Complexity of Unification and Matching Problems in the Varieties of Idempotent Semigroups

Ondřej Klíma

Dept. of Mathematics, Masaryk University, Janáčkovo nám. 2a,
662 95 Brno, Czech Republic
klima@math.muni.cz

Abstract

The complexity of the Matching problem in the theory of one associative, idempotent and commutative binary function symbol is known to be polynomial. On the other hand, it was proved that the Matching problem is NP-complete in the theory consisting of one binary function symbol which is only associative and idempotent (see [8]). We describe the complexity of the Matching problem for all equational theories of a single binary function symbol consisting of associativity, idempotency together with any set of additional identities. We also describe the complexity of the Unification problem for these theories.

Overview

From algebraic point of view every equational theory corresponds to a variety of algebras of a given type and equational unification is solving of equations in the free algebra of this variety.

An idempotent semigroup (also called a band) is a semigroup where the identity $x^2 = x$ is satisfied. The variety of all bands is denoted as $\mathcal{B}$. The lattice of all varieties of bands (see Figure 1) was described independently by Birjukov [3], Fennemore [4] and Gerhard [5].

Some varieties of bands from the bottom of the lattice are assigned certain names in literature:

$\mathcal{LSNB} = \mathrm{Mod}(x^2 = x, xyzxz = xyz)$ – all left seminormal bands,
$\mathcal{RSNB} = \mathrm{Mod}(x^2 = x, xzxyz = xyz)$ – all right seminormal bands,
$\mathcal{RB} = \mathrm{Mod}(x^2 = x, xyxzx = xyzx)$ – all regular bands,
$\mathcal{LRB} = \mathrm{Mod}(x^2 = x, xyx = xy)$ – all left regular bands,
$\mathcal{RRB} = \mathrm{Mod}(x^2 = x, xyx = yx)$ – all right regular bands,
$\mathcal{NB} = \mathrm{Mod}(x^2 = x, xyzx = xzyx)$ – all normal bands,
$\mathcal{RCB} = \mathrm{Mod}(x^2 = x, xyx = x)$ – all rectangular bands,
$\mathcal{SL} = \mathrm{Mod}(x^2 = x, xy = yx)$ – all semilattices,
$\mathcal{T}$ – all trivial semigroups.

Baader [1] and Schmidt-Schauss [9] proved that the Unification problem in the variety of all bands is of type zero. Then Baader obtained the following characterization of unification type for all varieties of bands.

Proposition 1 (**[2]**). *The Unification problem for a variety of bands $\mathcal{V}$ is of unitary type if $\mathcal{V} \in [\mathcal{T}, \mathcal{RCB}]$, finitary type if $\mathcal{V} \in [\mathcal{SL}, \mathcal{NB}]$ and type zero otherwise.*

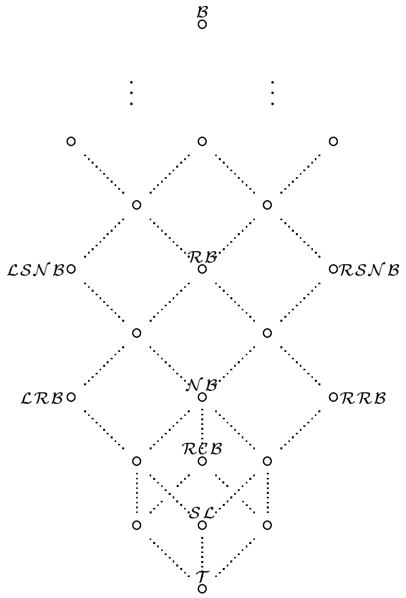

Fig. 1. Lattice of varieties of bands

As we are interested only in the existence of solutions, we concentrate on the Unification problem with constants, because every system of equations without constants is trivially solvable in an arbitrary variety of bands.

The Matching problem is a special case of the Unification problem where only systems of equations with variable-free right-hand sides (so called matching systems) are considered. Recall a result about complexity of the Matching problem in $\mathcal{B}$.

Proposition 2 **([8]).** *The Matching problem in the variety of all bands $\mathcal{B}$ is NP-complete.*

In contrast with [8] we assume that our function symbol satisfies some additional non-trivial identities. We describe the borderline between varieties with the Matching (resp. Unification) problems decidable in polynomial time and varieties with the NP-complete Matching (resp. Unification) problems (under the assumption P≠NP).

Our Results[1]

One can prove that the Unification problem in every proper subvariety of the variety $\mathcal{B}$ is in NP. The proof of such a proposition is based on the fact that the validity of identities for every variety of bands is decidable in polynomial time and on the following lemma.

Lemma 1. *Let $\mathcal{V}$ be a proper subvariety of the variety $\mathcal{B}$ which has exactly k subvarieties. Then for an arbitrary n-element set Σ and a word $u \in \Sigma^+$ there is a word $w \in \Sigma^+$ such that $|w| < 4n^k$ and $u = w$ is an identity for the variety $\mathcal{V}$.*

[1] For the proofs of the results see [7].

Most of the Unification and Matching problems in the varieties of bands are NP-hard.

Proposition 3. *Let $\mathcal{V}$ be a subvariety of the variety of all bands $\mathcal{B}$ which contains some non-regular band, i.e. $\mathcal{V} \not\subseteq \mathcal{RB}$. Then the Matching problem in the variety $\mathcal{V}$ is NP-hard.*

Proposition 4. *Let $\mathcal{V}$ be a proper subvariety of the variety of all bands $\mathcal{B}$ which contains some non-normal band, i.e. $\mathcal{V} \not\subseteq \mathcal{NB}$. Then the Unification problem in the variety $\mathcal{V}$ is NP-hard.*

We use a reduction from the NP-complete problem 3-SAT to prove NP-hardness of our problems. For a formula Φ we construct a system of equations S such that S is satisfiable in the varieties from the interval $[\mathcal{LSNB}, \mathcal{B}]$ (resp. $[\mathcal{LRB}, \mathcal{B}]$) if and only if Φ is satisfiable. The system for the proof of Proposition 3 can be taken from [8] and the system for the proof of Proposition 4 is similar.

We are able to find polynomial-time algorithms solving the Unification and Matching problems in certain varieties of bands.

Proposition 5 ([6]). *The Unification problem in the variety $\mathcal{SL}$ is decidable in polynomial time.*

An easy modification of the original proof of Proposition 5 gives the same result for all varieties $\mathcal{V} \subseteq \mathcal{NB}$.

It is not difficult to see that every satisfiable matching system in the variety $\mathcal{SL}$ has the maximal solution α in the sense that for each variable x, $\alpha(x)$ contains all letters occurring in $\beta(x)$ for some solution β. A similar result can be proved for the other subvarieties of the variety $\mathcal{RB}$. Moreover, such a maximal solution can be computed in polynomial time if it exists and if it is not the case then we are able to discover it also in polynomial time.

Conclusion

Theorem 1. *The Unification problem is decidable in polynomial time for all subvarieties of the variety $\mathcal{NB}$ and it is NP-complete for the other proper subvarieties of $\mathcal{B}$. The Matching problem is decidable in polynomial time for all subvarieties of the variety $\mathcal{RB}$ and it is NP-complete for the other subvarieties of $\mathcal{B}$. (See Figure 2.)*

In the languague of equational theories, this result can be formulated in the following way. The Unification problem in a theory of a single associative and idempotent binary function symbol satisfying some additional non-trivial identity is decidable in polynomial time if the function symbol satisfies the identity $xyzx = xzyx$ and it is NP-complete otherwise. An analogous result for the Matching problem and the identity $xyxzx = xyzx$ can be formulated.

For a complete description of the complexity of the Unification and Matching problems in the varieties of idempotent semigroups it remains to determine the complexity of the Unification problem in the variety of all idempotent semigroups $\mathcal{B}$. Up to our knowledge, it is an open problem.

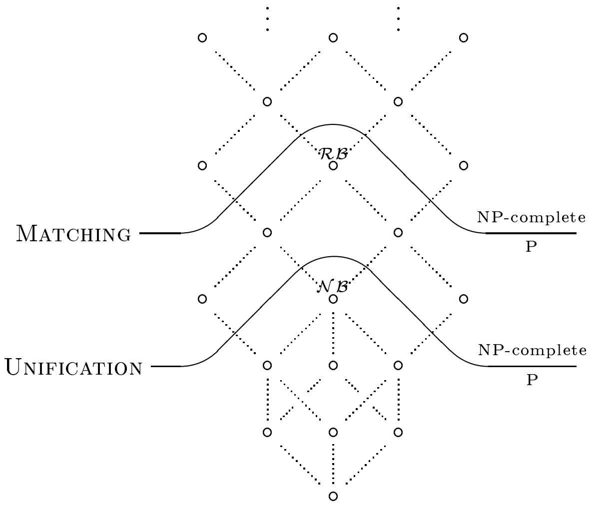

Fig. 2. Complexity of the Unification and Matching problems in the proper subvarie of the variety of all bands $\mathcal{B}$

References

1. Baader F.: The Theory of Idempotent Semigroups is of Unification Type Zero, J. of Automated Reasoning **2** (1986) 283–286.
2. Baader F.: Unification in Varieties of Idempotent Semigroups, Semigroup Forum **36** (1987) 127–145.
3. Birjukov A.P.: Varieties of Idempotent Semigroups, Algebra i Logika **9** (1970) 255–273 (Russian).
4. Fennemore C. F.: All Varieties of Bands I, II, Math. Nachr. **48** (1971) 237–252, 253–262.
5. Gerhard J. A.: The Lattice of Equational Classes of Idempotent Semigroups, J. Algebra **15** (1970) 195–224.
6. Kapur D., Narendran P.: Complexity of Unification Problems with Associative-commutative Operators, J. of Automated Reasoning **9**, No.2, (1992) 261–288.
7. Klíma O.: Complexity of Unification and Matching Problems in the Varieties of Idempotent Semigroups, `http://www.math.muni.cz/~klima/Math/publications.html`.
8. Klíma O., Srba J.: Matching Modulo Associativity and Idempotency is NP-complete, In Proceedings of MFCS'00, Vol. 1893 of LNCS (2000) 456–466.
9. Schmidt-Schauss M.: Unification under Associativity and Idempotence is of Type Nullary, J. of Automated Reasoning **2** (1986) 277–281.