A note on the existential theory of equations in plain groups

Volker Diekert, Markus Lohrey
Universität Stuttgart, Institut für Informatik
Breitwiesenstr. 20–22, 70565 Stuttgart, Germany

April 25, 2001

2000 Mathematics Subject Classification: 03B25, 20F05, 20F10, 20F65

Abstract

Based on a PSPACE-completeness result for free monoids with involution [4] it is shown that the existential theory of equations with rational constraints in plain groups is PSPACE-complete. As a corollary this settles a question from [16].

1 Introduction

In 1977 Makanin has shown that the existential theory of equations in free monoids is decidable [14]. This result is considered to be one of the most fundamental decidability results concerning free monoids. 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 [9], which is currently the best known upper bound on Makanin's algorithm, see also [3]. In 1983 Makanin extended his decidability result to the existential theory of equations in free groups [15]. In this case Kościelski and Pacholski [13] were able to prove that the scheme of Makanin is not primitive recursive.

Recently Plandowski has developed a new method for solving word equations which allowed him to prove that the existential theory of equations in free monoids is in PSPACE [17]. Plandowski's result was extended by Gutiérrez to the case of free groups [10]. This result was further generalized in [4], where it it shown that the existential theory of equations with rational constraints in free groups is PSPACE-complete.

In this paper we extend the results of [4] to the larger class of *plain* groups. According to Harring-Smith [11] a group is called plain, if it is a free product of a finitely generated free group and finitely many finite groups. The class of plain groups is contained in the class of word hyperbolic groups, which was introduced in [8], and furthermore it is known that the existential theory of equations in torsion-free word hyperbolic groups is decidable [18]. Since the intersection of the class of torsion-free word hyperbolic groups and the class of plain groups is exactly the class of free groups, our decidability result for plain groups is in some sense orthogonal to the result of [18]. Finally our result also solves an open problem from [16], where it was asked whether the solvability of word equations modulo a confluent and special finite semi-Thue system that presents a group is decidable.

2 Preliminaries

In this section we will introduce some notions concerning words and semi-Thue systems. Let Γ be a finite alphabet. The empty word over Γ is denoted by 1, it is the neutral element of the the free monoid Γ^*. More generally the neutral element of any monoid is denoted by 1, this will never lead to confusion. An *involution* on Γ is a function $\overline{} : \Gamma \to \Gamma$ such that $\overline{\overline{a}} = a$ for all $a \in \Gamma$. In our setting an involution may have fixed points, i.e., symbols a with $\overline{a} = a$. We extend $\overline{}$ to a function $\overline{} : \Gamma^* \to \Gamma^*$ by $\overline{a_1 \cdots a_n} = \overline{a}_n \cdots \overline{a}_1$. The structure $(\Gamma^*, \overline{})$ is called a *free monoid with involution*. A *semi-Thue system* S on the alphabet Σ is a finite subset of $\Gamma^* \times \Gamma^*$. The *reduction relation* $\to_S$ and the *Thue congruence* $\overset{*}{\leftrightarrow}_S$ are defined in the usual way, see, e.g., [1] or [12]. The pair (Γ, S) is also called a *presentation*. The monoid presented by (Γ, S) is the quotient monoid of the free monoid Γ^* with respect to the Thue congruence $\overset{*}{\leftrightarrow}_S$. The definition of the notion of a Noetherian (monadic, special, confluent) semi-Thue system can be found for instance in [1]. The set of all *irreducible words* with respect to S is $\mathrm{IRR}(S) = \Gamma^* \backslash \{w \in \Gamma^* \mid \exists u \in \Gamma^* : w \to_S u\}$. It is clear that this set forms a rational subset of Γ^*, moreover a non-deterministic finite automaton accepting $\mathrm{IRR}(S)$ can be constructed in polynomial time from S, see, e.g., [1, Lem. 2.1.3]. Recall also that for free monoids the notions of rational and regular coincide.

For a set $L \subseteq \Gamma^*$ we denote by $\Delta_S(L) = \{w \in \Sigma^* \mid \exists u \in L : u \overset{*}{\to}_S w\}$ the set of all *descendants* of L with respect to S. The following fact is well-known [1, Thm. 4.2.1].

Lemma 2.1. *Let $L \subseteq \Gamma^*$ be rational and S a monadic semi-Thue system over Γ. Then the language $\Delta_S(L)$ of all descendants of L is also rational, furthermore a non-deterministic finite automaton that accepts $\Delta_S(L)$ can be calculated in polynomial time.*

3 Plain groups

In the following Ω denotes a finite set of variables (or unknowns) and we let $\overline{} : \Omega \to \Omega$ be an involution without fixed points. First we will define the existential theory of equations with rational constraints in a free monoid with involution $(\Gamma^*, \overline{})$. Atomic formulae are of type $U = V$ where $U, V \in (\Gamma \cup \Omega)^*$ and of type $X \in L$ where $X \in \Omega$ and $L \subseteq \Gamma^*$ is a rational language specified by some non-deterministic finite automaton. A propositional formula is build up by atomic formulae using negations, conjunctions, and disjunctions. The input size of $U = V$ is 1 plus the length $|UV|$, the size of $X \in L$ is 1 plus the number of states used for a finite non-deterministic automaton accepting $L \subseteq \Gamma^*$. The total size of a formula is then the sum of the size of the alphabet Γ plus the sizes of the atomic subformulae plus the number of negations and Boolean operators which are used in the formula. The evaluation of such a formula over $(\Gamma^*, \overline{})$ is straightforward, and of course, if a variable X is interpreted by $w \in \Gamma^*$ then $\overline{X}$ is interpreted by $\overline{w}$. The existential theory refers to set of closed existentially quantified propositional formulae which evaluate to *true* in $(\Gamma^*, \overline{})$. The following theorem has been shown in [4]. It generalizes results of Plandowski [17], Rytter [17, Thm. 1], and Gutiérrez [10]. This result is the starting point for our extension from free to plain groups.

Theorem 3.1. *The following problem is* PSPACE*-complete.*

INPUT: An alphabet Γ with an involution $\overline{} : \Gamma \to \Gamma$ and a closed existentially quantified propositional formula with rational constraints in the free monoid with involution $(\Gamma^*, \overline{})$.

OUTPUT: The evaluation of the formula in $(\Gamma^*, \overline{})$.

Next we will define the existential theory of equations with rational constraints in a plain group. A group is called *plain* if it is a free product of a free group of finite rank and finitely many finite groups [11]. For the following consideration let us fix a plain group $G = F_n * G_1 * \cdots * G_m$, where F_n is the free group of rank n generated by $\{a_1, \ldots, a_n\}$ and $G_1, \ldots, G_m$ are finite groups. Let $\{\overline{a}_i \mid 1 \leq i \leq n\}$ be a disjoint copy of $\{a_i \mid 1 \leq i \leq n\}$ and assume that the sets $G_i \backslash \{1\}$ $(1 \leq i \leq m)$ and $\{a_i, \overline{a}_i \mid 1 \leq i \leq n\}$ are pairwise disjoint. We choose the following finite presentation of G: Let

$$\Gamma = \{a_i, \overline{a}_i \mid 1 \leq i \leq n\} \cup \bigcup_{i=1}^{m} (G_i \backslash \{1\})$$

be the alphabet of the presentation. For $b \in G_i \backslash \{1\}$ we denote by $\overline{b}$ the inverse of b in G_i. In this way we have defined an involution on the alphabet Γ. In particular $(\Gamma^*, \overline{})$ is a free monoid with involution. Note that the involution $\overline{}$ has fixed points if and only if the group G has an element of order 2. On Γ we define a monadic semi-Thue system S by

$$S = \{\overline{a}a \to 1 \mid a \in \Gamma\} \cup \{ab \to c \mid a, b, c \in G_i \backslash \{1\} \text{ and } ab = c \text{ in } G_i \text{ for some } i\}.$$

It is easy to see that (Γ, S) is indeed a presentation of G, we call it the *canonical presentation* of G. Moreover by considering the critical pairs of S it is easy to see that S is confluent. For example if $a, b, c \in G_i \backslash \{1\}$ such that $ab = c$ in G_i then $ab\overline{b} \to_S a$ and $ab\overline{b} \to_S c\overline{b}$ and thus, $(a, c\overline{b})$ is a critical pair of S. But since $ab = c$ implies $a = c\overline{b}$ in G_i, also $c\overline{b} \to a$ must be a rule of S and we can resolve the critical pair.

Let $\psi : (\Gamma^*, \overline{}) \to G$ be the canonical morphism that maps a word $w \in \Gamma^*$ to the group element represented by w. By definition, a subset $P \subseteq G$ is *rational* if $P = \psi(L)$ for some rational language $L \subseteq \Gamma^*$. The existential theory of equations with rational constraints in the plain group G is defined analogously to the case of a free monoid with involution but of course variables are interpreted by elements of G and if a variable X is interpreted by $x \in G$ then $\overline{X}$ is interpreted by x^{-1}. A rational constraint $P \subseteq G$ is specified by some non-deterministic finite automaton that accepts a language $L \subseteq \Gamma^*$ such that $P = \psi(L)$. The next theorem generalizes Theorem 1 from [4].

Theorem 3.2. *The following problem is* PSPACE*-complete.*

INPUT: A plain group G given by its canonical presentation (Γ, S) and a closed existentially quantified propositional formula with rational constraints in the plain group G.

OUTPUT: The evaluation of the formula in G.

Before we prove this theorem we shall derive a corollary. It is well-known that a group can be presented by some confluent and special semi-Thue system if and only if it is a free product of finitely many cyclic groups [2]. Hence we obtain the following corollary, answering a question raised in [16].

Corollary 3.3. *The following problem is decidable:*

INPUT: A confluent and special semi-Thue system S that presents a group and a word equation $U = V$.

OUTPUT: True *if $U = V$ has a solution modulo S, i.e, if there exists an interpretation σ of the variables occurring in UV such that $\sigma(U) \overset{*}{\leftrightarrow}_S \sigma(V)$, otherwise* false*.*

Remark 3.4. *In [16] the same problem as in Corollary 3.3 was shown to be undecidable, if the input system S does not necessarily present a group. Therefore the interest in Corollary 3.3.*

For the proof of Theorem 3.2 we need the following Lemma.

Lemma 3.5. *Let (Γ, S) be the canonical presentation of a plain group G. Let $x, y, z \in \Gamma^* \cap IRR(S)$. Then $xy \overset{*}{\rightarrow}_S z$ if and only if the following holds in $(\Gamma^*, {}^{-})$:*

$$\exists p, s, t \in \Gamma^* \left\{ \begin{array}{l} (x = sp \ \wedge \ y = \overline{p}t \ \wedge \ z = st) \quad \vee \\ \displaystyle\bigvee_{\substack{a,b,c \in \Gamma \\ (ab,c) \in S}} (x = sap \ \wedge \ y = \overline{p}bt \ \wedge \ z = sct) \end{array} \right\}. \tag{1}$$

Proof. If x, y, and z satisfy (1) then of course $xy \overset{*}{\rightarrow}_S z$. On the other hand assume that $x, y, z \in \Gamma^* \cap \mathrm{IRR}(S)$ satisfy $xy \overset{*}{\rightarrow}_S z$. We prove (1) by an induction on the length of this derivation. The case $xy = z$ is clear with $p = 1$, $s = x$, and $t = y$. Thus assume that $xy \overset{+}{\rightarrow}_S z$. Since $x, y \in \mathrm{IRR}(S)$ we have $x = x'a$, $y = by'$, $a, b \in \Gamma$, $(ab, c) \in S$, and $x'cy' \overset{*}{\rightarrow}_S z$. There are two cases. First if $a = \overline{b}$ and $c = 1$ we have $x'y' \overset{*}{\rightarrow}_S z$ and we can apply the induction hypothesis to this derivation. On the other hand if $a, b, c \in G_i \backslash \{1\}$ for some i then $x'a, by' \in$

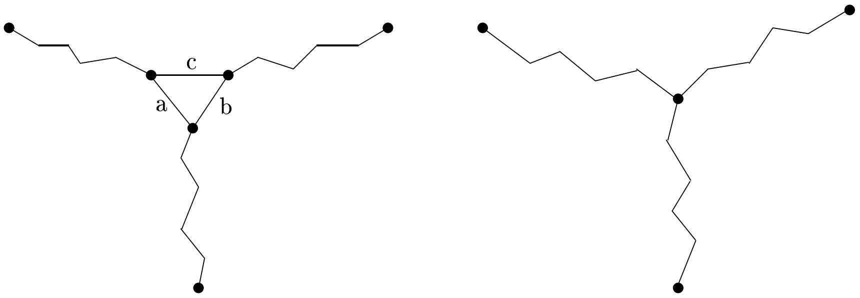

Figure 1: Geodesic triangles in plain groups

$\mathrm{IRR}(S)$ implies that x' (resp. y') does not end (resp. start) with a symbol from $(G_i \backslash \{1\})$. But then $x'cy' \in \mathrm{IRR}(S)$ and thus $x'cy' = z$. Then (1) is satisfied if we set $p = 1$, $s = x'$, and $t = y'$. $\square$

Lemma 3.5 has a nice geometrical interpretation in terms of geodesic triangles in the Cayley graph for the presentation (Γ, S). A geodesic path is a shortest path between two nodes of a Cayley graph. For more details on Cayley graphs and geodesic paths see for instance [7]. The two possible shapes of geodesic triangles in the Cayley graph for the presentation (Γ, S) are shown in Figure 1. The left triangle corresponds to the case $x = sap \wedge y = \overline{p}bt \wedge z = sct$, where $a, b, c \in \Gamma$ and $(ab, c) \in S$, whereas the right triangle corresponds to the case $x = sp \wedge y = \overline{p}t \wedge z = st$.

Proof of Theorem 3.2. PSPACE-hardness follows from Theorem 3.1. Containment in PSPACE will be proven by a reduction to Theorem 3.1. More precisely, given an input formula we will construct in polynomial time a new formula, which evaluates to true in the free monoid with involution $(\Gamma^*, ^-)$ if and only if the original input formula evaluates to true in the plain group G.

Consider an input formula which is interpreted in the plain group G. First we replace an inequality $U \neq V$ by $\exists X : UX = V \wedge X \notin \{1\}$, thus we may assume that all atomic subformulae have the form $U = V$, $X \in P$, or $X \notin P$, where $U, V \in (\Gamma \cup \Omega)^*$, w.l.o.g. $|UV| \geq 3$ (we may append $a\overline{a}$ for some $a \in \Gamma$ to an equation), and $P \subseteq G$ is rational. Finally we may assume that all equations are of the form $xy = z$, where $x, y, z \in \Gamma \cup \Omega$ (use the equivalence of $x_1 \cdots x_m = y_1 \cdots y_n$ and $\exists X : x_1 \cdots x_m = Xy_3 \cdots y_n \wedge X = y_1 y_2$).

Recall that $X \in P$ (resp. $X \notin P$) means in fact $X \in \psi(L)$ (resp. $X \notin \psi(L)$) where $L \subseteq \Gamma^*$ is a rational word language specified by some finite nondeterministic automaton. We replace syntactically each subformula $X \in P$ (resp. $X \notin P$) by $\psi(X) \in \psi(L)$ (resp. $\psi(X) \notin \psi(L)$) and we replace each subformula $xy = z$ by $\psi(xy) = \psi(z)$. We obtain an existential formula where the variables are now interpreted in the free monoid with involution $(\Gamma^*, ^-)$, but the truth value did not change.

We eliminate now all occurrences of ψ. Since the value of every variable may be assumed to be in $\mathrm{IRR}(S)$, since $\Gamma \subseteq \mathrm{IRR}(S)$, and since S is confluent, we can replace an equation $\psi(xy) = \psi(z)$ by $xy \xrightarrow{*}_S z$. At the same time we replace a constraint $\psi(X) \in \psi(L)$ by $X \in \Delta_S(L)$ and similarly we replace a constraint $\psi(X) \notin \psi(L)$ by $X \notin \Delta_S(L) \;\wedge\; X \in \mathrm{IRR}(S)$. This step is justified by Lemma 2.1. Finally by Lemma 3.5 we may replace a formula $xy \xrightarrow{*}_S z$ by the formula

$$\exists P, S, T \left\{ \begin{array}{l} (x = SP \;\wedge\; y = \overline{P}T \;\wedge\; z = ST) \quad \vee \\ \displaystyle\bigvee_{\substack{a,b,c \in \Gamma \\ (ab,c) \in S}} (x = SaP \;\wedge\; y = \overline{P}bT \;\wedge\; z = ScT) \end{array} \right\}.$$

Note that this formula is only polynomially large with respect to the input. Thus all transformation steps can be done in polynomial time and Theorem 3.2 is a consequence of Theorem 3.1 $\square$

4 Outlook

Recently in [5], the decidability results of [4] have also been extended to free partially commutative groups (graph groups). Graph groups are quotient groups of free groups where the defining relations are given by a partial commutation relation between generators, see, e.g., [6]. The common generalization of plain and graph groups leads to a notion of *partially commutative plain groups*. In a forthcoming paper the authors of the present paper will show that both, the existential and the positive theory of equations in partially commutative plain groups are decidable.

References

[1] R. Book and F. Otto. *String–Rewriting Systems.* Springer, 1993.

[2] Y. Cochet. Church-Rosser congruences on free semigroups. *Colloquia Mathematica Societatis János Bolyai*, 20:51–60, 1976.

[3] V. Diekert. Makanin's Algorithm. In M. Lothaire *Algebraic Combinatorics on Words.* Cambridge University Press, 2001

[4] 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 18th STACS, Dresden*, volume 2010 of *Lecture Notes in Computer Science*, pages 170–182. Springer, 2001.

[5] 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)*, Lecture Notes in Computer Science, Berlin-Heidelberg-New York, 2001. Springer.

[6] C. Droms. Graph groups, coherence and three-manifolds. *Journal of Algebra*, 106(2):484–489, 1985.

[7] D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson, and W. P. Thurston. *Word processing in groups.* Jones and Bartlett, Boston, 1992.

[8] M. Gromov. Hyperbolic groups. In S. M. Gersten, editor, *Essays in Group Theory*, number 8 in MSRI Publ., pages 75–263. Springer, 1987.

[9] 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.

[10] 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.

[11] R. H. Haring-Smith. Groups and simple languages. *Transactions of the American Mathematical Society*, 279:337–356, 1983.

[12] M. Jantzen. Confluent string rewriting. In *EATCS Monographs on theoretical computer science*, volume 14. Springer, 1988.

[13] A. Kościelski and L. Pacholski. Complexity of unification in free groups and free semi-groups. In *Proceedings of the 31st Annual Symposium on Foundations of Computer Science*, volume II, pages 824–829, Los Alamitos, 1990. IEEE Computer Society Press.

[14] 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).

[15] 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).

[16] P. Narendran and F. Otto. The word matching problem is undecidable for finite special string-rewriting systems that are confluent. In P. Degano, R. Gorrieri, and A. Marchetti-Spaccamela, editors, *Proceedings of the 24th International Colloquium on Automata, Languages and Programming (ICALP'97)*, volume 1256 of *Lecture Notes in Computer Science*, pages 638–648. Springer, 1997.

[17] 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.

[18] E. Rips and Z. Sela. Canonical representatives and equations in hyperbolic groups. *Inventiones Mathematicae*, 120:489–512, 1995.