ANDREWS-CURTIS AND TODD-COXETER PROOF WORDS

GEORGE HAVAS and COLIN RAMSAY[1]

School of Computer Science and Electrical Engineering,
The University of Queensland, Queensland 4072, Australia
Email: havas@csee.uq.edu.au and cram@csee.uq.edu.au

Abstract

Andrews and Curtis have conjectured that every balanced presentation of the trivial group can be transformed into a standard presentation by a finite sequence of elementary transformations. It can be difficult to determine whether or not the conjecture holds for a particular presentation. We show that the utility PEACE, which produces proofs based on Todd-Coxeter coset enumeration, can produce Andrews-Curtis proofs.

1 Introduction

There are infinitely many finite presentations of the trivial group, and the problem of determining whether or not a given presentation is of the trivial group is, in general, unsolvable. A presentation $\langle x_1, \ldots, x_n \,|\, r_1, \ldots, r_m \rangle$ is called *balanced* if $m = n$. The *standard* n-generator presentation of the trivial group is $\langle x_1, \ldots, x_n \,|\, x_1, \ldots, x_n \rangle$, and one method of proving that a balanced presentation represents the trivial group is to reduce it to a standard presentation.

Consider the following transformations on the n-tuple of relators $(r_1, \ldots, r_n)$:
(AC1) replace r_i by $r_i r_j$, for some $j \neq i$;
(AC2) replace r_i by r_i^{-1};
(AC3) replace r_i by $w^{-1} r_i w$, for some word w in the generators.
Each of these *AC-transformations* leaves r_k fixed for all $k \neq i$. Andrews and Curtis [1] conjectured that any balanced presentation of the trivial group can be transformed to the standard presentation by a sequence of AC-transformations. Such a sequence of transformations is called an *AC-proof*.

"The prevalent opinion is that the conjecture is false" [2], but no counterexample has been proved to exist. This makes the study of potential counterexamples interesting.

Further, generating AC-proofs is not easy, and Miasnikov [5] describes a genetic algorithm designed to produce such proofs. Using this, Miasnikov and Myasnikov [6] have shown that the conjecture holds for all balanced presentations of the trivial group on two generators with the total length of the relators at most twelve. They also note that the presentation $\langle a, b \,|\, a^3 = b^4, aba = bab \rangle$, of total length thirteen, is a smallest potential counterexample to the Andrews-Curtis conjecture at present. Havas and Ramsay [3] prove that it is unique up to AC-equivalence.

[1]Both authors were partially supported by the Australian Research Council

The Todd-Coxeter coset enumeration procedure [8] is a systematic method for enumerating, in a given finitely presented group, the cosets of a given finitely presented subgroup. Implicit in the workings of such an enumeration are formal proofs that particular words in the generators are in the subgroup (see, for example, Leech [4]). The utility PEACE [7] (proof extraction after coset enumeration) has been developed to automate the production of such proofs. PEACE produces *proof words* (see below), which can be regarded as certificates attesting to subgroup membership.

For enumeration over the trivial subgroup, proof words produced by PEACE consist of products of conjugates of relators and of their formal inverses, and AC-proofs can be viewed the same way. It is natural to ask whether or not PEACE proof words correspond to AC-proofs. This question seems to be difficult, but we exhibit some cases where we can obtain a constructive positive solution.

2 An AC-proof and its proof words

The length thirteen presentation quoted above is one of a well-known series of balanced presentations for the trivial group, $\langle\, a, b \,|\, a^n = b^{n+1}, aba = bab \,\rangle$, $n \geq 0$. Their triviality for $n = 0, 1$ is obvious, while for $n \geq 2$ some work is required. To illustrate our basic technique, we take the case $n = 1$ as our example. So, let $G = \langle\, a, b \,|\, aBB, abaBAB \,\rangle$, where we adopt the convention that $A = a^{-1}$ and $B = b^{-1}$.

Although the triviality of G is obvious, producing an AC-proof of this requires a little work with pencil and paper. One such proof is given in Table 1; this is not the natural proof which starts by eliminating occurrences of the first generator from the second relator, but more like the kind of proof that might be produced by machine. The r_1 and r_2 columns in the table illustrate the normal proof extraction process, where we freely cancel adjacent generator/inverse pairs as they occur. The $r_2^\star$ column illustrates an alternative where the relators are protected from cancellation by bracketing, and we only cancel outside of the relators. The word produced at the eighth transformation (or *move*), $w = A(abaBAB)b(aBB)b(bbA)BB(bbA)a$, is a proof word that b is trivial in G. To see this, simply note that w is a product of conjugates of relators (or their formal inverses) of G (so is trivial), and that it freely reduces to b.

Proof words are a convenient way of presenting a proof succinctly. They can be generated by a variety of methods, and checking them is a simple mechanical process which depends only on the presentation and the group axioms. A proof word for a in G is readily extracted from Table 1, and is simply $(aBB)ww$. We call such proof words generated by AC-transformations *AC-proofwords*.

3 Some PEACE proofs and their proof words

PEACE extracts proof words from a successful coset enumeration by storing additional information in the coset table as it is constructed. This additional information is used to continually rewrite the word to be proved until a proof word is

Table 1. An AC-proof for G

move	r_1	r_2	$r_2^\star$
0: -	aBB	$abaBAB$	$(abaBAB)$
1: $r_1 \to br_1B$	$baBBB$	$abaBAB$	$(abaBAB)$
2: $r_2 \to r_2r_1$	$baBBB$	$abaBBBB$	$(abaBAB)b(aBB)B$
3: $r_1 \to r_1^{-1}$	$bbbAB$	$abaBBBB$	$(abaBAB)b(aBB)B$
4: $r_1 \to br_1B$	$bbbbABB$	$abaBBBB$	$(abaBAB)b(aBB)B$
5: $r_2 \to r_2r_1$	$bbbbABB$	aB	$(abaBAB)b(aBB)b(bbA)BB$
6: $r_1 \to BBr_1bb$	bbA	aB	$(abaBAB)b(aBB)b(bbA)BB$
7: $r_2 \to r_2r_1$	bbA	abA	$(abaBAB)b(aBB)b(bbA)BB(bbA)$
8: $r_2 \to Ar_2a$	bbA	b	$A(abaBAB)b(aBB)b(bbA)BB(bbA)a$
9: $r_1 \to r_1^{-1}$	aBB	b	
10: $r_1 \to r_1r_2$	aB	b	
11: $r_1 \to r_1r_2$	a	b	

obtained. In general, these proof words consist of products of conjugates of relators and subgroup generators. If the subgroup is trivial then only the conjugated relators are present, as in the AC-proofwords.

The particular proof word generated by a coset enumeration depends on the exact sequence of operations during the enumeration, the additional information stored, and the rewriting. So the proofs generated by PEACE are very variable. However, it readily produces a variety of proof words that b is trivial in G where the proof words contain the same mix of four relators as w. Some examples are:

$ba(Abb)AB(baBABa)(Abb)b(BBa)B$;

$b(Abb)B(BabaBA)ba(Abb)B(BBa)bAB$;

$B(aBABab)AB(bbA)a(BaB)Aba(bAb)b$.

Note that PEACE often uses a relator in a cyclically permuted and/or inverted form. However, any cyclings are easily removed by conjugation. (PEACE does not do this automatically, but such a feature could easily be added.) For the examples above, this yields:

$b(bbA)BA(abaBAB)(bbA)abA(aBB)aB$;

$bA(bbA)aBB(abaBAB)bb(bbA)aBA(aBB)abAB$;

$BBA(abaBAB)abAB(bbA)aB(aBB)bAbaB(bbA)bb$.

Although none of these match w, they are similar. The question now is whether or not there is a sequence of AC-transformations which will generate one of these. Or, can one of these proof words from PEACE be used to generate an AC-proofword, and thus an AC-proof?

Note how the proof words exhibited here all contain the relator $abaBAB$ exactly once. This observation suggests the following procedure for proving that a proof word is an AC-proofword: append copies of aBB, inverted and/or conjugated as appropriate, to $abaBAB$; if there are any copies of aBB prefixing $abaBAB$, then invert the current relator, repeat the previous step (appending the inverse of what is required), and then invert the result. Applying this to the first example above readily yields the AC-transformation sequence in Table 2.

Thus, we see that the proof word $u = b(bbA)BA(abaBAB)(bbA)abA(aBB)aB$

Table 2. Generating a specific AC-proofword

move	$r_1^\star$	$r_2^\star$
0: -	(aBB)	$(abaBAB)$
1: $r_1 \to r_1^{-1}$	(bbA)	$(abaBAB)$
2: $r_2 \to r_2 r_1$	(bbA)	$(abaBAB)(bbA)$
3: $r_1 \to r_1^{-1}$	(aBB)	$(abaBAB)(bbA)$
4: $r_1 \to abAr_1aBA$	$abA(aBB)aBA$	$(abaBAB)(bbA)$
5: $r_2 \to r_2 r_1$	$abA(aBB)aBA$	$(abaBAB)(bbA)abA(aBB)aBA$
6: $r_2 \to r_2^{-1}$	$abA(aBB)aBA$	$abA(bbA)aBA(aBB)(babABA)$
7a: $r_1 \to aBAr_1abA$	(aBB)	$abA(bbA)aBA(aBB)(babABA)$
7b: $r_1 \to abr_1BA$	$ab(aBB)BA$	$abA(bbA)aBA(aBB)(babABA)$
8: $r_2 \to r_2 r_1$	$ab(aBB)BA$	$abA(bbA)aBA(aBB)(babABA)ab(aBB)BA$
9: $r_2 \to r_2^{-1}$	$ab(aBB)BA$	$ab(bbA)BA(abaBAB)(bbA)abA(aBB)aBA$
10: $r_2 \to Ar_2a$	$ab(aBB)BA$	$b(bbA)BA(abaBAB)(bbA)abA(aBB)aB$

produced automatically by PEACE is an AC-proofword. (In fact, Bub is also an AC-proofword, and is slightly shorter.) Since u freely reduces to b, it is a trivial matter to extend the sequence of AC-transformations given in Table 2 to an AC-proof for G. Similar manipulations readily yield AC-proofs from the other two examples.

4 A difficult example

In [5], Miasnikov notes that the four length twelve presentations $\langle\, a, b \,|\, Ab^2a = b^3, a = b^{\pm 1}ab^{\pm 1}A \,\rangle$ are particularly difficult. Let $G_2 = \langle\, a, b \,|\, AbbaBBB, aabAB \,\rangle$. Miasnikov gives a proof for this, in the form $\langle\, x, y \,|\, yxYXX, XyyxYYY \,\rangle$, in nineteen moves. Two of these moves are not in (AC1)–(AC3) but are *Whitehead automorphisms* (see [9]), so this is not an AC-proof. However, the Whitehead automorphisms can be replaced by AC-transformations, albeit at the expense of increasing the length of the proof.

Let $r = AbbaBBB$, $s = aabAB$, $R = r^{-1}$ and $S = s^{-1}$, and consider the following proof word for a in G_2 produced by PEACE,

$$(R)A(S)aabA(S)aB(S)a(s)bA(s)aBAA(s)a(r)AA(s)a.$$

From this, we were able to extract the nineteen move AC-proof given in Table 3. Both this proof and the one given by Miasnikov can be shortened by noting that the first few moves simply invert or cycle the relators, and so can be eliminated by starting with the presentations in slightly different forms.

We found our proof word by generating a number of PEACE proofs for the four presentations in the family, extracting the templates of the proof words (the one given has template $RSSSsssrs$) and then comparing these with a list of possible templates (easily generated by a breadth-first search using the (AC1) and (AC2) moves). The procedure has a low success rate, seemingly due to the paucity of templates which can be generated by AC-moves, but any match gives a candidate

Table 3. An AC-proof for G_2

move	r_1	r_2
0: -	$AbbaBBB$	$aabAB$
1: $r_1 \rightarrow r_1^{-1}$	$bbbABBa$	$aabAB$
2: $r_2 \rightarrow r_2^{-1}$	$bbbABBa$	$baBAA$
3: $r_2 \rightarrow Ar_2a$	$bbbABBa$	$AbaBA$
4: $r_1 \rightarrow r_1r_2$	$bbbABaBA$	$AbaBA$
5: $r_2 \rightarrow abr_2BA$	$bbbABaBA$	$abAbaBABA$
6: $r_1 \rightarrow r_1r_2$	$bbABA$	$abAbaBABA$
7: $r_2 \rightarrow aaBAr_2abAA$	$bbABA$	$abaBAAA$
8: $r_1 \rightarrow r_1r_2$	$bAAA$	$abaBAAA$
9: $r_2 \rightarrow AAAr_2aaa$	$bAAA$	$AAbaB$
10: $r_2 \rightarrow r_2r_1$	$bAAA$	$AAbAA$
11: $r_2 \rightarrow r_2^{-1}$	$bAAA$	$aaBaa$
12: $r_2 \rightarrow ar_2A$	$bAAA$	$aaaBa$
13: $r_1 \rightarrow r_1r_2$	a	$aaaBa$
14: $r_2 \rightarrow r_2^{-1}$	a	$AbAAA$
15: $r_2 \rightarrow ar_2A$	a	$bAAAA$
16–19: $r_2 \rightarrow r_2r_1$	a	b

proof word. There are usually several sequences of AC-transformations which yield a given template (these can be extracted from the breadth-first search), and we now have to find one where some sequence of conjugations yields the required proof word.

5 Conclusions

We have shown that it is possible to extract AC-proofs from the proofs produced by PEACE. However our technique is a trifle ad hoc, depending as it does on testing the pattern of the relators in a PEACE proof word against a set of possible AC-proofwords and then attempting to match up the conjugation. Only in the case where there are two relators and the PEACE proofs contain one of the relators exactly once can we consistently extract an AC-proof. We have no systematic method of determining whether or not the extraction is possible in general or performing it if it is. There does not seem to be any general method for determining whether or not a given proof word can be generated by a sequence of AC-transformations and, in fact, there does not seem to be any nice characterisation of the words which can be generated by a sequence of AC-transformations. Progress in these areas might enable us to extend the work here, and use the techniques described to eliminate some of the potential counterexamples to the Andrews-Curtis conjecture.

References

[1] J.J. Andrews and M.L. Curtis. Free groups and handlebodies. Proceedings of the American Mathematical Society, 16:192–195, 1965.
[2] G. Baumslag, A.G. Myasnikov and V. Shpilrain. Open problems in combinatorial group

theory. In Robert H. Gilman (ed.), *Groups, languages and geometry*, Contemporary Mathematics 250, American Mathematical Society, 1999, 1–27.

[3] G. Havas and C. Ramsay. Breadth-first search and the Andrews-Curtis conjecture. Technical Report 23, Centre for Discrete Mathematics and Computing, The University of Queensland, 2001.

[4] John Leech. Computer proof of relations in groups. In Michael P.J. Curran (ed.), *Topics in Group Theory and Computation*, pp. 38–61. Academic Press, 1977.

[5] A.D. Miasnikov. Genetic algorithms and the Andrews-Curtis conjecture. The International Journal of Algebra and Computation, 9(6):671–686, 1999.

[6] A.D. Miasnikov and A.G. Myasnikov. Balanced presentations of the trivial group on two generators and the Andrews-Curtis conjecture. In W.M. Kantor and A. Seress (eds.), *Groups and Computation III*, Ohio State University Mathematical Research Institute Publications 8, Walter de Gruyter, 2001, 257–263.

[7] Colin Ramsay. PEACE 1.000: Proof Extraction after Coset Enumeration. Technical Report 22, Centre for Discrete Mathematics and Computing, The University of Queensland, 2001.

[8] J.A. Todd and H.S.M. Coxeter. A practical method for enumerating cosets of a finite abstract group. Proceedings of the Edinburgh Mathematical Society, 5:26–34, 1936.

[9] J.H.C. Whitehead. On equivalent sets of elements in a free group. Annals of Mathematics, 2nd Ser., 37(4):782–800, 1936.