Masaryk University Brno
Faculty of Sciences

Unification Modulo Associativity and Idempotency (Abstract of Ph.D. thesis)

Ondřej Klíma

Brno, August 2003

Mathematics Subject Classification: 20M05, 68Q17, 68W30, 08B20.

1 Introduction

Unification is a fundamental process upon which many methods for automated deduction are based. Simply speaking, unification theory deals with solving equations. We consider *terms* that are built from function symbols (say f, a and b, where f is binary and a, b are nullary) and variables (say x and y). An instance of a *unification problem* is a pair of terms (an *equation*). The question is whether it is possible to replace the variables by terms such that the two terms obtained in this way are (syntactically) equal (i.e. whether there exists a *unifier* of the terms). For example, if $f(x,b) =^? f(f(a,b),y)$ is an equation, then we can see that there is a unifier $\{x \mapsto f(a,b), y \mapsto b\}$. For the equation $f(a,x) =^? f(x,b)$ there is no unifier, and for the equation $f(x,y) =^? f(y,x)$ there are infinitely many unifiers. Fortunately, if there is a unifier then there is a *most general unifier*, which has the property that any other unifier can be obtained from it by substitution. In the last example, $\{x \mapsto y\}$ is such a most general unifier.

This kind of unification is called *syntactic* unification. A different concept is obtained if one considers function symbols satisfying certain semantic properties. The most natural notion is *equational* unification where the symbols satisfy a given equational theory E (a set of identities). We speak about the E-*unification problem*. Now the question is whether there exists a unifier which makes terms equivalent with respect to the fully invariant congruence of the algebra of all terms generated by E.

For example, if $E = \{f(x,x) \doteq a\}$, then the equation $f(x,b) =^? f(f(a,b),y)$ has also an E-unifier $\{x \mapsto b, y \mapsto f(a,b)\}$. From the point of view of universal algebra, the syntactic unification problem is solving of equations in a algebra of all terms, and the E-unification problem is solving them in a relatively free algebra in the variety corresponding to the set of identities E. For equational unification, things are not as nice as for syntactic unification. In fact, depending on the theory E, the E-unification problem may be undecidable[1], and even if it is decidable, solvable equations need not have a most general E-unifier. Classification of equational theories according to their behavior in this respect is a rather interesting question of unification theory. In the case of syntactic unification any system is equivalent to a single equation. In the case of equational unification it is not true, and therefore consideration of systems of equations is more general.

The name “unification” and the first formal investigation of this notion is due to J. A. Robinson [18], who introduced unification as the basic operation of his resolution principle, showed that unifiable terms have a most general unifier and described an algorithm for computing this unifier. The resolution principle is the base of many automated provers.

The notions of “unification” and “most general unifier” were independently reinvented by Knuth and Bendix [13] as a tool for testing term rewriting systems for local confluence by computing critical pairs. Equational unification was introduced both in resolution-based theorem proving and in term rewriting as a means for treating certain troublesome equational axioms (like associativity and commutativity) in a special manner. For example, in term rewriting, the axiom $f(x,y) \doteq f(y,x)$ cannot be oriented into terminating rewrite rules. One way of solving this problem is to take such non-orientable identities completely out of the rewrite process, and perform rewriting with respect to the remaining (orientable) rules modulo the unoriented ones. Another area where we can find applications of unification theory is logic programming.

If the E-unification problem is decidable, then other questions are the complexity of the problem and a description of the set of all unifiers. There is a natural generalization of the concept of a most general unifier, namely a minimal complete set of unifiers, i.e. a set M having the property that any unifier can be obtained from some unifier from M by substitution and that the unifiers in M are independent in the sense that one can not be obtained from another one. If a minimal complete set of unifiers exists, it is determined uniquely up to equivalence of unifiers. It is empty if the system has no unifier.

In the literature, there are often discussed the theories of associativity (A), commutativity (C), idempotency (I) and their combinations. The decidability of the A-unification problem, i.e. solving of word equations, has been open for a long time.

[1] Such a theory is, for example, the theory of commutative rings with a unit for which the unification problem is just the well known Hilbert's tenth problem.

The original (deep) proof of its decidability by Makanin [14] (the algorithm using the Makanin's proof is in 3-NEXPTIME) was improved by Plandowski [16] (his algorithm is in PSPACE). On the other hand, it is not hard to prove that the problem is NP-hard. It was shown by Plotkin [17] that any system of word equations has a minimal complete set of unifiers, although it can be infinite. The AC-unification problem is decidable in polynomial time and a minimal complete set of unifiers always exists and it is finite. Another theories for which a numerous interesting results were established are the theories of groups, abelian groups, commutative and boolean rings (see [3, 4, 8, 20] for surveys on the area).

In the center of our interest in the thesis is the AI-unification problem, i.e. the unification problem for the theory of one associative and idempotent fiunction symbol. The problem is decidable because idempotent semigroups are locally finite (i.e. each finitely generated idempotent semigroup is finite, hence for any system we have to check only finitely many substitutions for being unifiers). AI-unification is important for unification theory, because it is a natural example of a theory for which a system without a minimal complete set of unifiers exists. It was proved independently by Baader [1] and Schmidt-Schauss [19]. Some results concerning the complexity of the problem were established in [7] and minimal complete sets of unifiers were studied in [2]. We simultaneously study the AIU-unification problem, where the theory contains in addition a unit. There is no substantial difference between these theories.

2 Overview

The thesis is based mainly on the material concerning the AI-unification problems that has been published previously. The original articles have been, of course, further elaborated. The structure of the thesis is the following. Each article comprises one separate chapter: paper [11] is included in Chapter 2, paper [9] in Chapter 3 and paper [10] in Chapter 4. The material in Chapter 5 will be contained in article [12], currently in preparation.

Chapter 1 contains technical notation used in the thesis. The second chapter contains the proof of the NP-completeness of the AI-matching problem, a special case of the AI-unification problem where only equations with variable-free right hand sides are considered. The main result of the thesis is contained in Chapter 3, where we prove that also the AI-unification problem is NP-complete. In Chapter 4 we consider the unification problem in the theory of a single associative and idempotent function symbol which satisfies some additional identities. A dichotomy theorem for these theories is established. We drop the subject of unification theory in Chapter 5 which contains a quite independent research. Here, we consider equations not in a free semigroup but in a given concrete finite semigroup. The last chapter simply summarizes the main results of the thesis.

3 Background and Notations

A *signature* $\mathscr{F}$ is a (finite or countably infinite) set of function symbols together with their arities. For a (contably) infinite set of variables X we denote by $\mathscr{T}(\mathscr{F},X)$ the term algebra (or absolutely free algebra) generated in a signature $\mathscr{F}$ by the set X.

An *equational theory* is a set of identities $\mathrm{E} \subseteq \mathscr{T}(\mathscr{F},X) \times \mathscr{T}(\mathscr{F},X)$. We denote by $=_{\mathrm{E}}$ the least congruence relation of the term algebra $\mathscr{T}(\mathscr{F},X)$ that is closed under substitutions (so-called *fully invariant congruence*) and contains E. From another point of view, we can consider the class $\mathscr{V} = \mathrm{Mod}(\mathrm{E})$ consisting of all algebras of signature $\mathscr{F}$ which satisfy all identities from the set E. The class $\mathscr{V}$ is called a *variety*. Now, the fully invariant congruence $=_{\mathrm{E}} \subseteq \mathscr{T}(\mathscr{F},X) \times \mathscr{T}(\mathscr{F},X)$ is the set of all identities which are satisfied in all algebras in $\mathscr{V}$ and the factoralgebra $\mathscr{T}(\mathscr{F},X)/{=_{\mathrm{E}}}$ is a free algebra over the set X in the variety $\mathscr{V}$.

For a given theory E, we denote by $\mathrm{Sig}(\mathrm{E})$ the set of all function symbols occurring in E. Symbols from the set $\mathscr{F} \setminus \mathrm{Sig}(\mathrm{E})$ are called *free*. An equational theory E is called *trivial* if $x =_{\mathrm{E}} y$ for two different variables x and y from X. We say that a function symbol $f \in \mathscr{F}$ is *independent* (in the theory E) if and only if the theory E is equivalent[2] to the theory $\mathrm{E}_f \cup \mathrm{E}'$, where the set E_f consists of all identities from E which contain only the function symbol f and the set E' consists of all identities from E which do not contain the function symbol f.

By a *system of equations* S we mean a finite set of equations $S = \{s_1 =^? t_1, \ldots, s_n =^? t_n\}$, where $s_1, t_1, \ldots, s_n, t_n \in \mathscr{T}(\mathscr{F},X)$. An E-*unifier* of the system S is a substitution $\sigma : \mathscr{T}(\mathscr{F},X) \to \mathscr{T}(\mathscr{F},X)$ such that $\sigma(s_i) =_{\mathrm{E}} \sigma(t_i)$ for all $i = 1, \ldots, n$.

1 Definition. Let E be an equational theory and $\mathscr{F}$ be a signature containing $\mathrm{Sig}(\mathrm{E})$. Given a system of equations S as an instance of the E-*unification problem*, the task is to decide whether this system S has an E-unifier.

Syntactic unification is the special case of this definition where $\mathrm{E} = \emptyset$. It is usual to distinguish the following variants of the E-unification problem in the literature.

2 Definition. An E-unification problem is an *elementary* E-unification problem iff $\mathscr{F} = \mathrm{Sig}(\mathrm{E})$; it is an E-unification problem *with constants* iff $\mathscr{F} \setminus \mathrm{Sig}(\mathrm{E})$ consists of infinitely many constant symbols; and it is a *general* E-unification problem iff $\mathscr{F} \setminus \mathrm{Sig}(\mathrm{E})$ contains infinitely many function symbols of every arity.

It was shown [5] that there exists an equational theory for which the elementary unification problem is decidable, but the unification problem with constants is undecidable. It is still an open problem whether there is such a gap between the unification with constants and the general unification. We recall the result which suggests that these two problems could be much closer.

[2] Two theories E and E' of signature $\mathscr{F}$ are *equivalent* if and only if for any pair of terms $s, t \in \mathscr{T}(\mathscr{F},X)$ we have $s =_{\mathrm{E}} t$ iff $s =_{\mathrm{E}'} t$.

3 Definition. Let $\mathscr{F} \setminus \mathrm{Sig}(\mathrm{E})$ contain only constant function symbols. An instance of the E-unification problem *with linear constant restriction* consists of a system S and a strict linear order $<$ on the set Γ_S of all variables and all free constant symbols occurring in S. The question is whether there exists an E-unifier σ of S that satisfies for all variables x and free constants c in Γ_S: $x < c \implies c$ does not occur in $\sigma(x)$.

4 Proposition ([3]). *Let* E *be an equational theory. The general* E*-unification problem is decidable (in NP) if and only if the* E*-unification problem with linear constant restriction is decidable (in NP).*

We recall an important modification of unification, namely matching. In E-matching we ask for an E-matcher of terms s and t, i.e. a substitution σ such that $\sigma(s) =_{\mathrm{E}} t$.

5 Definition. Let E be an equational theory and $\mathscr{F}$ be a signature containing Sig(E). Given a system of equations $S = \{s_1 =^? t_1, \ldots, s_n =^? t_n\}$ with terms $s_1, \ldots, s_n$ and ground[3] terms $t_1, \ldots, t_n$ as an instance of the *general* E*-matching problem*, the task is to decide whether there is a substitution $\sigma : \mathscr{T}(\mathscr{F}, X) \to \mathscr{T}(\mathscr{F}, X)$ such that $\sigma(s_i) =_{\mathrm{E}} t_i$ for all $i = 1, \ldots, n$. We speak about the E-*matching problem* if $\mathscr{F} \setminus \mathrm{Sig}(\mathrm{E})$ contains only constant symbols.

In the thesis we discuss unification problems for theories of associative and idempotent function symbols, so-called *ai-symbols*. Each theory of a single ai-symbol corresponds to a certain variety $\mathscr{V}$ of bands[4]; we speak about a $\mathscr{V}$*-symbol*. We meet especially the varieties from the bottom of the lattice of all varieties of bands which were assigned certain names in literature. Here is a list of some of them with the corresponding bases of identities. (The variety of all bands is denoted by $\mathscr{B}$.)

$\mathscr{R}\mathscr{B} = \mathrm{Mod}(x^2 \doteq x, xyxzx \doteq xyzx)$ – all regular bands,
$\mathscr{N}\mathscr{B} = \mathrm{Mod}(x^2 \doteq x, xyzx \doteq xzyx)$ – all normal bands,
$\mathscr{S}\mathscr{L} = \mathrm{Mod}(x^2 \doteq x, xy \doteq yx)$ – all semilattices,
$\mathscr{R}\mathscr{C}\mathscr{B} = \mathrm{Mod}(x^2 \doteq x, xyz \doteq xz)$ – all rectangular bands,

6 Lemma. *Let* E *consist of independent ai-symbols. Then the elementary* E*-unification problem is trivially decidable because any system of equations has a solution.*

Hence the crucial problem is the unification problem with constants because we are able to use Proposition 4 for the general unification problem as we show in Section 3.4. From these reasons we slightly rewrite previous general definitions for the case of unification with constants. Assume that $\mathscr{F} = C \cup \{\cdot\}$, where C is a set of free constants and $\cdot$ is an independent $\mathscr{V}$-symbol for a given variety of bands $\mathscr{V}$. (We add to $\mathscr{F}$ the constant symbol ε for neutral element when we consider AIU-unification.)

[3] A term is called *ground* if it contains no variable.
[4] A band is an idempotent semigroup, i.e a semigroup satisfying the identity $x^2 \doteq x$.

Because the symbol $\cdot$ is associative, we prefer to work with the congruence relation $\sim_{\mathscr{V},C}$ of the free semigroup C^+ (and the free monoid C^* respectively) corresponding to the variety $\mathscr{V}$ instead of the congruence relation $=_{\mathrm{E}}$ of the free groupoid $\mathscr{T}(\mathscr{F},X)$.

Let C be a (finite) set of *constants* and X be a (finite) set of *variables* such that $C \cap \mathrm{X} = \emptyset$. A *word equation* $L =^? R$ is a pair $(L,R) \in (C \cup \mathrm{X})^* \times (C \cup \mathrm{X})^*$. A *system of word equations* S is a finite set of equations, i.e. $S = \{L_1 =^? R_1, \ldots, L_n =^? R_n\}$ for $n \geq 0$. A *solution* of the system S in a variety of idempotent monoids $\mathscr{V}$ is a homomorphism $\alpha : (C \cup \mathrm{X})^* \to C^*$ which behaves as an identity on the set C and equates all the equations of S, i.e. $\alpha(L_i) \sim_{\mathscr{V},C} \alpha(R_i)$ for all $i = 1, \ldots, n$. If we want to work with a variety of bands, we consider the free semigroups instead of the free monoids.

We introduce the size of a solution α as $\mathrm{size}(\alpha) := \max_{x \in \mathrm{X}} |\alpha(x)|$, where $|u|$ denotes the length of a word u. A system of word equations $S = \{L_1 =^? R_1, \ldots, L_n =^? R_n\}$ is called a *matching system* if $R_i \in C^*$.

7 Definition. Let $\mathscr{V}$ be a variety of idempotent monoids or bands. Given a system of word equations $\{L_1 =^? R_1, \ldots, L_n =^? R_n\}$ with a set of variables X and a set of constants C as an instance of the $\mathscr{V}$-UNIFICATION problem, the task is to decide whether this system has a solution in the variety $\mathscr{V}$. The $\mathscr{V}$-MATCHING problem is the modification of the $\mathscr{V}$-UNIFICATION problem where only matching systems are considered.

We use standard terminology the AI-UNIFICATION and AIU-UNIFICATION problems instead of the $\mathscr{V}$-UNIFICATION problem in the case of the variety of all bands and idempotent monoids respectively. The same terminology is used for matching.

We recall a solution of the identity problem for bands. For $u \in C^*$ we define

$\mathsf{c}(u)$ – the set of all letters occurring in u,

$\overrightarrow{u}$ – the sequence of the first occurrences of all letters from $\mathsf{c}(u)$ in u,

$\overleftarrow{u}$ – the sequence of the last occurrences of all letters from $\mathsf{c}(u)$ in u,

$0(u)$ – the longest prefix of u which contains at most $u_\sharp - 1$ different letters,

$1(u)$ – the longest suffix of u which contains at most $u_\sharp - 1$ different letters,

with conventions $\overrightarrow{\varepsilon} = \overleftarrow{\varepsilon} = 0(\varepsilon) = 1(\varepsilon) = \varepsilon$ for the empty word ε.

8 Proposition ([6]). *Let $p, q \in C^+$. Then $p \sim_{\mathscr{B},C} q$ iff $\mathsf{c}(p) = \mathsf{c}(q)$, $0(p) \sim_{\mathscr{B},C} 0(q)$ and $1(p) \sim_{\mathscr{B},C} 1(q)$.*

4 AI-Matching Problem

In the first section of Chapter 2, we prove NP-hardness of the AI-MATCHING problem. The proof uses reduction from the NP-complete problem 3-SAT.

9 Proposition (2.1.1). *The* AIU-MATCHING *problem and the* AI-MATCHING *problem are NP–hard.*

Because matching problem is a special case of unification problem we immediately obtain the following consequence.

10 Corollary. *The* AIU-UNIFICATION *problem and the* AI-UNIFICATION *problem are NP–hard.*

In the rest of Chapter 2 we prove that the AIU-MATCHING problem belongs to NP. In order to do this, we employ the term rewriting system of J. Siekmann and P. Szabo [21] and show that any solvable matching system has a solution of polynomial length.

11 Proposition ([21]). *The rewriting system*

$$\{xx \to x \mid x \in C^*, \mathsf{c}(x) \neq \emptyset\} \cup \{uvw \to uw \mid u,v,w \in C^*, \emptyset \neq \mathsf{c}(v) \subseteq \mathsf{c}(u) = \mathsf{c}(w)\}$$

is confluent and terminating. Moreover for $p,q \in C^*$ we have $p \sim_{\mathscr{B},C} q$ if and only if p and q have the same normal form with respect to the system.

We refer this rewriting system as *RS*. Since *RS* contains two different types of rewriting rules we denote RS_1 the rewriting system $\{xx \to x \mid x \in C^*, \mathsf{c}(x) \neq \emptyset\}$ and RS_2 the rewriting system $\{uvw \to uw \mid u,v,w \in C^*, \emptyset \neq \mathsf{c}(v) \subseteq \mathsf{c}(u) = \mathsf{c}(w)\}$. The corresponding rewrite relations are denoted $\to$, $\to_1$ resp. $\to_2$ and for a word $p \in C^*$ the set of its normal forms is denoted by $\langle p \rangle$, $\langle p \rangle_1$ resp. $\langle p \rangle_2$.

12 Lemma (2.2.8). *For any $p,q \in C^*$ such that $p = \langle p \rangle_2$ and $p \to_1 q$ it holds that $\langle q \rangle_2 = q$. In particular for a word $p \in C^*$ we have $\langle \langle p \rangle_2 \rangle_1 = \langle p \rangle$.*

Realize that each reduction of *RS* just leaves out some factor, the case $uvw \to uw$ is clear, and in the case $xx \to x$ we leave out the right occurrence of x in the square. If we have a word uAv, we can speak about the *residual* of A in the sense that the residual consists of all letter occurrences of A that were not left out during the sequence of reductions.

13 Proposition (2.3.9). *There is a polynomial $p : \mathbb{N} \to \mathbb{N}$, such that for an arbitrary A_1, B, $A_2 \in C^*$ in normal form and $\langle A_1 B A_2 \rangle_2 = A_1' B' A_2'$ where A_i', $1 \leq i \leq 2$, is the residual of A_i and B' is the residual of B, we have $|B'| \leq p(|\langle A_1 B A_2 \rangle|)$.*

14 Theorem (2.3.10). *Let p be a polynomial that satisfies the condition from Proposition 13. If a matching system $\{L_1 =^? R_1, \ldots, L_n =^? R_n\}$ has a solution then there exists a solution α with*

$$\mathrm{size}(\alpha) \leq \sum_{i=1}^{n} |L_i| \cdot p(|R_i|).$$

15 Corollary (2.3.11). *The* AIU-MATCHING *problem and* AI-MATCHING *problem are in NP.*

5 AI-Unification Problem

The proof of the main result of the thesis is contained in Chapter 3.

Let $L =^? R$ be a word equation and $\alpha : \mathrm{X} \to C^*$ be a mapping. Which information about α do we need to know if we want to decide whether α is a solution of the equation $L =^? R$? We would like to apply Proposition 8. We have to compute $\mathsf{c}(\alpha(L))$ and $\mathsf{c}(\alpha(R))$, hence we need to know $\mathsf{c}(\alpha(x))$ for all variables $x \in \mathrm{X}$. If we want to compute $\mathsf{c}(0^i(\alpha(L)))$ for the i-th iteration of the invariant 0, then we need to know $\overrightarrow{\alpha(x)}$ for some variables. Therefore, we will assume that $\overrightarrow{\alpha(x)}$ and $\overleftarrow{\alpha(x)}$ are given for all variables $x \in \mathrm{X}$. This assumption is natural; the AIU-UNIFICATION problem with this assumption is almost the same as without it.

For two mappings $\alpha, \beta : \mathrm{X} \to C^*$ we write

$$\alpha \approx_{\mathrm{X}} \beta \quad \text{if and only if} \quad \overrightarrow{\alpha(x)} = \overrightarrow{\beta(x)},\ \overleftarrow{\alpha(x)} = \overleftarrow{\beta(x)} \quad \text{for all} \quad x \in \mathrm{X}.$$

A pair (S, ν) is called a *system with complete information about invariants* if $S = \{L_1 =^? R_1, \ldots, L_n =^? R_n\}$ is a system of word equations and $\nu : \mathrm{X} \to C^*$ is a mapping. A solution of the system with complete information about invariants (S, ν) is a solution $\alpha : \mathrm{X} \to C^*$ of the system S in the free idempotent monoid over C such that $\alpha \approx_{\mathrm{X}} \nu$. (We can assume that $|\nu(x)| \leq 2 \cdot \|C\|$ because we can always exchange $\nu(x)$ for the word $\overrightarrow{\nu(x)}\,\overleftarrow{\nu(x)}$.)

16 Definition (3.2.1). The SIMPLE AIU-UNIFICATION problem asks to provide an algorithm deciding whether a given system with complete information about invariants has a solution.

17 Lemma (3.2.2). *Let (S, ν) be a system with complete information about invariants. Then one can construct (in polynomial time) a system S' such that the set of all solutions of (S, ν) and the set of all solutions of $S \cup S'$ coincide.*

On the other hand, it is easy to see that there exist non-deterministic polynomial reductions from the AIU-UNIFICATION and AI-UNIFICATION problems to the SIMPLE AIU-UNIFICATION problem (they guess a mapping $\nu : \mathrm{X} \to C^*$ satisfying $|\nu(x)| \leq 2 \cdot \|C\|$).

The following result is fundamental for the thesis.

18 Proposition (3.3.1). *The* SIMPLE AIU-UNIFICATION *problem is decidable in polynomial time.*

We immediately obtain the following consequence.

19 Theorem (3.4.1). *The* AIU-UNIFICATION *problem and the* AI-UNIFICATION *problem are NP-complete.*

In order to prove the same result for the general AI-unification problem, the following lemma is usful.

20 Lemma (3.4.2). *There exists a polynomial reduction from the AI-unification problem with linear constant restriction to the* AIU-UNIFICATION *problem.*

The desired result is a consequence of the previuos results and Proposition 4.

21 Theorem (3.4.3). *The general AIU-unification and AI-unification problems are NP-complete.*

6 Unification in Proper Varieties of Bands

The main results of Chapter 4 are the following two theorems which describe (in the case P$\neq$NP) the borderline between varieties with UNIFICATION (resp. MATCHING) problems decidable in polynomial time and varieties with NP-complete UNIFICATION (resp. MATCHING) problems. This borderline is depicted on Figure 1.

22 Theorem (4.1.1). *Let $\mathscr{V}$ be a variety of bands. The $\mathscr{V}$-*UNIFICATION *problem is decidable in polynomial time if $\mathscr{V} \subseteq \mathscr{N}\mathscr{B}$ and it is NP-complete otherwise.*

23 Theorem (4.1.2). *Let $\mathscr{V}$ be a variety of bands. The $\mathscr{V}$-*MATCHING *problem is decidable in polynomial time if $\mathscr{V} \subseteq \mathscr{R}\mathscr{B}$ and it is NP-complete otherwise.*

Both theorems can be formulated for the UNIFICATION and MATCHING problems for the varieties of idempotent monoids as well. The varieties corresponding to varieties of idempotent monoids are noted by filled black circles on Figure 4.1.

24 Corollary. *Let $\mathscr{V}$ be a variety of idempotent monoids. The $\mathscr{V}$-*UNIFICATION *problem is decidable in polynomial time if $\mathscr{V} \subseteq \mathscr{S}\mathscr{L}$ and it is NP-complete otherwise. The $\mathscr{V}$-*MATCHING *problem is decidable in polynomial time if $\mathscr{V} \subseteq \mathscr{R}\mathscr{B}$ and it is NP-complete otherwise.*

In the last section of Chapter 4 we consider the general $\mathscr{V}$-UNIFICATION problem and the equational unification problem for theories consisting of more independent ai-symbols and free symbols.

25 Theorem (4.5.16). *Let $\mathscr{V}$ be a variety of bands. Then the general $\mathscr{V}$-unification problem and the general $\mathscr{V}$-matching problem are decidable in polynomial time if $\mathscr{V} \subseteq \mathscr{R}\mathscr{C}\mathscr{B}$ and they are NP-complete otherwise, i.e. if $\mathscr{S}\mathscr{L} \subseteq \mathscr{V}$.*

26 Theorem (4.5.24). *Let* E *be a theory of independent non-trivial ai-symbols, enough free constant symbols and other free function symbols of an arbitrary arity.*

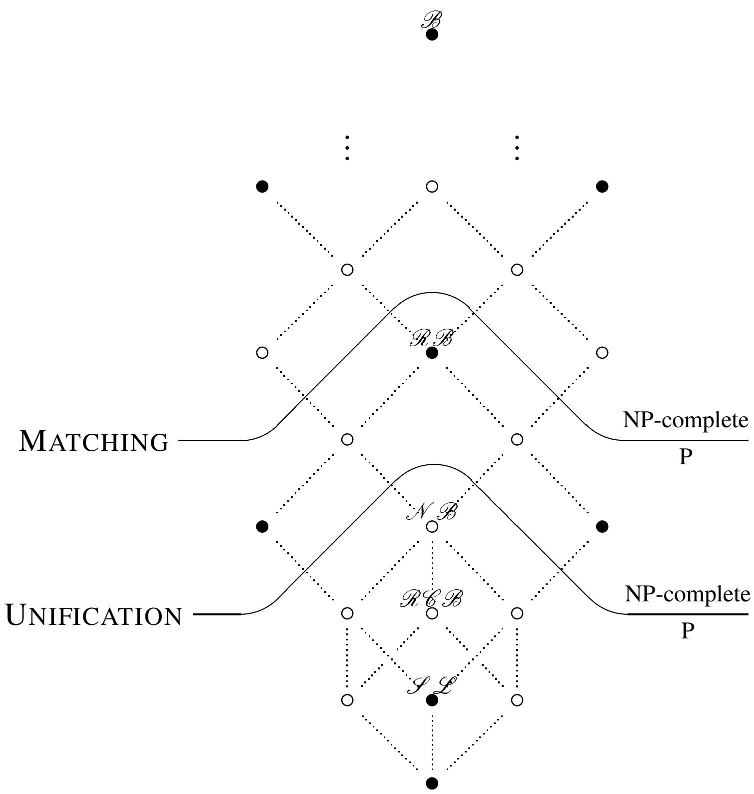

Figure 1: The complexity of the UNIFICATION and MATCHING problems in the subvarieties of the variety of all bands $\mathscr{B}$.

i) If E *contains only one non-zero*[5] *ai-symbol* $\cdot$ *and all free symbols are constant, then the* E*-unification problem is decidable in polynomial time if the symbol* $\cdot$ *satisfies the identity* $x \cdot y \cdot z \cdot x \doteq x \cdot z \cdot y \cdot x$ *and the* E*-unification problem is NP-complete otherwise, the* E*-matching problem is decidable in polynomial time if the symbol* $\cdot$ *satisfies the identity* $x \cdot y \cdot x \cdot z \cdot x \doteq x \cdot y \cdot z \cdot x$ *and the* E*-matching problem is NP-complete otherwise.*

ii) If E *contains only one non-zero ai-symbol* $\cdot$ *and some non-constant free symbol, then the* E*-unification problem and the* E*-matching problem are decidable in polynomial time if the symbol* $\cdot$ *satisfies the identity* $x \cdot y \cdot z \doteq x \cdot z$*, and both problems are NP-complete otherwise.*

iii) If E *contains at least two non-zero ai-symbols, then the* E*-unification problem and the* E*-matching problem are NP-complete.*

[5] An ai-symbol $\cdot$ is *non-zero* if does not satisfy the identity $x \cdot y \cdot z \doteq x \cdot z$.

7 Satisfiability of Equations over Bands

We have also studied systems of equations over fixed finite bands. It is surprising that the results concerning the complexity aspects are almost the same as in the case of equations in free bands, although there is no general relationship between complexities of these problems.

All results contained in Chapter 5 are based on our cooperation with Pascal Tesson and Denis Thérien. One can also find some of these results in the PhD thesis of Pascal Tesson [22] in a more general setting. In our thesis we only present the proofs which are related to bands. Some parts of the following theorem were published in [15].

27 Theorem (5.2.1, 5.2.3, 5.3.3 and 5.3.5). *Let S be a finite band. The problem of solving of equations with constant right hand sides is decidable in polynomial time if S is a regular band and it is NP-complete otherwise. The problem of solving of equations is decidable in polynomial time if S is commutative and it is NP-complete if S is not a normal band.*

The case of non-commutative normal bands, is quite difficult and we do not expect existence of any nice property which characterizes the bands having the problem tractable (in the case P$\neq$NP). Note that the case of idempotent monoids is fully established, because any normal idempotent monoid is commutative.

References

[1] Baader F.: The Theory of Idempotent Semigroups is of Unification Type Zero, J. Automated Reasoning **2** (1986) 283–286.

[2] Baader F.: Unification in Varieties of Idempotent Semigroups, Semigroup Forum **36** (1987) 127–145.

[3] Baader F., Schulz K. U.: Unification in the Union of Disjoint Equational Theories: Combining Decision Procedures, J. Symbolic Computation **21** (1996) 211–243.

[4] Baader F., Snyder W.: Unification Theory, In Handbook of Automated Reasoning (2001), Elsevier Science Publishers.

[5] Burckert H.-J.: Matching — a special case of unification?, J Symbolic Computation **8** (5) (1989) 532–536.

[6] Green J. A., Rees D.: On Semigroups in which $x^r = x$, Proc. Camb. Phil. Soc. **48** (1952) 35–40.

[7] Kapur D., Narendran P.: NP–completeness of the Set Unification and Matching Problems, In Proceedings of CADE'86, Vol. **230** of LNCS (1986) 489–495.

[8] Kapur D., Narendran P.: Complexity of Unification Problems with Associative-commutative Operators, J. Automated Reasoning **9**, No.2, (1992) 261–288.

[9] Klíma O.: Unification Modulo Associativity and Idempotency is NP-complete, In Proceedings of MFCS'02, Vol. **2420** of LNCS (2002) 423–432.

[10] Klíma O.: Complexity of unification and matching problems in the varieties of idempotent semigroups, 2003. To appear in International Journal of Algebra and Computation.

[11] Klíma O., Srba J.: Matching Modulo Associativity and Idempotency is NP-complete, In Proceedings of MFCS'00, Vol. **1893** of LNCS (2000) 456–466.

[12] Klíma O., Tesson P., Thérien D.: Notes on Systems of Equations over Finite Semigroups, (preprint).

[13] Knuth D. E., Bendix P.B.: Simple word problems in universal algebras, In Computational Problems in Abstract Algebra (1970) Pergamon Press, Oxford.

[14] Makanin G. S.: The Problem of Solvability of Equations in a Free Semigroup, Mat. Sbornik. **103(2)** (1977) 147–236. (In Russian) English translation in: Math. USSR Sbornik **32** (1977) 129–198.

[15] Moore C., Tesson P., Thérien D.: Satisfiability of systems of equations over finite monoids. In Proceedings of MFCS'01, Vol. **2136** of LNCS (2001) 537–547.

[16] Plandowski W.: Solvability of word equations with constants is in P-SPACE, in P. Beame (ed) Proceedings of FOCS (1999) IEEE Computer Society Press, New York.

[17] Plotkin G.: Building in Equational Theories, M. Intelligence **7** (1972) 73–90.

[18] Robinson J. A.: A Machine-oriented Logic Based on the Resolution Principle, J. Assoc. Comput. Mach. **12**, (1965) 23–41.

[19] Schmidt-Schauss M.: Unification under Associativity and Idempotence is of Type Nullary, J. of Automated Reasoning **2** (1986) 277–281.

[20] Siekmann J. H.: Unificaton theory: A survey, J. Symbolic Computation **7**(3,4) (1989) 207–274.

[21] Siekmann J. H., Szabó P.: A Noetherian and Confluent Rewrite System for Idempotent Semigroups, Semigroup Forum **25** (1982) 83–110.

[22] Tesson P.: Computational Complexity Questions Related to Finite Monoids and Semigroups. Ph.D. Thesis `http://www.cs.mcgill.ca/∼ptesso/`.

Department of Mathematics, Masaryk University
Janáčkovo nám. 2a, 662 95 Brno, Czech Republic
e-mail: `klima@math.muni.cz`
www: `http://www.math.muni.cz/˜klima`