International Journal of Algebra and Computation
Vol. 17, No. 4 (2007) 821–835
© World Scientific Publishing Company

World Scientific
www.worldscientific.com

SOLVABILITY OF SYSTEMS OF POLYNOMIAL EQUATIONS OVER FINITE ALGEBRAS

LÁSZLÓ ZÁDORI
Bolyai Intézet, Aradi vértanúk tere 1
H-6720, Szeged, Hungary
zadori@math.u-szeged.hu

Received 6 April 2006
Revised 3 December 2006

Communicated by R. R. McKenzie

We study the algorithmic complexity of determining whether a system of polynomial equations over a finite algebra admits a solution. We prove that the problem has a dichotomy in the class of finite groupoids with an identity element. By developing the underlying idea further, we present a dichotomy theorem in the class of finite algebras that admit a non-trivial idempotent Maltsev condition. This is a substantial extension of most of the earlier results on the topic.

Keywords: Constraint satisfaction; varieties; systems of polynomial equations; complexity.

Mathematics Subject Classification 1991: 08A70, 68Q17, 08B10.

1. Introduction

We investigate the complexity of determining if a given system of polynomial equations over a finite algebra admits a solution. For basic results in algorithmic complexity, we refer the reader to [14]. As usual, we use **P** and **NP** to denote the class of decision problems solvable in polynomial and non-deterministic polynomial time respectively. We say that a class of problems has a *dichotomy* if each of the problems from the class is either in **P** or **NP**-complete.

The problem we investigate has been studied and a dichotomy theorem has been obtained in the special cases of groups [4], monoids and some other subclasses of semigroups [8]. In [10], we adopted a new viewpoint of investigation and this led to a dichotomy result which encompasses the cases of lattices, rings, modules and quasigroups.

We introduce some basic notions in algebra. An *algebra* is a pair $\mathbb{A} = \langle A, \{f_i : i \in I\}\rangle$ where A is a non-empty set, I is a set and for each $i \in I$, f_i is an operation of finite arity n_i on A. The set A is called *the base set* of $\mathbb{A}$ and I with the map $i \mapsto n_i$

is called *the signature* of $\mathbb{A}$. The operations f_i are called the *basic operations* of $\mathbb{A}$. The algebra $\mathbb{A}$ is *finite* if A is finite and $\mathbb{A}$ is of *finite signature* if I is finite. Two algebras are *similar* if they have the same signature.

Let $\{x_1, x_2, \dots, x_n\}$ be a finite set of *variables.* If $\mathbb{A}$ is an algebra, an $\mathbb{A}$-*term*, built from the variables $x_1, x_2, \dots, x_n$ is defined as follows: (i) the variables $x_1, x_2, \dots, x_n$ are $\mathbb{A}$-terms and (ii) if f is an n-ary operation symbol and $g_1, \dots, g_n$ are $\mathbb{A}$-terms, then $f(g_1, \dots, g_n)$ is an $\mathbb{A}$-term. Every $\mathbb{A}$-term is interpreted as a *term operation* on an algebra similar to $\mathbb{A}$ in the natural way.

Polynomials of $\mathbb{A}$ are defined in a similar fashion. Let C be the set of operation symbols for all constant (0-ary) operations on A. By an $\mathbb{A}$-*polynomial* built from variables $x_1, x_2, \dots, x_n$, we mean an expression constructed as follows: (i) the variables $x_1, x_2, \dots, x_n$ are $\mathbb{A}$-polynomials, (ii) for every $c \in C$, c is an $\mathbb{A}$-polynomial and (iii) if p is an n-ary operation symbol and q_j are $\mathbb{A}$-polynomials then $p(q_1, \dots, q_n)$ is a $\mathbb{A}$-polynomial. The interpretation of a polynomial in the algebra $\mathbb{A}$ is defined in a straightforward manner. We shall feel free to use the polynomial expression to designate its associated polynomial function.

We shall investigate the algorithmic complexity of the following decision problem over a fixed (but arbitrary) finite algebra $\mathbb{A}$ of finite signature:

- SysPol($\mathbb{A}$)
  Input: A finite sequence of pairs (p_j, q_j) of $\mathbb{A}$-polynomials built from variables $x_1, x_2, \dots, x_n$.
  Question: Are there values $a_1, \dots, a_n \in A$ such that $p_j(a_1, \dots, a_n) = q_j(a_1, \dots, a_n)$ for all j?

A *relational structure* is a pair $\mathcal{T} = \langle T, \{r_j : j \in J\}\rangle$ where T is a non-empty set, J is a set and r_j is a relation on T of finite arity d_j, $j \in J$. The set T is called *the base set* of $\mathcal{T}$ and J with the map $j \mapsto d_j$ is called *the signature* of $\mathcal{T}$. The relations r_j are called the *basic relations* of $\mathcal{T}$. The structure $\mathcal{T}$ is *finite* if T is finite and $\mathcal{T}$ is of *finite signature* if J is finite. Two structures are *similar* if they have the same signature. Let $\mathcal{I} = \langle I, \{s_j : j \in J\}\rangle$ be a structure of signature J. A function $f : I \to T$ is a *homomorphism from* $\mathcal{I}$ *to* $\mathcal{T}$ if $f(s_j) \subseteq r_j$ for each $j \in J$.

Following Feder and Vardi [3], we define the *(restricted) constraint satisfaction problem (CSP)* for a fixed (but arbitrary) finite relational structure $\mathcal{T}$ of finite signature.

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

In passing, we note that CSP, which 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. The paper of Feder and Vardi [3] is a good source of ideas and tools to get acquainted with CSP.

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

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

If c is a constant (0-ary) operation then

$$c^\circ = \{c\}.$$

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. 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 $F \cup C$.*

We note that it follows from a result of Klíma, Tesson and Thérien [8] that for every finite structure $\mathcal{T}$, CSP($\mathcal{T}$) is polynomial-time equivalent to some SysPol($\mathbb{A}$) where $\mathbb{A}$ is a semigroup. So establishing a dichotomy for SysPol in the class of all finite algebras is equally hard as proving that CSP has a dichotomy in the class of all finite structures.

Let A be a finite, non-empty set. An operation f on A is *idempotent* if it satisfies the identity $f(x, \dots, x) = x$. An algebra $\mathbb{A}$ is *idempotent* if all of its basic operations are idempotent. We say that an algebra $\mathbb{A}$ *admits a non-trivial idempotent Maltsev condition*, if there exists a finite set of identities satisfied by some idempotent term operations of $\mathbb{A}$ that is not satisfied by projections of the two-element set. Admitting a non-trivial idempotent Maltsev condition is a decidable property of finite algebras of finite signature, see [6], and is even in **P** in the case of idempotent algebras, as shown in [1]. Most of the algebraic structures in classical algebra have this property, for example, algebras with a group or semilattice term operation.

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

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

where $x_j, y_j \in \{x, y\}$, for all $1 \le j \le n$. 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 asserts that idempotent Maltsev conditions and Taylor terms are equivalent concepts for finite algebras.

Theorem 1.2 [6, 18]. *A finite algebra admits a non-trivial idempotent Maltsev condition if and only if it has a Taylor term operation.*

Let A be a finite non-empty set, let θ be an h-ary relation on A and let f be an n-ary operation on A; we say that f *preserves* θ or that θ is *closed* under f if, given any matrix of size $h \times n$ with entries in A whose columns are elements of θ, applying the operation f to the rows of the matrix yields a column which is in θ. In particular, if $\mathbb{A} = \langle A, \{f_i : i \in I\}\rangle$ is an algebra and B is a non-empty unary relation closed under every f_i, then B is a *subalgebra* of $\mathbb{A}$; and if θ is an equivalence relation on A which is preserved by every f_i, then θ is a *congruence* of $\mathbb{A}$. The congruences of an algebra, ordered by inclusion, form a lattice.

A set of finitary operations on a fixed (but arbitrary) set is called a *clone* if it contains the projections and is closed under composition. The set of the term or polynomial operations of an algebra is a typical example of a clone. For any relational structure $\mathcal{T}$, the set of operations preserving the basic relations of the structure form a clone that we call *the clone of* $\mathcal{T}$. A clone is *idempotent* if all of its operations are idempotent. The following result reduces the study of the idempotent CSP to the class of those structures that admit a Taylor operation.

Theorem 1.3 [1, 9]. *Let* $\mathcal{T}$ *be a finite relational structure of finite type whose clone is idempotent and contains no Taylor operation. Then CSP*($\mathcal{T}$) *is* **NP**-complete.

Let $\mathbb{A}$ be a finite algebra of finite signature. By Theorem 1.1, SysPol($\mathbb{A}$) is polynomial-time equivalent to CSP($\langle A, R\rangle$) where R consists of all relations of the form f° where f is either a basic operation of the algebra $\mathbb{A}$ or a constant operation. Since all operations of the clone of $\langle A, R\rangle$ preserve every one-element subset of A, the clone of $\langle A, R\rangle$ is idempotent. So by Theorem 1.3, SysPol($\mathbb{A}$) is **NP**-complete if there is no Taylor operation that preserves all relations in R.

It is a simple exercise to verify the following: an operation t preserves the relation f° if and only if f preserves t°; if this is the case, we say that the operations f and t *commute*. Obviously, an operation t commutes with all the constant operations if and only if it is idempotent. Furthermore, an operation commutes with the term operations of an algebra if and only if it commutes with its basic operations. We say that an operation t is *compatible* with the algebra $\mathbb{A}$ if t commutes with every basic operation of $\mathbb{A}$. Consequently, by reformulating the criterion at the end of the previous paragraph we get:

Theorem 1.4 [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.*

A dichotomy for SysPol over all finite algebras yields a dichotomy for CSP over all finite structures and to decide the latter is considered hard. Hence, when we prove that SysPol has a dichotomy, we are compelled to make some assumptions on the structure of algebras we study. In the present paper, we investigate SysPol over the algebras that have a Taylor term operation, or equivalently admit a non-trivial idempotent Maltsev condition. This assumption on the algebras is weaker than the one we had in [10]. For example, every semilattice has a (binary) Taylor term operation but does not satisfy the requirements of the main theorem in [10].

Our strategy for proving a dichotomy theorem for SysPol over finite algebras with a Taylor term operation now is similar to the one we followed in [10]. We assume that $\mathbb{A}$ is a finite algebra of finite signature with a Taylor term operation and investigate the specific CSP related to SysPol($\mathbb{A}$), described in Theorem 1.1.

When doing this, by Theorem 1.4, we may consider only the case when $\mathbb{A}$ has a compatible Taylor operation. So we can restrict ourselves to the investigation of the specific CSP related to SysPol($\mathbb{A}$) where $\mathbb{A}$ has a Taylor term operation and a compatible Taylor operation. It will turn out that algebras with this latter property have a nice structure, which allows us to solve the specific CSP in polynomial time.

2. Preliminaries

We now present the relevant algebraic results and results from [10] that we need in the later proofs. For standard universal algebra, we refer the reader to [6, 12].

A *pseudovariety* is a class of similar algebras which is closed under finite products, subalgebras and homomorphic images. A *variety* (or equivalently an *equational class*) is a pseudovariety which is closed under arbitrary products. A variety $\mathcal{V}$ is *locally finite* if every finitely generated algebra in $\mathcal{V}$ is finite. For instance, the variety $\mathcal{V}(\mathbb{A})$ generated by a finite algebra $\mathbb{A}$, consisting of all homomorphic images of subalgebras of powers of $\mathbb{A}$, is locally finite. Tame congruence theory, first developed by Hobby and McKenzie in [6], is a powerful tool to study these varieties.

Let $\mathbb{A}$ be a finite algebra. If α and β are distinct congruences of $\mathbb{A}$ such that $\alpha \subseteq \beta$ but no congruence lies properly between them, then we say that the pair (α, β) is a *prime quotient* of congruences. In tame congruence theory, to each prime quotient is associated a *type* $i \in \{1, 2, 3, 4, 5\}$. We sketch briefly how this is done and also give some facts required from the theory for later proofs.

The starting point of the theory is to introduce a family of so-called (α, β)-*minimal* sets for each prime quotient (α, β) of congruences of $\mathbb{A}$. A unary operation r on a set A is called a *retraction*, if $r^2 = r$, in which case $r(A)$ is called a *retract* of A. We say that a subset U of $\mathbb{A}$ separates the congruences α and β if $\alpha|_U \neq \beta|_U$. It turns out that the (α, β)-minimal sets coincide with the minimal polynomial retracts of $\mathbb{A}$ that separate α and β. The following theorem, cf. [6, Exercise 2.9(2)], shows that the polynomial retractions corresponding to (α, β)-minimal sets separate the elements of $\mathbb{A}$.

Theorem 2.1 [6]. *For any two distinct elements a and b of a finite algebra $\mathbb{A}$, there is a prime quotient (α, β) of congruences of $\mathbb{A}$ and a polynomial retraction r of $\mathbb{A}$ such that $(r(a), r(b)) \in \beta \setminus \alpha$ and $r(\mathbb{A})$ is an (α, β)-minimal set.*

We call two algebras *polynomially equivalent* if they have the same base set and the same polynomial operations. Let U be an (α, β)-minimal set of $\mathbb{A}$. By restricting the polynomial operations of $\mathbb{A}$ that preserve U to U, we get a so-called (α, β)-*minimal algebra* on U. For any fixed (α, β), the corresponding (α, β)-minimal algebras turn out to be polynomially equivalent up to isomorphism. It is a crucial fact that any (α, β)-minimal algebra induces smaller fragmental algebras, so-called minimal algebras which have a very restrictive structure.

A finite algebra $\mathbb{A}$ is said to be *minimal* if every unary polynomial operation of $\mathbb{A}$ is either a constant or a permutation. A description of minimal algebras on more than two elements was given by Pálfy in [13]. By extending this description to the two-element case in [6], Hobby and McKenzie proved that, up to polynomial equivalence and isomorphism, the only minimal algebras are of the following 5 types:

1. algebras whose basic operations are permutations or constants;
2. vector spaces;
3. the 2-element Boolean algebra;
4. the 2-element lattice;
5. the 2-element semilattice.

It turns out that the minimal algebras induced by the same (α, β)-minimal algebra are polynomially equivalent up to isomorphism. Hence, every prime quotient (α, β) of congruences has a unique *type* 1–5. The collection of all types of all prime quotients (α, β) is called the *typeset* of $\mathbb{A}$. The *typeset of a variety* is the union of all typesets of its finite members.

By [6, Lemmas 4.15 and 4.20], (α, β)-minimal algebras possess certain well-behaved basic operations, provided that the type of (α, β) is different from type 1. As an immediate consequence of these results, we obtain the following theorem that plays a crucial role in the proof of the main result of this paper.

Theorem 2.2 [6]. *Let (α, β) be a prime quotient of congruences of an algebra $\mathbb{A}$ where the type of (α, β) differs from type* 1. *Then every (α, β)-minimal algebra of $\mathbb{A}$ has a binary basic operation with an identity element.*

Let i be an element of $\{1, 2, 3, 4, 5\}$. A finite algebra (a variety) is said to *omit type i* if its typeset does not contain type i. The connection between the typeset of a variety generated by a finite algebra and identities satisfied by the term operations of the algebra is illustrated in the following result, see [6, Lemma 9.4 and Theorem 9.6].

Theorem 2.3 [6]. *Let $\mathcal{V}(\mathbb{A})$ be the variety generated by a finite algebra $\mathbb{A}$. Then the following are equivalent*:

(i) $\mathcal{V}(\mathbb{A})$ *omits type* 1;
(ii) $\mathbb{A}$ *admits a non-trivial idempotent Maltsev condition*;
(iii) $\mathbb{A}$ *has a Taylor term operation.*

The next result was proved in [10] and independently by Seif [15].

Theorem 2.4 [10]. *Any finite algebra that has a compatible Taylor operation omits types* 3 *and* 4.

The following theorem states the main result of [10].

Theorem 2.5 [10]. *Let $\mathbb{A}$ be a finite algebra of finite signature and $\mathcal{V}(\mathbb{A})$ the variety generated by $\mathbb{A}$. Suppose that $\mathbb{A}$ omits type* 5 *and $\mathcal{V}(\mathbb{A})$ omits type* 1. *Then* $\mathrm{SysPol}(\mathbb{A})$ *is in* $\mathbf{P}$ *if $\mathbb{A}$ is polynomially equivalent to a module*, *and* $\mathrm{SysPol}(\mathbb{A})$ *is* $\mathbf{NP}$-*complete otherwise.*

In the remaining sections, we shall prove a similar but more sophisticated dichotomy theorem under the only assumption that $\mathcal{V}(\mathbb{A})$ omits type 1, i.e. $\mathbb{A}$ has a Taylor term operation.

3. Groupoids with an Identity Element and Compatible Taylor operation

The extension of a group with a new absorbing element is called a *group with zero.* The following characterization of finite monoids with a compatible Taylor operation is given in [10]. In this section, we shall extend this result to groupoids with an identity element.

Theorem 3.1 [10]. *For a finite monoid* $\mathbb{M}$, *the following are equivalent*:

(i) $\mathbb{M}$ *has a compatible Taylor operation.*
(ii) $\mathbb{M}$ *is a subdirect product of finite Abelian groups and finite Abelian groups with zero.*
(iii) $\mathbb{M}$ *is in the pseudovariety generated by the finite Abelian groups and finite semilattices.*

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 $\mathbb{S}$. We note that the equivalence of the last two conditions in the preceding theorem remains valid for arbitrary finite semigroups. For a proof of the following theorem, we refer to standard results in [5].

Theorem 3.2. *For a finite semigroup* $\mathbb{S}$, *the following are equivalent*:

(i) $\mathbb{S}$ *is a semilattice of finite Abelian groups.*
(ii) $\mathbb{S}$ *is a subpower of a finite Abelian group with zero.*
(iii) $\mathbb{S}$ *is a subdirect product of finite Abelian groups and finite Abelian groups with zero.*
(iv) $\mathbb{S}$ *is in the pseudovariety generated by the finite Abelian groups and finite semilattices.*

The semigroups satisfying the conditions of the preceding theorem are called finite *commutative Clifford semigroups* in semigroup theory. The semigroup operation of a commutative Clifford monoid is called *ccm-multiplication.* The *exponent* of a finite commutative Clifford semigroup is defined to be the least common multiplier of the exponents of its subgroups. We note that any finite commutative Clifford semigroup $\mathbb{S}$ has a unique idempotent term operation of the form $xy^{n-1}z,\ n > 1$. Indeed, if there are two such operations corresponding to m and n, respectively, then by idempotency, $x^{m+1} = x^{n+1}$ for all $x \in S$. Hence, the exponent of $\mathbb{S}$ divides $m - n$, and $y^{m-1} = y^{n-1}$, i.e. the operations $xy^{m-1}z$ and $xy^{n-1}z$ coincide.

The following theorem states the main result of the section.

Theorem 3.3. *Let M be a finite set. Let xy be a binary operation with an identity element and t a Taylor operation on M such that xy commutes with t. Then the following hold:*

(i) *xy is a ccm-multiplication on M.*

(ii) *The clone generated by t contains an idempotent ternary operation of the form $xy^{n-1}z$.*

Proof. Let $\mathbb{M}$ denote the the groupoid with base set M and basic operation xy. The identity element of $\mathbb{M}$ is denoted by 1 and we assume that t has arity k.

By Theorem 3.1, to prove the first claim of the theorem it suffices to show that $\mathbb{M}$ is a monoid. Since t is a Taylor operation, t is idempotent and for every $1 \leq i \leq k$, t satisfies an identity

$$t(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_k) = t(y_1, \ldots, y_{i-1}, y, y_{i+1}, \ldots, y_k)$$

where $x_j, y_j \in \{x, y\}$, for all $1 \leq j \leq k$.

We introduce the following notation:

$t_i(x) = t(1, \ldots, 1, x, 1, \ldots, 1)$ where x stands in the ith position;

$s_i(x) = t(1, \ldots, 1, x, \ldots, x)$ where the 1's stand in the first i positions;

$s(x) = t(x, \ldots, x)$.

We shall prove that $\mathbb{M}$ is associative. Let a, b and c be any element in $\mathbb{M}$. By using the first Taylor identity, we have that

$$t(a, z_2, \ldots, z_k) = t(1, w_2, \ldots, w_k)$$

where $z_i, w_i \in \{a, 1\}$. Let

$$\overline{z}_i = \begin{cases} 1, & \text{if } z_i = a, \\ a, & \text{if } z_i = 1. \end{cases}$$

Now we get that

$$\begin{aligned} s(a) &= t(a, z_2, \ldots, z_k)\, t(1, \overline{z}_2, \ldots, \overline{z}_k) \\ &= t(1, w_2, \ldots, w_k)\, t(1, \overline{z}_2, \ldots, \overline{z}_k) \\ &= t(1, w_2\overline{z}_2, \ldots, w_k\overline{z}_k). \end{aligned}$$

By using the expression obtained for $s(a)$, we get

$$\begin{aligned} (ab)c &= (s(a)s(b))s(c) \\ &= (t(1, w_2\overline{z}_2, \ldots, w_k\overline{z}_k)s(b))s(c) \\ &= t(bc, ((w_2\overline{z}_2)b)c, \ldots, ((w_k\overline{z}_k)b)c) \\ &= t_1(bc)t(1, ((w_2\overline{z}_2)b)c, \ldots, ((w_k\overline{z}_k)b)c) \\ &= t_1(bc)((t(1, w_2\overline{z}_2, \ldots, w_k\overline{z}_k)s_1(b))s_1(c)) \\ &= t_1(bc)((s(a)s_1(b))s_1(c)). \end{aligned}$$

Then by the use of the second Taylor identity similarly as before, we get

$$(s(a)s_1(b))s_1(c) = t_2(bc)((s(a)s_2(b))s_2(c))$$

and so

$$(ab)c = t_1(bc)(t_2(bc)((s(a)s_2(b))s_2(c)).$$

By repeating the preceding argument, using the other Taylor identities and $s_k(b) = s_k(c) = s(1) = 1$, we get

$$\begin{aligned}(ab)c &= t_1(bc)(t_2(bc)\cdots(t_k(bc)((s(a)s_k(b))s_k(c))\cdots)\\ &= t_1(bc)(t_2(bc)\cdots(t_k(bc)s(a))\cdots)\\ &= t((bc)a,\ldots,(bc)a)\\ &= (bc)a.\end{aligned}$$

Thus, for any $a, b, c \in \mathbb{M}$, $(ab)c = (bc)a$. In particular, by letting $b = 1$, we get $ac = ca$, i.e. $\mathbb{M}$ is commutative. Hence, $(ab)c = a(bc)$ for any $a, b, c \in \mathbb{M}$, i.e. $\mathbb{M}$ is associative.

Now, we prove the second claim of the theorem. By the first claim of the theorem, $\mathbb{M}$ is a commutative Clifford monoid. Let $\mathbb{E}$ denote the semilattice of the idempotent elements of $\mathbb{M}$. For every $e \in E$, let $\mathbb{G}_e$ be the group of elements of M with a power that equals e. Then M is the disjoint union of the G_e. Let n denote the exponent of $\mathbb{M}$. Then $m(x, y, z) = xy^{n-1}z$ clearly is an idempotent operation on M.

We want to show that m is in the clone generated by t. This statement was already verified in [10] when xy is a group operation and in [7] when xy is a semilattice operation, cf. [10, Lemmas 3.6, 3.8 and Theorem 3.10] and [7, Lemma 3.6]. Since, in case of $n = 1$, the operation xy is a semilattice operation, we assume $n > 1$. It is easy to see, since t is idempotent and commutes with xy, that E and the G_e are closed under t. The same sets are also closed under xy. Hence t, with a componentwise action, is a Taylor operation on the product G of the G_e. Moreover, t commutes with the group operation xy on G. By the group result mentioned at the beginning of the paragraph, m on G coincides with a ternary term operation in the clone generated by t on G.

Let $[t]$ denote the clone generated by t on M. Because of the similar claim just mentioned for G, there is a ternary idempotent operation $g \in [t]$ such that $g|_{G_e} = m|_{G_e}$ for all $e \in E$. By the semilattice result, there is a binary idempotent term operation $s \in [t]$ such that $s|_E(x, y) = xy|_E$. Our aim is to find an operation in $[t]$ that coincides with m. The initial candidate for such an operation is g, but g may not be equal to m when restricted to E. This defect of g can be eliminated as follows.

Let F be a maximal upwardly closed set of E with the property that there is a ternary operation $h \in [t]$ satisfying $h|_{G_e} = m|_{G_e}$ for all $e \in E$ and $h|_F = m|_F$. Let g be a ternary operation in $[t]$ such that g witnesses the maximality of F. We claim that $F = E$. Suppose that the claim does not hold and let f be a maximal element of $E \setminus F$. Since g commutes with xy and is idempotent

$$g(1, f, f)g(f, f, 1) = g(f, f, f) = f.$$

So either both of $g(1, f, f)$ and $g(f, f, 1)$ are in F, or one of them equals f, say $g(1, f, f) = f$. In the first case, for any $f_i \in F \cup \{f\},\ i = 1, 2, 3$, there exist elements $e_i, e'_i \in F,\ i = 1, 2, 3$, such that $f_i = e_i e'_i, i = 1, 2, 3$, and

$$g(f_1, f_2, f_3) = g(e_1, e_2, e_3)g(e'_1, e'_2, e'_3) = e_1e_2e_3e'_1e'_2e'_3 = f_1f_2f_3,$$

which contradicts the maximality of F. Hence $g(1, f, f) = f$.

We define

$$u(x, y) = g(x, s(x, y), s(x, y)) \in [t].$$

By the properties of g and s for all $e \in E$ and $x, y \in G_e$

$$u(x, y) = xs(x, y)^n = xy^n,$$

and for all $x, y \in F \cup \{f\}$, as $g(1, y, y) = y$ and $y = y^n$ in this case,

$$u(x, y) = g(x, s(x, y), s(x, y)) = g(x, xy, xy) = g(x, x, x)g(1, y, y) = xy^n.$$

Let

$$v(x, y, z) = s(s(x, y), z).$$

Observe that $v|_E = m|_E$.

Let

$$g'(x, y, z) = g(v(x, u(x, y), u(x, z)), v(u(y, x), y, u(y, z)), v(u(z, x), u(z, y), z)).$$

Clearly, $g' \in [t]$. Moreover, for all e and $x, y, z \in G_e$ or $x, y, z \in F \cup \{f\}$

$$\begin{aligned} g'(x, y, z) &= g(v(x, xy^n, xz^n), v(yx^n, y, yz^n), v(zx^n, zy^n, z)) \\ &= g(v(x^{n+1}, xy^n, xz^n), v(yx^n, y^{n+1}, yz^n), v(zx^n, zy^n, z^{n+1})) \\ &= g(xv(x^n, y^n, z^n), yv(x^n, y^n, z^n), zv(x^n, y^n, z^n)) \\ &= g(x, y, z)v(x^n, y^n, z^n) \\ &= m(x, y, z). \end{aligned}$$

Thus, $g' \in [t]$ satisfies $g'|_{G_e} = m|_{G_e}$ for all $e \in E$ and $g'|_{F\cup\{f\}} = m|_{F\cup\{f\}}$, a contradiction.

So far we have proved that there exists $g \in [t]$ such that $g|_{G_e} = m|_{G_e}$ for all $e \in E$ and $g|_E = m|_E$. Now, for any $x, y, z \in M$

$$\begin{aligned} g(x, y, z) &= g(x, y, z)g(x^n, y^n, z^n) \\ &= g(x, y, z)m(x^n, y^n, z^n) \\ &= g(xm(x^n, y^n, z^n), ym(x^n, y^n, z^n), zm(x^n, y^n, z^n)) \\ &= m(xm(x^n, y^n, z^n), ym(x^n, y^n, z^n), zm(x^n, y^n, z^n)) \\ &= m(x, y, z)m(x^n, y^n, z^n) \\ &= m(x, y, z). \end{aligned}$$

Thus, $g = m$ and this concludes the proof. □

We remark that the proof of the second claim of the preceding theorem can be made constructive by determining a term in $[t]$ that interprets as $xy^{n-1}z$. The procedure to construct such a term in the group case was pointed out to the author by Szendrei. Her construction is based on results contained in [16, 17]. On the other hand, in the semilattice case, a term in $[t]$ that interprets as xy can be constructed as follows. Let

$$t_i(x, y) = t(y, \ldots, y, x, y, \ldots, y)$$

where x on the right-hand side is in the ith position, and $i = 1, \ldots, k$. Notice that by the ith Taylor identity for t

$$t_i(1, y) = y \quad \text{ and hence } t_i(x, y) = t_i(x, 1)y.$$

Then

$$xy = t_1(x, t_2(x, \ldots, t_{k-1}(x, t_k(x, y)) \cdots)).$$

So the terms s and g in the proof of Theorem 3.3 can be constructed in $[t]$, and hence, by going along the lines of the proof, a term that interprets as $xy^{n-1}z$ can also be constructed in $[t]$.

The restriction of the following theorem to the class of monoids was proved earlier by Klíma, Tesson and Thérien in [8]. Combining their theorem with Theorems 1.4 and 3.3, we get the following result.

Theorem 3.4. *Let* $\mathbb{M}$ *be a finite groupoid with an identity element. Then* SysPol($\mathbb{M}$) *is in* **P** *if* $\mathbb{M}$ *is a commutative Clifford monoid, and* SysPol($\mathbb{M}$) *is* **NP**-complete otherwise.

4. Doubly Taylor Algebras and the Main Result

A *Taylor algebra* is an algebra with a Taylor term operation. A *doubly Taylor algebra* is a Taylor algebra with a compatible Taylor operation. In this section, we investigate the structure of doubly Taylor algebras. As an application of the results obtained, we prove a dichotomy theorem for SysPol over finite algebras admitting a non-trivial idempotent Maltsev condition.

Theorem 4.1. *Every finite idempotent doubly Taylor algebra is a subalgebra of a finite idempotent Taylor algebra with a compatible ccm-multiplication.*

Proof. Let $\mathbb{A}$ be a finite idempotent doubly Taylor algebra. Let $\mathbb{A}^*$ be the algebra whose base set equals that of $\mathbb{A}$ and whose basic operations coincide with the compatible operations of $\mathbb{A}$. By Theorem 2.1, for any two distinct elements a and b of $\mathbb{A}^*$, there is a prime congruence quotient (α, β) of $\mathbb{A}^*$ and a polynomial retraction r of $\mathbb{A}^*$ such that $(r(a), r(b)) \in \beta \setminus \alpha$ and $r(\mathbb{A}^*)$ is an (α, β)-minimal set. Since $\mathbb{A}$ is idempotent, the unary polynomial operations of $\mathbb{A}^*$ are endomorphisms of the algebra $\mathbb{A}$. Hence, $r(\mathbb{A}^*) = r(\mathbb{A})$ are subalgebras of $\mathbb{A}$, and $\mathbb{A}$ is a subdirect product of them as r separate the elements of $\mathbb{A}$. Since $\mathbb{A}$ is doubly Taylor, all the $r(\mathbb{A}^*)$ are also doubly Taylor. By Theorems 2.3 and 2.4, the type of (α, β) is 2 or 5. Hence, by Theorem 2.2, all the (α, β)-minimal algebras $r(\mathbb{A}^*)$ have a groupoid term operation with an identity element. By applying now Theorem 3.3, the algebras $r(\mathbb{A}^*)$ all have ccm-multiplication as a term operation. This ccm-multiplication is a compatible operation of the algebra $r(\mathbb{A})$. Finally, $\mathbb{A}$ is a subalgebra of the product of the algebras $r(\mathbb{A})$ and the compatible ccm-multiplications of $r(\mathbb{A})$ yield a compatible ccm-multiplication on the product. The product is an idempotent Taylor algebra, as it inherits the relevant properties of $\mathbb{A}$. □

The proof of the preceding theorem yields:

Corollary 4.2. *Every finite subdirectly irreducible idempotent doubly Taylor algebra has a compatible ccm-multiplication.*

The following is an immediate consequence of Corollary 4.2 and Theorem 3.3.

Corollary 4.3. *Every finite subdirectly irreducible idempotent doubly Taylor algebra $\mathbb{A}$ has an idempotent compatible term operation of the form $xy^{n-1}z$ where xy is a compatible ccm-multiplication of $\mathbb{A}$.*

Now, we give a characterization of doubly Taylor algebras.

Theorem 4.4. *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 $xy^{n-1}z$ of a finite commutative Clifford monoid.*

Proof. Let $\mathbb{B}$ be a finite doubly Taylor algebra with base set B. Without loss of generality, we assume that $\mathbb{B}$ contains all constant operations of B. Let $\mathbb{A}$ be the idempotent doubly Taylor algebra on B whose basic operations are the compatible operations of $\mathbb{B}$. By Theorem 4.1, there is an idempotent Taylor algebra $\mathbb{C}$ such that $\mathbb{A}$ is a subalgebra of $\mathbb{C}$ and $\mathbb{C}$ has a compatible ccm-multiplication xy. By Theorem 3.3, $\mathbb{C}$ has $xy^{n-1}z$ as its term operation. Hence, B is closed under $xy^{n-1}z$ and the restriction of $xy^{n-1}z$ to B yields a compatible idempotent ternary operation of $\mathbb{B}$. Thus, C with the ccm-multiplication xy is a finite commutative Clifford monoid, as required in the claim.

To prove the other direction of the claim, let $\mathbb{B}$ denote a finite Taylor algebra and $m(x, y, z)$, a compatible operation of $\mathbb{B}$ that extends to an idempotent term operation $xy^{n-1}z$ of a finite commutative Clifford monoid. Then

$$x_1 x_2 \cdots x_{n+1}|_B = m(x_1, x_{n+1}, m(x_2, x_{n+1}, \ldots, m(x_n, x_{n+1}, x_{n+1}), \ldots)$$

is a compatible Taylor operation of $\mathbb{B}$. Thus, $\mathbb{B}$ is a doubly Taylor algebra. □

By using the above characterization of doubly Taylor algebras, we shall prove the main theorem of this paper. We require the following reduction theorem, see [1, Corollary 3].

Theorem 4.5 [1]. *Let $\mathbb{A}$ be a finite algebra such that for every finite structure $\mathcal{S}$ of finite signature whose base set coincides with that of $\mathbb{A}$ and whose relations are finite subpowers of $\mathbb{A}$, there is a polynomial-time algorithm for solving CSP($\mathcal{S}$). Then for every finite member $\mathbb{B}$ of the variety generated by $\mathbb{A}$ and every structure $\mathcal{T}$ of finite signature whose base set coincides with that of $\mathbb{B}$ and whose relations are finite subpowers of $\mathbb{B}$, there is a polynomial-time algorithm for solving CSP($\mathcal{T}$).*

In [2], Dalmau *et al.* describe a polynomial-time algorithm for solving a special type of CSP. Their algorithm is put together from a local (so-called bounded width) algorithm and an algorithm that solves CSP for coset structures of a group. In fact, the following theorem that we require is a special case of [2, Theorem 3].

Theorem 4.6 [2]. *Let $\mathbb{M}$ be a finite commutative Clifford semigroup with exponent n and $\mathcal{T}$, a finite relational structure of finite signature whose base set equals that of $\mathbb{M}$. If the idempotent term operation $xy^{n-1}z$ of $\mathbb{M}$ preserves the base set and the relations of $\mathcal{T}$, then there exists a polynomial-time algorithm for solving CSP($\mathcal{T}$).*

By the previous two theorems we get the following.

Theorem 4.7. *Let $\mathbb{M}$ be a finite commutative Clifford semigroup and $\mathcal{T}$, a finite relational structure of finite signature with a base set contained in $\mathbb{M}$. If the idempotent term operation $xy^{n-1}z$ of $\mathbb{M}$ preserves the base set and the relations of $\mathcal{T}$, then there exists a polynomial-time algorithm for solving CSP($\mathcal{T}$).*

Proof. Let $\mathbb{G}$ be a finite Abelian group and $\mathbb{G}_0$, the extension of $\mathbb{G}$ with zero such that $\mathbb{M}$ is a subsemigroup of $\mathbb{G}_0^l$ for some finite l. Without loss of generality, we may assume that n equals the exponent of $\mathbb{G}$. Let m denote the term operation $xy^{n-1}z$ of $\mathbb{G}_0$. By Theorem 4.5, it suffices to show that for every structure $\mathcal{S}$ of finite signature whose base set is G_0 and relations are finite subpowers of the algebra $\langle G_0, m\rangle$, there is a polynomial-time algorithm for solving CSP($\mathcal{S}$). But this follows by Theorem 4.6, which concludes the proof. □

Now, by putting together Theorems 1.2, 1.4, 4.4 and 4.7, we get our main result.

Theorem 4.8. *Let $\mathbb{A}$ be a finite algebra of finite signature that admits a non-trivial idempotent Maltsev condition. Then* SysPol($\mathbb{A}$) *is in* **P** *whenever $\mathbb{A}$ has a compatible idempotent ternary operation that extends to the idempotent term operation $xy^{n-1}z$ of a finite commutative Clifford monoid, and* SysPol($\mathbb{A}$) *is* **NP***-complete otherwise.*

In the introduction, we have already mentioned the following result of Klíma, Tesson and Thérien in [8], although not in its precise form: for any finite structure $\mathcal{T}$ of finite signature, there is a finite right normal band $\mathbb{B}$ such that CSP($\mathcal{T}$) is polynomial-time equivalent to SysPol($\mathbb{B}$). In this respect, we note that apart from semilattices, every finite right normal band generates a variety whose type set contains type 1. Hence, Theorem 4.8 says nothing about SysPol over right normal bands different from semilattices. Thus, it is not possible to combine the theorem of Klíma *et al.* with Theorem 4.8 to prove that CSP has dichotomy over all finite structures.

The following theorem suggested by Larose generalizes Theorem 3.4 and covers some of the type 1 cases, not the case of right normal bands though.

Theorem 4.9. *Let* $\mathbb{A}$ *be a finite algebra of finite signature that has a binary polynomial operation* xy *with an identity element. Then* $\mathrm{SysPol}(\mathbb{A})$ *is in* $\mathbf{P}$ *if* xy *is a ccm-multiplication and the idempotent ternary operation* $xy^{n-1}z$ *is a compatible operation of* $\mathbb{A}$, *and* $\mathrm{SysPol}(\mathbb{A})$ *is* $\mathbf{NP}$*-complete otherwise.*

Proof. By Theorem 1.4, it suffices to consider only the case when $\mathbb{A}$ has a compatible Taylor operation. Let t be a compatible Taylor term operation of $\mathbb{A}$. Then, by the first claim of Theorem 3.3, xy is a ccm-multiplication. Since xy commutes with t, by the second claim of Theorem 3.3, the idempotent polynomial operation $xy^{n-1}z$ is in the clone $[t]$. Hence, $xy^{n-1}z$ is a compatible operation of $\mathbb{A}$, and by Theorem 4.6, $\mathrm{SysPol}(\mathbb{A})$ is in $\mathbf{P}$. □

We note that, during the editorial process of this paper, Maróti and McKenzie proved in [11] that every finite Taylor algebra has a so-called weak near-unanimity term operation. A weak near-unanimity operation is a special Taylor operation t which satisfies the following identities

$$t(y,x,\dots,x)=t(x,y,\dots,x)=\cdots=t(x,\dots,x,y).$$

In connection with the result of Maróti and McKenzie, the anonymous referee of this paper pointed out that the use of the identities for weak near-unanimity may reduce the complexity of notation introduced in the proof of the first part of Theorem 3.3. It is not clear at this point whether their new result may lead to a simpler proof, perhaps avoiding tame congruence theory, of the characterization of doubly Taylor algebras given in Theorem 4.4.

Acknowledgment

The author's research is supported by OTKA grants T034175, K60148 and T48809.

References

[1] A. Bulatov and P. Jeavons, Algebraic structures in combinatorial problems, Technical Report MATH AL-4-2001, Technische Universität Dresden (2001).

[2] V. Dalmau, R. Gavaldà, P. Tesson and D. Thérien, Tractable clones of polynomials over semigroups, *Electronic Colloquium on Computational Complexity*, Report No. 59 (2005).

[3] T. Feder and M. Y. Vardi, The computational structure of monotone monadic SNP and constraint satisfaction: A study through datalog and group theory, *SIAM J. Comput.* **28** (1998) 57–104.

[4] M. Goldmann and A. Russell, The complexity of solving equations over finite groups, *Inform. and Comput.* **178**(1) (2002) 253–262.

[5] P. A. Grillet, *Semigroups, An Introduction to the Structure Theory*, Monographs and Textbooks in Pure and Applied Mathematics, Vol. 193 (Marcel Dekker, New York, 1995), p. 398.

[6] D. Hobby and R. McKenzie, *The Structure of Finite Algebras*, Contemporary Mathematics, Vol. 76 (American Mathematical Society, Providence, RI, 1988).

[7] K. Kearnes and Á. Szendrei, Self-rectangulating varieties of type 5, *Internat. J. Algebra Comput.* **7**(4) (1997) 511–540.

[8] O. Klíma, P. Tesson and D. Thérien, Dichotomies in the complexity of solving systems of equations over finite semigroups, *Electronic Colloquium on Computational Complexity*, Report No. 91 (2004).

[9] B. Larose and L. Zádori, The complexity of the extendibility problem for finite posets, *SIAM J. Discrete Math.* **17**(1) (2003) 114–121.

[10] B. Larose and L. Zádori, Taylor terms, constraint satisfaction and the complexity of polynomial equations over finite algebras, *Internet. J. Algebra Comput.* **16**(3) (2006) 563–581.

[11] M. Maróti and R. McKenzie, Existence theorems for weakly symmetric operations, *Algebra Universalis*, submitted.

[12] R. N. McKenzie, G. F. McNulty and W. F. Taylor, *Algebras, Lattices and Varieties* (Wadsworth and Brooks/Cole, Monterey, CA, 1987).

[13] P. P. Pálfy, Unary polynomials in algebras I, *Algebra Universalis* **18** (1984) 262–273.

[14] C. H. Papadimitriou, *Computational Complexity* (Addison-Wesley, 1994).

[15] S. Seif, private communication.

[16] Á. Szendrei, On the idempotent reducts of modules I, in *Universal Algebra* (Proc. Conf. Esztergom, 1977), *Colloquia Mathematica Societatis János Bolyai*, Vol. 29 (North-Holland, Amsterdam, New York, Oxford, 1982), pp. 753–767.

[17] Á. Szendrei, On the idempotent reducts of modules II, in *Universal Algebra* (Proc. Conf. Esztergom, 1977), *Colloquia Mathematica Societatis János Bolyai*, Vol. 29 (North-Holland, Amsterdam, New York, Oxford, 1982), pp. 769–780.

[18] W. Taylor, Varieties obeying homotopy laws, *Canad. J. Math.* **29** (1977) 498–527.