havas and C. Ramsay, 'On proofs in finitely presented groups', in: *Groups, St Andrews, 2005*, London Mathematical Society Lecture Note Series, 340 (Cambridge University Press, Cambridge, 2007), pp. 457–474.

[7] G. Havas and E. F. Robertson, 'The $F^{a,b,c}$ conjecture, I', *Irish Math. Soc. Bull.* **56** (2005), 75–80.

[8] G. Havas, E. F. Robertson and D. C. Sutherland, 'The $F^{a,b,c}$ conjecture is true, II', *J. Algebra* **300** (2006), 57–72.

[9] J. Leech, 'Computer proof of relations in groups', in: *Topics in Group Theory and Computation* (Academic Press, New York, 1977), pp. 38–61.

[10] C. Ramsay, PEACE 1.100: Proof Extraction After Coset Enumeration, Technical Report 22, Centre for Discrete Mathematics and Computing, The University of Queensland, 2003.

[11] D. C. Sutherland, 'Computer-assisted proofs and the $F^{a,b,c}$ conjecture', PhD Thesis, University of St Andrews, 2005.

GEORGE HAVAS, ARC Centre for Complex Systems, School of Information Technology and Electrical Engineering, The University of Queensland, Queensland 4072, Australia
e-mail: havas@itee.uq.edu.au

EDMUND F. ROBERTSON, School of Mathematics and Statistics, University of St Andrews, North Haugh, St Andrews, Fife KY16 9SS, Scotland
e-mail: efr@st-andrews.ac.uk

DALE C. SUTHERLAND, School of Mathematics and Statistics, University of St Andrews, North Haugh, St Andrews, Fife KY16 9SS, Scotland