On solvability of systems of polynomial equations

László Zádori

Abstract. We study the computational complexity of the solvability problem of systems of polynomial equations over finite algebras. We prove a new dichotomy theorem that extends most of the dichotomy results which have been obtained over different families of finite algebras so far. As a corollary, for example, we get that, if $\mathbb{A}$ is a finite algebra of finite signature and omits the Hobby-McKenzie type **1**, then the problem is solvable in polynomial time whenever $\mathbb{A}$ is a reduct of a generalized affine algebra, and **NP**-complete otherwise.

1. Introduction

In this short note we investigate the algorithmic complexity of the solvability problem of systems of equations over finite algebras. The solvability problem of systems of polynomial equations over a finite algebra $\mathbb{A}$ of finite signature is formulated as follows.

- SysPol($\mathbb{A}$)
  Input: a finite system S of polynomial equations over $\mathbb{A}$.
  Question: does S have a solution over $\mathbb{A}$?

The basic conjecture related to these decision problems states that for every finite algebra $\mathbb{A}$ of finite signature, SysPol($\mathbb{A}$) is in **P** or **NP**-complete.

The conjecture was already confirmed for large classes of algebras. A dichotomy theorem was obtained in the special cases of groups [6], monoids and some other subclasses of semigroups [9]. In [10] a dichotomy theorem over a fairly large class of algebras was obtained which encompasses the cases of lattices, rings, modules and quasigroups, and was extended in [15] to cover the cases of semilattices, as well.

The main results in [15] are based on a theorem concerning a pair of operations commuting with each other (see Theorem 2.1 in the present paper). Our aim in this note is to prove some further consequences of this theorem such as

Presented by ...
Received ...; accepted in final form ...
2010 *Mathematics Subject Classification*: Primary 08A70; Secondary 68Q17, 08B10.
Key words and phrases: CSP, complexity, systems of equations, algebras, Hobby-Mckenzie types.
The author's research was partially supported by the TÁMOP-4.2.2/08/1/2008-0008 program of the Hungarian National Development Agency and OTKA grants K60148, K77409.

a new dichotomy theorem that extends most of the dichotomy results which have been obtained for SysPol so far.

The main result of this paper (formulated in Theorem 3.5) is a proper generalization of the dichotomy theorems for SysPol over finite algebras possessing a binary polynomial operation with an identity element and over finite algebras that generate a variety omitting the Hobby-McKenzie type **1**. As a new corollary of the main result, for example, we obtain a dichotomy theorem for SysPol over finite algebras that omit type **1**.

Following Feder and Vardi, for any finite relational structure $\mathcal{T}$ of finite signature [5] we define the *constraint satisfaction problem* over $\mathcal{T}$ as follows.

- CSP($\mathcal{T}$)
  Input: a finite relational structure $\mathcal{I}$ similar to $\mathcal{T}$.
  Question: is there a homomorphism from $\mathcal{I}$ to $\mathcal{T}$?

CSP that includes such standard decision problems as 3-satisfiability, graph unreachability and graph k-colorability, has attracted a great deal of attention in the last few years, and, as we shall see, plays an important role in our investigations of SysPol.

Let f be an n-ary operation on A. Let f° denote the *graph* of f, i.e. the following $(n+1)$-ary relation:

$$f^\circ = \{(x_1, \dots, x_n, y) : f(x_1, \dots, x_n) = y\}.$$

The following theorem makes it possible to study SysPol via CSP.

Theorem 1.1 ([10])**.** *Let $\mathbb{A} = \langle A, F\rangle$ be a finite algebra of finite signature. Let C denote the set of constants of A. The problem* SysPol($\mathbb{A}$) *is polynomial-time equivalent to the problem* CSP($\langle A, R\rangle$)*where R consists of all the relations of the form f°, with f in $F \cup C$.*

In [9] Klíma, Tesson and Thérien proved that for every finite structure $\mathcal{T}$, CSP($\mathcal{T}$) is polynomial-time equivalent to some SysPol($\mathbb{A}$) where $\mathbb{A}$ is a right normal band. A similar result were obtained by Feder, Madelaine and Stewart in [4] with right normal bands replaced by unary algebras that have exactly two basic operations.

These theorems together with Theorem 1.1 show that establishing a dichotomy theorem for SysPol over the class of all finite algebras is equivalent to proving that CSP has a dichotomy over the class of all finite structures, which is considered hard. These results also show that to prove a dichotomy theorem for SysPol looks hard even over so simply looking algebras as right normal bands or unary algebras with two basic operations.

Let A be a finite, non-empty set. An operation f on A is *idempotent* if it satisfies the identity $f(x, \dots, x) = x$. We say that an algebra $\mathbb{A}$ *admits a non-trivial idempotent Maltsev condition*, if there exists a finite set of identities that is not satisfied by projections of the two element set, but is satisfied by some idempotent term operations of $\mathbb{A}$. Admitting a nontrivial idempotent Maltsev condition is a decidable property of finite algebras of finite signature,

see [7]. Most of the algebraic structures in classical algebra have this property, such as, for example, algebras with a group or semilattice term operation.

An n-ary idempotent operation f is a *Taylor operation* if for every $1 \leq i \leq n$, f satisfies an identity of the form

$$f(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_n) = f(y_1, \ldots, y_{i-1}, y, y_{i+1}, \ldots, y_n)$$

where $x_j, y_j \in \{x, y\}$, for all $1 \leq j \leq n$. For instance, a groupoid (i.e. binary) operation is a Taylor operation if and only if it is idempotent and commutative; in particular, semilattice operations are Taylor operations. Another common example of a Taylor operation is the ternary term operation $xy^{-1}z$ of a group.

The following theorem makes a link between idempotent Maltsev conditions, Taylor terms and one of the Hobby-McKenzie types.

Theorem 1.2 ([7], cf. [14])**.** *For a finite algebra $\mathbb{A}$ the following are equivalent.*

(1) *$\mathbb{A}$ admits a nontrivial idempotent Maltsev condition.*
(2) *$\mathbb{A}$ has a Taylor term operation.*
(3) *$\mathbb{A}$ generates a variety that omits type* **1**.

In the recent history of Taylor operations it was shown that in the above theorem Taylor term operations can be replaced by more special Taylor operations, such as weak near unanimity term operations [12], idempotent cyclic term operations [1], or the single fourary Siggers term operation [13].

2. Algebras with a compatible Taylor operation

A semigroup $\mathbb{S}$ is called a *semilattice of Abelian groups* if $\mathbb{S}$ has a congruence θ such that $\mathbb{S}/\theta$ is a semilattice and the blocks of θ are Abelian subgroups of $\mathbb{S}$. Clearly, every semilattice of Abelian groups is an inverse semigroup. Moreover, for every finite semilattice of Abelian groups there exists an n such that the unique inverse of any element y can be expressed as y^{n-1}. Hence in finite semilattices of Abelian groups $xy^{-1}z$ is an idempotent ternary term operation.

Let $\mathbb{A}$ be an algebra. An operation f on the universe of $\mathbb{A}$ is *compatible* with $\mathbb{A}$ if it commutes with all basic operations of $\mathbb{A}$. The main results obtained in [15] were based on the following theorem.

Theorem 2.1 ([15])**.** *Let $\mathbb{A}$ be a finite algebra. Let xy be a binary polynomial operation of $\mathbb{A}$ with an identity element and t a compatible Taylor operation of $\mathbb{A}$. Then the following hold:*

(1) *xy is the multiplication of a semilattice of Abelian groups.*
(2) *The clone generated by t contains an idempotent ternary operation of the form $xy^{-1}z$.*

In Theorem 2.2 we give a generalization of part (2) of this result. The statement itself in Theorem 2.2 may look a bit technical, but we shall later

prove some nicely looking corollaries to it. We say that a set of transformations F of a set A is *separating* if for any two distinct elements a and b in A there exists a map $f \in F$ such that $f(a) \neq f(b)$.

Theorem 2.2. *Let $\mathbb{A}$ be a finite algebra which has a separating set F of unary polynomial operations such that for every $f \in F$ there exists a binary polynomial operation g_f of $\mathbb{A}$ whose restriction to the set $f(A)$ is a binary operation with an identity element. Let t be a compatible Taylor operation of $\mathbb{A}$. Then the clone generated by t contains an idempotent ternary operation that extends to the term operation $xy^{-1}z$ of a finite semilattice of Abelian groups.*

Proof. Clearly, the operations of F are all endomorphisms of the algebra (A, t), and for all $f \in F$ the $(f(A), t|_{f(A)})$ are subalgebras of (A, t). Since F is separating, (A, t) embeds into the direct product $\mathbb{B}$ of the $(f(A), t|_{f(A)})$, $f \in F$. The operation g acting componentwise as g_f, $f \in F$, on B is a compatible binary operation of $\mathbb{B}$ and has an identity element. By invoking the preceding theorem, $xy = g(x, y)$ is the multiplication of a semilattice of Abelian groups and $xy^{-1}z$ is in the clone generated by $t_{\mathbb{B}}$. So there is a finite semilattice of Abelian groups on the base set of $\mathbb{B}$ whose idempotent term operation $xy^{-1}z$ restricts to a copy of $\mathbb{A}$ as a compatible idempotent operation. This concludes the proof. □

A *Taylor algebra* is an algebra with a Taylor term operation. By using some facts established in [7], it was proved in [15] that Taylor algebras are typical examples of algebras that satisfy the assumption of the preceding theorem. A *doubly Taylor algebra* is a Taylor algebra with a compatible Taylor operation. The following characterization of doubly Taylor algebras appears in [15].

Theorem 2.3 ([15])**.** *A finite Taylor algebra is a doubly Taylor algebra if and only if it has a compatible idempotent ternary operation that extends to an idempotent term operation $xy^{-1}z$ of a finite semilattice of Abelian groups.*

We now improve this characterization of doubly Taylor algebras by showing that a compatible ternary operation of a Taylor algebra which appears in the statement of Theorem 2.3 must also be a term operation of the algebra. An algebra $\mathbb{A}$ is called *generalized affine* if it has a ternary idempotent compatible term operation that extends to the term operation $xy^{-1}z$ of a finite semilattice of Abelian groups. An n-ary operation t is *cyclic* if it satisfies the identity

$$t(x_1, x_2, \ldots, x_{n-1}, x_n) = t(x_2, x_3, \ldots, x_n, x_1).$$

Theorem 2.4. *A finite algebra is doubly Taylor if and only if it is generalized affine.*

Proof. For the first part of the proof let $\mathbb{B}$ be a doubly Taylor algebra, that has a Taylor term operation t_1 and a compatible Taylor operation t_2. Then, by applying Theorem 2.2 two times in two ways, for each $i \in \{1, 2\}$ the clone

generated by t_i has an idempotent ternary operation m_i that extends to an idempotent term operation $x*_i y*_i \dots *_i y*_i z$ of a finite semilattice of Abelian groups. Note that we may assume that y appears in the respective terms $n-1$ times for both $i = 1, 2$, since if y appears $k-1$ times then k may be replaced by any multiple of k without changing the corresponding term operation. Let

$$s_i(x_1, x_2, \dots, x_{n+1}) = m_i(x_1, x_{n+1}, m_i(x_2, x_{n+1}, \dots, m_i(x_n, x_{n+1}, x_{n+1}))\dots)$$

where $i = 1, 2$. Thus,

$$s_i(x_1, x_2, \dots, x_{n+1}) = x_1 *_i x_2 *_i \dots *_i x_{n+1}|_B$$

for $i = 1, 2$.

Now, it is clear that the operations s_1 and s_2 are idempotent, cyclic and commute with each other, hence they are equal as shown by the following calculation:

$$\begin{aligned}
&s_1(x_1, x_2, \dots, x_{n+1}) \\
&= s_2(s_1(x_1, x_2, \dots, x_{n+1}), \dots, s_1(x_1, x_2, \dots, x_{n+1})) \\
&= s_2(s_1(x_1, x_2, \dots, x_{n+1}), s_1(x_2, x_3, \dots, x_1), \dots, s_1(x_{n+1}, x_1, \dots, x_n)) \\
&= s_1(s_2(x_1, x_2, \dots, x_{n+1}), s_2(x_2, x_3, \dots, x_1), \dots, s_2(x_{n+1}, x_1, \dots, x_n)) \\
&= s_1(s_2(x_1, x_2, \dots, x_{n+1}), \dots, s_2(x_1, x_2, \dots, x_{n+1})) = s_2(x_1, x_2, \dots, x_{n+1}).
\end{aligned}$$

But then

$$m_1(x, y, z) = s_1(x, y, \dots, y, z) = s_2(x, y, \dots, y, z) = m_2(x, y, z)$$

which concludes the first part of the proof.

The second part of the proof follows from the fact that we can create a cyclic idempotent term operation for any generalized affine algebra by composing the appropriate restriction $m(x, y, z)$ of $xy^{-1}z$ in the same way as in the definition of the s_i. □

3. Systems of equations over finite algebras

In [10] we proved the following theorem.

Theorem 3.1 ([10])**.** *Let $\mathbb{A}$ be a finite algebra of finite signature. If $\mathbb{A}$ has no compatible Taylor operation then* SysPol($\mathbb{A}$) *is* **NP***-complete.*

As a consequence of this theorem, in our further investigations of SysPol($\mathbb{A}$) it suffices to study the cases where $\mathbb{A}$ has a compatible Taylor operation. Actually, our conjecture is that over such an algebra $\mathbb{A}$, SysPol($\mathbb{A}$) is polynomial-time.

Based on a polynomial-time algorithm of Dalmau, Gavaldà, Tesson and Thérien given in [3] we proved the following in [15].

Theorem 3.2 ([15])**.** *Let $\mathbb{M}$ be a finite semilattice of Abelian groups and $\mathcal{T}$ a finite relational structure of finite signature with a base set contained in $\mathbb{M}$. If the idempotent term operation $xy^{-1}z$ of $\mathbb{M}$ preserves the base set and the relations of $\mathcal{T}$, then there exists a polynomial-time algorithm for solving* $\mathrm{CSP}(\mathcal{T})$.

By using Theorem 2.1 as the main tool, in [15] we proved two dichotomy theorems that we reformulate below according to the new characterization of doubly Taylor algebras in Theorem 2.4.

Theorem 3.3 ([15])**.** *Let $\mathbb{A}$ be a finite algebra of finite signature that has a binary polynomial operation with an identity element. Then* $\mathrm{SysPol}(\mathbb{A})$ *is in* **P** *if $\mathbb{A}$ is generalized affine, and* $\mathrm{SysPol}(\mathbb{A})$ *is* **NP***-complete otherwise.*

Theorem 3.4 ([15])**.** *Let $\mathbb{A}$ be a finite algebra of finite signature that generates a variety omitting type* **1**. *Then* $\mathrm{SysPol}(\mathbb{A})$ *is in* **P** *if $\mathbb{A}$ is generalized affine, and* $\mathrm{SysPol}(\mathbb{A})$ *is* **NP***-complete otherwise.*

In this section we state and prove the following common generalization of Theorems 3.3 and 3.4.

Theorem 3.5. *Let $\mathbb{A}$ be a finite algebra of finite signature which has a separating set F of unary polynomial operations such that for every $f \in F$ there exists a binary polynomial operation g_f of $\mathbb{A}$ whose restriction to the set $f(A)$ is a binary operation with an identity element. Then* $\mathrm{SysPol}(\mathbb{A})$ *is in* **P** *if $\mathbb{A}$ is a reduct of a generalized affine algebra, and* $\mathrm{SysPol}(\mathbb{A})$ *is* **NP***-complete otherwise.*

Proof. Suppose first that $\mathbb{A}$ has a compatible Taylor operation t. Then by Theorem 2.2 the clone generated by t contains an idempotent ternary operation s that extends to the term operation $xy^{-1}z$ of a finite semilattice of Abelian groups. The operation s is a compatible operation of $\mathbb{A}$ and commutes with itself. Hence $\mathbb{A}$ is reduct of a generalized affine algebra, namely the algebra defined on A whose basic operations are all the operations commuting with s. Then by Theorems 1.1 and 3.2, $\mathrm{SysPol}(\mathbb{A})$ is in **P**.

If $\mathbb{A}$ has no compatible Taylor operation, then by Theorem 3.1, $\mathrm{SysPol}(\mathbb{A})$ is **NP**-complete. □

According to results from [7] (see Theorems 2.1 and 2.2 in [15]) the conditions of the preceding theorem are satisfied by any finite algebra of finite signature that omits type **1**. So we get the following generalization of Theorem 3.4.

Corollary 3.6. *Let $\mathbb{A}$ be a finite algebra of finite signature that omits type* **1**. *Then* $\mathrm{SysPol}(\mathbb{A})$ *is in* **P** *if $\mathbb{A}$ is a reduct of a generalized affine algebra, and* $\mathrm{SysPol}(\mathbb{A})$ *is* **NP***-complete otherwise.*

Note that Corollary 3.6 is a proper generalization of Theorem 3.4 since there are finite algebras $\mathbb{A}$ omitting type **1** such that the variety generated by $\mathbb{A}$ admits type **1**, see [7] for examples.

We saw in Theorem 1.1 that up to polynomial-time equivalence we may consider a SysPol problem as a CSP. By a result of Jeavons in [8], if the relations of two structures $\mathcal{S}$ and $\mathcal{T}$ are definable in a primitive positive way of each other's relations then CSP($\mathcal{S}$) and CSP($\mathcal{T}$) are polynomial-time equivalent. Hence SysPol($\mathbb{A}$) is polynomial-time equivalent to SysPol($\mathbb{B}$) where $\mathbb{B}$ is the algebra whose basic operations are all of the operations defined in a primitive positive way from the basic operations of $\mathbb{A}$. This observation and a result of Burris and Willard in [2], that there are finitely many primitive positive clones on a finite set, imply that on any fixed base set up to polynomial-time equivalence there are finitely many complexity classes for SysPol over the algebras of finite signature. No similar result is known for CSP. Also by the observation, one can strengthen Theorem 3.5, by replacing the polynomial operations in the claim by operations defined in a primitive positive way from the basic operations of the algebra and the constant operations.

References

[1] Barto, L., Kozik, M.: Full characterization of cyclic terms (for finite algebras) (2009, preprint)

[2] Burris, S., Willard, R.: Finitely many primitive positive clones, *Proceedings of the AMS*, **1**01, no. 3, 427–430 (1987)

[3] Dalmau, V., Gavaldà, R., Tesson, P., Thérien, D.: Tractable clones of polynomials over semigroups, *Electronic Colloquium on Computational Complexity*, Report No. **5**9 (2005)

[4] Feder, T., Madelaine, F., Stewart, I.A.: Dichotomies for classes of homomorphism problems involving unary functions, *Theoretical Computer Science*, **3**14, 1–43 (2004)

[5] Feder, T., Vardi, M. Y.: The Computational structure of monotone monadic SNP and constraint satisfaction: a study through datalog and group theory, *SIAM Journal of Computing*, **2**8, 57–104 (1998)

[6] Goldmann M., Russell, A.: The complexity of solving equations over finite groups.*Inform. and Comput.*, **1**78 no. 1, 253–262 (2002)

[7] Hobby, D., McKenzie, R.: The structure of finite algebras, *Contemporary Mathematics*, **7**6, American Mathematical Society, Providence, RI (1988)

[8] Jeavons, P. G.: On the algebraic structure of combinatorial problems, *Theoret. Comput. Sci.*, **2**00 no. 1–2, 185–204 (1998)

[9] Klíma, O., Tesson, P., Thérien, D.: Dichotomies in the complexity of solving systems of equations over finite semigroups, *Electronic Colloquium on Computational Complexity*, Report No. **9**1 (2004)

[10] Larose, B., Zádori, L.: Taylor terms, constraint satisfaction and the complexity of polynomial equations over finite algebras *Internat. J. Algebra Comput.*, **1**6, no. 3, 563–581 (2006)

[11] Larose, B., Zádori, L.: Bounded width problems and algebras, *Algebra Universalis*, **5**6, no. 3–4, 439–466 (2007)

[12] Maróti, M., McKenzie, R.: Existence theorems for weakly symmetric operations, *Algebra Universalis*, **5**9, no. 3-4, 463-489 (2008)

[13] Siggers, M. H.: A Strong Mal'cev Condition for Varieties Omitting the Unary Type, *Algebra Universalis* (in press)

[14] Taylor, W.: Varieties obeying homotopy laws, *Canadian J. Math.*, **2**9, 498–527 (1977)

[15] Zádori, L.: Solvability of systems of polynomial equations over finite algebras, *Internat. J. Algebra Comput.*, **1**7 no. 4, 821–835 (2007)

László Zádori

Bolyai Intézet, Aradi vértanúk tere 1, H-6720 Szeged, Hungary
e-mail: zadori@math.u-szeged.hu
URL: http://www.math.u-szeged.hu/∼zadori