The existential theory of equations with rational constraints in free groups is PSPACE–complete

Volker Diekert[1], Claudio Gutiérrez[2], Christian Hagenah[1]

[1] Inst. für Informatik, Universität Stuttgart, Breitwiesenstr. 20-22, D-70565 Stuttgart. Emails: diekert@informatik.uni-stuttgart.de, christian@hagenah.de
[2] Centro de Mod. Matemático y Depto. de Ciencias de la Computación, Universidad de Chile, Blanco Encalada 2120, Santiago, Chile. Email: cgutierr@dcc.uchile.cl

Abstract. This paper extends extends known results on the complexity of word equations and equations in free groups in order to include the presence of rational constraints, i.e., such that a possible solution has to respect a specification given by a rational language. Our main result states that the existential theory of equations with rational constraints in free groups is PSPACE–complete.

Keywords: Formal languages, equations, regular language, free group

1 Introduction

In 1977 (resp. 1983) Makanin proved that the existential theory of equations in free monoids (resp. free groups) is decidable by presenting algorithms which solve the satisfiability problem for a single word equation (resp. group equation) with constants [13–15]. These algorithms are very complex: For word equations the running time was first estimated by several towers of exponentials and it took more than 20 years to lower it down to the best known bound for Makanin's original algorithm, which is to date EXPSPACE [7]. For equations in free groups Kościelski and Pacholski have shown that the scheme of Makanin is not primitive recursive.

Recently Plandowski found a different approach to solve word equations and showed that the satisfiability problem for word equations is in PSPACE, [18]. Roughly speaking, his method uses data compression (first introduced for word equations in [19]) plus properties of factorization of words. Gutiérrez extended this method to the case of free groups, [9]. Thus, a non-primitive recursive scheme for solving equations in free groups was replaced by a polynomial space bounded algorithm.

In this paper we extend the results [18, 9] above in order to include the presence of rational constraints. Rational constraints mean that a possible solution has to respect a specification which is given by a regular word language. Our main result states that the existential theory of equations in free groups with rational constraints is PSPACE–complete. The corresponding PSPACE–completeness for word equations with regular constraints has been announced by first Rytter, see [18, Thm. 1] and [20].

The idea to consider regular constraints in the case of word equations is due to Schulz [21]. The importance of this concept, pointed out firstly by Schulz, can be exemplified by: the application of Schulz' result to monadic simultaneous rigid E-unification [6]; the use of regular constraints in [5] as a basic (an necessary) tool when showing that Makanin's result holds in free partially commutative monoids; the proof, in a forthcoming paper of Diekert and Muscholl, of the decidability of the existential theory of equations in graph groups (open problem stated in [5]) by using the present result; and the positive answer, by Diekert and Lohrey [4], to the question (cf [16]) about the existential theory of equations in free products of free and finite groups is decidable by relying on the general form of Theorem 2 below (we allow fixed points for the involution on Γ).

Our paper deals with the existential theory. For free groups it is also known that the positive theory without constraints is decidable, see [15]. Thus, one can allow also universal quantifiers but no negations. Note that we cannot expect that the positive theory of equations with rational constraints in free groups be decidable, since we can code the word case (with regular constraints) which is known to be undecidable. On the other hand, a negation leads to a positive constraint of a very restricted type, so it is a interesting question under which type of constraints the positive theory remains decidable.

Our proof of Theorem 1 is in the first step a reduction to the satisfiability problem of a single equation with regular constraints in a free monoid with involution. In order to avoid an exponential blow-up, we do not use a reduction as in [15], but a much simpler one. In particular, we can handle negations simply by a positive rational constraints. In the second step we show that the satisfiability problem of a single equation with regular constraints in a free monoid with involution is still in PSPACE. We extend the method of [18, 9] such that it copes with the involution and with rational constraints. There seems to be no direct reduction to the word case or to the case of free groups without constraints. So we cannot use these results as black boxes. Because there is not enough space to present the whole proof in this extended abstract, we focus on those parts where there is a substantial difference to the case without constraints. In particular, we develop the notion of maximal free interval, a concept which can be used even when there are no constraints, but when one is interested in other solutions rather than the one of minimal length. The missing proofs can be found in [10] which is available on the web.[1]

2 Equations with rational constraints in free groups

Rational languages, equations. Let Σ be a finite alphabet and let $\overline{\Sigma} = \{\, \overline{a} \mid a \in \Sigma \,\}$. We use the convention that $\overline{\overline{a}} = a$. Define $\Gamma = \Sigma \cup \overline{\Sigma}$. Hence $^{-} : \Gamma \to \Gamma$

[1] In http://inf.informatik.uni-stuttgart.de/ifi/ti/veroeffentlichungen/psfiles is the file HagenahDiss2000.ps

is an involution which is extended to Γ^* by $\overline{a_1 \cdots a_n} = \overline{a_n} \cdots \overline{a_1}$ for $n \geq 0$ and $a_i \in \Gamma$. We usually will write just Γ instead of $(\Gamma, \overline{\ })$. A word $w \in \Gamma^*$ is *freely reduced*, if it contains no factor of the form $a\overline{a}$ with $a \in \Gamma$.

The elements of the free group $F(\Sigma)$ are represented by freely reduced words in Γ^*. We read $\overline{a}$ as a^{-1} in $F(\Sigma)$. There is a canonical homomorphism $\hat{\ } : \Gamma^* \to F(\Sigma)$, which eliminates all factors of the form $a\overline{a}$ from a word.

The class of *rational languages* in $F(\Sigma)$ is inductively defined as follows: Every finite subset of $F(\Sigma)$ is rational. If $P_1, P_2 \subseteq F(\Sigma)$ are rational, then $P_1 \cup P_2$, $P_1 \cdot P_2$, and P_1^* are rational. Hence, $P \subseteq F(\Sigma)$ is rational if and only if $P = \{\hat{w} : w \in P'\}$ for some regular language $P' \subseteq \Gamma^*$. It is well-known that the family of rational group languages is an effective Boolean algebra, in particular, it is closed under complementation [1]. (See also [2, Sect. III. 2].)

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. An *equation with rational constraints in free groups* is an equation $W = 1$ in free groups plus constraints on the variables of the type $X \in P$, for P a rational language. The existential fragment of these equations is the set of closed formulas of the form $\exists X_1 \ldots \exists X_n B$, where $X_i \in \Omega$ and B is a Boolean combination of atomic formulas which are either of the form $(W = 1)$ or $(X_i \in P)$, where $W \in (\Gamma \cup \Omega)^*$ and $P \subseteq F(\Sigma)$ is a rational language. The *existential theory of equations with rational constraints in free groups* is the set of such formulas which are valid in the free group $F(\Sigma)$.

Theorem 1. *The existential theory of equations with rational constraints in free groups is* PSPACE*–complete.*

Proof (sketch). The PSPACE–hardness follows easily from [12] and is not discussed further. The proof for the inclusion in PSPACE is a reduction to the corresponding problem over free monoids with involution. It goes as follows.

First, we may assume that the input is given by some propositional formula which is in fact a conjunction of formulae of type $W = 1$, $X \in P$, $X \notin P$ with $W \in (\Gamma \cup \Omega)^*$, $X \in \Omega$, and $P \subseteq F(\Sigma)$ rational.[2] This is achieved by using DeMorgan rules to push negations to the level of atomic formulas, then replacing $W \neq 1$ by $\exists X : WX = 1 \wedge X \notin \{1\}$ (and pushing the quantifier to the out-most level), and finally eliminating the disjunctions by replacing non-deterministically every subformula of type $A \vee B$ by either A or B.

It is not difficult to see that we may also assume that $|W| = 3$ (use the equivalence of $x_1 \ldots x_n = 1$ and $\exists Y : x_1 x_2 Y = 1 \wedge \overline{Y} x_3 \cdots x_n = 1$).

Finally, we switch to the existential theory of equations with regular constraints in free monoids with involution. The key point of the translation here is the fact that rational languages P are in essence regular word languages over Γ such that $P \subseteq N$, where $N \subseteq \Gamma^*$ is the regular set of all freely reduced words. The language N is accepted by a deterministic finite automaton with $|\Gamma| + 1$ states. Then a positive constraint has just the interpretation over words and for

[2] The reason for keeping $X \notin P$ instead of $X \in \tilde{P}$ where $\tilde{P} = F(\Sigma) \setminus P$ is that complementation may involve an exponential blow-up of the state space.

a negative constraint we replace $X \notin P$ by $X \notin P \wedge X \in N$. Details are left to the reader.

As for the formulas $xyz = 1$, note that they have a solution if and only if they have a solution in freely reduced words. Then we can replace each subformulae $xyz = 1$ by the conjunction $\exists P \exists Q \exists R : x = PQ \wedge y = \overline{Q}R \wedge z = \overline{R}\,\overline{P}$ using simple arguments.

Using a standard procedure to replace a conjunction of word equations by a single word equation we may assume that our input is given by a single equation $L = R$ with $L, R \in (\Gamma \cup \Omega)^+$ and by two lists $(X_j \in P_j, 1 \leq j \leq m)$ and $(X_j \notin P_j, m < j \leq k)$ where each $P_j \subseteq \Gamma^*$ is specified by some non-deterministic automaton $\mathcal{A}_j = (Q_j, \Gamma, \delta_j, I_j, F_j)$.

The question is whether the input is satisfiable, i.e. whether there is a solution. At this point, Boolean matrices are a better representation than finite automata. Let Q be the disjoint union of the state spaces Q_j, assume $Q = \{1, \ldots, n\}$. Let $\delta = \bigcup_j \delta_j$, then $\delta \subseteq Q \times \Gamma \times Q$ and with each $a \in \Gamma$ we can associate a Boolean matrix $g(a) \in \mathbb{B}^{n \times n}$ such that $g(a)_{i,j}$ is the truth value of "$(i, a, j) \in \delta$".

Since our monoids need an involution, we will work with $2n \times 2n$-Boolean matrices. Henceforth M denotes the following monoid with involution,

$$M = \{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \mid A, B \in \mathbb{B}^{n \times n} \}$$

where $\overline{\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}} = \begin{pmatrix} B^T & 0 \\ 0 & A^T \end{pmatrix}$ and where the operator ^{T} means transposition. We define a homomorphism $h : \Gamma^* \to M$ by $h(a) = \begin{pmatrix} g(a) & 0 \\ 0 & g(\overline{a})^T \end{pmatrix}$ for $a \in \Gamma$, where the mapping $g : \Gamma \to \mathbb{B}^{n \times n}$ is defined as above. The homomorphism h can be computed in polynomial time and it respects the involution. Now, for each regular language P_j we compute vectors $I_j, F_j \in \mathbb{B}^{2n}$ such that for all $w \in \Gamma^*$ we have the equivalence: $w \in P_j \Leftrightarrow I_j^T h(w) F_j = 1$. Having done these computations we make a non-deterministic guess $\rho(X) \in M$ for each variable $X \in \Omega$. We verify $\rho(\overline{X}) = \overline{\rho(X)}$ for all $X \in \Omega$ and whenever there is a constraint of type $X \in P_j$ (resp. $X \notin P_j$) then we verify $I_j^T \rho(X) F_j = 1$ (resp. $I_j^T \rho(X) F_j = 0$).

Let us make a formal definition. Let $d, n \in \mathbb{N}$. We consider an equation of the length d over some Γ and Ω with constraints in M being specified by a list E containing the following items:

– The alphabet $(\Gamma, \overline{})$ with involution.
– A mapping $h : \Gamma \to M$ such that $h(\overline{a}) = \overline{h(a)}$ for all $a \in \Gamma$.
– The alphabet $(\Omega, \overline{})$ with involution without fixed points.
– A mapping $\rho : \Omega \to M$ such that $\rho(\overline{X}) = \overline{\rho(X)}$ for all $X \in \Omega$.
– The equation $L = R$ where $L, R \in (\Gamma \cup \Omega)^+$ and $|LR| = d$.

If no confusion arise, we will denote this list simply by

$$E = (\Gamma, \Omega, h, \rho, L, R).$$

A *solution* is a mapping $\sigma : \Omega \to \Gamma^*$ (being extended to a homomorphism $\sigma : (\Gamma \cup \Omega)^* \to \Gamma^*$ by leaving the letters from Γ invariant) such that the following three conditions are satisfied: $\sigma(L) = \sigma(R)$, $\sigma(\overline{X}) = \overline{\sigma(X)}$, and $h\sigma(X) = \rho(X)$ for all $X \in \Omega$. We refer to the list E as an equation with constraints (in M). By the reduction above, Theorem 1 is a consequence of:

Theorem 2. *The following problem can be solved in* PSPACE.
INPUT: An equation $E_0 = (\Gamma_0, \Omega_0, h_0, \rho_0, L_0, R_0)$.
QUESTION: Is there a solution $\sigma : \Omega \to \Gamma^*$*?*

3 Equations with regular constraints over free monoids with involution

During the procedure which solves Theorem 2 one has to consider various other equations with constraints in M. Following Plandowski we will use data compression for words in $(\Gamma \cup \Omega)^*$ in terms of exponential expressions.

Exponential expressions. Exponential expressions (their evaluation and their size) are inductively defined as follows:

- Every word $w \in \Gamma^*$ denotes an exponential expression. The evaluation $\mathrm{eval}(w)$ is equal to w, its size $\|w\|$ is equal to the length $|w|$.
- If e, e' are exponential expressions, so is ee', the evaluation is the concatenation, $\mathrm{eval}(ee') = \mathrm{eval}(e)\mathrm{eval}(e')$, and $\|ee'\| = \|e\| + \|e'\|$.
- If e be an exponential expression and $k \in \mathbb{N}$, then $(e)^k$ is an exponential expression, and $\mathrm{eval}((e)^k) = (\mathrm{eval}(e))^k$ and $\|(e)^k\| = \log(k) + \|e\|$.

It is not difficult to show that the length of $\mathrm{eval}(e)$ is at most exponential in the size of e. Moreover, let $u \in \Gamma^*$ be a factor of a word $w \in \Gamma^*$ which can be represented by some exponential expression of size p. Then we find an exponential expression of size at most $2p^2$ that represents the factor u.

We say that an exponential expression e is *admissible*, if its size $\|e\|$ is bounded by some fixed polynomial in the input size of the equation E_0. Let $E = (\Gamma, \Omega, h, \rho, L, R)$ and e_L, e_R be exponential expressions with $\mathrm{eval}(e_L) = L$ and $\mathrm{eval}(e_R) = R$. We say that $E_e = (\Gamma, \Omega, h, \rho, e_L, e_R)$ is *admissible*, if $e_L e_R$ is admissible, $|\Gamma \setminus \Gamma_0| \leq \|e_L e_R\| + 2d$, $\Omega \subseteq \Omega_0$, and $h(a) = h_0(a)$ for $a \in \Gamma \cap \Gamma_0$. We say that E_e *represents* the equation E. For two admissible equations with constraints E and E' we write $E \equiv E'$, if E and E' represent the same object.

Because of regular constraints, we have to formalize carefully the basic operations over these equations in order to move from one equation to another.

Base changes. Let $E' = (\Gamma', \Omega, h', \rho, L', R')$ be an equation. A mapping $\beta : \Gamma' \to \Gamma^*$ is a *base change* if both $\beta(\overline{a}) = \overline{\beta(a)}$ and $h'(a) = h\beta(a)$ for all $a \in \Gamma'$. The new equation is $\beta_*(E') = (\Gamma, \Omega, h, \rho, \beta(L), \beta(R))$. We say that β is *admissible* if $|\Gamma \cup \Gamma'|$ has polynomial size and if for each $a \in \Gamma'$, $\beta(a)$ has an admissible exponential representation.

If $\beta : \Gamma' \to \Gamma^*$ is an admissible base change and if $L' = R'$ is given by a pair of admissible exponential expressions, then we can represent $\beta_*(E')$ by some admissible equation with constraints which is computable in polynomial time.

Lemma 1. *Let E' be an equation with constraints in M and $\beta : \Gamma' \to \Gamma^*$ be a base change. If $\sigma' : \Omega \to \Gamma'^*$ is a solution of E', then $\sigma = \beta\sigma' : \Omega \to \Gamma^*$ is a solution of $\beta_*(E')$.*

Projections. Let $\Gamma \subseteq \Gamma'$ be alphabets with involution. A *projection* is a homomorphism $\pi : \Gamma'^* \to \Gamma^*$ preserving the involution and leaving Γ fixed. If $h : \Gamma \to M$ is given, then a projection π defines also $h' : \Gamma' \to M$ by $h' = h\pi$.

For an equation $E = (\Gamma, h, \Omega, \rho, L, R)$ we define $\pi^*(E) = (\Gamma', h\pi, \Omega, \rho, L, R)$. Note that every projection $\pi : \Gamma'^* \to \Gamma^*$ defines also a base change π_* such that $\pi_*\pi^*(E) = E$.

Lemma 2. *Let $\Gamma \subseteq \Gamma'$ be as above and let $E = (\Gamma, \Omega, h, \rho, L, R)$ and $E' = (\Gamma', \Omega, h', \rho, L, R)$. Then there is a projection $\pi : \Gamma'^* \to \Gamma^*$ such that $\pi^*(E) = E'$, if and only if both $h'(\Gamma') \subseteq h(\Gamma^*)$ and $a = \overline{a}$ implies $h'(a) \in h(\{w \in \Gamma^* \mid w = \overline{w}\})$ for all $a \in \Gamma'$. Moreover, if σ' is a solution of E', then we effectively find a solution σ for E with $|\sigma(L)| \leq 2|M||\sigma'(L)|$.*

Lemma 2 says that in order to test whether there exists a projection $\pi : \Gamma'^* \to \Gamma^*$ such that $\pi^*(E) = E'$, we need only space to store some Boolean matrices of $\mathbb{B}^{2n \times 2n}$, we do not need an explicit description of $\pi : \Gamma'^* \to \Gamma^*$ itself. Only if n becomes a substantial part of the input size, then we might need the full power of PSPACE (PSPACE–hardness of the satisfiability problem).

Shifts. Let $\Omega' \subseteq \Omega$ be a subset of the variables which is closed under involution, and let $\rho' : \Omega' \to M$ with $\rho'(\overline{x}) = \overline{\rho'(x)}$ (we do not require that ρ' is the restriction of ρ). A *shift* is a mapping $\delta : \Omega \to \Gamma^*\Omega'\Gamma^* \cup \Gamma^*$ such that the following conditions are satisfied:

i) $\delta(X) \in \Gamma^* X \Gamma^*$ for all $X \in \Omega'$,
ii) $\delta(X) \in \Gamma^*$ for all $X \in \Omega \setminus \Omega'$,
iii) $\delta(\overline{X}) = \overline{\delta(X)}$ for all $X \in \Omega$.

The mapping δ is extended to a homomorphism $\delta : (\Gamma \cup \Omega)^* \to (\Gamma \cup \Omega')^*$ by leaving the elements of Γ invariant. For and equation $E = (\Gamma, h, \Omega, \rho, L, R)$, we define the equation $\delta_*(E) = (\Gamma, \Omega', h, \rho', \delta(L), \delta(R))$ where ρ' is such that $\rho(X) = h(u)\rho'(X)h(v)$ for $\delta(X) = uXv$, and $\rho(X) = h(w)$ for $\delta(X) = w \in \Gamma^*$. We say that $\delta_*(E)$ is a *shift* of E.

Lemma 3. *In the notation of above, let $E' = \delta_*(E)$ for some shift $\delta : \Omega \to \Gamma^*\Omega\Gamma^* \cup \Gamma^*$. If $\sigma' : \Omega' \to \Gamma^*$ is a solution of E', then $\sigma = \sigma'\delta : \Omega \to \Gamma^*$ is a solution of E. Moreover, we have $\sigma(L) = \sigma'(L')$.*

Lemma 4. *The following problem can be solved in* PSPACE.

INPUT: Two equations with constraints E and E'.

QUESTION: Is there some shift $\delta : \Omega \to \Gamma^*\Omega\Gamma^* \cup \Gamma^*$ such that $\delta_*(E) \equiv E'$?

Moreover, if $\delta_*(E) \equiv E'$, then we have $\delta(X) = \mathrm{eval}(e_u)X\mathrm{eval}(e_v)$ for all $X \in \Omega'$ and for suitable admissible exponential expressions e_u, e_v. Similarly, $\delta(X) = \mathrm{eval}(e_w)$ for all $X \in \Omega \setminus \Omega'$.

Remark 1. We can think of a shift $\delta : \Omega \to \Gamma^*\Omega'\Gamma^* \cup \Gamma^*$ as a partial solution in the following sense. Assume we have an idea about $\sigma(X)$ for some $X \in \Omega$. Then we might guess $\sigma(X)$ entirely. In this case we can define $\delta(X) = \sigma(X)$ and we have $X \notin \Omega'$. For some other X we might guess only some prefix u and some suffix v of $\sigma(X)$. Then we define $\delta(X) = uXv$ and we have to guess some $\rho'(X) \in M$ such that $\rho(x) : h(u)\rho'(X)h(v)$. If our guess was correct, then such $\rho'(X)$ must exist. We have partially specified the solution and we continue this process by replacing the equation $L = R$ by the new equation $\delta(L) = \delta(R)$.

4 The Search Graph and Plandowski's algorithm

The nodes of the search graph are admissible equations with constraints in M. Let E, E' be two nodes. We define an arc $E \to E'$, if there are a projection π, a shift δ, and an admissible base change β such that $\delta_*(\pi^*(E)) \equiv \beta_*(E')$.

Lemma 5. *The following problem can be decided in* PSPACE.
INPUT: Admissible equations with constraints E and E'.
QUESTION: Is there an arc $E \to E'$ in the search graph?

Proof. (Sketch) We first guess some alphabet $(\Gamma'', \overline{})$ of polynomial size together with $h'' : \Gamma'' \to M$. Then we guess some admissible base change $\beta : \Gamma' \to \Gamma''^*$ such that $h' = h''\beta$ and we compute $\beta_*(E')$ in polynomial time. Next we check using Remark 1 and Lemma 4 that there is projection $\pi : \Gamma'' \to \Gamma$ and that there is a shift $\delta : \Omega \to \Gamma''^*\Omega'\Gamma''^* \cup \Gamma''^*$ such that $\delta_*(\pi^*(E)) \equiv \beta_*(E')$. ☐

Plandowski's algorithm works on $E_0 = (\Gamma_0, \Omega_0, h_0, \rho_0, L_0, R_0)$ as follows:

1. $E := E_0$
2. **while** $\Omega \neq \emptyset$ **do**
   Guess an admissible equation E' with constraints in M.
   Verify that $E \to E'$ is an arc in the search graph.
   $E := E'$
3. **return** "eval(e_L) = eval(e_R)"

By Lemmata 1, 2, and 3, if $E \to E'$ is an arc in the search graph and E' is solvable, then E is solvable, too. Thus, if the algorithm returns *true*, then E_0 is solvable. The proof of Theorem 2 is therefore reduced to the statement that if E_0 is solvable, then the search graph contains a path to some node without variables and the exponential expressions defining the equation evaluate to the same word (called a terminal node).

Remark 2. If $E \to E'$ is due to some $\pi : \Gamma''^* \to \Gamma^*$, $\delta : \Omega \to \Gamma''^*\Omega'\Gamma''^* \cup \Gamma''^*$, and $\beta : \Gamma'^* \to \Gamma''^*$, then a solution $\sigma' : \Omega' \to \Gamma'^*$ of E' yields the solution $\sigma = \pi(\beta\sigma')\delta$. Hence we may assume that the length of a solution has increased by at most an exponential factor. Since we are going to perform the search in a graph of at most exponential size, we get automatically a doubly exponential upper bound for the length of a minimal solution by backwards computation on such a path. This is still the best known upper bound (although an singly exponential bound is conjectured), see [17].

5 The Search Graph contains a path to a terminal node

This section is a proof of the existence of a path to a solvable solution in the Search Graph. The technique used is a generalization of the one used in [18] for word equations, in [9] for free group equations, and in [3] for word equations with regular constraints. Due to lack of space in this extended abstract we focus only on some few points where the technique differs substantially from those papers. For the other parts we will just refer the reader to the papers above.

The exponent of periodicity. Let $w \in \Gamma^*$ be a word. The exponent of periodicity $\exp(w)$ is defined as the supremum of the $\alpha \in \mathbb{N}$ such that $w = up^\alpha v$ for suitable $u, v, p \in \Gamma^*$ and $p \neq 1$. It is clear that $\exp(w) > 0$ if w is not empty. For an equation $E = (\Gamma, \Omega, h, \rho, L, R)$ the exponent of periodicity, denoted by $\exp(E)$, is defined as

$$\exp(E) = \inf\{\{\exp(\sigma(L)) \mid \sigma \text{ is a solution of } E\} \cup \{\infty\}\}.$$

The well-known result from word equations [11] transfers to the situation here: in order to prove Theorem 2 we may assume that E_0 is solvable and $\exp(E_0) \in 2^{\mathcal{O}(d+n\log n)}$. The case of word equations with regular constraints in done in [3] and for monoids with involution in [8]. A combinations of these methods give what we need here. The detailed proof has been given in [10].

Free intervals. The following development will be fully justified at the end of the subsection and has to do with handling the constraints. Without constraints, free intervals of length more than one do not appear in a minimal solutions, making this notion unnecessary. This is not true in the presence of constraints. Free intervals handle this case and moreover, tell us that the bounds on the exponent of periodicity are the only restriction we need on solutions.

Given a word $w \in \Gamma^*$, let $\{0, \ldots, |w|\}$ be the set of its *positions*. An *interval* on these positions is a formal object denoted $[\alpha, \beta]$ with $0 \leq \alpha, \beta \leq |w|$, and $\overline{[\alpha, \beta]} = [\beta, \alpha]$. For $w = a_1 \cdots a_m$, we define $w[\alpha, \beta] = a_{\alpha+1} \cdots a_\beta$ if $\alpha < \beta$, $w[\alpha, \beta] = \overline{a_{\alpha+1} \cdots a_\beta}$ if $\alpha > \beta$, and the empty word if $\alpha = \beta$. Observe that these notations are consistent so that $\overline{w[\alpha, \beta]} = w\overline{[\alpha, \beta]}$.

Let σ_0 be a solution of $L = R$, where $L_0 = x_1 \cdots x_g$ and $R_0 = x_{g+1} \cdots x_d$ and $x_i \in (\Gamma_0 \cup \Omega_0)$. Then we have $w_0 = \sigma_0(L_0) = \sigma_0(R_0)$. Denote $m_0 = |w_0|$. For each $i \in \{1, \ldots, d\}$ we define positions $\mathrm{l}(i)$ and $\mathrm{r}(i)$ as follows:

$$\begin{aligned} \mathrm{l}(i) &= |\sigma_0(x_1 \cdots x_{i-1})| \bmod m_0 \in \{0, \ldots, m_0 - 1\}, \\ \mathrm{r}(i) &= |\sigma_0(x_{i+1} \cdots x_d)| \bmod m_0 \in \{1, \ldots, m_0\}. \end{aligned}$$

In particular, we have $\mathrm{l}(1) = \mathrm{l}(g+1) = 0$ and $\mathrm{r}(g) = \mathrm{r}(d) = m_0$. The set of l and r positions is called the set of *cuts*. There are at most d cuts which cut the word w_0 in at most $d - 1$ factors. We say that $[\alpha, \beta]$ contains a cut γ if $\min\{\alpha, \beta\} < \gamma < \max\{\alpha, \beta\}$.

For convenience we henceforth assume $2 \leq g < d < m_0$ whenever necessary and make the assumption that $\sigma_0(x_i) \neq 1$ for all $1 \leq i \leq d$ (e.g. a guess in some preprocessing).

We have $\sigma_0(x_i) = w_0[\mathrm{l}(i), \mathrm{r}(i)]$ and $\sigma_0(\overline{x_i}) = w_0[\mathrm{r}(i), \mathrm{l}(i)]$ for $1 \le i \le d$. By our assumption, the interval $[\mathrm{l}(i), \mathrm{r}(i)]$ is positive.

Let us consider $i, j \in 1, \ldots, d$ and $x_i = x_j$ or $x_i = \overline{x_j}$. For $0 \le \mu, \nu \le \mathrm{r}(i) - \mathrm{l}(i)$, we define a relation $\sim$ among intervals as follows:

$$[\mathrm{l}(i) + \mu, \mathrm{l}(i) + \nu] \sim [\mathrm{l}(j) + \mu, \mathrm{l}(j) + \nu], \text{ if } x_i = x_j,$$
$$[\mathrm{l}(i) + \mu, \mathrm{l}(i) + \nu] \sim [\mathrm{r}(j) - \mu, \mathrm{r}(j) - \nu], \text{ if } x_i = \overline{x_j}.$$

Note that $\sim$ is a symmetric relation and $[\alpha, \beta] \sim [\alpha', \beta']$ implies both $[\beta, \alpha] \sim [\beta', \alpha']$ and $w_0[\alpha, \beta] = w_0[\alpha', \beta']$. By $\approx$ we denote the equivalence relation obtained by the reflexive and transitive closure of $\sim$.

An interval $[\alpha, \beta]$ is called *free* if none of its $\approx$-equivalent intervals contains a cut. Clearly, the set of free intervals is closed under involution and whenever $|\beta - \alpha| \le 1$ then $[\alpha, \beta]$ is free. It is also closed under taking subintervals:

Lemma 6. *Let $[\alpha, \beta]$ be a free interval and $\min\{\alpha, \beta\} \le \mu, \nu \le \max\{\alpha, \beta\}$. Then the interval $[\mu, \nu]$ is also free.*

If $[\alpha, \beta]$ (assume $\alpha < \beta$) is not free, then by definition there is some interval $[\alpha', \beta'] \approx [\alpha, \beta]$ which contains a cut γ'. The propagation of that cut to $[\alpha, \beta]$, that is the position γ such that $\gamma - \alpha = |\gamma' - \alpha'|$ is called an *implicit cut* of $[\alpha, \beta]$.

The following observation will be used throughout: If we have $\alpha \le \mu < \gamma < \nu \le \beta$ and γ is an implicit cut of $[\alpha, \beta]$, then γ is also an implicit cut of $[\mu, \nu]$. (The converse is not necessarily true.)

Lemma 7. *Let $0 \le \alpha \le \alpha' < \beta \le \beta' \le m_0$ be such that $[\alpha, \beta]$ and $[\alpha', \beta']$ are free intervals. Then the interval $[\alpha, \beta']$ is free, too.*

A free interval $[\alpha, \beta]$ is called *maximal free* if no free interval properly contains it, i.e., if $\alpha' \le \min\{\alpha, \beta\} \le \max\{\alpha, \beta\} \le \beta'$ and $[\alpha', \beta']$ free, then and $\beta' - \alpha' = |\beta - \alpha|$. So Lemma 7 states a key point that maximal free intervals do not overlap.

Lemma 8. *Let $[\alpha, \beta]$ be a maximal free interval. Then there are intervals $[\gamma, \delta]$ and $[\gamma', \delta']$ such that $[\alpha, \beta] \approx [\gamma, \delta] \approx [\gamma', \delta']$ and γ and δ' are cuts.*

Proposition 1. *Let Γ be the set of words $w \in \Gamma_0^*$ such that there is a maximal free interval $[\alpha, \beta]$ with $w = w_0[\alpha, \beta]$. Then Γ is a subset of Γ_0^+ of size at most $2d - 2$. The set Γ is closed under involution.*

Proof. Let $[\alpha, \beta]$ be maximal free. Then $|\beta - \alpha| \ge 1$ and $[\beta, \alpha]$ is maximal free, too. Hence $\Gamma \subseteq \Gamma_0^+$ and Γ is closed under involution. By Lemma 8 we may assume that α is a cut. Say $\alpha < \beta$. Then $\alpha \ne m_0$ and there is no other maximal free interval $[\alpha, \beta']$ with $\alpha < \beta'$ because of Lemma 7. Hence there are at most $d - 1$ such intervals $[\alpha, \beta]$. Symmetrically, there are at most $d - 1$ maximal free intervals $[\alpha, \beta]$ where $\beta < \alpha$ and α is a cut. $\square$

Why free intervals are needed. For a moment let us put $\Delta = \Gamma_0 \cup \Gamma$ where Γ is the set defined in Proposition 1. Observe that $\Delta \subseteq \Gamma_0^+$, and so it defines a natural projection $\pi : \Gamma_0^* \to \Delta$ and a mapping $h' : \Gamma_0^* \to M$ by $h' = h_0\pi$. (Note that here we need the fact that there is no overlapping among maximal intervals.) Consider the equation with constraints $\pi^*(E_0)$. There is an arc from E_0 to $\pi^*(E_0)$ since we may always allow the base change to be the identity and the shift to be an inclusion.

The reason to switch from Γ_0 to Δ is that, due to the constraints, the word w_0 may have long free intervals. Over Δ this can be avoided. Formally, we replace w_0 by a solution w_0' where $w_0' \in \Gamma^*$, whose definition is based on a factorization of w_0 in maximal free intervals. Recall that there is a unique sequence $0 = \alpha_0 < \alpha_1 < \cdots < \alpha_k = m_0$ such that $[\alpha_{i-1}, \alpha_i]$ are maximal free intervals and

$$w_0 = w_0[\alpha_0, \alpha_i] \cdots w_0[\alpha_k - 1, \alpha_k].$$

Moreover, all cuts occur as some α_p, so we can think of the factors $w_0[\alpha_{i-1}, \alpha_i]$ as letters in Γ. Because all constants which appear in L_0, R_0 are elements of Γ, the equation $L_0 = R_0$ appears identical in $\pi^*(E_0)$.

So, replacing w_0 by the word $w_0' \in \Gamma^*$, we can define $\sigma : \Omega \to \Gamma^*$ such that both $\sigma(L_0) = \sigma(R_0) = w_0'$ and $\rho_0 = h_0'\sigma$, that is, σ is a solution of $\pi^*(E)$. Clearly we have $w_0 = \pi(w_0')$ and $\exp(w_0') \leq \exp(w_0)$. The crucial point is that w_0' has no long free intervals anymore. (With respect to w_0' and Γ_0', all maximal free intervals have length exactly one.)

We can assume that Plandowski's algorithm follows in a first step exactly the arc from E_0 to $\pi^*(E_0)$. Phrased in a different way, we may assume that $E_0 = \pi^*(E_0)$, hence Γ is a subset Γ_0.

Moreover, the inclusion $\beta : \Gamma \to \Gamma_0^*$ defines an admissible base change. Consider $E_0' = \beta_*(\pi^*(E_0))$. Then we have $E_0' = (\Gamma, \Omega_0, h, \rho_0, L_0, R_0)$ where h is the restriction of $h_0 : \Gamma_0 \to M$. The search graph contains an arc from E_0 to E_0' and E_0' has a solution σ with $\sigma(L_0) = w_0'$ with $\exp(w_0') \leq \exp(w_0)$.

In summary, in order to save notations we may assume for simplicity that $E_0 = E_0'$ and $w_0 = w_0'$. We can make the following assumptions:

$$\begin{aligned}
L_0 &= x_1 \cdots x_g \text{ and } g \geq 2,\\
R_0 &= x_{g+1} \cdots x_d \text{ and } d > g,\\
\Gamma_0 &= \Gamma \text{ and } |\Gamma| \leq 2d - 2,\\
|\Omega_0| &\leq 2d,\\
M &\subseteq \mathbb{B}^{2n \times 2n}.
\end{aligned}$$

All variables X occur in $L_0 R_0 \overline{L_0 R_0}$. There is a solution $\sigma : \Omega_0 \to \Gamma$ such that $w_0 = \sigma(L_0) = \sigma(R_0)$ with $\sigma(X_i) \neq 1$ for $1 \leq i \leq d$ and $\rho_0 = h\sigma = h_0\sigma$. We have $|w_0| = m_0$ and $\exp(w_0) \in 2^{\mathcal{O}(d + n\log n)}$. All maximal free intervals have length exactly one, i.e., every positive interval $[\alpha, \beta]$ with $\beta - \alpha > 1$ contains an implicit cut.

The ℓ-factorization. For each integer ℓ, $1 \leq \ell \leq m_0$, we define the set of *critical words* C_ℓ as the closure under involution of set of all words $w_0[\gamma - \ell, \gamma + \ell]$ where γ is a cut with $\ell \leq \gamma \leq m_0 - \ell$.

A triple $(u, w, v) \in (\{1\} \cup \Gamma^\ell) \times \Gamma^+ \times (\{1\} \cup \Gamma^\ell)$ is called a *block* if, first, first, up to a possible prefix or suffix no other factor of the word uwv is a critical word, second, $u \neq 1$ if and only if a prefix of uwv of length 2ℓ belongs to C_ℓ, and third, $v \neq 1$ if and only if a suffix of uwv of length 2ℓ belongs to C_ℓ. The set of blocks is denoted by B_ℓ and can be viewed (as a possibly infinite) alphabet with involution defined by $\overline{(u, w, v)} = (\overline{v}, \overline{w}, \overline{u})$.

We can define a homomorphism $\pi_\ell : B_\ell^* \to \Gamma^*$ by $\pi_\ell(u, w, v) = w \in \Gamma^+$ being extended to a projection $\pi_\ell : (B_\ell \cup \Gamma)^* \to \Gamma^*$ by leaving Γ invariant. We define $h_\ell : (B_\ell \cup \Gamma) \to M$ by $h_\ell = h\pi_\ell$. In the following we shall consider finite subsets $\Gamma_\ell \subseteq B_\ell \cup \Gamma$ which are closed under involution. Then by $\pi_\ell : \Gamma_\ell^* \to \Gamma^*$ and $h_\ell : \Gamma_\ell^* \to M$ we understand the restrictions of the respective homomorphisms.

For every non-empty word $w \in \Gamma^+$ we define its *ℓ-factorization* as:

$$F_\ell(w) = (u_1, w_1, v_1) \cdots (u_k, w_k, v_k) \in B_\ell^+ \tag{1}$$

where $w = w_1 \cdots w_k$ and for $1 \leq i \leq k$ the following conditions are satisfied:

- v_i is a prefix of $w_{i+1} \cdots w_k$ and $v_i = 1$ if and only if $i = k$.
- u_i is a suffix of $w_1 \cdots w_{i-1}$ and $u_i = 1$ if and only if $i = 1$.

Note that the ℓ-factorization of a word w is unique. For a factorization (1), we define $\mathrm{head}_\ell(w) = w_1$, $\mathrm{body}_\ell(w) = w_2 \cdots w_{k-1}$ and $\mathrm{tail}_\ell(w) = w_k$. Similarly for $\mathrm{Head}_\ell(w) = (u_1, w_1, v_1)$, $\mathrm{Body}_\ell(w) = (u_2, w_2, v_2) \cdots (u_{k-1}, w_{k-1}, v_{k-1})$, and $\mathrm{Tail}_\ell(w) = (u_k, w_k, v_k)$. For $k \geq 2$ (in particular, if $\mathrm{body}_\ell(w) \neq 1$) we have

$$F_\ell(w) = \mathrm{Head}_\ell(w)\mathrm{Body}_\ell(w)\mathrm{Tail}_\ell(w) \quad \text{and} \quad w = \mathrm{head}_\ell(w)\mathrm{body}_\ell(w)\mathrm{tail}_\ell(w).$$

Moreover, u_2 is a suffix of w_1 and v_{k-1} is a prefix of w_k.

Assume $\mathrm{body}_\ell(w) \neq 1$ and let $u, v \in \Gamma^*$ be any words. Then we can view w in the context uwv and $\mathrm{Body}_\ell(w)$ appears as a proper factor in the ℓ-factorization of uwv. More precisely, let $F_\ell(uwv) = (u_1, w_1, v_1) \cdots (u_k, w_k, v_k)$. Then there are unique $1 \leq p < q \leq k$ such that:

$$F_\ell(uwv) = (u_1, w_1, v_1) \cdots (u_p, w_p, v_p)\mathrm{Body}_\ell(w)(u_q, w_q, v_q) \cdots (u_k, w_k, v_k)$$
$$w_1 \cdots w_p = u\,\mathrm{head}_\ell(w) \quad \text{and} \quad w_q \cdots w_k = \mathrm{tail}_\ell(w)v$$

Finally, we note that the above definitions are compatible with the involution. We have $F_\ell(\overline{w}) = \overline{F_\ell(w)}$, $\mathrm{Head}_\ell(\overline{w}) = \overline{\mathrm{Tail}_\ell(w)}$, and $\mathrm{Body}_\ell(\overline{w}) = \overline{\mathrm{Body}_\ell(w)}$.

The ℓ-transformation. Recall that $E_0 = (\Gamma, \Omega_0, h, \rho_0, x_1 \cdots x_g, x_{g+1} \cdots x_d)$ is our equation with constraints. We start with the ℓ-factorization of $w_0 = \sigma(x_1 \cdots x_g) = \sigma(x_{g+1} \cdots x_d)$. Let

$$F_\ell(w_0) = (u_1, w_1, v_1) \cdots (u_k, w_k, v_k).$$

A sequence $S = (u_p, w_p, v_p) \cdots (u_q, w_q, v_q)$ with $1 \leq p \leq q \leq k$ is called an *ℓ-factor*. We say that S is a *cover* of a positive interval $[\alpha, \beta]$, if both $|w_1 \cdots w_{p-1}| \leq \alpha$ and $|w_{q+1} \cdots w_k| \leq m_0 - \beta$. Thus, $w_0[\alpha, \beta]$ becomes a factor of $w_p \cdots w_q$. It is called a *minimal cover* if neither $(u_{p+1}, w_{p+1}, v_{p+1}) \cdots (u_q, w_q, v_q)$

nor $(u_p, w_p, v_p) \cdots (u_{q-1}, w_{q-1}, v_{q-1})$ is a cover of $[\alpha, \beta]$. The minimal cover exists and it is unique.

We let $\Omega_\ell = \{ X \in \Omega_0 \mid \mathrm{body}_\ell(\sigma(X)) \neq 1 \}$, and we are going to define a new left-hand side $L_\ell \in (B_\ell \cup \Omega_\ell)^*$ and a new right-hand side $R_\ell \in (B_\ell \cup \Omega_\ell)^*$. For L_ℓ we consider those $1 \leq i \leq g$ where $\mathrm{body}_\ell(\sigma(x_i)) \neq 1$. Note that this implies $x_i \in \Omega_\ell$ since $\ell \geq 1$ and then the body of a constant is always empty. Recall the definition of $\mathrm{l}(i)$ and $\mathrm{r}(i)$, and define $\alpha = \mathrm{l}(i) + |\mathrm{head}_\ell(\sigma(x_i))|$ and $\beta = \mathrm{r}(i) - |\mathrm{tail}_\ell(\sigma(x_i))|$. Then we have $w_0[\alpha, \beta] = \mathrm{body}_\ell(\sigma(x_i))$. Next consider the ℓ-factor $S_i = (u_p, w_p, v_p) \cdots (u_q, w_q, v_q)$ which is the minimal cover of $[\alpha, \beta]$. Then we have $1 < p \leq q < k$ and $w_p \cdots w_q = w_0[\alpha, \beta] = \mathrm{body}_\ell(\sigma(x_i))$. The definition of S_i depends only on x_i, but not on the choice of the index i.

We replace the ℓ-factor S_i in $F_\ell(w_0)$ by the variable x_i. Having done this for all $1 \leq i \leq g$ with $\mathrm{body}_\ell(\sigma(x_i)) \neq 1$ we obtain the left-hand side $L_\ell \in (B_\ell \cup \Omega_\ell)^*$ of the ℓ-transformation E_ℓ. For R_ℓ we proceed analogously by replacing those ℓ-factors S_i where $\mathrm{body}_\ell(\sigma(x_i)) \neq 1$ and $g + 1 \leq i \leq d$.

For E_ℓ we cannot use the alphabet B_ℓ, because it might be too large or even infinite. Therefore we let Γ'_ℓ be the smallest subset of B_ℓ which is closed under involution and which satisfies $L_\ell R_\ell \in (\Gamma'_\ell \cup \Omega_\ell)^*$. We let $\Gamma_\ell = \Gamma'_\ell \cup \Gamma$. The projection $\pi_\ell : \Gamma_\ell^* \to \Gamma^*$ and the mapping $h_\ell : \Gamma_\ell \to M$ are defined by the restriction of $\pi_\ell : B_\ell \to \Gamma^*$, $\pi_\ell(u, w, v) = w$ and $h_\ell(u, w, v) = h(w) \in M$ and by $\pi_\ell(a) = a$ and $h_\ell(a) = h(a)$ for $a \in \Gamma$.

Finally, we define the mapping $\rho_\ell : \Omega_\ell \to M$ by $\rho_\ell(X) = h(\mathrm{body}_\ell(\sigma(X)))$. This yields the definition of the ℓ-transformation: $E_\ell = (\Gamma_\ell, \Omega_\ell, h_\ell, \rho_\ell, L_\ell, R_\ell)$.

The ℓ-transformation E_ℓ is admissible. The proof of the following proposition uses standard techniques like those in [18] and [9] and it is therefore omitted.

Proposition 2. *There is a polynomial of degree four such that each E_ℓ is admissible for all $\ell \geq 1$.*

At this stage we know that all ℓ-transformations are admissible. Thus, the equations $E_1, \ldots, E_{m_0}$ are nodes of the search graph. What is left to prove is that the search graph contains arcs $E_0 \to E_1$ and $E_\ell \to E_{\ell+1}$ for $1 \leq \ell < \ell' \leq 2\ell$. This involves again the concept of base change, projection, and shift. But the presence of constraints does not interfere very much anymore.t Thus, the technical details are similar to those of Plandowski's paper [18] as generalized in [9].

Acknowledgement. C. Gutiérrez was supported by FONDAP, Matemáticas Aplicadas.

References

1. M. Benois. Parties rationelles du groupe libre. *C. R. Acad. Sci. Paris, Sér. A*, 269:1188–1190, 1969.
2. J. Berstel. *Transductions and context-free languages.* Teubner Studienbücher, Stuttgart, 1979.
3. V. Diekert. Makanin's Algorithm. In M. Lothaire, *Algebraic Combinatorics on Words.* Cambridge University Press, 2001. To appear. A preliminary version is on the web: http: //www-igm.univ-mlv.fr/ berstel/Lothaire/index.html.

4. V. Diekert and M. Lohrey. A note on the existential theory of plain groups. Submitted for publication, 2000.
5. V. Diekert, Yu. Matiyasevich, and A. Muscholl. Solving word equations modulo partial commutations. *Th. Comp. Sc.*, 224:215–235, 1999. Special issue of LFCS'97.
6. Yu. Gurevich and A. Voronkov. Monadic simultaneous rigid E-unification and related problems. In P. Degano et al., editor, *Proc. 24th ICALP, Bologna (Italy) 1997*, number 1256 in Lect. Not. Comp. Sc., pages 154–165. Springer, 1997.
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. Equations in free semigroups with anti-involution and their relation to equations in free groups. In G. H. Gonnet et al., editor, *Proc. Lat. Am. Theor. Inf., LATIN'2000*, number 1776 in LNCS, pages 387–396. Springer, 2000.
9. C. Gutiérrez. Satisfiability of equations in free groups is in PSPACE. In *32nd ACM Symp. on Theory of Computing (STOC'2000)*, pages 21–27. ACM Press, 2000.
10. Ch. Hagenah. *Gleichungen mit regulären Randbedingungen über freien Gruppen.* PhD-thesis, Institut für Informatik, Universität Stuttgart, 2000.
11. A. Kościelski and L. Pacholski. Complexity of Makanin's algorithm. *Journal of the Association for Computing Machinery*, 43(4):670–684, 1996. Preliminary version in *Proc. of the 31st Ann. Symp. on Foundations of Computer Science, FOCS 90*, pages 824–829, Los Alamitos, 1990. IEEE Computer Society Press.
12. D. Kozen. Lower bounds for natural proof systems. In *Proc. of the 18th Ann. Symp. on Foundations of Computer Science, FOCS 77*, pages 254–266, Providence, Rhode Island, 1977. IEEE Computer Society Press.
13. 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).
14. 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).
15. 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.
16. P. Narendran and F. Otto. The word matching problem is undecidable for finite special string-rewriting systems that are confluent. In P. Degano et al., editor, *Proc. 24th ICALP, Bologna (Italy) 1997*, number 1256 in Lect. Not. Comp. Sc., pages 638–648. Springer, 1997.
17. W. Plandowski. Satisfiability of word equations with constants is in NEXPTIME. In *Proc. 31st Ann. Symp. on Theory of Computing, STOC'99*, pages 721–725. ACM Press, 1999.
18. W. Plandowski. Satisfiability of word equations with constants is in PSPACE. In *Proc. of the 40th Ann. Symp. on Foundations of Computer Science, FOCS 99*, pages 495–500. IEEE Computer Society Press, 1999.
19. W. Plandowski and W. Rytter. Application of Lempel-Ziv encodings to the solution of word equations. In Kim G. Larsen et al., editors, *Proc. of the 25th ICALP, 1998*, number 1443 in Lect. Not. Comp. Sc., pages 731–742. Springer, 1998.
20. W. Rytter. On the complexity of solving word equations. Lecture given at the 16th British Colloquium on Theoretical Computer Science, Liverpool (http://www.csc.liv.ac.uk/ bctcs16/abstracts.html), 2000.
21. K. U. Schulz. Makanin's algorithm for word equations — Two improvements and a generalization. In Klaus U. Schulz, editor, *Word Equations and Related Topics*, number 572 in Lect. Not. Comp. Sc., pages 85–150. Springer, 1991.