Complexity problems over algebraic structures

Theses of PhD dissertation

Created by: Horváth Gábor

Mathematical Doctoral School
Theor. Mathematical Doctoral Program

Dir. of School: Dr. Laczkovich Miklós
Dir. of Program: Dr. Szenthe János
Supervisor: Dr. Szabó Csaba, DSc,
associate professor

Eötvös Loránd University
Faculty of Natural Sciences
2010

Nowadays, computers play larger and larger role in everyday life and in scientific research. This is especially true in mathematics and algebra, where one often wants to perform calculations or computations with a machine. To determine whether or not two expressions are identically equal or whether an equation has a solution are important questions in the areas of universal algebra or in the theory of automata and formal languages.

The *equivalence* problem over a finite algebra $\mathbf{A}$ asks whether or not two expressions p and q attain the same value for every substitution from $\mathbf{A}$, i.e. whether or not $p \approx q$ is an identity over $\mathbf{A}$. The *equation solvability* problem over $\mathbf{A}$ asks, whether or not the equation $p = q$ has any solution over $\mathbf{A}$. The input expressions can be terms, i.e. expressions that are built up from variables and the basic operations of $\mathbf{A}$, or polynomials, i.e. expressions that are built up from variables, constants from $\mathbf{A}$ and the basic operations of $\mathbf{A}$. Thus we distinguish four problems altogether: the term equivalence problem (shortly equivalence), the polynomial equivalence problem, the term equation solvability problem, and the polynomial equation solvability problem (shortly equation solvability).

Each of these problems is decidable for a finite algebra $\mathbf{A}$ by checking all possible substitutions. The interesting question is therefore whether these problems can be solved fast, and what computational complexity they have. We investigate the complexity of these questions for finite rings and groups.

Definition (Definition 2.1)**.** The *equivalence* problem (for a finite algebra $\mathbf{A}$) consists of two input term expressions s and t over $\mathbf{A}$ and asks whether or not s and t are equivalent over $\mathbf{A}$, i.e. whether or not $s \approx t$ is an identity over $\mathbf{A}$. The *polynomial equivalence* problem (for a finite algebra $\mathbf{A}$) consists of two input polynomial expressions p and q over $\mathbf{A}$ and asks whether or not p and q are equivalent over $\mathbf{A}$, i.e. whether or not $p \approx q$ is an identity over $\mathbf{A}$. The *equation solvability* problem (for a finite algebra $\mathbf{A}$) consists of two input polynomial expressions p and q over $\mathbf{A}$ and asks if there exists a substitution for which the functions $p^{\mathbf{A}}$ and $q^{\mathbf{A}}$ attain the same value, i.e. whether or not $p = q$ has a solution over $\mathbf{A}$.

We do not examine the term equation solvability problem, because the

equation $s = t$ always admits a trivial solution whenever s and t are terms over a ring or over a group. We consider the complexities of the equivalence, of the polynomial equivalence and of the equation solvability problems in the length of the input terms or polynomials.

Definition (Definition 2.2). Let $\mathbf{A}$ be a finite algebra. We define the length $\|p\|$ of a term or polynomial expression p inductively. The length of a variable x or a constant c is 1: $\|x\| = \|c\| = 1$. For an m-ary basic operation f the length of the polynomial $f(p_1, \ldots, p_m)$, whenever it is defined, is the sum of $\|p_i\|$, i.e. $f(p_1, \ldots, p_m) = \sum_{i=1}^{m} \|p_i\|$. The length of $f(x_1, \ldots, x_m)$ is m.

Besides being interesting problems on their own, the equivalence and equation solvability problems have deep applications in other mathematical areas. An important universal algebraic question is to decide whether an algebra $\mathbf{A}$ is a member of a variety $\mathcal{V}$. Here, the variety $\mathcal{V}$ can be given either by the identities that hold in $\mathcal{V}$ or by an algebra $\mathbf{B}$ that generate $\mathcal{V}$. In the latter case an identity holds in $\mathcal{V}$ if and only if it holds in $\mathbf{B}$. Thus the membership problem can be decided by simple determining for each identity whether or not it holds in $\mathbf{A}$. The equation solvability problem is used in automata theory. Recognizing a language can be reduced to equation solvability over the syntactic monoid of the language.

Early investigations into the equivalence problem for various finite algebraic structures were carried out by computer scientists, in particular at Syracuse University where the terminology *the term equivalence problem* was introduced. They considered finite commutative rings and finite lattices. Their motivation came from industry: the synchronization of various chemical experiments led to the equivalence problem over finite commutative rings. In the early 1990's it was shown by Hunt and Stearns (see [10]) that the equivalence problem over a finite commutative ring either has polynomial time complexity or is coNP-complete. Later Burris and Lawrence proved in [6] that the same holds for rings in general.

In their proof Burris and Lawrence reduced the SAT problem to the equivalence of polynomials written as products of sums. Nevertheless, these polynomials can be exponential long if are written in the usual ring-theoretic

form, i.e. as sums of monomials. This observation motivated Ross Willard in defining the *sigma equivalence* and *sigma equation* solvability problem, where the input polynomials are written as sums of monomials. Willard and Lawrence [12] conjectured that the sigma equivalence problem over a finite ring has polynomial time complexity whenever the factor by the Jacobson radical is commutative or coNP-complete otherwise. Szabó and Vértesi proved the coNP-complete part of the statement. In [14, 15, 16] they prove that the sigma equivalence problem is coNP-complete over a finite ring if the factor by the Jacobson radical is not commuative. In Chapter 3 of the thesis we verify the conjecture for commutative rings.

Theorem (Theorem 3.1). *Let $\mathcal{R}$ be a finite commutative ring. Then the equivalence problem over $\mathcal{R}$ has polynomial time complexity.*

As of now, there are no published results about the sigma equation solvability problem. Nevertheless, using the method of Szabó and Vértesi it is easy to prove that the sigma equation solvability is NP-complete over a finite ring if the factor by the Jacobson radical is not commutative. In Chapter 3 we determine the complexity of the sigma equation solvability problem for certain finite rings.

Theorem (Theorem 3.2). *Let the finite ring $\mathcal{R}$ be the direct sum of finite fields, nilpotent rings and rings isomoprhic to $\mathbb{Z}_4$. Then the sigma equivalence problem over $\mathcal{R}$ has polynomial time complexity.*

The equivalence and equation solvability over finite groups proved to be a more challenging topic than that for finite rings. The equivalence problem over a finite nilpotent group has polynomial time complexity by Burris and Lawrence [7]. Goldmann and Russell [8, 9] proved that the equations solvability problem over a finite nilpotent ring has polynomial time complexity. They reduced the equation solvability problem to recognizing languages by deterministic, non-uniform, finite automatons obtained from a nilpotent group. Such automatons have been investigated earlier by Péladeau and Thérien in [13]. Nevertheless, many of the properties required are not proved in the french paper [13], but in [17]. Hence the reader can easily get lost in trying to uncover the main idea behind the proof of Goldmann and Russel. In

Chapter 5 we give a direct proof, which is slightly clearer than the one behind the abovementioned three papers, it does not cite publications and the equivalence follows from it as well.

Theorem (Theorem 5.2). *Let* $\mathbf{G}$ *be a nilpotent group. The (polynomial) equivalence and equation solvability problems over* $\mathbf{G}$ *have polynomial time complexities.*

After investigating nilpotent groups, it is natural to consider finite groups being a semidirect product of two Abelian groups. Burris and Lawrence in [7] posed the problem of determining the complexity of the equivalence over every solvable, not nilpotent group. Ondrej Klíma investigated the equivalence and equation solvability problem over finite semigroups. In [11] he determined the complexity of these questions over every semigroup containing at most 6 elements, except for the group $\mathbf{S}_3$. Goldmann and Russell explicitly ask in [8] to decide the complexity of solving an equation over $\mathbf{S}_3$. In Chapter 6 we determine these complexities for some solvable, not nilpotent groups. We answer the questions of Klíma, Goldmann and Russel, and we take the first step in answering the question of solvable, not nilpotent groups.

Theorem (Corollary 6.3). *The (polynomial) equivalence problem over any of the following groups has polynomial time complexity.*

1. $\mathbf{G} = \mathbf{A} \rtimes \mathbf{B}$, *where* $\mathbf{A}$ *and* $\mathbf{B}$ *are Abelian,*
2. $\mathbf{G} = \mathbf{Z}_n \rtimes \mathbf{B}$, *where the (polynomial) equivalence over* $\mathbf{B}$ *has polynomial time complexity.*
3. $\mathbf{G} = \mathbf{Z}_{n_1} \rtimes (\mathbf{Z}_{n_2} \rtimes \cdots \rtimes (\mathbf{Z}_{n_k} \rtimes (\mathbf{A} \rtimes \mathbf{B})))$, *where each* n_i *is a positive integer and* $\mathbf{A}$, $\mathbf{B}$ *are commutative groups.*

Theorem (Corollary 6.5). *The equation solvability over any of the following groups has polynomial time complexity.*

1. $\mathbf{G} = \mathbf{Z}_p \rtimes \mathbf{B}$, *where* $\mathbf{B}$ *is a finite commutative group and* p *is a prime;*
2. $\mathbf{G} = \mathbf{Z}_4 \rtimes \mathbf{B}$, *where* $\mathbf{B}$ *is a finite commutative group;*

3. $\mathbf{G} = \mathbf{Z}_2^2 \rtimes \mathbf{B}$, *where* $\mathbf{B}$ *is a finite commutative group,* $2 \nmid |\mathbf{B}|$*;*

4. $\mathbf{G} = \mathbf{Z}_p^2 \rtimes \mathbf{Z}_2$, *where* p *is an odd prime.*

Some of these results are published in [5] in English, in [1] in Hungarian. The proof we communicate in Chapter 6 reduces the equivalence and equation solvability problems over $\mathbf{A} \rtimes \mathbf{B}$ to the equivalence and equation solvability problems over the End $\mathbf{A}$-module $\mathbf{A}$. The equivalence and equation solvability problems have not yet been introduced. In Chapter 4 we define module-polynomials and module-monomials. Then we define the sigma equivalence and sigma equation solvability problems over finite modules. Even though the results of Chapter 4 are interesting on their own, we mostly use them to prove other theorems. Thus we consider the results of Chapter 4 as useful techniques. The following theorems play an important role in proving the results of Chapter 6.

Theorem (Theorem 4.1). *Let* $\mathcal{R}$ *be a finite, commutative, unital ring and let* $\mathcal{M}$ *be a faithful* $\mathcal{R}$*-module. Let* $\mathcal{S}$ *be the subgroup of* $\mathcal{R}^*$*. If* f *is a module-polynomial written as a sum of module-monomials, then it is decidable in polynomial time whether or not* $(\mathcal{R}, \mathcal{M}) \models f \approx 0$ *for substitutions from* $\mathcal{S}$*.*

Theorem (Theorem 4.2). *Let* $\mathcal{R} = \oplus_{i=1}^{l} \mathcal{F}_i$*, for some finite fields* $\mathcal{F}_i$*. Let* $\mathcal{M}$ *be a faithful* $\mathcal{R}$*-module. Let* $\mathcal{S} = \oplus \mathcal{S}_i$*, where each* $\mathcal{S}_i$ *is a subgroup of* $\mathcal{F}_i^*$*. If* f *is a module-polynomial written as a sum of module-monomials, then it is decidable in polynomial time whether or not* $f = 0$ *is solvable with substitutions from* $\mathcal{S}$*.*

In Chapter 7 we examine nonsolvable groups. The equation solvability problem over a non-solvable group is NP-complete [8, 9]. The following theorem is published in [2] in English, in [3] in Hungarian.

Theorem (Theorem 7.1). *The (polynomial) equivalence problem over a finite nonsolvable group is coNP-complete.*

Some expressions can be much shorter if expressed not only by the basic operations of the algebra but by some new operations as well. For example,

the expression $[[[x_1, x_2], x_3], \ldots, x_n]$ has length n if the commutator is a basic operation, but has exponential length in n when expressed by only the group multiplication. Such a decrease in the length suggests that the complexities of the equivalence or equation solvability problems might change if the commutator (or another operation) is a basic operation. This motivates the definition of the extended problems in Chapter 8, when the input expression can contain new term operations expressed by the group multiplication.

Definition (Definition 8.1)**.** Let $\mathbf{G} = (G, \cdot)$ be a finte group. We say that the extended (polynomial) equivalence (equation solvability) problem over $\mathbf{G}$ has polynomial time complexity if for arbitrary term expressions $f_1, \ldots, f_k$ the (polynomial) equivalence (equation solvability) problem over $(G, \cdot, f_1, \ldots, f_k)$ has polynomial complexity. We say that the extended (polynomial) equivalence (equation solvability) problem over $\mathbf{G}$ is coNP-complete (NP-complete) if there exist term expressions $f_1, \ldots, f_k$ such that the (polynomial) equivalence (equation solvability) problem over $(G, \cdot, f_1, \ldots, f_k)$ is coNP-complete (NP-complete).

The main result of Chapter 8 is the dichotomy theorem for the equivalence and equation solvability problems over finite groups.

Theorem (Theorem 8.2)**.** *Let $\mathbf{G} = (G, \cdot)$ be a finite group. If $\mathbf{G}$ is nilpotent then the exteneded (polynomial) equivalence and the extended equation solvability problems over $\mathbf{G}$ have polynomial time complexities. If $\mathbf{G}$ is not nilpotent, then there exists a term f such that the (polynomial) equivalence over $(G, \cdot, f)$ is coNP-complete, and the equation solvability over $(G, \cdot, f)$ is NP-complete.*

Most of the results discussed in the dissertation are not yet published. My publications in the topic are [2, 4, 5] in English and [1, 3] in Hungarian.

Publications in the topic of the dissertation

[1] G. Horváth. Identities over finite groups (in Hungarian). *Matematikai Lapok. New Series*, 13 (2006/07)(2):12–19, 2008.

[2] G. Horváth, J. Lawrence, L. Mérai, and Cs. Szabó. The complexity of the equivalence problem for non-solvable groups. *Bulletin of the London Mathematical Society*, 39(3):433–438, 2007.

[3] G. Horváth and L. Mérai. The complexity of checking identities over non-solvable groups (in Hungarian). *Matematikai Lapok. New Series*, 13 (2006/07)(2):20–27, 2008.

[4] G. Horváth, C. L. Nehaniv, and Cs. Szabó. An assertion concerning functionally complete algebras and NP-completeness. *Theoretical Computer Science*, 407:591–595, 2008.

[5] G. Horváth and Cs. Szabó. The complexity of checking identities over finite groups. *International Journal of Algebra Computation*, 16(5):931–940, 2006.

Bibliography

[6] S. Burris and J. Lawrence. The equivalence problem for finite rings. *J. of Symb. Comp.*, 15:67–71, 1993.

[7] S. Burris and J. Lawrence. Results on the equivalence problem for finite groups. *Alg. Univ.*, 52(4):495–500, 2004. (2005).

[8] M. Goldmann and A. Russell. The complexity of solving equations over finite groups. In *Proceedings of the 14th Annual IEEE Conference on Computational Complexity*, pages 80–86, Atlanta, Georgia, 1999.

[9] M. Goldmann and A. Russell. The complexity of solving equations over finite groups. *Information and Computation*, 178(253–262), 2002.

[10] H. Hunt and R. Stearns. The complexity for equivalence for commutative rings. *Journal of Symbolic Computation*, 10:411–436, 1990.

[11] O. Klíma. Complexity issues of checking identities in finite monoids. *Semigroup Forum*, 79(3):435–444, 2009.

[12] J. Lawrence and R. Willard. The complexity of solving polynomial equations over finite rings. manuscript, 1997.

[13] P. Péladeau and D. Thérien. Sur les langages reconnus par des groupes nilpotents. *C. R. Acad. Sci. Paris Sér. I Math*, 306(2):93–95, 1988.

[14] Cs. Szabó and V. Vértesi. The complexity of checking identities for finite matrix rings. *Algebra Universalis*, 51:439–445, 2004.

[15] Cs. Szabó and V. Vértesi. The complexity of the word-problem for finite matrix rings. *Proceedings of the American Mathematical Society*, 132:3689–3695, 2004.

[16] Cs. Szabó and V. Vértesi. The complexity of checking identities over finite rings. manuscript, 2010.

[17] D. Thérien. Subword counting and nilpotent groups. In *Combinatorics on words (Waterloo, Ont., 1982)*, pages 297–305. Academic Press, Toronto, Ont., 1983.