Solving Systems of Equations in Supernilpotent Algebras

Erhard Aichinger
Institute for Algebra, Johannes Kepler University Linz, Linz, Austria
https://www.jku.at/institut-fuer-algebra/
erhard@algebra.uni-linz.ac.at

Abstract

Recently, M. Kompatscher proved that for each finite supernilpotent algebra $\mathbf{A}$ in a congruence modular variety, there is a polynomial time algorithm to solve polynomial equations over this algebra. Let μ be the maximal arity of the fundamental operations of $\mathbf{A}$, and let

$$d := |A|^{\log_2 \mu + \log_2 |A| + 1}.$$

Applying a method that G. Károlyi and C. Szabó had used to solve equations over finite nilpotent rings, we show that for $\mathbf{A}$, there is $c \in \mathbb{N}$ such that a solution of every system of s equations in n variables can be found by testing at most cn^{sd} (instead of all $|A|^n$ possible) assignments to the variables. This also yields new information on some circuit satisfiability problems.

2012 ACM Subject Classification Mathematics of computing → Combinatorial algorithms; Theory of computation → Complexity classes

Keywords and phrases Supernilpotent algebras, polynomial equations, polynomial mappings, circuit satisfiability

Digital Object Identifier 10.4230/LIPIcs.MFCS.2019.72

Related Version A preliminary version is available on https://arxiv.org/abs/1901.07862.

Funding Supported by the Austrian Science Fund FWF P29931: Clonoids: a unifying approach to equational logic and clones

Acknowledgements The author thanks G. Horváth and M. Kompatscher for dicussions on solving equations over nilpotent algebras. Several of these discussions took place during a workshop organized by P. Aglianò at the University of Siena in June 2018. The author also thanks A. Földvári, C. Szabó, M. Kompatscher, and S. Kreinecker for their comments on preliminary versions of the manuscript, and the anonymous referees for several useful suggestions.

1 Introduction

We study systems of polynomial equations over a finite algebraic structure $\mathbf{A}$. Such a system is given by equations of the form $p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n)$, where p, q are polynomial terms of $\mathbf{A}$; a polynomial term of $\mathbf{A}$ is a term of the algebra $\mathbf{A}^*$ which is obtained by expanding $\mathbf{A}$ with one nullary function symbol for each $a \in A$. A *solution* to a system $p_i(x_1, \ldots, x_n) \approx q_i(x_1, \ldots, x_n)$ $(i = 1, \ldots, s)$ is an element $\boldsymbol{a} = (a_1, \ldots, a_n) \in A^n$ such that $p_i^{\mathbf{A}}(\boldsymbol{a}) = q_i^{\mathbf{A}}(\boldsymbol{a})$ for all $i \in \{1, \ldots, s\}$. The problem to decide whether such a solution exists has been called $\textsc{PolSysSat}(\mathbf{A})$, and $\textsc{PolSat}(\mathbf{A})$ if the system consists of one single equation, and the terms of the input are encoded as strings over $\{x_1, \ldots, x_n\} \cup A \cup F$, where F is the set of function symbols of $\mathbf{A}$. A survey of results on the computational complexity of this problem is given, e.g., in [13, 17]. In algebras such as groups, rings or Boolean algebras, one can reduce an equation $p(\boldsymbol{x}) \approx q(\boldsymbol{x})$ to an equation of the form $f(\boldsymbol{x}) \approx y$, where $y \in A$. A system of equations of this form then has the form $f_i(\boldsymbol{x}) \approx y_i$ $(i = 1, \ldots, s)$. For $n \in \mathbb{N}$, let $\mathrm{Pol}_n(\mathbf{A})$ denote the n-ary polynomial functions on $\mathbf{A}$ [19, Definition 4.4]. For a finite

44th International Symposium on Mathematical Foundations of Computer Science (MFCS 2019).
Editors: Peter Rossmanith, Pinar Heggernes, and Joost-Pieter Katoen; Article No. 72; pp. 72:1–72:9
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

nilpotent ring or group $\mathbf{A}$, [10, 12] establish the existence of a natural number $d_{\mathbf{A}}$ such that for every $f \in \mathrm{Pol}_n(\mathbf{A})$ and for every $\boldsymbol{a} \in A^n$, there exists $\boldsymbol{b}$ such that $f^{\mathbf{A}}(\boldsymbol{a}) = f^{\mathbf{A}}(\boldsymbol{b})$ and $\boldsymbol{b}$ has at most $d_{\mathbf{A}}$ components that are different from 0. Hence the equation $f(\boldsymbol{x}) \approx y$ has a solution if and only if it has a solution with at most $d_{\mathbf{A}}$ nonzero entries. Thus for the algebra $\mathbf{A}$, testing only vectors with at most $d_{\mathbf{A}}$ nonzero entries is an algorithm, which, given an equation $f(\boldsymbol{x}) \approx y$ of length n, takes at most $c(\boldsymbol{A}) \cdot n^{d_{\mathbf{A}}+1}$ many steps to find whether this equation is solvable: there are at most $\sum_{i=0}^{d_{\mathbf{A}}} \binom{n}{i}(|A|-1)^i \leq c_1(\mathbf{A}) \cdot n^{d_{\mathbf{A}}}$ many evaluations to be done, each of them taking at most $c_2(\mathbf{A}) \cdot n$ many steps. The number $d_{\mathbf{A}}$ in [12] is obtained from Ramsey's Theorem and therefore rather large. In [17], it is proved that for every finite supernilpotent algebra in a congruence modular variety, such a number $d_{\mathbf{A}}$ exists, again using Ramsey's Theorem. For rings, lower values of $d_{\mathbf{A}}$ have been obtained in [15] (cf. [14]). In [7, 8], A. Földvári provides polynomial time algorithms for solving equations over finite nilpotent groups and rings relying on the structure theory of these algebras. In this paper, we extend the method developed in [15] from finite nilpotent rings to arbitrary finite supernilpotent algebras in congruence modular varieties. For such algebras, we compute $d_{\mathbf{A}}$ as $|A|^{\log_2 \mu + \log_2 |A| + 1}$, where μ is the maximal arity of the fundamental operations of $\mathbf{A}$ (Theorem 10). The technique that allows to generalize Károlyi's and Szabó's method is the coordinatization of nilpotent algebras of prime power order by elementary abelian groups from [1, Theorem 4.2]. The method can be generalized to systems of equations: we show for a given finite supernilpotent algebra $\mathbf{A}$ in a congruence modular variety, and a given $s \in \mathbb{N}_0$, there is a polynomial time algorithm to test whether a system of at most s polynomial equations over $\mathbf{A}$ has a solution. If s is not fixed in advance, then [18, Corollary 3.13] implies that if $\mathbf{A}$ is not abelian, $\textsc{PolSysSat}(\mathbf{A})$ is NP-complete.

Let us finally explain to which class of algebras our results applies: A finite algebra $\mathbf{A}$ from a congruence modular variety with finitely many fundamental operations is supernilpotent if and only if it is a direct product of nilpotent algebras of prime power order; modulo notational differences explained, e.g., in [1, Lemma 2.4], this result has been proved in [16, Theorem 3.14]. Such an algebra is therefore always nilpotent, has a Mal'cev term (cf. [9, Theorem 6.2], [16, Theorem 2.7]), and hence generates a congruence permutable variety. For a more detailed introduction to supernilpotency and, for $k \in \mathbb{N}$, to k-supernilpotency, we refer to [2, 3, 1].

2 A theorem of Károlyi and Szabó

In this section, we state a special case of [15, Theorem 3.1]. Since their result is much more general than needed for our purpose, we also include a self-contained proof, which is a reduction Károlyi's and Szabó's proof to the case of elementary abelian groups.

For $n \in \mathbb{N} = \{1, 2, 3, \ldots\}$, we denote the set $\{1, 2, \ldots, n\}$ by $\underline{n}$. Let A be a set with an element $0 \in A$, and let $J \subseteq \underline{n}$. For $\boldsymbol{a} \in A^n$, $\boldsymbol{a}^{(J)}$ is defined by $\boldsymbol{a}^{(J)} \in A^n$, $\boldsymbol{a}^{(J)}(j) = \boldsymbol{a}(j)$ for $j \in J$ and $\boldsymbol{a}^{(J)}(j) = 0$ for $j \in \underline{n} \setminus J$. Suppose that 1 is an element of A. Then by $\boldsymbol{1}$, we denote the vector $(1, 1, \ldots, 1)$ in A^n, and for $J \subseteq \underline{n}$, $\boldsymbol{1}^{(J)}$ is the vector $(v_1, \ldots, v_n)$ with $v_j = 1$ if $j \in J$ and $v_j = 0$ if $j \notin J$. For any sets C, D, we write $C \subset D$ for ($C \subseteq D$ and $C \neq D$).

We first need the following variation of [5, Theorem 1] and [15, Theorem 3.2], which is proved using several arguments from the proof of [4, Theorem 3.1] and from [5].

▶ **Lemma 1.** *Let F be a finite field, let $k, m, n \in \mathbb{N}$, let $q := |F|$, let $p_1, \ldots, p_m \in F[x_1, \ldots, x_n]$ be polynomials such that for each $i \in \underline{m}$, each monomial of p_i contains at most k variables. Then there exists $J \subseteq \underline{n}$ such that $|J| \leq km(q-1)$ and $p_i(\boldsymbol{1}^{(J)}) = p_i(\boldsymbol{1})$ for all $i \in \underline{m}$.*

Proof. We proceed by induction on n. If $n \leq km(q-1)$, then we take $J := \underline{n}$. For the induction step, we assume that $n > km(q-1)$.

We first produce a set $J_1 \subset \underline{n}$ such that $p_i(\boldsymbol{1}^{(J_1)}) = p_i(\boldsymbol{1})$ for all $i \in \underline{m}$. Seeking a contradiction, we suppose that no such J_1 exists. Following an idea from the proof of [4, Theorem 3.1], we consider the polynomials

$$\begin{aligned} q_1(x_1, \ldots, x_n) &:= \textstyle\prod_{i=1}^{m} (1 - (p_i(\boldsymbol{x}) - p_i(\boldsymbol{1}))^{q-1}), \\ q_2(x_1, \ldots, x_n) &:= x_1 x_2 \cdots x_n - q_1(x_1, \ldots, x_n). \end{aligned}$$

We first show that for all $\boldsymbol{a} \in \{0,1\}^n$, $q_2(\boldsymbol{a}) = 0$. To this end, we first consider the case $\boldsymbol{a} = \boldsymbol{1}$. Then $q_2(\boldsymbol{a}) = 1 - \prod_{i=1}^{m} 1 = 0$. If $\boldsymbol{a} \in \{0,1\}^n \setminus \{\boldsymbol{1}\}$, then by the assumptions, there is $i \in \underline{m}$ such that $p_i(\boldsymbol{a}) \neq p_i(\boldsymbol{1})$. Then $1 - (p_i(\boldsymbol{a}) - p_i(\boldsymbol{1}))^{q-1} = 0$. Therefore $q_2(\boldsymbol{a}) = 0$. Hence the polynomial q_2 vanishes at $\{0,1\}^n$. By the Combinatorial Nullstellensatz [4, Theorem 1.1] applied to $g_j(x_j) := x_j^2 - x_j$, q_2 then lies in the ideal V of $F[x_1, \ldots, x_n]$ generated by $G = \{x_j^2 - x_j \mid j \in \underline{n}\}$. Hence $x_1 x_2 \cdots x_n - q_1(x_1, \ldots, x_n) \in V$. Since the leading monomials of the polynomials in G are coprime, G is a Gröbner basis of V (with respect to $x_1 > x_2 > \cdots > x_n$, lexicographic order, cf. [6, p.337]). Therefore, reducing $q_1(x_1, \ldots, x_n)$ modulo G, we must obtain $x_1 x_2 \cdots x_n$ as the remainder (as defined, e.g., in [6, p.334]). Because of the form of all polynomials in G (all variables of g_j occur in the leading term of g_j), none of the reduction steps increases the number of variables in any monomial. Therefore, $q_1(x_1, \ldots, x_n)$ must contain a monomial that contains all n variables. Computing the expansion of q_1 by multiplying out all products from its definition, we see that each monomial in q_1 contains at most $km(q-1)$ variables. Hence $n \leq km(q-1)$, which contradicts the assumption $n > km(q-1)$. This contradiction shows that there is a set $J_1 \subset \underline{n}$ such that $p_i(\boldsymbol{1}^{(J_1)}) = p_i(\boldsymbol{1})$ for all $i \in \underline{m}$. Now we let $n' := |J_1|$, and we assume that $J_1 = \{j_1, \ldots, j_{n'}\}$ with $j_1 < \cdots < j_{n'}$. For $i \in \underline{m}$, we define $p_i' \in F[y_1, \ldots, y_{n'}]$ by

$$p_i'(x_{j_1}, \ldots, x_{j_{n'}}) = p_i(\boldsymbol{x}^{(J_1)}).$$

By the induction hypothesis, there exists $J_2 \subseteq \underline{n'}$ with $|J_2| \leq km(q-1)$ such that $p_i'(\boldsymbol{1}^{(J_2)}) = p_i'(\boldsymbol{1})$ for all $i \in \underline{m}$. Now we define $J := \{j_t \mid t \in J_2\}$. We have $J \subseteq J_1$, and therefore $\boldsymbol{1}^{(J)} = (\boldsymbol{1}^{(J)})^{(J_1)}$. Then $p_i(\boldsymbol{1}^{(J)}) = p_i((\boldsymbol{1}^{(J)})^{(J_1)}) = p_i'(\boldsymbol{1}^{(J)}(j_1), \ldots, \boldsymbol{1}^{(J)}(j_{n'})) = p_i'(\boldsymbol{1}^{(J_2)}) = p_i'(\boldsymbol{1}) = p_i(\boldsymbol{1}^{(J_1)}) = p_i(\boldsymbol{1})$, which completes the induction step. ◀

We will need the following special case of [15, Theorem 3.1]. For a set U, let $\mathcal{P}_{\leq k}(U)$ denote the set $\{I \subseteq U : |I| \leq k\}$ of subsets of U with at most k elements.

▶ **Theorem 2** (cf. [15, Theorem 3.1]). *Let $n \in \mathbb{N}$, let $k \in \mathbb{N}_0$, let p be a prime, and let $m \in \mathbb{N}$. Let $\varphi : \mathcal{P}_{\leq k}(\underline{n}) \to \mathbb{Z}_p^m$. Then there is $U \subseteq \underline{n}$ with $|U| \leq km(p-1)$ such that*

$$\sum_{J \in \mathcal{P}_{\leq k}(\underline{n})} \varphi(J) = \sum_{J \in \mathcal{P}_{\leq k}(U)} \varphi(J).$$

Proof. We denote the vector $\varphi(J)$ by $((\varphi(J))_1, \ldots, (\varphi(J))_m)$, and we define m polynomial functions $f_1, \ldots, f_m \in \mathbb{Z}_p[x_1, \ldots, x_n]$ by

$$f_i(x_1, \ldots x_n) := \sum_{J \in \mathcal{P}_{\leq k}(\underline{n})} \big((\varphi(J))_i \cdot \prod_{j \in J} x_j\big).$$

for $i \in \underline{m}$. By Lemma 1, there is a subset U of $\underline{n}$ with $|U| \leq km(p-1)$ such that for all $i \in \underline{m}$, we have $f_i(\boldsymbol{1}) = f_i(\boldsymbol{1}^{(U)})$. Hence $\sum_{J \in \mathcal{P}_{\leq k}(\underline{n})} (\varphi(J))_i = f_i(\boldsymbol{1}) = f_i(\boldsymbol{1}^{(U)}) = \sum_{J \in \mathcal{P}_{\leq k}(\underline{n}), J \subseteq U} (\varphi(J))_i = \sum_{J \in \mathcal{P}_{\leq k}(U)} (\varphi(J))_i$. ◀

3 Absorbing components

Let A be a set, let 0_A be an element of A, let $\mathbf{B} = (B, +, -, 0)$ be an abelian group, let $n \in \mathbb{N}$, let $f : A^n \to B$, and let $I \subseteq \underline{n}$. By $\mathrm{Dep}(f)$ we denote the set $\{i \in \underline{n} \mid f \text{ depends on its } i\text{th argument}\}$. We say that f is *absorbing in its j th argument* if for all $\boldsymbol{a} = (\boldsymbol{a}(1), \dots, \boldsymbol{a}(n)) \in A^n$ with $\boldsymbol{a}(j) = 0_A$ we have $f(\boldsymbol{a}) = 0$. In the sequel, we will denote 0_A simply by 0. We say that f is *absorbing in I* if $\mathrm{Dep}(f) \subseteq I$ and for every $i \in I$, f is absorbing in its ith argument.

▶ **Lemma 3.** *Let A be a set, let 0 be an element of A, let $\mathbf{B} = (B, +, -, 0)$ be an abelian group, let $n \in \mathbb{N}$, and let $f : A^n \to B$. Then there is exactly one sequence $(f_I)_{I \subseteq \underline{n}}$ of functions from A^n to B such that for each $I \subseteq \underline{n}$, f_I is absorbing in I and $f = \sum_{I \subseteq \underline{n}} f_I$. Furthermore, each function f_I lies in the subgroup $\mathbf{F}$ of $\mathbf{B}^{A^n}$ that is generated by the functions $\boldsymbol{x} \mapsto f(\boldsymbol{x}^{(I)})$, where $I \subseteq \underline{n}$.*

Proof. We first prove the existence of such a sequence. To this end, we define f_I by recursion on $|I|$. We define $f_\varnothing(\boldsymbol{a}) := f(0, \dots, 0)$ and for $I \neq \varnothing$, we let

$$f_I(\boldsymbol{a}) := f(\boldsymbol{a}^{(I)}) - \sum_{J \subset I} f_J(\boldsymbol{a}).$$

By induction on $|I|$, we see that $\mathrm{Dep}(f_I) \subseteq I$ and that f_I lies in the subgroup $\mathbf{F}$. We will now show that each f_I is absorbing in I, and we again proceed by induction on $|I|$. Let $i \in I$, and let $\boldsymbol{a} \in A^n$ be such that $\boldsymbol{a}(i) = 0$. We have to show $f_I(\boldsymbol{a}) = 0$. We compute $f_I(\boldsymbol{a}) = f(\boldsymbol{a}^{(I)}) - \sum_{J \subset I} f_J(\boldsymbol{a})$. By the induction hypothesis, we have $f_J(\boldsymbol{a}) = 0$ for those J with $i \in J$. Hence $f(\boldsymbol{a}^{(I)}) - \sum_{J \subset I} f_J(\boldsymbol{a}) = f(\boldsymbol{a}^{(I)}) - \sum_{J \subseteq I \setminus \{i\}} f_J(\boldsymbol{a})$, and because of $\boldsymbol{a}^{(I)} = \boldsymbol{a}^{(I \setminus \{i\})}$, this is equal to $f(\boldsymbol{a}^{(I \setminus \{i\})}) - \sum_{J \subseteq I \setminus \{i\}} f_J(\boldsymbol{a}) = f(\boldsymbol{a}^{(I \setminus \{i\})}) - \sum_{J \subset I \setminus \{i\}} f_J(\boldsymbol{a}) - f_{I \setminus \{i\}}(\boldsymbol{a})$. By the definition of $f_{I \setminus \{i\}}$, the last expression is equal to $f_{I \setminus \{i\}}(\boldsymbol{a}) - f_{I \setminus \{i\}}(\boldsymbol{a}) = 0$. This completes the induction proof; hence each f_I is absorbing in I. In order to show $f = \sum_{I \subseteq \underline{n}} f_I$, we choose $\boldsymbol{a} \in A^n$ and compute $\sum_{I \subseteq \underline{n}} f_I(\boldsymbol{a}) = f_{\underline{n}}(\boldsymbol{a}) + \sum_{I \subset \underline{n}} f_I(\boldsymbol{a}) = f(\boldsymbol{a}^{(\underline{n})}) - \sum_{J \subset \underline{n}} f_J(\boldsymbol{a}) + \sum_{I \subset \underline{n}} f_I(\boldsymbol{a}) = f(\boldsymbol{a})$. This completes the proof of the existence of such a sequence.

For the uniqueness, assume that $f = \sum_{I \subseteq \underline{n}} f_I = \sum_{I \subseteq \underline{n}} g_I$ and that for all I, f_I and g_I are absorbing in I. We show by induction on $|I|$ that $f_I = g_I$. Let $I := \varnothing$. First we notice that $f(0, \dots, 0) = \sum_{J \subseteq \underline{n}} f_J(0, \dots, 0) = \sum_{J \subseteq \underline{n}} g_J(0, \dots, 0)$. Since f_J and g_J are absorbing, the summands with $J \neq \varnothing$ are 0, and thus $f_\varnothing(0, \dots, 0) = \sum_{J \subseteq \underline{n}} f_J(0, \dots, 0) = f(0, \dots, 0) = \sum_{J \subseteq \underline{n}} g_J(0, \dots, 0) = g_\varnothing(0, \dots, 0)$. Since both $f_\varnothing$ and $g_\varnothing$ are constant functions, they are equal. For the induction step, we assume $|I| \geq 1$. Let $\boldsymbol{a} \in A^n$. Then $\sum_{J \subseteq \underline{n}} f_J(\boldsymbol{a}^{(I)}) = \sum_{J \subseteq \underline{n}} g_J(\boldsymbol{a}^{(I)})$. Only the summands with $J \subseteq I$ can be nonzero, and therefore $\sum_{J \subseteq I} f_J(\boldsymbol{a}^{(I)}) = \sum_{J \subseteq I} g_J(\boldsymbol{a}^{(I)})$. By the induction hypothesis, $f_J = g_J$ for $J \subset I$. Therefore, $f_I(\boldsymbol{a}^{(I)}) = g_I(\boldsymbol{a}^{(I)})$. Since f_I and g_I depend only on the arguments at positions in I, we obtain $f_I(\boldsymbol{a}) = f_I(\boldsymbol{a}^{(I)}) = g_I(\boldsymbol{a}^{(I)}) = g_I(\boldsymbol{a})$. Thus $f_I = g_I$. ◀

Actually, the component f_I can be computed by $f_I(\boldsymbol{a}) = \sum_{J \subseteq I} (-1)^{|I|+|J|} f(\boldsymbol{a}^{(J)})$.

▶ **Definition 4.** *Let A be a set, let 0 be an element of A, let $\mathbf{B} = (B, +, -, 0)$ be an abelian group, let $n \in \mathbb{N}$, let $f : A^n \to B$, and let $J \subseteq \underline{n}$. Then we call the sequence $(f_I)_{I \subseteq \underline{n}}$ such that for each $I \subseteq \underline{n}$, f_I is absorbing in I, and $f = \sum_{I \subseteq \underline{n}} f_I$ the* absorbing decomposition *of f, and f_J the J-*absorbing component *of f. We define the* absorbing degree *of f by* $\mathrm{adeg}(f) := \max\left(\{-1\} \cup \{|J| : J \subseteq \underline{n} \text{ and } f_J \neq 0\}\right)$.

▶ **Theorem 5.** *Let A be a set, let 0 be an element of A, let p be a prime, let $k \in \mathbb{N}_0$, let $n \in \mathbb{N}$, and let $f_1, \ldots, f_m : A^n \to \mathbb{Z}_p$. We assume that each f_i is of absorbing degree at most k. Let $\boldsymbol{a} \in A^n$. Then there is U with $|U| \leq km(p-1)$ such that for all $i \in \underline{m}$, we have $f_i(\boldsymbol{a}) = f_i(\boldsymbol{a}^{(U)})$.*

Proof. We define a function $\varphi : \mathcal{P}_{\leq k}(\underline{n}) \to \mathbb{Z}_p^m$ by $\varphi(J) := ((f_1)_J(\boldsymbol{a}), \ldots, (f_m)_J(\boldsymbol{a}))$, where for $i \in \underline{m}$, $\big((f_i)_J\big)_{J \subseteq \underline{n}}$ is the absorbing decomposition of f_i. Then Theorem 2 yields a subset U of $\underline{n}$ with $|U| \leq km(p-1)$ such that $\sum_{J \in \mathcal{P}_{\leq k}(\underline{n})} \varphi(J) = \sum_{J \in \mathcal{P}_{\leq k}(U)} \varphi(J)$. Since $(f_i)_J = 0$ for all J with $|J| > k$, we have $\sum_{J \in \mathcal{P}_{\leq k}(\underline{n})} \varphi(J) = \sum_{J \in \mathcal{P}_{\leq k}(\underline{n})} ((f_1)_J(\boldsymbol{a}), \ldots, (f_m)_J(\boldsymbol{a})) = \sum_{J \subseteq \underline{n}} ((f_1)_J(\boldsymbol{a}), \ldots, (f_m)_J(\boldsymbol{a})) = (f_1(\boldsymbol{a}), \ldots, f_m(\boldsymbol{a}))$ and

$$\begin{aligned} \sum_{J \in \mathcal{P}_{\leq k}(U)} \varphi(J) &= \sum_{J \in \mathcal{P}_{\leq k}(U)} ((f_1)_J(\boldsymbol{a}), \ldots, (f_m)_J(\boldsymbol{a})) \\ &= \sum_{J \subseteq U} ((f_1)_J(\boldsymbol{a}), \ldots, (f_m)_J(\boldsymbol{a})) = \sum_{J \subseteq U} ((f_1)_J(\boldsymbol{a}^{(U)}), \ldots, (f_m)_J(\boldsymbol{a}^{(U)})) \\ &= \sum_{J \subseteq \underline{n}} ((f_1)_J(\boldsymbol{a}^{(U)}), \ldots, (f_m)_J(\boldsymbol{a}^{(U)})) = (f_1(\boldsymbol{a}^{(U)}), \ldots, f_m(\boldsymbol{a}^{(U)})). \end{aligned}$$

◀

4 Polynomial mappings

In this section, we develop a property of polynomial mappings of finite supernilpotent algebras in congruence modular varieties. We call an algebra $\mathbf{A} = (A, +, -, 0, (f_i)_{i \in S})$ an *expanded group* if its reduct $\mathbf{A}^+ = (A, +, -, 0)$ is a group, an *expanded abelian group* if $\mathbf{A}^+$ is an abelian group, and an *expanded elementary abelian group* if $\mathbf{A}^+$ is elementary abelian, meaning that $\mathbf{A}^+$ is abelian and all its nonzero elements have the same prime order.

▶ **Lemma 6.** *Let $k, n \in \mathbb{N}$, let $\mathbf{A}$ be a k-supernilpotent expanded abelian group, and let $f \in \mathrm{Pol}_n(\mathbf{A})$. Then f is of absorbing degree at most k.*

Proof. Let $J \subseteq \underline{n}$ with $|J| > k$, and let f_J be the J-absorbing component of f. Let $m := |J|$ and let $J = \{i_1, \ldots, i_m\}$. Using Lemma 3, we obtain that the function $g : A^m \to A$ defined by $g(a_{i_1}, \ldots, a_{i_m}) := f_J(\mathbf{a})$ for $\mathbf{a} \in A^n$ is an absorbing function in $\mathrm{Pol}_m(\mathbf{A})$. Hence [1, Lemma 2.3] and the remark immediately preceding that Lemma yield that g is the zero function. Thus $f_J = 0$. Hence the absorbing degree of f is at most k. ◀

We first consider polynomial mappings of supernilpotent expanded elementary abelian groups of prime power order.

▶ **Theorem 7.** *Let $k, n, s, \alpha \in \mathbb{N}$, let $p \in \mathbb{P}$, and let $\mathbf{A}$ be a k-supernilpotent expanded elementary abelian group of order p^α. Let $F = (f_1, \ldots, f_s) \in \mathrm{Pol}_n(\mathbf{A})^s$, and let $\boldsymbol{a} \in A^n$. Then there is $U \subseteq \underline{n}$ with $|U| \leq ks\alpha(p-1)$ such that $F(\boldsymbol{a}) = F(\boldsymbol{a}^{(U)})$.*

Proof. We let π be a group isomorphism from $(A, +, -, 0)$ to $\mathbb{Z}_p^\alpha$, and for $a \in A$, we denote $\pi(a)$ by $(\pi_1(a), \ldots, \pi_\alpha(a))$. For each $r \in \underline{s}$ and each $\beta \in \underline{\alpha}$, let $f_{r,\beta} : A^n \to \mathbb{Z}_p$ be defined by $f_{r,\beta}(\boldsymbol{a}) = \pi_\beta(f_r(\boldsymbol{a}))$; hence $f_{r,\beta}(\boldsymbol{a})$ is the βth component of $f_r(\boldsymbol{a})$. Since $f_r \in \mathrm{Pol}_n(\mathbf{A})$ and $\mathbf{A}$ is k-supernilpotent, Lemma 6 implies that each of these $f_{r,\beta}$ is of absorbing degree at most k. Setting $m := s\alpha$, Theorem 5 yields U with $|U| \leq ks\alpha(p-1)$ such that $f_{r,\beta}(\boldsymbol{a}) = f_{r,\beta}(\boldsymbol{a}^{(U)})$ for all $r \in \underline{s}$ and $\beta \in \underline{\alpha}$. Then clearly $F(\boldsymbol{a}) = F(\boldsymbol{a}^{(U)})$. ◀

We apply this result to polynomial mappings of *direct products* of finite supernilpotent expanded elementary abelian groups. For a vector $\boldsymbol{a} \in A^n$, we call the number of its nonzero entries the *weight* of $\mathbf{a}$; formally, $\mathrm{wt}(\boldsymbol{a}) := |\{j \in \underline{n} : \boldsymbol{a}(j) \neq 0\}|$.

▶ **Theorem 8.** *Let $n, s, t, k_1, \dots, k_t \in \mathbb{N}$. For each $i \in \underline{t}$, let $\mathbf{B}_i$ a k_i-supernilpotent expanded elementary abelian group with $|\mathbf{B}_i| = p_i^{\alpha_i}$, where p_i is a prime and $\alpha_i \in \mathbb{N}$. Let $\mathbf{A} := \prod_{i=1}^t \mathbf{B}_i$, let $F \in \mathrm{Pol}_n(\mathbf{A})^s$, and let $\boldsymbol{a} \in A^n$. Then there is $\boldsymbol{y} \in A^n$ with $\mathrm{wt}(\boldsymbol{y}) \leq \sum_{i=1}^t k_i s \alpha_i (p_i - 1)$ such that $F(\boldsymbol{a}) = F(\boldsymbol{y})$.*

Proof. For $i \in \underline{t}$, let ν_i be the ith projection kernel. Applying Theorem 7 to $\mathbf{A}/\nu_i$, which is isomorphic to $\mathbf{B}_i$, and $\boldsymbol{b} := \boldsymbol{a}/\nu_i$, we obtain $U_i \subseteq \underline{n}$ with $|U_i| \leq k_i s \alpha_i (p_i - 1)$ such that $F^{\mathbf{A}/\nu_i}(\boldsymbol{b}^{(U_i)}) = F^{\mathbf{A}/\nu_i}(\boldsymbol{b})$. Lifting $\boldsymbol{b}^{(U_i)}$ to A, we obtain $(x_{i,1}, \dots, x_{i,n}) \in A^n$ such that $(x_{i,1}, \dots, x_{i,n})/\nu_i = \boldsymbol{b}^{(U_i)}$ and $x_{i,j} = 0$ for $j \in \underline{n} \setminus U_i$. Now for every $j \in \underline{n}$, we define $y_j \in A$ by the equations

$$y_j \equiv_{\nu_i} x_{i,j} \text{ for all } i \in \underline{t}.$$

For each $i \in \underline{t}$, we have $F(y_1, \dots, y_n)/\nu_i = F^{\mathbf{A}/\nu_i}(x_{i,1}/\nu_i, \dots, x_{i,n}/\nu_i) = F^{\mathbf{A}/\nu_i}(\boldsymbol{b}^{(U_i)}) = F^{\mathbf{A}/\nu_i}(\boldsymbol{b}) = F^{\mathbf{A}/\nu_i}(\boldsymbol{a}/\nu_i) = F(\boldsymbol{a})/\nu_i$. Hence $F(\boldsymbol{y}) = F(\boldsymbol{a})$. For $j \in \underline{n} \setminus (U_1 \cup \dots \cup U_t)$, and for all $i \in \underline{t}$, we have $x_{i,j} = 0$, and therefore $y_j = 0$. Hence the number of nonzero entries in $\boldsymbol{y}$ is at most $\sum_{i=1}^t |U_i| \leq \sum_{i=1}^t k_i s \alpha_i (p_i - 1)$. ◀

Now we consider *arbitrary* finite supernilpotent algebras in congruence modular varieties. In these algebras, we can introduce group operations preserving nilpotency using [1].

▶ **Lemma 9.** *Let $\mu \in \mathbb{N}$, let $\mathbf{A} = (A, (f_i)_{i \in S})$ be a finite supernilpotent algebra in a congruence modular variety all of whose fundamental operations have arity at most μ, and let $z \in A$. Let $t \in \mathbb{N}_0$, let $p_1, \dots, p_t$ be different primes, and let $\alpha_1, \dots, \alpha_t \in \mathbb{N}$ such that $|\mathbf{A}| = \prod_{i=1}^t p_i^{\alpha_i}$. For $i \in \underline{t}$, let $k_i := (\mu(p_i^{\alpha_i} - 1))^{\alpha_i - 1}$. Then there are operations $+$ (binary), $-$ (unary), 0 (nullary) on A such that $\mathbf{A}' = (A, +, -, 0, (f_i)_{i \in S})$ is isomorphic to a direct product $\prod_{i=1}^t \mathbf{B}'_i$, where each $\mathbf{B}'_i$ is a k_i-supernilpotent expanded elementary abelian group, and $0^{\mathbf{A}'} = z$.*

Proof. Since the result is true for $|A| = 1$, we henceforth assume $|A| \geq 2$. By [16], $\mathbf{A}$ is isomorphic to a direct product $\prod_{i=1}^t \mathbf{B}_i$ of nilpotent algebras of prime power order. We let $(\pi_1(a), \dots, \pi_t(a))$ denote the image of a of the underlying isomorphism. As a finite supernilpotent algebra in a congruence modular variety, $\mathbf{A}$ is nilpotent (cf. [1, Lemma 2.4]) and therefore has a Mal'cev term [9, Theorem 6.2]. We use [1, Theorem 4.2] to expand each $\mathbf{B}_i$ with operations $+_i$ and $-_i$ such that the expansion $\mathbf{B}'_i$ is a nilpotent expanded elementary abelian group with zero element $\pi_i(z)$. By [1, Theorem 1.2], $\mathbf{B}'_i$ is k_i-supernilpotent. ◀

We note that the supernilpotency degree of $\mathbf{A}'$ may be strictly larger than the supernilpotency degree of $\mathbf{A}$.

Combining these results, we obtain the following result on polynomial mappings on arbitrary finite supernilpotent algebras in congruence modular varieties.

▶ **Theorem 10.** *Let $\mu \in \mathbb{N}$, let $\mathbf{A}$ be a finite supernilpotent algebra in a congruence modular variety all of whose fundamental operations have arity at most μ. Let $p_1, \dots, p_t$ be distinct primes, and let $\alpha_1, \dots, \alpha_t \in \mathbb{N}$ such that $|\mathbf{A}| = \prod_{i=1}^t p_i^{\alpha_i}$. Let $F \in \mathrm{Pol}_n(\mathbf{A})^s$ be a polynomial map from A^n to A^s, and let $z \in A$. Then for every $\boldsymbol{a} \in A^n$ there is $\boldsymbol{y} \in A^n$ such that $F(\boldsymbol{y}) = F(\boldsymbol{a})$ and $|\{j \in \underline{n} : \boldsymbol{y}(j) \neq z\}| \leq s \sum_{i=1}^t (\mu(p_i^{\alpha_i} - 1))^{\alpha_i - 1} \alpha_i (p_i - 1) \leq s\mu^{-1} |A|^{\log_2 \mu + \log_2 |A|} \log_2 |A| \leq s|A|^{\log_2 \mu + \log_2 |A| + 1}$.*

Proof. Let $\mathbf{A}' = \prod_{i=1}^{t} \mathbf{B}_i'$ with $|\mathbf{B}_i'| = p_i^{\alpha_i}$ be the expansion of $\mathbf{A}$ produced by Lemma 9. Clearly, F is a also a polynomial map of $\mathbf{A}'$. Let $k_i = (\mu(p_i^{\alpha_i} - 1))^{\alpha_i - 1}$. Then Theorem 8 yields $\boldsymbol{y} \in A^n$ such that $|\{j \in \underline{n} : \boldsymbol{y}(j) \neq z\}| \leq \sum_{i=1}^{t} k_i s \alpha_i (p_i - 1)$. Using the obvious estimate $\alpha_i \leq \log_2 |A|$, we obtain

$$\begin{aligned}
&\sum_{i=1}^{t} k_i s \alpha_i (p_i - 1) = s \sum_{i=1}^{t} (\mu(p_i^{\alpha_i} - 1))^{\alpha_i - 1} \log_2 |A| (p_i - 1) \\
&\leq s \log_2 |A| \sum_{i=1}^{t} \mu^{\alpha_i - 1} (p_i^{\alpha_i})^{\alpha_i - 1} p_i^{\alpha_i} \leq s \log_2 |A| \sum_{i=1}^{t} \mu^{\log_2 |A| - 1} (p_i^{\alpha_i})^{\alpha_i} \\
&\leq s \mu^{\log_2 |A| - 1} \log_2 |A| \sum_{i=1}^{t} (p_i^{\alpha_i})^{\log_2 |A|} \leq s \mu^{\log_2 |A| - 1} \log_2 |A| (\sum_{i=1}^{t} p_i^{\alpha_i})^{\log_2 |A|} \\
&\leq s \mu^{\log_2 |A| - 1} \log_2 |A| (\prod_{i=1}^{t} p_i^{\alpha_i})^{\log_2 |A|} \leq s \mu^{\log_2 |A| - 1} \log_2 |A| \, |A|^{\log_2 |A|} \\
&\qquad\qquad\qquad = s \mu^{-1} |A|^{\log_2 \mu + \log_2 |A|} \log_2 |A| \leq s |A|^{\log_2 \mu + \log_2 |A| + 1}.
\end{aligned}$$

◀

5 Systems of equations

We will now explain how these results give a polynomial time algorithm for solving systems of a fixed number of equations over the finite supernilpotent algebra $\mathbf{A}$. The size m of a system of polynomial equations is measured as the length of the polynomial terms used to represent the system. For measuring the "running time" of our algorithm, we count the number of $\mathbf{A}$-operations: each such $\mathbf{A}$-operation, may, for example, be done by looking up one value in the operation tables defining $\mathbf{A}$.

▶ **Theorem 11.** *Let $\mathbf{A}$ be a finite supernilpotent algebra in a congruence modular variety all of whose fundamental operations are of arity at most μ, and let $s \in \mathbb{N}$. We consider the following algorithmic problem s-*PolSysSat*$(\mathbf{A})$:*

Given: *$2s$ polynomial terms $f_1, g_1, \ldots, f_s, g_s$ over $\mathbf{A}$.*
Asked: *Does the system $f_1 \approx g_1, \ldots, f_s \approx g_s$ have a solution in $\mathbf{A}$?*

Let m be the length of the input of this system, and let

$$e := s|A|^{\log_2 \mu + \log_2 |A| + 1} + 1.$$

*Then we can decide s-*PolSysSat*$(\mathbf{A})$ using at most $O(m^{e-1})$ evaluations of all terms occuring in the system. Therefore, we have an algorithm that determines whether a system of s polynomial equations over $\mathbf{A}$ has a solution using $O(m^e)$ many $\mathbf{A}$-operations.*

Proof. Let n be the number of different variables that occur in the given system. We may assume that these variables are $x_1, \ldots, x_n$, and that our system is $\bigwedge_{i=1}^{s} f_i(x_1, \ldots, x_n) \approx g_i(x_1, \ldots, x_n)$. We choose an element $z \in A$, and we will show: if this system has a solution in A^n, then it has a solution in

$$C := \{\boldsymbol{y} \in A^n : |\{j \in \underline{n} : \boldsymbol{y}(j) \neq z\}| \leq e - 1\}.$$

For proving this claim, we first observe that $\mathbf{A}$ is a finite nilpotent algebra in a congruence modular variety, and it therefore has a Mal'cev term d. We consider the polynomial map

$H = (h_1, \dots, h_s)$, where $h_i(\boldsymbol{x}) := d(f_i(\boldsymbol{x}), g_i(\boldsymbol{x}), z)$ for $i \in \underline{s}$ and $\boldsymbol{x} \in A^n$. Since $\boldsymbol{a}$ is a solution of the system, $H(\boldsymbol{a}) = (z, z, \dots, z)$. By Theorem 10, there is $\boldsymbol{y} \in C$ such that $H(\boldsymbol{y}) = H(\boldsymbol{a})$. Then for every $i \in \underline{s}$, we have $d(f_i(\boldsymbol{y}), g_i(\boldsymbol{y}), z) = z$. By [9, Corollary 7.4], the function $x \mapsto d(x, g_i(\boldsymbol{y}), z)$ is injective. Since $d(f_i(\boldsymbol{y}), g_i(\boldsymbol{y}), z) = z = d(g_i(\boldsymbol{y}), g_i(\boldsymbol{y}), z)$, this injectivity implies that $f_i(\boldsymbol{y}) = g_i(\boldsymbol{y})$. Hence $\boldsymbol{y}$ is a solution that lies in C.

The algorithm for solving the system now simply evaluates the system at all places in C; if a solution is found, the answer is “yes”. If we find no solution inside C , we answer “no”, and by the argument above, we know that in this case, the system has no solution inside $\mathbf{A}^n$ at all.

We now estimate the complexity of this procedure: There is a $c \in \mathbb{N}$ such that for all $n \in \mathbb{N}$, $|C| \le cn^{e-1}$, hence we have to do $O(n^{e-1})$ evaluations of all the terms f_i, g_i in the system. Such an evaluation can be done using at most $O(m)$ many $\mathbf{A}$-operations. Since the length of the input m is at least the number of variables n occuring in it, this solves s-PolSysSat($\mathbf{A}$) using at most $O(m^e)$ many $\mathbf{A}$-operations. ◀

We remark that the exponent e involves neither the nilpotency nor the supernilpotency degree of the algebra $\mathbf{A}$; this is a result of the fact that Theorem 1.2 from [1] bounds the supernilpotency degree of $\mathbf{A}$ in terms of only μ, $|A|$, and the height of the congruence lattice of $\mathbf{A}$, which is bounded from above by $\log_2 |A|$. In the same vein, we can now also bound the exponent in the complexity bound for the *identity checking* or *polynomial equivalence* problem for supernilpotent algebras (cf. [2, Theorem 2.2]). For every algebra $\mathbf{A}$ satisfying the assumptions of Theorem 11, there is $c \in \mathbb{N}$ such that for any two n-ary polynomial terms $s(x_1, \dots, x_n)$ and $t(x_1, \dots, x_n)$, we can check whether $\mathbf{A} \models s \approx t$ using at most cn^d evaluations of both s and t, where $d := (\mu(|A| - 1))^{\log_2 |A| - 1}$ comes from Corollary 1.3 of [1].

6 Circuit satisfiability

With every finite algebra $\mathbf{A}$, [13] associates a number of computational problems that involve circuits whose gates are taken from the fundamental operations of $\mathbf{A}$. One of these problems is SCsat($\mathbf{A}$). It takes as an input $2s$ circuits $f_1, g_1, \dots, f_s, g_s$ over $\mathbf{A}$ with n input variables, and asks whether there is an $\boldsymbol{a} \in A^n$ such that the evaluations at $\boldsymbol{a}$ satisfy $f_i(\boldsymbol{a}) = g_i(\boldsymbol{a})$ for all $i \in \underline{s}$. For finite algebras of finite type (i.e., with finitely many fundamental operations) in congruence modular varieties, [18, Corollary 3.13] implies that SCsat($\mathbf{A}$) is in P when $\mathbf{A}$ is abelian, and NP-complete otherwise. However, if we restrict the number s of circuits, we obtain a different problem, which we call s-SCsat($\mathbf{A}$) in the sequel. Obviously, 1-SCsat($\mathbf{A}$) is the circuit satisfiability problem called Csat($\mathbf{A}$) in [13]. The method used to prove Theorem 11 immediately yields:

▶ **Theorem 12.** *Let $\mathbf{A}$ be a finite supernilpotent algebra of finite type in a congruence modular variety, and let $s \in \mathbb{N}$. Then s-SCsat($\mathbf{A}$) is in* P.

Hence a supernilpotent, but not abelian algebra $\mathbf{A}$ has s-SCsat($\mathbf{A}$) in P, whereas SCsat is NP-complete. In the converse direction, Theorem 9.1 from [13] has the following corollary.

▶ **Corollary 13.** *Let $\mathbf{A}$ be a finite algebra of finite type from a congruence modular variety. If $\mathbf{A}$ has no homomorphic image $\mathbf{A}'$ such that* 2-SCsat($\mathbf{A}'$) *is* NP-*complete, then $\mathbf{A}$ is nilpotent.*

Proof. Suppose that $\mathbf{A}$ has a homomorphic image $\mathbf{A}'$ for which Csat($\mathbf{A}'$) is NP-complete. Then also 2-SCsat($\mathbf{A}'$) is NP-complete because an algorithm solving 2-SCsat can be used to solve an instance $(\exists \boldsymbol{a})(f(\boldsymbol{a}) = g(\boldsymbol{a}))$ of Csat($\mathbf{A}'$) by solving 2-SCsat on the input

$(\exists \boldsymbol{a})(f(\boldsymbol{a}) = g(\boldsymbol{a})\ \&\ f(\boldsymbol{a}) = g(\boldsymbol{a}))$. Thus the assumptions imply that for no homomorphic image $\mathbf{A}'$ of $\mathbf{A}$, the problem CSAT($\mathbf{A}'$) is NP-complete. Now by [13, Theorem 9.1], $\mathbf{A}$ is isomorphic to $\mathbf{N} \times \mathbf{D}$, where $\mathbf{N}$ is nilpotent and $\mathbf{D}$ is a subdirect product of 2-element algebras each of which is polynomially equivalent to a two element lattice. If $|\mathbf{D}| > 1$, then there is a homomorphic image $\mathbf{A}_2$ of $\mathbf{A}$ such that $\mathbf{A}_2$ is polynomially equivalent to a two element lattice. By [11], 2-SCSAT($\mathbf{A}_2$) is NP-complete, contradicting the assumptions. Hence $|\mathbf{D}| = 1$, and therefore $\mathbf{A}$ is nilpotent. ◀

References

1 E. Aichinger. Bounding the free spectrum of nilpotent algebras of prime power order. *Israel J. Math.*, 230(2):919–947, 2019.

2 E. Aichinger and N. Mudrinski. Some applications of higher commutators in Mal'cev algebras. *Algebra Universalis*, 63(4):367–403, 2010.

3 E. Aichinger, N. Mudrinski, and J. Opršal. Complexity of term representations of finitary functions. *Internat. J. Algebra Comput.*, 28(6):1101–1118, 2018.

4 N. Alon. Combinatorial Nullstellensatz. *Combin. Probab. Comput.*, 8(1-2):7–29, 1999. Recent trends in combinatorics (Mátraháza, 1995).

5 D. Brink. Chevalley's theorem with restricted variables. *Combinatorica*, 31(1):127–130, 2011.

6 D. Eisenbud. *Commutative algebra*. Springer-Verlag, New York, 1995.

7 A. Földvári. The complexity of the equation solvability problem over semipattern groups. *Internat. J. Algebra Comput.*, 27(2):259–272, 2017.

8 A. Földvári. The complexity of the equation solvability problem over nilpotent groups. *Journal of Algebra*, 495:289–303, 2018.

9 R. Freese and R. N. McKenzie. *Commutator Theory for Congruence Modular varieties*, volume 125 of *London Math. Soc. Lecture Note Ser.* Cambridge University Press, 1987.

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

11 T. Gorazd and J. Krzaczkowski. The complexity of problems connected with two-element algebras. *Rep. Math. Logic*, 46:91–108, 2011.

12 G. Horváth. The complexity of the equivalence and equation solvability problems over nilpotent rings and groups. *Algebra Universalis*, 66(4):391–403, 2011.

13 P. M. Idziak and J. Krzaczkowski. Satisfiability in multi-valued circuits. In *LICS '18—33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 550–558. ACM, New York, 2018.

14 G. Károlyi and C. Szabó. The complexity of the equation solvability problem over nilpotent rings. Manuscript available at `http://web.cs.elte.hu/~csaba/publications/`, 2015.

15 G. Károlyi and C. Szabó. Evaluation of Polynomials over Finite Rings via Additive Combinatorics. *ArXiv e-prints*, 1809.06543, 2018. `arXiv:1809.06543`.

16 K. A. Kearnes. Congruence modular varieties with small free spectra. *Algebra Universalis*, 42(3):165–181, 1999.

17 M. Kompatscher. The equation solvability problem over supernilpotent algebras with Mal'cev term. *Internat. J. Algebra Comput.*, 28(6):1005–1015, 2018.

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

19 R. N. McKenzie, G. F. McNulty, and W. F. Taylor. *Algebras, lattices, varieties, Volume I*. Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, California, 1987.