International Journal of Algebra and Computation

EQUATIONS IN FREE INVERSE MONOIDS.

Timothy Deis
Department of Mathematics, University of Wisconsin, Platteville, WI 53818,USA.
deist@uwplatt.edu

John Meakin
Department of Mathematics and Statistics, University of Nebraska, Lincoln, NE 68588, USA .
jmeakin@math.unl.edu

G. Sénizergues
Department of Computer Science, Bordeaux 1 university,351, cours de la Libération F-33405 Talence Cedex, France. ges@labri.fr

Received (Day Month Year)
Revised (Day Month Year)

Communicated by [editor]

It is known that the problem of determining consistency of a finite system of equations in a free group or a free monoid is decidable, but the corresponding problem for systems of equations in a free inverse monoid of rank at least two is undecidable. Any solution to a system of equations in a free inverse monoid induces a solution to the corresponding system of equations in the associated free group in an obvious way, but solutions to systems of equations in free groups do not necessarily lift to solutions in free inverse monoids. In this paper we show that the problem of determining whether a solution to a finite system of equations in a free group can be extended to a solution of the corresponding system in the associated free inverse monoid is decidable. We are able to use this to solve the consistency problem for certain classes of single variable equations in free inverse monoids.

Keywords: Free inverse monoid; Equations; Consistency problem; Extendibility problem.

1. Introduction

An *inverse* monoid is a monoid M with the property that for each $a \in M$ there exists a unique element $a^{-1} \in M$ such that $a = aa^{-1}a$ and $a^{-1} = a^{-1}aa^{-1}$. Equivalently, M is a von-Neumann regular monoid whose idempotents commute. The idempotents of such a monoid form a (lower) semilattice with respect to multiplication as the meet operation, and we denote the semilattice of idempotents of an inverse monoid M by $E(M)$. Inverse monoids arise naturally as monoids of partial symmetries (partial one-one structure-preserving maps) throughout mathematics. We refer the reader to the books by Petrich [21], Lawson [12], and Patterson [20] for much information about the structure of inverse monoids and their connections with other branches of mathematics.

Inverse monoids form a variety of algebras (in the sense of universal algebra) with respect to the operations of multiplication, inversion, and choosing the identity. As such, free inverse monoids exist. We denote the free inverse monoid on a set A by $FIM(A)$. The free monoid on A will be denoted by A^* and the free group on A will be denoted by $FG(A)$. It is convenient to denote the alphabet $A \cup A^{-1}$ by $\tilde{A}$ and the free monoid on this alphabet by $\tilde{A}^*$. The monoid $FIM(A)$ and the group $FG(A)$ are quotient of $\tilde{A}^*$. We denote by $=_I$ (resp. $=_G$) the kernel of the projection $\tilde{A}^* \to FIM(A)$ (resp. $\tilde{A}^* \to FG(A)$. It is easy to see that $FG(A)$ is the maximal group homomorphic image of $FIM(A)$. The structure of $FIM(A)$ is determined by considering finite subtrees of the Cayley tree of the free group (with respect to the usual presentation of $FG(A)$).

Denote the Cayley tree of $FG(A)$ by $\Gamma(A)$. The vertices of $\Gamma(A)$ may be identified with reduced words (elements of $FG(A)$), and there is an edge in $\Gamma(A)$ labeled by an element $a \in \tilde{A}$ from g to ga for each $g \in FG(A)$. Note that if a labels an edge from g to ga, then a^{-1} labels an edge from ga to a. For each word $w \in \tilde{A}^*$, let $MT(w)$ be the Munn tree of w. Here $MT(w)$ is the finite subtree of $\Gamma(A)$ obtained when the word w is read as a path in $\Gamma(A)$ starting at 1 and ending at the reduced form $r(w)$ of w. A theorem of Munn [19] (see also [26,21,12]) states that two words u and v in $\tilde{A}^*$ are equal in $FIM(A)$ if and only if $MT(u) = MT(v)$ and $r(u) = r(v)$. This provides a solution to the word problem for $FIM(A)$. If Γ is any finite subtree of $\Gamma(A)$ containing the vertex 1 and if g is any vertex of Γ, then there is at least one word $u \in \tilde{A}^*$ (in fact infinitely many words, as soon as Γ has at least two vertices) such that $(MT(u), r(u)) = (\Gamma, g)$. The monoid $FIM(A)$ may be identified with the set $\{(MT(w), r(w)) : w \in \tilde{A}^*\}$ with multiplication

$$(MT(u), r(u)) \times (MT(v), r(v)) = ((MT(u) \cup r(u)MT(v), r(uv)). \qquad (1)$$

The idempotents of $FIM(A)$ are represented by Dyck words in $\tilde{A}^*$, i.e. words whose reduced form is 1. Two such Dyck words represent the same idempotent in $FIM(A)$ if and only if they have the same Munn tree. There is a natural partial order on any inverse monoid M defined by $a \leq b$ if and only if $a = eb$ for some idempotent $e \in E(M)$. The congruence on M induced by this relation is denoted by σ_M (or just σ if M is understood) and is the minimum group congruence on M (i.e. M/σ_M is the maximum group homomorphic image of M). For $FIM(A)$, each σ-class contains a maximum element (the reduced form of a word in the σ-class) and of course $FIM(A)/\sigma \cong FG(A)$.

Let X be an alphabet that is disjoint from A. We will view letters of $\tilde{X}$ as *variables* and elements of $\tilde{A}^*$ as *constants*. The sets A and X will be assumed to be *finite and non-empty* throughout this paper. An *equation* in $FG(A)$ or in $FIM(A)$ with coefficients in $FG(A)$ (or in $FIM(A)$) is a pair (u, v), where $u, v \in (\tilde{A} \cup \tilde{X})^*$. Usually we will denote such an equation by $u = v$. Similarly an equation in $\tilde{A}^*$ is a pair

(u, v) with $u, v \in (\tilde{A} \cup \tilde{X})^*$, and again we will denote this by $u = v$. If needed to distinguish where equations are being viewed, we will denote an equation $u = v$ in $\tilde{A}^*$, [resp. $FG(A)$, $FIM(A)$] by $u =_M v$ [resp. $u =_G v, u =_I v$].

Any map $\phi : X \to \tilde{A}^*$ extends to a homomorphism (again denoted by ϕ) from $(\tilde{A} \cup \tilde{X})^*$ in such a way that ϕ fixes the letters of A and $\phi(y^{-1}) = (\phi(y))^{-1}$ for every $y \in A \cup X$. We say that ϕ is a *solution* to the equation $u =_G v$ in $FG(A)$ [resp. $u =_I v$ in $FIM(A)$ or $u =_M v$ in $\tilde{A}^*$] if $\phi(u) = \phi(v)$ in the appropriate setting. A solution to a set of equations $u_i = v_i$ for $i = 1, \ldots n$ is a map ϕ that is a solution to each equation in the set. If a set of equations has at least one solution it is called *consistent*: otherwise it is called *inconsistent*. It is easy to give examples of equations that are inconsistent in any of the three possible settings where we are considering such equations, and it is easy to give examples of equations that are consistent in $FG(A)$ but not in $FIM(A)$ or in $\tilde{A}^*$. For example, if $A = \{a, b\}$, then the equation $ax = xb$ is inconsistent in all three settings, while the equation $ax = b$ is consistent in $FG(A)$ but inconsistent in $\tilde{A}^*$ and in $FIM(A)$. On the other hand it is obvious that any set of equations that is consistent in $FIM(A)$ must be consistent in $FG(A)$: if ψ is any solution to a set of equations in $FIM(A)$, then ψ is also a solution to the same set of equations, viewed as equations in $FG(A)$.

The *consistency problem* for systems of equations in A^* [resp. $FG(A), FIM(A)$] is the problem of determining whether there is an algorithm that, on input a finite set $\{u_i = v_i : i = 1 \ldots n\}$ of equations in A^* [resp. $FG(A), FIM(A)$], produces an output of "Yes" if the system is consistent and "No" if it is inconsistent. Theorems of Makanin [16,17] imply that the consistency problems for systems of equations in A^* and in $FG(A)$ are decidable. Much work has been done on solutions to systems of equations in free monoids and free groups: we refer the reader to [14,10,22,24,5,11,9] for just some of the extensive literature on this subject. On the other hand, a theorem of Rozenblat [25] shows that while the consistency problem for systems of equations in $FIM(A)$ is decidable if $|A| = 1$, this problem is undecidable if $|A| > 1$. The consistency problem for equations of some restricted type (for example, *single variable* equations, or *quadratic* equations) is open as far as we are aware. Some work on special cases of this problem has been done by Deis [6]. For example, Deis [6] has shown that while the consistency problem for single *multilinear* equations in $FIM(A)$ is decidable, the consistency problem for finite *systems* of multilinear equations is undecidable. We will show later in this paper that the consistency problem for single-variable equations of a particular type is decidable.

Now consider an equation $u =_I v$ in $FIM(A)$, let ψ be a solution to this in $FIM(A)$, and let ϕ be a solution to the corresponding equation in $FG(A)$, where $\phi(x)$ is a reduced word for each $x \in X$. We say that ψ is an *extension* of ϕ (or that ϕ *extends to* ψ) if for each $x \in X$ there is some Dyck word e_x such that $\psi(x) =_I e_x\phi(x)$. If ψ is a solution to an equation $u = v$ in $FIM(A)$ and if $\phi(x) =_M r(\psi(x))$ for each $x \in X$, then of course ϕ is a solution to $u = v$ in $FG(A)$ and ψ is an extension of ϕ.

A given solution ϕ to an equation $u = v$ in $FG(A)$ may admit finitely many extended solutions (up to $=_I$), infinitely many extended solutions (up to $=_I$), or no extended solutions, to the same equation in $FIM(A)$. For example, the equation $bb^{-1}x = aa^{-1}bb^{-1}$ has trivial solution in $FG(a,b)$, and this has exactly two extensions $\psi_1(x) = aa^{-1}bb^{-1}$ and $\psi_2(x) = aa^{-1}$ in $FIM(a,b)$. The equation $bb^{-1}x = aa^{-1}x$ has trivial solution in $FG(a,b)$ that extends to infinitely many solutions $\psi_e(x) = e$ for any idempotent $e \leq aa^{-1}bb^{-1}$ in the natural order on $FIM(a,b)$. The equation $a^{-1}ax = aa^{-1}$ has trivial solution in $FG(a,b)$ but no solution in $FIM(a,b)$. These facts are easy to check via the multiplication of Munn trees in the free inverse monoid, as described in equation (1).

A natural question arises here: when does a solution to an equation $u = v$ in $FG(A)$ extend to a solution to the same equation in $FIM(A)$? We refer to the corresponding algorithmic problem as the *extendibility problem* for equations in $FIM(A)$. More precisely, the extendibility problem for equations in $FIM(A)$ asks whether there is an algorithm that, on input a finite set $\{u_i = v_i : i = 1, \ldots n\}$ of equations in $FIM(A)$ that is consistent in $FG(A)$ and a solution ϕ to this system in $FG(A)$, produces the output "Yes" if ϕ can be extended to a solution to the system of equations in $FIM(A)$ and "No" if ϕ cannot be extended to a solution to this system in $FIM(A)$. Some special cases of the extendibility problem were considered by Deis [6]. The main result of this paper shows that *the extendibility problem is decidable* (theorem 7 in section 2).

In section 3, we show how the main result may be applied to study the consistency problem for systems consisting of one *single-variable* equation in $FIM(A)$.
In section 4, we mainly discuss some relations with other works.

2. The Extendibility Problem

In order to study the extendibility problem, we first reformulate it somewhat in terms of Munn trees. Let $u = v$ be an equation in $FIM(A)$ and $\phi : X \to \tilde{A}^*$ a solution to this equation in $FG(A)$. Thus $\phi(u) = \phi(v)$ in $FG(A)$ (but not necessarily in $FIM(A)$ of course). The edges of $MT(u)$ [and $MT(v)$] are labeled over the alphabet $\tilde{A} \cup \tilde{X}$. For each variable x that occurs in the word u, there is at least one edge in $MT(u)$ labeled by x. The Munn tree $MT(\phi(u))$ has edges labeled over the alphabet $A \cup A^{-1}$. It is obtained from $MT(u)$ by replacing each (directed) edge e labeled by a variable $x \in X$ by the tree $MT(\phi(x))$: in this replacement, the initial root (i.e. 1) of this copy of $MT(\phi(x))$ is identified with the initial vertex of the edge e and the terminal root of $MT(\phi(x))$ is identified with the terminal vertex of e. This process is well defined since if u' is another word with $MT(u') = MT(u)$ and $r(u') = r(u)$ then $u' = u$ in $FIM(A \cup X)$, so $\phi(u') = \phi(u)$ in $FIM(A)$, and so $MT(\phi(u')) = MT(\phi(u))$. The relationship between $MT(v)$ and $MT(\phi(v))$ is described in a similar fashion.

The extension of ϕ to a homomorphism (again denoted by ϕ) from $(\tilde{A} \cup \tilde{X})^*$ to

$\tilde{A}^*$ naturally induces a homomorphism $\bar{\phi}$ from $FG(A \cup X)$ to $FG(A)$. Thus each vertex of $MT(u)$ [resp. $MT(v)$] that is the initial vertex of an edge of $MT(u)$ [resp. $MT(v)$] labeled by a letter $x \in X$ has a unique image in $MT(\phi(u))$ [resp. $MT(\phi(v))$] under this homomorphism. We refer to the vertices obtained this way as images of initial vertices of edges of $MT(u)$ [resp. $MT(v)$] labeled by the letter $x \in X$ as *designated x-vertices* of $MT(\phi(u))$ [resp. $MT(\phi(v))$]. For example, if $w = abx_1b^{-1}bbx_2^{-1}a$ and $\phi(x_1) = b^{-1}$ and $\phi(x_2) = a$, then $MT(\phi(w))$ has two designated vertices: namely ab is a designated x_1-vertex and aba^{-1} is a designated x_2-vertex. Similarly, if $w' = abx_1b^{-1}bbx_2a$ and we take the same map ϕ as above, then ab is both a designated x_1-vertex and a designated x_2-vertex.

Now suppose that $\psi(x) = e_x\phi(x)$ for all $x \in X$, where each e_x is a Dyck word. Since the terminal root of $MT(e_x)$ is the same as its initial root (1), it follows that the designated x-vertices of $MT(\phi(w))$ and of $MT(\psi(w))$ coincide, for each word w and each $x \in X$. Furthermore, $MT(\psi(w))$ is obtained from $MT(\phi(w))$ by adjoining to $MT(\phi(w))$ a copy of $MT(e_x)$ rooted at each designated x-vertex of $MT(\phi(w))$. Recall that this map ψ defines an extension of ϕ if ψ is a solution to $u = v$ in $FIM(A)$, i.e. if $MT(\psi(u)) = MT(\psi(v))$.

Now let $\{u_i = v_i : i = 1, \ldots, n\}$ be a system of equations in $FIM(A)$, and let ϕ be a solution to this system in $FG(A)$. For each variable $x \in X$ denote the set of designated x-vertices of $MT(\phi(u_i))$ [resp. $MT(\phi(v_i))$] by $\alpha_{i,x}$ [resp. $\alpha'_{i,x}$] and denote the set of vertices of $MT(\phi(u_i))$ [resp. $MT(\phi(v_i))$] by β_i [resp. β'_i]. It is convenient to denote multiplication in $FG(A)$ by $\cdot$ and to denote the union $S \cup T$ of two subsets of $FG(A)$ or $(A \cup A^{-1})^*$ by $S + T$. Finally, let us denote the set of vertices of the Munn tree $MT(e_x)$ of some (unknown) Dyck word e_x by T_x (for each $x \in X$).

The requirement that ϕ should be extendible to some solution $\psi(x) = e_x\phi(x)$ to the system in $FIM(A)$ translates as follows. Consider the system of equations over $\mathcal{P}_f(FG(A))$:

$$\sum_x \alpha_{i,x} \cdot T_x + \beta_i =_{\mathcal{P}_f(FG(A))} \sum_x \alpha'_{i,x} \cdot T_x + \beta'_i : i = 1, \ldots, n. \tag{2}$$

Here the $\alpha_{i,x}, \alpha'_{i,x}, \beta_i, \beta'_i$ are finite subsets of $FG(A)$ and the T_x are unknowns. A solution of (2) is any vector $\{T_x : x \in X\}$ of finite subsets of $FG(A)$, that satisfies this system of equations. We would like to decide whether the system of equations (2) has at least one solution such that each T_x is prefix closed. (A subset T of $FG(A)$ is *prefix closed* if the corresponding set of reduced words is prefix closed). We will show that this problem is decidable by appealing to Rabin's tree theorem [23]. From the discussion above, this will show that the extendibility problem is decidable.

We assume some familiarity with basic definitions and ideas of (first order) logic. See, for example, Barwise [3]. In monadic second order logic, quantifiers refer to sets (i.e. unary or monadic predicates) as well as to individual members of a structure.

The syntax and semantics of terms and well formed formulae are defined inductively in the usual way. Atomic formulae include those of the form $t \in Y$ where t is a term and Y is a set variable. A sentence of the form $\forall Y \nu(Y)$ where Y is a set variable, in particular, is true in a structure M iff $\nu(Y)$ is (inductively) true in M for all subsets Y of the universe of M. We denote by $MSOL(M)$ the set of well-formed formula . If a formula $\theta \in MSOL(M)$ is true in the structure M we write $M \models \theta$ and we define $Th_2(M) = \{\theta \in MSOL(M) : M \models \theta\}$. The (second order monadic) theory of M is *decidable* if there is an algorithm that tests whether a given sentence $\theta \in MSOL(M)$ belongs to $Th_2(M)$ or not.

Let A be a set, which is finite or countable, and consider the structure $T_A = (A^*, \{r_a : a \in A\}, \leq)$. Here $r_a : A^* \to A^*$ is right multiplication by a, $xr_a = xa, \forall x \in A^*$ and $\leq$ is the prefix order $x \leq y$ iff $\exists u \in A^*(xu = y)$. The theory $Th_2(T_A)$ is called the theory of A-successor functions. For $|A| = 2$ this is often denoted by $S2S$, and sentences in $MSOL(T_{\tilde{A}})$ can be reformulated as sentences in $MSOL(T_{\{a,b\}})$. Rabin's tree theorem stated below is one of the most powerful decidability results known in model theory: the decidability of many other results can be reduced to $Th_2(T_A)$ (see, for example, [3]).

Theorem 1. *(Rabin [23]) For every countable set A, $Th_2(T_A)$ is decidable.*

The main theorem of this paper is the following.

Theorem 2. *There is an algorithm that will decide, on input a system of equations of the form (2), whether this system of equations has at least one solution $\{T_x : x \in X\}$ such that each T_x is a finite prefix-closed subset of $FG(A)$.*

In order to use Rabin's theorem to prove this, we need to show that the existence of a solution of the desired type to (2) is expressible in $MSOL(T_{\tilde{A}})$.

Step 1: View each element of each set $\alpha_{i,x}, \alpha'_{i,x}, \beta_i, \beta'_i$ and T_x as a reduced word in $\tilde{A}^*$. In order to translate the equations (2) over subsets of FG(A) into similar equations, but over subsets of $\tilde{A}^*$, we decompose the coefficients $\alpha_{i,x}, \alpha'_{i,x}$ and as well, the sets T_x into a finite number of components.

Let us consider the set

$$S = \{(a, u) \in (\tilde{A} \cup \{\epsilon\}) \times \tilde{A}^* \mid \exists v \in \tilde{A}^*, v \cdot u \in \sum_{x \in X, 1 \leq i \leq n} \alpha_{i,x} + \alpha'_{i,x} \text{ and } a = v^{(1)}\}$$

where $v^{(1)}$ denotes the last letter of v , if $|v| \geq 1$, and the empty word, ϵ, otherwise. Let us denote the elements of S by $\{(a_j, u_j) \mid 1 \leq j \leq k\}$. For every $j \in [1, k]$ we write:

$$T_{j,x} = \{u \in \tilde{A}^* \mid u_j^{-1} \cdot u \in T_x \text{ and first-letter}(u) \neq a_j^{-1}\} \text{ (if } a_j \in \tilde{A}) \tag{3}$$

$$T_{j,x} = \{u \in \tilde{A}^* \mid u_j^{-1} \cdot u \in T_x\} \text{ (if } a_j = \epsilon) \tag{4}$$

Accordingly, for every $1 \leq i \leq n, 1 \leq j \leq k, x \in X$, we define the sets

$$\alpha_{i,j,x} = \{v \in A^* \mid v \cdot u_j \in \alpha_{i,x} \text{ and } v^{(1)} = a_j\}$$

and $\alpha'_{i,j,x}$ is defined similarly.

The equations (2) reduce to the system of equations and inequations:

$$\sum_{x\in X}\sum_{j=1}^{k}\alpha_{i,j,x}\cdot T_{j,x}+\beta_i =_{\mathcal{P}_f(\tilde{A}^*)} \sum_{x\in X}\sum_{j=1}^{k}\alpha'_{i,j,x}\cdot T_{j,x}+\beta'_i, i=1,\ldots,n \tag{5}$$

$$\begin{aligned} u_j^{-1}\cdot T_{j,x} &\subseteq RED(\tilde{A}^*)\\ T_{j,x} &\subseteq RED(\tilde{A}^*)-a_j^{-1}\tilde{A}^* \end{aligned}\tag{6}$$

(where $RED(\tilde{A}^*)$ denotes the set of all reduced words over $\tilde{A}^*$). Note that the effect of our chosen decompositions of the sets $\alpha_{i,x},\alpha'_{i,x},T_x$, is that all products in the system (5) are reduced as written - so (5) may be viewed as a system of equations over $\mathcal{P}_f(\tilde{A}^*)$, where $\alpha_{i,j,x}$, $\alpha'_{i,j,x}$, β_i and β'_i are prescribed elements of $\mathcal{P}_f(\tilde{A}^*)$, and the $T_{j,x}$ are the unknowns. A *solution* to (5) is a vector $\{T_{j,x} : x\in X, 1\le j\le k\}$ of elements of $\mathcal{P}_f(\tilde{A}^*)$ that satisfies (5). We seek to decide whether (5) has a solution which also fulfills (6) and such that that each $T_{j,x}$ is *prefix-closed*.

Lemma 3. *The system (2) has a solution $\{T_x : x\in X\}$ which is prefix-closed if and only if the system (5)(6) has a solution $\{T_{j,x} : x\in X, 1\le j\le k\}$ which is prefix-closed.*

Proof. 1- Suppose $\{T_x : x\in X\}$ is a prefix-closed solution to system (2).
Let us consider it as a vector of sets of reduced words. Let $\{T_{j,x} : x\in X, 1\le j\le k\}$ be defined by formula (3,4). One can check that

$$r(\alpha_{i,x}\cdot T_x)=\sum_{j=1}^{k}\alpha_{i,j,x}\cdot T_{j,x}$$

Applying the map r on both sides of equations (2) we thus obtain equations (5). Hence $\{T_{j,x} : x\in X, 1\le j\le k\}$ is a solution to system (5). Formula (3,4) show that inequalities (6) are fulfilled too. Finally, the assumption that T_x is prefix-closed implies that $T_{j,x}$ is prefix-closed too.
2- Suppose $\{T_{j,x} : x\in X, 1\le j\le k\}$ is a prefix-closed solution to system (5)(6).
Let us define, for every $x\in X$,

$$T_x=\sum_{j=1}^{k}u_j^{-1}\cdot T_{j,x}. \tag{7}$$

Each T_x is clearly a finite subset of $\tilde{A}^*$. By the first inclusion of (6), $T_x\subseteq RED(\tilde{A}^*)$. The definition of the set S shows that $\{u_j \mid 1\le j\le k\}$ is suffix-closed, which implies that $\{u_j^{-1} \mid 1\le j\le k\}$ is prefix-closed. As well each $T_{j,x}$ is assumed prefix-closed. It follows that formula (7) defines a prefix-closed subset T_x. The second inclusion of (6) entails:

$$r(\alpha_{i,x}\cdot T_x)=\sum_{j=1}^{k}\alpha_{i,j,x}\cdot T_{j,x}$$

which, together with system (5), shows that $\{T_x : x \in X\}$ is a solution to system

$$\sum_x r(\alpha_{i,x} \cdot T_x) + r(\beta_i) =_{\mathcal{P}_f(\tilde{A}^*)} \sum_x r(\alpha'_{i,x} \cdot T_x) + r(\beta'_i), \quad i = 1, \ldots, n$$

Hence, the vector $\{T_x : x \in X\}$, viewed as a vector of subsets of $FG(A)$, is a solution to (2). □

Step 2: For each set U of words in $\tilde{A}^*$, let $Pref(U)$ denote the set of prefixes of words in U. Though the existence of a finite solution $\{E_{j,x} : x \in X, j = 1, \ldots, k\}$ to (5)(6) does not necessarily imply the existence of a finite prefix-closed solution to these equations, we can note that this is in a sense "almost" the case, and we will see how to impose additional conditions to obtain a finite prefix closed solution to this system of equations. Let N be the maximum length of a word in any of the sets $\alpha_{i,j,x}, \alpha'_{i,j,x}, \beta_i$, and β'_i.

Suppose that $\{E_{j,x} : x \in X, j = 1, \ldots, k\}$ is a solution to (5)(6). We first prove the following Lemma.

Lemma 4. *Suppose that $u \in Pref(E_{j,x})$ for some j and some x, and that $|u| > N$. Then for all $i = 1, \ldots, n$, if $v \in \alpha_{i,j,x}$, then $v \cdot u \in \sum_x \sum_j \alpha'_{i,j,x} \cdot Pref(E_{j,x}) + \beta'_i$.*

Proof. There exists a reduced word $s \in \tilde{A}^*$ such that $u \cdot s \in E_{j,x}$ and $u \cdot s$ is reduced as written. It follows that $v \cdot u \cdot s \in \sum_x \sum_j \alpha'_{i,j,x} \cdot E_{j,x} + \beta'_i$. Since $|u| > N$ it follows that $v \cdot u \cdot s \notin \beta'_i$, so $v \cdot u \cdot s \in \sum_x \sum_j \alpha'_{i,j,x} \cdot E_{j,x}$. Hence there exist $y, \bar{\jmath}$ and $v' \in \alpha'_{i,\bar{\jmath},y}$, $e' \in E_{\bar{\jmath},y}$ such that $v \cdot u \cdot s = v' \cdot e'$. But again, since $|u| > N$, s must be a suffix of e', so $e' = u' \cdot s$ for some u'. So we have $v \cdot u \cdot s = v' \cdot u' \cdot s$ in $\tilde{A}^*$. It follows that $v \cdot u = v' \cdot u'$ where $u' \in Pref(E_{\bar{\jmath},y})$. □

Step 3: Lemma 1 shows that if $\{E_{j,x} : x \in X,\ j = 1, \ldots, k\}$ is a solution to (5,6), then $\{Pref(E_{j,x}) : x \in X,\ j = 1, \ldots, k\}$ is "almost" a solution to (5,6). In order to arrange for a prefix-closed solution to (5,6) we need only assume some additional conditions on the "short" prefixes of elements of each set $E_{x,j}$. Since these prefixes must be included in a finite set that we know in advance, we are able to formulate appropriate additional conditions as follows.

Denote by $\tilde{A}^N$ [resp. $\tilde{A}^{\leq N}$] the set of words in $\tilde{A}^*$ of length N [resp. $\leq N$]. Let us introduce another vector of unknowns, $\{P_{j,x} : x \in X,\ j = 1, \ldots, k\}$ and consider the additional conditions:

$$P_{j,x} \subseteq E_{j,x},\ x \in X,\ j = 1, \ldots, k \tag{8}$$

$$E_{j,x} \subseteq P_{j,x} + (P_{j,x} \cap \tilde{A}^N) \cdot \tilde{A}^*,\ x \in X,\ \ j = 1, \ldots, k \tag{9}$$

$$P_{j,x} \subseteq \tilde{A}^{\leq N},\ x \in X,\ j = 1, \ldots, k \tag{10}$$

We have the following two lemmas.

Lemma 5. *Let $\{(P_{j,x}, E_{j,x}) : x \in X,\ j = 1, \ldots, k\}$ be a solution to (5,6,8,9,10) such that each $P_{j,x}$ is prefix-closed. Then $\{Pref(E_{j,x}) : x \in X,\ j = 1, \ldots, k\}$ is a prefix-closed solution to (5,6).*

Proof. Since $\{E_{j,x} : x \in X, j = 1, \dots k\}$ is a solution to (5), it is clear that $\beta_i \subseteq \sum_x \sum_j \alpha'_{i,j,x} \cdot E_{j,x} + \beta'_i$ for each $i = 1, \dots, n$. Let $u \in Pref(E_{j,x})$ and $v \in \alpha_{i,j,x}$ for some i, j, x. If $|u| > N$ then we already know by Lemma 1 that $v \cdot u \in \sum_x \sum_j \alpha'_{i,j,x} \cdot E_{j,x} + \beta'$. So assume that $|u| \leq N$. There exists some (reduced) word s such that $u \cdot s \in E_{j,x}$ and $u \cdot s$ is reduced as written. If $u \cdot s \in P_{j,x}$, then $u \in P_{j,x}$ since we are assuming that each $P_{j,x}$ is prefix-closed. Otherwise we must have $u \cdot s \in (P_{j,x} \cap A^N) \cdot A^*$ by (9). But then since u is a prefix of $u \cdot s$ of length $\leq N$, we must have that u is a prefix of a word in $P_{j,x}$, and so (again since $P_{j,x}$ is prefix-closed) we must have $u \in P_{j,x}$. Hence $v \cdot u \in \alpha_{i,j,x} \cdot E_{j,x}$ by (8). Since $\{E_{j,x} : x \in X, j = 1, \dots, k\}$ is a solution to (5), this implies that $v \cdot u \in \sum_x \sum_j \alpha'_{i,j,x} \cdot E_{j,x} + \beta'_i$. It follows that $\sum_x \sum_j \alpha_{i,j,x} \cdot Pref(E_{j,x}) + \beta_i \subseteq \sum_x \sum_j \alpha'_{i,j,x} \cdot Pref(E_{j,x}) + \beta'_i$ for each $i = 1, \dots, n$. The reverse inclusion follows dually and so $\{Pref(E_{j,x}) : x \in X, j = 1, \dots, k\}$ is a solution to (5), as required.
The hypothesis that $E_{j,x}$ satisfy (6) implies that $Pref(E_{j,x})$ satisfy the same inclusions (6). $\square$

Lemma 6. *Let $\{T_{j,x} : x \in X, j = 1, \dots, k\}$ be a finite prefix-closed solution to (5,6) and set $E_{j,x} = T_{j,x}$ and $P_{j,x} = T_{j,x} \cap A^{\leq N}$ for each $x \in X$ and $j = 1, \dots, k$. Then $\{(P_{j,x}, E_{j,x}) : x \in X, j = 1, \dots, k\}$ is a solution to (5,6,8,9,10) and each $P_{j,x}$ is prefix-closed.*

Proof. It is trivial to verify that conditions (5,6), (8), and (10) are satisfied by our choice of the $P_{j,x}$ and $E_{j,x}$. To verify (9), simply note first that any word in $T_{j,x}$ of length $\leq N$ is in $P_{j,x}$ by definition of $P_{j,x}$. Also, if u is a word in $T_{j,x}$ of length $\geq N$, then we may write $u = u' \cdot s$ where u' is a prefix of u of length N and $s \in \tilde{A}^*$. But then since $T_{j,x}$ is prefix-closed, $u' \in T_{j,x}$ and so $u \in (P_{j,x} \cap \tilde{A}^N) \cdot \tilde{A}^*$. This completes the verification that (9) is satisfied. $\square$

Step 4 - The Decision Algorithm: By Lemmas 5 and 6, we are reduced to deciding whether, among all the prefix-closed $P_{j,x}$ satisfying (10), there is a collection such that (5,6) (where the unknowns are renamed $E_{j,x}$), (8), and (9) are also satisfied by some finite sets of words.

Enumerate effectively all of the prefix-closed $P_{j,x}$ satisfying (10). We now translate each of the conditions (5),(6), (8), and (9) into their “mirror” conditions in the dual semigroup to $\tilde{A}^*$. For each word $w = s_1 s_2 \dots s_k$ (with each $s_j \in \tilde{A}$), we define $\hat{w}$ to be the mirror word $\hat{w} = s_k \dots s_2 s_1$. For each subset $F \subseteq \tilde{A}^*$ we define $\hat{F} = \{\hat{w} : w \in F\}$. For a given collection of prefix-closed sets $P_{j,x}$, $x \in X, j = 1, \dots, k$, one can consider the mirror versions of (5),(6), (8), and (9).

The mirror version of (5) is

$$\sum_x \sum_j F_{j,x} \cdot \hat{\alpha}_{i,j,x} + \hat{\beta}_i = \sum_x \sum_j F_{j,x} \cdot \hat{\alpha}'_{i,j,x} + \hat{\beta}'_i, \; i = 1, \dots, n. \tag{11}$$

Notice that in these equations, the variables $F_{j,x}$ are on the left and the constants are on the right. Also, the equations (11) have a solution $\{F_{j,x} : x \in X, j = 1, \dots, k\}$

if and only if the equations (5) have a solution $\{E_{j,x} : x \in X, j = 1, \ldots, k\}$, where $F_{j,x} = \hat{E}_{j,x}$ for each $x \in X, j = 1, \ldots k$. Also notice that the existence of a solution to (11) is expressible in $MSOL(T_{\tilde{A}})$, because right product by given words is a finite composition of successor functions. Similarly, a system of mirror inequations can be written for (6):

$$\begin{aligned} F_{j,x} \cdot \hat{u}_j^{-1} &\subseteq RED(\tilde{A}^*) \\ F_{j,x} &\subseteq RED(\tilde{A}^*) - \tilde{A}^* a_j^{-1} \end{aligned} \tag{12}$$

But this implies that the existence of a *finite* solution to (5,6) (i.e. a solution where all sets $F_{j,x}$ are finite) is also expressible in $MSOL(T_{\tilde{A}})$, simply because finiteness is expressible in $MSOL(T_{\tilde{A}})$. [Let us recall this standard trick: by König's Lemma, a set $F \subseteq \tilde{A}^*$ is infinite iff it admits a set of prefixes F' such that every element of F' has some successor inside F'; this characterisation is expressible in $MSOL(T_{\tilde{A}})$].

The mirror version of (8) is

$$\hat{P}_{j,x} \subseteq F_{j,x},\ x \in X, j = 1, \ldots, k. \tag{13}$$

Here each $\hat{P}_{j,x}$ is a fixed finite subset of $\tilde{A}^*$ (corresponding to the fixed choice of the $P_{j,x}$ that we are working with), and each $F_{j,x}$ is a variable. Clearly the existence of a solution to these conditions is expressible in $MSOL(T_{\tilde{A}})$.

In order to express the mirror version of (9) in $MSOL(T_{\tilde{A}})$, notice that the mirror image $R_{j,x}$ of $(P_{j,x} \cap \tilde{A}^N) \cdot \tilde{A}^*$ is the smallest subset X of $\tilde{A}^*$ such that $w \cdot s \in X$ for all $w \in \tilde{A}^*$ and all s in the fixed finite set consisting of mirror images of words in $(P_{j,x} \cap \tilde{A}^N)$. Since there are again just finitely many choices for these words s, since all variables w occur on the left, and since it is possible to express in $MSOL(T_{\tilde{A}})$ the fact that a set X is the smallest subset satisfying some other property that is expressible in $MSOL(T_{\tilde{A}})$, membership in the sets $R_{j,x}$ is expressible in $MSOL(T_{\tilde{A}})$. The mirror version of (9) then becomes

$$F_{j,x} \subseteq \hat{P}_{j,x} + R_{j,x},\ x \in X, j = 1, \ldots, k. \tag{14}$$

where the $F_{j,x}$ are variables and the $R_{j,x}$ are described above. Hence it is possible to express in $MSOL(T_{\tilde{A}})$ the fact that the $F_{j,x}$ satisfy these conditions.

Finally, notice now that for fixed finite prefix-closed sets $P_{j,x}$ $(x \in X, j = 1, \ldots, k)$ satisfying (10), the existence of sets $E_{j,x}(x \in X, j = 1, \ldots, k)$ that satisfy (5,6,8,9) is translated in the mirror conditions to the existence of sets $F_{j,x}$ that satisfy (11),(12),(13) and (14), and that $F_{j,x} = \hat{E}_{j,x}$ for each x and j. We can decide, using Rabin's tree theorem, whether (11,12,13,14) has at least one finite solution $\{F_{j,x} : x \in X, j = 1, \ldots, k\}$ in $\mathcal{P}(\tilde{A}^*)$, and the answer to this decides whether (5,6,8,9) has at least one solution $\{E_{j,x} : x \in X, j = 1, \ldots, k\}$ in $\mathcal{P}_f(\tilde{A}^*)$ (for the $P_{j,x}$ under scrutiny). If, for some finite prefix-closed sets $P_{j,x}$ satisfying (10), the answer is "Yes", then (5,6) has some prefix-closed solution: otherwise, (5,6) has no prefix-closed solution. This completes the proof of Theorem 2. □

As an immediate corollary we obtain the following result.

Theorem 7. *Let A be a finite set. Then the extendibility problem for $FIM(A)$ is decidable.*

3. The Consistency Problem for Single-variable Equations

Recall that the theorem of Rozenblat [25] shows that the consistency problem for finite systems of equations in $FIM(A)$ is undecidable. Deis [6] has shown that the consistency problem for a system consisting of one multilinear equation in $FIM(A)$ (i.e. an equation $u = v$ in which each variable labels exactly one edge in $MT(u) \cup MT(v)$) is decidable, but that the consistency problem for finite systems of multilinear equations in $FIM(A)$ is undecidable. In this section we show how the results of the previous section may be applied to study the consistency problem for systems consisting of one *single-variable* equation in $FIM(A)$. A single-variable equation in $FIM(A)$ is an equation involving just one variable x (that may occur many times in the equation, with exponent ± 1). We are able to solve the consistency problem for a large class of single variable equations in $FIM(A)$.

It is clear from Theorem 7 that the consistency problem for a class of equations in $FIM(A)$ is decidable if the corresponding equations in $FG(A)$ have only finitely many solutions. A class of single-variable equations for which this is the case was identified in a paper of Silva [27].

In the following, we consider a single-variable equation $w(x) = 1$ in $FG(A)$, where $w(x)$ is the reduced word

$$w(x) = c_1 x^{\epsilon_1} c_2 x^{\epsilon_2} \dots c_t x^{\epsilon_t} c_{t+1}, \tag{15}$$

with each $c_i \in \tilde{A}^*$ and $\epsilon_i \in \{-1, 1\}$.

The proof of the following result in [27] is attributed to James Howie.

Theorem 8. *Let $w(x) = 1$ be a single-variable equation in $FG(A)$ and suppose that the exponent sum of the single variable x in $w(x)$ is not zero. Then the equation $w(x) = 1$ can have at most one solution in $FG(A)$.*

As an immediate corollary of this and Theorem 7, we obtain the following fact.

Corollary 9. *Consider the class $\mathcal{C}$ consisting of single-variable equations $u = v$ in $FIM(A)$ in which the sum of the exponents of the variable in u is not equal to the sum of the exponents of the variable in v. Then the consistency problem for this class is decidable.*

That is, there is an algorithm such that on input one equation $u = v$ in $\mathcal{C}$, will produce the output "Yes" if the equation is consistent in $FIM(A)$, and "No" if it is inconsistent.

Remark 10. The same result holds for finite systems of equations , all written with the same single variable.

In order to extend this result to other classes of single variable equations in $FIM(A)$, we recall some of the established literature on single variable equations in free groups. A parametric description of the set of all solutions to a single-variable equation $w = 1$ in $FG(A)$ was obtained by Lyndon [15]. Lyndon's result was refined somewhat by Appel [1] and subsequently by Lorents [13] (Gilman-Myasnykov [9] give a variant).

Let M be twice the maximum of the lengths of the c_i in equation (15). In the following result, a *parametric word* is a word of the form $u = w_1 w_2^{\alpha} w_3$ in which α is a parameter, $w_1 w_2^{\epsilon} w_3$ is reduced for $\epsilon \in \{-1, 1\}$, and w_2 is cyclically reduced and not a proper power. A value of u is the element of $FG(A)$ obtained by substituting an integer value for α. The refinement of Lyndon's and Appel's result that we shall use (due to Lorents [13]) is the following.

Theorem 11. *The set of solutions to any equation of the form $w(x) = 1$ in $FG(A)$, where $w(x)$ is the word (15), is the union of:*
(A) a finite set of solutions whose lengths are $\leq 4M$; and
*(B) the set of **all** values of some finite set of parametric words.*

We remark that the proofs of the theorems in the papers by Appel and Lorents are effective, so the set of parametric words that can yield solutions to $w(x) = 1$ in $FG(A)$ is effectively constructible (in fact $|w_1 w_2 w_3| \leq 5M$, in the notation above). This, together with the following definition, will enable us to extend Theorem 8 to a larger class of single-variable equations for which the consistency problem is decidable.

Define $\mathcal{V} : (\tilde{A} \cup \{x, x^{-1}\})^* \rightarrow FIM(x)$ by $\mathcal{V}(a) = 1$ if $a \in \tilde{A}$ and $\mathcal{V}(x) = x$. Thus if $u = w_1 x^{\epsilon_1} w_2 \cdots x^{\epsilon_n} w_n$ where $w_j \in \tilde{A}^*$ for $j = 1, \ldots, n$ and $\epsilon_i = \pm 1$, then $\mathcal{V}(u) = x^{\epsilon_1} x^{\epsilon_2} \cdots x^{\epsilon_n}$ in $FIM(x)$.

Theorem 12. *Let $\mathcal{C}$ be the class of single-variable equations of the form $u = v$ in $FIM(A)$ for which $\mathcal{V}(u) \neq \mathcal{V}(v)$ as elements of $FIM(x)$. Then the consistency problem for $\mathcal{C}$ is decidable.*

That is there is an algorithm that on input an equation $u = v$ in $\mathcal{C}$, produces the output "Yes" if this equation is consistent and "No" if it is inconsistent. Since $u, v \in (\tilde{A} \cup \{x, x^{-1}\})^*$ then we have

$$u = u_1 x^{\epsilon_1} u_2 x^{\epsilon_2} \cdots x^{\epsilon_{n-1}} u_n \text{ and } v = v_1 x^{\delta_1} v_2 x^{\delta_2} \cdots x^{\delta_{t-1}} v_t \tag{16}$$

where $u_i, v_j \in \tilde{A}^*$ for $1 \leq i \leq n$, $1 \leq j \leq t$ and $\epsilon_i, \delta_j \in \{1, -1\}$ for $1 \leq i \leq n$, $1 \leq j \leq t$.

If there are only finitely many solutions to $u = v$ in $FG(A)$ then there is an effective bound on the length of all such solutions, by Theorem 11. Thus in this case we can decide whether the equation $u = v$ is consistent in $FIM(A)$ since the extendibility problem is decidable. So suppose that there are infinitely many solutions to $u = v$ in $FG(A)$. Then again by Theorem 11, we may effectively find finitely many parametric words of the form $w_1 w_2^\alpha w_3$ such that $\phi_m(x) = w_1 w_2^m w_3$ is a solution to $u = v$ in $FG(A)$ for any integer m. We will show that there are only finitely many values of the integer m (for each such parametric word) such that ϕ_m can possibly extend to a solution to $u = v$ in $FIM(A)$. Again, since the extendibility problem is decidable, this will enable us to decide whether the equation $u = v$ is consistent in $FIM(A)$.

Recall that the free group on x, $FG(x)$, is isomorphic to the additive group $\mathbf{Z}$ of integers. Thus every Munn tree in the Cayley graph of $FG(x)$ can be viewed as an integer interval containing 0

$$\{i \in \mathbf{Z} \mid p \leq i \leq s\} = [p, s] \text{ where } p \leq 0 \leq s,$$

and if $w \in FIM(x)$ the rooted tree $(MT(w), r(w))$ can be identified with the triple (p, q, s) with $-p, s \in \mathbf{N}$ and $p \leq q \leq s$. The initial root of the corresponding birooted tree is 0 and $r(w) = x^q$.

Let $\mathcal{V}(u)$ be identified with the triple (l_u, n_u, r_u) and let $\mathcal{V}(v)$ be identified with the triple (l_v, n_v, r_v). Since $\mathcal{V}(u) \neq \mathcal{V}(v)$ it follows that $(l_u, n_u, r_u) \neq (l_v, n_v, r_v)$. If $n_u \neq n_v$ then the sum of the exponents of the variable x in u is not equal to the sum of the exponents of the variable x in v. But then from [27] there exists at most one solution to $u = v$ in $FG(A)$. Since we are assuming that $u = v$ has infinitely many solutions, this does not occur. Thus $n_u = n_v$ and since $(l_u, n_u, r_u) \neq (l_v, n_v, r_v)$ then either $l_u \neq l_v$ or $r_u \neq r_v$. Without loss of generality assume that

$$r_u > r_v \tag{18}$$

(A dual argument will apply to the case when $l_u \neq l_v$).

Before proceeding to the proof of theorem 12 we need some preliminar results about word combinatorics.

Let us restate a definition from [7, section 6], (generalizing the definition from [14, section 12.1.5]). Let $\omega \in \tilde{A}^*$ be some primitive, reduced word. Given a word $z \in \tilde{A}^*$, its *ω-stable normal decomposition* is the sequence of words

$$(z_1, \omega^{p_1}, z_2, \ldots, \omega^{p_\ell}, z_{\ell+1}) \tag{19}$$

such that $\ell \geq 0, z_k \in \tilde{A}^*$ (for all $1 \leq k \leq \ell + 1$), $p_k \in \mathbf{Z}$ (for all $1 \leq k \leq \ell$) and the following conditions are satisfied:

- $w = z_1 \cdot \omega^{p_1} \cdot z_2 \cdot \ldots \cdot \omega^{p_\ell} \cdot z_{\ell+1}$
- $\ell = 0$ if and only if neither ω^2 nor ω^{-2} is a factor of w
- if $\ell \geq 1$ then:
  - $z_0 \in \tilde{A}^*\omega^{s(p_1)} - \tilde{A}^*\omega^{\pm 2}\tilde{A}^*$

– $z_k \in \omega^{s(p_{k-1})}\tilde{A}^* \cap \tilde{A}^*\omega^{s(p_k)} - \tilde{A}^*\omega^{\pm 2}\tilde{A}^* - \{\omega, \omega^{-1}\}$, for all $2 \leq k \leq \ell$
– $z_{\ell+1} \in \omega^{s(p_\ell)}\tilde{A}^* - \tilde{A}^*\omega^{\pm 2}\tilde{A}^*$

where $s(p)$, the *sign* of p is $+1$ (resp. -1) when $p > 0$ (resp. $p < 0$).

From the hypothesis that ω is reduced and primitive, one can derive the unicity, for every word z, of its ω-stable normal decomposition. We define a function θ from the set of reduced words in $\tilde{A}^*$ to $\mathbf{Z}$ in the following manner. Let $z \in \tilde{A}^*$ be a reduced word. We define

$$\theta(z) = \sum_{k=1}^{\ell} p_\ell \tag{20}$$

where the integers p_ℓ are those appearing in the ω-stable normal decomposition (19) of z. For every non-empty finite subset $S \subseteq FG(A)$ we define

$$\hat{\theta}(S) = \max\{\theta(z) \mid z \in S\}; \quad \check{\theta}(S) = \min\{\theta(z) \mid z \in S\}; \tag{21}$$

(in the above definition, we identify an element of the free group with its associated reduced word).

Lemma 13. *Let z be a reduced word over $\tilde{A}$. Then $\theta(z^{-1}) = -\theta(z)$.*

Proof: It suffices to notice that the inverse of a ω-stable normal decomposition of z is a ω-stable normal decomposition of z^{-1}. □

Lemma 14. *Let z, z' be reduced words over $\tilde{A}$. Then $|\theta(r(z \cdot z')) - \theta(z) - \theta(z')| \leq 9$.*

Proof: We treat first the particular case where $z \cdot z'$ is reduced too, and treat the general case afterwards.
Case 1: suppose that $z \cdot z'$ is reduced.
Let us consider the ω-stable normal decompositions of z, z':

$$(z_1, \omega^{p_1}, z_2, \ldots, \omega^{p_\ell}, z_{\ell+1}), \;\; (z'_1, \omega^{p'_1}, z'_2, \ldots, \omega^{p'_{\ell'}}, z'_{\ell'+1})$$

Clearly:

$$z \cdot z' = z_1 \cdot \omega^{p_1} \cdot z_2 \cdots \omega^{p_\ell} \cdot z_{\ell+1} \cdot z'_1 \cdot \omega^{p'_1} \cdot z'_2 \cdots \omega^{p'_{\ell'}} \cdot z'_{\ell'+1}.$$

The word $z_{\ell+1} \cdot z'_1$ is thus reduced and has a ω-stable normal decomposition:

$$(y_1, \omega^{q_1}, y_2, \ldots, \omega^{q_m}, y_{m+1}).$$

The length m, of this decomposition must fulfill

$$m \in \{0, 1, 2\}, \tag{22}$$

since a value greater or equal to 3 would imply that ω^2 or ω^{-2} is a factor of at least one of the words $z_{\ell+1}, z'_1$, which is impossible by definition of a normal ω-stable decomposition. For every $k \in \{1, m\}$ we must have

$$|q_k| \leq 1, \tag{23}$$

otherwise, again, ω^2 or ω^{-2} would be a factor of at least one of the words $z_{\ell+1}, z'_1$. In the case where $z_{\ell+1} \cdot z'_1 = \omega^h$, for some $h \in \mathbf{Z}$, by the same argument we must have

$$|h| \leq 3. \tag{24}$$

Subcase 1.1:$z_{\ell+1} \cdot z'_1 = \omega^h$, for some $h \in \mathbf{Z}$
The ω-stable normal decomposition of zz' is thus

$$(z_1, \omega^{p_1}, z_2, \ldots, \omega^{p_\ell+h+p'_1}, z'_2, \ldots, \omega^{p'_{\ell'}}, z'_{\ell'+1}).$$

Using inequality (24), we obtain: $|\theta(r(z \cdot z')) - \theta(z) - \theta(z')| \leq 3$.
Subcase 1.2:$z_{\ell+1} \cdot z'_1$ is not a power of ω.
The ω-stable normal decomposition of zz' is thus

$$(z_1, \omega^{p_1}, z_2, \ldots, \omega^{p_\ell}, y_1, \omega^{q_1}, y_2, \ldots, \omega^{q_m}, y_{m+1}, \omega^{p'_1}, z'_2, \ldots, \omega^{p'_{\ell'}}, z'_{\ell'+1}).$$

Using inequalities (22)(23), we obtain: $|\theta(r(z \cdot z')) - \theta(z) - \theta(z')| \leq 2$.
Case 2:General case.
Suppose that $z = z_1 \cdot z_2$,$z' = z_2^{-1} \cdot z_3$ where z_1, z_2, z_3 are reduced words and $z_1 z_3$ is reduced. Using case 1 we know that the three integers

$$|\theta(z_1 z_3) - \theta(z_1) - \theta(z_3)|, \;\; |\theta(z) - \theta(z_1) - \theta(z_2)|, \;\; |\theta(z') - \theta(z_2^{-1}) - \theta(z_3)|,$$

are smaller or equal to 3. Decompositiong the expression $|\theta(z_1 z_3) - \theta(z) - \theta(z')|$ as

$$|\theta(z_1 z_3) - \theta(z_1) - \theta(z_3) - \theta(z) + \theta(z_1) + \theta(z_2) - \theta(z') + \theta(z_2^{-1}) + \theta(z_3)|,$$

and using the triangular inequality we obtain

$$|\theta(z_1 z_3) - \theta(z) - \theta(z')| \leq 9.$$

□

Proof of theorem 12: Let us use the mapping θ associated with the word w_2, which is reduced and primitive (and in addition, cyclically reduced). Let

$$P = \cup_{k=1}^{n}\{u_k\} \cup \cup_{k=1}^{t}\{v_k\}; \;\; D = \max\{|\theta(z)| \mid z \in Pref(P)\}$$

$$K = 9(n+t)(2 + |\theta(w_1)| + |\theta(w_3)| + D).$$

We claim that if $|m| > 2K + 2$, then the solution ϕ_m of $u = v$ in $FG(A)$ does not extend to a solution in $FIM(A)$.

Let i be an integer such that

$$r_u = \sum_{k=1}^{i} \epsilon_k > 0. \tag{25}$$

From hypothesis (18) it follows that $i > 0$ and $\epsilon_i = 1$. We shall denote by α the word

$$\alpha = \Phi_m((\prod_{k=1}^{i-1} u_k x^{\epsilon_k}) u_i)$$

($r(\alpha)$ is a designated vertex of the lefthand-side u, for the solution Φ_m in the free group). Assume, for sake of contradiction, that:

$$m > 2K + 2 \text{ and } \phi_m \text{ is extended to a solution } \psi \tag{26}$$

of $u = v$ in $FIM(A)$, where $\psi(x) = e\phi_m(x)$ for some idempotent e.
Choose a vertex $a \in MT(e)$ for which

$$\theta(a) = \hat{\theta}(MT(e)). \tag{27}$$

We distinguish several cases for a node $c \in MT(\psi(v))$ (see figures 1,2) and show, in every case, that $\theta(c) < \hat{\theta}(MT(\psi(u)))$.
Case 1:$\beta = \Phi_m((\prod_{k=1}^{j-1} v_k x^{\delta_k})v_j), \delta_j = 1, b \in MT(e), c = r(\beta \cdot b)$.

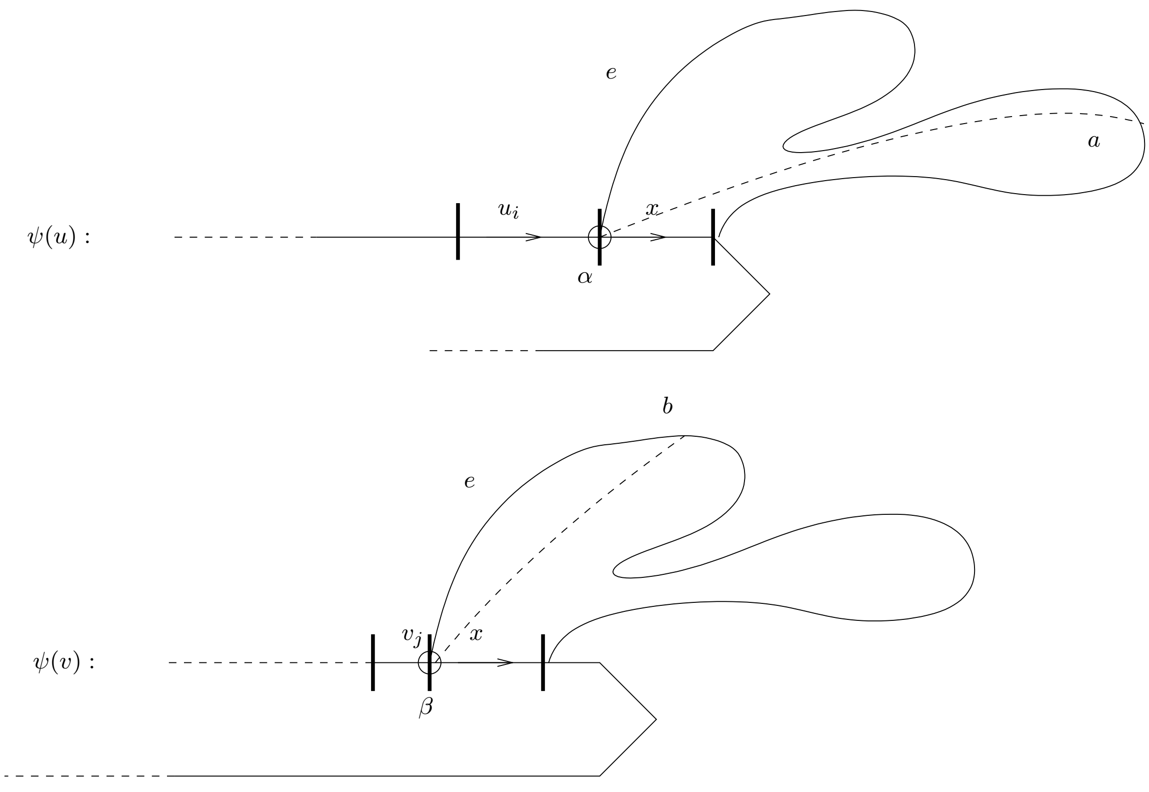

Fig. 1. Case 1.

Using the quasi-additivity of θ (Lemma 14), the choice of i (property (25)) and the

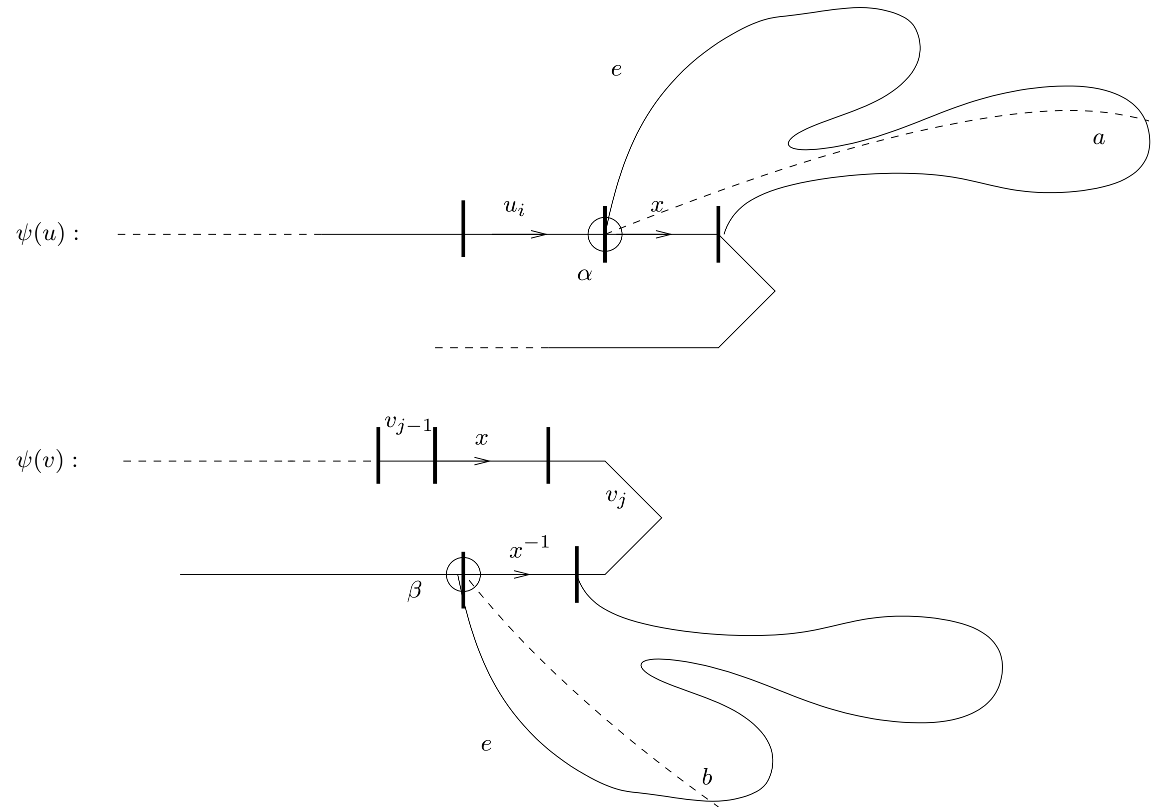

Fig. 2. Case 2.

fact that $\theta(w_2^m) = m - 2$, we get the two following sequences of inequalities:

$$
\begin{aligned}
\theta(r(\beta \cdot b)) &\leq (\sum_{k=1}^{j-1} \delta_k)(m-2) + (\theta(w_1) + \theta(w_3))(j-1) + \sum_{k=1}^{j} \theta(v_k) + \theta(b) + 18t \\
&\leq (\sum_{k=1}^{j-1} \delta_k)(m-2) + \theta(b) + K \\
&\leq (\sum_{k=1}^{j} \delta_k)(m-2) - (m-2) + \theta(b) + K \\
&\leq (\sum_{k=1}^{i} \epsilon_k)(m-2) - 2(m-2) + \theta(b) + K.
\end{aligned}
$$

$$\begin{aligned}\theta(r(\alpha\cdot a)) &\geq (\sum_{k=1}^{i-1}\epsilon_k)(m-2)+\sum_{k=1}^{i}\theta(u_k)+\theta(a)-18n\\ &\geq (\sum_{k=1}^{i}\epsilon_k)(m-2)-(m-2)+\theta(a)-K. \qquad (28)\end{aligned}$$

Since, by (26), $(m-2) > 2K$, the two above inequalities give

$$\theta(r(\beta\cdot b)) < \theta(r(\alpha\cdot a)) \leq \hat{\theta}(MT(\Phi_m(u))).$$

Case 2:$\beta = \Phi_m(\prod_{k=1}^{j} v_k x^{\delta_k}), \delta_j = -1, b \in MT(e), c = r(\beta\cdot b))$.
Here we get

$$\begin{aligned}\theta(r(\beta\cdot b)) &\leq (\sum_{k=1}^{j}\delta_k)(m-2)+(\theta(w_1)+\theta(w_3))(j)+\sum_{k=1}^{j}\theta(v_k)+\theta(b)+18t\\ &\leq (\sum_{k=1}^{j}\delta_k)(m-2)+\theta(b)+K\\ &\leq (\sum_{k=1}^{j-1}\delta_k)(m-2)-(m-2)+\theta(b)+K\\ &\leq (\sum_{k=1}^{i}\epsilon_k)(m-2)-2(m-2)+\theta(b)+K,\end{aligned}$$

which, together with (28) and assumption that $m > 2K$ leads again to

$$\theta(r(\beta\cdot b)) < \theta(r(\alpha\cdot a)) \leq \hat{\theta}(MT(\Phi_m(u))).$$

Case 3:$c = r(\Phi_m((\prod_{k=1}^{j} v_k x^{\delta_k})\cdot v'_{j+1}))$ with v'_{j+1} prefix of v_{j+1}.
We get

$$\begin{aligned}\theta(c) &\leq (\sum_{k=1}^{j}\delta_k)(m-2)+\sum_{k=1}^{j}\theta(v_k)+\theta(v'_{j+1})+18t\\ &\leq (\sum_{k=1}^{j}\delta_k)(m-2)+K\\ &\leq (\sum_{k=1}^{i}\epsilon_k)(m-2)-(m-2)+K.\end{aligned}$$

Since, by (26), $(m-2) > 2K$,using (28) we obtain

$$\theta(c) < \theta(r(\alpha\cdot a)) \leq \hat{\theta}(MT(\Phi_m(u))).$$

But every node $c \in MT(\psi(v))$ fulfills one of cases (1),(2) or (3). It follows that

$$\hat{\theta}(MT(\psi(v))) < \hat{\theta}(MT(\psi(u)))$$

contradicting assumption (26) that ψ is a solution in FIM(A) of the equation $u = v$. By similar arguments, one can prove that the assumption that

$$m < -2K - 2 \text{ and } \phi_m \text{ is extended to a solution } \psi \tag{29}$$

leads to some contradiction too: just consider an element $\check{a} \in MT(e)$ for which

$$\theta(\check{a}) = \check{\theta}(MT(e)). \tag{30}$$

and show that, for every $c \in MT(\psi(v)), \theta(c) > \theta(r(\alpha \cdot \check{a})) \geq \check{\theta}(MT(\psi(u)))$. It is thus established that the only extendible solutions in the free group ly among a finite set of solutions that we can compute. Decidability of the consistency problem follows from Theorem 7. □

Remark 15. Decidability of the consistency problem also holds for finite systems of equations, all of which fulfill the hypothesis of theorem 12.

In order to study the consistency problem for equations $u = v$ for which $\mathcal{V}(u) = \mathcal{V}(v)$, it is convenient to note the following lemma.

Lemma 16. *Let $u = v$ be an arbitrary equation in $FIM(A)$ and let $\phi : X \to \tilde{A}^*$ be a solution to $u = v$ in $FG(A)$. If the set of designated vertices in $MT(\phi(u))$ is equal to the set of designated vertices in $MT(\phi(v))$, then ϕ extends to a solution in $FIM(A)$.*

Proof: Let $\{w_1, w_2, \cdots, w_k\}$ be the union of the sets of designated vertices in $MT(\phi(u))$ and in $MT(\phi(v))$. View each w_j as a reduced word in $\tilde{A}^*$. Let

$$g = \phi(u)\phi(u)^{-1}\phi(v)\phi(v)^{-1}$$

and note that $MT(g) = MT(\phi(u)) \cup MT(\phi(v))$. Let

$$E = (w_1^{-1} g w_1)(w_2^{-1} g w_2) \cdots (w_k^{-1} g w_k),$$

and let $T = MT(E)$.

Extend the map ϕ by defining

$$\psi : X \to \tilde{A}^* \text{ by } \psi(x_i) = E\phi(x_i)$$

for each variable x_i in the content of u and in the content of v.

From the definition of a designated vertex, it follows that at each vertex labeled by w_j $(j = 1, \ldots, k)$, the tree

$$w_j T = \cup_{i=1}^{k} w_j MT(w_i^{-1} g w_i)$$

is a subtree of $MT(\psi(u))$ and that in fact

$$MT(\psi(u)) = w_1 T \cup w_2 T \ldots w_k T \cup MT(\phi(u)).$$

From the sequence of inclusions

$$MT(\phi(u)) \subseteq MT(g) \subseteq w_j MT(w_j^{-1} g w_j) \subseteq w_j MT(E) = w_j T,$$

it follows that $MT(\phi(u)) \subseteq w_jT$ for all j, and so $MT(\psi(u)) = w_1T \cup w_2T \dots w_kT$. Similarly, $MT(\psi(v)) = w_1T \cup w_2T \dots w_kT$, and so $MT(\psi(u)) = MT(\psi(v))$, whence ψ is a solution to $u = v$ in $FIM(A)$ that extends ϕ. $\Box$

We will introduce the concept of a standard factorization or a Choffrut factorization of a word. Let $u \in \tilde{A}^*$. A *reduced factorization* of $r(u)$ is a tuple of words

$$(u_1, u_2, \cdots, u_n)$$

such that every u_i is a non-empty word and $r(u) = u_1 \cdot u_2 \cdots u_n$. For $i = 1, 2, \cdots, n$ set $u_i = u'_i c_i$ where c_i is the last letter of u_i.

Theorem 17 (Choffrut [4]). *Let $u \in \tilde{A}^*$ and let $(u_1, u_2, \cdots, u_n)$ be a reduced factorization of $r(u)$. Then there exists a tuple of words $(e_0, u_1, e_1, u_2, \cdots, e_{n-1}, u_n, e_n)$ (which we call a* Choffrut factorization *of u) of $\tilde{A}^*$ such that*
CF1- $e_0, e_1, e_2, \cdots, e_n$ define idempotents of $FIM(A)$
CF2- $u =_I e_0u_1e_1u_2 \cdots e_{n-1}u_ne_n$
CF3- for all $i = 1, 2, \cdots, n$, $u'_i u'^{-1}_i \geq e_{i-1}$
CF4- for all $i = 1, 2, \cdots, n$, $u_i u_i^{-1} \not\geq e_{i-1}$
CF5- for all $i = 1, 2, \cdots, n$, $c_i^{-1} c_i \not\geq e_i$.
Moreover, this tuple is unique, up to componentwise equality in $FIM(A)$.

(See figure 3).

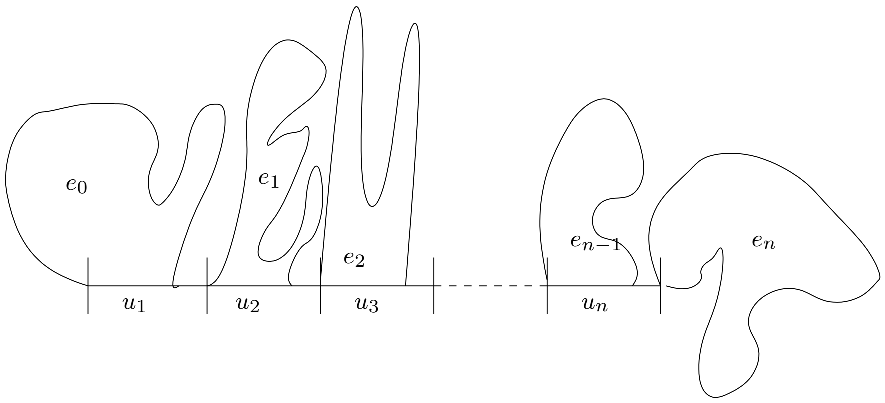

Fig. 3. Choffrut factorization.

The two following lemmas about Choffrut factorizations are useful. Let us denote by d the usual distance over $FG(A)$: for every $x, y \in FG(A)$, $\mathrm{d}(x, y) = |r(x^{-1}y)|$.The diameter of a subset $Q \subseteq FG(A)$ is then: $\mathrm{diam}(Q) = \max\{\mathrm{d}(x, y) \mid x, y \in Q\}$.

Lemma 18 (contraction). *Let $u \in \tilde{A}^*$ with Choffrut factorization:*

$$(e_0, u_1, e_1, \dots, u_{i-1}, e_{i-1}, u_i, e_i, u_{i+1}, e_{i+1}, \dots, u_n, e_n).$$

Then

$$(e_0, u_1, e_1, \ldots, u_{i-1}, e'_{i-1}, u_i u_{i+1}, e_{i+1}, \ldots, u_n, e_n),$$

where $e'_{i-1} = e_{i-1}(u_i e_i u_i^{-1})$ *is again a Choffrut-factorization of the same word.*

Proof: Easy verification: just check that the proposed tuple satisfies conditions CF1-CF5 of theorem 17. □

Lemma 19 (product). *Let* $u \in \tilde{A}^*$ *with Choffrut factorization:*

$$(e_0, u_1, e_1, \ldots, u_n, e_n),$$

and let $w \in \tilde{A}^*$.
1- If $\mathrm{diam}(MT(w)) < |u_1|$ *then* $w \cdot u$ *admits a Choffrut factorization of the form*

$$(e'_0, r(wu_1), e_1, u_2, e_2, \ldots, u_n, e_n).$$

2- If $\mathrm{diam}(MT(w)) < |u_n|$ *then* $u \cdot w$ *admits a Choffrut factorization of the form*

$$(e_0, u_1, e_1, u_2, e_2, \ldots, u_{n-1}, e'_{n-1}, r(u_n w), e'_n).$$

Proof: 1- Suppose $(e_0, u_1, e_1, \ldots, u_n, e_n)$ and w fulfill the hypothesis. Let us check that the choice

$$e'_0 = w e_0 w^{-1},$$

satisfies the announced property.
CF1: It suffices to see that e'_0 is a Dyck word, hence defines an idempotent element of $FIM(A)$.
CF2: The equality

$$e'_0 r(wu_1) =_I w e_0 u_1 \tag{36}$$

is equivalent with $w e_0 w^{-1} r(wu_1) =_I w e_0 u_1$, which amounts to

$$\{r(x) \mid x \in Pref(w e_0 w^{-1} r(wu_1))\} = \{r(x) \mid x \in Pref(w e_0 u_1)\}.$$

This last equality can be easily checked. From (36) follows that

$$e'_0 r(wu_1) e_1 u_2 e_2 \cdots u_n e_n =_I w e_0 u_1 e_1 \cdots u_n e_n$$

hence that CF2 is fulfilled.
CF3: Let us check that $r(wu'_1) r(wu'_1)^{-1} \geq w e_0 w^{-1}$. There exists reduced words w_1, w_2, v_2 such that

$$w = w_1 w_2, \;\; u'_1 = w_2^{-1} v_2, \;\; r(wu'_1) = w_1 v_2.$$

By hypothesis

$$u'_1 u_1^{'-1} \geq e_0.$$

Multiplying on the left by $w = w_1 w_2$ on the right by $w^{-1} = w_2^{-1} w_1^{-1}$ we get

$$w_1 w_2 u_1' u_1'^{-1} w_2^{-1} w_1^{-1} \geq w e_0 w^{-1}.$$

Replacing u_1' by $w_2^{-1} v_2$ we get

$$w_1 w_2 w_2^{-1} v_2 v_2^{-1} w_2 w_2^{-1} w_1^{-1} \geq w e_0 w^{-1}.$$

Since for every $u \in \tilde{A}^*, 1 \geq uu^{-1}$, we obtain:

$$w_1 v_2 v_2^{-1} w_1^{-1} \geq w_1 w_2 w_2^{-1} v_2 v_2^{-1} w_2 w_2^{-1} w_1^{-1}$$

and, finally, by the two last inequalities

$$w_1 v_2 v_2^{-1} w_1^{-1} \geq w e_0 w^{-1},$$

i.e. $r(wu_1') r(wu_1')^{-1} \geq w e_0 w^{-1}$.
CF4: Let us check that $r(wu_1) r(wu_1)^{-1} \not\geq e_0'$.
The Munn-tree of e_0' decomposes as:

$$MT(w e_0 w^{-1}) = MT(w) \cup r(w) \cdot MT(e_0). \tag{37}$$

Let us consider $x = r(wu_1)$.
Since $\mathrm{d}(r(w), x) = |u_1|, r(w) \in MT(w)$ and $\mathrm{diam}(MT(w)) < |u_1|$, we are sure that

$$x \notin MT(w). \tag{38}$$

By hypothesis $u_1 u_1^{-1} \not\geq e_0$ and $u_1' u_1'^{-1} \geq e_0$, hence $u_1 \notin MT(e_0)$, so that

$$x = r(wu_1) \notin r(w) \cdot MT(e_0) \tag{39}$$

By (38,39) and the decomposition (37), $x \notin MT(e_0')$, hence $r(wu_1) r(wu_1)^{-1} \not\geq e_0'$.
CF5: Since the values of e_i, c_i for $1 \leq i \leq n$ did not change, this property is trivially preserved.

2-Let us choose the idempotents e_{n-1}', e_n' such that

$$(e_{n-1}', r(u_n w), e_n') \tag{40}$$

is a Choffrut factorization of $e_{n-1} u_n e_n w$. Let us check properties CF1-CF5 for the tuple $(e_0, u_1, e_1, u_2, e_2, \ldots, u_{n-1}, e_{n-1}', r(u_n w), e_n')$ thus defined.
CF1: is clearly true.
CF2: is true because $e_{n-1} u_n e_n w =_I e_{n-1}' r(u_n w) e_n'$.
CF3,CF4: follow from the hypothesis that $(e_0, u_1, e_1, u_2, e_2, \ldots, u_{n-1}, e_{n-1}, u_n, e_n)$ and (40) do fulfill CF3,CF4.
CF5: For $i \neq n-1$ here again the property follows from CF5 applied on the two initial Choffrut factorizations. Let us check that $c_{n-1}^{-1} \notin MT(e_{n-1}')$.
The Munn-tree of $e_{n-1} u_n e_n w$ decomposes as:

$$MT(e_{n-1} u_n e_n w) = MT(e_{n-1} u_n) \cup u_n \cdot MT(e_n) \cup u_n \cdot MT(w). \tag{41}$$

By CF5 applied on the initial Choffrut factorization we know that $c_{n-1}^{-1} \notin MT(e_{n-1})$ and, since $c_{n-1} u_n$ is a reduced word, $c_{n-1}^{-1} \notin MT(u_n)$, which, alltogether, show that

$$c_{n-1}^{-1} \notin MT(e_{n-1} u_n). \tag{42}$$

If c_{n-1}^{-1} belongs to $u_n \cdot MT(e_n)$, then the geodesics from c_{n-1}^{-1} to u_n would be included in $u_n \cdot MT(e_n)$; since the vertex $r(u_n c_n^{-1})$ belongs to this geodesics, by left-translation by u_n we would get that $c_n^{-1} \in MT(e_n)$, contradicting CF5 on the initial Choffrut factorization. It follows that

$$c_{n-1}^{-1} \notin u_n \cdot MT(e_n). \tag{43}$$

Since $\mathrm{d}(c_{n-1}^{-1}, u_n) = |u_n| + 1$, $u_n \in u_n \cdot MT(w)$ and $\mathrm{diam}(u_n \cdot MT(w)) < |u_n|$, we are sure that

$$c_{n-1}^{-1} \notin u_n \cdot MT(w). \tag{44}$$

The decomposition (41) combined with properties (42),(43),(44) show that $c_{n-1}^{-1} \notin MT(e_{n-1}u_n e_n w)$, and, a fortiori

$$c_{n-1}^{-1} \notin MT(e'_{n-1}),$$

which proves that $c_{n-1}^{-1}c_{n-1} \not\geq e'_{n-1}$. $\square$

Theorem 20. *The consistency problem for equations of the form* $u_1 x^{\zeta_1} u_2 = v_1 x^{\zeta_2} v_2$ *where* $u_i, v_i \in (A \cup A^{-1})^*$ *and* $\zeta_i = \pm 1$ *for* $i = 1, 2$ *in* $FIM(A)$ *is decidable.*

Proof: If $\zeta_1 \neq \zeta_2$ then the consistency problem is decidable by Corollary 9. We will assume that $\zeta_1 = \zeta_2$. Without loss of generality assume that $\zeta_1 = \zeta_2 = 1$. The case when $\zeta_1 = \zeta_2 = -1$ will follow by considering the equation $u_2^{-1} x u_1^{-1} = v_2^{-1} x v_1^{-1}$. From Theorem 11 we know that there exists a finite set of parametric words defining the solution set to this equation in $FG(A)$. Choose one such parametric word: there are corresponding reduced words w_1, w_2 and w_3 so that $w_1 w_2^{\pm 1} w_3$ is reduced as written, w_2 is cyclically reduced and primitive, and $w_1 w_2^n w_3$ is a solution in $FG(A)$ for all $n \in \mathbf{Z}$.

Let

$$E = (u_1 w_1 w_1^{-1} u_1^{-1})(u_2^{-1} w_3^{-1} w_3 u_2)(v_1 w_1 w_1^{-1} v_1^{-1})(v_2^{-1} w_3^{-1} w_3 v_2)(w_2 w_2^{-1}),$$

$$D = \mathrm{diam}(MT(E)).$$

Assume that for some value of n, the solution $w_1 w_2^n w_3$ extends to a solution to the equation in $FIM(A)$. Without loss of generality we may assume that $n \geq 0$ (replace w_2 by w_2^{-1} if necessary). Choose $N \in \mathbf{N}$ *minimal* such that $\phi(x) = w_1 w_2^N w_3$ extends to a solution $\psi(x)$ in $FIM(A)$. We will show that $N < 8D + 2$.

Suppose on the contrary that

$$N \geq 8D + 2. \tag{45}$$

Factor $\psi(x)$ using the Choffrut factorization based on the reduced word $w_1 w_2^N w_3$ to get

$$\psi(x) =_I e_{-1} w_1 e_0 w_2 e_1 \cdots e_{N-1} w_2 e_N w_3 e_{N+1}. \tag{46}$$

Let α, β be the integers defined by:

$$|w_1 w_2^{\alpha-1}| \leq D < |w_1 w_2^{\alpha}|, \;\; |w_3^{-1} w_2^{-\beta+1}| \leq D < |w_3^{-1} w_2^{-\beta}|. \tag{47}$$

Claim 21. *: $\alpha \leq D+1, \;\; \beta \leq D+1$.*

By definition of α, β ,

$$(\alpha - 1)|w_2| \leq D, \;\; (\beta - 1)|w_2| \leq D \tag{48}$$

hence $\alpha \leq D+1$, and $\beta \leq D+1$. $\Box$
Since $|u_1| \leq D < |w_1 w_2^{\alpha}|$, the last letter of w_2 cannot be cancelled in any reduction from $u_1 w_1 w_2^{\alpha}$ to its normal form $r(u_1 w_1 w_2^{\alpha})$. Hence, as w_2 is cyclically reduced, all the words

$$r(u_1 w_1 w_2^{\alpha}) w_2^h$$

are reduced , for $h \geq 0$. Similarly all the words $r(v_1 w_1 w_2^{\alpha}) w_2^h, w_2^h r(w_2^{\beta} w_3 u_2), w_2^h r(w_2^{\beta} w_3 v_2)$ are reduced , for $h \geq 0$. By claim 21 and the above properties, the two following factorizations are reduced:

$$(r(u_1 w_1 w_2^{\alpha}), \underbrace{w_2, \cdots, w_2}_{N-(\alpha+\beta)}, r(w_2^{\beta} w_3 u_2) \tag{49}$$

$$(r(v_1 w_1 w_2^{\alpha}), \underbrace{w_2, \cdots, w_2}_{N-(\alpha+\beta)}, r(w_2^{\beta} w_3 v_2)). \tag{50}$$

Either $r(u_1) = r(v_1)$ or $r(u_1) \neq r(v_1)$ in $FG(A)$. When $r(u_1) = r(v_1)$, then the designated u-vertex and designated v-vertex are the same and so by Lemma 16 the equation $u = v$ is consistent, so we may suppose that $r(u_1) \neq r(v_1)$ in $FG(A)$. This implies that $r(u_1 w_1 w_2^{\alpha}) \neq r(v_1 w_1 w_2^{\alpha})$ in $\tilde{A}^*$. Thus the reduced factorizations (49) and (50) of $r(\phi(u)) = r(\phi(v))$ are not identical.

Without loss of generality assume that $r(v_1 w_1 w_2^{\alpha})$ is a proper prefix of $r(u_1 w_1 w_2^{\alpha})$. Then there exists $w' \in \tilde{A}^*$ such that

$$r(u_1 w_1 w_2^{\alpha}) = r(v_1 w_1 w_2^{\alpha}) w', \;\; w' w_2^{N-(\alpha+\beta)} r(w_2^{\beta} w_3 u_2) = w_2^{N-(\alpha+\beta)} r(w_2^{\beta} w_3 v_2) \tag{51}$$

in $\tilde{A}^*$.

Claim 22. *$|r(u_1 w_1 w_2^{\alpha})| \leq 3D$ and $|r(v_1 w_1 w_2^{\alpha})| \leq 3D$.*

By inequality (48) $|w_2^{\alpha-1}| \leq D$ hence $|w_2^{\alpha}| \leq D + |w_2| \leq 2D$. Since $|r(u_1 w_1)| \leq D$, the claim follows. $\Box$
Let us show that the word w' is a power of w_2. Let $q \in \mathbf{N}$ such that

$$q|w_2| \leq |w'| < (q+1)|w_2|.$$

If the first inequality was strict, then the following comparisons between the lengths of prefixes of $r(\psi(u))$ would hold:

$$|r(v_1 w_1 w_2^{\alpha}) w_2^q| < |r(v_1 w_1 w_2^{\alpha}) w'| < |r(v_1 w_1 w_2^{\alpha}) w_2^{(q+1)}| < |r(u_1 w_1 w_2^{\alpha}) w_2| < |r(v_1 w_1 w_2^{\alpha}) w_2^{q+2}|, \tag{52}$$

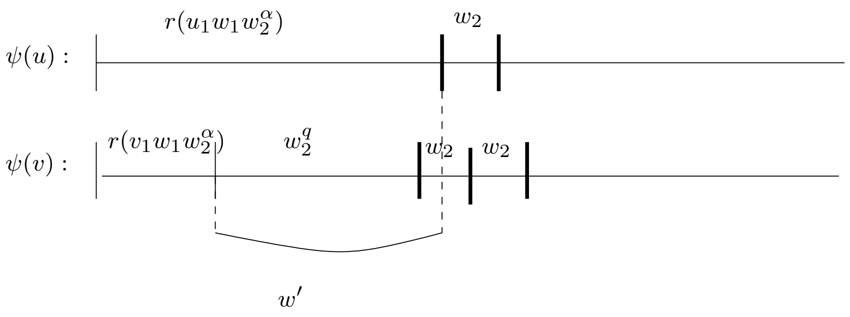

Fig. 4. the occurence of w'.

(see figure 4).

The first two inequalities follow from the definition of q. The third and fourth inequality are obtained from the first and second one, just by adding $|w_2|$ on both sides of it. By claim 22, $|r(u_1w_1w_2^\alpha)w_2w_2| \leq 5D$, while , by claim 21, and inequality (45), $N-\alpha-\beta \geq 5D$, hence the fifth word in the above inequality is really a prefix of $r(v_1w_1w_2^\alpha)w_2^{N-(\alpha+\beta)}$.

Suppose that $q|w_2| < |w'| < (q+1)|w_2|$, and let us examine several occurences of the word w_2 inside the same word $r(\psi(u)) = r(\psi(v))$:
-an occurence of w_2 ends at distance $|r(u_1w_1w_2^\alpha)w_2|$ of the leftside
-an occurrence of w_2^2 begins at distance $|r(v_1w_1w_2^\alpha)w_2^q|$ and ends at distance $|r(v_1w_1w_2^\alpha)w_2^{q+2}|$.
By the inequalities (52), the first occurence of w_2 would ly strictly inside the second occurrence of w_2^2, which is impossible since w_2 is primitive. We have established that

$$q|w_2| = |w'|$$

and, since w' is a prefix of $w_2^{N-\alpha-\beta}$ (see (51)),

$$w' = w_2^q. \tag{53}$$

Claim 23. $q \leq 3D$.

By Claim (22) the word $r(u_1w_1w_2^\alpha)$ has a length smaller than $3D$. Since w' is a suffix of this word, the claim holds. □
We now compare two Choffrut factorizations of $\psi(u) =_I \psi(v)$ deduced from the Choffrut factorization (46) of $\psi(x)$ by means of the contraction lemma 18 and the product lemma 19. Let

$$K = N - (\alpha + \beta + q).$$

Applying iteratively the contraction-lemma to the Choffrut factorization (46), we obtain the Choffrut factorization of $\psi(x)$:

$$(e'_0, r(w_1w_2^\alpha), e_\alpha, \ldots, e_{\alpha+K-1}, w_2, e'_1, r(w_2^{\beta+q}w_3), e_{N+1}). \tag{54}$$

By the product-lemma, since $|u_1| \leq D < |r(w_1 w_2^\alpha)|$, and $|u_2^{-1}| \leq D < |r(w_3^{-1} w_2^{-\beta})|$, we obtain a Choffrut factorization of $\psi(u)$:

$$(g_0, r(u_1 w_1 w_2^\alpha), e_\alpha, \ldots, e_{\alpha+K-1}, w_2, g_1, r(w_2^{\beta+q} w_3 u_2), g_2) \tag{55}$$

and by similar arguments, a Choffrut factorization of $\psi(v)$:

$$(g_0', r(v_1 w_1 w_2^{\alpha+q}), e_{\alpha+q}, \ldots, e_{\alpha+K+q-1}, w_2, g_1', r(w_2^\beta w_3 v_2), g_2''), \tag{56}$$

for some idempotents $g_0, g_1, g_2, g_0', g_1', g_2''$.

By unicity of the Choffrut factorization associated to a given reduced factorization, (55) and (56) must coincide:

$$(e_\alpha, e_{\alpha+1}, \ldots, e_{\alpha+K-1}) =_I (e_{\alpha+q}, e_{\alpha+q+1}, \ldots, e_{\alpha+q+K-1}). \tag{57}$$

By Claim 21 and Claim 23 and hypothesis (45)we know that $\alpha + \beta + 2q \leq 2D + 2 + 6D \leq N$ or, in other words

$$q \leq K.$$

Equating the prefixes of length q of both sides of equation (57) gives:

$$(e_\alpha, e_{\alpha+1}, \ldots, e_{\alpha+q-1}) =_I (e_{\alpha+q}, e_{\alpha+q+1}, \ldots, e_{\alpha+2q-1}). \tag{58}$$

Let $\phi'(x) =_M w_1 w_2^{N-q} w_3$ and consider the map:

$\psi'(x) =_M e_{-1} w_1 e_0 w_2 e_1 \cdots w_2 e_{\alpha-1} w_2 e_{\alpha+q} w_2 e_{\alpha+q+1} \cdots e_{\alpha+q+i} w_2 \cdots e_{N-1} w_2 e_N w_3 e_{N+1}$,

In other words, $\psi'(x)$ is obtained from the righthand side of (46) by cutting out the factor $w_2 e_\alpha w_2 e_{\alpha+1} \cdots w_2 e_{\alpha+q-1}$, as shown on figure 5.

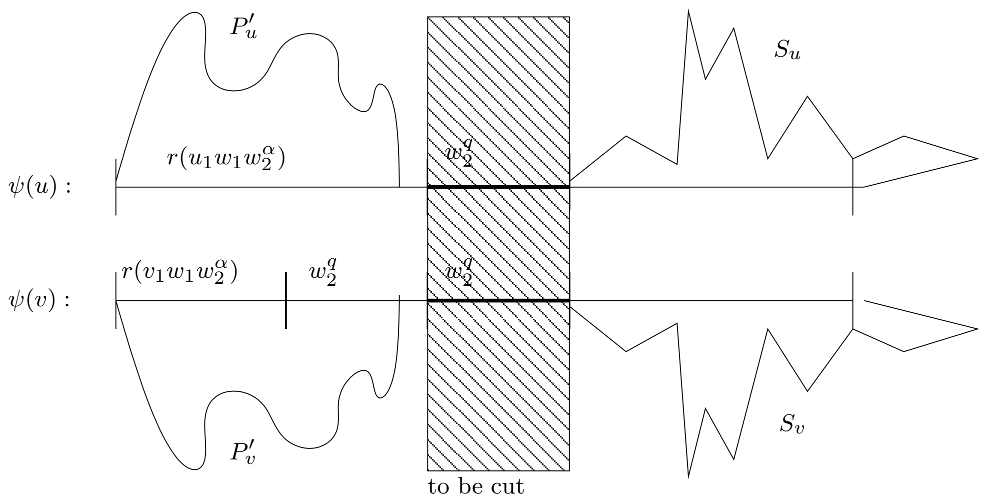

Fig. 5. Shrinking ψ.

Let us consider the decompositions over $FIM(A)$: $\psi(u) =_I P_u \cdot S_u, \psi(v) =_I P_v \cdot S_v$, where:

$$P_u =_M u_1 e_{-1} w_1 e_0 w_2 \cdots e_{\alpha+q-1} w_2, \quad S_u =_M e_{\alpha+q} w_2 \cdots e_{N-1} w_2 e_N w_3 u_2,$$

$$P_v =_M v_1 e_{-1} w_1 e_0 w_2 \cdots e_{\alpha+2q-1} w_2, \quad S_v =_M e_{\alpha+2q} w_2 \cdots e_{N-1} w_2 e_N w_3 u_2.$$

Claim 24. $P_u =_I P_v, \quad S_u =_I S_v.$

Since $r(P_u) = r(u_1 w_1 w_2^{\alpha+q})$ and $r(P_v) = r(v_1 w_1 w_2^{\alpha+2q})$, we know that $r(P_u) = r(P_v)$, and by cancellativity of the product in the group $FG(A)$ we also know that $r(S_u) = r(S_v)$. Let us consider the decomposition of the tree $MT(\psi(u))$ as

$$MT(\psi(u)) = T_1 \cup T_2,$$

where $T_1 - \{r(P)\}$ (resp. $T_2 - \{r(P)\}$) is the connected component of $MT(\psi(u)) - \{r(P_u)\}$ which posesses 1, (resp. is the union of the connected components which do not posess 1) and $\{r(P_u)\} = T_1 \cap T_2$. Since $\mathrm{diam}(MT(u_1)) \leq D < |w_1 w_2^{\alpha}|$, every vertex of $MT(P_u)$ belongs to T_1. Analogously, since $\mathrm{diam}(MT(u_2)) \leq D < |w_2^{\beta} w_3|$, every vertex of $r(T) \cdot MT(S_u)$ belongs to T_2. Using the same arguments about P_v, S_v we arrive at:

$$MT(P_u) \subseteq T_1, \quad MT(P_v) \subseteq T_1, \quad r(P_u) \cdot MT(S_u) \subseteq T_2, \quad r(P_v) \cdot MT(S_v) \subseteq T_2.$$

This shows that $MT(P_u) = T_1 = MT(P_v)$ and $MT(S_u) = r(P_u)^{-1} \cdot T_2 = MT(S_v)$. $\square$

Let $P'_u =_M u_1 e_{-1} w_1 e_0 w_2 e_1 \cdots e_{\alpha-1} w_2$ and $P'_v =_M v_1 e_{-1} w_1 e_0 w_2 e_1 \cdots e_{\alpha+q-1} w_2$.

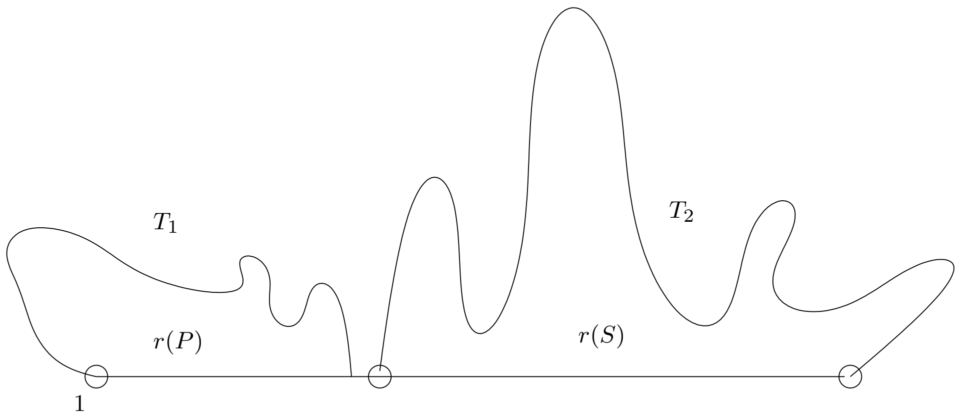

Fig. 6. Decomposition of $MT(\psi(u))$.

Claim 25. $P'_u =_I P'_v$.

This claim is obtained by the same kind of argument as Claim 24: just consider the decomposition of $MT(\psi(u)) - \{r(P'_u)\}$ in connected components. □
Let us look at the following decompositions (which follow from the mere definition of $\psi'(x)$):

$$\psi'(u) =_M (u_1 e_{-1} w_1 e_0 w_2 e_1 \cdots w_2 e_{\alpha-1} w_2) \cdot (e_{\alpha+q} \cdots e_{N-1} w_2 e_N w_3 u_2) \tag{60}$$

$$\psi'(v) =_M (v_1 e_{-1} w_1 e_0 w_2 e_1 \cdots w_2 e_{\alpha-1} w_2) \cdot (e_{\alpha+q} w_2 \cdots e_{\alpha+2q-1} w_2) \cdot (e_{\alpha+2q} \cdots w_2 e_N w_3 v_2) \tag{61}$$

Plugging identity (58) into the equality (61) results in:

$$\psi'(v) =_I (v_1 e_{-1} w_1 e_0 w_2 e_1 \cdots w_2 e_{\alpha-1} w_2) \cdot (e_\alpha w_2 \cdots e_{\alpha+q-1} w_2) \cdot (e_{\alpha+2q} \cdots w_2 e_N w_3 v_2). \tag{62}$$

With the above notations, equalities (60) (62) express that

$$\psi'(u) =_M P'_u \cdot S_u, \;\; \psi'(v) =_I P'_v \cdot S_v.$$

It follows from these two decompositions and Claims 24-25 that

$$\psi'(u) =_I \psi'(v).$$

Finally, ψ' is a solution of the equation in $FIM(A)$ that extends ϕ' contradicting the minimality of N. Hence, if there is any integer $n \in \mathbf{Z}$ such that $w_1 w_2^n w_3$ extends to a solution in $FIM(A)$, then there must be such an integer n with $|n| < 8D + 2$. By Theorem 7, this implies that the consistency problem is decidable. □

4. Final comments

In fact our treatment of the extension-theorem 7 does not use the full power of Rabin's theorem, since we only use decidability of the *weak* Monadic Second-Order Logic over the tree T_A. The decidability of WMSOL over T_A was proved by Doner in [8].
Since we established theorem 7, M. Lohrey and N. Ondrusch have extended the result to inverse monoids presented by a finite number of idempotent relators over the free inverse monoid (such monoids were previously studied in [18]); their extension of our arguments really use the full power of Rabin's tree theorem.
The treatment of left-linear equations over finite subsets of the free monoid (without the *prefix-closedness* constraint) by means of reduction to WMSOL and tree-automata was already achieved in [2], where the authors also give a precise complexity analysis of this problem: it is exactly Exp-Time complete.
The consistency problem for *all* single-variable equations in $FIM(A)$, remains open; we hope that the arguments involved in the proofs presented here may be extended to more general cases and, possibly, to all single-variable equations.

Acknowledgments

The second author was supported by NSF grant No. DMS-9970471. The third author thanks V. Diekert for invitating him in Stuttgart University with the support of the Humboldt fundation. We thank F. Baader, R. Gilman, M. Lohrey and N. Ondrusch for useful information on the subject.

References

[1] K. I. Appel, One-variable equations in free groups, *Proc. Amer. Math. Soc.* 19 (1968), 912–918.

[2] F. Baader and P. Narendran, Unification of concept terms in description logics, *J. Symbolic Computation* 31 (2001), 277–305.

[3] J. Barwise (Ed.) *Handbook of Mathematical Logic*, North Holland (1978).

[4] C. Choffrut, Conjugacy in free inverse monoids, *Int. J. Alg. Comp.* 3.2 (1993), 169–188.

[5] L. P. Comerford and C. C. Edmunds, Products of Commutators and Products of Squares in a Free Group, *Int. J. Alg. Comp.* 4.3 (1994) 469-480.

[6] T. Deis, *Equations in Free Inverse Monoids*, Ph.D. Thesis, Univ. of Nebraska (1999).

[7] V.Diekert, C.Gutierrez,and C.Hagenah, The existential theory of equations with rational constraints in free groups is PSPACE-complete, *to appear in Information and Computation* (2005), 1–45.

[8] J. Doner, Tree acceptors and some of their applications, *J. Comput. System Sci.* 4 (1970), 406–451.

[9] R.H. Gilman and A.G. Myasnikov, One-variable equations in free groups via context-free languages, *Computational and experimental group theory, Contemp. Math.* 349 (2004), 83–88.

[10] C. Gutiérrez, Satisfiability of Equations in Free Groups is in PSPACE, *32nd Ann. ACM Symp. Theory Comput. (STOC'2000)*, ACM Press 2000.

[11] O. Kharlampovich and A.G. Myasnikov, Tarski's problem about the elementary theory of free groups has a positive solution , *Electron. Res. Announc. Amer. Math. Soc.*4 (1998), 101–108.

[12] Mark. V. Lawson, *Inverse Semigroups; the theory of Partial Symmetries*, (World Scientific 1998).

[13] A. A. Lorents, Representations of sets of solutions of systems of equations with one unknown in a free group, *Dokl. Akad. Nauk. SSSR* 178 (1968), 290–292 (Russian).

[14] M. Lothaire, *Algebraic Combinatorics on Words*, (Cambridge University Press 2001).

[15] R. C. Lyndon, Equations in free groups, *Trans. Amer. Math. Soc.* 96 (1960), 445–457.

[16] G. S. Makanin, Equations in a Free Group, *Izv. Akad. Nauk. SSR, Ser. Math* 46 (1983) 1199-1273. English transl. in *Math. USSR Izv.* 21 (1983).

[17] G. S. Makanin, Problem of Solvability of Equations in Free Semigroup, *Math. Sbornik* 103 (1977) 147-236. English transl. in *Math. USSR Sbornik* 32 (1977).

[18] S. Margolis and J. Meakin, Inverse monoids, trees and context-free languages, *Trans. Amer. Math. Soc.* 335.1 (1993), 259–276.

[19] W. D. Munn, Free inverse semigroups, *Proc. London Math .Soc.* (3) 29 (1974), 385–404.

[20] A.L.T. Patterson, *Groupoids, Inverse Semigroups, and their* $\mathbf{C}^*$*-algebras*, (Birkhäuser 1998).

[21] M. Petrich, *Inverse semigroups*, (Wiley 1984).

[22] W. Plandowski, Satisfiability of Word Equations with Constants is in PSPACE, *Proc. 40th Ann. Symp. Found. Comput. Sci. (FOCS'99), IEEE Computer Society Press*, (1999) 495-500.

[23] M. O. Rabin, Decidability of Second Order Theories and Automata on Infinite Trees, *Trans. Amer. Math. Soc.* 141 (1969) 1-35.

[24] A. A. Razborov, On Systems of Equations in a Free Group, *Math. USSR-Izv.* 25 (1985) 115-162.

[25] B. V. Rozenblat, Diophantine theories of free inverse semigroups, *Sibirskii Mat. Zhurnal* (6) 26 (1986), 101–107 (Russian); english transl. in pp. 860–865.

[26] H.E. Scheiblich, Free inverse semigroups, *Semigroup Forum* (4) 29 (1972), 351–359.
[27] P. V. Silva, Word Equations and Inverse Monoid Presentations, in *Semigroups and Applications, Including Semigroup Rings*, ed. S. Kublanovsky, A. Mikhalev, P. Higgins, J. Ponizovskii, "Severny Ochag", St. Petersburg (1999).