Habib Abdulrab Jean-Pierre Pécuchet (Eds.)

Word Equations and Related Topics

Second International Workshop, IWWERT '91
Rouen, France, October 7-9, 1991
Proceedings

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Volume Editors

Habib Abdulrab
Jean-Pierre Pécuchet
LMAI Laboratory, INSA de Rouen
PO 08, F-76131 Mont-Saint-Aignan Cedex, France

CR Subject Classification (1991): F.4.1-3, E.1, I.2.3

ISBN 3-540-56730-5 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-56730-5 Springer-Verlag New York Berlin Heidelberg

Typesetting: Camera ready by author
45/3140-543210 - Printed on acid-free paper

Preface

This volume contains papers presented at the second International Workshop on Word Equations and Related Topics (IWWERT '91), which was held in SCUEOR, University of Rouen, from the 7th to the 9th of October 1991.

Motivated by various activities and new results in the past five years, and by the first IWWERT, which was organized in October 1990 in Tübingen, FRG, by Prof. K.U. Schulz, the contribution of the second IWWERT '91 was a very good continuation of the first one.

Several researchers working on word equations and on their applications (logic programming, automatic demonstration, system of formal calculus, combinatory of words, etc.) were present and very active at the workshop.

The workshop was chaired by Prof. G.S. Makanin whose historical contribution in this area is well known. A new research project aiming at finding a new finite description of the general solution of word equations is presented in this workshop by G.S. Makanin.

We would like to express our great thanks to LIR (Laboratoire d'Informatique de Rouen/Université de Rouen) and LMI (Laboratoire de Mathématique et Informatique/ INS de Rouen), to all the speakers and authors, and to Springer-Verlag for their optimal collaboration.

Rouen, March 1993

H. Abdulrab and J.P. Pécuchet

On general solution of equations in a free semigroup

G.S. Makanin

Steklov Mathematical Institute, Moscow

Suppose Π is a free semigroup with finite alphabet of generator

$$a_1, a_2 \ldots, a_k \qquad (1)$$

A *coefficientless* equation in Π is given by an alphabet of word variables

$$x_1, x_2 \ldots, x_n \qquad (2)$$

and a *noncancellable* equation

$$\varphi(x_1, x_2 \ldots, x_n) = \psi(x_1, x_2 \ldots, x_n) \qquad (3)$$

A list of words in the alphabet (1) $X_1, X_2 \ldots, X_n$ is called a *solution* of the equation (2), (3) whenever the words $\varphi(X_1, X_2 \ldots, X_n) = \psi(X_1, X_2 \ldots, X_n)$ coincide.

By of equation (2), (3) in Π we mean a description of all solutions of this equation by means of free word variables. In addition, the number of free word variables must not exceed n-1.

The general solution of any equation in two variables $\varphi(x_1, x_2) = \psi(x_1, x_2)$ is of the form $x_1 = (u)^\lambda$, $x_2 = (u)^\mu$, where u is a free word variable, λ and μ are either natural parameters or natural integers.

The general solution of any equation in three variables $x_1x_2x_3 = x_3x_2x_1$ is of the form $x_1 = (u_1u_2)^\lambda u_1$, $x_2 = u_2(u_1u_2)^\mu$, $x_3 = (u_1u_2)^\nu u_1$, where u_1 and u_2 are free word variables and the λ, μ, ν are natural parameters.

The general solution of any equation in three variables $\varphi(x_1, x_2, x_3) = \psi(x_1, x_2, x_3)$ is representable by a finite number of formulas which is constructed from free word variables u_1, u_2 by means of operation of multiplication and raising to a power with a variable exponent.

The general solution of the equation $x_1x_2x_3 = x_3x_4x_1$ is not representable by a finite number of formulas which is constructed from free word variables u_1, u_2, u_3 by means of operation of multiplication and raising to a power with a variable exponent.

Let $\tau = (\alpha_1, \alpha_2, \ldots, \alpha_q)$ be an arbitrary vector of integers. The integer α_q will be denoted by the symbol $\omega(\tau)$, the number q by $\upsilon(\tau)$. If $\upsilon(\tau) > 1$, the vector $(\alpha_1, \alpha_2, \ldots, \alpha_{q-1})$ will be denoted by the symbol $\mu(\tau)$.

We define here the function $[u_1, u_2, \ldots, u_p]_i^\tau$, where $p > 1$; $i = 1, 2, \ldots, p$; $u_1, u_2, \ldots, u_p$ are word variables; and τ is a vector of integers.

— If $\upsilon(\tau) = 1$, then

$[u_1, u_2, \ldots, u_p]_i^\tau \stackrel{\text{def}}{=} u_i$, $1 \le i \le p$.

— If $\upsilon(\tau) > 1$ and $\omega(\tau) \ge 0$, then

1) if $i = 1$,

$[u_1, u_2, \ldots, u_p]_i^\tau \stackrel{\text{def}}{=} ([u_1, u_2, \ldots, u_p]_2^{\mu(\tau)} [u_1, u_2, \ldots, u_p]_1^{\mu(\tau)})^{\omega(\tau)+1} [u_1, u_2, \ldots, u_p]_2^{\mu(\tau)}$

2) if $2 \le i \le p-1$

$[u_1, u_2, \ldots, u_p]_i^\tau \stackrel{\text{def}}{=} [u_1, u_2, \ldots, u_p]_{i+1}^{\mu(\tau)}$

3) if $i = p$,

$[u_1, u_2, \ldots, u_p]_i^\tau \stackrel{\text{def}}{=} ([u_1, u_2, \ldots, u_p]_2^{\mu(\tau)} [u_1, u_2, \ldots, u_p]_1^{\mu(\tau)})^{\omega(\tau)} [u_1, u_2, \ldots, u_p]_2^{\mu(\tau)}$

— If $\upsilon(\tau) > 1$ and $\omega(\tau) < 0$, then

1) if $i = 1$

$[u_1, u_2, \ldots, u_p]_i^\tau \stackrel{\text{def}}{=} ([u_1, u_2, \ldots, u_p]_{p-1}^{\mu(\tau)} [u_1, u_2, \ldots, u_p]_p^{\mu(\tau)})^{-\omega(\tau)-1} [u_1, u_2, \ldots, u_p]_{p-1}^{\mu(\tau)}$

2) if $2 \le i \le p-1$

$[u_1, u_2, \ldots, u_p]_i^\tau \stackrel{\text{def}}{=} [u_1, u_2, \ldots, u_p]_{i-1}^{\mu(\tau)}$

3) if $i = p$

$[u_1, u_2, \ldots, u_p]_i^\tau \stackrel{\text{def}}{=} ([u_1, u_2, \ldots, u_p]_{p-1}^{\mu(\tau)} [u_1, u_2, \ldots, u_p]_p^{\mu(\tau)})^{-\omega(\tau)} [u_1, u_2, \ldots, u_p]_{p-1}^{\mu(\tau)}$

The general solution of mirror equation in p variables

$$x_1 x_2 \ldots x_{p-1} x_p = x_p x_{p-1} \ldots x_2 x_1 \qquad (4)$$

is represented by means of the following formulas

$X_i = [1, y_1, y_2, \ldots, y_{p-i}]_i^\tau \quad (i = 1, 2, \ldots, p) \qquad y_1 y_2 \ldots y_{p-1} = y_{p-1} \ldots y_2 y_1$

$$X_i = [y_1, y_2, \dots, y_{p-1}, 1]_i^\tau \quad (i = 1, 2, \dots, p) \qquad y_1y_2 \cdots y_{p-1} = y_{p-1} \cdots y_2y_1 \quad (5)$$

$$X_i = [y_{p-1}, y_1, y_2, \dots, y_{p-2}, y_{p-1}]_i^\tau \quad (i = 1, 2, \dots, p) \qquad y_1y_2 \cdots y_{p-2} = y_{p-2} \cdots y_2y_1$$

Here τ is an arbitrary vector of integers, and $y_1, y_2, \dots, y_{p-1}$ are word variables connected by corresponding mirror equation with less than p variables.

Using the formulas (5) it is easy to construct a finite number of formulas describing the general solution of mirror equation (4).

By an *elementary* equation in *n* variables we mean an equation of the form

$$x_1x_2 \dots x_{n-1}x_n = x_{i_1}x_{i_2} \dots x_{i_n} \quad (6)$$

where $i_1, \dots, i_n$ is a permutation of $1, \dots, n$, and $i_1 \neq 1$, $i_n \neq n$.

For each elementary equation (6) we can construct some corresponding formulas (similar to formulas for mirror equation) which describe the general solution of equation (6).

Hypothesis

The general solution of any equation in n variables $\varphi(x_1, x_2 \dots, x_n) = \psi(x_1, x_2 \dots, x_n)$ is represented by a finite number of formulas constructed from formulas of elementary equations.

An equation (2), (3) is called *full* if both $\varphi(x_1, x_2 \dots, x_n)$ and $\psi(x_1, x_2 \dots, x_n)$ contain all letters $x_1, x_2, \dots, x_n$.

By a *directed equation* in Π, we mean an equation of the form $x_t\varphi(x_1, x_2 \dots, x_n) = x_s\psi(x_1, x_2 \dots, x_n)$ with the additional condition $\partial x_t > \partial x_s$.

This directed equation will be written as follows

$$x_t\varphi(x_1, x_2 \dots, x_n) \rightarrow x_s\psi(x_1, x_2 \dots, x_n)$$

It is easy to show that the general solution of any equation in Π is representable by means of general solutions corresponding to directed equations in Π.

Let

$$x_1\varphi(x_1, x_2 \dots, x_n) \rightarrow x_2\alpha(x_2, \dots, x_n)x_1\beta(x_1, x_2 \dots, x_n) \quad (7)$$

be an arbitrary directed equation in Π, (with a possible renumbering of variables).

The transformation of this equation

$$x_1 \rightarrow x_2\alpha_1(x_2, \dots, x_n)(\alpha_2(x_2, \dots, x_n)x_2\alpha_1(x_2 \dots, x_n))^\lambda x_1 \quad (8)$$

where $\alpha(x_2, \dots, x_n)$ is identical to $\alpha_1(x_2 \dots, x_n)\alpha_2(x_2, \dots, x_n)$, and λ is a natural parameter, is called *complete*.

The result of applying the complete transformation (8) to the equation (7) is the directed full equation

$$x_1\varphi(\tilde{x}_1, x_2 \ldots, x_n) \leftarrow \alpha_2(x_2, \ldots, x_n)x_2\alpha_1(x_2 \ldots, x_n)x_1\beta(\tilde{x}_1, x_2 \ldots, x_n) \qquad (9)$$

where $\tilde{x}_1$ is the right-hand side of transformation (8).

Starting from the equation (7) and applying the complete transformation (8), we construct a list of directed full equations $\Sigma_1, \ldots, \Sigma_{\delta\alpha+1}$ with natural parameters.

Then we will apply the complete transformation of each equation Σ_i. (Sometimes we need to replace the equation containing a component A^λ by two equations containing components 1 and AA^λ, respectively).

We will continue the construction of this "tree" of directed full equations, with natural parameters.

By a *polarizated* equation in n variables we mean any system consisting of the following four parts (with a possible renumbering of variables).

1) Polarizated alphabet

$$x_2^*, \ldots, x_n^*, \ x_1^+, \ x_2^+, \ldots, \ x_n^+$$

2) Directed full equations

$$x_2^* \vee^+ \varphi(x_2^*, \ldots, x_n^*, x_1^+, x_2^+, \ldots, x_n^+) \rightarrow x_1^+\psi(x_2^*, \ldots, x_n^*, x_1^+, x_2^+, \ldots, x_n^+) \quad (10)$$

where $x_2^* \vee^+ \varphi(\ldots) \rightarrow x_1 \ldots$ denotes

— either the equation $x_2^*\varphi(\ldots) \rightarrow x_1 \ldots$,

— or the equation $x_2^+\varphi(\ldots) \rightarrow x_1 \ldots$.

3) Polarization

A polarizated equation contains the functions $\alpha(i)$ and $\beta(i)$ with the following domains and ranges:

$\alpha(i) : \{2, \ldots, n\} \rightarrow \{1, \ldots, n\}$, $\qquad \alpha(i) = i \Rightarrow i = 2.$

$\beta(i) : \{2, \ldots, n\} \rightarrow \{1, \ldots, n\}$, $\qquad \beta(i) \neq i.$

The variables $x_2^*, \ldots, x_n^*$ are polarizated in the equation (10) by the following rule:

$$x_i^* \rightarrow x_{\alpha(i)}^* \vee x_{\alpha(i)}^*, x_{\alpha(i)}^+ \vee x_{\alpha(i)}^*, x_1^+ \vee x_{\alpha(i)}^*, x_{\alpha(i)}^+, x_1^+ \qquad (11)$$

(That is, only $x_{\alpha(i)}^*$ can be placed after x_i^* in the equation (10), or only $x_{\alpha(i)}^*$ and $x_{\alpha(i)}^+$ can be placed after x_i^*, or only $x_{\alpha(i)}^*$ and x_1^+, or only $x_{\alpha(i)}^*$ and $x_{\alpha(i)}^+$, and x_1^+).

$$x_{\beta(i)}^* \vee x_{\beta(i)}^+ \leftarrow x_i^+ \qquad (12)$$

(That is, only $x_{\beta(i)}^*$ can be placed before x_i^+ in the equation (10), or only $x_{\beta(i)}^+$ can be placed before x_i^+).

We will say that x_i^* *has* the variable v, if the polarization (11) contains $x_i^* \rightarrow v$.

We will say that x_i^+ *has* the variable v, if the polarization (12) contains $v \leftarrow x_i^+$.

4) Additional conditions

— x_i^* has $x_k^+ \Leftrightarrow x_k^+$ has x_i^*.

— If x_i^* has x_1^+, then $\alpha(i) = 2$.

— $\forall$ i [$\exists$ t (x_i^* has x_t^+),

$\vee \exists$ s, t (x_i^* has x_s^+ & x_s^* has x_t^+),

$\vee \exists$ r, s, t (x_i^* has x_r^+ & x_r^* has x_s^+ & x_s^* has x_t^+),

...]

Here is an example of a polarizated equation in four variables x_2^*, x_3^*, x_4^*, x_1^+, x_2^+, x_3^+, x_4^+.

$$x_2^*\varphi(\ldots) \rightarrow x_1^+ \psi(x_1, x_2 \ldots, x_n)$$

$x_2^* \rightarrow x_4^*, x_4^+$ $\qquad$ $x_3^* \leftarrow x_1^+$

$x_3^* \rightarrow x_2^*, x_1^+$ $\qquad$ $x_1^* \leftarrow x_2^+$

$x_4^* \rightarrow x_3^*$ $\qquad$ $x_1^* \leftarrow x_3^+$

$\qquad\qquad\qquad\qquad$ $x_2^* \leftarrow x_4^+$

♦

Theorem

If an equation $S(x_1, \ldots, x_n) \rightarrow T(x_1, \ldots, x_n)$ belongs to the "tree" of equations (7) and its branch contains all variables $x_1, \ldots, x_n$, then this equation is polarizated.

Remark

If the branch of the equation $S(x_1, \ldots, x_n) \rightarrow T(x_1, \ldots, x_n)$ contains the variables $x_1, \ldots, x_k$, $(k < n)$, then it is *partially polarizated*, that is its alphabet is $x_2^*, \ldots, x_k^*$, $x_1^+, x_2^+, \ldots, x_k^+, x_{k+1}, \ldots, x_n$ and its polarization is given by the following:

$$x_i^* \rightarrow \gamma_i(x_{k+1}, \ldots, x_n)x_t^*\vee^+ \qquad x_t^*\vee^+ \delta_i(x_{k+1}, \ldots, x_n) \leftarrow x_i^+$$

♦

If the word $R(x_1, \ldots, x_n)$ contains all the letters $x_1, \ldots, x_n$, then by the *prefix* of this word, we mean a word $P(x_1, \ldots, x_n)$ of minimal length which contains all the letters $x_1, \ldots, x_n$ and such that $R(x_1, \ldots, x_n)$ is identical to $P(x_1, \ldots, x_n)$ $Q(x_1, \ldots, x_n)$ for some $Q(x_1, \ldots, x_n)$.

By the *prefix-equation* of the equation $S(x_1, \ldots, x_n) \rightarrow T(x_1, \ldots, x_n)$ we mean the equation $S'(x_1, \ldots, x_n) \rightarrow T'(x_1, \ldots, x_n)$, where $S'(x_1, \ldots, x_n)$ is the prefix of $S(x_1, \ldots, x_n)$ and $T'(x_1, \ldots, x_n)$ is the prefix of $T(x_1, \ldots, x_n)$.

Theorem

The set of prefix-equations of the "tree" of equations (7) is finite and can be constructed by means of formulas of elementary equations.

♦

CONJUGACY IN FREE INVERSE MONOIDS

Christian CHOFFRUT
Laboratoire d'Informatique Théorique et de Programmation
Université Paris 7, Tour 55-56, 1er étage
2 Pl. Jussieu, Paris 75 251 Cedex 05
email: cc@litp.ibp.fr

Abstract: the notion of conjugacy in groups can be extended in two ways to monoids. We keep on calling conjugacy the first version (two elements x and y are conjugate if xz=zy holds for some z), while we call transposition the second one (two elements x and y are transposed conjugate if x=uv and y=vu holds for some u,v). Using the characterization of elements in free inverse monoids due to Munn, we show that restricted to non idempotents, the relation of conjugacy is the transitive closure of the relation of transposition. Furthermore, we show that conjugacy between two elements of a free inverse monoid can be tested in linear time.

Résumé: la notion de conjugaison dans les groupes peut être étendue de deux façons aux monoides. Nous appelons conjugaison la première version (deux éléments x et y sont conjugués si xz=zy est vrai pour un certain z), alors que nous appelons transposition la seconde version (deux éléments x et y sont transposés si x=uv et y=vu sont vrais pour certains u,v). Utilisant la caractérisation due à Munn des éléments d'un monoide inversif libre, nous montrons que restrainte aux éléments non idempotents, la première relation est la fermeture transitive de la première. De plus nous prouvons que l'on peut tester en temps linéaire si deux éléments d'un monoide libre inversif sont conjugués.

1.INTRODUCTION

Two elements x and y of a group G are conjugate if and only if there exists z in G such that $x=zyz^{-1}$. This notion is usually extended in two different ways to monoids (cf., e.g., [Os] and [Ot]). Indeed, say two elements x,y of a monoid M are *conjugate* and write Conj(x,y) if there exists $z\in M$ such that xz=zy. Say they are *transposed* and write Trans(x,y) if there exist $u,v \in M$ such that x=uv and y=vu. Clearly, conjugacy is reflexive and transitive but not necessarily symmetric. Moreover, transposition is reflexive and symmetric but not necessarily transitive. Nevertheless the following inclusions hold in all cases (where the exponents refer to the operation of composition of realations and where the star refers to the transitive closure):

$$\text{Trans} \subseteq \text{Trans}^2 \ldots \subseteq \text{Trans}^k \ldots \subseteq \text{Trans}^* \subseteq \text{Conj}$$

A few papers have dealt with comparing these two relations (essentially [LS], [Ot],[Dub] and [Zh]). Here we study the case of free inverse monoids, i.e., of the free objects in the category of regular monoids for which all idempotents commute (cf. paragraph 3.1 for a precise definition). The main purpose is to prove that in free inverse monoids, conjugacy restricted to non idempotents is the transitive closure of transposition:

Theorem *In free inverse monoids, all idempotents form a unique class of conjugacy. Moreover, two non idempotent elements* x *and* y *satisfy* xz=zy *for some element* z *if and only if there exist an integer* $n\geq 0$ *and a sequence* $x=x_0,x_1\ldots, x_n=y$ *of elements such that for* i=0,...n-1 *there exist* u,v *satisfying* $x_i=uv$ *and* $x_{i+1}=vu$.

This research was supported by the PRC Mathématique-Informatique

Also based on this result, a linear algorithm is given that tests for conjugacy in free inverse monoids. The main tool for proving this result is the characterization of the elements of free inverse monoids by ways of walks in certain trees due to Munn. This technique has been employed by other authors in connection with the solution of the word problem in some inverse monoids (cf., e.g., [Me] and [St]).

In section 2 the main definitions and notions are recalled. Section 3 is devoted to the valuable Munn's characterization of free inverse monoids and states some useful elementary properties. In section 4 the theorem is proven and complexity considerations are developed.

2. PRELIMINARIES

Given a finite nonempty alphabet Σ, we denote by Σ^* the free monoid it generates. An element of Σ^* is a *word* and the unit 1 of Σ^* is the *empty* word. Given a word $w \in \Sigma^*$, we denote by $|w|_a$ the number of occurrences of the letter a in w, and by $|w|$ its *length* : $|w| = \sum_{a \in \Sigma} |w|_a$.

A word u is a *prefix* of a word w if $w=uv$ holds for some $v \in \Sigma^*$. Two words u,v are *comparable* if u is a prefix of v or v is a prefix of u. A word $w \in \Sigma^*$ is *primitive* if $w=u^n$ implies $n=1$ otherwise it is *imprimitive*. It is well-known that each non empty word is some power of a unique primitive word called its *root* (cf.,e.g., [LyS] Corollary 4.1).

Example 2.1: aba is primitive but abab is not and its root is ab□

Given a linear order on Σ we recall that it can be extended to Σ^* by defining the relation $u<v$ if and only if:
either $|u|<|v|$
or $|u|=|v|$ and for some $x,u',v' \in \Sigma^*$, $a,b \in \Sigma$, $a<b$ we have $u=xau'$, $v=xbv'$
This ordering is known as the *alphabetic* ordering.

Example 2.2: if a<b then b<ab<ba

In this work, a monoid M will be given by *generators* and *relators*, i.e., by one of its *presentations* $\langle \Sigma;E \rangle$ where $E \subseteq \Sigma^* \times \Sigma^*$. Alternatively, it is customary to denote any pair (u,v) of E (also called *relator* or *rule*) as u=v. Thus, e.g., $\langle a,b; ab=ba \rangle$ denotes the free commutative monoid on the two generators a,b.Thus, M is isomorphic to the quotient $\Sigma^*/\tilde{E}$ where $\tilde{E}$ is the congruence over Σ^* generated by the relation E.

As said in the introduction, conjugacy in groups leads naturally to two different definitions in general monoids. Indeed, starting with the condition $x=zyz^{-1}$, either we observe that it yields the factorizations $x=(z)(yz^{-1})$ and $y=(yz^{-1})(z)$ or we multiply it by z to the right and we get: xz=zy.

In the first case we define the relation of *transposition* :