UPMAIL Technical Report No. 137
February 11, 1997
Revised June 20, 1997

Monadic Simultaneous Rigid E-Unification and Related Problems

Yuri Gurevich*

EECS Department
University of Michigan
Ann Arbor, MI, 48109-2122
USA

email gurevich@umich.edu

Andrei Voronkov†

Computing Science Department
Uppsala University
Box 311, S-751 05 Uppsala,
Sweden

email voronkov@csd.uu.se

*Partially supported by grants from NSF, ONR and the Faculty of Science and Technology of Uppsala University.
†Supported by a TFR grant

Abstract

We study the monadic case of a decision problem know as simultaneous rigid E-unification. We show its equivalence to an extension of word equations. We prove decidability and complexity results for special cases of this problem.

Section 1

Introduction

Simultaneous rigid E-unification is a combinatorial problem in equational logic which is closely connected with some formulations of the Herbrand theorem and with automated theorem proving by the tableau method and the connection (or mating) method. In this section we define simultaneous rigid E-unification, discuss its connection with several decision problems in logic and survey some known results.

We shall consider *equational logic,* i.e. logic whose only predicate is the equality predicate $\simeq$, but our results can easily be generalized to general first-order logic with equality. Let $s_1, t_1, \ldots, s_n, t_n, s, t$ be terms. All atomic formulas in equational logic are *equations,* i.e. expressions of the form $s \simeq t$. We do not distinguish an equation $s \simeq t$ from the equation $t \simeq s$. We write $s_1 \simeq t_1, \ldots, s_n \simeq t_n \vdash s \simeq t$ to denote that the formula $\forall(s_1{\simeq}t_1 \wedge \ldots \wedge s_n{\simeq}t_n \supset s{\simeq}t)$ is true, i.e. it is provable in first-order (classical or intuitionistic) logic. Equivalently, we can say that s and t lie in the same class of the congruence induced by $\{s_1{\simeq}t_1, \ldots, s_n{\simeq}t_n\}$.

A *rigid equation* is an expression $\mathcal{E} \vdash_\forall s{\simeq}t$, where $\mathcal{E}$ is a finite set of equations. The set $\mathcal{E}$ is called the *left side* of this rigid equation, and the equation $s \simeq t$ — its *right side.* A *solution to a rigid equation* $\{s_1{\simeq}t_1, \ldots, s_n{\simeq}t_n\} \vdash_\forall s{\simeq}t$ is any substitution θ such that $s_1\theta \simeq t_1\theta, \ldots, s_n\theta \simeq t_n\theta \vdash s\theta \simeq t\theta$. A *system of rigid equations* is a finite set of rigid equations. A *solution to a system of rigid equations* $\mathcal{R}$ is any substitution that is a solution to every rigid equation in $\mathcal{R}$. The problem of solvability of rigid equations is known as *rigid E-unification.* The problem of solvability of systems of rigid equations is known as *simultaneous rigid E-unification,* in the sequel abbreviated as SREU.

We shall denote sets of equations by $\mathcal{E}$, systems of rigid equations by $\mathcal{R}$ and rigid equations by R. We shall sometimes write the left side of a rigid equation as a *sequence* of equations, for example $x{\simeq}a \vdash_\forall g(x){\simeq}x$ instead of $\{x{\simeq}a\} \vdash_\forall g(x){\simeq}x$.

In [2] it is shown that the decidability of SREU is equivalent to the decidability of some other fundamental problems, for example the following ones:

Problem 1 (Formula Instantiation)
Given a quantifier-free formula $\varphi(\bar{x})$, is there a term sequence $\bar{t}$ such that the formula $\varphi(\bar{t})$ is provable?

Problem 2 (Existential Intuitionistic)
Is a given existential formula $\exists\bar{x}\varphi(\bar{x})$ provable in intuitionistic logic?

Problem 3 (Prenex Intuitionistic)
Is a given prenex formula provable in intuitionistic logic?

For a suitable notion of a derivation skeleton, SREU is also equivalent to the following problem.

Problem 4 (Skeleton Instantiation)
Given a formula φ and a derivation skeleton, is there a derivation of φ having this skeleton?

Some known results on SREU are the following.

- SREU is undecidable (Degtyarev and Voronkov [5]). This result implies that Problems 1–4 are undecidable.
- SREU with ground left sides is undecidable (Plaisted [11]).
- SREU with ground left sides and two variables is undecidable (Veanes [14]).
- SREU with one variable is DEXPTIME-complete (Degtyarev, Gurevich, Narendran, Veanes, and Voronkov [3]).

The last two results imply a complete classification of decidable prenex fragments of intuitionistic predicate calculus with equality: the $\exists\exists$ fragment is undecidable and the $\forall^*\exists\forall^*$ fragment is decidable. All the above mentioned undecidability results require that the signature contain a function symbol of arity ≥ 2.

When all function symbols have arity ≤ 1, Problems 1–4 are equivalent to *monadic SREU,* i.e. SREU in the signature where all function symbols have arity ≤ 1.

The decidability of monadic SREU is an open problem. The following facts are known about monadic SREU (Degtyarev, Matiyasevich and Voronkov [4]).

- The word equation problem is effectively reducible to monadic SREU.
- Monadic SREU with one function symbol is decidable (this fact has a non-elementary proof).
- Monadic SREU is decidable if and only if it is decidable in the signature with two function symbols.

This paper studies monadic SREU. Although the general case remains an open problem, we prove its equivalence to a combinatorial problem on words defined in Section 5. This problem is defined in terms of *ideals* on the set of pairs of words and called *the ideal membership problem.* We prove

Theorem 4 Monadic SREU is decidable if and only if the ideal membership problem is decidable.

We also prove the decidability of some special cases of monadic SREU. In Section 4 we prove a result similar to the result of [3]:

Theorem 3 Monadic SREU with one variable is PSPACE-complete.

As we already mentioned, Plaisted [11] proved that SREU with ground left sides is undecidable. The corresponding monadic case is shown to be decidable in Section 3:

Theorem 2 Monadic SREU with ground left sides is decidable.

The complexity of monadic SREU with ground left sides is not known. We prove

Theorem 1 Monadic SREU with one variable and ground left sides is PSPACE-hard.

Section 2

Preliminaries

In this section we introduce basic definitions concerning terms, equations, words, word equations, automata and rewrite rules. We have to define so many concepts since it is unreasonable to expect of a reader to know everything. We also assert some statements proved elsewhere and prove some properties of the introduced notions which will be used in subsequent sections.

The symbol $\rightleftharpoons$ means "equal by definition".

2.1 Terms and equations

The set of all variables of a term t is denoted $var(t)$. A term is *ground* iff it has no variables, i.e. $var(t) = \emptyset$. The symbol $\vdash$ denotes provability in first-order logic. When we write $\varphi_1, \ldots, \varphi_n \vdash \varphi$, where $\varphi_1, \ldots, \varphi_n, \varphi$ are formulas, it means provability of the formula $\varphi_1 \wedge \ldots \wedge \varphi_n \supset \varphi$. *Substitutions* of terms $t_1, \ldots, t_n$ for variables $x_1, \ldots, x_n$ are denoted $\{t_1/x_1, \ldots, t_n/x_n\}$. The *application of such a substitution θ to a term t,* is the operation of simultaneous replacement of all occurrences of x_i by t_i. The result of the application is the term denoted $t\theta$. We shall also apply substitutions to equations and sets of equations and use the same notation for the result of the application.

The *domain* and the *range* of a substitution θ, denoted by $dom(\theta)$ and $ran(\theta)$, respectively, are defined as

$$
\begin{aligned}
dom(\theta) &\rightleftharpoons \{x \mid x \text{ is a variable and } x\theta \neq x\} \\
ran(\theta) &\rightleftharpoons \{x\theta \mid x \in dom(\theta)\}
\end{aligned}
$$

For any expression E (for example, term, or a set of equations), we denote by E_c^t the expressions obtained from E by the replacement of all occurrences of the constant c by a term t. We write $s[t]$ to denote a particular occurrence of a subterm t of a term s.

In this paper, we shall only consider *monadic signatures* consisting of a finite set $\mathcal{F}$ of unary function symbols and a finite set $\mathcal{C}$ of constants. Such signatures are denoted $(\mathcal{F}, \mathcal{C})$. The set of ground terms of a signature $(\mathcal{F}, \mathcal{C})$ is denoted by $T_{(\mathcal{F},\mathcal{C})}$. We always assume $\mathcal{C} \neq \emptyset$ and hence $T_{(\mathcal{F},\mathcal{C})} \neq \emptyset$. For any set of equations $\mathcal{E}$ we denote by $T(\mathcal{E})$ the set of all terms occurring in $\mathcal{E}$ and their subterms. For example, if $\mathcal{E} = \{f(x) \simeq g(c), c \simeq g(f(x))\}$, then $T(\mathcal{E}) = \{x, f(x), c, g(c), g(f(x))\}$.

We shall denote variables by x, y, z, constants by a, b, c, d, function symbols by f, g, h, terms by r, s, t and substitutions by θ.

We shall use the following statement

Lemma 2.1 (Derivability of equations is in PTIME)
There is a polynomial-time algorithm checking, by a given finite set of equations $\mathcal{E}$ and terms s, t,

whether $\mathcal{E} \vdash s \simeq t$.

Proof. See [8] or [13]. (In fact, this problem is P-complete.) □

We write $\mathcal{E}' \vdash \mathcal{E}$ iff for any equation $(s \simeq t) \in \mathcal{E}$ we have $\mathcal{E}' \vdash s \simeq t$. We call two sets of equations $\mathcal{E}$ and $\mathcal{E}'$ *equivalent,* denoted $\mathcal{E} \equiv \mathcal{E}'$, iff $\mathcal{E} \vdash \mathcal{E}'$ and $\mathcal{E}' \vdash \mathcal{E}$.

In the sequel we shall use the following two lemmas.

Lemma 2.2 (Lemma on constants)
Let $\mathcal{E}$ and $\mathcal{E}'$ be sets of equations. For any constant c and term t, if $\mathcal{E} \vdash \mathcal{E}'$, then $\mathcal{E}^t_c \vdash \mathcal{E}'^t_c$.

Proof. Standard. □

Lemma 2.3 Let $\mathcal{E}$ be a set of ground equations, E be a ground equation, c be a constant and t be a ground term in which c does not occur. Then $\mathcal{E} \cup \{c \simeq t\} \vdash E$ if and only if $\mathcal{E}^t_c \vdash E^t_c$.

Proof. Immediate by Lemma 2.2. □

2.2 Words and finite automata

This section defines *words* and *finite automata.* We shall also introduce a notation for monadic terms which allows us to easily come from terms to words and back.

Let $\mathcal{F}$ be a finite non-empty set, called the *alphabet.* Its elements are called *letters. Words* are finite sequences of letters. We denote words by a juxtaposition of its letters, as

$$W = a_1 a_2 \dots a_n.$$

The natural number n is called the *length* of the word W and denoted $|W|$. We denote by ε the *empty word,* which is the unique word of length zero. The set of all words with letters in $\mathcal{F}$ is denoted by $\mathcal{F}^*$.

It will be convenient for us to use the alphabet $\mathcal{F}$ also as the set of unary function symbols of a monadic signature $(\mathcal{F}, \mathcal{C})$. Every term s in such a signature has the form $f_1(f_2(\dots f_n(t)\dots))$ where $n \geq 0$, $f_1, \dots, f_n$ are unary function symbols and t is a constant or a variable. We shall denote such a term s in the reversed Polish notation, i.e. as $tf_n \dots f_2 f_1$. Thus, every term can be represented in the form tW, where t is a constant or a variable and W is a word. Similarly, any term of the form $f_1(f_2(\dots f_n(t)\dots))$, where t is an arbitrary term, will be written as $tf_n \dots f_2 f_1$.

A *finite automaton* $\mathcal{A}$ on the alphabet $\mathcal{F}$ is a quadruple (Q, I, T, E), where Q is a finite set, called *the set of states, I* and T are distinguished subsets of Q, called the sets of *initial* and *terminal* states, respectively. The set $E \subseteq Q \times \mathcal{F} \times Q$ is *the set of edges of* $\mathcal{A}$. An edge (p, f, q) is also denoted $p \xrightarrow{f} q$. The automaton is *deterministic* iff whenever $(p, f, q_1) \in E$ and $(p, f, q_2) \in E$, then $q_1 = q_2$.

A word $f_1 \dots f_n$ is *recognized by an automaton* (Q, I, T, E) iff there is a sequence of states $q_0 \dots q_n$ such that $q_0 \in I$, $q_n \in T$ and $q_{i-1} \xrightarrow{f_i} q_i$ for all $i \in \{1, \dots, n\}$. A set of words is *regular* iff it is the set of words recognized by some automaton.

The *DFA intersection nonemptiness problem* is the following decision problem. Given any finite set $\{\mathcal{A}_1, \dots, \mathcal{A}_n\}$ of deterministic finite automata, is there a word recognized by each automaton in this set. The following statement is proved in [8]:

Lemma 2.4 (DFA intersection nonemptiness problem)
The DFA intersection nonemptiness problem is PSPACE-complete.

2.3 Word equations

In addition to the alphabet $\mathcal{F}$, we shall also consider a countable set $\mathcal{V}$ of *word variables,* denoted u, v, w. A *word equation* is any expression of the form $V \simeq W$, where $V, W \in (\mathcal{F} \cup \mathcal{V})^*$. A *word substitution* is any expression $\sigma = \{V_1/v_1, \ldots, V_n/v_n\}$, where v_i are word variables and V_i are words in $\mathcal{F}^*$. Its *domain,* denoted $dom(\sigma)$ is the set $\{v_1, \ldots, v_n\}$. The *application of such a word substitution σ to a word $W \in (\mathcal{F} \cup \mathcal{V})^*$,* is the operation of simultaneous replacement of all occurrences of v_i by V_i. The result of the application is the word denoted $W\sigma$. A word substitution σ is a *solution to a word equation $U \simeq V$* iff all variables in U, V belong to $dom(\sigma)$ and we have $U\sigma = V\sigma$. A *system of word equations* is any finite set of word equations, its *solution* is any substitution solving all equations in the system. Words will be denoted by U, V, W and word substitutions by σ. We say that a word substitution σ' *extends* a word substitution σ if (i) $dom(\sigma) \subseteq dom(\sigma')$, and (ii) for every $v \in dom(\sigma)$ we have $v\sigma = v\sigma'$.

Makanin [9] proved that word equations are decidable. Analyzing Makanin's algorithm, Schultz [12] proves the following result.

Lemma 2.5 (Decidability of word equations with regular constraints)
The problem of solvability of word equations where every word variable u_i ranges over a regular set S_i, is decidable.

It is known that the problem of solvability of word equations is NP-hard. No good upper bound for the complexity of this problem has been obtained so far, it is only known that the problem is in 3-NEXP (Kościelski and Pacholski[6, 7]).

2.4 Equational logic and rigid equations

Let $\mathcal{R}$ be a system of rigid equations. The *signature of* $\mathcal{R}$ is defined as the signature consisting of all constants and function symbols occurring in $\mathcal{R}$; and in addition a fixed constant if $\mathcal{R}$ contains no constants. A solution θ to $\mathcal{R}$ is called *grounding for* $\mathcal{R}$ iff for every variable x occurring in $\mathcal{R}$ the term $x\theta$ is ground. A substitution θ is called *relevant* for $\mathcal{R}$ iff all terms in $ran(\theta)$ are terms in the signature of $\mathcal{R}$.

In the sequel, we shall need the following technical property of systems of rigid equations. We omit the straightforward proof.

Lemma 2.6 (Existence of relevant grounding solutions)
Let $\mathcal{R}$ be a solvable system of rigid equations. Then there exists a solution θ to $\mathcal{R}$ that is grounding and relevant for $\mathcal{R}$.

We shall introduce one particular kind of rigid equations that will be used as a technical tool for proofs in this paper. For any monadic signature $(\mathcal{F}, \mathcal{C})$, any variable x and any constant $c \in C$ introduce the following rigid equation:

$$Gr_{(\mathcal{F},\mathcal{C})}(x) \rightleftharpoons \{d \simeq c \mid d \in \mathcal{C}\} \cup \{cf \simeq c \mid f \in \mathcal{F}\} \vdash_\forall x \simeq c$$

We shall use the following obvious lemma:

Lemma 2.7 A substitution θ is a solution to $Gr_{(\mathcal{F},\mathcal{C})}(x)$ iff $x\theta \in T_{(\mathcal{F},\mathcal{C})}$.

As a consequence, we have

Lemma 2.8 For any system $\mathcal{R}$ of rigid equations there is a system $\mathcal{R}'$ of rigid equations such that for any substitution θ, θ is a solution to $\mathcal{R}'$ if and only if θ is a grounding relevant solution to $\mathcal{R}$. In addition, (i) $\mathcal{R}'$ can be found by $\mathcal{R}$ using a polynomial-time algorithm; and (ii) $\mathcal{R}'$ has ground left sides if $\mathcal{R}$ has ground left sides.

Proof. Let $x_1, \ldots, x_n$ be all variables in $\mathcal{R}$ and $(\mathcal{F}, \mathcal{C})$ be the signature of $\mathcal{R}$. Define $\mathcal{R}' \rightleftharpoons \mathcal{R} \cup \{Gr_{(\mathcal{F},\mathcal{C})}(x_i) \mid i \in \{1, \ldots, n\}\}$. Then apply Lemma 2.7. □

2.5 Rewrite rules

This section introduces a technique standard in the theory of ground systems of rewrite rules. However, we shall use ordinary equations instead of rewrite rules.

Introduce an ordering $\succ$ on terms in $T_{(\mathcal{F},\mathcal{C})}$ in the following way. Let $>$ be any total ordering on $\mathcal{F} \cup \mathcal{C}$ and $s = cf_1 \ldots f_m$, $t = dg_1 \ldots g_n$. Then $s \succ t$ iff one of the following conditions is true:

1. $m > n$;
2. $m = n$ and the string $cf_1 \ldots f_m$ is greater than $dg_1 \ldots g_n$ in the lexicographic ordering induced by $>$.

The ordering $\succ$ is total, well-founded and can be extended to a simplification ordering [1]. Some properties of the ordering formulated below are simple consequence of standard statements in the theory of rewrite systems. Their proofs may be found in e.g. [1]. Note that the ordering $\succ$ depends on the ordering $>$. In the definitions below we assume that we have chosen a fixed ordering $>$ on $\mathcal{F} \cup \mathcal{C}$, and hence $\succ$ is also fixed.

Let $\mathcal{E}, \mathcal{E}'$ be finite sets of ground equations and $\mathcal{E}$ contains distinct equations $s \simeq t$ and $r[s] \simeq u$. We say that $\mathcal{E}'$ *is obtained from* $\mathcal{E}$ *by simplification from* $s \simeq t$ *into* $r[s] \simeq u$, denoted $\mathcal{E} \to \mathcal{E}'$ iff

$$\mathcal{E}' = (\mathcal{E} \setminus \{r[s] \simeq u\}) \cup \{r[t] \simeq u\}$$

The reflexive and transitive closure of the relation $\to$ on sets of ground equations is denoted by $\to^*$. A set of equations $\mathcal{E}$ is called *irreducible* iff there exists no $\mathcal{E}'$ such that $\mathcal{E} \to \mathcal{E}'$. We shall use the following statements which are easy to prove.

Lemma 2.9 Let $\mathcal{E}$ be a finite set of equations. Then there exists an irreducible set of equations $\mathcal{E}'$ such that $\mathcal{E} \to^* \mathcal{E}'$.

Lemma 2.10 Let $\mathcal{E} \to^* \mathcal{E}'$. Then $\mathcal{E} \equiv \mathcal{E}'$.

Let $\mathcal{E}$ be an irreducible set of ground equations. We write $t \to_{\mathcal{E}} t'$ if there exists an equation $(r \simeq s) \in \mathcal{E}$ such that $r \succ s$, and t' is obtained from t by the replacement of one occurrence of the subterm r by s. The relation $\to_{\mathcal{E}}^*$ is the reflexive and transitive closure of $\to_{\mathcal{E}}$. A term t is called *irreducible with respect to* $\mathcal{E}$ iff there is no term s such that $t \to_{\mathcal{E}} s$. *The normal form of a term* t *w.r.t.* $\mathcal{E}$, denoted $t\downarrow_{\mathcal{E}}$, is the term s such that $t \to_{\mathcal{E}}^* s$ and s is irreducible w.r.t. $\mathcal{E}$. The normal form of any term exists and is unique. We shall use the following statements which are easy to prove.

Lemma 2.11 Let $\mathcal{E}$ be an irreducible set of ground equations and s, t be terms. Then $\mathcal{E} \vdash s \simeq t$ if and only if $s\downarrow_{\mathcal{E}} = t\downarrow_{\mathcal{E}}$.

Lemma 2.12 Let $\mathcal{E}$ be an irreducible set of ground equations and $s \downarrow_{\mathcal{E}}= t$. Then for any subterm t' of t there is a term $r \in T(\mathcal{E} \cup \{s \simeq s\})$ such that $\mathcal{E} \vdash t' \simeq r$.

Lemma 2.13 Let $\mathcal{E} \to^* \mathcal{E}'$. Then for any term $t' \in T(\mathcal{E}')$ there is a term $t \in T(\mathcal{E})$ such that $\mathcal{E} \vdash t' \simeq t$.

2.6 Mixing words and rigid equations

We call a *word term,* or simply *w-term,* in the signature $(\mathcal{F}, \mathcal{C})$ any expression of the form cW such that $c \in \mathcal{C}$ and $W \in (\mathcal{F} \cup \mathcal{V})^*$. A *w-equation* is any expression $cV \simeq dW$, where cV and dW are w-terms. A *rigid w-equation* is any expression of the form $\mathcal{W} \vdash_\forall cV \simeq dW$, where $\mathcal{W}$ is a finite set of w-equations, cV and dW are w-terms. A *system of rigid w-equations* is any finite set of rigid w-equations. *The signature of a system of rigid w-equations* is defined similar to that of a system of rigid equations. Sets of w-equations will be denoted by $\mathcal{W}$, and sets of rigid w-equations by $\mathcal{S}$.

A *solution to a rigid w-equation* $\mathcal{W} \vdash_\forall cV \simeq dW$ is any word substitution σ whose domain contains all word variables in $\mathcal{W}, V, W$ such that $\mathcal{W}\sigma \vdash cV\sigma \simeq dW\sigma$. A *solution to a system $\mathcal{S}$ of rigid w-equations* is any word substitution that is a solution to every rigid w-equation in $\mathcal{S}$.

Note that a ground w-equation is also an ordinary equation.

Grounding word substitutions and *relevant solutions to systems of rigid w-equations* are defined similar to those of systems of rigid equations. Similar to Lemma 2.6, we have the following property:

Lemma 2.14 Let $\mathcal{S}$ be a solvable system of rigid w-equations. Then there is a solution σ to $\mathcal{S}$ that is relevant for $\mathcal{S}$.

In Lemma 2.16 below we show that one can consider systems of rigid w-equations instead of systems of rigid equations. First, we shall prove a technical lemma.

Lemma 2.15 There is a polynomial-time algorithm which, given any system $\mathcal{S}$ of rigid w-equations, gives an equi-solvable system $\mathcal{S}'$ of rigid w-equations such that for every rigid w-equation $S \in \mathcal{S}'$ we have

1. each word variable has at most one occurrence in S;
2. one of the following conditions hold:
   (a) S has the form $\vdash_\forall cu \simeq cvw$, where u, v, w are pairwise distinct word variables; or
   (b) for every w-term cW occurring in S, we have $|W| \leq 1$.

Proof. First, we show how to transform $\mathcal{S}$ to make every word variable have at most one occurrence in any rigid w-equation in $\mathcal{S}$. Let a word variable u has more then one occurrence in a rigid w-equation $S \in \mathcal{S}$. Replace one occurrence of u by a fresh word variable v and add to $\mathcal{S}$ the rigid w-equation $\vdash_\forall cu \simeq cv$. Evidently, the resulting system and $\mathcal{S}$ are equi-solvable.

Then we show how to reduce the length of words occurring in $\mathcal{S}$ by adding to $\mathcal{S}$ rigid w-equations $\vdash_\forall cu \simeq cvw$. Let cVW be any word occurring in $\mathcal{S}$. Introduce three fresh word variables u, v, w and do the following. Replace this occurrence of cVW by cu and add to $\mathcal{S}$ rigid w-equations $\vdash_\forall cv \simeq cV$, $\vdash_\forall cw \simeq cW$ and $\vdash_\forall cu \simeq cvw$. Evidently, the resulting system and $\mathcal{S}$ are equi-solvable.

It is easy to prove that after several such transformations of $\mathcal{S}$ we obtain, in polynomial time, a system $\mathcal{S}'$ satisfying the conditions. $\square$

Lemma 2.16 The problem of solvability of systems of rigid w-equations is polynomial-time reducible to monadic SREU. There is a nondeterministic polynomial time algorithm reducing monadic SREU to the problem of solvability of systems of rigid w-equations.

Proof.

1. Let $\mathcal{S}$ be a system of rigid w-equations and $(\mathcal{F},\mathcal{C})$ be its signature. By Lemma 2.15 we can assume that all rigid w-equations in $\mathcal{S}$ satisfy the conditions of that lemma. For every variable v occurring in $\mathcal{S}$, introduce a fresh constant c_v. Define a system of rigid equations $\mathcal{R}$ in the following way. First, we make a system of rigid equations $\mathcal{R}'$ out of $\mathcal{S}$ by the following transformations applied to every rigid w-equation S in $\mathcal{S}$.

   (a) *S has the form $\vdash_\forall cu \simeq cvw$, where u, v, w are pairwise distinct word variables.* Then replace S by the rigid equation $c_u \simeq c_v, c_w \simeq v \vdash_\forall w \simeq u$.

   (b) *For every w-term cW occurring in S, we have $|W| \leq 1$.* For every w-term of the form cu occurring in S, replace it by u. Let the resulting system of rigid equations have the form $\mathcal{E} \vdash_\forall E$. Then add to $\mathcal{E}$ equations $c \simeq c_u$ for every w-term cu occurring in S.

   Finally, add to $\mathcal{R}'$ rigid equations $Gr_{(\mathcal{F},\{c_u\})}(u)$ for every word variable u occurring in $\mathcal{S}$. We prove that the resulting system of rigid equations $\mathcal{R}$ and the system $\mathcal{S}$ are equi-solvable.

   First, note that because of rigid equations $Gr_{(\mathcal{F},\{c_u\})}(u)$, every solution to $\mathcal{R}$ has the form $\{c_u W_u/u, \ldots, c_v W_v/v\}$, where $u, \ldots, v$ are all variables occurring in $\mathcal{S}$ and $W_u, \ldots, W_v \in \mathcal{F}^*$.

   By Lemmas 2.6 and 2.14, we can restrict ourselves to relevant solutions. Now we shall prove that for any word substitution $\sigma = \{W_u/u, \ldots, W_v/v\}$ grounding and relevant for $\mathcal{S}$, σ is solution to $\mathcal{S}$ if and only if the substitution $\theta = \{c_u W_u/u, \ldots, c_v W_v/v\}$ is a solution to $\mathcal{R}$.

   (a) First, consider rigid w-equations $s \in \mathcal{S}$ of the form $\vdash_\forall cu \simeq cvw$. In this case $\mathcal{R}$ contains the equation $r = (c_u \simeq c_v, c_w \simeq v \vdash_\forall w \simeq u)$. Obviously, σ is a solution to s if and only if $W_u = W_v W_w$.

   Consider now when θ is a solution to $c_u \simeq c_v, c_w \simeq v \vdash_\forall w \simeq u$. It is a solution if and only if $c_u \simeq c_v, c_w \simeq c_v W_v \vdash c_w W_w \simeq c_u W_u$. Applying Lemma 2.3 twice, we can show that this is equivalent to $\vdash c_v W_v W_w \simeq c_v W_u$, i.e. to $W_v W_w = W_u$.

   (b) Consider now the case of rigid w-equations $S \in \mathcal{S}$ such that for every w-term cW occurring in S, we have $|W| \leq 1$. We demonstrate this case on an example. For example, let S have the form $au \simeq cv, a \simeq aw \vdash_\forall az \simeq cf$. Then $\mathcal{R}$ contains the rigid equation $R = (a \simeq c_u, c \simeq c_v, a \simeq c_w, a \simeq c_z, u \simeq v, a \simeq w \vdash_\forall z \simeq cf)$. The word substitution σ is a solution to S if and only if

   $$aW_u \simeq cW_v, a \simeq aW_w \vdash aW_z \simeq cf$$

   The substitution θ is a solution to R if and only if

   $$a \simeq c_u, c \simeq c_v, a \simeq c_w, a \simeq c_z, c_u W_u \simeq c_v W_v, a \simeq c_w W_w \vdash c_z W_z \simeq cf$$

   Applying Lemma 2.3, we see that these conditions are equivalent (the key point in applying this lemma is that every word variable occurs in $\mathcal{S}$ at most once).

   The rest of the proof of the first part of the claim is obvious.

2. Let $\mathcal{R}$ be a system of rigid equations and $(\mathcal{F}, \mathcal{C})$ be its signature. Let X be the set of all variables of $\mathcal{R}$. For any mapping $\tau : X \to \mathcal{C}$, define the system $\mathcal{S}_\tau$ of rigid w-equations in the following way: $\mathcal{S}_\tau$ is obtained from $\mathcal{R}$ by replacing each occurrence of any variable x by the w-term $\tau(x)x$. Applying Lemmas 2.6 and 2.14 of the existence of relevant and grounding solutions, we can show that $\mathcal{R}$ is solvable if and only if one of $\mathcal{S}_\tau$ is solvable.

The corresponding nondeterministic polynomial time algorithm nondeterministically guesses τ and then constructs $\mathcal{S}_\tau$. $\square$

Section 3

Ground left sides

In this section we prove that monadic SREU with ground left sides is decidable and PSPACE-hard.

3.1 SREU with ground left sides is PSPACE-hard

Lemma 3.1 Let $\mathcal{A} = (Q, I, T, E)$ be a deterministic finite automaton over $\mathcal{F}$. There exists a system $\mathcal{R}$ of two monadic rigid equations of one variable x with the following properties:

1. $\mathcal{R}$ has ground left sides;
2. for every solution θ to $\mathcal{R}$ we have $x\theta = cW$, where $W \in \mathcal{F}^*$ and c is a fixed constant;
3. for any word $W \in \mathcal{F}$, the substitution $\{cW/x\}$ is a solution to $\mathcal{R}$ if and only if W is recognized by $\mathcal{A}$.

In addition, $\mathcal{R}$ can be effectively constructed from $\mathcal{A}$ using a polynomial-time algorithm.

Proof. Without loss of generality we can assume that I consists of one state (see e.g. [10]). By renaming states, we can assume that $I = \{c\}$. Let F be a unary function symbol fresh for $\mathcal{F}$ and d be a constant fresh for Q. Define $\mathcal{R}$ as $\{R_1, R_2\}$, where

$$\begin{array}{l} R_1 = \{pf \simeq q \mid (p \xrightarrow{f} q) \in E\} \cup \{rF \simeq d \mid r \in T\} \vdash_\forall xF \simeq d \\ R_2 = Gr_{(\mathcal{F},\{c\})}(x) \end{array}$$

Consider any substitution $\theta = \{t/x\}$. By Lemma 2.7, θ is a solution to R_2 if and only if t has the form cW such that $W \in \mathcal{F}^*$. Consider when such substitution $\{cW/x\}$ is also a solution to R_1. By definition, this means

$$\{pf \simeq q \mid (p \xrightarrow{f} q) \in E\} \cup \{rF \simeq d \mid r \in T\} \vdash cWF \simeq d \tag{3.1}$$

Since the automaton is deterministic, the left side of (3.1) is irreducible. Using Lemma 2.11, one can see that (3.1) holds if and only if W is recognizable by $\mathcal{A}$. Evidently, $\mathcal{R}$ is constructed by $\mathcal{A}$ in polynomial time. □

Lemma 3.2 The DFA intersection nonemptiness problem is polynomial-time reducible to monadic SREU with one variable and ground left sides.

Proof. Let $\mathcal{A}_1, \ldots, \mathcal{A}_n$ be deterministic automata. Let $\mathcal{R}_i$, where $i \in \{1, \ldots, n\}$ be the system of rigid equations constructed from $\mathcal{A}_i$ as in Lemma 3.1. Define $\mathcal{R} = \bigcup_{i=1}^{n} \mathcal{R}_i$. By Lemma 3.1, every solution to $\mathcal{R}$ has the form $\{cW/x\}$ and any substitution $\{cW/x\}$ is a solution to $\mathcal{R}$ if and only if W is recognized by each $\mathcal{A}_i$. Hence, $\mathcal{R}$ is solvable if and only if there is a word recognizable by all $\mathcal{A}_i$. Evidently, $\mathcal{R}$ is constructed by $\mathcal{A}_1, \ldots, \mathcal{A}_n$ in polynomial time. □

Combining Lemmas 2.4 and 3.2 we obtain

Theorem 1 Monadic SREU with one variable and ground left sides is PSPACE-hard.

3.2 Monadic SREU with ground left sides is decidable

A finite set $\mathcal{E}$ of equations is *in automaton form* iff

1. every equation in $\mathcal{E}$ has the form $cf \simeq d$;
2. for every two w-equations $cf \simeq d_1$ and $cf \simeq d_2$ in $\mathcal{E}$ we have $d_1 = d_2$;

Note that any set of equations in automaton form is irreducible.

Lemma 3.3 Given any rigid w-equation S with a ground left side, one can effectively find in polynomial time a rigid w-equation S' with a ground left side such that

1. S and S' have the same solutions;
2. the left side of S' is in automaton form;
3. the right side of S' does not contain subterms of the form cf.

Proof. We define a series of equivalence-preserving transformations of the current w-equation S which produces a w-equation whose left side is in the automaton form. For the reader's convenience, we illustrate the process on the example where the initial S is $ahh \simeq a, ag \simeq b \vdash_\forall bxg \simeq bhyg$.

Let T be the set of all ground terms occurring in S and their subterms. In our example $T = \{ahh, ah, a, ag, b, bh\}$. Introduce a set of new constants $C_T = \{c_t \mid t \in T\}$.

1. Replace each constant d occurring in S by c_d. In our example S becomes

$$c_a hh \simeq c_a, c_a g \simeq c_b \vdash_\forall c_b xg \simeq c_b hyg$$

   Obviously, this transformation does not change the set of solutions.

2. Add to the left side of S the set of equations $\{c_t f \simeq c_{tf} \mid tf \in T\}$. In our example, S becomes

$$c_{ah} h \simeq c_{ahh}, c_a h \simeq c_{ah}, c_a g \simeq c_{ag}, c_b h \simeq c_{bh}, c_a hh \simeq c_a, c_a g \simeq c_b \vdash_\forall c_b xg \simeq c_b hyg$$

   Applying Lemma 2.3, one can show that the set of solutions to S does not change.

3. Get rid of all ground non-constant terms in the right side by repeatedly replacing terms of the form $c_t f$ by c_{tf}. In our example, S becomes

$$c_{ah}h \simeq c_{ahh}, c_a h \simeq c_{ah}, c_a g \simeq c_{ag}, c_b h \simeq c_{bh}, c_a hh \simeq c_a, c_a g \simeq c_b \vdash_\forall c_b xg \simeq c_{bh} yg$$

   Obviously, the set of solutions does not change since the left side contains the equations of the form $c_t f \simeq c_{tf}$.

4. Let $\mathcal{E}$ be the left side of S. Replace $\mathcal{E}$ by an irreducible set $\mathcal{E}'$ such that $\mathcal{E} \to^* \mathcal{E}'$. In our example, S becomes

$$c_{ah}h \simeq c_{ahh}, c_a h \simeq c_{ah}, c_a g \simeq c_{ag}, c_b h \simeq c_{bh}, c_{ahh} \simeq c_a, c_{ag} \simeq c_b \vdash_\forall c_b xg \simeq c_{bh} yg$$

   It is easy to prove that the left side of $\mathcal{E}'$ consists of equations of the form $cf \simeq d$ or $c \simeq d$. By Lemma 2.10, $\mathcal{E} \equiv \mathcal{E}'$. Hence, the set of solutions does not change.

5. Get rid of all equations of the form $c \simeq d$ in the left side of S by removing them and replacing c by d in S. In our example, S becomes

$$c_{ah}h \simeq c_a, c_a h \simeq c_{ah}, c_a g \simeq c_b, c_b h \simeq c_{bh}, \vdash_\forall c_b xg \simeq c_{bh} yg$$

   By Lemma 2.2, the set of solutions does not change. Since the left side of S is irreducible, it is in automaton form.

Evidently, S' is constructed by S in polynomial time. □

Let $\mathcal{E}$ be a set of equations in automaton form and c, d be any constants. Denote by $\mathcal{A}(\mathcal{E}, c, d)$ the following automaton (Q, I, T, E). Its alphabet is the set of function symbols occurring in $\mathcal{E}$. The set of states Q is the set of all constants occurring in $\mathcal{E}, c, d$. The sets of initial states and terminal states are defined by $I \rightleftharpoons \{c\}$ and $T \rightleftharpoons \{d\}$. Finally, the set of edges is defined by

$$E \rightleftharpoons \{a \xrightarrow{f} b \mid (af \simeq b) \in \mathcal{E}\}.$$

Lemma 3.4 A word W is recognized by $\mathcal{A}(\mathcal{E}, c, d)$ if and only if $\mathcal{E} \vdash cW \simeq d$.

Proof. Immediate by Lemma 2.11. □

Lemma 3.5 Let $\mathcal{E}$ be a set of equations in automaton form, $W, W' \in \mathcal{F}^*$ and c, c' be constants. Then $\mathcal{E} \vdash cW \simeq c'W'$ if and only if there is a constant d and words U, U', V such that $W = UV$, $W' = U'V$, U is recognized by $\mathcal{A}(\mathcal{E}, c, d)$ and U' is recognized by $\mathcal{A}(\mathcal{E}, c', d)$.

Proof.

($\Rightarrow$) We have $\mathcal{E} \vdash cW \simeq c'W'$. By Lemma 2.11 we have $cW\downarrow_\mathcal{E} = c'W'\downarrow_\mathcal{E}$. Choose d and V such that $cW\downarrow_\mathcal{E} = dV$. Define U and U' such that $W = UV$ and $W' = U'V$. We have $\mathcal{E} \vdash cU \simeq d$ and $\mathcal{E} \vdash c'U' \simeq d$. By Lemma 3.4 words U and U' are recognized by $\mathcal{A}(\mathcal{E}, c, d)$ and $\mathcal{A}(\mathcal{E}, c', d)$, respectively.

($\Leftarrow$) We have $W = UV$, $W' = U'V$, U is recognized by $\mathcal{A}(\mathcal{E}, c, d)$ and U' is recognized by $\mathcal{A}(\mathcal{E}, c', d)$. By Lemma 3.4 we have $\mathcal{E} \vdash cU \simeq d$ and $\mathcal{E} \vdash c'U' \simeq d$. Hence, $\mathcal{E} \vdash cUV \simeq dV$ and $\mathcal{E} \vdash c'U'V \simeq dV$. Then $\mathcal{E} \vdash cUV \simeq c'U'V$, i.e. $\mathcal{E} \vdash cW \simeq c'W'$. □

Let $R_0, R_1, \ldots$ be an enumeration of all regular sets of words on $\mathcal{F}$. We call a *regular constraint* any expression $R_i(U)$ where U is a word on $\mathcal{F} \cup \mathcal{V}$. A solution to such regular constraint is any word substitution σ such that $U\sigma \in R_i$.

Lemma 3.6 The problem of solvability of systems of rigid w-equations with ground left sides effectively reduces to word equations with regular constraints.

Proof. Let $\mathcal{S} = \{S_1, \ldots, S_n\}$ be such a system of rigid w-equations. By Lemma 3.3 we can assume that the left sides of all S_i are in automaton form. Let $S_i = (\mathcal{E}_i \vdash_\forall c_i W_i \simeq c_i' W_i')$, for all $i \in \{1, \ldots, n\}$. Let $u_1, \ldots, u_n$, $v_1, \ldots, v_n$ and $u_1', \ldots, u_n'$ be word variables fresh for $\mathcal{S}$. By Lemma 3.5, the system $\mathcal{S}$ is solvable if and only if there are constants d_i occurring in S_i, for all $i \in \{1, \ldots, n\}$ such that the following system of word equations and regular constraints is solvable:

$$
\begin{array}{ll}
W_1 \simeq u_1 v_1 & u_1 \text{ is recognized by } \mathcal{A}(\mathcal{E}_1, c_1, d_1) \\
\ldots & \ldots \\
W_n \simeq u_n v_n & u_n \text{ is recognized by } \mathcal{A}(\mathcal{E}_n, c_n, d_n) \\
W_1' \simeq u_1' v_1 & u_1' \text{ is recognized by } \mathcal{A}(\mathcal{E}_1, c_1', d_1) \\
\ldots & \ldots \\
W_n' \simeq u_n' v_n & u_n' \text{ is recognized by } \mathcal{A}(\mathcal{E}_n, c_n', d_n)
\end{array}
$$

To conclude the proof we note that there is only a finite number of choices for d_i. □

Theorem 2 Monadic SREU with ground left sides is decidable.

Proof. By Lemma 2.16 monadic SREU with ground left sides is effectively reducible to the problem of solvability of systems of rigid w-equations. By Lemma 3.6 the latter problem is effectively reducible to word equations with regular constraints. Then apply Lemma 2.5. □

Section 4

One-variable case

In this section we consider rigid equations with one variable x. We shall write $\mathcal{E}(x)$ to denote all occurrences of a variable x in $\mathcal{E}$, and write $\mathcal{E}(t)$ to denote the set of equations obtained from $\mathcal{E}$ by replacement of all occurrences of x by t. We shall use similar notation for terms, for example $s(x)$. Using this notation, we can write any rigid equation of one variable x as $\mathcal{E}(x) \vdash_{\forall} s(x) \simeq t(x)$.

Lemma 4.1 Let $\mathcal{E}(x)$ be a finite set of equations of one variable x and $s(x), t(x)$ be terms of one variable x such that $\mathcal{E}(x) \not\vdash s(x) \simeq t(x)$. Let c be a constant fresh for $\mathcal{E}(x), s(x), t(x)$ and r be a ground term such that c does not occur in r. If $\mathcal{E}(r) \vdash s(r) \simeq t(r)$, then there exists a ground term $r' \in T(\mathcal{E}(c) \cup \{s(c) \simeq t(c)\})$ such that $\mathcal{E}(c) \vdash r \simeq r'$.

Proof. Suppose $\mathcal{E}(r) \vdash s(r) \simeq t(r)$. Hence, $r \simeq c, \mathcal{E}(r) \vdash s(r) \simeq t(r)$. This implies $r \simeq c, \mathcal{E}(c) \vdash s(c) \simeq t(c)$. Consider any ordering $\succ$ in which c is the least element. By Lemma 2.9 there exists an irreducible $\mathcal{E}'$ such that $\mathcal{E}(c) \rightarrow^* \mathcal{E}'$. Let s' and t' be the normal forms of $s(c)$ and $t(c)$, respectively, w.r.t. $\mathcal{E}'$. Let us prove that $s' \neq t'$. Suppose, by contradiction, $s' = t'$. By Lemma 2.11 we have $\mathcal{E}' \vdash s(c) \simeq t(c)$. By Lemma 2.10 we have $\mathcal{E}(c) \vdash s(c) \simeq t(c)$. By Lemma 2.2 we have $\mathcal{E}(x) \vdash s(x) \simeq t(x)$. Contradiction.

Evidently, we have $r \simeq c, \mathcal{E}' \vdash s' \simeq t'$. Consider two cases:

1. The set of equations $\{r \simeq c\} \cup \mathcal{E}'$ is reducible. Since $\mathcal{E}'$ is irreducible, we have $r \in T(\mathcal{E}')$. By Lemma 2.13, there is $r' \in T(\mathcal{E}(c))$ such that $\mathcal{E}(c) \vdash r \simeq r'$.

2. The set of equations $\{r \simeq c\} \cup \mathcal{E}'$ is irreducible. By Lemma 2.11, normal forms of s' and t' w.r.t. $\{r \simeq c\} \cup \mathcal{E}'$ coincide. Since $s' \neq t'$, one of the terms s', t', for example s', is different from its normal form w.r.t. $\{r \simeq c\} \cup \mathcal{E}'$. Since s' is irreducible w.r.t. $\mathcal{E}'$, the term r is a subterm of s'. By Lemma 2.12, there is a subterm r' of $s(c)$ such that $\mathcal{E}(c) \vdash r \simeq r'$. □

Lemma 4.2 Let $\mathcal{E}(x) \vdash_{\forall} s(x) \simeq t(x)$ be a rigid equation of one variable x, c be a constant fresh for this rigid equation, r be a ground term in which c does not occur and $\mathcal{E}(x) \not\vdash s(x) \simeq t(x)$. Then the substitution $\theta = \{r/x\}$ is a solution to this rigid equation if and only if there is a ground term $r' \in T(\mathcal{E}(c) \cup \{s(c) \simeq t(c)\})$ such that $\mathcal{E}(c), \mathcal{E}(r') \vdash s(r') \simeq t(r')$ and θ is a solution to $\mathcal{E}(c) \vdash_{\forall} r' \simeq x$.

Proof.

- $\Rightarrow$ We have that θ is a solution to $\mathcal{E}(x) \vdash_\forall s(x) \simeq t(x)$. Then $\mathcal{E}(r) \vdash s(r) \simeq t(r)$. By Lemma 4.1 there is a term $r' \in T(\mathcal{E}(c) \cup \{s(c) \simeq t(c)\})$ such that $\mathcal{E}(c) \vdash r \simeq r'$. Then $\mathcal{E}(r'), \mathcal{E}(c) \vdash s(r') \simeq t(r')$.

- $\Leftarrow$ We have $\mathcal{E}(c), \mathcal{E}(r') \vdash s(r') \simeq t(r')$ and $\mathcal{E}(c) \vdash_\forall r' \simeq r$. Then $\mathcal{E}(c), \mathcal{E}(r) \vdash s(r) \simeq t(r)$. By Lemma 2.2 we can substitute r for c obtaining $\mathcal{E}(r) \vdash s(r) \simeq t(r)$. □

Lemmas 4.1 and 4.2 also hold for non-monadic signatures [3].

Lemma 4.3 Monadic SREU with one variable is in PSPACE.

Proof. We shall give a non-deterministic algorithm reducing monadic SREU with one variable to the DFA intersection nonemptiness problem.

Let $\mathcal{R}$ be a system of rigid equations of one variable x whose signature is $(\mathcal{F}, \mathcal{C})$. It has the form

$$\begin{array}{l} \mathcal{E}_1 \vdash_\forall s_1(x) \simeq t_1(x) \\ \dots \\ \mathcal{E}_n \vdash_\forall s_n(x) \simeq t_n(x) \end{array}$$

By Lemma 2.6 we can restrict ourselves to relevant grounding solutions $\theta = \{r/x\}$ only. Let c be a variable fresh for $(\mathcal{F}, \mathcal{C})$. By Lemma 4.2 θ is a solution to $\mathcal{R}$ if and only if there are ground terms $r'_i \in T(\mathcal{E}_i(c) \cup \{s_i(c) \simeq t_i(c)\})$, where $i \in \{1, \dots, n\}$ such that $\mathcal{E}(c), \mathcal{E}(r') \vdash s(r') \simeq t(r')$ and θ is a solution to the system

$$\begin{array}{l} \mathcal{E}_1(c) \vdash_\forall r'_1 \simeq x \\ \dots \\ \mathcal{E}_n(c) \vdash_\forall r'_n \simeq x \end{array}$$

Nondeterministically select such $r'_1, \dots, r'_n$ and verify the condition $\mathcal{E}(c), \mathcal{E}(r') \vdash s(r') \simeq t(r')$ (it can be checked in polynomial time using Lemma 2.1).

Such θ is a solution to this system of rigid equations if and only if there is a constant $d \in \mathcal{C}$ such that the following system of rigid w-equations is solvable:

$$\begin{array}{l} \mathcal{E}_1(c) \vdash_\forall r'_1 \simeq dx \\ \dots \\ \mathcal{E}_n(c) \vdash_\forall r'_n \simeq dx \end{array}$$

Nondeterministically select such d. By Lemma 3.3 we can equivalently replace this system with a system

$$\begin{array}{l} \mathcal{E}'_1 \vdash_\forall c_1 \simeq d_1 x \\ \dots \\ \mathcal{E}'_n \vdash_\forall c_n \simeq d_n x \end{array}$$

where $\mathcal{E}'_i$ are in automaton form. By Lemma 3.4, this system is solvable if and only if the intersection of automata $\mathcal{A}(\mathcal{E}'_1, d_1, c_1), \dots, \mathcal{A}(\mathcal{E}'_n, d_n, c_n)$ is non-empty.

We have given a non-deterministic algorithm reducing monadic SREU with one variable to the DFA intersection nonemptiness problem. On each branch, the algorithm makes polynomially many steps. Applying Lemma 2.4 on the complexity of the DFA intersection nonemptiness problem we get that monadic SREU with one variable is in NPSPACE, and hence in PSPACE. □

Combining Theorem 1 and Lemma 4.3, we obtain

Theorem 3 Monadic SREU with one variable is PSPACE-complete.

Section 5

General case

We call a word substitution σ *grounding* for an expression E if for every word variable u occurring in E, the word $u\sigma$ is a word on $\mathcal{F}$.

Denote by $\mathbf{W}$ the set of pairs of words on $\mathcal{F}$. Introduce on $\mathbf{W}$ a binary function $*$, a unary function ^{r} and a binary relation $\leq$ in the following way:

$$(U_1, U_2) * (V_1, V_2) \quad \rightleftharpoons \quad \begin{cases} (U_1, V_2) & \text{if } U_2 = V_1 \\ (V_1, V_2) & \text{otherwise} \end{cases}$$

$$(U_1, U_2)^r \quad \rightleftharpoons \quad (U_2, U_1)$$

$$(U_1, U_2) \leq (V_1, V_2) \quad \rightleftharpoons \quad \text{there is a word } W \text{ such that } (V_1, V_2) = (U_1 W, U_2 W)$$

An *ideal* on $\mathbf{W}$ is any set of pairs containing $(\varepsilon, \varepsilon)$, closed under functions $*$ and ^{r} and upward closed under $\leq$. The *ideal generated by a set of pairs S*, denoted $ideal(S)$ is defined as the least ideal containing S.

An ideal membership equation is an expression

$$(U, V) \in ideal(\{(U_1, V_1), \dots, (U_n, V_n)\}),$$

where $n \geq 0$ and $U, V, U_1, \dots, U_n, V_1, \dots, V_n \in (\mathcal{F} \cup \mathcal{V})^*$. A *solution to such ideal membership equation* is any word substitution σ such that

1. σ is grounding for $U, V, U_1, \dots, U_n, V_1, \dots, V_n$;

2. the word $(U\sigma, V\sigma)$ belongs to the ideal generated by $\{(U_1\sigma, V_1\sigma), \dots, (U_n\sigma, V_n\sigma)\}$.

A *system of ideal membership equations* is any finite set of ideal membership equations. *A solution to a system of ideal membership equations* is any substitution that solves each equation in the system. The *ideal membership problem* is the decision problem of solvability of systems of ideal membership equations.

The aim of this section is to show that monadic SREU is equivalent to the ideal membership problem. First, we shall prove several lemmas illustrating the expressive power of ideal membership equations.

Lemma 5.1 Let U, V be words on $\mathcal{F}$. Then for any substitution σ, it is a solution to $U = V$ if and only if it is a solution to $(U, V) \in ideal(\emptyset)$.

Proof. Note that $ideal(\emptyset)$ is the set of all pairs (W, W). □

The following lemma means that ideal membership equations are at least as expressive as word equations.

Lemma 5.2 Let U, V be words on $\mathcal{F} \cup \mathcal{V}$. Then the word equation $U \simeq V$ has a solution if and only if the ideal membership equation $(U, V) \in ideal(\emptyset)$ has a solution.

Proof. Immediate from Lemma 5.1. □

Besides word equations, some other interesting relations on words are also expressible by ideal membership equations. For example, for any words U, V on $\mathcal{F}$ we have $(U, \varepsilon) \in ideal((V, \varepsilon))$ if and only if $U = V^n$ for some natural number n.

The following lemma is the main reason for introducing the notion of an ideal.

Lemma 5.3 Let $U_1, \ldots, U_n, V_1, \ldots, V_n, U, V$ be words on $\mathcal{F}$ and a be any constant. Then $aU_1 \simeq aV_1, \ldots, aU_n \simeq aV_n \vdash aU \simeq aV$ if and only if $(U, V) \in ideal(\{(U_1, V_1), \ldots, (U_n, V_n)\})$.

Proof. It is well-known that the set of all logical consequences of a set of ground equations $\{s_1 \simeq t_1, \ldots, s_n \simeq t_n\}$ can be characterized as the smallest set of equations $\mathcal{E}$ such that

1. $\mathcal{E}$ contains all equations of the form $t \simeq t$;
2. $\{s_1 \simeq t_1, \ldots, s_n \simeq t_n\} \subseteq \mathcal{E}$;
3. if $(s \simeq t) \in \mathcal{E}$, then $(t \simeq s) \in \mathcal{E}$;
4. if $(r \simeq s) \in \mathcal{E}$, and $(s \simeq t) \in \mathcal{E}$, then $(r \simeq t) \in \mathcal{E}$.
5. if $(s \simeq t) \in \mathcal{E}$ then $(r[s] \simeq r[t]) \in \mathcal{E}$.

When all terms s_i and t_i have the form aW, this characterization immediately implies the statement. □

Lemma 5.4 The ideal membership problem is effectively reducible to the problem of solvability of systems of rigid w-equations. More precisely, for any system $\mathcal{I}$ of ideal membership equations we can effectively find a system of rigid w-equations $\mathcal{S}$ such that for any substitution σ grounding for $\mathcal{I}, \mathcal{S}$, it is a solution to $\mathcal{I}$ if and only if it is a solution to $\mathcal{S}$.

Proof. Consider any ideal membership equation $(U, V) \in ideal(\{(U_1, V_1), \ldots, (U_n, V_n)\})$. By Lemma 5.3 it has the same solutions as the rigid w-equation $aU_1 \simeq aV_1, \ldots, aU_n \simeq aV_n \vdash_\forall aU \simeq aV$. □

5.1 Another ordering on terms

In Subsection 2.5 we introduced an ordering $\succ$ on $T_{(\mathcal{F},\mathcal{C})}$. Here we shall introduce another ordering on $T_{(\mathcal{F},\mathcal{C})}$, also denoted $\succ$. The ordering $\succ$ is induced by some total ordering $>$ on $\mathcal{F} \cup \mathcal{C}$. We assume that such an ordering is fixed for the rest of this section. Let $s = cg_1 \ldots g_n$ and $t = dh_1 \ldots h_m$. Then $s \succ t$ if and only if one of the following conditions holds

1. $c > d$; or
2. $c = d$ and $n > m$; or
3. $c = d$, $n = m$ and $g_1 \dots g_n$ is greater than $h_1 \dots h_m$ in the lexicographic ordering induced by $>$.

The ordering $\succ$ is also a reduction ordering. For this ordering $\succ$, we shall use the same definitions as we have used in Subsection 2.5, for example, the definition of an irreducible set of equations. Lemmas 2.9–2.13 hold for this ordering.

For the rest of this section we assume that $\mathcal{C} = \{c_1, \dots, c_k\}$ and the ordering $>$ is defined by $c_k > c_{k-1} > \dots > c_1$. Note that $c_j V \succ c_i W$, whenever $j > i$.

Using Lemmas 2.9–2.11, we shall give a constructive characterization of provability in equational logic which will later be used in the reduction of monadic SREU to the ideal membership problem.

Let $\mathcal{E}_i$ be systems of ground equations and s_i, t_i be ground terms, where $i \in \{1, \dots, n\}$. Evidently, the system of rigid equations $\mathcal{R} = \{\mathcal{E}_i \vdash_\forall s_i \simeq t_i \mid 1 \leq i \leq n\}$ has a solution if and only if $\mathcal{E}_i \vdash s_i \simeq t_i$, for every i.

We introduce four types of transformations on systems of rigid equations

$$\mathcal{R} = \{\mathcal{E}_i \vdash_\forall s_i \simeq t_i \mid 1 \leq i \leq n\}.$$

These transformations will be needed for reducing monadic SREU to the ideal membership problem in the following way. First, we shall show that the transformations are enough to reduce any solvable system of rigid equations to the empty system. Second, we shall bound the number of transformations needed. Third, we shall show that this transformations can be expressed by systems of ideal membership equations.

0 Suppose that $\mathcal{E}_i$ contains an equation $aV \simeq aW$ such that $aV \succ aW$ and the rigid equation $\mathcal{E}_i \vdash_\forall s_i \simeq t_i$ contains an equation $aVU \simeq r$. Then *the transformation of type 0* replaces this occurrence of $aVU \simeq r$ in $\mathcal{E}_i \vdash_\forall s_i \simeq t_i$ by $aWU \simeq r$.

1 A *transformation of type 1* is any finite sequence of transformations of type 0.

2 Suppose that $\mathcal{E}_i$ contains an equation $c_k V \simeq c_j W$ such that $k > j$ and the rigid equation $\mathcal{E}_i \vdash_\forall s_i \simeq t_i$ contains an equation $c_k VU \simeq r$. Then *the transformation of type 2* replaces this occurrence of $c_k VU \simeq r$ in $\mathcal{E}_i \vdash_\forall s_i \simeq t_i$ by $c_j WU \simeq r$.

3 Suppose that $s_i = t_i$. Then *the transformation of type 3* removes $\mathcal{E}_i \vdash_\forall s_i \simeq t_i$ from $\mathcal{R}$.

Lemma 5.5 Suppose that the ground system of rigid equations $\mathcal{R}$ has a solution. Then after a finite number of transformations of types 1–3 one can obtain from $\mathcal{R}$ the empty system.

Proof. Follows from Lemmas 2.9, 2.10 and 2.11 using the following considerations. First, a reduction of any system $\mathcal{E}$ to an irreducible system $\mathcal{E}'$ such that $\mathcal{E} \to^* \mathcal{E}'$ can be considered a sequence of transformations of types 1 and 2. Thus, we can assume that all $\mathcal{E}_i$ are irreducible. A reduction of terms s_i, t_i to their normal forms w.r.t. $\mathcal{E}_i$ can also be considered as a sequence of transformations of types 1 and 2. Finally, when the normal forms coincide, we can get rid of solved equations using transformations of type 3. $\square$

We would like to restrict the number of transformations to be done with a system. To this end, we introduce a notion of a rank.

We define *the rank of a system of rigid w-equations* $\mathcal{R}$ as a natural number calculated as follows. The rank of a rigid w-equation $c_iU \simeq c_jV$ is the number $i+j$. The rank of a system of w-equations $\mathcal{E}$ is the sum of ranks of w-equations in $\mathcal{E}$. The rank a rigid w-equation $\mathcal{E} \vdash_\forall s \simeq t$ is the sum of the ranks of $\mathcal{E}$ and $s \simeq t$. The rank of a system of rigid w-equations $\{R_1, \ldots, R_n\}$ is the sum of ranks of $R_1, \ldots, R_n$. For example, the rank of the system consisting of two equations $c_1 \simeq c_2g, c_2 \simeq c_5h \vdash_\forall c_1u \simeq c_4$ and $\vdash_\forall c_2 \simeq c_3v$ is $1+2+2+5+1+4+2+3=20$.

Since any ground system of rigid equations can be regarded as a system of rigid w-equations, the notion of a rank can be applied to ground systems of rigid equations. Evidently, transformations of types 2 and 3 decrease the rank of such systems.

Lemma 5.6 Suppose that a ground system $\mathcal{R}$ of rigid equations of rank r has a solution. Then after $\leq 2r$ transformations of types 1–3 one can obtain from $\mathcal{R}$ the empty system.

Proof. Follows from Lemma 5.5 by the following considerations. First, any sequence of transformations of type 1 can be considered as one transformation of type 1. Thus, we can assume that any transformation of type 1 is followed by a transformation of types 2 or 3. Second, any transformation of types 2 or 3 decreases the rank of the system. Hence, there can be at most $\leq r$ transformations of types 2 or 3. □

5.2 Equivalence theorem

We call a *mixed system* any finite set of rigid w-equations and ideal membership equations. We shall denote mixed systems as $\mathcal{S} \cup \mathcal{I}$, where $\mathcal{S}$ is the set of all rigid w-equations in the system and $\mathcal{I}$ is the set of all ideal membership equations in the system. A *solution* to a mixed system is any word substitution that solves every rigid w-equation and every ideal membership equation in the system. Similar to transformations of types 1–3 of ground systems of rigid equations, we shall define three types of *w-transformations of mixed systems.* We assume that the mixed system is $\mathcal{S} \cup \mathcal{I}$, where $\mathcal{S} = \{\mathcal{E}_i \vdash_\forall s_i \simeq t_i \mid 1 \leq i \leq n\}$.

For any constant a and set of w-equations $\mathcal{E}$, denote by $\mathcal{E}^a$ the set of all w-equations in $\mathcal{E}$ having the form $aU \simeq aV$.

1 *The w-transformation of type 1* simultaneously makes all replacements of the following form. Suppose that aW occurs in a w-equation $aW \simeq t$ in $\mathcal{E}_i \vdash_\forall s_i \simeq t_i$ and

$$\mathcal{E}_i^a = \{aU_1 \simeq aV_1, \ldots, aU_m \simeq aV_m\}.$$

Then this occurrence of aW is replaced by aw, where w is a new word variable, and we add to $\mathcal{I}$ the ideal membership equation $(w, W) \in \mathit{ideal}(\{(U_1, V_1), \ldots, (U_m, V_m)\})$. This transformation is *simultaneously* made for all constants a and all occurrences of aW.

2 Suppose that $\mathcal{E}_i$ contains a w-equation $c_kV \simeq c_jW$ such that $k > j$ and the rigid w-equation $\mathcal{E}_i \vdash_\forall s_i \simeq t_i$ contains a w-equation $c_kU \simeq r$. Then *the w-transformation of type 2* replaces this occurrence of $c_kU \simeq r$ in $\mathcal{E}_i \vdash_\forall s_i \simeq t_i$ by $c_jWu \simeq r$, where u is a new word variable, and adds to $\mathcal{I}$ the ideal membership equation $(U, Vu) \in \mathit{ideal}(\emptyset)$.

3 Suppose that s_i and t_i have the forms aV and aW, respectively. Then *the w-transformation of type 3* removes $\mathcal{E}_i \vdash_\forall s_i \simeq t_i$ from $\mathcal{S}$ and adds to $\mathcal{I}$ the ideal membership equation $(V, W) \in \mathit{ideal}(\emptyset)$.

We give an example of a w-transformation of type 1. Suppose that $\mathcal{S}$ consists of one rigid w-equation

$$aU_1 \simeq aV_1, aU_2 \simeq bV_2, bU_3 \simeq bV_3 \vdash_\forall cU_4 \simeq aV_4$$

where $U_1, \dots, U_4$ and $V_1, \dots, V_4$ are arbitrary words. Denote the left side of this rigid w-equation by $\mathcal{E}$. Then

$$\begin{aligned} \mathcal{E}^a &= \{aU_1 \simeq aV_1\} \\ \mathcal{E}^b &= \{bU_3 \simeq bV_3\} \\ \mathcal{E}^c &= \emptyset \end{aligned}$$

Let $u_1, \dots, u_4$ and $v_1, \dots, v_4$ be new word variables. Then this rigid w-equation will be replaced by

$$au_1 \simeq av_1, au_2 \simeq bv_2, bu_3 \simeq bv_3 \vdash_\forall cu_4 \simeq av_4$$

and the following ideal membership equations will be added to $\mathcal{I}$:

$$\begin{array}{lll} (u_1, U_1) \in ideal(\{(U_1, V_1)\}), & (v_2, V_2) \in ideal(\{(U_3, V_3)\}), & (u_4, U_4) \in ideal(\emptyset) \\ (v_1, V_1) \in ideal(\{(U_1, V_1)\}), & (u_3, U_3) \in ideal(\{(U_3, V_3)\}), & \\ (u_2, U_2) \in ideal(\{(U_1, V_1)\}), & (v_3, V_3) \in ideal(\{(U_3, V_3)\}), & \\ (v_4, V_4) \in ideal(\{(U_1, V_1)\}), & & \end{array}$$

Lemma 5.7 Let a mixed system $\mathcal{S}' \cup \mathcal{I}'$ be obtained by a w-transformation of type 1, 2 or 3 from a mixed system $\mathcal{S} \cup \mathcal{I}$ and σ be a word substitution grounding for $\mathcal{S}, \mathcal{S}', \mathcal{I}, \mathcal{I}'$. If a substitution σ is a solution to $\mathcal{S}' \cup \mathcal{I}'$ then σ is also a solution to $\mathcal{S} \cup \mathcal{I}$.

Proof. As usual, we assume that $\mathcal{S}$ consists of rigid w-equations $\mathcal{E}_i \vdash s_i \simeq t_i$. Since $\mathcal{I} \subseteq \mathcal{I}'$, it is enough to prove that σ is a solution to $\mathcal{S}$. Consider the tree cases corresponding to the three kinds of transformations.

1 Suppose that a w-transformation of type 1 replaces some rigid w-equation $\mathcal{E} \vdash_\forall s \simeq t$ by $\mathcal{E}' \vdash_\forall s' \simeq t'$. We have $\mathcal{E}'\sigma \vdash s'\sigma \simeq t'\sigma$. We have to prove $\mathcal{E}\sigma \vdash s\sigma \simeq t\sigma$.

From Lemma 5.3 it follows that $\mathcal{E}\sigma \vdash \mathcal{E}'\sigma$, $\mathcal{E}\sigma \vdash s\sigma \simeq s'\sigma$ and $\mathcal{E}\sigma \vdash t\sigma \simeq t'\sigma$. Evidently, these and $\mathcal{E}'\sigma \vdash s'\sigma \simeq t'\sigma$ implies $\mathcal{E}\sigma \vdash s\sigma \simeq t\sigma$.

2 Suppose that $\mathcal{E}_i$ contains a w-equation $c_kV \simeq c_jW$ such that $k > j$ and the rigid w-equation $\mathcal{E}_i \vdash_\forall s_i \simeq t_i$ contains a w-equation $c_kU \simeq r$. We denote this rigid w-equation by $R[c_kU \simeq r]$. The w-transformation of type 2 replaces $R[c_kU \simeq r]$ by $R[c_jWu \simeq r]$ and $\mathcal{I}'$ contains the ideal membership equation $(U, Vu) \in ideal(\emptyset)$. By Lemma 5.1 we have $U\sigma = (Vu)\sigma$. Hence $(R[c_kU \simeq r])\sigma = (R[c_kVu \simeq r])\sigma$. Since σ is a solution to $R[c_jWu \simeq r]$, then σ is also a solution to $R[c_kU \simeq r]$.

3 The w-transformation of type 3 removes $\mathcal{E}_i \vdash_\forall aV \simeq aW$ from $\mathcal{S}$ and $\mathcal{I}'$ contains the ideal membership equation $(V, W) \in ideal(\emptyset)$. By Lemma 5.1 we have $V\sigma = W\sigma$. Hence, σ is a solution to $\mathcal{E}_i \vdash_\forall aV \simeq aW$. □

Let $\mathcal{S} \cup \mathcal{I}$ be a mixed system and $\mathcal{R}$ be a system of ground rigid equations. We call $\mathcal{R}$ *a σ-instance of* $\mathcal{S} \cup \mathcal{I}$ if

1. σ is a solution to $\mathcal{I}$;
2. $\mathcal{S}\sigma$ coincides with $\mathcal{R}$.

Lemma 5.8 Let $\mathcal{S} \cup \mathcal{I}$ be a mixed system and $\mathcal{R}$ be its σ-instance. Let $\mathcal{R}'$ be obtained from $\mathcal{R}$ by a transformation of type 1,2 or 3. Then there exists a word substitution σ' extending σ and a mixed system $\mathcal{S}' \cup \mathcal{I}'$ obtained from $\mathcal{S} \cup \mathcal{I}$ by a w-transformation of the same type such that $\mathcal{R}'$ is a σ'-instance of $\mathcal{S}' \cup \mathcal{I}'$.

Proof. Consider the three cases corresponding to the type of the transformation.

1. Let $\mathcal{S}$ have the form

$$\begin{array}{l} \mathcal{E}_1 \vdash_\forall s_1 \simeq t_1 \\ \dots \\ \mathcal{E}_n \vdash_\forall s_n \simeq t_n \end{array}$$

   Apply the w-transformation of type 1 to $\mathcal{S}$ that only introduces new word variables not occurring in $dom(\sigma)$. First, we define the substitution σ'. Let aV be any w-term so that a w-equation $aV \simeq t$ occurs in $\mathcal{E}_i \vdash_\forall s_i \simeq t_i$. Since $\mathcal{R}$ is an instance of $\mathcal{S} \cup \mathcal{I}$, the term $aV\sigma$ occurs in $\mathcal{R}$. As a result of transformation of type 1, the term $aV\sigma$ is replaced by a term aV' occurring in $\mathcal{R}'$. Consider the w-term av' such that aV is replaced by av' in the w-transformation from $\mathcal{S}$ to $\mathcal{S}'$. We shall say that the *word V' is associated with the word variable v'*. Since the transformation of type 1 replaces the term $aV\sigma$ by a term equal to it w.r.t. $\mathcal{E}_i^a\sigma$, we have

$$\mathcal{E}_i^a\sigma \vdash aV\sigma \simeq aV'. \tag{5.1}$$

   We define σ' as follows. The domain of σ' is $dom(\sigma)$ plus the set of all new word variables introduced by the w-transformation. On any such new word variable v we define $v'\sigma' \rightleftharpoons V'$, where V' is the word associated with v'. We prove that σ' satisfies the conditions. The property $\mathcal{S}'\sigma' = \mathcal{R}'$ is straightforward by the construction of σ'. It remains to show that σ' is a solution to $\mathcal{I}'$. Since σ' extends σ, we have that σ' is a solution to $\mathcal{I}$. Hence, we have to only prove that σ' is a solution to any ideal membership equation in $\mathcal{I}' \setminus \mathcal{I}$.

   We consider now the form of ideal membership equations in $\mathcal{I}' \setminus \mathcal{I}$. Let aV be any w-term so that a w-equation $aV \simeq t$ occurs in $\mathcal{E}_i \vdash_\forall s_i \simeq t_i$ and v', V' be defined as above. Suppose that $\mathcal{E}_i^a = \{aU_1 \simeq aV_1, \dots, aU_m \simeq aV_m\}$. Then $\mathcal{I}' \setminus \mathcal{I}$ contains the ideal membership equation $(V, v') \in ideal((U_1, V_1), \dots, (U_m, V_m))$. By Lemma 5.3, the substitution σ' is a solution to this ideal membership equation if and only if

$$aU_1\sigma' \simeq aV_1\sigma', \dots, aU_m\sigma' \simeq aV_m\sigma' \vdash aV\sigma' \simeq av'\sigma'. \tag{5.2}$$

   Using that σ' extends σ and using $v'\sigma' = V'$, it is easy to see that (5.2) is the same as (5.1).

   We note that this proof works for *all* ideal membership equations in $\mathcal{I}' \setminus \mathcal{I}$.

2. Suppose that $\mathcal{E}_i$ contains a w-equation $c_kV \simeq c_jW$ such that $k > j$ and the rigid w-equation $\mathcal{E}_i \vdash_\forall s_i \simeq t_i$ contains a w-equation $c_kU \simeq r$. Then the word $U\sigma$ has the form $V\sigma U'$ such that the transformation of type 2 replaces $c_kV\sigma U' \simeq r\sigma$ by $c_jW\sigma U' \simeq r\sigma$. Consider the corresponding w-transformation of type 2 replacing $c_kU \simeq r$ by $c_jWu \simeq r$ and adding the

ideal membership equation $(U, Vu) \in ideal(\emptyset)$, where u is any new variable not belonging to $dom(\sigma)$. First, we define σ' as follows. The domain of σ' is $dom(\sigma) \cup \{u\}$ and $u\sigma' \rightleftharpoons U'$.

By the construction of σ it is easy to see that $\mathcal{R}\sigma' = \mathcal{R}'$. As before, we have to show that σ' is a solution to $\mathcal{I}' \setminus \mathcal{I}$, i.e. σ' is a solution to $(U, Vu) \in ideal(\emptyset)$. By the construction we have $U\sigma' = V\sigma'U'$ and $u\sigma' = U'$. Hence, $U\sigma' = (Vu)\sigma'$. By Lemma 5.1 σ' is a solution to $(U, Vu) \in ideal(\emptyset)$.

3. The case of transformations of type 3 is similar. In this case $\sigma' = \sigma$. □

Lemma 5.9 Let $\mathcal{S} \cup \mathcal{I}$ be a mixed system and $\mathcal{R}$ be its σ-instance. Let $\mathcal{R}'$ be obtained from $\mathcal{R}$ by a sequence of k transformations of type 1,2 or 3. Then there exist a substitution σ' extending σ and a mixed system $\mathcal{S}' \cup \mathcal{I}'$ obtained from $\mathcal{S} \cup \mathcal{I}$ by a sequence of k w-transformations of the same type such that $\mathcal{R}'$ is a σ'-instance of $\mathcal{S}' \cup \mathcal{I}'$.

Proof. Immediate from Lemma 5.8. □

Lemma 5.10 The problem of solvability of systems of mixed equations is effectively reducible to the ideal membership problem. More precisely, for every system $\mathcal{S} \cup \mathcal{I}$ of mixed equations one can effectively construct a finite set $\mathbf{I}$ of systems of ideal membership equations such that for any word substitution σ with $dom(\sigma) = var(\mathcal{S} \cup \mathbf{I})$, it is a solution to $\mathcal{S} \cup \mathcal{I}$ if and only if some extension of σ is a solution to some $\mathcal{I}' \in \mathbf{I}$.

Proof. Let r be the rank of $\mathcal{S}$. Consider all systems of ideal membership equations $\mathcal{I}'$ such that $\emptyset \cup \mathcal{I}'$ is obtained from $\mathcal{S} \cup \mathcal{I}$ by a sequence of $\leq 2r$ w-transformations. It is enough to prove that σ is a solution to $\mathcal{S}$ if and only if some σ' extending σ is a solution to some such $\mathcal{I}'$.

$\Leftarrow$ Immediate by Lemma 5.7.

$\Rightarrow$ By Lemma 5.6 by a sequence of transformations of types 1,2,3 we can obtain from $\mathcal{S}\sigma' = \mathcal{S}\sigma$ the empty system:

$$\mathcal{S}\sigma' = \mathcal{R}_0 \to \ldots \to \mathcal{R}_k = \emptyset,$$

where $k \leq 2r$. Since $\mathcal{S}\sigma'$ is obviously a σ'-instance of $\mathcal{S} \cup \mathcal{I}$, by Lemma 5.9 we can construct a sequence of w-transformations

$$\mathcal{S} \cup \mathcal{I} = \mathcal{S}_0 \cup \mathcal{I}_0 \to \ldots \mathcal{S}_k \cup \mathcal{I}_k$$

such that $\mathcal{R}_k$ is a σ'-instance of $\mathcal{S}_k \cup \mathcal{I}_k$. By the definition of σ'-instance we have that $\mathcal{S}_k = \emptyset$ and σ' is a solution to $\mathcal{I}_k$. □

Lemma 5.11 The problem of solvability of systems of rigid w-equations is decidable if and only if the problem of solvability of mixed systems is decidable, if and only if the ideal membership problem is decidable.

Proof. Immediate by Lemmas 5.4 and 5.10. □

Theorem 4 Monadic SREU is decidable if and only if the ideal membership problem is decidable.

Proof. By Lemmas 2.16 we can consider systems of rigid w-equations instead of monadic SREU. Then apply Lemma 5.11. □

This theorem implies the following.

Theorem 5 The ideal membership problem is decidable if and only if any of the Problems 1–4 is decidable in the case of monadic signatures.

5.3 More about the ideal membership problem

In this section we consider the ideal membership problem in more detail. We show that the (un)decidability of this problem does not change if we add regular constraints (every word variable v_i range over a regular set R_i) and the inequality relation.

The proofs is this section will be presented less formally than in the previous sections.

Lemma 5.12 The ideal membership problem is decidable if and only if the ideal membership problem augmented with regular constraints is decidable.

Proof. Similar to Lemma 3.1, for any deterministic finite automaton representing a regular set R, we can effectively find a rigid w-equation W of one word variable v whose solutions are word substitutions $\{V/v\}$ such that $V \in R$. Hence, regular constrains can be expressed by mixed equations. By Lemma 5.11, the decidability of systems of mixed equations is equivalent to the ideal membership problem. □

Lemma 5.13 The ideal membership problem is decidable if and only if the ideal membership problem augmented with regular constraints and the inequality constraints $U \not\simeq V$ is decidable.

Proof. It is enough to note that for any inequality constraint $U \not\simeq V$ we can effectively find a finite set $\mathbf{S}$ of systems of rigid w-equations such that for any substitution σ, we have $U\sigma \neq V\sigma$ if and only if σ is a solution to some member of $\mathbf{S}$.

Let $\mathcal{F} = \{f_1, \ldots, f_k\}$. We define the following systems of rigid w-equations:

1. Systems $\mathcal{S}_i$, where $1 \leq i \leq k$:

$$\vdash_\forall aU \simeq aVf_iu$$

   where u is a new word variable.

2. Systems $\mathcal{S}^i$, where $1 \leq i \leq k$:

$$\vdash_\forall aUf_iv \simeq aV$$

   where v is a new word variable.

3. Systems $\mathcal{S}^i_j$, where $1 \leq i, j \leq k$ and $i \neq j$:

$$\begin{array}{l} \vdash_\forall aU \simeq awf_iu \\ \vdash_\forall aV \simeq awf_jv \end{array}$$

   where u, v, w are new word variables.

It is easy to see that the set

$$\mathbf{S} = \{\mathcal{S}_i \mid 1 \leq i \leq n\} \cup \{\mathcal{S}^i \mid 1 \leq i \leq n\} \cup \{\mathcal{S}^i_j \mid 1 \leq i, j \leq n \text{ and } i \neq j\}$$

satisfies the statement. $\square$

Note that the solutions to inequality constraints are searched among words on the original alphabet $\mathcal{F}$.

Acknowledgments

We thank Anatoli Degtyarev and Gennadi Makanin.

Bibliography

[1] N. Dershowitz and J.-P. Jouannaud. Rewrite systems. In J. Van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B: Formal Methods and Semantics, chapter 6, pages 243–309. North Holland, Amsterdam, 1990.

[2] A. Degtyarev, Yu. Gurevich, and A. Voronkov. Herbrand's theorem and equational reasoning: Problems and solutions. In *Bulletin of the European Association for Theoretical Computer Science*, volume 60, pages 78–95. October 1996. The "Logic in Computer Science" column.

[3] A. Degtyarev, Yu. Gurevich, P. Narendran, M. Veanes, and A. Voronkov. The decidability of simultaneous rigid E-unification with one variable. UPMAIL Technical Report 139, Uppsala University, Computing Science Department, March 1997.

[4] A. Degtyarev, Yu. Matiyasevich, and A. Voronkov. Simultaneous rigid E-unification and related algorithmic problems. In *Eleventh Annual IEEE Symposium on Logic in Computer Science (LICS'96)*, pages 494–502, New Brunswick, NJ, July 1996. IEEE Computer Society Press.

[5] A. Degtyarev and A. Voronkov. The undecidability of simultaneous rigid E-unification. *Theoretical Computer Science*, 166(1–2):291–300, 1996.

[6] A. Kościelski and L. Pacholski. Complexity of unification in free groups and free semigroups. In *Proc. 31st Annual IEEE Symposium on Foundations of Computer Science*, pages 824–829, Los Alamitos, 1990.

[7] A. Kościelski and L. Pacholski. Complexity of Makanin's algorithm. *Journal of the Association for Computing Machinery*, 43(4):670–684, 1996.

[8] D. Kozen. Complexity of finitely presented algebras. In *Proc. of the 9th Annual Symposium on Theory of Computing*, pages 164–177, New York, 1977. ACM.

[9] G.S. Makanin. The problem of solvability of equations in free semigroups. *Mat. Sbornik (in Russian)*, 103(2):147–236, 1977. English Translation in American Mathematical Soc. Translations (2), vol. 117, 1981.

[10] D. Perrin. Finite automata. In J. Van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B: Formal Methods and Semantics, chapter 1, pages 1–57. Elsevier Science, Amsterdam, 1990.

[11] D.A. Plaisted. Special cases and substitutes for rigid E-unification. Technical Report MPI-I-95-2-010, Max-Planck-Institut für Informatik, November 1995.

[12] K.U. Schultz. Makanin's algorithm: Two improvements and a generalization. In K.U. Schultz, editor, *Proceedings of the First International Workshop on Word Equations and Related Topics, Tübingen*, volume 572 of *Lecture Notes in Computer Science*, 1990.

[13] R. Shostak. An algorithm for reasoning about equality. *Communications of the ACM*, 21:583–585, July 1978.

[14] M. Veanes. Uniform representation of recursively enumerable sets with simultaneous rigid E-unification. UPMAIL Technical Report 126, Uppsala University, Computing Science Department, 1996.