The $F^{a,b,c}$ conjecture is true

Edmund F Robertson

University of St Andrews

Groups in Galway

19 May 2007

efr@st-and.ac.uk

http://www-history.mcs.st-and.ac.uk/~edmund/

Donald Coxeter (University of Toronto) wrote to John Leech (University of Stirling) in December 1974 about the groups $F^{a,b,c}$.

He wanted to know the orders of the groups

$$F^{a,b,c} = < r, s \mid r^2 = r s^a r s^b r s^c = 1 >$$

for small values of $|a|$, $|b|$ and $|c|$.

John Leech asked Colin Campbell and myself to help. We began to correspond with Coxeter.

In a letter to CMC and EFR, Coxeter explained why the groups were interesting:

"The groups $F^{a,b,c}$ arose because some of them have Cayley diagrams which are '0-symmetric' or 'faithful'. I am writing a paper on such groups jointly with Foster, Frucht and Watkins. This is progressing very slowly."

R M Foster was a leading electrical engineer, who became interested in symmetrical graphs that could be used as electrical networks, in the 1920s.

At a conference held in Waterloo, Ontario, in April, 1966, Foster presented a census of symmetric trivalent graphs with up to 400 vertices. This document, of which only a few copies were available, became part of the folklore of the subject. Coxeter became interested. [In fact *The Foster census* was published in 1988 with a foreword by Coxeter.]

The groups $F^{a,b,c}$ yield many examples of graphs of this type with one generating involution and these examples are studied in the book.
In a letter written to Coxeter on 7 October 1975, Colin and I made "the $F^{a,b,c}$ conjecture" which I will now state after some preliminaries:

Let

$$n = a + b + c$$

$$d = (a - b, b - c).$$

First we classified the groups

$H^{a,b,c} =$

$$< r, s \mid r^{2} = s^{2n} = rs^{a}rs^{b}rs^{c} = 1>.$$

Let $(a, b, c) = 1$. Then if $n \neq 0$ and $(d, 6) \neq 6$, the groups $H^{a,b,c}$ are finite metabelian groups.

If $(d, 6) = 6$, then $H^{a,b,c}$ is infinite.

If $n = 0$ the groups $F^{a,b,c}$ are infinite.

If $t = (a, b, c) \neq 1$ then $F^{a,b,c}$ is infinite unless $H^{a/t,b/t,c/t}$ is abelian in which case

$F^{a,b,c} \cong H^{a,b,c} \cong C_{2n}$

The $F^{a,b,c}$ conjecture is as follows:

Let N be the kernel of the natural homomorphism from $F^{a,b,c}$ to $H^{a,b,c}$. Then

(i) $N = 1$ if $d = 1$

(ii) $N = 1$ if $d = 2$

(iii) $N \cong C_2$ if $d = 3$

(iv) $N \cong Q_8$ if $d = 4$

(v) $N \cong SL(2,5)$ if $d = 5$

The conjecture, and the complete description of the groups $H^{a,b,c}$, appeared in print in 1977 in a paper by CMC, EFR and Coxeter.

In a paper in the Proceedings of the Edinburgh Mathematical Society that appeared in 1980, CMC and EFR proved (i) to be true.

In 1984 Colin and myself published our fifth paper on the groups $F^{a,b,c}$. We were, however, still far from proving (ii), (iii), (iv) and (v).

In a paper published in 1985 Manley Perkel identified certain subgroups of the group of affine linear transformations with the groups $F^{a,b,c}$. Using this he was able to show that the orders of certain of the groups involved Mersenne primes, Fermat primes, or semi-Fermat primes.

In 1997 Fulvia Spaggiari reproved some of the results of our 1977 paper with Coxeter. She also observed that $F^{a,b,b}$ are fundamental groups of closed connected orientable 3-manifolds of Heegaard genus two.

In 2003-2004 I had study leave and decided that I better have another attempt at proving the conjecture. George Havas and EFR proved part (v) of the conjecture.

The proof proceeds as follows:

1. s^{2n} commutes with rs^5r.

2. s^{10n} is central in $F^{a,b,c}$.

3. $e = s^{2n}$, $f = rs^{2n}r$ generate N.

4. e^5, f^5, $(ef)^3$ and $(fe^2)^2$ are central in N.

5. Put $M = < e^5, f^5, (ef)^3, (fe^2)^2 >$. Then

$N/M \cong A_5$.

6. N is perfect.

7. M is contained in the multiplier of A_5.

8. $N \cong SL(2,5)$.

This method totally fails for the cases $d = 2, 3$ and 4 since in each case d fails to be coprime to $2n$.

The next idea was to look and see how the computer was able to solve small cases. Leech, before his involvement with $F^{a,b,c}$, had developed a method of converting a computer coset enumeration into an algebraic proof. He had described such methods in his lectures *Computer proof of relations in groups* given at Galway in 1973 (published 1977).

George Havas (with Colin Ramsay) had written a package PEACE (Proof Extraction After Coset Enumeration) that produced an algebraic proof after completing a coset enumeration.

PEACE proof that $s^{22} = 1$ in $F^{1,3,7}$.

(Note: Upper case letters are inverses of lower case letters) It is called a "proofword".

sssssssssssssrsr(*sssrsssssssrsr*)*RSRSSSS*

SSS(*RR*)*S*(*RR*)*rsr*(*sssrsssssssrsr*)*RSRSSSSS*

SSRSR(*rr*)*RSR*(*rr*)(*RSRSSSSSSSRSSS*)*sssrss*

ssssrsr(*sssrsssssssrsr*)*RSRSSSSSSr*(*RSRSS*

SSSSSRSSS)*RR*(*rr*)*SSSrsr*(*RR*)*rsr*(*RR*)*rsrss*

sssssrsr(*RSRSSSSSSSRSSS*)*RSRSSS*(*RR*)*rr*

(*sssrsssssssrsr*) *RRS*(*RR*)*SSS*(*sssrsssssssrsr*)

RSR

Freely cancel as it stands. One obtains s^{22}.

Remove the relations inside round brackets. Now freely cancel to obtain 1. Hence $s^{22} = 1$.

Now this proof convinces any doubters that the computer is correct, but it provides no insight. My Ph.D. student Dale Sutherland wrote GAP code to translate these proofwords into a lemma based line by line proof. One could now "understand" the machine based proof and GH, EFR and Dale attacked $F^{a,b,c}$.

First we make a number of observations regarding Dale's 'lemma version' of PEACE/GAP based proofs.

1. Even starting with a short PEACE proofword, the lemma based proofs obtained from GAP will still be long. For example, for $F^{3,5,7}$ the proof that $s^{30} = 1$ contains 270 steps.

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

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

$$r\, s^{7}\, r\, s^{3}\, r\, s^{5} = 1$$

$$s^{3}\, r\, s^{5} = s^{-2}\, r^{-1}\, s^{-3}\, r^{-1}\, s^{-2}$$

$$r^{-1}\, s^{-3}\, r^{-1}\, s^{-7}\, r^{-1}\, s^{-5} = 1$$

$$s^{2}\, r^{-2}\, s^{-2} = 1.$$

These are all obvious. We need to search for non-trivial facts in the PEACE/GAP generated proofs.

We looked at the PEACE/GAP 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 did not seem to increase with increasing k.

b. No expression longer than 4 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

$$rs^p rs^q rs^r rs^t = 1.$$

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

Using these facts 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/GAP for the first few values of k did increase in difficulty with increasing k. More than 4 syllables were involved. The proof for $F^{1,3,k}$ did not generalise.

However we did observe a significant type of that relation which appeared in these PEACE/GAP proofs. For $F^{3,5,7}$ we observed relations of the form

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

$$(rs^{14}rs)^2 = 1$$

held. Proving that relations in such a sequence all hold is sufficient since $(rs^{0}rs^{15})^2 = 1$ is a member of the sequence and this reduces to $s^{30} = 1$ as required. Examining different proofs for small k led us to observe that $F^{3,5,k}$ had relations of the form

$$(rs^{2m+3}rs^{k-2m+5})^2 = 1$$

We used induction to obtain a proof of this result. Since k is odd, $k + 5$ is even. Put $m = (k + 5)/2$ to obtain $s^{2k+16} = 1$ 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 recognise significant lemmas in the PEACE/GAP 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 then 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, generalising to $F^{a-2j,a,a+2k}$ where $(j, k) = 1$ led to a proof of the conjecture for $d = 2$.

A similar method led to a proof in the cases $d = 3$ and $d = 4$. In the end it all came down to proving the following.

Write the groups in the form $F^{a-jd,a,a+kd}$ where $(j, k) = 1$. Then, we showed that, for all i

$$(rs^{2a+d(i+k-j)}\, rs^{a-id})^2 = 1$$

$$(rs^{2a-id}\, rs^{a+d(i+k-j)})^2 = 1$$

From this, with some effort, cases $d = 1, 2, 3, 4$ can all be deduced.

What happens if $(a, b, c) \neq 1$? We know that $F^{a,b,c}$ is infinite but we can still ask: Is $F^{a,b,c} \cong H^{a,b,c}$?

Theorem. Suppose $(a, b, c) \neq 1$. Then if $d \mid 2a$ we have $F^{a,b,c} \cong H^{a,b,c}$.

Corollary If $(a, b, c) \neq 1$ and d is prime then have $F^{a,b,c} \cong H^{a,b,c}$.

Theorem Suppose $(a, b, c) \neq 1$. Then if d does not divide $6a$ then $F^{a,b,c}$ is not isomorphic to $H^{a,b,c}$.

There is a gap between the two theorems!

The first ‘problem’ is $d = 6$.

If $(a, 6) = 2$ we have no answer.

However we can find index 4 subgroups in $F^{a,b,c}$ and $H^{a,b,c}$ with different abelian quotients proving in this case that they are non-isomorphic.

Some applications:

In 1990 CMC, EFR and Peter Williams proved that the group $\mathsf{PSL}(2, p^n)$, p and odd prime, could be presented with three generators and seven relations. The significance here is that the number of relations is bounded, it is independent of p and does not increase with n.

This makes heavy use of the results on $\mathsf{H}^{a,b,c}$.
The way this works is that a trinomial in $\mathsf{GF}(p^n)$ translates into a relation in $\mathsf{PSL}(2, p^n)$ which, together with one more relation, allows us to deduce n commutator relations (as in the proof that the derived group of $\mathsf{H}^{a,b,c}$ is abelian).

Korchagina and Lubotzky call this trick of replacing n commutator relations by 2 relations the CRW-trick. They use if several times, and use the 1990 CMC, EFR, PDW theorem, in proving that every untwisted simple group of Lie type of rank m over $GF(p^n)$ can be presented with at most $C(m)$ relations (i.e. independent of p and n). (To appear 2006).

They conjecture this holds for twisted simple groups of Lie type.

They pose the problem of whether there is a constant C independent of n and m such that a simple group of Lie type of rank m over $GF(p^n)$ can be presented with at most C relations.

In *Presentations of finite simple groups: a quantitative approach* by Guralnick, Kantor, Kassabov and Lubotzky, it is shown that every finite simple group (except perhaps the Ree groups) has a presentation with a bounded number of relators (certainly less than 500). Again this makes heavy use of the CRW-trick.