On the Complexity Dichotomy for the Satisfiability of Systems of Term Equations over Finite Algebras

Peter Mayr
Department of Mathematics, University of Colorado Boulder, CO, USA
Institute for Algebra, Johannes Kepler Universität Linz, Austria

Abstract

For a fixed finite algebra $\mathbf{A}$, we consider the decision problem SysTerm($\mathbf{A}$): does a given system of term equations have a solution in $\mathbf{A}$? This is equivalent to a constraint satisfaction problem (CSP) for a relational structure whose relations are the graphs of the basic operations of $\mathbf{A}$. From the complexity dichotomy for CSP over fixed finite templates due to Bulatov [4] and Zhuk [18], it follows that SysTerm($\mathbf{A}$) for a finite algebra $\mathbf{A}$ is in P if $\mathbf{A}$ has a not necessarily idempotent Taylor polymorphism and is NP-complete otherwise. More explicitly, we show that for a finite algebra $\mathbf{A}$ in a congruence modular variety (e.g. for a quasigroup), SysTerm($\mathbf{A}$) is in P if the core of $\mathbf{A}$ is abelian and is NP-complete otherwise. Given $\mathbf{A}$ by the graphs of its basic operations, we show that this condition for tractability can be decided in quasi-polynomial time.

2012 ACM Subject Classification Theory of computation → Problems, reductions and completeness

Keywords and phrases systems of equations, general algebras, constraint satisfaction

Digital Object Identifier 10.4230/LIPIcs.MFCS.2023.66

Funding Partially supported by the Austrian Science Fund (FWF): P33878.

Acknowledgements I want to thank E. Aichinger for discussions on this problem and the referees for their diligent reading and comments.

1 Introduction

How hard is it to check whether a system of term equations is solvable in an algebra? The *System of Term Equations Satisfiability Problem* over a fixed algebra $\mathbf{A}$ is the following decision problem:

SysTerm($\mathbf{A}$)	
Input:	terms $s_1, t_1, \dots, s_m, t_m$ in the signature of $\mathbf{A}$
Problem:	Does $s_1 \approx t_1, \dots, s_m \approx t_m$ have a solution in $\mathbf{A}$?

For example, SysTerm for the ring of integers $(\mathbb{Z}, +, \cdot, 1)$ is Hilbert's tenth problem and undecidable by Matiyasevich's theorem. In this note we only consider SysTerm for finite algebras (meaning algebraic structures of finite size and finite signature), which clearly can be solved in non-deterministic polynomial time (NP).

Obviously SysTerm($\mathbf{A}$) has always a positive answer if $\mathbf{A}$ has a trivial subalgebra $\{o\}$ by setting all variables to o. Hence it is trivial for most classical algebras like groups, rings (without 1 as basic operation), lattices, and semigroups with idempotents[1]. This is one reason why the related problem SysPol, the satisfiability problem for a system of polynomial equations (allowing also constants), has received more attention in the past. Note that SysPol can be considered as the restriction of SysTerm to algebras for which each constant

[1] Rings with 1, quasigroups, more generally magmas, and G-sets are some of the few named algebras without trivial subalgebras. However, among finite algebras with randomly chosen operations, almost none have trivial subalgebras by a result of Murskiĭ [2, Theorem 6.16].

is a basic operation. We will show that for any finite $\mathbf{A}$ there exists some algebra $\mathbf{A}'$ (the core of $\mathbf{A}$) such that SysTerm($\mathbf{A}$) and SysPol($\mathbf{A}'$) are equivalent under logspace reductions (see Lemmas 6 and 7).

Goldmann and Russell [11] showed that SysPol (which they denote as EQN*) is in P for abelian and NP-complete for non-abelian finite groups. Klíma, Tesson and Thérien [14] investigated SysPol over finite semigroups and showed that it is in P for commutative monoids that are unions of their subgroups and NP-complete for other monoids. Larose and Zádori [15] studied SysPol over finite algebras in general and observed that they are logspace-equivalent to constraint satisfaction problems (CSP) of a specific form. They showed in particular that SysPol for any finite $\mathbf{A}$ in a congruence modular variety (including most classical algebras like groups, modules, rings, quasigroups, lattices but not semigroups) is in P if $\mathbf{A}$ is abelian (meaning the operations of $\mathbf{A}$ are affine functions over an abelian group) and NP-complete otherwise. By using the universal algebraic definition of commutators and abelianness, this generalizes the previously mentioned result of Goldmann and Russell. Broniek [3] investigated SysPol and SysTerm for unary algebras (where all basic operations are unary). He showed in particular that SysTerm for unary algebras of size at most 3 is in P or NP-complete.

Our goal in this note is first to explicitly state the connections between SysTerm, SysPol and CSP by a straightforward adaptation of the approach of Larose and Zádori in Section 3. From the celebrated complexity dichotomy for CSP by Bulatov [4] and Zhuk [18], we then obtain immediately that SysTerm for any finite algebra is either in P or NP-complete in Theorem 1. For finite $\mathbf{A}$ in a congruence modular variety, we give an algebraic criterion for when SysTerm($\mathbf{A}$) is tractable in Theorem 2. Finally we show that this criterion can be decided in quasi-polynomial time for $\mathbf{A}$ given by the graphs of its operations in Theorem 3.

For the precise statement of our results we recall some notions that play an important role in the classification of CSPs and algebras. For a structure $\mathcal{C}$ (possibly with function and relation symbols) define *polymorphisms* of $\mathcal{C}$ as the homomorphisms from finite powers of $\mathcal{C}$ to $\mathcal{C}$ and denote the set of polymorphisms as

$$\mathrm{Pol}(\mathcal{C}) := \bigcup_{n\in\mathbb{N}} \mathrm{Hom}(\mathcal{C}^n, \mathcal{C}).$$

For example, the polymorphisms of a vector space $\mathbf{A}$ are just the linear maps from $\mathbf{A}^n$ to $\mathbf{A}$ for $n \in \mathbb{N}$.

Let $f\colon A^n \to A$ for $n > 1$. Then f is *Taylor* if it satisfies n identities in distinct variables x, y of the form

$$f(\dots, \underset{i}{x}, \dots) \approx f(\dots, \underset{i}{y}, \dots) \text{ for all } i \in \{1, \dots, n\}$$

where the omitted variables on either side may be x or y. These identities were chosen so that no projection map on a non-trivial domain can satisfy them.

Next $f\colon A^4 \to A$ is *Siggers* if it satisfies

$$f(a, r, e, a) \approx f(r, a, r, e).$$

For example, a binary commutative operation f is Taylor by virtue of $f(x, y) \approx f(y, x)$. By adding two fictitous variables we also obtain a Siggers operation from f. Clearly every Siggers operation is Taylor. In fact, every finite structure $\mathcal{C}$ has a Taylor polymorphism of some arity iff $\mathcal{C}$ has a Siggers polymorphism [13, 17].

As in [1] we do not require that Taylor and Siggers operations are idempotent like in older literature (see Lemma 8 for the relation with their idempotent version). This allows for a convenient formulation of the dichotomy for CSP and consequently the dichotomy for SysTerm.

▶ **Theorem 1.** *Let* $\mathbf{A}$ *be a finite algebra. Then* SysTerm($\mathbf{A}$) *is in* P *if* $\mathbf{A}$ *has a (not necessarily idempotent) Taylor (equivalently Siggers) polymorphism; else* SysTerm($\mathbf{A}$) *is* NP*-complete.*

We will show Theorem 1 in Section 3 by encoding SysTerm over an algebra as CSP over a relational structure and invoking the dichotomy for CSPs.

We already observed that SysTerm for $\mathbf{A}$ with a trivial subalgebra $\{o\}$ is trivial. Still to put this into the context of Theorem 1, note that such an algebra has $f(x, y) := o$ as a Taylor polymorphism. For a less obvious example, $\mathbf{A} = (\mathbb{Z}_2, +, 0, 1)$ has $x + y + z$ as Taylor polymorphism and consequently tractable SysTerm.

Theorem 1 generalizes all the dichotomy results for SysPol in [11, 14, 15] mentioned above and fully settles the P/NP-complete dichotomy for SysTerm. Still it would be desirable to describe its boundary in more explicit structural terms of the algebra $\mathbf{A}$ than by the existence of certain polymorphisms. We manage to do this under the assumption of additional structural properties on $\mathbf{A}$.

Here we just review the bare minimum of notions from universal algebra that we need to state our results. For more details we refer to [2, 5, 16] and Section 2 below. A *variety* is a class of algebras of fixed signature that is defined by identities. For example, groups form a variety with a binary operation $\cdot$, a unary $^{-1}$ and constant 1 satisfying the usual group axioms. Varieties are usually classified by so-called Mal'cev conditions, essentially the term identities they satisfy. We list the conditions which occur in this note in increasing strength.

- A variety V is *Taylor* if it has a term t which induces an idempotent Taylor operation on all its algebras. Here idempotent means that V satisfies $t(x, \dots, x) \approx x$.
  For example, semilattices form a Taylor variety with Taylor term $t(x, y) := xy$ but (commutative) semigroups and G-sets do not.
- A variety V is *congruence modular* if every algebra $\mathbf{A}$ in V has a modular congruence lattice.
  Most classical algebras, in particular those that have (quasi)group operations, like groups, modules, rings, loops, ... or lattice operations, like lattices, Boolean algebras, Heyting algebras,... are members of congruence modular varieties. On the other hand, semilattices and more generally semigroups do not form congruence modular varieties.
- A variety is *congruence distributive* if all its algebras have distributive congruence lattices.
  Every algebra with lattice operations is contained in a congruence distributive variety but non-trivial groups are not.

Since distributivity implies modularity for lattices, congruence distributive varieties are congruence modular. Further congruence modular varieties are Taylor.

There exist various generalizations of commutators from groups to arbitrary algebras. These may differ in general but most of them lead to the same concept of abelianess in Taylor varieties (see [9, 12]). In particular, a finite algebra $\mathbf{A}$ in a Taylor variety is *abelian* (with respect to the standard term condition commutator) iff all its basic operations are affine functions of some commutative group $(A, +, -, 0)$. Although such an abelian algebra $\mathbf{A}$ may not have $+$ or $-$ as term operations, the ternary function $x - y + z$ is a term operation and is called the *Mal'cev term operation* of $\mathbf{A}$. A group is abelian in this sense iff it is abelian in the classical group theoretic sense. A loop is abelian iff it is an abelian group. Since for a ring the commutator of congruences corresponds to the product of ideals, a ring is abelian iff its multiplication is 0. For a lattice or any algebra in a congruence distributive variety, the commutator of two congruences is just their intersection. Hence these algebras are abelian iff they are trivial.

Next we extend some established notions and facts on relational structures to the setting of algebras. A finite structure $\mathcal{C}$ (possibly with function and relational symbols) is a *core* if every endomorphism of $\mathcal{C}$ is an embedding (equivalently, an automorphism). It is well-known

and not hard to see that if h is an endomorphism of a finite structure $\mathcal{C}$ such that $h(\mathcal{C})$ is minimal with respect to inclusion among all endomorphic images of $\mathcal{C}$, then $h(\mathcal{C})$ is a core. Moreover this core is unique up to isomorphism and hence called *the core of* $\mathcal{C}$. An algebra has trivial core iff it has a trivial subalgebra. An algebra expanded with all constants is its own core. For a non-degenerate example, the core of the symmetric group $(S_3, \cdot, (), (1,2))$ expanded with the additional constant $(1,2)$ is isomorphic to $(\mathbb{Z}_2, +, 0, 1)$.

We will prove the following generalization of a result by Larose and Zádori on the complexity of systems of polynomial equations [15, Corollary 3.14] in Section 4.

▶ **Theorem 2.** *Let* $\mathbf{A}$ *be a finite algebra in a congruence modular variety. Then* SysTerm($\mathbf{A}$) *is in* P *if the core of* $\mathbf{A}$ *is abelian; else* SysTerm($\mathbf{A}$) *is* NP*-complete.*

Since any non-trivial ring with 1 is non-abelian by the discussion of commutators above, it follows that its SysTerm is NP-complete.

Also, since non-trivial algebras in congruence distributive varieties are non-abelian, Theorem 2 yields that SysTerm($\mathbf{A}$) for such a finite $\mathbf{A}$ is NP-complete unless $\mathbf{A}$ has a trivial subalgebra and hence trivial core, in which case SysTerm($\mathbf{A}$) is trivial.

A natural follow-up to the dichotomy results above is the metaquestion of deciding for a given algebra $\mathbf{A}$ whether it has tractable SysTerm. Or, for practical purposes, how much preprocessing is necessary on a given algebra $\mathbf{A}$ with abelian core such that one can solve SysTerm for $\mathbf{A}$ in polynomial time in the size of the system of equations? Here and in the following we assume that algebras are given by the graphs of their basic operations.

Recall that a finite structure has a (not necessarily idempotent) Taylor polymorphism iff it has a (not necessarily idempotent) 4-ary Siggers polymorphism. The latter condition can clearly be decided in NP. So the metaquestion for SysTerm, i.e., deciding whether a given finite algebra $\mathbf{A}$ has a (not necessarily idempotent) Taylor polymorphism, is in NP.

Chen and Larose showed that the metaquestion for CSP, i.e., deciding whether a given finite relational structure $\mathbb{A}$ has a (not necessarily idempotent) Taylor polymorphism, is actually NP-complete [6]. Klíma, Tesson and Thérien constructed for every finite relational structure $\mathbb{A}$ a finite semigroup $\mathbf{A}$ such that CSP($\mathbb{A}$) is polynomial time equivalent to SysPol($\mathbf{A}$) [14, Theorem 8]. Similarly, Broniek constructed for every finite relational structure $\mathbb{A}$ a finite unary algebra $\mathbf{A}$ such that CSP($\mathbb{A}$) is polynomial time equivalent to SysTerm($\mathbf{A}$) [3, Theorem 3.4]. However, for both these constructions, the size of the algebra $\mathbf{A}$ is exponential in the size of relational structure $\mathbb{A}$. Hence they do not allow to transfer the NP-hardness of the metaquestion for CSP to the metaquestion for SysTerm. To the best of our knowledge, it may be easier to decide for algebras whether they have a Taylor polymorphism than for relational structures.

In particular, for an algebra in a congruence modular variety, the existence of a (not necessarily idempotent) Taylor polymorphism can be decided in quasi-polynomial time by the following slightly stronger result, which we will prove in Section 5. Recall that congruence modular varieties are Taylor.

▶ **Theorem 3.** *There exists a quasi-polynomial time algorithm that, given a finite algebra* $\mathbf{A}$ *in a Taylor variety, decides if the core of* $\mathbf{A}$ *is abelian, in which case the core of* $\mathbf{A}$ *and the graph of its Mal'cev term operation can also be computed in quasi-polynomial time.*

Thus given a finite algebra $\mathbf{A}$ in a Taylor variety, we can compute its core $\mathbf{C}$ in quasi-polynomial time if $\mathbf{C}$ is abelian. Moreover, if the core $\mathbf{C}$ is abelian, we can use its Mal'cev term operation $x - y + z$ to reduce SysTerm($\mathbf{A}$) to a linear system of equations over the abelian group $(C, +)$. If a system of term equations over abelian $\mathbf{C}$ (equivalently over $\mathbf{A}$) has a solution, then we can also find it in polynomial time in the size of the system.

We do not know whether the quasi-polynomial time algorithms in Theorem 3 can be improved to polynomial time.

Of course one can also ask how hard it is to check the assumptions of Theorem 3 in case that the idempotent Taylor term operation of $\mathbf{A}$ is not given as part of the input. For that Freese and Valeriote showed that deciding whether a given finite algebra $\mathbf{A}$ is in a Taylor variety or whether it is in a congruence modular variety is EXPTIME-complete [10, Corollary 9.3] but that these problems are in P for idempotent $\mathbf{A}$, i.e., if all basic operations f of $\mathbf{A}$ satisfy $f(x,\dots,x) \approx x$ [10, Theorem 6.2, 6.3].

2 Preliminaries

We review the algebraic results that we will need. For standard universal algebraic background we refer the reader to [2, 5, 9, 12, 16].

2.1 Algebras and varieties

An *algebra* $\mathbf{A} = (A, \{f^{\mathbf{A}} : f \in F\})$ is a pair where A is a non-empty set (the *universe* of $\mathbf{A}$), F is a set of function symbols equipped with a map arity$\colon F \to \mathbb{N}$ that assigns to each function symbol its arity (the *signature* of $\mathbf{A}$), and $f^{\mathbf{A}}$ are the interpretations of the symbols $f \in F$ as operations of the corresponding arity on A (the *basic operations* of $\mathbf{A}$). We say $\mathbf{A}$ is *finite* if its universe and its signature are finite. An algebra is *trivial* if its universe has size 1.

F-terms or *terms in the signature* of $\mathbf{A}$ are constructed from function symbols F and variables $x_1, x_2, \dots$ in the usual way: every variable is an F-term, and if $f \in F$ is k-ary and $t_1,\dots,t_k$ are F-terms, then $f(t_1,\dots,t_k)$ is an F-term. Every F-term t in variables $x_1,\dots,x_k$ induces a k-ary *term function* $t^{\mathbf{A}}\colon A^k \to A$ by interpreting a variable x_i as the i-th projection from A^k onto A and interpreting function symbols f as $f^{\mathbf{A}}$.

Polynomials over $\mathbf{A}$ are defined like terms except that additionally for every element $a \in A$ there is a constant polynomial a. Again every polynomial p in variables $x_1,\dots,x_k$ induces a k-ary *polynomial function* $p^{\mathbf{A}}\colon A^k \to A$ via the interpretation of function symbols in F on A and the interpretation of a constant a as the corresponding element $a \in A$. Two algebras $\mathbf{A}_1 = (A, F_1)$ and $\mathbf{A}_2 = (A, F_2)$ on the same universe are *polynomially equivalent* if $\mathbf{A}_1$ and $\mathbf{A}_2$ have the same set of polynomial functions of all arities.

An *identity* is a pair of terms (s,t), which we usually write as $s \approx t$. For k-ary terms s,t, the k-tuple $(a_1,\dots,a_k) \in A^k$ is a *solution* of $s(x_1,\dots,x_k) \approx t(x_1,\dots,x_k)$ if $s^{\mathbf{A}}(a_1,\dots,a_k) = t^{\mathbf{A}}(a_1,\dots,a_k)$. An algebra $\mathbf{A}$ *satisfies* an identity $s \approx t$ if $s^{\mathbf{A}} = t^{\mathbf{A}}$.

A *variety* V is a class of algebras over the same fixed signature F that is defined by a set of identities Σ, that is, $V = \{\mathbf{A} : \mathbf{A} \text{ satisfies } \Sigma\}$. Birkhoff showed that the variety generated by a class K of algebras over F consists of all homomorphic images of subalgebras of direct powers of elements in K.

A variety V is *locally finite* if all its finitely generated algebras are finite. For example, the variety generated by a finite algebra $\mathbf{A}$ is locally finite.

2.2 Commutators

Commutators have been generalized from normal subgroups of groups to congruences of general algebras by Smith, Hagemann, Herrmann, Gumm, Freese, McKenzie and others. See [9] for the history and overview of their development.

For congruences α, β of an algebra $\mathbf{A}$, let $M_{\mathbf{A}}(\alpha, \beta)$ be the subalgebra of $\mathbf{A}^{2\times 2}$ that is generated by all elements of the form

$$\begin{bmatrix} a & a \\ b & b \end{bmatrix}, \begin{bmatrix} c & d \\ c & d \end{bmatrix} \quad \text{for } a\alpha b, c\beta d.$$

Writing quadruples as 2×2 tables is just a notational convenience here. The operations of $\mathbf{A}$ simply apply componentwise. The *commutator* $[\alpha, \beta]$ is the smallest congruence γ of $\mathbf{A}$ such that

$$\forall \begin{bmatrix} x & y \\ z & w \end{bmatrix} \in M_{\mathbf{A}}(\alpha, \beta) \colon x\gamma y \Rightarrow z\gamma w.$$

For an algebra $\mathbf{A}$ let 1_A denote the total congruence and 0_A denote the trivial congruence (equality). Then $\mathbf{A}$ is *abelian* if $[1_A, 1_A] = 0_A$.

Abelianess has strong structural consequences of an algebra. Assume $\mathbf{A}$ is a finite abelian algebra in a Taylor variety. Then $\mathbf{A}$ is polynomially equivalent to a module by [12, 9]. More explicitly, there exist operation $+, -, 0$ such that $(A, +, -, 0)$ is an abelian group with a set of endomorphisms R. Every k-ary basic operation $f^{\mathbf{A}}$ of $\mathbf{A}$ can be represented in the form

$$f^{\mathbf{A}}(x_1, \dots, x_k) = \sum_{i=1}^{k} r_i(x_i) + c$$

for some endomorphisms $r_1, \dots, r_k \in R$ and some constant $c \in A$. Given a term t of $\mathbf{A}$ it can be rewritten iteratively as a sum of endomorphisms of $(A, +, -, 0)$ and constants in polynomial time as well. Hence SysTerm($\mathbf{A}$) reduces to solving a system of linear equations over $(A, +, -, 0)$, which is clearly in P.

2.3 Tame congruence theory

For congruence α, β of an algebra $\mathbf{A}$ we say α is *covered* by β (written $\alpha \prec \beta$) if α is strictly contained in β and there is no congruence strictly between α and β.

A finite non-trivial algebra is *minimal* if all its unary polynomial operations are either constant or permutations. Pálfy showed that every minimal algebra is polynomially equivalent to an algebra of one the following five types:

1. a G-set (i.e., an algebra all of whose basic operations are permutations);
2. a vector space;
3. the Boolean algebra of size 2;
4. the lattice of size 2;
5. the semilattice of size 2.

Tame congruence theory (TCT) as developed by Hobby and McKenzie in [12] associates with any pair of congruences $\alpha \prec \beta$ of a finite algebra $\mathbf{A}$ a set of minimal algebras all of which have the same type 1-5. The precise construction is quite technical and will not be needed in this paper. Hence we will not discuss it beyond stating that every pair $\alpha \prec \beta$ is labelled with a unique type. The set of all types of pairs $\alpha \prec \beta$ of $\mathbf{A}$ is denoted by typ$\{\mathbf{A}\}$. For a variety V the set of all types of $\alpha \prec \beta$ of all finite algebras $\mathbf{A}$ in V is denoted by typ$\{V\}$.

There are deep connections between the typeset of a variety V, that is, the local behaviour of polynomial functions on its finite members, and the identities that hold in V. For example:

- [12, Theorem 9.6] A locally finite variety V is Taylor iff $1 \notin \text{typ}\{V\}$.
- [12, Theorem 8.5] If a locally finite variety V is congruence modular, then typ$\{V\} \subseteq \{2, 3, 4\}$.

3 SysTerm, SysPol and CSP

In this section we collect easy facts on the correspondence between systems of equations and constraint satisfaction problems that may be known at least implicitely in one form or the other. Still we hope it is useful to provide an explicit and consistent overview for the reader.

3.1 Reduction to CSP

First we reduce a system of equations to a particular constraint satisfaction problem. The *Constraint Satisfaction Problem* over a fixed relational structure $\mathbb{A}$ is the decision problem:

CSP($\mathbb{A}$)
Input: a structure $\mathbb{X}$ in the signature of $\mathbb{A}$
Problem: Is there a homomorphism from $\mathbb{X}$ to $\mathbb{A}$?

Many classical decision problems like 3-SAT, graph coloring, solvability of linear systems... can be formulated as CSP for an appropriately chosen structure $\mathbb{A}$. For background on CSP on fixed templates we refer to the survey [1] by Barto, Krokhin and Willard.

Denote the *graph* of a k-ary operation $f\colon A^k \to A$ by the $k+1$-ary relation

$$f^\circ := \{(x_1, \dots, x_k, f(x_1, \dots, x_k)) \ : \ x_1, \dots, x_k \in A\}.$$

For an algebra $\mathbf{A} = (A, F)$ with universe A and basic operations F, let $\mathbb{A}^\circ := (A, \{f^\circ \ : \ f \in F\})$ denote the relational structure with the graphs of the basic operations as relations.

Larose and Zádori observed the following correspondence between SysPol and CSP. The proof for systems of term equations is essentially the same and added here for the convenience of the reader.

▶ **Lemma 4** ([15, cf. Theorem 2.2]). *Let* $\mathbf{A}$ *be a finite algebra. Then* SysTerm($\mathbf{A}$) *is logspace-equivalent to* CSP($\mathbb{A}^\circ$).

Proof. For a CSP($\mathbb{A}^\circ$)-instance $\mathbb{X}$, each constraint $(x_{i_1}, \dots, x_{i_{k+1}}) \in f^\circ$ can be reformulated as $f(x_{i_1}, \dots, x_{i_k}) \approx x_{i_{k+1}}$ in constant time. Clearly the conjunction of constraints is satisfiable iff the system of corresponding equations is solvable in $\mathbf{A}$.

Conversely, for a SysTerm($\mathbf{A}$)-instance $s_1 \approx t_1, \dots, s_m \approx t_m$, rewrite each occurring term $t = f(u_1, \dots, u_k)$ for a basic operation f of $\mathbf{A}$ as a sequence of constraints $(y_{u_1}, \dots, y_{u_k}, y_t) \in f^\circ$ in variables y indexed by subterms and correspondingly for the subterms $u_1, \dots, u_k$. If $t = x$ is a variable, just write $y_t = x$. All these constraints together with $y_s = y_t$ for every given equation $s \approx t$ form a CSP($\mathbb{A}^\circ$)-instance which is satisfiable iff the original system of equations over $\mathbf{A}$ is solvable. This rewriting creates as many new variables as there are function symbols and variables in $s_1, t_1, \dots, s_m, t_m$ and can be done in logarithmic space. ◀

It is straightforward to check that the polymorphisms of $\mathbf{A}$ are the same as those of $\mathbb{A}^\circ$.

▶ **Lemma 5.** Pol($\mathbf{A}$) = Pol($\mathbb{A}^\circ$) *for every algebra* $\mathbf{A}$.

Proof. Let $h\colon A^n \to A$, $f\colon A^k \to A$ and $x_1 = (x_{11}, \dots, x_{1n}), \dots, x_k = (x_{k1}, \dots, x_{kn})$ in A^n. Then $hf(x_1, \dots, x_k) = f(h(x_1), \dots, h(x_k))$ with f acting on A^n componentwise iff

$$h\left(\begin{bmatrix} x_{11} \\ \vdots \\ x_{k1} \\ f(x_{11}, \dots, x_{k1}) \end{bmatrix}, \dots, \begin{bmatrix} x_{1n} \\ \vdots \\ x_{kn} \\ f(x_{1n}, \dots, x_{kn}) \end{bmatrix}\right) \in f^\circ.$$

Hence h is a polymorphism of the algebra (A, f) iff h is a polymorphism of the relational structure (A, f°). The assertion follows. ◀

The previous two lemmas are already enough to obtain the complexity dichotomy for SysTerm from that for CSP.

Proof of Theorem 1. By Lemma 4 and 5 it suffices to consider CSP($\mathbb{A}^\circ$). Then the hardness part only uses that 3-SAT reduces to CSP($\mathbb{A}^\circ$) if $\mathbb{A}^\circ$ has no Taylor polymorphism [1, Theorem 40].

The tractability part follows from the celebrated result by Bulatov [4] and Zhuk [18] that CSP($\mathbb{A}$) for a finite relational structura $\mathbb{A}$ is in P if $\mathbb{A}$ has a (not necessarily idempotent) Taylor polymorphism. ◀

3.2 Cores

As for CSP, it suffices to investigate SysTerm for cores $\mathbf{A}$ by the next observation.

▶ **Lemma 6.** SysTerm($\mathbf{A}$) = SysTerm($h(\mathbf{A})$) *for each endomorphism* h *of* $\mathbf{A}$.

Proof. Let h be an endomorphism of $\mathbf{A}$. Obviously, if a system of term identities Σ has a solution in the subalgebra $h(\mathbf{A})$ of $\mathbf{A}$, then also in $\mathbf{A}$. Conversely, if Σ has a solution in $\mathbf{A}$, then clearly also in its homomorphic image $h(\mathbf{A})$. ◀

It is well-known that a CSP over a core relational structure is equivalent to the CSP over its expansion with singletons. Correspondingly, systems of term equations over a core algebra $\mathbf{A}$ are equivalent to systems of polynomial equations over $\mathbf{A}$. We give a direct proof of this fact since it is short and makes the reduction from SysPol to SysTerm more apparent.

▶ **Lemma 7.** *Let* $\mathbf{A}$ *be a finite algebra that is a core. Then* SysPol($\mathbf{A}$) *is logspace-equivalent to* SysTerm($\mathbf{A}$).

Proof. SysTerm($\mathbf{A}$) reduces trivially to SysPol($\mathbf{A}$). For the converse, the crucial observation is that the graphs of endomorphisms of $\mathbf{A}$ are the solutions of a system of term equations. By definition a map $h\colon A \to A$ is an endomorphism of $\mathbf{A}$ iff for all $f \in F$, say k-ary, and for all $a_1, \dots, a_k \in A$

$$f(h(a_1), \dots, h(a_k)) = h(f(a_1, \dots, a_k)).$$

Hence $\{(a, h(a)) \;:\; a \in A\}$ is the graph of an endomorphism of $\mathbf{A}$ iff $y_a = h(a)$ for $a \in A$ is a solution of the system of term equations

$$f(y_{a_1}, \dots, y_{a_k}) \approx y_{f(a_1,\dots,a_k)} \quad \text{for } f \in F \text{ (k-ary)}, a_1, \dots, a_k \in A. \tag{1}$$

Given an instance of SysPol($\mathbf{A}$) with variables $x_1, \dots, x_n$, we introduce $|A|$ new variables y_a for $a \in A$ and replace every occurrence of a constant a in a polynomial equation by y_a. To the resulting set of term equations we also add the equations (1) to obtain an instance of SysTerm($\mathbf{A}$). Note that the added system (1) does not depend on the original input, only on $\mathbf{A}$. Hence the new term system can be obtained from the original polynomial system in logspace by rewriting any occuring constant a as variable y_a.

If the original polynomial system has a solution, then clearly the new term system has a solution with $y_a = a$. Conversely, if the new system has a solution $x_1 = b_1, \dots, x_n = b_n$ and $y_a = h(a)$ for $a \in A$, then h is an endomorphism of $\mathbf{A}$. Since $\mathbf{A}$ is a core by assumption, h is in fact an automorphism. Hence $x_1 = h^{-1}(b_1), \dots, x_n = h^{-1}(b_n)$ and $y_a = a$ for $a \in A$ is also a solution of the new system. Thus $x_1 = h^{-1}(b_1), \dots, x_n = h^{-1}(b_n)$ is a solution of the original polynomial system. ◀

3.3 Polymorphisms satisfying height-1 identities

An identity has *height* 1 if it is of the form $f(u_1, \dots, u_k) \approx g(v_1, \dots, v_\ell)$ for operation symbols f, g and not necessarily distinct variables $u_1, \dots, u_k, v_1, \dots, v_\ell$.

For example, commutativity of a binary operation f is expressed by a height-1 identity but associativity is not since that requires nested applications of f.

Since the identities for a Taylor operation all have height 1, the next lemma yields that a structure has a (not necessarily idempotent) Taylor polymorphism iff its core has the corresponding idempotent polymorphism. For relational structures this is well-known and the same easy proof applies to general structures.

▶ **Lemma 8** ([6, cf. Lemma 6.4]). *Let Σ be a set of height-1 identities. Then a finite structure $\mathcal{C}$ (possibly with function and relation symbols) has polymorphisms satisfying Σ iff the core of $\mathcal{C}$ has idempotent polymorphisms satisfying Σ.*

Proof. Let h be an endomorphism of $\mathcal{C}$ such that $h(\mathcal{C})$ is the core of $\mathcal{C}$.

If F is a set of polymorphisms of $h(\mathcal{C})$ satisfying Σ, then $f'(x_1, \dots, x_k) := f(h(x_1), \dots, h(x_k))$ for $f \in F$ (k-ary) are polymorphisms of $\mathcal{C}$ and still satisfy the same height-1 identities.

Conversely, let F be polymorphisms of $\mathcal{C}$ satisfying Σ. For $f \in F$ (k-ary), let $f^*(x_1, \dots, x_k)$ be the restriction of $hf(x_1, \dots, x_k)$ to the substructure $h(\mathcal{C})$. Then $\{f^* : f \in F\}$ is a set of polymorphism of $h(\mathcal{C})$ which still satisfies the height-1 identities of Σ. Moreover, for every $f \in F$, we have that $f_1(x) := f^*(x, \dots, x)$ is an endomorphism of $h(\mathcal{C})$, hence an automorphism. Thus $f_1^{-1} f^*$ is an idempotent polymorphism of $h(\mathcal{C})$. If $f^*(u_1, \dots, u_k) \approx g^*(v_1, \dots, v_\ell)$ is in Σ, then $f_1 = g_1$ and consequently $f_1^{-1} f^*(u_1, \dots, u_k) \approx g_1^{-1} g^*(v_1, \dots, v_\ell)$ holds on $h(\mathcal{C})$. Hence $f_1^{-1} f^*$ for $f \in F$ are idempotent polymorphisms of $h(\mathcal{C})$ that still satisfy Σ. ◀

4 Systems over algebras in congruence modular varieties

Larose and Zádori explicitely characterized finite algebras without congruences $\alpha \prec \beta$ of TCT type 5 in Taylor varieties that have idempotent Taylor polymorphisms.

▶ **Theorem 9** ([15, Theorem 3.12]). *Let $\mathbf{A}$ be a finite algebra in a Taylor variety such that $5 \notin \mathrm{typ}\{\mathbf{A}\}$. Then $\mathbf{A}$ has an idempotent Taylor polymorphism iff $\mathbf{A}$ is abelian.*

Note that there exist non-abelian algebras with idempotent Taylor term operations that commute with themselves, e.g., semilattices. Hence the assumption $5 \notin \mathrm{typ}\{\mathbf{A}\}$ cannot be omitted in Theorem 9.

Theorem 9 yields an explicit characterization of the complexity of SysTerm over cores that parallels those of SysPol by Larose and Zádori.

▶ **Corollary 10** ([15, cf. Corollary 3.13]). *Let $\mathbf{A}$ be a finite algebra in a Taylor variety such that $5 \notin \mathrm{typ}\{\mathbf{A}\}$. Then $\mathrm{SysTerm}(\mathbf{A})$ is in P if the core of $\mathbf{A}$ is abelian; else $\mathrm{SysTerm}(\mathbf{A})$ is NP-complete.*

Proof. If the core $h(\mathbf{A})$ of $\mathbf{A}$ is abelian, then $h(\mathbf{A})$ is polynomially equivalent to a module with group operations $+, -$ by [12]. Further $\mathrm{SysTerm}(h(\mathbf{A}))$ reduces to a system of linear equations over that module. Then $d(x, y, z) = x - y + z$ is a polymorphism of $h(\mathbf{A})$ and also of the corresponding relational structure $h(\mathbb{A}^\circ)$ by Lemma 5. Hence $\mathrm{CSP}(h(\mathbb{A}^\circ))$ is a so-called general subgroup problem and can be solved in polynomial time by a result of Feder and Vardi [8, Theorem 33]. Then $\mathrm{SysTerm}(\mathbf{A})$ is in P by Lemmas 4 and 6.

Else if the core of $\mathbf{A}$ is not abelian, then it has no idempotent Taylor polymorphism by Theorem 9. Hence SysTerm($\mathbf{A}$) is NP-complete by the hardness of CSP over structures without Taylor polymorphisms and Lemma 6. ◀

The proof of Corollary 10 does not require the full strength of the CSP-dichotomy by Bulatov and Zhuk but only that linear systems over modules are in P. Moreover, for an abelian algebra $\mathbf{A}$ in a Taylor variety we can give a parametrization of all solutions of a system of term equations and determine their number by linear algebra in polynomial time. All of this applies in particular to algebras in congruence modular varieties.

Proof of Theorem 2. Let $\mathbf{A}$ be a finite algebra in a congruence modular variety. Then the variety V generated by $\mathbf{A}$ is locally finite and congruence modular. By [12, Theorem 8.5] V omits types 1 (i.e., V is Taylor) and 5. In particular $\mathbf{A}$ itself has no congruences $\alpha \prec \beta$ of type 5. Hence the result is a special case of Corollary 10. ◀

5 Metaquestions about the complexity dichotomy

In the following we assume that algebras $(A, f_1, \dots, f_m)$ are given by the graphs of their basic operations $f_1, \dots, f_m$. So, for n the maximum arity of $f_1, \dots, f_m$, this representation has size at least $|A|^n$.

We give a quasi-polynomial time algorithm to decide whether a given algebra in a Taylor variety has abelian core.

Proof of Theorem 3. Let $\mathbf{A}$ be a finite algebra in a Taylor variety. First we claim that the core of $\mathbf{A}$ is abelian iff there exists a homomorphism from the maximal abelian quotient $\bar{\mathbf{A}} := \mathbf{A}/[1,1]$ of $\mathbf{A}$ to $\mathbf{A}$.

For the "only if"-direction, assume that the core $h(\mathbf{A})$ for some endomorphism h of $\mathbf{A}$ is abelian. By the Homomorphism Theorem $h(\mathbf{A})$ is isomorphic to the quotient of $\mathbf{A}$ by the kernel $\ker h := \{(x,y) \in A^2 \ : \ h(x) = h(y)\}$ of h. In particular $\mathbf{A}/\ker h$ is abelian as well. By the definition of the commutator, $[1,1]$ is the unique smallest congruence of $\mathbf{A}$ such that $\mathbf{A}/[1,1]$ is abelian. Hence $[1,1] \leq \ker h$. Let $x/[1,1]$ denote the class of x modulo $[1,1]$ in $\bar{\mathbf{A}}$. Then $\bar{h}\colon \bar{\mathbf{A}} \to \mathbf{A},\ x/[1,1] \to h(x)$, is a well-defined homomorphism.

Conversely, for the "if"-direction, assume we have a homomorphism $\bar{h}\colon \bar{\mathbf{A}} \to \mathbf{A}$. Then $\bar{h}$ lifts to an endomorphism $h\colon \mathbf{A} \to \mathbf{A},\ x \mapsto \bar{h}(x/[1,1])$. Clearly the images of h and $\bar{h}$ are the same and the kernel $\ker h$ contains $[1,1]$. So by the Homomorphism Theorem $h(\mathbf{A})$ is isomorphic to a quotient of $\bar{\mathbf{A}}$. Note that $\bar{\mathbf{A}}$ is abelian in a Taylor variety and hence has a Mal'cev term operation d by [12, Theorem 9.6]. Hence $\bar{\mathbf{A}}$ is polynomially equivalent to a module and all its quotients are abelian as well by [9] (We note in passing that outside of Taylor varieties, unfortunately quotients of abelian algebras may not be abelian again). In particular $h(\mathbf{A})$ is abelian. While $h(\mathbf{A})$ may not be the core of $\mathbf{A}$, all images $g(\mathbf{A})$ for an endomorphism g of $\mathbf{A}$ that are contained in $h(\mathbf{A})$ are subalgebras of an abelian algebra, thus abelian themselves (This holds for arbitrary algebras by the definition of the commutator). Since the core of $\mathbf{A}$ is isomorphic to a minimal such image $g(\mathbf{A})$, it is abelian.

Hence it suffices to check whether there exists a homomorphism from $\bar{\mathbf{A}}$ to $\mathbf{A}$. Recall that the commutator $[1,1]$ can be enumerated in polynomial time by an algorithm due to Willard [7, Proposition 4.1]. Thus computation in $\bar{\mathbf{A}}$ effectively reduces to computation in $\mathbf{A}$ in the following steps.

Using the description of the structure of abelian algebras in congruence modular varieties from [9], we see that the subalgebra $M_{\bar{\mathbf{A}}}(1,1)$ of $\bar{\mathbf{A}}^{2\times 2}$ that is generated by all elements of the form

$$\begin{bmatrix} a & a \\ b & b \end{bmatrix}, \begin{bmatrix} c & d \\ c & d \end{bmatrix} \quad \text{for } a,b,c,d \in \bar{A}$$

has the universe

$$M_{\bar{\mathbf{A}}}(1,1) = \left\{ \begin{bmatrix} y & x \\ z & d(x,y,z) \end{bmatrix} \;:\; x,y,z \in \bar{A} \right\}.$$

Hence the Mal'cev term operation d on $\bar{\mathbf{A}}$ is unique and its graph can be computed by enumerating the elements in $M_{\bar{\mathbf{A}}}(1,1)$ by a straightforward closure algorithm in polynomial time. More specifically for any fixed element $u_0 \in \bar{A}$, the operations $x + y := d(x, u_0, y)$ and $-x := d(u_0, x, u_0)$ on $\bar{A}$ yield an abelian group $(\bar{A}, +, -, u_0)$ with zero element u_0. Further $d(x,y,z) = x - y + z$ for all $x,y,z \in \bar{A}$. Now we can grow a generating set $u_1, \dots, u_n$ of $(\bar{A}, +)$ with $n \leq \log_2 |\bar{A}|$ as follows. If $u_0, \dots, u_i$ are fixed and the generated subgroup $B_i := \langle u_0, \dots, u_i \rangle$ of $(\bar{A}, +)$ is not all of $\bar{A}$, then pick some $u_{i+1} \in \bar{A} \setminus B_i$. Note that the index of B_i in B_{i+1} is at least 2 by Lagrange's Theorem. So the process stops with $B_n = \bar{A}$ after $n \leq \log_2 |\bar{A}|$ steps each of which requires only polynomial time in $|A|$. Finally we have obtained a generating set $u_0, u_1, \dots, u_n$ for $(\bar{A}, x - y + z)$ and in particular for $\bar{\mathbf{A}}$ in polynomial time in $|A|$.

Clearly every homomorphism $h\colon \bar{\mathbf{A}} \to \mathbf{A}$ is uniquely determined by its images on the generators $u_0, \dots, u_n$. For $v_0, \dots, v_n \in A$ we can enumerate

$$\langle (u_0, v_0), \dots, (u_n, v_n) \rangle \leq \bar{\mathbf{A}} \times \mathbf{A}$$

in polynomial time to see whether the partial map with $h(u_i) := v_i$ for $i \in \{0, \dots, n\}$ extends to a homomorphism from $\bar{\mathbf{A}}$ to $\mathbf{A}$. Checking the $|A|^{n+1} \leq 2^{(\log |A|)^2 + \log |A|}$ potential images of $u_0, \dots, u_n$ yields an algorithm that decides the existence of a homomorphism from $\bar{\mathbf{A}}$ to $\mathbf{A}$ in quasi-polynomial time in $\mathbf{A}$.

If such a homorphism exists, then the homomorphism with smallest image maps $\bar{\mathbf{A}}$ to the abelian core of $\mathbf{A}$ with Mal'cev term operation induced by d on $\bar{\mathbf{A}}$. Thus the universe of the core of $\mathbf{A}$ can be obtained in quasi-polynomial time as well. ◀

References

1. L. Barto, A. Krokhin, and R. Willard. Polymorphisms, and how to use them. In Andrei A. Krokhin and Stanislav Zivný, editors, *The Constraint Satisfaction Problem: Complexity and Approximability*, volume 7 of *Dagstuhl Follow-Ups*, pages 1–44. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2017. doi:10.4230/DFU.Vol7.15301.1.
2. C. Bergman. *Universal algebra*, volume 301 of *Pure and Applied Mathematics (Boca Raton)*. CRC Press, Boca Raton, FL, 2012. Fundamentals and selected topics.
3. P. Broniek. *Computational complexity of solving equation systems*. SpringerBriefs in Philosophy. Springer, Cham, 2015. doi:10.1007/978-3-319-21750-5.
4. A. Bulatov. A dichotomy theorem for nonuniform CSPs. In Chris Umans, editor, *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 319–330. IEEE Computer Society, 2017. doi:10.1109/FOCS.2017.37.
5. S. Burris and H. P. Sankappanavar. *A course in universal algebra*. Springer New York Heidelberg Berlin, 1981.

6 H. Chen and B. Larose. Asking the metaquestions in constraint tractability. *ACM Trans. Comput. Theory*, 9(3):Art. 11, 27, 2017. doi:10.1145/3134757.

7 W. DeMeo, R. Freese, and M. Valeriote. Polynomial-time tests for difference terms in idempotent varieties. *Internat. J. Algebra Comput.*, 29(6):927–949, 2019. doi:10.1142/S021819671950036X.

8 T. Feder and M. Vardi. The computational structure of monotone monadic SNP and constraint satisfaction: a study through Datalog and group theory. *SIAM J. Comput.*, 28(1):57–104 (electronic), 1999. doi:10.1137/S0097539794266766.

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. Available from http://math.hawaii.edu/~ralph/Commutator/comm.pdf.

10 R. Freese and M. A. Valeriote. On the complexity of some Maltsev conditions. *Internat. J. Algebra Comput.*, 19(1):41–77, 2009. doi:10.1142/S0218196709004956.

11 M. Goldmann and A. Russell. The complexity of solving equations over finite groups. *Inf. Comput.*, 178(1):253–262, 2002. doi:10.1006/inco.2002.3173.

12 D. Hobby and R. McKenzie. *The structure of finite algebras*, volume 76 of *Contemporary mathematics*. American Mathematical Society, 1988.

13 K. Kearnes, P. Marković, and R. McKenzie. Optimal strong Mal'cev conditions for omitting type 1 in locally finite varieties. *Algebra Universalis*, 72(1):91–100, 2014. doi:10.1007/s00012-014-0289-9.

14 O. Klíma, P. Tesson, and D. Thérien. Dichotomies in the complexity of solving systems of equations over finite semigroups. *Theory Comput. Syst.*, 40(3):263–297, 2007. doi:10.1007/s00224-005-1279-2.

15 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. doi:10.1142/S0218196706003116.

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

17 M. Siggers. A strong Mal'cev condition for locally finite varieties omitting the unary type. *Algebra Universalis*, 64(1-2):15–20, 2010. doi:10.1007/s00012-010-0082-3.

18 D. Zhuk. A proof of CSP dichotomy conjecture. In Chris Umans, editor, *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 331–342. IEEE Computer Society, 2017. doi:10.1109/FOCS.2017.38.