UPMAIL Technical Report No. 104
April 26, 1995

Simultaneous Rigid E-Unification is not so Simple

Anatoli Degtyarev*
Computing Science Department
Uppsala University
Box 311, S-751 05 Uppsala,
Sweden
email anatoli@csd.uu.se

Yuri Matiyasevich†
Steklov Institute of Mathematics
St. Petersburg Division
27 Fontanka
St.Petersburg, 191011
Russia
email yumat@pdmi.ras.ru

Andrei Voronkov‡
Computing Science Department
Uppsala University
Box 311, S-751 05 Uppsala,
Sweden
email voronkov@csd.uu.se

*Supported by a grant from the Swedish Institute
†Partially supported by a grant from the Swedish Royal Academy of Sciences
‡Supported by a TFR grant

Abstract

Simultaneous rigid E-unification has been introduced in the area of theorem proving with equality. It is used in *extension procedures,* like the tableau method or the connection method. Many articles in this area tacitly assume the existence of an algorithm for simultaneous rigid E-unification. There were several faulty proofs of the decidability of this problem.

In this article we prove several results about the simultaneous rigid E-unification. Two results are reductions of known problems to simultaneous rigid E-unification. Both these problems are very hard. The word equation solving (unification under associativity) is reduced to the monadic case of simultaneous rigid E-unification. The variable-bounded semi-unification problem is reduced to the general simultaneous rigid E-unification. The word equation problem used in the first reduction is known to be decidable, but the decidability result is extremely non-trivial. As for the variable-bounded semi-unification, its decidability is not even known.

We also prove that a special case of simultaneous rigid E-unification with one unary function symbol is decidable. This is shown by reducing it to the Diophantine problem for addition and divisibility whose decidability is known. The technique we use is a combination of a technique of the number theory and a technique of the theory of rewrite systems.

Section 1

Simultaneous rigid E-unification

The simultaneous rigid E-unification problem plays a crucial role in automatic proof methods for first order logic with equality based on sequent calculi, such as semantic tableaux [Fitting 88], the connection method [Bibel 87] (also known as the mating method [Andrews 81]), model elimination [Loveland 68] and a dozen other procedures. All these methods express the idea that the proof-search can be considered as the problem of checking that every path through a matrix of the goal formula is complementary (for this reason these methods are sometimes characterized as *matrix methods*). This idea was originally justified by Prawitz [Prawitz 60]. Instead of generating instances of a quantifier-free formula $M(\bar{x})$, he proposed to search for a substitution σ for $\bar{x}_1, \ldots, \bar{x}_n$ such that every path in $(M(\bar{x}_1) \wedge \ldots \wedge M(\bar{x}_n))\sigma$ becomes complementary. In the case without equality, the search for such a substitution can be carried out using ordinary (simultaneous) unification. Thus, for a given matrix $M(\bar{x}_1) \wedge \ldots \wedge M(\bar{x}_n)$, the problem of the existence of an appropriate substitution is decidable and can be performed by any known unification algorithm.

The situation is not so simple for the predicate calculus with equality. In fact, the first algorithm was constructed by Kanger [Kanger 63]. The algorithm implicitly used simultaneous rigid E-unification: Kanger noted that we have to solve this problem at some stage of the algorithm, but proposed a solution based on so called minus-normality [Maslov 67]: instead of unification, one should search in a *finite* set of terms.

The approach based on rigid E-unification has been developed by Bibel [Bibel 87] and Gallier et. al. [GRS 87, GNRS 92]. According to this approach, complementary literals are replaced by eq-connections instantiated by eq-unifiers [Bibel 87] or mated sets instantiated by *rigid E-unifiers* [GRS 87] which is the same despite the different terminology.

The use of simultaneous rigid E-unification was a very natural generalization of the techniques used in the non-equality case, but the problem happened to be perfidious, causing many surprises to the researchers[1]. After all unsuccessful attempts to solve this problem, it is not even known if it is decidable at all. In fact, it is not even known for the monadic case.

Results from this paper partially explain the unsuccessful attempts to prove the decidability of simultaneous rigid E-unification by modifications of the ordinary (non-simultaneous) rigid E-unification which was proven to be NP-complete by Gallier et. al. [GNPS 88]. Our reduction of the word equation solving to the simultaneous rigid E-unification (in fact, even to its monadic case) shows that the latter problem is inherently difficult and can hardly be solved by simple constructions

[1]It has been proven NP-complete in [GNRS 92], twice proven to be NEXPTIME-complete [Goubault 93c, Goubault 93d] and once DEXPTIME-complete [Goubault 94]. The monadic case was proven PSPACE-complete in [Goubault 93c, Goubault 93d, Goubault 94]. Proofs of these papers contained irrecoverable errors. (According to [Goubault 93b], [Goubault 93a] also proved the monadic case to be outside of PSPACE.)

used so far.

These results suggest that theorem proving with equality based on the matrix methods should look for foundations different from simultaneous rigid E-unification. In [DegVor 94b, DegVor 95a] the first and the third authors proposed an alternative solution based on *equality elimination.* The equality elimination method is based on a combination of a top-down matrix rule with the bottom-up equation solving. Equality elimination uses ordinary unification and efficient strategies for equality handling via basic superposition with simplification and redundancy deletion. It takes advantage of ordering strategies and gives a hint on how to search for a suitable quantifier duplication due to the possibility of the incremental use of equation solutions.

Equality elimination was used for equational logic programming [DegVor 94a], the tableau method [DegVor 94b], the inverse method [DegVor 94c] and the connection method [DegVor 95a]. In [DeKoVo 95b] equality elimination is combined with basic folding, in order to transform equational logic programs into logic programs without equality.

This paper is organized as follows. In Section 1.1 we introduce main definitions concerning equations and substitutions. In Section 1.2 we define simultaneous rigid E-unification. In Section 2 we show how to reduce the word equation problem (which can also be considered as a special case of unification under associativity) to the monadic case of simultaneous rigid E-unification. It shows that even the monadic case of simultaneous rigid E-unification is extremely hard. In Section 3 we reduce variable-bounded semi-unification to the general case of simultaneous rigid E-unification. We note that the decidability of the variable-bounded semi-unification is an open problem. In Section 4 prove the decidability of simultaneous rigid E-unification in the signature with one unary function symbol and any number of constants. The proof is done by reduction to the Diophantine problem for addition and divisibility whose (non-trivial) decidability was known.

1.1 Equations and substitutions

The notion of terms, substitutions, equations and rewrite rules are standard and may be found e.g. in [DerJou 90]. A term, equation or rewrite rule is *ground* iff it has no variables. The set of all terms of a signature Σ with variables in the set X is denoted by $T_\Sigma(X)$, the set of all ground terms of the signature Σ by T_Σ. We denote

- Equations by $s = t$ (note that $=$ is used to denote the equality predicate);
- Rewrite rules by $s \to t$;
- Substitutions by $\{t_1/x_1, \ldots, t_n/x_n\}$.

In order to distinguish identity from the equality predicate, the former will be denoted by $\approx$. The notation $\rightleftharpoons$ stands for "equal by definition". For a substitution σ of the form $\{t_1/x_1, \ldots, t_n/x_n\}$, $dom(\sigma) \rightleftharpoons \{x_1, \ldots, x_n\}$ and $ran(\sigma) \rightleftharpoons \{t_1, \ldots, t_n\}$. For any expression E, $var(E)$ denotes the set of all variables occurring in E.

We shall also use the substitution notation $\{t_1/c_1, \ldots, t_n/c_n\}$ where c_i are constants. This will denote the operation of the simultaneous replacement of *all* occurrences of c_i by t_i.

Let a set of rewrite rules S of the form $s \to t$ be fixed. The relation of immediate rewriting in the given system will also be denoted by $\to$. By $\to^*$ we denote the reflexive and transitive closure of the relation $\to$.

Definition 1.1 *The set S is called* noetherian *iff the $\rightarrow$ relation defined by S is well-founded. The set S is said to have the* diamond property *iff for every terms s, t_1, t_2 such that $s \rightarrow t_1$, $s \rightarrow t_2$ and $t_1 \not\approx t_2$ there is a term t such that $t_1 \rightarrow t$ and $t_2 \rightarrow t$. We call a set S of rewrite rules* perfect *iff*

1. *All rewrite rules in S are ground;*
2. *S has the diamond property;*
3. *S is noetherian.*

Definition 1.2 *A* normal form *of a term t is any term $t\downarrow$ such that*

1. *$t \rightarrow^* t\downarrow$;*
2. *There is no term s such that $t\downarrow \rightarrow s$.*

In general, a normal form is not unique.

We shall often use the following obvious lemma:

Lemma 1.1 *Let S be a perfect set of rewrite rules*

$$\begin{array}{l} s_1 \rightarrow t_1 \\ \cdots \\ s_n \rightarrow t_n \end{array}$$

and E be the equational theory $s_1 = t_1, \ldots, s_n = t_n$. Then

1. *For every term t the term $t\downarrow$ exists and is unique;*
2. *$E \vdash s = t$ iff $s\downarrow \approx t\downarrow$.*

1.2 Simultaneous rigid E-unification

Definition 1.3 *A* rigid E-unification problem *is any expression of the form $E \vdash_\forall s = t$, where E is a finite set of equations. By $E \models_\forall s = t$ we denote the fact that the formula $\forall((\bigwedge_{F \in E} F) \supset s = t)$ is provable in first-order logic with equality.*

A substitution σ is a solution *(or a rigid E-unifier) of $E \vdash_\forall s = t$ iff $E\sigma \models_\forall (s = t)\sigma$. A* simultaneous rigid E-unification problem *is a finite set $\{\mathcal{E}_1, \ldots, \mathcal{E}_n\}$ of rigid E-unification problems. A term substitution $\sigma \rightleftharpoons \{t_1/x_1, \ldots, t_m/x_m\}$ is its* solution *iff it is a solution of all $\mathcal{E}_i$, $i \in \{1, \ldots, n\}$. Such a solution is* ground *iff $E\sigma, s\sigma, t\sigma$ and all t_i are ground.*

A simultaneous rigid E-unification problem is monadic *iff its signature contains only unary function symbols and constants.*

Note that when E, s, t are ground, we have $E \models_\forall s = t$ iff $E \vdash s = t$.

It is known that the problem of solvability of a (non-simultaneous) rigid E-unification problem is NP-complete [GRS 87].

Lemma 1.2 *If a simultaneous rigid E-unification problem E is solvable then it has a ground solution.*

Proof. Immediately follows from the following obvious observation: if σ is a solution of E then for any substitution θ the substitution $\sigma\theta$ is a solution of E.

□

We shall introduce one particular kind of a rigid E-unification problem that will be used as a technical tool for many proofs in this paper. For a signature Σ, denote by Σ_n the set of all function symbols of arity n in Σ. For every signature Σ and constant $c \in \Sigma_0$ introduce the following set of equations:

$$Gr(\Sigma, c) \rightleftharpoons \bigcup_{n=0}^{\infty} \{f(a_1, \ldots, a_n) = c \mid f \in \Sigma_n \setminus \{c\},\ a_1, \ldots, a_n \in \Sigma_0\}$$

Lemma 1.3 *Consider the following rigid E-unification problem:*

$$Gr(\Sigma, c) \vdash_\forall x = c$$

Then a substitution θ is a solution of this problem iff $x\theta \in T_\Sigma$.

Proof. Note that the set of rewrite rules

$$\bigcup_{n=0}^{\infty} \{f(a_1, \ldots, a_n) \to c \mid f \in \Sigma_n \setminus \{c\}\}$$

is perfect. Thus, $t = c$ can be proven from $Gr(\Sigma, c)$ iff $t \downarrow\approx c$. It is easy to see that the set of all such t is exactly the set of all ground terms of Σ.

□

There were two kinds of mistaken proofs of the decidability of simultaneous rigid E-unification. The proof of [GNRS 92] used an assumption that one can restrict oneself to substitutions which are minimal for each problem. In [BecPet 94] there is a counterexample to this assumption. In a series of faulty articles [Goubault 93c, Goubault 93d, Goubault 94] a simultaneous rigid E-unification algorithm is given with no proof of completeness. There are many simple examples when this algorithm cannot find a solution of a solvable system. Consider the following example which does not even use function symbols:

$$\begin{array}{l} a = b \vdash_\forall x = y \\ \vdash_\forall x = a \\ \vdash_\forall y = b \end{array}$$

It has one obvious solution $\{a/x, b/y\}$. However, this solution is not found by the Goubault's algorithm from [Goubault 94].

The reductions introduced in subsequent sections show that the decidability of simultaneous rigid E-unification can hardly have a simple proof.

Section 2

Word equations

The problem of solvability of word equations belongs to the classics of the computability theory. The study of the word equation solving was initiated by Markov in the 1950s after his example of a finitely presented semigroup with the undecidable word problem. The decidability of the word equations has been proven only in 1977 by Makanin [Makanin 77]. Despite the very simple formulation, the problem happened to be extremely hard (the mathematically dense proof in [Makanin 77] occupies 88 journal pages). Almost no essential improvements have been made since 1977 despite the numerous attempts by other researchers[1]. No interesting upper bounds for complexity of this problem are yet known[2]. It is known that the problem is NP-hard [BeKaNa 87]. The Makanin's algorithm gives several exponents. It has not been properly investigated how many exponents there are, maybe because it is far from the known lower bound.

2.1 Definitions

Let $\mathcal{F} = \{f_1, \ldots, f_n\}$ be a finite alphabet of *symbols.*

Definition 2.1 *A* word *in the alphabet $\mathcal{F}$ is any sequence $g_1 \ldots g_k$, $k \geq 0$ of symbols in $\mathcal{F}$.*

By $W_1 \approx W_2$ we mean that words W_1 and W_2 are identical.

We shall also consider an infinite alphabet $\mathcal{X} = \{x_1, x_2, \ldots\}$ of *variables*, such that $\mathcal{X} \bigcap \mathcal{F} = \emptyset$.

Definition 2.2 *A* word equation *E is an expression $W_1 = W_2$, where W_i are words in the alphabet $\mathcal{X} \bigcup \mathcal{F}$. In other terms, every word equation E has the form*

$$\alpha_1 \ldots \alpha_k = \alpha_{k+1} \ldots \alpha_l \tag{2.1}$$

where each α_i and is either a symbol in $\mathcal{F}$ or a variable in $\mathcal{X}$. The set $var(E)$ is the set of all variables occurring in E.

A word substitution *θ is an expression of the form*

$$\langle W_1/x_1, \ldots, W_n/x_n \rangle \tag{2.2}$$

such that $x_i \in \mathcal{X}$ and $W_i \in \mathcal{F}^*$.

The application of a word substitution θ of the form (2.2) to a word W (denoted $W\theta$) is the word obtained from W by the simultaneous replacement of all x_i by W_i.

A word substitution θ of the form (2.2) is a solution *of the word equation $V_1 = V_2$ iff*

[1] There are even workshops dedicated to the word equations solving [Schulz 90].

[2] A.Kościelski, G.Makanin, L.Pacholski, K.Schulz, J.Siekmann, (private communications).

1. *$var(V_1 = V_2) \subseteq \{x_1, \ldots, x_n\}$;*

2. *$V_1\theta \approx V_2\theta$.*

A word substitution θ is a solution *of a set of equations iff it is a solution of each equation in this set. An equation or a set of equations is* solvable *iff it has a solution.*

Definition 2.3 *A set E of word equations is* reduced *iff each equation in E has one of the following forms:*

$$x_i x_j = x_p \tag{2.3}$$
$$x_i = f_q \tag{2.4}$$
$$x_i = x_j \tag{2.5}$$

where in any such equation $i \neq j$, $i \neq p$, $j \neq p$, $x_i, x_j, x_p \in \mathcal{X}$ and $f_q \in \mathcal{F}$.

Lemma 2.1 *For every word equation E there is a set of word equations E' such that*

1. *E is solvable iff E' is solvable;*

2. *E' is reduced.*

Proof. Without loss of generality we assume $0 < k < l$. Let E be equation (2.1), $y_1, \ldots, y_l, v_1, \ldots, v_l$ be variables in $\mathcal{F}$ different from variables in $var(E)$. Define E' as the system consisting of the following word equations:

1. All equations of the form $y_i = \alpha_i$;

2. Equations

$$\begin{array}{ll} y_1 = v_1 & y_{k+1} = v_{k+1} \\ v_1 y_2 = v_2 & v_{k+1} y_{k+2} = v_{k+2} \\ \cdots & \cdots \\ v_{k-1} y_k = v_k & v_{l-1} y_l = v_l \end{array}$$

3. The equation $v_k = v_l$.

It is clear that E' is reduced.

Now every solution of E' is evidently a solution of E. On the other hand, every solution θ of E can be extended to a solution of E' by defining

$$y_i\theta \rightleftharpoons \alpha_i\theta$$
$$v_i\theta \rightleftharpoons \begin{cases} (\alpha_1 \ldots \alpha_i)\theta, & i \leq k \\ (\alpha_{k+1} \ldots \alpha_i)\theta, & i > k \end{cases}$$

for all $i \in \{1, \ldots, l\}$.

$\square$

Lemma 2.2 *For every set of word equations E there is a set of word equations E_1 such that*

1. *E is solvable iff E_1 is solvable;*
2. *E_1 is reduced.*

Proof. Replace each equation in E by the corresponding system E' constructed as in Lemma 2.1 choosing different new variables for different equations.

$\square$

2.2 The reduction of word equations

In this section we consider the monadic predicate calculus, i.e. all function symbols are unary. Moreover, we assume that all function symbols are symbols of the alphabet $\mathcal{F} = \{f_1, \ldots, f_n\}$ defined above. We shall write terms in such a signature without parentheses. For example, instead of $f(g(h(a)))$ we simply write $fgha$. If W is a word in the alphabet $\mathcal{F}$, and t a term, we shall denote by Wt the term obtained from t by prefixing it with W. For example, if t is $fghx$ and W is fh, then Wt is $fhfghx$.

Let E be a reduced system of word equations all whose variables are $x_1, \ldots, x_m$. Let $a_1, \ldots, a_m$ be a set of constants. By $R(E)$ we denote the simultaneous rigid E-unification problem containing all the following rigid E-unification problems:

1. For every $i \in \{1, \ldots, m\}$

$$G_i \rightleftharpoons Gr(\{a_i, f_1, \ldots, f_n\}, a_i) \vdash_\forall x_i = a_i$$

2. For every word equation in E of the form $x_i = f_j$

$$F_{ij} \rightleftharpoons \vdash_\forall x_i = f_j a_i$$

3. For every word equation in E of the form $x_i = x_j$

$$E_{ij} \rightleftharpoons a_i = a_j \vdash_\forall x_i = x_j$$

4. For every word equation in E of the form $x_i x_j = x_k$

$$C_{ijk} \rightleftharpoons a_i = x_j, a_j = a_k \vdash_\forall x_i = x_k$$

Lemma 2.3

1. *For every solution θ of $R(E)$ the term $x_i\theta$ has the form Wa_i, where W is a word in the alphabet $\mathcal{F}$;*

2. *The word substitution*

$$\langle W_1/x_1, \ldots, W_m/x_m \rangle$$

is a solution of E iff the term substitution

$$\{W_1 a_1/x_1, \ldots, W_m a_m/x_m\}$$

is a solution of $R(E)$.

Proof. Observe the following:

1. The substitution θ is a solution of G_i iff $x_i\theta \approx W a_i$ for some word W in the alphabet $\mathcal{F}$;

2. The substitution θ is a solution of F_{ij} iff $x_i\theta \approx f_j a_i$.

3. The substitution θ is a solution of $\{G_i, G_j, E_{ij}\}$ iff $x_i\theta \approx W a_i$ and $x_j\theta \approx W a_j$ for some word W in the alphabet $\mathcal{F}$;

4. The substitution θ is a solution of $\{G_i, G_j, G_k, C_{ijk}\}$ iff $x_i\theta \approx V a_i$, $x_j\theta \approx W a_j$ and $x_k\theta \approx VW a_k$ for some words V, W in the alphabet $\mathcal{F}$;

Let us prove these statements one by one.

1. Follows from Lemma 1.3.

2. This case is obvious.

3. Since θ is a solution of G_i, G_j, we have $x_i\theta \approx W_1 a_i$ and $x_j\theta \approx W_2 a_j$. Obviously, the set of rewrite rules $\{a_i \to a_j\}$ is perfect. By Lemma 1.1 $a_i = a_j \models_\forall W_1 a_i = W_2 a_j$ iff $W_1 a_i \downarrow \approx W_2 a_j \downarrow$. Note that $W_1 a_i \downarrow \approx W_1 a_j$ and $W_2 a_j \approx W_2 a_j \downarrow$. Hence, $W_1 \approx W_2$. In the other direction we have to prove $a_i = a_j \models_\forall W a_i = W a_j$, which is obvious.

4. Since θ is a solution of G_i, G_j, G_k, we have $x_i\theta \approx V a_i$, $x_j\theta \approx W a_j$ and $x_k\theta \approx U a_k$. Note that the set of rewrite rules

$$\begin{array}{l} a_i \to W a_j \\ a_k \to a_j \end{array} \tag{2.6}$$

is perfect because i, j, k are pairwise different. By Lemma 1.1, $V a_i \downarrow \approx U a_k \downarrow$. Note that $V a_i \downarrow \approx VW a_j$ and $U a_k \downarrow \approx U a_j$. Thus, $U \approx VW$.

In the other direction we have to prove $a_i = W a_j, a_k = a_j \models_\forall V a_i = VW a_k$, which is obvious.

The rest of the proof is obvious. □

This lemma proves

Theorem 2.1 *The word equation problem is polynomially reducible to monadic simultaneous rigid E-unification.*

Section 3

The variable-bounded semi-unification

Semi-unification has been introduced in several areas of logic and computer science [LanMus 78, Henglein 88, KMNS 88, Pudlák 88, KfTiUr 89, Leiß 89], most notably because of its relation to the typability problem for polymorphic recursive definitions [Leiß 90]. After several faulty proofs of the decidability of semi-unification, the undecidability of this problem was proven in [KfTiUr 93].

First we introduce ordinary semi-unification, following [KfTiUr 93].

Definition 3.1 *A* semi-unification *problem is a finite set of expressions*

$$\begin{array}{l} s_1 \le t_1 \\ \cdots \\ s_n \le t_n \end{array} \tag{3.1}$$

where s_i, t_i are terms in a signature Σ. A solution *of the problem (3.1) is a tuple of substitutions $\sigma, \tau_1, \ldots, \tau_n$ in that signature such that*

$$\begin{array}{l} s_1\sigma\tau_1 \approx t_1\sigma \\ \cdots \\ s_n\sigma\tau_n \approx t_n\sigma \end{array} \tag{3.2}$$

A semi-unification problem is solvable *iff it has a solution. Semi-unification is undecidable [KfTiUr 93].*

Lemma 3.1 *Semi-unification problem (3.1) is solvable iff there is a set of variables W different from variables of the problem and a solution $\langle \sigma, \tau_1, \ldots, \tau_n \rangle$ of this problem such that*

1. *$dom(\sigma) = var(s_1, \ldots, s_n, t_1, \ldots, t_n)$;*
2. *$var(ran(\sigma)) \subseteq W$;*
3. *$var(ran(\tau_i)) \subseteq W$, for all $i \in \{1, \ldots, n\}$;*
4. *$dom(\tau_i) \subseteq W$, for all $i \in \{1, \ldots, n\}$.*

Proof. The proof is based on the observation that we can always rename variables in $ran(\sigma)$ and $dom(\tau_i)$ to satisfy 1–4.

$\square$

Definition 3.2 *Let $\mathcal{P}$ be a semi-unification problem, W be a set of variables different from variables of $\mathcal{P}$. A solution of $\mathcal{P}$ is a W-*solution *iff it satisfies all properties (1–4) of Lemma 3.1.*

Definition 3.3 *A* variable-bounded *semi-unification problem is a pair $(\mathcal{P}, m)$, where $\mathcal{P}$ is a semi-unification problem of the form (3.1), m a natural number. A* solution *of the variable-bounded semi-unification problem is any W-solution of $\mathcal{P}$ such that $\mid W \mid \leq m$.*

It is still unknown whether variable-bound semi-unification is decidable[1].

In this section we reduce variable-bounded semi-unification to simultaneous rigid E-unification.

Let $(\mathcal{P}, m)$ be a variable-bounded semi-unification problem with $\mathcal{P}$ is of the form (3.1). Let $u_1, \ldots, u_k$ be the set of all variables occurring in $\mathcal{P}$. Let x_i^j, y_i, v_i^j, z_l^j be pairwise different variables and $a_{i,l}^j, b_l$ be pairwise different constants not occurring in $\mathcal{P}$, where $i \in \{1, \ldots, k\}, j \in \{1, \ldots, n\}, l \in \{1, \ldots, m\}$. Denote by Σ the signature of $\mathcal{P}$.

Define the following rigid E-unification problems X_i^j, Y_i, V_i^j, Z_l^j, where $i \in \{1, \ldots, k\}, j \in \{1, \ldots, n\}, l \in \{1, \ldots, m\}$ by

$$X_i^j \rightleftharpoons Gr(\Sigma \bigcup \{a_{i,1}^j, \ldots, a_{i,m}^j\}, a_{i,1}^j) \vdash_\forall x_i^j = a_{i,1}^j$$

$$Y_i \rightleftharpoons Gr(\Sigma \bigcup \{b_1, \ldots, b_m\}, b_1) \vdash_\forall y_i = b_1$$

$$V_i^j \rightleftharpoons Gr(\Sigma \bigcup \{b_1, \ldots, b_m\}, b_1) \vdash_\forall v_i^j = b_1$$

$$Z_l^j \rightleftharpoons Gr(\Sigma \bigcup \{b_1, \ldots, b_m\}, b_1) \vdash_\forall z_l^j = b_1$$

Note that Lemma 1.3 applies to all these problems.

In addition, consider rigid E-unification problems O_i^j, C_i^j and S^j, where $i \in \{1, \ldots, k\}, j \in \{1, \ldots, n\}$ defined by

$$O_i^j \rightleftharpoons a_{i,1}^j = b_1, \ldots, a_{i,m}^j = b_m \vdash_\forall x_i^j = y_i$$

$$C_i^j \rightleftharpoons a_{i,1}^j = z_1^j, \ldots, a_{i,m}^j = z_m^j \vdash_\forall x_i^j = v_i^j$$

$$S^j \rightleftharpoons \vdash_\forall s_j\{v_1^j/u_1, \ldots, v_k^j/u_k\} = t_j\{y_1/u_1, \ldots, y_k/u_k\}$$

[1] J.Tiuryn, H.Leiß, F.Henglein, private communications. We cite a part of our communication with H.Leiß and F.Henglein:

> Another interesting, related, but not identical question, in my mind, is to investigate the following problem: Let $f(n)$ be a recursive function. Given signature Σ and an infinite sequence of variables $x_1, \ldots, x_i, \ldots$ denote by $x[m]$ the first m variables in this sequence. The problem is: Given a semi-unification problem instance over $T_\Sigma(x[n])$ does there exist a solution over $T_\Sigma(x[f(n)])$?

Define the simultaneous rigid E-unification problem

$$
\begin{array}{rll}
R_{(\mathcal{P},m)} \rightleftharpoons & \{X_i^j \mid i \in \{1,\ldots,k\}, j \in \{1,\ldots,n\}\} & \cup \\
& \{Y_i \mid i \in \{1,\ldots,k\}\} & \cup \\
& \{V_i^j \mid i \in \{1,\ldots,k\}, j \in \{1,\ldots,n\}\} & \cup \\
& \{Z_l^j \mid j \in \{1,\ldots,n\}, l \in \{1,\ldots,m\}\} & \cup \\
& \{O_i^j \mid i \in \{1,\ldots,k\}, j \in \{1,\ldots,n\}\} & \cup \\
& \{C_i^j \mid i \in \{1,\ldots,k\}, j \in \{1,\ldots,n\}\} & \cup \\
& \{S^j \mid j \in \{1,\ldots,n\}\} &
\end{array}
$$

Theorem 3.1 *The variable-bounded semi-unification problem $(\mathcal{P}, m)$ is solvable iff the rigid E-unification problem $R_{(\mathcal{P},m)}$ is solvable.*

This theorem immediately follows from Lemma 3.2 below. This lemma characterizes the relation between solutions of the two problems.

Lemma 3.2 *The tuple $\langle \sigma, \tau_1, \ldots, \tau_n \rangle$ is a $w_1, \ldots, w_m$-solution of $\mathcal{P}$ iff the substitution θ defined by*

$$x_i^j\theta \rightleftharpoons u_i\sigma\{a_{i,1}^j/w_1, \ldots, a_{i,m}^j/w_m\} \tag{3.3}$$
$$y_i\theta \rightleftharpoons u_i\sigma\{b_1/w_1, \ldots, b_m/w_m\} \tag{3.4}$$
$$z_l^j\theta \rightleftharpoons w_l\tau_j\{b_1/w_1, \ldots, b_m/w_m\} \tag{3.5}$$
$$v_i^j\theta \rightleftharpoons u_i\sigma\tau_j\{b_1/w_1, \ldots, b_m/w_m\} \tag{3.6}$$

is a solution of $R_{(\mathcal{P},m)}$. Moreover, for each solution θ of $R_{(\mathcal{P},m)}$ there is a $\{w_1, \ldots, w_m\}$-solution $\langle \sigma, \tau_1, \ldots, \tau_n \rangle$ of $\mathcal{P}$ satisfying (3.3)–(3.6).

Proof. We shall use the tuple notation for terms and substitutions so that (3.3)–(3.6) can be rewritten as

$$x_i^j\theta \approx u_i\sigma\{\bar{a}_i^j/\bar{w}\} \tag{3.7}$$
$$y_i\theta \approx u_i\sigma\{\bar{b}/\bar{w}\} \tag{3.8}$$
$$z_l^j\theta \approx w_l\tau_j\{\bar{b}/\bar{w}\} \tag{3.9}$$
$$v_i^j\theta \approx u_i\sigma\tau_j\{\bar{b}/\bar{w}\} \tag{3.10}$$

We shall prove the statement in the $\Leftarrow$ direction. Let θ be an arbitrary solution of $R_{(\mathcal{P},m)}$. Since θ is a solution of X_i^j, Y_i, V_i^j, Z_l^j and by Lemma 1.3

$$
\begin{array}{l}
x_i^j\theta \in T_{\Sigma \cup \{a_{i,1}^j, \ldots, a_{i,m}^j\}} \\
y_i\theta, v_i^j\theta, z_l^j\theta \in T_{\Sigma \cup \{b_1, \ldots, b_m\}}
\end{array}
\tag{3.11}
$$

Denote by p_i the term $y_i\theta\{\bar{w}/\bar{b}\}$, where $i \in \{1, \ldots, k\}$. From (3.11) it follows that $p_i \in T_\Sigma(\{w_1, \ldots, w_m\})$ and

$$y_i\theta \approx p_i\{\bar{b}/\bar{w}\} \tag{3.12}$$

Consider the set of rewrite rules (see the definition of O_i^j):

$$\begin{array}{l} a_{i,1}^j \to b_1 \\ \dots \\ a_{i,m}^j \to b_m \end{array}$$

This set is perfect. By Lemma 1.1, θ is a solution of O_i^j iff $x_i^j\theta \downarrow = y_i\theta \downarrow$. By (3.11) we have $y_i\theta \downarrow = y_i\theta$. From this and (3.12) we get

$$x_i^j\theta \approx p_i\{\bar{a}_i^j/\bar{w}\} \tag{3.13}$$

Denote by q_l^j the term $z_l^j\theta\{\bar{w}/\bar{b}\}$, where $l \in \{1,\dots,m\}, j \in \{1,\dots,n\}$. From (3.11) it follows that $q_l^j \in T_\Sigma(\{w_1,\dots,w_m\})$ and

$$z_l^j\theta \approx q_l^j\{\bar{b}/\bar{w}\} \tag{3.14}$$

Introduce the following substitutions:

$$\sigma \rightleftharpoons \{p_1/u_1,\dots,p_k/u_k\} \tag{3.15}$$

$$\tau^j \rightleftharpoons \{q_1^j/w_1,\dots,q_m^j/w_m\} \tag{3.16}$$

We are going to prove that $\langle\sigma,\tau^1,\dots,\tau^n\rangle$ is a $\{w_1,\dots,w_m\}$-solution of $\mathcal{P}$. Note that all conditions on variables of σ,τ^i are satisfied. All we have to prove is that $\langle\sigma,\tau^1,\dots,\tau^n\rangle$ is a solution of $\mathcal{P}$.

Denote by r_i^j the term $v_i^j\theta\{\bar{w}/\bar{b}\}$, where $i \in \{1,\dots,k\}, j \in \{1,\dots,n\}$. From (3.11) it follows that $r_i^j \in T_\Sigma(\{w_1,\dots,w_m\})$ and

$$v_i^j\theta \approx r_i^j\{\bar{b}/\bar{w}\} \tag{3.17}$$

Since θ is a solution of C_i^j, we have

$$a_{i,1}^j = z_1^j\theta,\dots,a_{i,m}^j = z_m^j\theta \models_\forall x_i^j\theta = v_i^j\theta$$

By (3.14), (3.13) and (3.17) it is equivalent to

$$a_{i,1}^j = q_1^j\{\bar{b}/\bar{w}\},\dots,a_{i,m}^j = q_m^j\{\bar{b}/\bar{w}\} \models_\forall p_i\{\bar{a}_i^j/\bar{w}\} = r_i^j\{\bar{b}/\bar{w}\} \tag{3.18}$$

Note that the set of rewrite rules

$$\begin{array}{l} a_{i,1}^j \to q_1^j\{\bar{b}/\bar{w}\} \\ \dots \\ a_{i,m}^j \to q_m^j\{\bar{b}/\bar{w}\} \end{array}$$

is perfect. By Lemma 1.1 and (3.18) we have

$$p_i\{\bar{a}_i^j/\bar{w}\} \downarrow \approx r_i^j\{\bar{b}/\bar{w}\} \downarrow$$

It is equivalent to

$$p_i\{\bar{q}^j\{\bar{b}/\bar{w}\}/\bar{w}\} \approx r_i^j\{\bar{b}/\bar{w}\}$$

which is the same as

$$p_i\{\bar{q}^j/\bar{w}\}\{\bar{b}/\bar{w}\} \approx r_i^j\{\bar{b}/\bar{w}\}$$

This implies

$$p_i\{\bar{q}^j/\bar{w}\} \approx r_i^j$$

By (3.16) we obtain

$$p_i\tau^j \approx r_i^j \tag{3.19}$$

Consider now S^j. Since θ is a solution of S^j, we have

$$s_j\{v_1^j/u_1,\ldots,v_k^j/u_k\}\theta \approx t_j\{y_1/u_1,\ldots,y_k/u_k\}\theta$$

This is equivalent to

$$s_j\{v_1^j\theta/u_1,\ldots,v_k^j\theta/u_k\} \approx t_j\{y_1\theta/u_1,\ldots,y_k\theta/u_k\}$$

By (3.17) and (3.12) we obtain

$$s_j\{r_1^j\{\bar{b}/\bar{w}\}/u_1,\ldots,r_k^j\{\bar{b}/\bar{w}\}/u_k\} \approx t_j\{p_1\{\bar{b}/\bar{w}\}/u_1,\ldots,p_k\{\bar{b}/\bar{w}\}/u_k\}$$

which implies

$$s_j\{r_1^j/u_1,\ldots,r_k^j/u_k\}\{\bar{b}/\bar{w}\} \approx t_j\{p_1/u_1,\ldots,p_k/u_k\}\{\bar{b}/\bar{w}\}$$

and hence

$$s_j\{r_1^j/u_1,\ldots,r_k^j/u_k\} \approx t_j\{p_1/u_1,\ldots,p_k/u_k\}$$

By (3.19) this gives

$$s_j\{p_1\tau^j/u_1,\ldots,p_k\tau^j/u_k\} \approx t_j\{p_1/u_1,\ldots,p_k/u_k\}$$

or, equivalently

$$s_j\{p_1/u_1,\ldots,p_k/u_k\}\tau^j \approx t_j\{p_1/u_1,\ldots,p_k/u_k\}$$

By (3.15) we have

$$s_j\sigma\tau^j \approx t_j\sigma$$

Thus, $\langle\sigma,\tau^1,\ldots,\tau^n\rangle$ is a solution of $\mathcal{P}$.

Now we have to verify (3.7)–(3.10). Equation (3.7) follows from (3.13) and (3.15). Equation (3.8) follows from (3.12) and (3.15). Equation (3.9) follows from (3.14) and (3.16). Equation (3.10) follows from (3.17), (3.15) and (3.19). The proof of the ($\Leftarrow$) direction is completed.

The ($\Rightarrow$) direction of the lemma is similar. $\square$

Section 4

A decidable subcase of simultaneous rigid E-unification

In this section we prove the decidability of the simultaneous rigid E-unification problem in the signature consisting of one unary function symbol s and a countable number of constants. The proof is by reduction to the Diophantine problem for addition and divisibility that was proven decidable in [Beltyukov 76], [Lipshitz 78] and [Mart'janov 77]. While the proof of the decidability of this problem is not trivial, it is much simpler than the Makanin's proof of the decidability of word equations. Note that (using the standard coding technique) solving an arbitrary equation can be reduced to the case of a two-letter alphabet and hence, according to Section 2, to solving simultaneous rigid E-unification with just two unary function symbols.

The Diophantine problem for addition and divisibility is equivalent to the decidability of the class of formulas of the form

$$\exists x_1 \ldots \exists x_n \bigwedge_{i=1}^{k} A_i \tag{4.1}$$

in natural numbers, where A_i have the form $x_m = x_j + x_k$, $x_m \mid x_j$ or $x_m = p$ and p is a natural number, $\mid$ is the divisibility predicate.

The technique of Section 2 can be used to reduce the Diophantine problem for addition and divisibility to simultaneous rigid E-unification. As usual, for a word W and a natural number n we denote by W^n the word

$$\underbrace{W \ldots W}_{n \text{ times}}$$

Representing a natural number n by the word s^n, we can express the addition of two numbers m and n by the concatenation of the words s^m and s^n. In order to express divisibility, one can use the following trick.

Consider the following simultaneous rigid E-unification problem:

$$Gr(\{s, a_1\}, a_1) \vdash_{\forall} x_1 = a_1 \tag{4.2}$$

$$Gr(\{s, a_2\}, a_2) \vdash_{\forall} x_2 = a_2 \tag{4.3}$$

$$x_2 = a_2, a_1 = a_2 \vdash_{\forall} x_1 = a_1 \tag{4.4}$$

By Lemma 1.3, for any solution θ of (4.2), (4.3) we have $x_1\theta \approx Va_1$ and $x_2\theta \approx Wa_2$, where V, W are words in the alphabet $\{s\}$. This means that $x_1 \approx s^k a_1$ and $x_2 \approx s^l a_2$, for some natural numbers k, l. Consider (4.4). Assume $l > 0$ (the case $l = 0$ is obvious). The rewrite rule system

$$\begin{aligned} &a_1 \to a_2 \\ &s^l a_2 \to a_2 \end{aligned}$$

is perfect. By Lemma 1.1 we have $s^k a_1 \downarrow \approx a_1 \downarrow$. Note that $a_1 \downarrow \approx a_2$ and $s^k a_1 \downarrow \approx s^m a_2$, where m is the remainder of division of k by l. Then we have $l \mid k$.

Using the techniques of Section 2, this consideration can be changed into a complete proof of representability of the Diophantine problem for addition and divisibility in the simultaneous rigid E-unification problem.

We are interested in the opposite reduction of simultaneous rigid E-unification to the Diophantine problem with addition and divisibility. To this end we introduce several definitions.

For the rest of this section Σ will denote the signature $\{s, a_1, a_2, \ldots\}$, where s is a unary function symbol and a_i, $i \geq 1$ are constants.

Definition 4.1 *A* pseudo-term *is an expression of the form $s^n xa$, where n is a natural number, x is a variable and a is a constant. A* pseudo-equation *is an expression $s = t$, where s, t are either ground terms or pseudo-terms.*

Definition 4.2 *A* number substitution *σ is an expression of the form $[m_1/x_1, \ldots, m_n/x_n]$, where x_i are variables, m_i are natural numbers. The* domain *$dom(\sigma)$ of σ is the set $x_1, \ldots, x_n$. An* application *of a number substitution to an arbitrary expression E is the expression obtained from E by the simultaneous replacement of all occurrences of x_i by m_i.*

Using the above interpretation of n as s^n, we can treat a number substitution as a word substitution. For example, the application of the number substitution $[m/x]$ to the pseudo-term $s^n xa$ gives the term $s^n s^m a$, or simply $s^{n+m}a$.

The following definition generalizes the class of formulas used in (4.1).

Definition 4.3 *A D-*equation *is an atomic formula of the form $\mathrm{MB}(t_1, t_2, t_3, t_4)$ or of the form $t_1 \lambda t_2$, where λ is a binary relation among $=, |, <, \leq$ and t_i are terms constructed from natural numbers and variables using binary function symbols $+, \gcd$. An example of a D-equation is $\mathrm{MB}(\gcd(x_1, 18), 1, y+3, y)$.*

A solution *of a D-equation is any number substitution $[m_1/x_1, \ldots, m_n/x_n]$ which makes this D-equation true on natural numbers, where $\gcd(k, l)$ is interpreted as the greatest common divisor of k, l, the divisibility predicate $i \mid j$ is interpreted as "there is a natural number k such that $ik = j$" and $\mathrm{MB}(j, k, l, m)$ is interpreted as "$l \leq j < k \leq m$ and $k - l \mid m - j$".*

*A D-*problem *is any closed formula of the form*

$$\exists x_1 \ldots \exists x_n \bigwedge_{i=1}^{k} D_i \tag{4.5}$$

where all D_i are D-equations.

A solution *of such a D-problem is any number substitution that solves all D_i.*

Let us state some properties of gcd and MB:

Lemma 4.1 *Let j, k, l be natural numbers. Then $j = \gcd(k, l)$ iff $j \mid k$ and $j \mid l$ and there exist natural numbers d, e such that $kd = le + j$.*

Proof. Standard number theory.

□

Lemma 4.2 *Let k, l, m be natural numbers such that $l < k \leq m$. Then there exists a unique j such that* $\mathrm{MB}(j, k, l, m)$.

Proof. Obvious. □

In fact, this class of D-problems is an inessential generalization of formulas of the form (4.1):

Lemma 4.3 *The class of solvable D-problems is decidable.*

Proof. By reduction to the Diophantine problem for addition and divisibility. All we have to show is how to represent every relation and function symbol in D_i from (4.5) in terms of divisibility and addition with existential quantifiers and conjunctions as the only logical tools. A representation is given below:

$$\begin{aligned}
&x_j = \gcd(x_k, x_l) \Longleftrightarrow x_j \mid x_k \wedge x_j \mid x_l \wedge \exists y \exists z (x_k \mid y \wedge x_l \mid z \wedge y + x_j = z) \\
&x_j = x_k \Longleftrightarrow x_j \mid x_k \wedge x_k \mid x_j \\
&\mathrm{MB}(x_j, x_k, x_l, x_m) \Longleftrightarrow \; x_l \leq x_j \wedge x_j < x_k \wedge x_k \leq x_m \wedge \\
&\qquad\qquad\qquad\qquad\qquad \exists y \exists z (y + x_l = x_k \wedge z + x_j = x_m \wedge y \mid z)
\end{aligned}$$

The definition of gcd follows from Lemma 4.1. Other cases are obvious.

□

Definition 4.4 *An R-*equation *is any expression of the form $E \vdash_\forall F$, where E is a finite set of pseudo-equations and F is a pseudo-equation. The number substitution σ is a* solution *of such an R-equation iff $var(E, F) \subseteq dom(\sigma)$ and $E\sigma \models_\forall F\sigma$.*

*An R-*problem *is any expression of the form*

$$\exists x_1 \ldots \exists x_n \bigwedge_{i=1}^{k} R_i \tag{4.6}$$

where all R_i are R-equations all whose variables are in the set $\{x_1, \ldots, x_n\}$. A number substitution σ is a solution *of this problem iff it is a solution of all R_i.*

For example, the number substitution $[2/x, 0/y]$ is a solution of the R-equation $sxa_0 = ya_1 \vdash_\forall s^3ya_0 = a_1$.

The next definition puts together D-problems and R-problems:

Definition 4.5 *A DR-problem is any expression of the form*

$$\exists x_1 \ldots \exists x_n \bigwedge_{i=1}^{k} B_i \tag{4.7}$$

where every B_i is either a D-equation or an R-equation all whose variables are in the set $\{x_1, \ldots, x_n\}$.

A solution *of such a DR-problem (4.7) is any number substitution which solves all B_i.*

We say that a problem P is equivalent to a set of problems S to mean that P is solvable iff some problem in S is solvable. The main scheme of our decidability proof is as follows. We reduce an arbitrary simultaneous rigid E-unification problem P in the signature Σ to an equivalent finite set S of D-problems and then use the decidability of D-problems. This reduction is performed in two stages. First, we reduce a simultaneous rigid E-unification problem to a finite set of R-problems, and hence, DR-problems. Then we show that every DR-problem can be reduced to a finite set of D-problems.

Lemma 4.4 *For every simultaneous rigid E-unification problem in the signature Σ one can effectively find an equivalent finite set of R-problems.*

Proof. Let E be any rigid E-unification problem in the signature Σ with variables in $\{x_1, \ldots, x_n\}$ and constants in $a_1, \ldots, a_q$ and f be any mapping from $\{1, \ldots, n\}$ to $\{1, \ldots, q\}$. Denote by E_f the expression obtained from E by replacing all occurrences of variables x_i by $x_i a_{f(i)}$. For example, if E has the form

$$s^3 x_1 = x_2 \vdash_\forall x_2 = x_3$$

and $f(1) = 1, f(2) = 2, f(3) = 4$, then E_f is

$$s^3 x_1 a_1 = x_2 a_2 \vdash_\forall x_2 a_2 = x_3 a_4$$

Denote the set of all mappings from $\{1, \ldots, n\}$ to $\{1, \ldots, q\}$ by $\mathcal{M}$.

Let P be a simultaneous rigid E-unification problem. Consider the set S of R-problems defined by

$$S \rightleftharpoons \{\exists x_1 \ldots \exists x_n (\bigwedge_{E \in P} E_f) \mid f \in \mathcal{M}\}$$

We show that P and S are equivalent.

Assume that P has a solution. By Lemma 1.2, P has a ground solution σ. All ground terms of Σ have the form $s^m(a_i)$, where m is a natural number and $1 \le i \le q$. Let σ have the form $\{s^{m_1}(a_{i_1})/x_1, \ldots, s^{m_n}(a_{i_n})/x_n\}$. Consider f defined by $f(j) \rightleftharpoons i_j$. Then obviously the number substitution $[m_1/x_1, \ldots, m_n/x_n]$ is a solution for

$$\exists x_1 \ldots \exists x_n (\bigwedge_{E \in S} E_f)$$

The reverse direction is similar. Let for some $f \in \Phi$ the number substitution $[m_1/x_1, \ldots, m_n/x_n]$ be a solution for

$$\exists x_1 \ldots \exists x_n (\bigwedge_{E \in S} E_f)$$

Then $\{s^{m_1}(a_{f(1)})/x_1, \ldots, s^{m_n}(a_{f(n)})/x_n\}$ is a solution of S.

□

Definition 4.6 *An R-equation E is called* regular *iff for every pseudo-equation $t_1 a_i = t_2 a_j$ occurring in E both expressions t_1 and t_2 are variables. A DR-problem P is* regular *iff all R-equations in P are regular.*

Lemma 4.5 *Given any DR-problem P, one can effectively find a regular DR-problem P' equivalent to P.*

Proof. We can get rid of all non-regular R-equations using the following trick.

1. Assume that the pseudo-term $s^p x_k a_i$ occurs in the DR-problem $\exists x_1 \ldots \exists x_n B$. Let B' be obtained from B by replacing this occurrence of $s^p x_k a_i$ by $x_{n+1} a_i$. Then this DR-problem is equivalent to $\exists x_1 \ldots \exists x_{n+1}(x_{n+1} = x_k + p \wedge B')$.

2. Assume that the term $s^p a_i$ occurs in the DR-problem $\exists x_1 \ldots \exists x_n B$. Let B' be obtained from B by replacing this occurrence of $s^p a_i$ by $x_{n+1} a_i$. Then this DR-problem is equivalent to $\exists x_1 \ldots \exists x_{n+1}(x_{n+1} = p \wedge B')$.

□

Definition 4.7 *The* height *of an R-equation E is the sum of the indices of all occurrences of symbols a_i. For example, the height of the R-equation*

$$s^3 x_1 a_1 = x_4 a_2,\ s^2 x_1 a_2 = s x_3 a_3 \vdash_\forall x_1 a_1 = x_2 a_6$$

is $1 + 2 + 2 + 3 + 1 + 6 = 15$. The height *of a DR-problem B is the sum of the heights of all R-equations occurring in B.*

Definition 4.8 *Let E be a DR-problem of the form*

$$\exists x_1 \ldots \exists x_n \bigwedge_{i=1}^{k} B_i \tag{4.8}$$

It is called completely ordered *iff for every $j \in \{1, \ldots, n-1\}$, one of B_i has the form $x_j < x_{j+1}$.*

Our reduction consists of steps decreasing the height of a DR-problem until the height becomes 0, i.e. we obtain a set of D-problems. The steps will be of two kinds. On steps of the first kind we reduce an arbitrary DR-problem to an equivalent set of completely ordered DR-problems of the same height. On the steps of the second kind we reduce an arbitrary completely ordered DR-problem to an equivalent (not necessarily completely ordered) DR-problem of a smaller height.

Lemma 4.6 *Given any DR-problem P of the height h, one can effectively find an equivalent set S of completely ordered DR-problems of the same height.*

Proof. Let B be any conjunction of DR-equations. Denote by $B_{x_i \leftarrow x_j}$ the expression obtained from B by replacing all occurrences of x_i by x_j. The lemma follows from the fact that the DR-problem

$$\exists x_1 \ldots \exists x_n B$$

is equivalent to the set of three DR-problems

$$\exists x_1 \ldots \exists x_n (x_i < x_j \wedge B), \exists x_1 \ldots \exists x_n (x_j < x_i \wedge B), \exists x_1 \ldots \exists x_n B_{x_i \leftarrow x_j}$$

Note that all these DR-problems have the height h.

Using this fact, we can reduce a DR-problem to an equivalent set of completely ordered DR-problems, renaming variables if necessary.

□

We introduce a linear ordering $\succ$ on the set of ground terms of the signature σ:

Definition 4.9 *The* ordering $\succ$ *on* T_Σ *is defined as follows:* $t_1 \succ t_2$ *iff one of the following is true:*

1. t_2 *is a proper subterm of* t_1*;*
2. $t_1 \approx s^n a_i$, $t_2 \approx s^m a_j$ *and* $i > j$.

Although we do not state it explicitly, the technique used in several lemmas below is in fact based on simplifications w.r.t. the reduction ordering $\succ$. We shall note that the result of such simplifications is predictable, i.e. the rewrite system obtained from a given set of equations by ordering and simplification can be described using D-equations.

Definition 4.10 *Let* E_1, E_2 *be two sets of equations. Then* $E_1 \equiv_\forall E_2$ *means that for every* $(s = t) \in E_2$ *we have* $E_1 \models_\forall s = t$*, and for every* $(s' = t') \in E_1$ *we have* $E_2 \models_\forall s' = t'$.

The following lemma states that a subset of equations in a rigid E-unification problem can be replaced by a set of equations equivalent w.r.t. $\equiv_\forall$:

Lemma 4.7 *Let* E_1, E_2 *be two sets of equations. The following conditions are equivalent:*

1. $E_1 \equiv_\forall E_2$*;*
2. *For every set of equations* E *and equation* $s = t$ *we have* $E, E_1 \models_\forall s = t$ *iff* $E, E_2 \models_\forall s = t$.

Proof. Obvious. □

Lemma 4.8 *Let* j, k, l, m, n *be natural numbers such that* $l < j, m \leq l, m < k$ *and* $n = \gcd(j - l, k - m) + m$. *Then* $s^j a_i = s^l a_i, s^k a_i = s^m a_i \equiv_\forall s^n a_i = s^m a_i$.

Proof.

1. Since $n - m = \gcd(j - l, k - m)$ we have $d(n - m) = j - l$, for some natural number d. Applying the rewrite rule $s^n a_i \to s^m a_i$ d times to $s^j a_i$, we obtain $s^l a_i$. Hence, $s^n a_i = s^m a_i \models_\forall s^j a_i = s^l a_i$. Similarly, $s^n a_i = s^m a_i \models_\forall s^k a_i = s^m a_i$.
2. By Lemma 4.1, there are numbers d, e such that $(j - l)d = (k - m)e + (n - m)$. Let p be any number such that $(k - m)p \geq l$. Applying the rewrite rule $s^m a_i \to s^k a_i$ to $s^n a_i$ $p + e$ times we get $s^{n+(k-m)p+(k-m)e} a_i$. Applying to $s^m a_i$ the rewrite rule $s^m a_i \to s^k a_i$ p times and then the rewrite rule $s^l a_i \to s^j a_i$ d times, we obtain $s^{m+(k-m)p+(j-l)d} a_i$. Thus, $s^j a_i = s^l a_i, s^k a_i = s^m a_i \models_\forall s^{n+(k-m)p+(k-m)e} a_i = s^n a_i$ and $s^j a_i = s^l a_i, s^k a_i = s^m a_i \models_\forall s^{n+(k-m)p+(j-l)d} a_i = s^m a_i$. It suffices to note that $n + (k - m)p + (k - m)e = m + (k - m)p + (j - l)d$.

□

Lemma 4.9 *Let* k, l, m, n, p *be natural numbers such that* $l < k \leq m$ *and* $\mathrm{MB}(n, k, l, m)$. *Then* $s^k a_i = s^l a_i, s^m a_i = s^p a_j \equiv_\forall s^k a_i = s^l a_i, s^n a_i = s^p a_j$.

Proof. By the definition of MB we have $k - l \mid m - n$, i.e. there is a natural number d such that $(k - l)d = m - n$. Since $n \geq l$, we can apply the rewrite rule $s^l a_i \to s^k a_i$ d times to $s^n a_i$, obtaining $s^m a_i$. Thus $s^l a_i = s^k a_i \models_\forall s^n a^i = s^m a^i$. The claim of the lemma follows immediately.

□

Lemma 4.10 *Let k, l, m, n, p be natural numbers such that $l < k, m < k$ and $n = k - m + p$. Then $s^k a_i = s^l a_i, s^m a_i = s^p a_j \equiv_\forall s^l a_i = s^n a_j, s^m a_i = s^p a_j$.*

Proof. Obvious.

□

Lemma 4.11 *Let k, l, m, n, p, r be natural numbers such that $l < k \leq m$, $\mathrm{MB}(n, k, l, m)$ and $r = k - n + p$. Then $s^k a_i = s^l a_i, s^m a_i = s^p a_j \equiv_\forall s^l a_i = s^r a_j, s^n a_i = s^p a_j$.*

Proof. By Lemma 4.9 $s^k a_i = s^l a_i, s^m a_i = s^p a_j \equiv_\forall s^k a_i = s^l a_i, s^n a_i = s^p a_j$. Note that $\mathrm{MB}(n, k, l, m)$ implies $n < k$. By Lemma 4.10 $s^k a_i = s^l a_i, s^n a_i = s^p a_j \equiv_\forall s^l a_i = s^r a_j, s^n a_i = s^p a_j$.

□

Lemma 4.12 *Let r, l, m, n, p be natural numbers such that $m \leq r$ and $n = r - m + p$. Then $s^r a_i = s^l a_j, s^m a_i = s^p a_k \equiv_\forall s^n a_k = s^l a_j, s^m a_i = s^p a_k$.*

Proof. Obvious.

□

The following definition introduces the notion of a *final* rigid E-unification problem $E \vdash_\forall F$ and corresponding notion of a final DR-problem. As we show below, final rigid E-unification problems $E \vdash_\forall F$ have certain good properties: after orientation according to $\succ$, E becomes a perfect system and the reduction of a term t to its normal form $t\downarrow$ w.r.t. E can be expressed in the language of D-equations.

Definition 4.11 *Let $E \vdash_\forall F$ be a ground rigid E-unification problem or an R-equation in the signature Σ. It is called* final *iff E contains no pseudo-equations of the form $t = t$ and for every constant $a_i \in \Sigma$ there is at most one pseudo-equation in E of the form $ua_i = va_j$ for which $j \leq i$.*

A DR-problem S is final *iff all R-equations in it are final.*

Lemma 4.13 *Let $E \vdash_\forall F$ be a ground final rigid E-unification problem in the signature Σ. Let E' be a rewrite system obtained by orienting E according to $\succ$. Then E' is perfect.*

Proof. Obviously, E' is noetherian. For every term t there is at most one rewrite rule in E' applicable to t. Hence, t satisfies the diamond property.

□

Lemma 4.14 *Given any non-final regular DR-problem P, one can effectively find an equivalent set S of regular DR-problems of a smaller height.*

Proof. By Lemma 4.6, we can assume that P is completely ordered. Let P have the form

$$\exists x_1 \ldots \exists x_n (E \vdash_\forall F \wedge \Phi)$$

such that $E \vdash_\forall F$ is non-final. We show how to obtain a regular problem P' equivalent to P and having a smaller height. Since P is non-final, one of the following three conditions holds:

1. *There is $a_i \in \Sigma$ such that E contains two different equations $x_j a_i = x_l a_i$ and $x_k a_i = x_m a_i$.* If $j = l$ (or $m = k$), we can remove $x_j a_i = x_l a_i$ (or $x_m a_i = x_k a_i$) obtaining an equivalent system with a smaller height. By symmetry, we can assume $l < j, m \leq l, m < k$. Let E' be obtained from E by replacement of $x_j a_i = x_l a_i, x_k a_i = x_m a_i$ by $x_{n+3} a_i = x_m a_i$, and let $\mathcal{P}'$ be

$$\begin{aligned}\exists x_1 \ldots \exists x_n \exists x_{n+1} \exists x_{n+2} \exists x_{n+3}\ & (x_{n+1} + x_l = x_j \wedge x_{n+2} + x_m = x_k \wedge \\ & x_{n+3} = x_m + \gcd(x_{n+1}, x_{n+2}) \wedge E' \vdash_\forall F \wedge \Phi)\end{aligned}$$

By Lemmas 4.8 and 4.7, P is equivalent to P'.

2. *There are $a_i, a_j \in \Sigma$ such that $i > j$ and E contains equations $x_k a_i = x_l a_i$ and $x_m a_i = x_p a_j$.* If $k = l$, then $x_k a_i = x_l a_i$ can be removed from E, obtaining an equivalent problem with a smaller height. By symmetry, we can assume $l < k$. Consider two possible cases

   (a) $k > m$. By Lemmas 4.10 and 4.7, P is equivalent to the problem P' of the form

   $$\exists x_1 \ldots \exists x_n \exists x_{n+1} (x_{n+1} + x_m = x_k + x_p \wedge E' \vdash_\forall F \wedge \Phi)$$

   where E' is obtained from E by replacing $x_k a_i = x_l a_i$ by $x_{n+1} a_j = x_l a_i$.

   (b) $k \leq m$. By Lemmas 4.11 and 4.7, P is equivalent to the problem P' of the form

   $$\begin{aligned}\exists x_1 \ldots \exists x_n \exists x_{n+1} \exists x_{n+2}\ & (\mathrm{MB}(x_{n+1}, x_k, x_l, x_m) \wedge x_{n+2} + x_{n+1} = x_k + x_p \wedge \\ & E' \vdash_\forall F \wedge \Phi)\end{aligned}$$

   where E' is obtained from E by replacing $x_k a_i = x_l a_i, x_m a_i = x_p a_j$ by $x_l a_i = x_{n+2} a_j, x_{n+1} a_i = x_p a_j$.

3. *There are $a_i, a_j, a_k \in \Sigma$ such that $i > j$, $i > k$ and E contains two different equations $x_r a_i = x_l a_j$ and $x_m a_i = x_p a_k$.* By symmetry, we can assume $m \leq r$. By Lemma 4.12, P is equivalent to the problem P' of the form

   $$\exists x_1 \ldots \exists x_n \exists x_{n+1} (x_{n+1} + x_m = x_r + x_p \wedge E' \vdash_\forall F \wedge \Phi)$$

   where E' is obtained from E by replacing $x_r a_i = x_l a_j$ by $x_{n+1} a_k = x_l a_j$.

It is easy to check that in all cases the height of P' is smaller than the height of P.

□

The following lemma in fact gives an algorithm for computing normal forms of terms in final rigid E-unification problems.

Lemma 4.15 *Let $E \vdash_\forall F$ be a ground final rigid E-unification problem in the signature Σ. Let E' be obtained from E by orienting all equations w.r.t. $\succ$, i.e. $(s \rightarrow t) \in E'$ iff $s = t \in E$ and $s \succ t$. Then*

$$s^m a_i \downarrow = \begin{cases} s^n a_i, \text{ where } \mathrm{MB}(n,k,l,m) & \text{if } (s^k a_i \rightarrow s^l a_i) \in E' \text{ and } k \leq m \\ s^{m-k+l} a_j \downarrow & \text{if } (s^k a_i \rightarrow s^l a_j) \in E',\ i > j \text{ and } k \leq m \\ s^m a_i & \text{otherwise} \end{cases}$$

Proof. Straightforward. □

We shall use this lemma to make the final step in the reduction of DR-problems to D-problems.

Lemma 4.16 *Given a final regular DR-problem P of the height > 0, one can effectively find an equivalent set of regular DR-problems with a smaller height.*

Proof. In view of Lemma 4.6, we can assume that P is completely ordered. Let P have the form

$$\exists x_1 \ldots \exists x_n (E \vdash_\forall F \wedge \Phi) \tag{4.9}$$

Consider the following cases. In each of the cases we shall explicitly show a problem P' equivalent to P.

1. F has the form $t = t$. Then let $P' \rightleftharpoons \exists x_1 \ldots \exists x_n \Phi$. The equivalence of P and P' is obvious.
2. F has the form $x_m a_i = x_p a_i$, $m \neq p$ and E contains an equation $x_k a_i = x_l a_i$, where $k \leq m, k \leq p$ and $k > l$. Then define P' by

   $$\exists x_1 \ldots \exists x_n \exists x_{n+1} (\mathrm{MB}(x_{n+1}, x_k, x_l, x_m) \wedge \mathrm{MB}(x_{n+1}, x_k, x_l, x_p) \wedge \Phi)$$

   The equivalence of P and P' follows from the properties of perfect systems of rewrite rules (Lemma 1.1) and from Lemma 4.15.
3. F has the form $x_m a_i = x_p a_i$ and E contains an equation $x_k a_i = x_l a_i$, where $k \leq m, k > p$ and $k > l$. Define P' by

   $$\exists x_1 \ldots \exists x_n (\mathrm{MB}(x_p, x_k, x_l, x_m) \wedge \Phi)$$

   The proof is as in the case 2.
4. F has the form $x_m a_i = t$ and E contains an equation $x_k a_i = x_l a_j$, where $i > j$ and $k \leq m$. Define P' by

   $$\exists x_1 \ldots \exists x_n \exists x_{n+1} (E \vdash_\forall x_{n+1} a_j = t \wedge x_{n+1} + x_k = x_m + x_l \wedge \Phi)$$

   The proof is as in case 2.
5. If none of the previous cases is applicable then by Lemmas 1.1 and 4.15 P has no solution and can be replaced by any unsolvable D-problem, e.g. $\exists x_1 (x_1 < x_1)$.

It is easy to see that in all cases P' has a smaller height than P. □

Lemma 4.17 *There is an algorithm that transforms a simultaneous rigid E-unification problem P in the signature Σ into an equivalent set of D-problems.*

Proof. Combining Lemmas 4.4, 4.5, 4.14 and 4.16 we obtain that P can be reduced to a set of regular DR-problems of the height 0, i.e. D-problems. □

This lemma and Lemma 4.3 yield

Theorem 4.1 *The simultaneous rigid E-unification problem for the signature consisting of one unary function symbol and a countable number of constants is decidable.*

Note that if we consider the reduction as a non-deterministic algorithm, we can prove that the Diophantine problem for addition and divisibility is in NP iff simultaneous rigid E-unification in signature with one unary function symbol is in NP. However, it is not known whether the Diophantine problem for addition and divisibility is in NP [Lipshitz 81].

The above reduction shows that there can hardly be a simple direct decidability proof even for the case with one unary function symbol because proofs of the decidability of the Diophantine problem for addition and divisibility use deep number-theoretic facts.

We hope that our technique can be generalized so that monadic simultaneous rigid E-unification will be proven decidable by reduction to the word equation problem. Such a result could have shed new light on the complexity of the word equation problem. However it is hardly possible that the technique of this section can be generalized to prove the decidability of simultaneous rigid E-unification in the general case.

Bibliography

[Andrews 81] P.B. Andrews. Theorem proving via general matings. *Journal of the Association for Computing Machinery*, 28(2):193–214, 1981.

[BecPet 94] G. Becher and U. Petermann. Rigid unification by completion and rigid paramodulation. In B. Nebel and L. Dreschler-Fischer, editors, *KI-94: Advances in Artificial Intelligence. 18th German Annual Conference on Artificial Intelligence*, volume 861 of *Lecture Notes in Artificial Intelligence*, pages 319–330, Saarbrücken, Germany, September 1994. Springer Verlag.

[Beltyukov 76] A.P. Beltyukov. Decidability of the universal theory of natural numbers with addition and divisibility (in Russian). *Zapiski Nauchnyh Seminarov LOMI*, 60:15–28, 1976. English translation in: Journal of Soviet Mathematics.

[BeKaNa 87] D. Benanav, D. Kapur, and P. Narendran. Complexity of matching problems. *Journal of Symbolic Computations*, 3:203–216, 1987.

[Bibel 87] W. Bibel. *Automated theorem proving.* Vieweg Verlag, 1987. 2nd edition.

[DegVor 94a] A. Degtyarev and A. Voronkov. A new procedural interpretation of Horn clauses with equality. UPMAIL Technical Report 89, Uppsala University, Computing Science Department, November 1994.

[DegVor 94b] A. Degtyarev and A. Voronkov. Equality elimination for semantic tableaux. UPMAIL Technical Report 90, Uppsala University, Computing Science Department, December 1994.

[DegVor 94c] A. Degtyarev and A. Voronkov. Equality elimination for the inverse method and extension procedures. UPMAIL Technical Report 92, Uppsala University, Computing Science Department, December 1994.

[DegVor 95a] A. Degtyarev and A. Voronkov. General connections via equality elimination. UPMAIL Technical Report 93, Uppsala University, Computing Science Department, January 1995.

[DeKoVo 95b] A. Degtyarev, Yu. Koval, and A. Voronkov. Handling equality in logic programming via basic folding. UPMAIL Technical Report 101, Uppsala University, Computing Science Department, March 1995.

[DerJou 90] 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.

[Fitting 88] M. Fitting. First-order modal tableaux. *Journal of Automated Reasoning*, 4:191–213, 1988.

[GNPS 88] J.H. Gallier, P. Narendran, D. Plaisted, and W. Snyder. Rigid E-unification is NP-complete. In *Logic in Computer Science (LICS'88) (Edinburgh, Scotland)*, pages 338–346. IEEE Computer Society Press, July 1988.

[GNRS 92] J. Gallier, P. Narendran, S. Raatz, and W. Snyder. Theorem proving using equational matings and rigid E-unification. *Journal of the Association for Computing Machinery*, 39(2):377–429, 1992.

[GRS 87] J.H. Gallier, S. Raatz, and W. Snyder. Theorem proving using rigid E-unification: Equational matings. In *Logic in Computer Science (LICS'87) (Ithaca, N.Y.)*, pages 338–346. IEEE Computer Society Press, 1987.

[Goubault 93a] J. Goubault. *Démonstration Automatique en Logique Classique: Complexité et Méthodes.* PhD thesis, Laboratoire d'informatique de l'école polytechnique, 1993.

[Goubault 93b] J. Goubault. A rule-based algorithm for rigid E-unification. In Georg Gottlob, Alexander Leitsch, and Daniele Mundici, editors, *Computational Logic and Proof Theory. Proceedings of the Third Kurt Gödel Colloquium, KGC'93*, volume 713 of *Lecture Notes in Computer Science*, pages 202–210, Brno, August 1993.

[Goubault 93c] J. Goubault. Simultaneous rigid E-unification is NEXPTIME-complete. Technical Report 93045, Bull, 1993.

[Goubault 93d] J. Goubault. Simultaneous rigid E-unification is NEXPTIME-complete (correction). Technical Report 93047, Bull, 1993.

[Goubault 94] J. Goubault. Rigid $\vec{E}$-unifiability is DEXPTIME-complete. In *Logic in Computer Science (LICS'94)*. IEEE Computer Society Press, 1994.

[Henglein 88] F. Henglein. Type inference and semi-unification. In *Proceedings of the 1988 ACM Conference on LISP and Functional Programming*, pages 184–197, Snowbird, Utah, USA, July 25–27 1988.

[HueOpe 80] G. Huet and D.C. Oppen. Equations and rewrite rules. In Book, editor, *Formal Languages: Perspectives and Open Problems.* Academic Press, 1980.

[Kanger 63] S. Kanger. A simplified proof method for elementary logic. In J. Siekmann and G. Wrightson, editors, *Automation of Reasoning. Classical Papers on Computational Logic*, volume 1, pages 364–371. Springer Verlag, 1983. Originally appeared in 1963.

[KMNS 88] D. Kapur, D. Musser, P. Narendran, and J. Stillman. Semi-unification. In *Proceedings of the 8th Conference on Foundations of Software Technology and Theoretical Computer Science*, volume 338 of *Lecture Notes in Computer Science*, pages 435–454, Pune, India, December 21–23 1988. Springer Verlag.

[KfTiUr 89] A.J. Kfoury, J. Tiuryn, and P. Urzyczyn. Computational consequences and partial solutions of a generalized unification problem. In *Fourth IEEE Symposium on Logic in Computer Science*, Asilomar, CA, June 5–8 1989.

[KfTiUr 93] A.J. Kfoury, J. Tiuryn, and P. Urzyczyn. The undecidability of the semi-unification problem. *Information and Computation*, 102:83–101, 1993.

[LanMus 78] D.S. Lankford and D.R. Musser. A finite termination criterion. Technical report, USC Information Sciences Institute, Marina del Rey, CA, 1978.

[Leiß 89] H. Leiß. Semi-unification and type inference for polymorphic recursion. Technical Report INF2-ASE-5-89, Siemens AG, Munich, May 1989.

[Leiß 90] H. Leiß. Polymorphic recursion and semi-unification. In E. Börger, G. Jäger, H. Kleine Büning, and M.M. Richter, editors, *CSL'89 (Proc. 3rd Workshop on Computer Science Logic)*, volume 440 of *Lecture Notes in Computer Science*, pages 211–224, Kaiserslautern, Germany, 1990. Springer Verlag.

[Lipshitz 78] L. Lipshitz. The Diophantine problem for addition and divisibility. *Transactions of the American Mathematical Society*, 235:271–283, January 1978.

[Lipshitz 81] L. Lipshitz. Some remarks on the Diophantine problem for addition and divisibility. *Bull. Soc. Math. Belg. Sér. B*, 33(1):41–52, 1981.

[Loveland 68] D.W. Loveland. Mechanical theorem proving by model elimination. *Journal of the Association for Computing Machinery*, 15:236–251, 1968.

[Makanin 77] G.S. Makanin. The problem of solvability of equations in free semigroups. *Mat. Sbornik (in Russian)*, 103(2):147–236, 1977. English Translation in Math. USSR Sbornik, 32, 1977.

[Mart'janov 77] V.I. Mart'janov. Universal extended theories of integers. *Algebra i Logika*, 16(5):588–602, 1977.

[Maslov 67] S.Yu. Maslov. An invertible sequential variant of intuitionistic predicate calculus (in Russian). *Zapiski Nauchnyh Seminarov LOMI*, 4:96–111, 1967.

[Matiyasevič 68] Yu.V. Matiyasevič. A connection between systems of word and length equations and Hilbert's tenth problem (in Russian). *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, 8:132–144, 1968. English Translation in: Sem. Math. V.A. Steklov Math. Inst. Leningrad 8 (1968).

[Prawitz 60] D. Prawitz. An improved proof procedure. In J. Siekmann and G. Wrightson, editors, *Automation of Reasoning. Classical Papers on Computational Logic*, volume 1, pages 162–201. Springer Verlag, 1983. Originally appeared in 1960.

[Pudlák 88] P. Pudlák. On a unification problem related to Kreisel's conjecture. *Mathematicae Universitatis Carolinae*, 29(3):551–556, 1988.

[Schulz 90] K.U. Schulz, editor, *Word Equations and Related Topics*, volume 572 of *Lecture Notes in Computer Science,* pages 1–12, Tübingen, Germany, October 1990.