Theories of Equations in Finitely Presented Groups

Markus Lohrey

Universität Stuttgart, Institut für Informatik
Breitwiesenstr. 20–22, 70565 Stuttgart, Germany

This abstract reports some ongoing work on theories of equations in some finitely presented groups. The question whether an equation has a solution in some finitely presented group corresponds to a particular unification problem.

We start with a short historical overview on the topic. In 1977 Makanin has shown that for a free monoid the existential theory of equations is decidable [11]. Due to the technical difficulty of Makanin's proof it is not easy to give precise bounds on the complexity of the algorithm developed by Makanin. A first estimate by several towers of exponentials was finally be reduced to exponential space [7], which is currently the best known upper bound on Makanin's algorithm. A very good exposition of Makanin's algorithm can be found in [1]. In 1983 Makanin extended his decidability result to the existential theory of equations of a free group [12]. In this case Kościelski and Pacholsky [10] were able to prove that the scheme of Makanin is not primitive recursive for free groups. Based on results of Merzlyakov [14], Makanin has also shown that for a free group the positive theory of equations is decidable [13]. In 1999 Plandowski has developed a new method for solving word equations which allowed him to prove that for a free monoid the existential theory of equations is in PSPACE [15]. Plandowski's result was extended by Gutiérrez to the case of free groups [8]. Recently these decidability results were further extended to wider classes of finitely presented groups, namely free partially commutative groups [4] and plain groups [3]. Finally let us mention that the many of the decidability results mentioned above have been generalized to include the possibility of specifying constraints for variables, which typically have the form of recognizable sets [2, 16].

Currently we are trying to extend the decidability results mentioned above to a larger class of groups, which we call *partially commutative plain groups*, briefly *pcp groups*. These groups generalize both plain groups [9] and free partially commutative groups, which in algebra are also known as graph groups, see e.g [5]. Let us first define these groups. Let (V, E) be a finite undirected graph (i.e. E is a symmetric and irreflexive relation on V), where the set of nodes is partitioned into two sets V_{free} and V_{fin}. Each node $v \in V$ is labeled with a group G_v. In the case $v \in V_{\text{free}}$, G_v is the free group of rank 1, generated by a symbol a_v, and in the case $v \in V_{\text{fin}}$, G_v is a finite group. For $v \in V_{\text{fin}}$ define $\Gamma_v = G_i \backslash \{1\}$ and let $\overline{a} \in \Gamma_v$ be the inverse of $a \in \Gamma_v$ in G_v. For $v \in V_{\text{free}}$ define $\Gamma_v = \{a_v, \overline{a_v}\}$ and let $\overline{\overline{a_v}} = a_v$. We assume that the sets Γ_v for $v \in V$ are pairwise disjoint. Finally the pcp group $G(V, E)$ is the group generated (as a monoid) by the set $\Gamma = \bigcup_{v \in V} \Gamma_v$ and that satisfies the following defining relations:

- $a\overline{a} = 1$ for all $a \in \Gamma$

- $ab = c$ if there exists a $v \in V_{\mathrm{fin}}$ such that $a, b, c \in \Gamma_v$ and $ab = c$ in the finite group G_v
- $ab = ba$ if there exists a $(u, v) \in E$ such that $a \in \Gamma_u$ and $b \in \Gamma_v$

Thus the group $G(V, E)$ results from the free product of the groups G_v $(v \in V)$ by allowing elements of E-adjacent groups to commute. This construction is a special case of the graph product investigated in [6]. If $E = \emptyset$ then $G(V, E)$ is also called a *plain group* [9] and if $V_{\mathrm{fin}} = \emptyset$ then $G(V, E)$ is called a *free partially commutative group* or a *graph group*. For the following consideration let us fix a pcp group $G = G(V, E)$.

In the following Ω denotes a finite set of variables (or unknowns) and we let $\bar{\ } : \Omega \to \Omega$ be an involution without fixed points. First we will define the existential theory of equations of the pcp group G. Atomic formulas are of type $U = V$, where $U, V \in (\Gamma \cup \Omega)^*$. A propositional formula is build up by atomic formulas using negations, conjunctions, and disjunctions. The evaluation of such a formula in G is completely straightforward, but of course if a variable X is interpreted by $x \in G$ then $\overline{X}$ is interpreted by x^{-1}. The existential theory of equations of the pcp group G consists of all closed existentially quantified propositional formulas which evaluate to *true* in G.

Conjecture 1. For every pcp group G the existential theory of equations is decidable.

The above conjecture was proven in [4] for the case of a free partially commutative group and in [3] for the case of a plain group.

A positive formula is build up by equations using conjunctions, disjunctions, existential quantifiers, and universal quantifiers, but does not contain negations. The positive theory of equations of the pcp group G consists of all closed positive formulas that evaluate to *true* in G. As already mentioned, Makanin has shown that for a free group the positive theory of equations is decidable [13]. Makanin used a result of Merzlyakov [14] in order to reduce the positive theory of equations of a free group to the existential fragment. We conjecture that we can extend this reduction to the case of general pcp groups, which together with Conjecture 1 leads to the following conjecture.

Conjecture 2. For every pcp group G the positive theory of equations is decidable.

Other interesting topics for further research include the search for good upper complexity bounds and the inclusion of constraints (e.g. recognizable constraints or even larger classes) for the variables.

References

1. V. Diekert. Makanin's Algorithm. In J. Berstel and D. Perrin, editors, *Algebraic Combinatorics on Words*. Cambridge University Press. A preliminary version is on the web: `http://www-igm.univ-mlv.fr/~berstel/Lothaire/index.html`.

2. V. Diekert, C. Gutiérrez, and C. Hagenah. The existential theory of equations with rational constraints in free groups is PSPACE-complete. In A. Ferreira and H. Reichel, editors, *Proceedings of the 18th Annual Symposium on Theoretical Aspects of Computer Science (STACS 01), Dresden (Germany) 2001*, number 2010 in Lecture Notes in Computer Science, pages 170–182. Springer, 2001.
3. V. Diekert and M. Lohrey. A note on the existential theory of equations in plain groups. *International Journal of Algebra and Computation*, 2001. to apear.
4. V. Diekert and A. Muscholl. Solvability of equations in free partially commutative groups is decidable. In *Proceedings of the 28th International Colloquium on Automata, Languages and Programming (ICALP 01), Crete (Greece) 2001*, Lecture Notes in Computer Science. Springer, 2001. to appear.
5. C. Droms. Isomorphisms of graph groups. *Proceedings of the American Mathematical Society*, 100:407–408, 1987.
6. E. R. Green. *Graph Products of Groups*. PhD thesis, The University of Leeds, 1990.
7. C. Gutiérrez. Satisfiability of word equations with constants is in exponential space. In *Proc. of the 39th Ann. Symp. on Foundations of Computer Science, FOCS 98*, pages 112–119, Los Alamitos, California, 1998. IEEE Computer Society Press.
8. C. Gutiérrez. Satisfiability of equations in free groups is in PSPACE. In *32nd Ann. ACM Symposium on Theory of Computing (STOC'2000)*. ACM Press, 2000.
9. R. H. Haring-Smith. Groups and simple languages. *Transactions of the American Mathematical Society*, 279:337–356, 1983.
10. A. Kościelski and L. Pacholski. Complexity of unification in free groups and free semigroups. In *Proceedings of the31st Annual Symposium on Foundations of Computer Science*, volume II, pages 824–829, Los Alamitos, 1990. IEEE Computer Society Press.
11. G. S. Makanin. The problem of solvability of equations in a free semigroup. *Math. Sbornik*, 103:147–236, 1977. English transl. in Math. USSR Sbornik 32 (1977).
12. G. S. Makanin. Equations in a free group. *Izv. Akad. Nauk SSR*, Ser. Math. 46:1199–1273, 1983. English transl. in Math. USSR Izv. 21 (1983).
13. G. S. Makanin. Decidability of the universal and positive theories of a free group. *Izv. Akad. Nauk SSSR*, Ser. Mat. 48:735–749, 1984. In Russian; English translation in: *Math. USSR Izvestija, 25*, 75–88, 1985.
14. Y. I. Merzlyakov. Positive formulas on free groups. *Algebra i Logika Sem.*, 5(4):25–42, 1966. (Russian).
15. W. Plandowski. Satisfiability of word equations with constants is in PSPACE. In *Proceedings of the 40th Annual Symposium on Foundations of Computer Science (FOCS 99)*, pages 495–500. IEEE Computer Society Press, 1999.
16. K. U. Schulz. Makanin's algorithm for word equations — Two improvements and a generalization. In K. U. Schulz, editor, *Word Equations and Related Topics*, number 572 in Lecture Notes in Computer Science, pages 85–150, Berlin-Heidelberg-New York, 1991. Springer.