Kalpa Publications in Computing

Volume 18, 2024, Pages 131–136

LPAR 2024 Complementary Volume

Towards computer-assisted proofs of parametric Andrews-Curtis simplifications, II

Alexei Lisitsa

University of Liverpool, Liverpool, UK
a.lisitsa@liverpool.ac.uk

Abstract

We present recent developments in the applications of automated theorem proving in the investigation of the Andrews-Curtis conjecture. We demonstrate previously unknown simplifications of groups presentations from a parametric family $MS_n(w_*)$ of trivial group presentations for $n = 3, 4, 5, 6, 7, 8$ (subset of well-known Miller-Schupp family). Based on the human analysis of these simplifications we formulate two conjectures on the structure of simplifications for the infinite family $MS_n(w_*)$, $n \geq 3$.

This is an extended and updated version of the abstract [11] presented at AITP 2023 conference.

1 Introduction

The Andrews-Curtis conjecture (ACC) [1] is one of the most well-known open problems in combinatorial group theory. In short, it states that every balanced presentation of the trivial group can be transformed into a trivial presentation by a sequence of simple transformations. Various computational approaches have been proposed for the efficient search of such simplifications, see e.g. [4, 12, 14, 7, 5]. Still there are infinite families of balanced trivial group presentations which remain potential counterexamples to the conjecture, that is for which the required simplifications are not known.

For a group presentation $\langle x_1, \ldots, x_n; r_1, \ldots r_m \rangle$ with generators x_i, and relators r_j, consider the following transformations.

AC1 Replace some r_i by r_i^{-1}.

AC2 Replace some r_i by $r_i \cdot r_j$, $j \neq i$.

AC3 Replace some r_i by $w \cdot r_i \cdot w^{-1}$ where w is any word in the generators.

AC4 Introduce a new generator y and relator y or delete a generator y and relator y.

Two presentations g and g' are called *Andrews-Curtis equivalent (AC-equivalent)* if one of them can be obtained from the other by applying a finite sequence of transformations of the types (AC1) - (AC3). Two presentations are stably AC-equivalent if one of them can be obtained from the other by applying a finite sequence of transformations of the types (AC1)–(AC4). A presentation $\langle x_1, \ldots, x_n; r_1, \ldots r_m \rangle$ is called *balanced* if $n = m$.

Conjecture 1 (Andrews-Curtis [1]). *If $\langle x_1, \ldots, x_n; r_1, \ldots r_n\rangle$ is a balanced presentation of the trivial group it is AC-equivalent to the trivial presentation $\langle x_1, \ldots, x_n; x_1, \ldots x_n\rangle$*

The weak form of the conjecture states that every balanced presentation for a trivial group is stably AC-equivalent (i.e. transformations AC4 are allowed) to the trivial presentation. Both variants of the conjecture remain open and challenging problems.

1.1 Miller-Schupp presentations

In [6] the authors have defined an infinite family of balanced presentations of the trivial group $MS_n(w) = \langle a, b \mid a^{-1}b^n a = b^{n+1}, a = w\rangle$, where $n \geq 1$ and w is a word which has exponent sum 0 on a. Since these presentations have been used as a test-bed for testing various computational methods for finding AC-trivializations, see e.g. [4, 12, 13, 3]. Both novel trivializations and some remaining open cases for n=2 can be found in [13]. Subfamily $MS_n(w_*)$ for a fixed $w_* = b^{-1}aba^{-1}$, $n \geq 1$ was considered in [4, 12, 3]. The trivializations for $MS_n(w_*)$, $n \leq 2$ were demonstrated in [4, 12], while in [3] it was shown that $MS_3(w_*)$ is *stably* AC- trivializable. The AC-trivializability of cases of $MS_n(w_*)$ with $n \geq 3$ remained open [3].

Automated theorem proving for AC-simplifications

In [8, 9, 10] we have developed an approach based on using automated deduction in first-order logic in the search of trivializations and have shown that the approach is very competitive. In our approach we formalized the AC-transformations in terms of term rewriting modulo group theory and first-order deduction. In this section we outline the approach largely following the presentation in [9]

Let T_G be the equational theory of groups. In what follow we consider only balanced presentations of the dimension $n = 2$

For each $n \geq 2$ we formulate a term rewriting system modulo T_G, which captures AC-transformations of presentations of dimension n. We start with dimension $n = 2$.

For an alphabet $A = \{a_1, a_2\}$ a term rewriting system ACT_2 consists the following rules:

R1L $f(x, y) \to f(r(x), y))$

R1R $f(x, y) \to f(x, r(y))$

R2L $f(x, y) \to f(x \cdot y, y)$

R2R $f(x, y) \to f(x, y \cdot x)$

R3L$_i$ $f(x, y) \to f((a_i \cdot x) \cdot r(a_i), y)$ for $a_i \in A, i = 1, 2$

R3R$_i$ $f(x, y) \to f(x, (a_i \cdot y) \cdot r(a_i))$ for $a_i \in A, i = 1, 2$

The term rewriting system ACT_2 gives rise to the rewrite relation $\to_{ACT}$ on the set of all terms defined in the standard way [2]. For terms t_1, t_2 in groups vocabulary we write $t_1 =_G t_2$ if equality $t_1 = t_2$ is derivable in T_G. We extend $=_G$ homomorphically by defining $f(t_1, t_2) =_G f(s_1, s_2)$ iff $t_1 =_G s_1$ and $t_2 =_G s_2$. Denote by $[t]_G$ the equivalence class of t wrt $=_G$, that is $[t]_G = \{t' \mid t =_G t'\}$.

Then rewrite relation $\to_{ACT/G}$ for ACT modulo theory T_G is defined [2] as follows: $t \to_{ACT/G} s$ iff there exist $t' \in [t]_G$ and $s' \in [s]_G$ such that $t' \to_{ACT} s'$.

Claim 1 (on formalization). *The notion of rewrite relation $\to_{ACT/G}$ captures adequately the notion of AC-rewriting, that is for presentations p_1 and p_2 we have $p_1 \to^*_{AC} p_2$ iff $t_{p_1} \to^*_{ACT/G}$. Here t_p denotes a term encoding of a presentation p, that is for $p = \langle a_1, a_2 \mid t_1.t_2 \rangle$ we have $t_p = f(t_1, t_2)$.*

The term rewriting system ACT_2 can be simplified without changing the transitive closure of the rewriting relation. Reduced term rewriting system $rACT_2$ consists of the following rules:

R1L $f(x, y) \to f(r(x), y))$

R2L $f(x, y) \to f(x \cdot y, y)$

R2R $f(x, y) \to f(x, y \cdot x)$

R3L$_i$ $f(x, y) \to f((a_i \cdot x) \cdot r(a_i), y)$ for $a_i \in A, i = 1, 2$

Proposition 1. *Term rewriting systems ACT_2 and $rACT_2$ considered modulo T_G are equivalent, that is $\to^*_{ACT_2/G}$ and $\to^*_{rACT_2/G}$ coincide.*

Proposition 2. *For ground t_1 and t_2 we have $t_1 \to^*_{ACT_2/G} t_2 \Leftrightarrow t_2 \to^*_{ACT_2/G} t_1$, that is $\to^*_{ACT_2/G}$ is symmetric.*

Now we present two variants of translations of ACT_2 into first-order logic with an intention to use automated theorem proving to show AC-equivalence.

1.2 Equational Translation

Denote by E_{ACT_2} an equational theory $T_G \cup rACT^=$ where $rACT^=$ includes the following axioms (equality variants of the above rewriting rules):

E-R1L $f(x, y) = f(r(x), y))$

E-R2L $f(x, y) = f(x \cdot y, y)$

E-R2R $f(x, y) = f(x, y \cdot x)$

E-R3L$_i$ $f(x, y) = f((a_i \cdot x) \cdot r(a_i), y)$ for $a_i \in A, i = 1, 2$

Proposition 3. *For ground terms t_1 and t_2 $t_1 \to^*_{ACT_2/G} t_2$ iff $E_{ACT_2} \vdash t_1 = t_2$*

In a variant of the equational translation the axioms $\mathbf{E-R3L_i}$ are replaced by "non-ground" axiom $\mathbf{E-RLZ}: f(x, y) = f((z \cdot x) \cdot r(z), y)$ and the corresponding analogue of Proposition 3 holds true.

1.3 Implicational Translation

Denote by I_{ACT_2} the first-order theory $T_G \cup rACT_2^{\to}$ where $rACT_2^{\to}$ includes the following axioms:

I-R1L $R(f(x, y)) \to R(f(r(x), y)))$

I-R2L $R(f(x, y)) \to R(f(x \cdot y, y))$

I-R2R $R(f(x, y)) \to R(f(x, y \cdot x))$

n	simplification steps	time, s
2	34	0.05
3	85	0.66
4	242	5.97
5	573	265
6	1282	10637

Table 1: Number of simplification steps and time required to find simplifications for $MS_n(w_*)$

I-R3L$_i$ $R(f(x,y)) \rightarrow R(f((a_i \cdot x) \cdot r(a_i), y))$ for $a_i \in A, i = 1, 2$

Proposition 4. *For ground terms t_1 and t_2 $t_1 \rightarrow^*_{ACT_2/G} t_2$ iff $I_{ACT_2} \vdash R(t_1) \rightarrow R(t_2)$*

Similarly to the case of equational translation "non-ground" axiom **I-R3Z**: $R(f(x,y)) \rightarrow R(f((z \cdot x) \cdot r(z), y))$ can be used instead of **I-R3L**$_i$ with a corresponding analogue of Proposition 4 holding true.

In summary we have proposed four main variants of the translations: EG ("equational ground"); EN ("equational non-ground"); IG ("implicational ground"); IN ("implicational non-ground").

2 Automated deduction for $MS_n(w_*)$

In [11] we demonstrated new AC-trivializations obtained by automated reasoning:

Proposition 5. *[11] Group presentations $MS_n(w_*)$ are AC-trivializable for n=3,4,5,6.*

These trivializations were found by automated theorem proving using IG encoding and Prover9 prover. We have published all proofs and extracted trivializations online [1]. The short summary of the results can be found in Table 1. The number of simplification steps appears to grow exponentially in n (more than doubles when going from n to $n+1$, at least for $3 \leq n < 6$). The results also illustrate the power of the method in searching AC-simplifications. Starting from n=3 the length of found simplifications sequences exceeds by far the length of any AC-simplification found by any alternative computational approach. Our ongoing work includes analysis of these long sequences of transformations in order to comprehend and generalize these proofs with the aim to arrive at general and likely inductive argument of trivializability applicable to the whole family $MS_n(w_*), n \geq 3$. While we were not able to complete it yet the analysis for n=3,4,5 has shown that the proofs demonstrate some regularity, which we formalize in the following conjecture.

Conjecture 2. *[11] All presentations $MS_n(w_*)$ are AC-trivializable for $n \geq 3$ using the following sequence of transformations*

$MS_n(w_*) \Rightarrow^* \langle a, b | b^{-(n-1)} a^{-4} ba, w_1 \rangle \Rightarrow^* \ldots \Rightarrow^* \langle a, b | b^{-(n-k)} a^{-4} ba, w_k \rangle \Rightarrow^* \ldots \Rightarrow^* \langle a, b | b^{-2} a^{-4} ba, w_{n-2} \rangle \Rightarrow^* \langle a, b | a, b \rangle$, *$k = 1 \ldots n-2$, where $w_k = a^{-1}b^{-1}aba^{-1}$ or $w_k = ab^{-1}a^{-1}ba$.*

Example 1. $MS_5(w_*) \Rightarrow^* \langle a, b | b^{-4} a^{-4} ba, w_1 \rangle \Rightarrow^* \langle a, b | b^{-3} a^{-4} ba, w_2 \rangle \Rightarrow^* \langle a, b | b^{-2} a^{-4} ba, w_3 \rangle \Rightarrow^* \langle a, b | a, b \rangle$

Note 1. *Interestingly, the only available at the time of [11] transformation sequence for n=6 did not fit the pattern indicated in the conjecture. As it is very long sequence (1282 simplification*

[1] https://doi.org/10.5281/zenodo.8267429

steps obtained in excess of 10,600s) there might well be alternative simplification sequences satisfying the patterns of the conjecture.

The cases $n \geq 7$

The case of $MS_7(w_*)$ poses considerable challenge for any computational approach. We were not able to find AC-simplification using automated reasoning with IG encoding (unlike the cases with $n \leq 6$).

We first were able to confirm AC-trivialization of $MS_7(w_*)$ using automated reasoning with EN encoding. It took Prover9 42681s to complete the search.

Proposition 6. *Group presentation $MS_7(w_*)$ is AC-trivializable.*

Unlike the proofs using IG encoding the equational proof with EN encoding uses multiple lemmas, each corresponding to a *macrostep* in AC-simplifications. Obtained proof consisted 892 macrosteps. An example of a non-trivial lemma is $f(x * y, y * (z^{-1} * (y * x^{-1}))) = f(x * y, x * (x * (x * z)))$. It is a topic of our ongoing work to implement an AC simplification steps extraction procedure by "delemmatization" of equational proofs using EN encoding.

The experiments with IN encoding yielded further interesting observations. We were able to produce alternative AC-trivializations for all $MS_n(w_*)$ for $2 \leq n \leq 7$ which demonstrated another type of regularity. We generalize these observations in the following conjecture

Conjecture 3. *For $n \geq 3$ all $MS_n(w_*)$ are AC-trivializable using the following sequences of transformations $MS_n(w_*) \Rightarrow^*_- \langle ab^{-1}a^{-3}, a^{-1}b^{-1}aba^{-1}\rangle \Rightarrow^{(11)} \langle a, b\rangle$, where $\Rightarrow^*_-$ denotes AC-rewriting without using a transformation encoded in axiom* **I-R2R***, and by that preserving the second component of the presentation. The conjecture holds true for $n = 3 \ldots 7$.*

The behaviour of trivializations found with IN encoding opens further opportunities for optimizations of search. In particular, if Conjecture 3 holds true for all n, the search of trivializations can be restricted to the search of $MS_n(w_*) \Rightarrow^*_- \langle ab^{-1}a^{-3}, a^{-1}b^{-1}aba^{-1}\rangle$. Furthermore, since $\Rightarrow^*_-$ rewriting does not change the second component of the presentation, the rewriting system and its logical encoding(s) can be re-formulated as one-dimensional variants by dropping the second component of presentations altogether.

We conducted the search of AC-trivializations for n=8 of the form described in Conjecture 3 and using IN encoding and said optimizations. The search was successfully completed[2] to establish that $MS_8(w_*) \Rightarrow^*_- \langle ab^{-1}a^{-3}, a^{-1}b^{-1}aba^{-1}\rangle \Rightarrow^{(11)} \langle a, b\rangle$. It took Prover9[3] 189707s and 9Gb of memory to find a proof. The length of the proof is 6270 and its detailed analysis is ongoing and will be presented elsewhere.

Proposition 7. *Group presentation $MS_8(w_*)$ is AC-trivializable.*

2.1 Other families of presentations

We tested the methodology "get automated proofs for a few values of parameter, then generalise by human reasoning" for other parametric families of balanced presentations of trivial group. The results are mixed so far. In one case of slightly modified family of $MS_n(w_{**}) = \{\langle a, b \mid a^{-1}b^n a = b^{n+1}, a^{-1} = w\rangle\}, n \geq 2$ we were able to get an inductive argument for general case by analysis of automated proofs for particular values of n (=2,3,4), but it should not be overestimated as in this case there a simple direct (and different) argument of trivializability, which we leave to an interested reader to find as an exercise.

[2] on 17 of May 2024

[3] as a part of ProverX platform for this case

3 Conclusion

We have shown that generic automated first-order proving can be used in combinatorial group theory, both in tackling open questions and as a competitive alternative to specialized algorithms. The obtained AC-trivilaiztion sequences for previously unknown to be trivializable presentations exceed in length by far those obtained by all alternative search methods. Considering parametric families of balanced group presentations brings interesting challenges for automated proofs comprehension, generalisation and regularisation, which could be tackled by combinations of methods from automated reasoning, machine learning, data and process mining. This is subject of our ongoing work.

References

[1] J. Andrews and M.L. Curtis. Free groups and handlebodies. *Proc. Amer. Math. Soc.*, 16:192–195, 1965.

[2] Franz Baader and Tobias Nipkow. *Term Rewriting and All That*. Cambridge University Press, New York, NY, USA, 1998.

[3] Ximena Fernández. Morse theory for group presentations. arxiv:1912.00115, 2019.

[4] George Havas and Colin Ramsay. Andrews-Curtis and Todd-Coxeter proof words. Technical report, in Oxford. Vol. I, London Math. Soc. Lecture Note Ser, 2001.

[5] George Havas and Colin Ramsay. Breadth-first search and the Andrews-Curtis conjecture. *International Journal of Algebra and Computation*, 13(01):61–68, 2003.

[6] C. F. Miller III and P. E. Schupp. *Some presentations of the trivial group*, volume 250 of *Contemp. Math.*, pages 113–115. Amer. Math. Soc., Providence, RI, 1999.

[7] Krzysztof Krawiec and Jerry Swan. AC-trivialization proofs eliminating some potential counterexamples to the Andrews-Curtis conjecture. `www.cs.put.poznan.pl/kkrawiec/wiki/uploads/Site/ACsequences.pdf`, 2015.

[8] Alexei Lisitsa. First-order theorem proving in the exploration of Andrews-Curtis conjecture. *TinyToCS*, 2, 2013.

[9] Alexei Lisitsa. The Andrews-Curtis Conjecture, Term Rewriting and First-Order Proofs. In *Mathematical Software - ICMS 2018 - 6th International Conference, South Bend, IN, USA, July 24-27, 2018, Proceedings*, pages 343–351, 2018.

[10] Alexei Lisitsa. Automated reasoning for the Andrews-Curtis conjecture. In *AITP 2019, Fourth Conference on Artificial Intelligence and Theorem Proving, Abstracts of the Talks April 7–12, 2019, Obergurgl, Austria*, pages 82–83, 2019.

[11] Alexei Lisitsa. Towards computer-assisted proofs of parametric Andrews-Curtis simplifications. In *AITP 2023, 8th Conference on Artificial Intelligence and Theorem Proving, Abstracts of the Talks September 3–8, 2023, Aussois, France*, 2023.

[12] Alexei D. Miasnikov. Genetic algorithms and the Andrews-Curtis conjecture. *International Journal of Algebra and Computation*, 09(06):671–686, 1999.

[13] Dmitry Panteleev and Alexander Ushakov. Conjugacy search problem and the andrews-curtis conjecture. arxiv:1609.00325, 2016.

[14] Jerry Swan, Gabriela Ochoa, Graham Kendall, and Martin Edjvet. Fitness Landscapes and the Andrews-Curtis Conjecture. *IJAC*, 22(2), 2012.