International Journal of Algebra and Computation
Vol. 16, No. 3 (2006) 563–581

World Scientific
www.worldscientific.com

TAYLOR TERMS, CONSTRAINT SATISFACTION AND THE COMPLEXITY OF POLYNOMIAL EQUATIONS OVER FINITE ALGEBRAS

BENOIT LAROSE

Department of Mathematics and Statistics
Concordia University, 1455 de Maisonneuve West
Montréal, Qc, Canada, H3G 1M8
larose@mathstat.concordia.ca
http://cicma.mathstat.concordia.ca/faculty/larose/

LÁSZLÓ ZÁDORI

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

Received 7 April 2004
Revised 15 May 2005

Communicated by R. McKenzie

We study the algorithmic complexity of determining whether a system of polynomial equations over a finite algebra admits a solution. We characterize, within various families of algebras, which of them give rise to an **NP**-complete problem and which yield a problem solvable in polynomial time. In particular, we prove a dichotomy result which encompasses the cases of lattices, rings, modules, quasigroups and also generalizes a result of Goldmann and Russell for groups [15].

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

Mathematics Subject Classification 2000: Primary 08A70; Secondary 68Q17, 08B10

1. Introduction

We investigate the complexity of determining if a given system of polynomial equations over a finite algebra admits a solution. This problem has been studied in the special cases of groups [15], monoids [21, 30, 43], and similar decision problems are also considered in [37–39] in the case of semigroups. The constraint satisfaction problems studied in [12] can also be viewed as problems of systems of equations over unary algebras. The counting version of systems of equations is investigated in [24, 31], and the case of counting solutions of CSPs is discussed in [5, 6]. Various decision and counting problems over finite lattices are studied in [35].

Let $\mathbb{A}$ be a finite algebra of finite signature, i.e. a pair $\mathbb{A} = \langle A, \{f_i : i \in I\}\rangle$ where A, the *universe* of $\mathbb{A}$, is a finite non-empty set, I is a finite set of *operation symbols*, equipped with a function $t : I \to \mathbb{N}$, where $t(i)$ is the *arity* of the operation symbol i, and for each $i \in I$, f_i is a $t(i)$-ary operation on A, i.e. a function $f_i : A^{t(i)} \to A$. The algebra is *non-trivial* if $|A| > 1$. The operations f_i are called the *basic* or *fundamental operations* of $\mathbb{A}$. Let $\{x_1, x_2, \ldots\}$ be a countable set of *variables* and let C be the set of operation symbols for all constant (0-ary) operations on A. By a *polynomial* of $\mathbb{A}$ we mean an expression built from variables and operation symbols from $I \cup C$ as usual: (i) for every k, x_k is a polynomial, (ii) for every $c \in C$, c is a polynomial and (iii) if p is an n-ary operation symbol and q_j are polynomials then $p(q_1, \ldots, q_n)$ is a polynomial. The interpretation of a polynomial in the algebra $\mathbb{A}$ is defined in a straightforward manner and we shall feel free to use the polynomial expression to designate its associated polynomial function. It will also be convenient to use the following convention: if $\overline{a} = a_1, a_2, \ldots$ is a sequence of elements of A and p is a polynomial of $\mathbb{A}$, then $p(\overline{a})$ shall denote the value of the polynomial operation of $\mathbb{A}$ corresponding to p when we replace each occurence of the variable x_k in p by a_k.

As usual, we use the names $x, y, z, \ldots$ for variables, symbols such as $+, \cdot, \wedge, \vee, \ldots$ for our operations symbols, and write expressions such as $x \wedge y$ instead of the more cumbersome $\wedge(x, y)$. Here are some typical polynomials for various classical algebras; in these examples $a, b, c, d, \ldots$ denote elements of the universe A (constants). We can view modules as universal algebras by defining, for every element r of the (unitary) ring R a unary operation $f_r(x) = rx$ for all $x \in A$.

lattices	$\mathbb{A} = \langle A; \vee, \wedge\rangle$	$((x \vee c) \wedge (x \vee d)) \vee (y \wedge z)$
semigroups	$\mathbb{A} = \langle A; \cdot\rangle$	$xa^3z^4bx^4b^3uxy$
groups	$\mathbb{A} = \langle A; \cdot, ^{-1}\rangle$	$x^{-5}a^3z^{-4}bx^4b^3ux^{-1}y$
rings	$\mathbb{A} = \langle A; \cdot, +, -, 0\rangle$	$xa^3z^4 + bx^4b^3 + uxyb^{12} + c$
modules	$\mathbb{A} = \langle A; +, 0, \{f_r : r \in R\}\rangle$	$r_1x + r_2y + r_3z + a$
etc.	$\mathbb{A} = \langle A; F\rangle$	$f(x, g(d, y, h(x, y), g(x, z, u, y)), f(a, d, x))$

We shall investigate the algorithmic complexity of the following decision problem:

- $SysPol(\mathbb{A})$
  Input: A finite sequence of pairs of polynomials (p_j, q_j) of $\mathbb{A}$.
  Question: Are there values $a_i \in A$ such that

$$p_j(\overline{a}) = q_j(\overline{a}) \text{ for all } j?$$

We will show that this problem is equivalent (via log-space reductions) to a constraint satisfaction problem (CSP) of a very specific form (Theorem 2.2). CSPs, which include such standard decision problems as 3-satisfiability, graph

unreachability and graph k-colorability, have attracted a great deal of attention in the last few years, see for instance [6, 10, 11, 14, 22, 23, 26, 27]. A conjecture of Feder and Vardi [13] states that a CSP is either solvable in polynomial time or is **NP**-complete. Using a connection between finite algebras and CSPs first uncovered by Jeavons [18] and further developed in [7], Bulatov has generalized Schaefer's Dichotomy Theorem for structures on 2 elements [34] to various classes of CSPs [2–4]. We note that it follows from a result of Klima, Tesson and Thérien [21] that the dichotomy conjecture actually reduces to proving dichotomy for the problems $SysPol(\mathbb{A})$ where $\mathbb{A}$ is a semigroup.

A precise dichotomy conjecture for CSPs was stated by Bulatov, Krokhin and Jeavons in [7] (see [8] for the correctly reformulated conjecture): loosely speaking, to each CSP is associated a finite algebra, which we can assume without loss of generality to have only surjective term operations. The conjecture then states that the associated CSP is solvable in polynomial time if the algebra has no factor which is a G-set. We use an alternative approach (which is equivalent to the above by standard results in tame congruence theory): to each CSP is associated a finite relational structure, and without loss of generality we may assume that this structure is a *core*, i.e. that all endomorphisms of the structure are automorphisms. The conjecture may be phrased as follows (Taylor operations are idempotent operations satisfying special identities, see below):

Dichotomy Conjecture [7]. *Let R be a core. If the structure R is invariant under a Taylor operation then $CSP(R)$ is in* **P**; *otherwise it is* **NP***-complete.*

The fact that structures that admit no compatible Taylor operation have an **NP**-complete CSP (Theorem 2.3) is the key tool we use in proving hardness result (see [7, 25]). Because of the very special nature of the CSP's we shall investigate, this criterion turns out to have a very nice interpretation in our setting: the problem $SysPol(\mathbb{A})$ is **NP**-complete if there is no Taylor operation that commutes with the basic operations of the algebra $\mathbb{A}$. In many instances this criterion will suffice to characterize the tractable cases and confirm the dichotomy conjecture. In particular, we shall determine precisely which algebras yield a tractable problem and which give rise to an **NP**-complete problem for various classes of classic algebras such as rings (Corollary 3.16) and quasigroups (Corollary 3.17). In [35] it is shown that, over a finite lattice, deciding if one equation has a solution is solvable in polynomial-time if the lattice is distributive and **NP**-complete otherwise. We prove an analog of this last hardness result by proving that solving a system of polynomial equations over any non-trivial lattice is **NP**-complete (Corollary 3.4). In fact, we will show quite a bit more: this holds over any finite algebra in a congruence-distributive variety. We shall also generalize the dichotomy result for groups first proved by Goldmann and Russell [15], by proving that if $\mathbb{A}$ is an algebra in a congruence-modular variety, then the problem $SysPol(\mathbb{A})$ is solvable in polynomial time if $\mathbb{A}$ is polynomially equivalent to a module and **NP**-complete otherwise (Corollary 3.14). In fact, this itself is a special case of Corollary 3.13 which states that the same dichotomy holds

if $\mathbb{A}$ is in a variety whose congruence lattices satisfy any non-trivial lattice identity. Finally we revisit in Theorem 3.18 the dichotomy result for monoids of Tesson [43] and see how Taylor operations can be used to obtain the classification, and confirm the Bulatov–Krokhin–Jeavons conjecture in this case.

2. Preliminaries

2.1. *Basic algebraic results*

We now present the relevant algebraic results that we shall require; for standard universal algebraic results we refer the reader to [9, 17, 29, 40]. We adopt the following notation for identities: we write

$$f(x_1, \ldots, x_n) \approx g(x_1, \ldots, x_n)$$

instead of

$$\forall x_1 \cdots \forall x_n f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n).$$

Let $\mathbb{A} = \langle A; \{f_i : i \in I\}\rangle$ be an algebra. The set I together with the arity t (as defined in the introduction) is the *signature* of $\mathbb{A}$. Two algebras are *similar* if they have the same signature. If σ is a signature, a σ-*term* is defined similarly to polynomials except that constant operation symbols are not allowed: (i) any variable x_i is a σ-term and (ii) if f is an n-ary operation symbol and $g_1, \ldots, g_n$ are σ-terms then $f(g_1, \ldots, g_n)$ is a σ-term. Every σ-term is interpreted as a *term operation* on an algebra of signature σ in the natural way. Two algebras are *polynomially equivalent* if they have the same universe and exactly the same polynomial operations.

Let A be a finite, non-empty set. An operation f on A of arity at least 2 is *idempotent* if it satisfies the identity $f(x, \ldots, x) \approx x$. An n-ary idempotent operation f is a *Taylor operation* if it satisfies, for every $1 \leq i \leq n$, an identity of the form

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

where $x_j, y_j \in \{x, y\}$ for all $1 \leq j \leq n$ (see [41, 17]). For instance, a groupoid (i.e. a binary operation) is a Taylor operation if and only if it is idempotent and commutative; in particular, semilattice operations are Taylor operations. Here are some of the most common instances of Taylor operations:

- a 3-ary operation M is a *majority* operation if it satisfies the identities

$$M(x, x, y) \approx M(x, y, x) \approx M(y, x, x) \approx x.$$

- a 3-ary operation m is a *Mal'tsev* operation if it satisfies

$$m(x, x, y) \approx m(y, x, x) \approx y.$$

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 *invariant* 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 invariant under every f_i, then B is a *subuniverse* 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 *variety* (or equivalently an *equational class*) is a class of similar algebras which is closed under products, subalgebras and homomorphic images. A variety $\mathcal{V}$ is said to be *congruence-modular* (*congruence-permutable*, *congruence-distributive*) if for every algebra $\mathbb{A} \in \mathcal{V}$, the lattice of congruences of $\mathbb{A}$ is *modular* (*permutable*, *distributive* respectively). For instance, the variety of groups and the variety of rings are congruence-permutable, while the variety of lattices is congruence-distributive. Both congruence-distributivity and congruence-permutability imply congruence-modularity. Varieties satisfying these conditions have an alternate description via so-called *Mal'tsev conditions*: for instance, it is known that a variety is congruence-permutable if and only if there exists a term m in the language of $\mathcal{V}$ such that its interpretation in any algebra of $\mathcal{V}$ is a Mal'tsev operation; for groups, one may take the Mal'tsev term $m(x, y, z) = xy^{-1}z$. The characterizations of congruence-modular and congruence-distributive varieties are similar but slightly more involved. We note in passing that the presence of a majority term implies congruence-distributivity of the variety.

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 developped by Hobby and McKenzie in [17], 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 write $\alpha \prec \beta$ and we say that β *covers* α. To each such pair is associated a *type* $i \in \{1, 2, 3, 4, 5\}$, and we sketch briefly how this is done. A finite algebra is said to be *minimal* if its only non-constant polynomial operations are permutations. A theorem of P. P. Pálfy [32] states that, up to polynomial equivalence and isomorphism, the only minimal algebras are of the following five 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.

In tame congruence theory, to each covering pair $\alpha \prec \beta$ of congruences is associated a family of so-called minimal sets which induce minimal algebras, all of the same type 1–5; hence every pair has a unique *type*. The collection of all types of all pairs $\alpha \prec \beta$ is called the *typeset* of $\mathbb{A}$ and is denoted by $typ\{\mathbb{A}\}$. If $\mathcal{V}$ is a variety its typeset is the union of all typesets of its finite members and is denoted by $typ\{\mathcal{V}\}$.

The connection between the typeset of a variety and identities is illustrated in the following result we will require later (see [17, Lemma 9.4 and Theorem 9.6]):

Theorem 2.1. *Let $\mathcal{V}$ be a locally finite variety. Then the following are equivalent*:

(1) $1 \notin typ\{\mathcal{V}\}$;
(2) *there exists a term t in the language of $\mathcal{V}$ that defines a Taylor operation on each algebra in $\mathcal{V}$.*

2.2. *A reduction*

For basic results in algorithmic complexity we refer the reader to [33]. As usual we use **P** and **NP** to denote the class of decision problems solvable in polynomial and non-deterministic polynomial time respectively.

Our first result will be to show that the decision problem $SysPol(\mathbb{A})$ is equivalent to a constraint satisfaction problem of a very special form. For our purposes, we define (*restricted*) *constraint satisfaction problems* as follows (this is in fact equivalent to the definition found in [7]): fix a relational structure $\mathcal{T} = \langle A, T\rangle$ where A is a finite non-empty set, and $T = \{\tau_j : j \in J\}$ where τ_j is a finitary relation on A of arity d_j, $j \in J$ where J is a finite set, the *signature* of $\mathcal{T}$. Let $\mathcal{X} = \langle B, U\rangle$ where $U = \{\mu_j : j \in J\}$ be a structure of signature J; a function $f : B \to A$ is a *homomorphism from $\mathcal{X}$ to $\mathcal{T}$* if $f(\mu_j) \subseteq \tau_j$ for each $j \in J$.

- $CSP(\mathcal{T})$
  Input: A relational structure $\mathcal{X} = \langle X, U\rangle$ of signature J.
  Question: Is there a homomorphism from $\mathcal{X}$ to $\mathcal{T}$?

By extension, if R is a finite set of relations on the set A, $CSP(R)$ will denote the problem $CSP(\mathcal{T})$ where $\mathcal{T}$ is the relational structure $\langle A, R\rangle$ with some fixed indexing.

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

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

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

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

Theorem 2.2. *Let $\mathbb{A} = \langle A; F\rangle$ be a finite algebra of finite signature. The problem $SysPol(\mathbb{A})$ is equivalent via logspace Turing reductions to the problem $CSP(T)$ where T consists of all the relations of the form f°, with f in $F \cup \{id\} \cup C$.*

Proof. (1) Let $\mathcal{S} = \langle X, S\rangle$ be an input to the problem $CSP(\mathcal{T})$. We may assume without loss of generality that $X \subseteq \{x_1, x_2, \ldots\}$. We construct an instance of $SysPol(\mathbb{A})$ as follows: for each tuple of the form

$$(x_{i_1}, \ldots, x_{i_n}, x_{i_{n+1}}) \in f^\circ$$

we create the equation

$$f(x_{i_1}, \ldots, x_{i_n}) = x_{i_{n+1}}.$$

Obviously the system obtained has a solution if and only if there is a homomorphism from $\mathcal{S}$ to $\mathcal{T}$. Also it is clear that this can be accomplished in constant space.

(2) Let $\{(p_i, q_i)\}$ be a finite sequence of pairs of polynomials of $\mathbb{A}$. We want to construct an instance $\mathcal{S} = \langle X, S\rangle$ of $CSP(\mathcal{T})$ such that there is a solution to the system $\{p_1 = q_1, p_2 = q_2, \ldots\}$ if and only if there is a homomorphism from $\mathcal{S}$ to $\mathcal{T}$. We proceed as follows: we treat each equation $p_i = q_i$ separately. For convenience let $p = p_i$ and $q = q_i$. Create new variables $y_1^p, y_2^p, \ldots$ and $y_1^q, y_2^q, \ldots$ where there are as many new variables as the number of symbols in the polynomials p and q respectively. First output the constraint $(y_1^p, y_1^q) \in id^\circ$. Now we rewrite the polynomial p (and similarly for q) as a sequence of constraints of the form

$$(y_{i_1}, \ldots, y_{i_k}, y_{i_{k+1}}) \in f^\circ$$

where f is a k-ary operation symbol in $F \cup \{id\} \cup C$. For instance, if p is the polynomial

$$f(g(x_1, x_2), c, x_1, h(x_4))$$

then we will output (assuming that the input contains the parentheses and commas, we have created the variables $y_1, \ldots, y_{22}$ where we drop the superscript p for convenience) the following constraints:

$$\begin{aligned}
(y_3, y_{12}, y_{14}, y_{17}, y_1) &\in f^\circ \\
(y_5, y_8, y_3) &\in g^\circ \\
y_{12} &\in c^\circ \\
(x_1, y_{14}) &\in id^\circ \\
(y_{19}, y_{17}) &\in h^\circ \\
(x_1, y_5) &\in id^\circ \\
(x_2, y_8) &\in id^\circ \\
(x_4, y_{19}) &\in id^\circ.
\end{aligned}$$

We use counters to keep track of (i) the operation symbol being treated, (ii) the depth of the nesting as we search for the positions of the arguments y_j to be output in the current constraint and (iii) the position of the cursor as it reads the input term. □

2.3. *A hardness criterion*

Recall that a finite relational structure $\mathcal{T}$ is a *core* if every homomorphism from $\mathcal{T}$ to itself is an automorphism (i.e. is injective). We shall require the following in

proving hardness results:

Theorem 2.3 [7, 25]. *Let $\mathcal{T}$ be a finite relational structure which is a core. If there is no Taylor operation that preserves all relations in $\mathcal{T}$ then the problem $CSP(\mathcal{T})$ is* **NP***-complete.*

Let $\mathbb{A}$ be a finite algebra of finite signature. By Theorem 2.2 the problem $SysPol(\mathbb{A})$ is polynomial-time equivalent to $CSP(T)$ where T consists of all relations of the form f° where f is either a fundamental operation of the algebra $\mathbb{A}$ or a constant operation. The only homomorphism from the relational structure $\langle A; T\rangle$ to itself is the identity since it must preserve every one-element subset. Hence the structure is a core. Hence by Theorem 2.3 the problem $SysPol(\mathbb{A})$ is **NP**-complete if there is no Taylor operation that preserves all the relations in T. Conversely, the Bulatov–Krokhin–Jeavons conjecture states that the problem $SysPol(\mathbb{A})$ should be solvable in polynomial time if there exists such a Taylor operation. This allows us to translate the $SysPol(\mathbb{A})$ problem into an interesting universal algebraic setting. Indeed, 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 fundamental operations. We will say that an operation t is *compatible* with the algebra $\mathbb{A}$ if t commutes with every fundamental operation of $\mathbb{A}$. Consequently, we reformulate our criterion:

Theorem 2.4. *Let $\mathbb{A}$ be a finite algebra of finite signature. If $\mathbb{A}$ has no compatible Taylor operation then the problem $SysPol(\mathbb{A})$ is* **NP***-complete.*

3. Results

3.1. *Semilattices and lattices*

It is well-known that if the relations in R are preserved by a semilattice operation then $CSP(R)$ is in **P** [19]. One can verify immediately that a semilattice operation commutes with itself and so the following result is immediate:

Proposition 3.1. *If $\mathbb{A}$ is a semilattice then the problem $SysPol(\mathbb{A})$ is in* **P***.*

On the other hand, the next result, which will also be of use later, shows that the situation is rather different for lattices.

Lemma 3.2. *Let M be a majority operation on a finite set A, $|A| > 1$. Then no Taylor operation commutes with M.*

Proof. Suppose for a contradiction that there is an n-ary Taylor operation t that commutes with M. Consider the relation

$$\theta = \{(x_1, \ldots, x_n, y_1, \ldots, y_n) : t(x_1, \ldots, x_n) = t(y_1, \ldots, y_n)\}.$$

It is easy to see that M must preserve θ. For every $1 \leq i < j \leq 2n$ let

$$\theta_{i,j} = \{(u_i, u_j) : \text{ there exist entries } u_l \text{ such that } (u_1, \ldots, u_{2n}) \in \theta\}.$$

Claim 3.3. *$\theta_{i,j} = A^2$ for all $1 \leq i < j \leq 2n$.*

Proof of Claim. The only case which is not quite immediate is when $1 \leq i \leq n$ and $j = n+i$. Choose $(u, v) \in A^2$. By the definition of Taylor operation, there exist tuples $\overline{w}, \overline{z}$ with entries in $\{u, v\}$ such that $t(\overline{w}) = t(\overline{z})$ where the u appears in the ith place in the left-hand term and v appears in the ith place on the right; hence $(u, v) \in \theta_{i,j}$.

It is known that a relation preserved by a majority operation is entirely determined by its projections on two coordinates [1], i.e. $(u_1, \ldots, u_{2n}) \in \theta$ whenever $(u_i, u_j) \in \theta_{i,j}$ for all $1 \leq i < j \leq 2n$. Hence by the claim we have that $\theta = A^{2n}$, which means that t is constant, a contradiction. □

Corollary 3.4. *If $\mathbb{A}$ is a non-trivial lattice then the problem $SysPol(\mathbb{A})$ is* **NP***-complete.*

Proof. For a lattice $\mathbb{A} = \langle A; \vee, \wedge \rangle$ the polynomial operation defined by

$$M(x, y, z) = (x \vee y) \wedge [(x \vee z) \wedge (y \vee z)]$$

is easily seen to be a majority operation. It follows from the last lemma that no Taylor operation can commute with the basic operations of $\mathbb{A}$ and hence by Theorem 2.4 we are done. □

3.2. *Algebras with type 3 or 4*

We shall now generalize Lemma 3.2 and Corollary 3.4. Let $\mathbb{A}$ be a finite algebra with universe A, let $N \subseteq A$ and let f be a k-ary operation on A that satisfies $f(N^k) \subseteq N$. Then as usual $f|_N$ will denote the operation induced on N by f simply by restriction of its domain to N^k. The next result was proved independently by Seif [36]:

Theorem 3.5. *Let $\mathbb{A}$ be a finite algebra such that $typ\{\mathbb{A}\} \cap \{3, 4\} \neq \emptyset$. Then $\mathbb{A}$ has no compatible Taylor operation.*

Proof. If $typ\{\mathbb{A}\} \cap \{3, 4\} \neq \emptyset$ then by [17, Theorem 4.17] there exist a subset U of A and a unary polynomial e of $\mathbb{A}$ such that the following hold: $e(A) = U$ and $e^2 = e$; and there exist binary polynomials p and q of $\mathbb{A}$ and a 2-element subset $\{0, 1\} \subseteq U$ such that the operations $ep|_U$ and $eq|_U$ preserve $\{0, 1\}$ and the algebra $\langle \{0, 1\}; ep|_{\{0,1\}}, eq|_{\{0,1\}} \rangle$ is a lattice.

Let t be an n-ary Taylor operation commuting with the basic operations of $\mathbb{A}$. It is easy to verify that $et|_U$ is a Taylor operation that commutes with $ep|_U$ and $eq|_U$. Consider the ternary polynomial operation M obtained from ep and eq as in Corollary 3.4: clearly it preserves the set $\{0, 1\}$ and $M|_{\{0,1\}}$ is a majority operation.

Let ρ be the $2n$-ary relation on $\{0,1\}$ defined by

$$\rho = \{(x_1,\dots,x_n,y_1,\dots,y_n) \in \{0,1\}^{2n} : et(x_1,\dots,x_n) = et(y_1,\dots,y_n)\}.$$

Since M commutes with $et|_U$ it preserves ρ; by an argument similar to the one in Lemma 3.2 we see that $\rho = \{0,1\}^{2n}$; in particular,

$$0 = et(0,0,\dots,0) = et(1,1,\dots,1) = 1,$$

a contradiction. □

Corollary 3.6. *Let $\mathbb{A}$ be a non-trivial finite algebra that generates a congruence-distributive variety. Then $SysPol(\mathbb{A})$ is* **NP***-complete.*

Proof. If a variety $\mathcal{V}$ is congruence-distributive then by [17, Theorem 8.6] we have that $typ\{\mathbb{A}\} \cap \{1,2,5\} = \emptyset$ for every algebra $\mathbb{A} \in \mathcal{V}$ so by the last result we are done. □

It is well-known that lattices are congruence-distributive, and in fact that any algebra that has a majority term generates a congruence-distributive variety [29] so Lemma 3.2 and Corollary 3.4 follow from Corollary 3.6.

3.3. *Algebras in varieties omitting type 1*

The main result of this section is a characterization of algebras omitting type 5 with a compatible Taylor operation in varieties whose typeset does not contain 1 (Theorem 3.12). In particular we characterize algebras with a compatible Taylor operation in varieties omitting types 1 and 5: among these are the congruence-permutable and congruence-modular varieties, and so we will obtain a dichotomy for the problem $SysPol(\mathbb{A})$ for a class of finite algebras that contains groups, rings, quasigroups and modules over a unitary ring.

Definition 3.7. An algebra $\mathbb{A}$ is said to satisfy the *term condition* (or is a *TC-algebra*)[a] if the following holds: for every $n+1$-ary term f of $\mathbb{A}$ and every $u,v,x_1,\dots,x_n,y_1,\dots,y_n \in A$, we have that

$$f(u,x_1,\dots,x_n) = f(u,y_1,\dots,y_n) \Leftrightarrow f(v,x_1,\dots,x_n) = f(v,y_1,\dots,y_n).$$

For instance, a group is a TC-algebra if and only if it is Abelian and a ring is a TC-algebra if and only if it is a zero ring, i.e. it satisfies the identity $xy \approx 0$. Any module over a ring is a TC-algebra (see [29, p. 251] or [17, p. 40]). Semigroups of finite exponent that satisfy the term condition have been characterized by McKenzie [28], and the general case is settled in [44].

Lemma 3.8. *Let $\mathbb{B}$ be a finite algebra. If $\mathbb{B}$ has a compatible Mal'tsev operation then it is a TC-algebra.*

[a]The terminology *Abelian algebra* is also used.

Proof. Let m denote the Mal'tsev operation that commutes with the basic operations of $\mathbb{B}$ and let t be any term of $\mathbb{B}$. Let $u, v, x_2, \ldots, x_n, y_1, \ldots, y_n$ be such that

$$t(u, x_2, \ldots, x_n) = t(u, y_2, \ldots, y_n).$$

Consider the following $3 \times 2(n+1)$ matrix:

$$\begin{pmatrix} u & x_2 & \cdots & x_n & u & y_2 & \cdots & y_n \\ u & u & \cdots & u & u & u & \cdots & u \\ v & u & \cdots & u & v & u & \cdots & u \end{pmatrix}.$$

By hypothesis, if we apply the term t to the first $n+1$ entries of any row we get the same result as applying it to the last $n+1$ entries:

$$\begin{aligned} t(u, x_2, \ldots, x_n) &= t(u, y_2, \ldots, y_n) \\ t(u, u, \ldots, u) &= t(u, u, \ldots, u) \\ t(v, u, \ldots, u) &= t(v, u, \ldots, u). \end{aligned}$$

Since m and t commute, applying the operation m to the columns of the matrix of the entries will yield

$$\begin{aligned} t(v, x_2, \ldots, x_n) &= t(m(u,u,v), m(x_2,u,u), \ldots, m(x_n,u,u)) \\ &= m(t(u, x_2, \ldots, x_n), t(u,u,\ldots,u), t(v,u,\ldots,u)) \\ &= m(t(u, y_2, \ldots, y_n), t(u,u,\ldots,u), t(v,u,\ldots,u)) \\ &= t(m(u,u,v), m(y_2,u,u), \ldots, m(y_n,u,u)) \\ &= t(v, y_2, \ldots, y_n). \end{aligned}$$

□

An algebra $\mathbb{A} = \langle A, F \rangle$ is said to be *affine* if there exists an Abelian group $\langle A; +, -, 0 \rangle$ such that

(1) the operation $m(x, y, z) = x - y + z$ is a term of $\mathbb{A}$;
(2) every polynomial operation of $\mathbb{A}$ is *affine*, i.e. of the form

$$\sum_{i=1}^{n} r_i x_i + a$$

where the r_i are endomorphisms of $\langle A; +, -, 0 \rangle$.

Theorem 3.9 (see [40]). *Let $\mathbb{B}$ be an algebra with a Mal'tsev term. Then the following are equivalent*:

(1) *$\mathbb{B}$ is affine*;
(2) *$\mathbb{B}$ is a TC-algebra*;
(3) *$\mathbb{B}$ is polynomially equivalent to a module.*

We shall require the following technical lemma which is an amalgam of several results of [17].

Lemma 3.10. *Let $\mathbb{A}$ be a finite algebra such that $1 \notin typ\{\mathcal{V}(\mathbb{A})\}$. If $typ\{\mathbb{A}\} = \{2\}$, in particular if $\mathbb{A}$ is a TC-algebra, then $\mathbb{A}$ admits a Mal'tsev term.*

Proof. It follows from [17, Proposition 3.7 and Theorem 7.2] that if $\mathbb{A}$ is a *TC*-algebra in a variety omitting type 1 then $typ\{\mathbb{A}\} = \{2\}$. In particular, $\mathbb{A}$ is a so-called locally solvable algebra, and then by [17, Corollary 7.6 and Theorem 7.11] the variety $\mathcal{V}(\mathbb{A})$ is congruence-permutable, and thus $\mathbb{A}$ has a Mal'tsev term. □

Lemma 3.11. *Let $\mathbb{A}$ be a finite algebra with a Mal'tsev term. If $\mathbb{A}$ has a compatible Taylor operation then $\mathbb{A}$ is polynomially equivalent to a module.*

Proof. Let m denote the Mal'tsev term of $\mathbb{A}$ and let t denote the Taylor term that is compatible with $\mathbb{A}$. The variety $\mathcal{V}(\mathbb{B})$ generated by the algebra $\mathbb{B} = \langle A; t\rangle$ is locally finite and so $1 \notin typ\{\mathcal{V}(\mathbb{B})\}$ by Theorem 2.1. By Lemma 3.8 the algebra $\mathbb{B}$ is a TC-algebra; and hence by the last lemma $\mathbb{B}$ has a Mal'tsev term. Thus by Theorem 3.3 the algebra $\mathbb{B}$ is affine. It follows that there exists an Abelian group $\langle A; +, -, 0\rangle$ such that the operation $\mu(x, y, z) = x - y + z$ is a term of $\mathbb{B}$, and thus every basic operation of $\mathbb{A}$ commutes with μ. By [40, Proposition 2.1] it follows that every basic operation of $\mathbb{A}$ is affine. Finally, it is easy to verify that if m is an affine operation then $m = \mu$, so $\mathbb{A}$ is affine, and hence polynomially equivalent to a module. □

We are now in a position to prove the main result of this section:

Theorem 3.12. *Let $\mathbb{A}$ be a finite algebra such that $1 \notin typ\{\mathcal{V}(\mathbb{A})\}$.*
If $5 \notin typ\{\mathbb{A}\}$ then the following statements are equivalent:

(1) *$\mathbb{A}$ has a compatible Taylor operation*;
(2) *$\mathbb{A}$ is polynomially equivalent to a module.*

Proof. (2) ⇒ (1): This follows immediately from the fact that the term $\mu(x, y, z) = x - y + z$ is a Taylor operation and that it commutes with every affine operation.

(1) ⇒ (2): Follows immediately from Theorem 3.5 and Lemmas 3.10 and 3.11. □

Corollary 3.13. *Let $\mathbb{A}$ be a finite algebra such that $1 \notin typ\{\mathcal{V}(\mathbb{A})\}$. If $5 \notin typ\{\mathbb{A}\}$ then the problem $SysPol(\mathbb{A})$ is in* **P** *if $\mathbb{A}$ is polynomially equivalent to a module, and it is* **NP***-complete otherwise.*

Proof. The hardness part follows from Theorems 3.12 and 2.4. If $\mathbb{A}$ is polynomially equivalent to a module then there is an Abelian group $\mathbb{G} = \langle A; +, -, 0\rangle$ such that the Mal'tsev operation $\mu(x, y, z) = x - y + z$ commutes with the basic operations

of $\mathbb{A}$, which implies that the basic relations of the corresponding CSP problem are invariant under this operation. It is easy to see that if a k-ary relation is invariant under μ then it is a coset of the group $\mathbb{G}^k$. Consequently the CSP problem is a so-called general subgroup problem, which is solvable in polynomial time by a result of Feder and Vardi ([13], Theorem 33).[b] □

By a result of Kearnes [20], a locally finite variety $\mathcal{V}$ omits types 1 and 5 precisely when at least one non-trivial lattice identity holds in every congruence lattice of algebras in $\mathcal{V}$. In particular:

Corollary 3.14. *Let $\mathbb{A}$ be a finite algebra in a congruence-modular variety. Then the problem $SysPol(\mathbb{A})$ is in* **P** *if $\mathbb{A}$ is polynomially equivalent to a module, and it is* **NP***-complete otherwise.*

Proof. If $\mathcal{V}$ is a locally finite congruence-modular variety, then by [17, Theorem 9.5], $typ\{\mathcal{V}\} \cap \{1, 5\} = \emptyset$ so Corollary 3.13 applies. □

We immediately get the following special cases:

Corollary 3.15 [15]. *Let $\mathbb{A}$ be a finite group. The problem $SysPol(\mathbb{A})$ is in* **P** *if $\mathbb{A}$ is Abelian, and it is* **NP***-complete otherwise.*

Corollary 3.16. *Let $\mathbb{A}$ be a finite ring. The problem $SysPol(\mathbb{A})$ is in* **P** *if $\mathbb{A}$ is a zero ring, and it is* **NP***-complete otherwise.*

A finite *quasigroup* is an algebra $\mathbb{A} = \langle A; \star \rangle$ such that the equations $a \star x = b$ and $x \star a = b$ have a unique solution, for any $a, b \in A$.

Corollary 3.17. *Let $\mathbb{A}$ be a finite quasigroup. The problem $SysPol(\mathbb{A})$ is in* **P** *if there exists an Abelian group $\mathbb{G} = \langle A, + \rangle$ such that $x \star y = a(x) + b(y) + c$ for some automorphisms a, b of $\mathbb{G}$ and $c \in A$, and it is* **NP***-complete otherwise.*

Proof. Since every finite quasigroup admits a Mal'tsev term (see [40]), $\mathbb{A}$ generates a congruence-permutable, and *a fortiori* congruence-modular variety. Suppose that $\mathbb{A}$ is polynomially equivalent to a module, so that the quasigroup operation is affine, i.e. $x \star y = a(x) + b(y) + c$ for some Abelian group $\mathbb{G} = \langle A, + \rangle$ and endomorphisms a and b of $\mathbb{G}$. It is clear that the defining conditions of the quasigroup imply that a and b are one-to-one. Conversely, if $x \star y$ can be expressed in this way then every term operation of $\mathbb{A}$ is affine. In particular, as we remarked at the end of the proof of Lemma 3.11, the Mal'tsev term of $\mathbb{A}$ can be no other than $\mu(x, y, z) = x - y + z$. It follows from Theorem 3.9 that $\mathbb{A}$ is polynomially equivalent to a module. Now the result follows from Corollary 3.14. □

[b] A. Bulatov has generalized Feder and Vardi's result by showing that every CSP whose basic relations are invariant under a Mal'tsev operation is in **P** [4].

We should also point out that Corollary 3.6 follows from Corollary 3.14: indeed, there are no non-trivial algebras polynomially equivalent to a module in a congruence-distributive variety.

3.4. *Equations over monoids*

In the preceding section we noted that, by a result of Klima, Tesson and Thérien, a dichotomy for the class of all restricted CSPs can be obtained by proving dichotomy for *SysPol* problems over a very special class of semigroups, namely over the class of left normal bands [21]. In [21] Klima *et al.* also provide an example of semigroups $\mathbb{A}$ and $\mathbb{B}$ such that $\mathbb{B}$ is a homomorphic image of $\mathbb{A}$, $SysPol(\mathbb{A})$ is in **P** and $SysPol(\mathbb{B})$ is **NP**-complete. If we restrict *SysPol* to the class of finite monoids however, the situation is quite different. In [43] P. Tesson managed to prove dichotomy for *SysPol* over finite monoids. A *pseudovariety* is a class of finite similar algebras closed under subalgebras, homomorphic images and finite products.

Theorem 3.18 ([43] see also [30]). *Let $\mathbb{M}$ be a finite monoid. If $\mathbb{M}$ is in the pseudovariety generated by the finite Abelian groups and finite semilattices then $SysPol(\mathbb{M})$ is in* **P** *and $SysPol(\mathbb{M})$ is* **NP***-complete otherwise.*

In this section we describe the class of finite monoids with a compatible Taylor operation. We show that this class coincides with the class of all monoids in the pseudovariety generated by finite Abelian groups and finite semilattices. Hence our theorem will immediately yield the hardness part of Theorem 3.18 and moreover, together with Theorem 3.18 it will confirm the Bulatov–Krokhin–Jeavons conjecture for another class of decision problems.

As usual, a subset I of a semigroup $\mathbb{S}$ is called an *ideal* if $sI \subseteq I \supseteq Is$ for all $s \in \mathbb{S}$. By a *group with zero* we mean a semigroup obtained by the adjunction of an absorbing element 0 to a group. A semigroup with a zero element 0 is a *nilsemigroup* if for every $s \in \mathbb{S}$ there is an n such that $s^n = 0$. If a semigroup $\mathbb{S}$ has a unit element then we define $\mathbb{S}^1 = \mathbb{S}$, otherwise $\mathbb{S}^1$ is the monoid obtained from $\mathbb{S}$ by the adjunction of a unit element. Let $\mathbb{M}$ and $\mathbb{A}_1, \ldots, \mathbb{A}_n$ be semigroups. We say that $\mathbb{M}$ is a *subdirect product* of the $\mathbb{A}_i$ if there is an embedding $e : \mathbb{M} \hookrightarrow \prod \mathbb{A}_i$ such that the restriction of each projection to $e(\mathbb{M})$ is onto.

Theorem 3.19. *For a finite monoid $\mathbb{M}$ the following are equivalent*:

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

Proof. (1) $\Rightarrow$ (2) : Let us suppose that (1) holds and let t be an n-ary compatible Taylor operation on $\mathbb{M}$. So t is idempotent and satisfies n identities in two different

variables x and y as follows:

$$\begin{aligned} t(x,\ldots,\ldots,\ldots) &= t(y,\ldots,\ldots,\ldots) \\ t(\ldots,x,\ldots,\ldots) &= t(\ldots,y,\ldots,\ldots) \\ &\ldots \\ t(\ldots,\ldots,\ldots,x) &= t(\ldots,\ldots,\ldots,y). \end{aligned}$$

First we show that $\mathbb{M}$ is commutative.[c] Let a and b be any elements from $\mathbb{M}$. Since t is compatible with the product in the monoid we get

$$\begin{aligned} ab &= t(a,a,\ldots,a)\,t(b,b,\ldots,b) \\ &= [t(1,\ldots,1,a)\cdots t(1,a,1,\ldots,1)\,t(a,1,\ldots,1)]\;t(b,b,\ldots,b); \end{aligned}$$

we make the last two terms commute by rewriting $t(b,\ldots,b)$ using the first Taylor identity. If we have that

$$t(b,z_2,\ldots,z_n) = t(1,w_2,\ldots,w_n)$$

where $z_i, w_i \in \{b,1\}$ let

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

Now we get that

$$\begin{aligned} t(b,\ldots,b) &= t(b,z_2,\ldots,z_n)\,t(1,\overline{z}_2,\ldots,\overline{z}_n) \\ &= t(1,w_2,\ldots,w_n)\,t(1,\overline{z}_2,\ldots,\overline{z}_n) \end{aligned}$$

so

$$\begin{aligned} ab &= t(1,\ldots,1,a)\cdots t(1,a,1,\ldots,1)\,t(a,1,\ldots,1)\,t(1,w_2,\ldots,w_n)\,t(1,\overline{z}_2,\ldots,\overline{z}_n) \\ &= t(1,\ldots,1,a)\cdots t(1,a,1,\ldots,1)\,t(1,w_2,\ldots,w_n)\,t(a,1,\ldots,1)\,t(1,\overline{z}_2,\ldots,\overline{z}_n) \\ &= t(1,\ldots,1,a)\cdots t(1,a,1,\ldots,1)\,t(1,w_2,\ldots,w_n)\,t(1,\overline{z}_2,\ldots,\overline{z}_n)\,t(a,1,\ldots,1) \\ &= t(1,\ldots,1,a)\cdots t(1,a,1,\ldots,1)\,t(b,b,\ldots,b)\,t(a,1,\ldots,1) \end{aligned}$$

since 1 commutes with a and b. Repeating this argument using successively the other Taylor identities we can commute $t(b,\ldots,b)$ to the front and thus

$$\begin{aligned} ab &= t(b,\ldots,b)\,t(1,\ldots,1,a)\cdots t(1,a,1,\ldots,1)\,t(a,1,\ldots,1) \\ &= ba. \end{aligned}$$

We now invoke a subdirect decomposition theorem of Ponizovsky on finite commutative semigroups [16]. Let $\mathbb{S}$ be a finite commutative semigroup. There is a quasiorder on $\mathbb{S}$ defined by $a \leq b$ iff there exists a $c \in \mathbb{S}^1$, such that $a = bc$. Note that the idempotents in $\mathbb{S}$ form a semilattice $\mathbb{E}$ and $\leq$ restricted to $\mathbb{E}$ is the usual semilattice order on $\mathbb{E}$.

[c]This argument is due to W. Taylor, see [42].

For each idempotent $e \in \mathbb{S}^1$ we define a homomorphic image of $\mathbb{S}$, called the *Ponizovsky factor* related to e:

$$\mathbb{P}_e = e\mathbb{S}/\big(\cup_{f\in\mathbb{E},f<e} f\mathbb{S}\big)$$

and $\mathbb{P}_e = e\mathbb{S}$ if e is the smallest idempotent in $\mathbb{S}$.

Ponizovsky's theorem states that every finite commutative semigroup is a subdirect product of its Ponizovsky factors. Moreover, every Ponizovsky factor is a group, or a nilsemigroup, or a disjoint union of a group and a nilsemigroup that is an ideal. We call the latter type of Ponizovsky factors a factor of *mixed type*. As $\mathbb{M}$ is a monoid, so are its Ponizovsky factors. Hence the Ponizovsky factors of $\mathbb{M}$ are groups or factors of mixed type.

Let $e \in \mathbb{M}$ be an idempotent, and let $\mathbb{P}_e = e\mathbb{M}/I$ be a Ponizovsky factor of mixed type where $I = \cup_{f\in\mathbb{E},f<e} f\mathbb{M}$. We show that $\mathbb{P}_e$ is a group with 0. Let $\mathbb{P}_e = \mathbb{G} \cup \mathbb{N}'$ where $\mathbb{G}$ is a group and $\mathbb{N}'$ is a nilsemigroup that is an ideal in $\mathbb{P}_e$. Let $\mathbb{N}$ be the inverse image of $\mathbb{N}'$ under the homomorphism related to I. Thus, $I \subseteq \mathbb{N} \subseteq e\mathbb{M}$, and there is an m such that $\mathbb{N}^m \subseteq I$. Moreover, et is a compatible Taylor operation on $e\mathbb{M}$. Without loss of generality we assume $e = 1$.

Notice that if a is maximal in $\mathbb{N}\backslash I$ and $a = bc$ for some $b, c \in \mathbb{M}$, then b or c belongs to $\mathbb{G}$. By way of contradiction let us suppose that both b and c are in $\mathbb{N}$. Since $a \leq b$ and a is *maximal* we have $b \leq a$. So there exists $d \in \mathbb{M}$ such that $b = ad$. Thus $a = adc$ and thus $a = ad^m c^m$. Now $c \in \mathbb{N}$ implies $c^m \in I$ and so $a \in I$, a contradiction.

We prove that $\mathbb{N} = I$. Let us suppose that $\mathbb{N}\backslash I$ is non-empty and a is a maximal element of $\mathbb{N}\backslash I$. Fix a coordinate $1 \leq i \leq n$ and consider the ith Taylor identity for $x = 1$ and $y = a$, i.e.

$$t(z_1, \dots, z_{i-1}, 1, z_{i+1}, \dots, z_n) = t(w_1, \dots, w_{i-1}, a, w_{i+1}, \dots, w_n)$$

for some $z_i, w_i \in \{1, a\}$. Proceeding as we did for the commutativity of $\mathbb{M}$ and using the same notation $\overline{z}_i$ we obtain

$$\begin{aligned} a &= t(a, \dots, a) \\ &= t(z_1, \dots, z_{i-1}, 1, z_{i+1}, \dots, z_n)\, t(\overline{z}_1, \dots, \overline{z}_{i-1}, a, \overline{z}_{i+1}, \dots, \overline{z}_n) \\ &= t(w_1, \dots, w_{i-1}, a, w_{i+1}, \dots, w_n)\, t(\overline{z}_1, \dots, \overline{z}_{i-1}, a, \overline{z}_{i+1}, \dots, \overline{z}_n). \end{aligned}$$

Since a is maximal, one of the factors on the right is in $\mathbb{G}$. For each identity $(1 \leq i \leq n)$ pick a factor on the right side which is in $\mathbb{G}$ and denote their product by p. Thus $p \in \mathbb{G}$. On the other hand, the compatibility of t gives

$$\begin{aligned} p &= t(a, \dots, \dots, \dots)\, t(\dots, a, \dots, \dots, \dots) \cdots t(\dots, \dots, \dots, a) \\ &= t(au_1, au_2, \dots, au_n) \\ &= t(a, \dots, a)\, t(u_1, \dots, u_n) \\ &= a\, t(u_1, \dots, u_n). \end{aligned}$$

for some $u_i \in \mathbb{M}$. Since $a \in \mathbb{N}$, and $\mathbb{N}$ is an ideal of $\mathbb{M}$, $p \in \mathbb{N}$, a contradiction. Thus, if $\mathbb{P}_e$ is not a group then $e\mathbb{M} = \mathbb{G} \cup I$ and $\mathbb{P}_e = e\mathbb{M}/I$ is a group with zero. So all Ponizovsky factors of $\mathbb{M}$ are groups or groups with zero and by applying Ponizovsky's theorem we get (2).

(2) $\Rightarrow$ (3): Let $\mathbb{G}$ be an Abelian group and let $\mathbb{G}^0$ be $\mathbb{G}$ extended with zero. Now, $\mathbb{G}^0$ is the homomorphic image of the product of $\mathbb{G}$ and the 2-element semilattice under the natural homomorphism related to the ideal $\mathbb{G} \times \{0\}$. Hence (2) implies (3).

(3) $\Rightarrow$ (1): If (3) holds then $\mathbb{M}$ is commutative and belongs to the variety generated by a finite group of some finite exponent m and the 2-element semilattice. Observe that both of these generators satisfy the identity $x^{m+1} = x$ so $\mathbb{M}$ satisfies the same identity. Consider the term $t(x_0, \ldots, x_m) = x_0 \cdots x_m$. The idempotency of t is ensured by the identity $x^{m+1} = x$. Since $\mathbb{M}$ is commutative, the term is a compatible operation of $\mathbb{M}$; and furthermore it is a Taylor operation since it satisfies

$$t(x, y, \ldots, y) \approx t(y, x, y, \ldots, y) \approx \cdots \approx t(y, \ldots, y, x). \qquad \square$$

Acknowledgments

We are grateful to Andrei Krokhin and Pascal Tesson for useful discussions and comments. We thank Michal Koucký for his nice reduction in Theorem 2.2 (2) and Matt Valeriote for the simplifying argument of Lemma 3.10.

The first author's research is supported by a grant from NSERC. The second author's research is supported by OTKA grants T034175 and T037877.

References

[1] K. A. Baker and A. F. Pixley, Polynomial interpolation and the Chinese remainder theorem for algebraic systems, *Math. Z.* **143**(2) (1975) 165–174.

[2] A. Bulatov, A dichotomy theorem for constraints on a three-element set, in *Proc. 43rd IEEE Symposium on Foundations of Computer Science (FOCS'02)*, Vancouver, Canada (2002), pp. 649–658.

[3] A. Bulatov, Tractable conservative constraint satisfaction problems, in *Proc. 18th IEEE Symposium on Logic in Computer Science (LICS'03)*, Ottawa, Canada (2003), pp. 321–330.

[4] A. Bulatov, Malt'sev constraints are tractable, Research Report RR-02-05, Oxford University Computing Laboratory (April 2002).

[5] A. Bulatov and V. Dalmau, Towards a dichotomy theorem for the counting constraint satisfaction problem, *Foundations of Computer Science*, Boston, MA (2003), 562–571; *IEEE Comput. Soc.* (2003).

[6] A. Bulatov and M. Grohe, The complexity of partition functions, in *Proceedings of the 31st International Colloquium on Automata, Languages and Programming (ICALP'04)*, Lecture Notes in Computer Science, Vol. 3142 (2004), pp. 294–306.

[7] A. Bulatov, P. Jeavons and A. Krokhin, Constraint satisfaction problems and finite algebras, in *Proc. 27th Int. Colloquim on Automata, Languages and Programming (ICALP'00)*, Geneva, Switzerland, *Lecture Notes in Comput. Sci.* **1853** (2000) 272–282.

[8] A. Bulatov, P. Jeavons and A. Krokhin, Classifying the complexity of constraints using finite algebras, *SIAM J. Comput.* **34**(3) (2005) 720–742.

[9] M. Clasen and M. Valeriote, Finite algebra, in *Lectures on Algebraic Model Theory*, eds. B. Hart and M. Valeriote, Fields Institute Monographs, Vol. 15 (Dec. 2001).
[10] N. Creignou, S. Khanna and M. Sudan, *Complexity Classifications of Boolean Constraint Satisfaction Problems*, SIAM Monographs on Discrete Mathematics and Applications, Vol. 7 (SIAM, Philadelphia, 2001).
[11] V. Dalmau, Ph. G. Kolaitis and M. Y. Vardi, Constraint satisfaction, bounded treewidth, and finite-variable logics. Principles and Practice of Constraint Programming (Ithaca, NY, 2002), *Lecture Notes in Comput. Sci.* **2470** (2002) 310–326.
[12] T. Feder, F. Madelaine and I. A. Stewart, Dichotomies for classes of homomorphism problems involving unary functions, *Theoret. Comput. Sci.* **314** (2004) 1–43.
[13] T. Feder and M. Vardi, The computational structure of monotone monadic SNP and constraint satisfaction: A study through Datalog and group theory, in *Proc. 25th Ann. ACM Symp. on Theory of Computing* (1993), pp. 612–622.
[14] 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.
[15] M. Goldmann and A. Russell, The complexity of solving equations over finite groups, *Inform. and Comput.* **178**(1) (2002) 253–262.
[16] P. A. Grillet, *Semigroups, An Introduction to the Structure Theory*, Monographs and Textbooks in Pure and Applied Mathematics, **193** (Marcel Dekker, New York, 1995).
[17] D. Hobby and R. McKenzie, The structure of finite algebras, *Contemp. Math.* **76** (1988).
[18] P. G. Jeavons, On the algebraic structure of combinatorial problems, *Theoret. Comput. Sci.* **200** (1998) 185–204.
[19] P. G. Jeavons, D. A. Cohen and M. Cooper, Constraints consistency and closure, *Artificial Intelligence* **101**(1–2) (1998) 251–265.
[20] K. Kearnes, Congruence join semidistributivity is equivalent to a congruence identity, *Algebra Universalis* **46**(3) (2001) 373–387.
[21] O. Klíma, P. Tesson and D. Thérien, Dichotomies in the complexity of solving systems of equations over finite semigroups, preprint (2004).
[22] Ph. G. Kolaitis and M. Y. Vardi, Conjunctive-query containment and constraint satisfaction, *J. Comput. System Sci.* **61** (2000) 302–332.
[23] A. Krokhin A. Bulatov and P. Jeavons, The complexity of constraint satisfaction: An algebraic approach, preprint.
[24] O. Klíma, B. Larose and P. Tesson, Systems of Equations over Finite Semigroups and the #CSP Dichotomy Conjecture, 12 pages, accepted, MFCS 2006.
[25] B. Larose and L. Zádori, The complexity of the extendibility problem for finite posets, *SIAM J. Discrete Math.* **17**(1) (2003) 114–121.
[26] T. Łuczak and J. Nešetřil, A probabilistic approach to the dichotomy problem, Technical Report 2003–640, Kam–Dimatia Series (2003).
[27] A. K. Mackworth. Constraint satisfaction, in *Encyclopedia of Artificial Intelligence*, Vol. 1, ed. S. C. Shapiro (Wiley Interscience, 1992), pp. 285–293.
[28] R. McKenzie, The number of non-isomorphic models in quasi-varieties of semigroups, *Algebra Universalis* **16** (1983) 195–203.
[29] R. N. McKenzie, G. F. McNulty and W. F. Taylor, *Algebras, Lattices and Varieties* (Wadsworth and Brooks/Cole, Monterey, California, 1987).
[30] C. Moore, P. Tesson and D. Thérien, Satisfiability of systems of equations over finite monoids, in *Proc. MFCS* 2001, LNCS 2136 (Springer), 537–547.
[31] P. Jonsson and G. Nordh, The complexity of counting the number of solutions to systems of equations over finite algebraic structures, preprint (2003).

[32] P. P. Pálfy, Unary polynomials in algebras I, *Algebra Universalis* **18** (1984) 262–273.
[33] C. H. Papadimitriou, *Computational Complexity* (Addison-Wesley, 1994).
[34] T. J. Schaefer, The complexity of the satisfiability problems, *Proc. 10th ACM Symp. on Theory of Computing* (STOC) No. 15 (1978), pp. 216–226.
[35] B. Schwarz, The complexity of satisfiability problems over finite lattices, in *Proc. 21st Annual Symposium on Theoretical Aspects of Computer Science* (STACS), Montpellier, France, *Lecture Notes in Comput. Sci.* **2996** (2004) 31–43.
[36] S. Seif, private communication.
[37] S. Seif and Cs. Szabó, Algebra complexity problems involving graph homomorphism, semigroups and the constraint satisfaction problem, *J. Complexity* **19** (2003) 153–160.
[38] S. Seif, Cs. Szabó and Z. Sokolovic, Complexity problems associated with matrix rings, matrix semigroups, and Rees matrix semigroups, preprint (1997).
[39] S. Seif and Cs. Szabó, Computational complexity of checking identities in simple semigroups and matrix semigroups over finite fields, preprint (2003).
[40] Á. Szendrei, *Clones in Universal Algebra*, Sém. de Mathématiques Supérieures, **99**, Séminaire Scientifique OTAN (les presses de l'Université de Montréal, 1986).
[41] W. Taylor, Varieties obeying homotopy laws, *Canad. J. Math.* **29** (1977) 498–527.
[42] W. Taylor, Laws obeyed by topological algebras — Extending results of Hopf and Adams, *J. Pure Appl. Algebra* **21** (1981) 75–98.
[43] P. Tesson, Computational complexity questions related to finite semigroups and monoids, Ph.D. Thesis, School of Computer Science, McGill University, Montréal (2003).
[44] R. J. Warne, Semigroups obeying the term condition, *Algebra Universalis* **31**(1) (1994) 113–123.