Hardness Results for the Subpower Membership Problem

by

Jeffrey Alan Shriner

B.A., Hope College, 2007

M.S., Purdue University Fort Wayne, 2010

A thesis submitted to the

Faculty of the Graduate School of the

University of Colorado in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

Department of Mathematics

2018

This thesis entitled:
Hardness Results for the Subpower Membership Problem
written by Jeffrey Alan Shriner
has been approved for the Department of Mathematics

_____

Professor Ágnes Szendrei

_____

Assistant Professor Peter Mayr

Date _____

The final copy of this thesis has been examined by the signatories, and we find that both the content and the form meet acceptable presentation standards of scholarly work in the above mentioned discipline.

Shriner, Jeffrey Alan (Ph.D., Mathematics)

Hardness Results for the Subpower Membership Problem

Thesis directed by Professor Ágnes Szendrei

We first provide an example of a finite algebra with a Taylor term whose subpower membership problem is NP-hard. We then prove that for any consistent strong linear Maltsev condition $\mathcal{M}$ which does not imply the existence of a cube term, there exists a finite algebra satisfying $\mathcal{M}$ whose subpower membership problem is EXPTIME-complete. We characterize consistent strong linear Maltsev conditions which do not imply the existence of a cube term, and show as a corollary that there are finite algebras which generate congruence distributive and congruence k-permutable ($k \geq 3$) varieties whose subpower membership problem is EXPTIME-complete. Finally, we show that the spectrum of complexities of the problems SMP($\mathbb{A}$) for finite algebras $\mathbb{A}$ in varieties which are congruence distributive and congruence k-permutable ($k \geq 3$) is fuller than P and EXPTIME-complete by giving examples of finite algebras in such a variety whose subpower membership problems are NP-complete and PSPACE-complete, respectively.

Dedication

For Kinsi and Luella. Kinsi, your support of me is humbling, and I can't wait for our future adventures! Luella, I strive to be as creative as you are.

Acknowledgements

I thank my advisor, Prof. Ágnes Szendrei, for her extreme patience and investment in me, and for her invaluable guidance in producing the work in this thesis. I have grown tremendously through our discussions and observing her approach, and I am honored to have had the opportunity to work with her. I would also like to thank Peter Mayr for his feedback in response to my talks, for offering helpful suggestions for improvements, and for his careful reading of this thesis. I am grateful to my thesis committee for their time and involvement.

To the members of MATH 366: thank you for your willingness to engage and for your friendship.

This material is based upon work supported by the National Science Foundation under Grant No. DMS 1500254.

Contents

Tables

Table

Figures

Figure

Chapter 1

Introduction

In 2007 [27], Ross Willard posed the **subpower membership problem**, which is a combinatorial decision problem involvling computations in **algebraic structures**. An **algebraic structure**, briefly **algebra**, $\mathbb{A}$ is a nonempty set of elements A along with a set of operations defined on A. For example, groups, rings, and fields are all algebras. A **subalgebra** $\mathbb{B}$ **of** $\mathbb{A}$ is an algebra whose element set is a subset B of A, and whose operations are the operations of $\mathbb{A}$ restricted to the elements in B. For example, a subgroup of a group is a subalgebra. For a fixed integer m, the m^{th} **direct power of** $\mathbb{A}$ is the algebra $\mathbb{A}^m$ whose element set consists of the m-tuples of A, and whose operations are the operations of $\mathbb{A}$ defined coordinate-wise.

A space-efficient way to represent a subalgebra is by using generators. Thus, given an element b and generators $a_1, \ldots, a_n$, deciding whether b is a member of the subalgebra $\langle a_1, \ldots, a_n \rangle$ generated by $a_1, \ldots, a_n$ is an important problem in computational algebra. For a fixed finite algebra $\mathbb{A}$, the question of whether a given element $b \in \mathbb{A}^m$ is generated by generators $a_1, \ldots, a_n \in \mathbb{A}^m$ is precisely the subpower membership problem for $\mathbb{A}$, denoted SMP($\mathbb{A}$).

We are interested in analyzing the time complexity of the subpower membership problem for a fixed finite algebra $\mathbb{A}$. Assuming the input consists of n generators $a_1, \ldots, a_n$ and one distinguished element b in the m^{th} direct power of $\mathbb{A}$, the time complexity of this problem is measured with respect to the input size $(n+1)m$. A naive algorithm can compute the answer to this problem by computing the full subalgebra $\langle a_1, \ldots, a_n \rangle$, and checking if b is a member. Since the size of a subalgebra is bounded by $|A|^m$, this computation can be done in exponential time with respect to

the input size $(n+1)m$ (i.e., the problem is in the complexity class EXPTIME). M. Kozik [17] provided an example which shows this problem can be as hard as possible (EXPTIME-complete).

We know many cases in which this problem can be answered in polynomial time with respect to the input size (i.e., the problem is in the complexity class P). For example, if $\mathbb{A}$ is a finite dimensional vector space over a finite field, then SMP($\mathbb{A}$) is solved in polynomial time by using Gaussian elimination. Other examples where SMP($\mathbb{A}$) can be shown to be in P include when $\mathbb{A}$ is a finite group [9], finite ring [27], or finite lattice (using the Baker–Pixley theorem [1]).

The examples of algebras $\mathbb{A}$ listed above for which SMP($\mathbb{A}$) is in P all have an **m-cube term** for some integer $m \geq 2$. An m-cube term is an operation satisfying a particular list of m identities (which will be defined in Section 2.6). For example, groups have a 2-cube term $c(x,y,z) = xy^{-1}z$ which satisfies the identities

$$c(y,y,x) \approx x \text{ and}$$
$$c(x,y,y) \approx x,$$

and lattices have a 3-cube term $c(x,y,z) = (x \vee y) \wedge (x \vee z) \wedge (y \vee z)$ which satisfies the identities

$$c(y,y,x) \approx y,$$
$$c(y,x,y) \approx y, \text{ and}$$
$$c(x,y,y) \approx y.$$

The following has been conjectured:

Conjecture 1.1. *The decision problem* SMP($\mathbb{A}$) *is in* P *for all finite algebras* $\mathbb{A}$ *which have an* m*-cube term for some integer* $m \geq 2$*.*

The conjecture is known to be true for some classes of algebras [4, 18], but is unknown in general. The answer to this conjecture has applications in computer science. For example, there are applications to the constraint satisfaction problem (CSP) [13] and problems on learnability [6, 13]. First, we describe applications to the CSP. An instance of the CSP consists of a finite set of variables,

a finite set of elements (the domain), and a finite set of constraints. A **constraint** consists of an m-tuple of variables along with an m-ary relation R over the domain for some positive integer m. The task is then to determine whether we can assign the variables values from the domain such that, under this assignment, every constraint is satisfied; that is, whenever the tuple of variables from a constraint are assigned their respective values of the domain, the result is a tuple which belongs to the constraint relation. Since relations over the domain are part of the input, it matters how they are represented when considering computational complexity. If the constraint relations are subalgebras of powers of a finite algebra $\mathbb{A}$, then we may represent the relations using generators, as opposed to listing every member. Checking whether a proposed solution satisfies a constraint is an instance of the subpower membership problem for the algebra $\mathbb{A}$.

Now we describe applications to learnability. A **concept** c is a subset of the set of all finitary tuples over a fixed finite set A. A **concept class** C is a set of concepts, and is said to be **polynomially evaluable** if there is a polynomial-time algorithm which, given a concept c from C and any finitary tuple b over A, determines if b is in c. This is a highly desired property in computational learning theory. When C is taken to be all finitary relations over A which are subalgebras of powers of a finite algebra $\mathbb{A}$ and relations c of C are represented by generating sets [6], checking whether C is polynomially evaluable is multiple instances of the subpower membership problem for the algebra $\mathbb{A}$.

In this thesis, we provide hardness results for the subpower membership problem. An **m-cube term** (see Example 2.3) is a specific example of a **Taylor term** (see Example 2.2). We first construct an example of a finite algebra $\mathbb{A}$ with a Taylor term for which SMP($\mathbb{A}$) is NP-hard by reducing a known NP-complete problem (POSITIVE $1,3$-SAT [11]) to SMP($\mathbb{A}$). We then provide examples of finite algebras with more structure whose subpower membership problem is EXPTIME-complete by proving a more general hardness result, which makes use of previous hardness results for the subpower membership problem. We now briefly describe this general hardness result.

The existence of an m-cube term for some integer $m \geq 2$ is an example of a **strong linear Maltsev condition**, which is a condition requiring the existence of finitely many terms that satisfy

a given finite set of identities. These have proven useful in characterizing important structural properties of algebras and varieties. For example, there is a Maltsev condition, weaker than the existence of an m-cube term, which characterizes varieties for which each member's congruence lattice is modular [7]. The main result of this thesis is that if a consistent strong linear Maltsev condition $\mathcal{M}$ does not imply the existence of an m-cube term for any $m \geq 2$, then for any finite algebra $\mathbb{A}$, there exists a finite algebra $\mathbb{A}_{\mathcal{M}}$ such that $\mathbb{A}_{\mathcal{M}}$ satisfies the Maltsev condition $\mathcal{M}$ and SMP($\mathbb{A}_{\mathcal{M}}$) is at least as hard as SMP($\mathbb{A}$). We will characterize consistent strong linear Maltsev conditions which do not imply the existence of an m-cube term for any $m \geq 2$. We will then apply these results to Kozik's algebra $\mathbb{B}$ [17] for which SMP($\mathbb{B}$) is EXPTIME-complete to construct a finite algebra $\mathbb{A}$ which generates a congruence distributive and congruence k-permutable ($k \geq 3$) variety for which SMP($\mathbb{A}$) is EXPTIME-complete. Though Conjecture 1.1 remains unresolved, this result suggests that the conjecture is focused on the correct class of finite algebras.

From the work of Bulatov, Kozik, Mayr, and Steindl [3, 26, 25], we know there exist examples of finite semigroups whose subpower membership problem is NP-complete and examples of finite semigroups whose subpower membership problem is PSPACE-complete. From the general hardness result described above, we can deduce that if we expand these semigroups to algebras that belong to certain 'nice' classes, the subpower membership problem for the expanded algebra is at least as hard as the subpower membership problem for the original algebra. It is natural to ask about the upper bound for the complexity of these problems. We provide an answer by showing that when we expand a finite algebra to belong to a congruence 3-permutable and congruence 3-distributive variety, the subpower membership problem for the expanded algebra is no harder than the subpower membership problem for the original algebra.

Chapter 2

Preliminaries

In this chapter, we introduce the requisite definitions and notation for the results of Chapters 3, 4, and 5. For more details, see [24, 11, 5].

2.1 Complexity Theory

A decision problem is in the complexity class **P** (respectively, **EXPTIME**) if there is an algorithm which decides any instance in polynomial (respectively, exponential) time with respect to the size of the instance. A decision problem is in **NP** if any instance with a 'yes' answer is verifiable, given a certificate of proof, in polynomial time with respect to the size of the instance. A decision problem is in **PSPACE** if there is an algorithm which decides any instance in polynomial space with respect to the size of the instance, and is in **NPSPACE** if any instance with a 'yes' answer is verifiable in polynomial space with respect to the size of the instance. The following inclusions of complexity classes are well known:

$$\mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} = \mathrm{NPSPACE} \subseteq \mathrm{EXPTIME}$$

Whether or not the above inclusions are proper is unknown.

Given two decision problems Π_1 and Π_2, a **polynomial time many-one reduction** from Π_1 to Π_2 is a polynomial time algorithm for transforming any instance of Π_1 to a corresponding instance of Π_2 such that both instances have the same answer. If Π_1 has a polynomial time many-one reduction to Π_2, we also say Π_1 **has a polynomial time reduction to** Π_2, or Π_2 **is at**

least as hard as Π_1. The problem Π_2 is at least as hard as the problem Π_1 in the sense that an algorithmic solution to Π_2 provides an algorithmic solution to Π_1 of the same complexity. We say the decision problems Π_1 and Π_2 are **polynomial time equivalent** if Π_2 is at least as hard as Π_1, and Π_1 is at least as hard as Π_2.

Given a complexity class $\mathfrak{C}$, a decision problem is said to be **$\mathfrak{C}$-hard** if it is at least as hard as any other problem in $\mathfrak{C}$. A problem is **$\mathfrak{C}$-complete** if it is in $\mathfrak{C}$ and it is $\mathfrak{C}$-hard. Thus to show that a problem Π is $\mathfrak{C}$-complete, it suffices to show that Π is polynomial time equivalent to a known $\mathfrak{C}$-complete problem.

2.2 Algebras and the Subpower Membership Problem

For a nonempty set A we set $A^0 = \{\emptyset\}$, and for $n > 0$, we set A^n equal to the set of all n-tuples with elements from A. An **n-ary operation on** A is a map from A^n to A. An **algebraic language** is a family $\mathscr{F}$ of operation symbols for which each symbol $f \in \mathscr{F}$ is assigned a nonnegative integer n. We call n the **arity of** f, and say f is an n-ary operation symbol. An **algebra $\mathbb{A}$ in the language** $\mathscr{F}$ is an ordered pair $\langle A; \mathcal{F} \rangle$, where A is a nonempty set and $\mathcal{F}$ is a family of finitary operations on A indexed by the language $\mathscr{F}$; i.e., for each n-ary $f \in \mathscr{F}$, there is an n-ary operation $f^{\mathbb{A}} \in \mathcal{F}$ on A. An algebra $\mathbb{A}$ is **finite** if the underlying set A is finite, and is **trivial** if A has one element.

Let $\mathbb{A} = \langle A; \mathcal{F} \rangle$ be an algebra in the language $\mathscr{F}$. We will now define several related algebras in the language $\mathscr{F}$. A **subalgebra** $\mathbb{B}$ of $\mathbb{A}$ is an algebra whose element set is a subset B of A which is closed under the operations of $\mathbb{A}$, and for each $f \in \mathscr{F}$, $f^{\mathbb{B}}$ is defined to be $f^{\mathbb{A}}$ restricted to B. If $a_1, \ldots, a_n \in A$, we use $\langle a_1, \ldots, a_n \rangle$ to denote the smallest subalgebra of $\mathbb{A}$ which contains the elements $a_1, \ldots, a_n$, and call this subalgebra **the subalgebra generated by** $a_1, \ldots, a_n$. For a positive integer m, we define **the m^{th} direct power of** $\mathbb{A}$ to be the algebra $\mathbb{A}^m$ whose underlying set is A^m, and for each $f \in \mathscr{F}$, $f^{\mathbb{A}^m}$ is defined by computing $f^{\mathbb{A}}$ coordinate-wise.

For a fixed finite algebra $\mathbb{A}$, we define the **subpower membership problem for** $\mathbb{A}$ to be

the following combinatorial decision problem:

SMP($\mathbb{A}$)

Input: A positive integer m and m-tuples $a_1, \ldots, a_n, b \in \mathbb{A}^m$.

Question: Is b in the subalgebra $\langle a_1, \ldots, a_n \rangle$ of $\mathbb{A}^m$ generated by $a_1, \ldots, a_n$?

2.3 Compatible Relations and Congruences

For a set A, an **m-ary relation on** A is a subset of A^m. If f is an operation on A and R is an m-ary relation on A, we say R is **compatible** with f, or f **preserves** R, if R is a subalgebra of the m^{th} direct power of $\langle A; f \rangle$.

A **congruence** of an algebra $\mathbb{A} = \langle A; \mathcal{F} \rangle$ is an equivalence relation on A which is compatible with every operation in $\mathcal{F}$. The set of all congruences of $\mathbb{A}$ is denoted $\mathrm{Con}(\mathbb{A})$, and forms a lattice $\langle \mathrm{Con}(\mathbb{A}); \{\wedge, \vee\} \rangle$. The compatibility property of a congruence θ allows us to form a **quotient algebra** on the set of equivalence classes of θ. The lattice structure of $\mathrm{Con}(\mathbb{A})$ can also be of use in determining properties of the algebra $\mathbb{A}$, as we will see below (Examples 2.4 and 2.5).

2.4 Terms, Identities, and Varieties

Let $V = \{v_1, v_2, \ldots\}$ be a countably infinite set of distinct variables. For an algebraic language $\mathscr{F}$ and an initial segment $X \subseteq V$, a **term in the language $\mathscr{F}$ over** X, briefly a **term**, is defined by recursion:

(i) Every variable in X and every 0-ary operation symbol in $\mathscr{F}$ is a term.

(ii) If $p_1, \ldots, p_n$ are terms and f is an n-ary operation symbol in $\mathscr{F}$, then $f(p_1, \ldots, p_n)$ is a term.

We write $t(v_1, \ldots, v_n)$ to indicate that the variables which appear in the term t are among $v_1, \ldots, v_n$. If v_i appears in the term t, we say t **depends on** v_i. For any algebra $\mathbb{A}$ in the language $\mathscr{F}$ and any term t in the language $\mathscr{F}$ over X, the operation $t^{\mathbb{A}}$ is called a **term operation**. We note here that

for any algebra $\mathbb{A}$, there is a connection between generated subalgebras of $\mathbb{A}$ and term operations of $\mathbb{A}$. Specifically, $b \in \langle a_1, \ldots, a_n \rangle$ if and only if $b = t^{\mathbb{A}}(a_1, \ldots, a_n)$ for some n-ary term t.

It will be useful for us to visualize a term by its **term tree**. We use the convention that the leaves of the tree are labeled by variables, and every node which is not a leaf is labeled by a single operation symbol. An example in the language f (unary), g (unary), and t (binary) is given in Figure 2.1. The **height** of a vertex is the number of edges in the longest path from that vertex

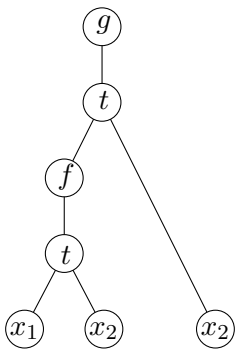

Figure 2.1: The term tree $\mathfrak{T}_r$ for the term $r(x_1, x_2) = g(t(f(t(x_1, x_2)), x_2))$.

to a leaf. We refer to the vertex of maximum height in this tree as the **root**, and denote the term tree of a term r by $\mathfrak{T}_r$. For any term r in an algebraic language $\mathscr{F}$, we define the **size of** r to be the number of vertices in $\mathfrak{T}_r$ which are labeled by operation symbols from $\mathscr{F}$.

An **identity in the language** $\mathscr{F}$ **over** X is any expression of the form $p \approx q$, where p and q are terms in the language $\mathscr{F}$ over X. Note we may always write $p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n)$, where p and q do not necessarily depend on every variable $x_1, \ldots, x_n$. An algebra $\mathbb{A}$ in the language $\mathscr{F}$ **satisfies** $p \approx q$ if $p^{\mathbb{A}}(a_1, \ldots, a_n) = q^{\mathbb{A}}(a_1, \ldots, a_n)$ for every choice $(a_1, \ldots, a_n) \in A^n$.

If Σ is a set of identities in the language $\mathscr{F}$, we may consider the class $\mathcal{V}$ of all algebras which satisfy every identity of Σ. We call $\mathcal{V}$ **the variety determined by** Σ.

Example 2.1 (Groups)**.** Let Σ be the following set of identities in the language $\{+, -, 0\}$, where

$+$ is binary, $-$ is unary, and 0 is nullary:

$$x + (y + z) \approx (x + y) + z$$

$$x + 0 \approx 0 + x \approx x$$

$$x + -(x) \approx -(x) + x \approx 0.$$

The variety $\mathcal{G}$ determined by Σ is the variety of groups. The variety $\mathcal{A}$ determined by $\Sigma \cup \{x + y \approx y + x\}$ is the variety of Abelian groups.

For a fixed algebra $\mathbb{A}$, the **variety generated by** $\mathbb{A}$ is the variety determined by all identities satisfied by $\mathbb{A}$. We denote this variety by $\mathcal{V}(\mathbb{A})$.

2.5 Linear Identities and Kelly's Completeness Theorem

For a fixed algebraic language, a term in that language is called **linear** if it contains at most one operation symbol, and an identity $s \approx t$ is called **linear** if both s and t are linear terms. If $\Sigma \cup \{\phi\}$ is a set of linear identites, then ϕ is a **consequence** of Σ, written $\Sigma \models \phi$, if every model of Σ is a model of ϕ. David Kelly's Completeness Theorem [16, 15] characterizes the $\models$ relation using a simple proof system for linear identities, which we will now describe.

If Σ is a set of linear identities over the variable set X, the **weak closure of Σ in the variables** X is the smallest set $\overline{\Sigma}$ of linear identities containing Σ for which the following properties hold:

(1) $u \approx u \in \overline{\Sigma}$ for all linear terms u with variables from X.

(2) If $u \approx v \in \overline{\Sigma}$, then $v \approx u \in \overline{\Sigma}$.

(3) If $u \approx v \in \overline{\Sigma}$ and $v \approx w \in \overline{\Sigma}$, then $u \approx w \in \overline{\Sigma}$.

(4) If $u \approx v \in \overline{\Sigma}$ and $\gamma : X \to X$ is a function, then $u[\gamma] \approx v[\gamma] \in \overline{\Sigma}$, where $u[\gamma]$ denotes the linear term obtained from u by replacing each variable $x \in X$ with $\gamma(x) \in X$.

We write $\Sigma \vdash_X \phi$ if $\phi \in \overline{\Sigma}$. Kelly's Completeness Theorem states that $\Sigma \models \phi$ if and only if $\Sigma \vdash_X \phi$ or $\Sigma \vdash_X x \approx y$ (for $x \neq y$), provided that X is **large enough** for $\Sigma \cup \{\phi\}$; that is,

- X contains at least 2 variables,
- $|X| \geq \text{arity}(f)$ for any operation symbol f occurring in Σ, and
- $|X|$ is at least as large as the number of distinct variables occurring in any identity in $\Sigma \cup \{\phi\}$.

If X and Y are variable sets both large enough for $\Sigma \cup \{\phi\}$, then Kelly's Completeness Theorem implies that $\Sigma \vdash_X \phi$ if and only if $\Sigma \vdash_Y \phi$. Thus, if $\Sigma \vdash_X \phi$ for some X which is large enough for $\Sigma \cup \{\phi\}$, we simply write $\Sigma \vdash \phi$ and say Σ **entails** ϕ. Accordingly, we will refer to properties (1) through (4) above as **entailment properties**.

We say Σ is **inconsistent** if Σ entails $x \approx y$ for distinct variables x and y. Using Kelly's Completeness Theorem, we see Σ is inconsistent if and only if the only models of Σ are the trivial (one element) algebras. If Σ is not inconsistent (or equivalently, has a non-trivial model), we say Σ is **consistent**.

2.6 Interpretability and Strong Maltsev Conditions

Let $\mathcal{V}$ and $\mathcal{W}$ be two varieties, and let $\{f_i\}_{i \in I}$ be the languange of $\mathcal{V}$. We say that $\mathcal{V}$ **is interpretable in** $\mathcal{W}$ if for every operation symbol f_i, there is a term t_i (of the same arity) in the language of $\mathcal{W}$ such that for all $\mathbb{A} \in \mathcal{W}$, the algebra $\langle A; \{t_i^{\mathbb{A}}\}_{i \in I} \rangle$ is a member of $\mathcal{V}$. If $\mathcal{V}$ is interpretable in $\mathcal{W}$, we write $\mathcal{V} \leq \mathcal{W}$. For example, if $\mathcal{G}$ is the variety of groups and $\mathcal{A}$ is the variety of Abelian groups, then $\mathcal{G} \leq \mathcal{A}$. The relation $\leq$ is a quasi-order, and by identifying varieties which interpret into each other, this becomes a partial order. This partial order forms a lattice known as the **lattice of interpretability types of varieties** [10].

Let $\mathcal{M} = (\mathcal{H}, \Sigma)$, where $\mathcal{H}$ is a finite set of operation symbols and Σ is a finite set of identities involving terms in the language $\mathcal{H}$. We denote the variety determined by Σ by $\mathcal{V}_{\mathcal{M}}$. For any variety

$\mathcal{V}$, $\mathcal{V}_{\mathcal{M}} \leq \mathcal{V}$ means that for every n-ary operation symbol $h \in \mathcal{H}$, there is a term $t_h(v_1, \ldots, v_n)$ in the language of $\mathcal{V}$ such that for all $\mathbb{A} \in \mathcal{V}$, the algebra $\langle A; \{t_h^{\mathbb{A}}\}_{h \in \mathcal{H}} \rangle$ satisfies the identities in Σ. In this case, we say $\mathcal{V}$ **satisfies** $\mathcal{M}$. We call a condition which requires the existence of term operations indexed by $\mathcal{H}$ which satisfy the identities of Σ a **strong Maltsev condition**. For notational convenience, we will represent a strong Maltsev condition by the pair $\mathcal{M} = (\mathcal{H}, \Sigma)$ with the existential condition being implied. If the existential statement is true in an algebra $\mathbb{A}$, we say $\mathbb{A}$ **satisfies** $\mathcal{M}$. A strong Maltsev condition is **linear** if all of the identities in Σ are linear, and a strong linear Maltsev condition is **consistent** if Σ is consistent.

We conclude this section with some important examples of strong linear Maltsev conditions.

Example 2.2 (Existence of a Taylor term)**.** We describe a strong linear Maltsev condition which is implied by any idempotent Maltsev condition that is not satisfied in every algebra [20]. A term t in the language of a variety $\mathcal{V}$ is a **Taylor term for** $\mathcal{V}$ if $\mathcal{V}$ satisfies that t is **idempotent** (i.e., $t(x, x, \ldots, x) \approx x$), and also satisfies a set of identities of the form

$$\begin{aligned} t(x, *, *, \ldots, *) &\approx t(y, *, *, \ldots, *), \\ t(*, x, *, \ldots, *) &\approx t(*, y, *, \ldots, *), \\ &\vdots \\ t(*, *, * \ldots, x) &\approx t(*, *, *, \ldots, y), \end{aligned}$$

where $*$ may be replaced with either x or y. An algebra $\mathbb{A}$ has a Taylor term if there is a term t in the language of $\mathbb{A}$ for which $\mathbb{A}$ satisfies a set of identities of the above form. M. Olšák [20] showed that the existence of a Taylor term is a strong linear Maltsev condition when he characterized varieties containing a Taylor term by the existence of an idempotent 6-ary term t for which every algebra in the variety satisfies the identitities

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

Example 2.3 (Existence of an m-cube term for fixed $m \geq 2$)**.** We describe a linear Maltsev condition which characterizes finite algebras with **few subpowers** [2]; that is, algebras for which

the cardinality of the set of subalgebras of $\mathbb{A}^n$ is exponential in n (as opposed to doubly exponential in n). Fix an integer $m \geq 2$. A term c in the language of a variety $\mathcal{V}$ is an **m-cube term for $\mathcal{V}$** if $\mathcal{V}$ satisfies a set of m identities given by the rows of

$$c\left(\begin{bmatrix} \\ x_1 \\ \\ \end{bmatrix}, \ldots, \begin{bmatrix} \\ x_n \\ \\ \end{bmatrix}\right) \approx \begin{bmatrix} y \\ \vdots \\ y \end{bmatrix},$$

where $x_1, \ldots, x_n \in \{x, y\}^m \setminus (y, \ldots, y)$. An algebra $\mathbb{A}$ has an m-cube term if there is a term c in the language of $\mathbb{A}$ for which $\mathbb{A}$ satisfies a set of m identities of the above form. It was shown in [2] that the finite algebras with few subpowers are precisely the finite algebras which contain an m-cube term for some $m \geq 2$. We refer to the above identities as **a set of m cube identities for c**. If the integer m is clear from context or irrelevant, then we may say more briefly that c is a **cube term** for $\mathcal{V}$ or $\mathbb{A}$.

For example, the variety of groups has a cube term since the term $c(x, y, z) = xy^{-1}z$ satisfies the identites given by the rows of

$$c\begin{pmatrix} x & x & y \\ y & x & x \end{pmatrix} \approx \begin{bmatrix} y \\ y \end{bmatrix},$$

and the variety of lattices has a cube term since the term $c(x, y, z) = (x \vee y) \wedge (x \vee z) \wedge (y \vee z)$ satisfies the identities given by the rows of

$$c\begin{pmatrix} x & y & y \\ y & x & y \\ y & y & x \end{pmatrix} \approx \begin{bmatrix} y \\ y \\ y \end{bmatrix}.$$

Example 2.4 (Strong Maltsev condition for congruence k-distributivity)**.** For an algebra $\mathbb{A}$, the lattice $\langle \mathrm{Con}(\mathbb{A}); \{\wedge, \vee\} \rangle$ satisfies the **distributive law** if for all congruences $\theta_1, \theta_2, \theta_3 \in \mathrm{Con}(\mathbb{A})$,

$$\theta_1 \vee (\theta_2 \wedge \theta_3) = (\theta_1 \vee \theta_2) \wedge (\theta_1 \vee \theta_3).$$

If an algebra's congruence lattice satisfies the distributive law, we say the algebra is **congruence distributive**. We say a variety $\mathcal{V}$ is **congruence distributive** if every algebra in $\mathcal{V}$ is congruence

distributive. B. Jónsson [14] characterized congruence distributive varieties by the existence of ternary terms $d_0, \ldots, d_k$ (for some $k \geq 1$) for which every algebra in the variety satisfies the following set of identities:

$$\begin{aligned}
&d_0(x,y,z) \approx x,\\
&d_k(x,y,z) \approx z,\\
&d_i(x,y,x) \approx x \text{ for all } 0 \leq i \leq k,\\
&d_i(x,x,y) \approx d_{i+1}(x,x,y) \text{ for all even } i, \text{ and}\\
&d_i(x,y,y) \approx d_{i+1}(x,y,y) \text{ for all odd } i.
\end{aligned}$$

The terms $d_0, \ldots, d_k$ are referred to as **Jónsson terms**, and $\mathrm{CD}(k)$ is often used to refer to the class of algebras which have Jónsson terms $d_0, \ldots, d_k$. Note that the sequence of classes $\mathrm{CD}(k)$ is an increasing sequence; that is, if $\mathbb{A}$ is a member of $\mathrm{CD}(k)$, $\mathbb{A}$ is also a member of $\mathrm{CD}(\ell)$ for all $\ell > k$.

Example 2.5 (Strong Maltsev condition for congruence k-permutability)**.** For an algebra $\mathbb{A}$ and congruences $\theta_1, \theta_2 \in \mathrm{Con}(\mathbb{A})$, the **relational product** of θ_1 and θ_2 is the binary relation $\theta_1 \circ \theta_2$ defined by

$$(a,b) \in \theta_1 \circ \theta_2 \iff \text{there exists a } c \text{ such that } (a,c) \in \theta_1 \text{ and } (c,b) \in \theta_2.$$

The **k-fold relational product** is defined as

$$\theta_1 \circ_k \theta_2 = \theta_1 \circ \theta_2 \circ \theta_1 \circ \ldots,$$

where there are $k-1$ occurrences of $\circ$ on the right hand side. An algebra $\mathbb{A}$ is said to be **congruence k-permutable** if for every $\theta_1, \theta_2 \in \mathrm{Con}(\mathbb{A})$,

$$\theta_1 \circ_k \theta_2 = \theta_2 \circ_k \theta_1.$$

We say a variety $\mathcal{V}$ is **congruence k-permutable** if every algebra in $\mathcal{V}$ is congruence k-permutable. J. Hagemann and A. Mitschke [12] characterized congruence k-permutable varieties by the existence

of ternary terms $p_0, \ldots, p_k$ for which every algebra in the variety satisfies the following set of identities:

$$p_0(x, y, z) \approx x,$$

$$p_k(x, y, z) \approx z, \text{ and}$$

$$p_i(x, x, y) \approx p_{i+1}(x, y, y) \text{ for all } i.$$

The terms $p_0, \ldots, p_k$ are referred to as **Hagemann–Mitschke terms**, and CP(k) is often used to refer to the class of algebras which have $k+1$ Hagemann–Mitschke terms $p_0, \ldots, p_k$. We note that the sequence of classes CP(k) is also an increasing sequence.

2.7 Structure of this thesis

In Chapter 3, we construct a finite algebra $\mathbb{A}$ with a binary Taylor term such that SMP($\mathbb{A}$) is NP-hard by reducing a known NP-complete problem (POSITIVE 1, 3-SAT [11]) to SMP($\mathbb{A}$). The existence of a Taylor term is an example of a consistent strong linear Maltsev condition which does not imply the existence of a cube term.

In Chapter 4, we prove Theorem 4.1 which claims that the above mentioned property of a consistent strong linear Maltsev condition $\mathcal{M}$ is sufficient to construct, from any finite algebra $\mathbb{A}$, a new finite algebra $\mathbb{A}_{\mathcal{M}}$ which satisfies $\mathcal{M}$ such that SMP($\mathbb{A}_{\mathcal{M}}$) is at least as hard as SMP($\mathbb{A}$). We will also characterize consistent strong linear Maltsev conditions which do not imply the existence of a cube term in Corollary 4.4. We use this characterization along with Theorem 4.1 to show that there exist examples of finite algebras $\mathbb{A}$ which generate congruence distributive and congruence k-permutable ($k \geq 3$) varieties for which SMP($\mathbb{A}$) is EXPTIME-complete.

Finally, in Chapter 5, we show that we can expand a finite algebra to belong to varieties which are congruence distributive and congruence k-permutable ($k \geq 3$) so that the subpower membership problem for the original algebra is polynomial time equivalent to the subpower membership problem for the expanded algebra. As a consequence, we show that the spectrum of complexities of the problems SMP($\mathbb{A}$) for finite algebras $\mathbb{A}$ in varieties which are congruence distributive and congruence

k-permutable ($k \geq 3$) is fuller than P and EXPTIME-complete by giving examples of finite algebras in such a variety whose subpower membership problems are NP-complete and PSPACE-complete, respectively.

Chapter 3

The SMP and algebras with a Taylor term

In this chapter, we will construct a finite algebra $\mathbb{A}$ with a Taylor term such that SMP($\mathbb{A}$) is NP-hard by reducing a known NP-complete problem (POSITIVE 1, 3-SAT [11]) to SMP($\mathbb{A}$). Several computations were made using the Universal Algebra Calculator [8] to gain intuition during the initial phases of constructing this example.

Let $\mathbb{A} = \langle A; \mathcal{F} \rangle$ be the algebra with element set

$$A = \{0, 1, 2, 3, c_1, c_2, c_3, c_{1,2}, c_{1,3}, c_{2,3}, c_{2,1}, c_{3,1}, c_{3,2}, d_{1,2}, d_{1,3}, d_{2,3}, e_1, e_2, e_3, e, a\},$$

and set of operations

$$\mathcal{F} = \{+^{\mathbb{A}}, f^{\mathbb{A}}, g^{\mathbb{A}}\}.$$

The operation $f^{\mathbb{A}}$ is unary such that

$$f^{\mathbb{A}}(i) = \begin{cases} c_i & \text{if } i \in \{1, 2, 3\}, \\ 0 & \text{if } i = 0, \\ a & \text{otherwise,} \end{cases}$$

and g is unary such that

$$g^{\mathbb{A}}(x) = \begin{cases} e & \text{if } x \in \{e_1, e_2, e_3\}, \\ a & \text{otherwise.} \end{cases}$$

We want $\mathbb{A}$ to have a Taylor term, which will be accomplished with the operation $+^{\mathbb{A}}$. The symmetric binary operation $+^{\mathbb{A}}$ is given in Table 3.1 (since $+^{\mathbb{A}}$ is symmetric, we only include the

upper diagonal of the table). Note that since $+^{\mathbb{A}}$ is idempotent and symmetric, it follows that $+$ is a Taylor term for $\mathbb{A}$. We will typically omit the superscript from operation symbols since the algebra we are computing in will be clear from context. We will assume terms are evaluated from left to right if no parentheses are given.

The intuition behind the definitions of the operations f, g, and $+$ is that an element $x \in A \setminus \{0, 1, 2, 3, a\}$ encodes a 'simplest' usage of elements in $\{1, 2, 3\}$ and operations in $\{f, g, +\}$ to generate x:

- The elements c_i are generated by $f(i)$.
- The elements $c_{i,j}$ are generated by $f(i) + j$.
- The elements $d_{i,j}$ are generated by $i + j$.
- The elements e_i are generated by applying f to i and adding the remaining non-zero elements, such as $f(i) + j + k$, where $\{i, j, k\} = \{1, 2, 3\}$.
- The element e is generated by applying f to exactly one element in $\{1, 2, 3\}$, adding the remaining non-zero elements, then applying g. For example, $e = g(f(i) + j + k)$, where $\{i, j, k\} = \{1, 2, 3\}$.

The element a acts as an absorbing element with respect to the operations; that is,

- $a + * = * + a = a$ for every element $*$,
- $f(a) = a$, and
- $g(a) = a$.

We will show the following:

Theorem 3.1. *The decision problem* SMP($\mathbb{A}$) *is* NP*-hard.*

$+^{\mathbb{A}}$	0	1	2	3	c_1	c_2	c_3	$c_{1,2}$	$c_{1,3}$	$c_{2,3}$	$c_{2,1}$	$c_{3,1}$	$c_{3,2}$	$d_{1,2}$	$d_{1,3}$	$d_{2,3}$	e_1	e_2	e_3	e	a
0	0	1	2	3	c_1	c_2	c_3	$c_{1,2}$	$c_{1,3}$	$c_{2,3}$	$c_{2,1}$	$c_{3,1}$	$c_{3,2}$	$d_{1,2}$	$d_{1,3}$	$d_{2,3}$	e_1	e_2	e_3	e	a
1		1	$d_{1,2}$	$d_{1,3}$	a	$c_{2,1}$	$c_{3,1}$	a	a	e_2	a	a	e_3	a	a	a	a	a	a	a	a
2			2	$d_{2,3}$	$c_{1,2}$	a	$c_{3,2}$	a	e_1	a	a	e_3	a	a	a	a	a	a	a	a	a
3				3	$c_{1,3}$	$c_{2,3}$	a	e_1	a	a	e_2	a	a	a	a	a	a	a	a	a	a
c_1					c_1	a	a	a	a	a	a	a	a	a	a	e_1	a	a	a	a	a
c_2						c_2	a	a	a	a	a	a	a	a	e_2	a	a	a	a	a	a
c_3							c_3	a	a	a	a	a	a	e_3	a	a	a	a	a	a	a
$c_{1,2}$								$c_{1,2}$	a	a	a	a	a	a	a	a	a	a	a	a	a
$c_{1,3}$									$c_{1,3}$	a	a	a	a	a	a	a	a	a	a	a	a
$c_{2,3}$										$c_{2,3}$	a	a	a	a	a	a	a	a	a	a	a
$c_{2,1}$											$c_{2,1}$	a	a	a	a	a	a	a	a	a	a
$c_{3,1}$												$c_{3,1}$	a	a	a	a	a	a	a	a	a
$c_{3,2}$													$c_{3,2}$	a	a	a	a	a	a	a	a
$d_{1,2}$														$d_{1,2}$	a	a	a	a	a	a	a
$d_{1,3}$															$d_{1,3}$	a	a	a	a	a	a
$d_{2,3}$																$d_{2,3}$	a	a	a	a	a
e_1																	e_1	a	a	a	a
e_2																		e_2	a	a	a
e_3																			e_3	a	a
e																				e	a
a																					a

Table 3.1: The operation table for the binary operation $+^{\mathbb{A}}$.

We will prove Theorem 3.1 by reducing a known NP-complete problem to SMP($\mathbb{A}$). The known NP-complete problem we will use is POSITIVE 1, 3-SAT [11]:

POSITIVE $1, 3$**-SAT**

Input: A set X of variables and a collection $C_1, \ldots, C_m$ of clauses over X such that $|C_i| = 3$ for all i and no clause contains a negated literal.

Question: Is there a truth assignment for X such that each clause has exactly one true literal?

To prove Theorem 3.1, we must show that for every instance of POSITIVE 1, 3-SAT, we can construct a corresponding instance of SMP($\mathbb{A}$) in polynomial time which has a 'yes' answer if and only if the POSITIVE 1, 3-SAT instance has a 'yes' answer. We will argue this in two parts:

(1) Given a fixed instance of POSITIVE 1, 3-SAT, we will construct a corresponding instance of SMP($\mathbb{A}$), and show the construction can be done in polynomial time. We will then show that if the instance of POSITIVE 1, 3-SAT has a satisfying truth assignment, then the corresponding instance of SMP($\mathbb{A}$) has a 'yes' answer.

(2) We will show that if the corresponding instance of SMP($\mathbb{A}$) has a 'yes' answer, then the instance of POSITIVE 1, 3-SAT has a satisfying truth assignment.

Fix an instance $C_1, \ldots, C_m$ of POSITIVE 1, 3-SAT over the variables $\{x_1, \ldots, x_n\}$. To show part (1), for each C_i, fix an ordering of the three variables in C_i and label them 1 through 3. We then create the instance of SMP($\mathbb{A}$)

$$a_0, \ldots, a_n, b \in \mathbb{A}^m,$$

where a_j^i, $1 \leq j \leq n$, $1 \leq i \leq m$, is the label of the variable x_j in C_i if one exists, and 0 otherwise. We set $a_0 = (0, \ldots, 0)$ and $b = (e, \ldots, e)$. We include a_0 for technical reasons.

In constructing the instance of SMP($\mathbb{A}$), we run over $C_1, \ldots, C_m$ once to label the variables, and n times to create the generators $a_1, \ldots, a_n$. We can write down a_0 and b in m steps each, so the reduction requires $\mathcal{O}((n+3)m)$ steps. Since $m \leq \binom{n}{3}$, we can produce the instance of SMP($\mathbb{A}$) in polynomial time with respect to the input size (at least n) of POSITIVE 1, 3-SAT.

Now suppose the instance of POSITIVE 1, 3-SAT is satisfiable, and let $x_{i_1}, \ldots, x_{i_k}$ be the variables assigned FALSE and $x_{i_{k+1}}, \ldots, x_{i_n}$ be the variables assigned TRUE in a satisfying assignment. Then we claim

$$p(a_0, \ldots, a_n) := g(a_{i_1} + \cdots + a_{i_k} + f(a_{i_{k+1}} + \cdots + a_{i_n})) = b. \qquad (\dagger)$$

Indeed, fix a coordinate $1 \leq i \leq m$, and let $x_{t_1}, x_{t_2}, x_{t_3}$ be the variables used in clause C_i. Then $\{a_{t_1}^i, a_{t_2}^i, a_{t_3}^i\} = \{1, 2, 3\}$ and all other generators are 0 in the i^{th} coordinate. Since we have a satisfying truth assignment, exactly one argument of f is non-zero (say $a_{t_3}^i$), and exactly two arguments outside of f are non-zero ($a_{t_1}^i$ and $a_{t_2}^i$). Since 0 is an additive identity with respect to

+, we have

$$\begin{aligned} p(a_0, \ldots, a_n)|_i &= g(a^i_{t_1} + a^i_{t_2} + f(a^i_{t_3})) \\ &= g(d_{a^i_{t_1}, a^i_{t_2}} + c_{a^i_{t_3}}) \\ &= g(e_{a^i_{t_3}}) \\ &= e. \end{aligned}$$

Thus, $p(a_0, \ldots, a_n) = b$, so $b \in \langle a_0, \ldots, a_n \rangle$. This completes part (1).

We will complete part (2) by showing that if $b \in \langle a_0, \ldots, a_n \rangle$ in the corresponding instance of SMP($\mathbb{A}$), then the instance of POSITIVE 1, 3-SAT has a satisfying truth assignment (and thus complete the proof of Theorem 3.1). We will do this by proving the following theorem:

Theorem 3.2. *Let $C_1, \ldots, C_m$ be an instance of* POSITIVE 1,3-SAT *over the variable set $\{x_1, \ldots, x_n\}$, and let $a_0, \ldots, a_n, b \in \mathbb{A}^m$ be the corresponding instance of* SMP($\mathbb{A}$). *If $b \in \langle a_0, \ldots, a_n \rangle$, then there exists a term $p(x_0, \ldots, x_n)$ such that*

(1) *$p(a_0, \ldots, a_n) = b$,*

(2) *each variable $x_1, \ldots, x_n$ labels exactly one leaf in the term tree of p, and*

(3) *for all $1 \leq i \leq m$, exactly one variable in C_i belongs to a subterm of p whose root is f.*

Hence, assigning a variable TRUE if and only if it belongs to a subterm of p whose root is f is a satisfying assignment for the instance $C_1, \ldots, C_m$ of POSITIVE 1,3-SAT.

Fix an instance $C_1, \ldots, C_m$ of POSITIVE 1, 3-SAT over the variable set $\{x_1, \ldots, x_n\}$ such that the corresponding instance $a_0, \ldots, a_n \in \mathbb{A}^m$ of SMP($\mathbb{A}$) has a 'yes' answer. We spend the remainder of this chapter proving Theorem 3.2. Toward this goal, we introduce some notation and terminology.

For any term $r(x_0, \ldots, x_n)$, we recall that the term tree of r is denoted by $\mathfrak{T}_r$. We use $\overline{\mathfrak{T}}_r$ to denote the isomorphic tree in which the leaf in $\mathfrak{T}_r$ labeled x_j is labeled a_j, and $\overline{\mathfrak{T}}^i_r$, $1 \leq i \leq m$, to

denote the isomorphic tree in which the leaf in $\mathfrak{T}_r$ labeled x_j is labeled a_j^i. In $\overline{\mathfrak{T}}_r^i$, if a leaf is labeled a_j^i we say that leaf **has color** a_j^i.

Definition 3.3. Let $r(x_0, \ldots, x_n)$ be any term.

(a) The **conflict of** r **in the** i^{th} **coordinate** is the number of leaves of $\overline{\mathfrak{T}}_r^i$ with color in $\{1, 2, 3\}$. We denote this number by $c_i(r)$.

(b) The **conflict of** r is the number $\mathcal{C}(r) := \max\limits_{1 \leq i \leq m} c_i(r)$.

Definition 3.4. A term is an f**-term** if it has the form $f\left(\sum_{i=1}^{w} x_{k_i}\right)$ and $\mathcal{C}\left(\sum_{i=1}^{w} x_{k_i}\right) = 1$. A term is in f**-form** if it is a g-free term, and every subterm whose root is f is an f-term.

We will make frequent use of the following proposition:

Proposition 3.5. *Let $r(x_0, \ldots, x_n)$ be a g-free term.*

(1) *If r is in f-form and $\mathcal{C}(r) > 1$, then the root of $\mathfrak{T}_r$ is $+$.*

(2) *If $\mathcal{C}(r) = 1$ and $r(x_0, \ldots, x_n) = f(r'(x_0, \ldots, x_n))$ where r' is an f-free subterm, then there exists an f-term $\hat{r}(x_0, \ldots, x_n)$ such that $r(a_0, \ldots, a_n) = \hat{r}(a_0, \ldots, a_n)$.*

Proof. For (1), we prove the contrapositive statement. If r is in f-form and the root of $\mathfrak{T}_r$ is f, then by definition r is an f-term, so $\mathcal{C}(r) = 1$.

For (2), let $\mathscr{L}$ be the set of leaves of $\mathfrak{T}_{r'}$ (or equivalently, of $\mathfrak{T}_r$) and $\overline{\mathscr{L}}$ the corresponding set of leaves of $\overline{\mathfrak{T}}_{r'}$ (or equivalently, of $\overline{\mathfrak{T}}_r$). Consider the f-term $f\left(\sum_{\ell \in \mathscr{L}} \text{label}(\ell)\right)$. If $c_i(r) = 0$, then every label of $\overline{\mathfrak{T}}_r^i$ is 0, so

$$f(r'(a_0, \ldots, a_n))|_i = 0 = f\left(\sum_{\ell \in \overline{\mathscr{L}}} \text{label}(\ell)\right)\Big|_i.$$

If $c_i(r) = 1$, let x be the non-zero label of a leaf in $\overline{\mathfrak{T}}_r^i$. Then since 0 is an additive identity with respect to $+$, we have that

$$f(r'(a_0, \ldots, a_n))|_i = c_x = f\left(\sum_{\ell \in \overline{\mathscr{L}}} \text{label}(\ell)\right)\Big|_i.$$

Thus, the proof is complete by letting $\hat{r}(x_0, \ldots, x_n) = f\left(\sum_{\ell \in \mathscr{L}} \text{label}(\ell)\right)$. □

Recall that the element a acts as an absorbing element with respect to the operations. Thus since $b^i = e$ for all $1 \leq i \leq m$, if a term p satisfies $p(a_0, \ldots, a_n) = b$, then no subterm of p may evaluate to a in any coordinate. We will use this fact often.

We are assuming $b \in \langle a_0, \ldots, a_n \rangle$, so there is a term p such that $p(a_0, \ldots, a_n) = b$. We make the following two assumptions on the term p:

(1) The term p is the **shortest term of minimal conflict**, meaning that there is no term p' such that

- $p'(a_0, \ldots, a_n) = b$ and
- $|\mathfrak{T}_{p'}| + \sum_{i=1}^{m} c_i(p') < |\mathfrak{T}_p| + \sum_{i=1}^{m} c_i(p)$,

where $|\mathfrak{T}_r|$ is the size of r.

(2) Every subterm of p of the form $f(r'(x_0, \ldots, x_n))$ where the subterm r' is

- g-free, f-free, and
- satisfies $\mathcal{C}(r') = 1$

is an f-term.

Assumption (2) is valid since any subterm of p which satisfies the listed criteria may be replaced by an f-term which is equal on evaluation at $(a_0, \ldots, a_n)$ by Proposition 3.5(2).

We will show that the term p is the desired term of Theorem 3.2. We will do this in the following manner:

I. We establish in Lemma 3.6 that $p(x_0, \ldots, x_n) = g(s(x_0, \ldots, x_n))$, where s is a g-free subterm which evaluates to elements of the form e_* in every coordinate. The role of the operation g is only to 'normalize' the elements of the form e_*: the labeling of the variables in $\{1, 2, 3\}$ is random and is performed per clause. The same variable may have different non-zero labels in different clauses, so we cannot predict what the specific output will be in any

given coordinate. Thus, we need the operation g to 'accept' any output of the form e_*. After proving Lemma 3.6, the remainder of the work is to analyze the g-free term s.

II. We collect results (Lemma 3.7 – Corollary 3.9) which describe how the range (at the coordinate level) of a subterm r of s in f-form is connected to the non-zero labels present in $\overline{\mathfrak{T}}_r^i$.

III. We establish multiple properties about the term s, the most notable being

(a) the term s is in f-form (Lemma 3.17),

(b) the term s satisfies $c_i(s) = 3$ for all $1 \leq i \leq m$ (Corollary 3.20), and

(c) the non-zero labels of $\overline{\mathfrak{T}}_s^i$ are distinct for each $1 \leq i \leq m$ (Corollary 3.16).

We will then observe that (a), (b), (c), and Lemma 3.7 prove Theorem 3.2.

We note here that we do not actually argue that p has the exact form in (†). It is possible to deduce that p must have exactly one f-term as in (†), though this is not neccessary to obtain a satisfying assignment for our given instance of POSITIVE $1,3$-SAT.

Lemma 3.6. *The term p has the form $g(s(x_0, \ldots, x_n))$, where $s(x_0, \ldots, x_n)$ is a g-free subterm and $s(a_0, \ldots, a_n)|_i = e_{j_i}$ for some $j_i \in \{1, 2, 3\}$, for all $1 \leq i \leq m$.*

Proof. First, note that p cannot be a g-free term, since $a_0, \ldots, a_n \in \{0, 1, 2, 3\}^m$ and e is not generated by the operations f and $+$ on the domain $\{0, 1, 2, 3\}$. Now consider a subterm r of p whose root is a minimal occurrence of g in $\mathfrak{T}_p$ (with respect to height).

Since the range of g is $\{a, e\}$, we must have that r outputs e in each coordinate; that is, $r(a_0, \ldots, a_n) = b$. Since r is a subterm of p and p is the shortest term of minimal conflict which evaluates to b, we must have $p(x_0, \ldots, x_n) = r(x_0, \ldots, x_n) = g(s(x_0, \ldots, x_n))$. Since the root of r is a minimal occurrence of g, we have that s is a g-free subterm.

Further, $g(x) \neq a$ if and only if $x = e_j$ for some $j \in \{1, 2, 3\}$, so in fact $p(x_0, \ldots, x_n) = g(s(x_0, \ldots, x_n))$, where $s(a_0, \ldots, a_n)|_i = e_{j_i}$ for some $j_i \in \{1, 2, 3\}$, for all $1 \leq i \leq m$. □

Lemma 3.7. *Let r be a subterm of s in f-form. Suppose a coordinate i is such that $\overline{\mathfrak{T}}_r^i$ has exactly 3 leaves, ℓ_1, ℓ_2, ℓ_3, whose colors are in $\{1,2,3\}$ and are distinct. Then exactly one of ℓ_1, ℓ_2, ℓ_3 belongs to an f-term (call it ℓ_j), and $r(a_0, \ldots, a_n)|_i = e_{\text{label}(\ell_j)}$.*

Proof. Let x, y, z denote the distinct labels of ℓ_1, ℓ_2, ℓ_3. Suppose more than one of ℓ_1, ℓ_2, ℓ_3 belongs to an f-term. Since the conflict of an f-term is 1 and ℓ_1, ℓ_2, ℓ_3 all have non-zero colors, the leaves must belong to distinct f-terms. If all of ℓ_1, ℓ_2, ℓ_3 belong to an f-term, then since all other leaves of $\overline{\mathfrak{T}}_r^i$ besides ℓ_1, ℓ_2, ℓ_3 are colored 0, $r(a_0, \ldots, a_n)|_i$ evaluates as $f(x)+f(y)+f(z)$, up to permutation of x, y, and z. Since x, y, and z are distinct, this always evaluates to a, a contradicition. If exactly two of ℓ_1, ℓ_2, ℓ_3 belong to an f-term, then $r(a_0, \ldots, a_n)|_i$ evaluates as $f(x) + f(y) + z$ or $f(x) + y + f(z)$, up to permutation of x, y, and z. This always evaluates to a, again a contradiction. Thus, at most one of ℓ_1, ℓ_2, ℓ_3 belongs to an f-term.

Suppose now that none of ℓ_1, ℓ_2, ℓ_3 belong to an f-term. Then $r(a_0, \ldots, a_n)|_i$ evaluates as $x + y + z$, up to permutation of x, y, and z. This always evaluates to a, a contradiciton. Hence, exactly one of ℓ_1, ℓ_2, ℓ_3 belongs to an f-term.

Finally, if x is the label of the leaf belonging to an f-term, then since x, y, and z are distinct, $r(a_0, \ldots, a_n)|_i$ evaluates as

$$(f(x) + y) + z = c_{x,y} + z = e_x,$$

$$(f(x) + z) + y = c_{x,z} + y = e_x, \text{ or}$$

$$(y + z) + f(x) = d_{y,z} + c_x = e_x.$$

Thus, we see that $r(a_0, \ldots, a_n)|_i = e_x$. □

In the following, we denote the set of leaves of $\mathfrak{T}_r$ by $\mathscr{L}_r$, the set of leaves of $\overline{\mathfrak{T}}_r^i$ by $\overline{\mathscr{L}}_r^i$, and the set of non-zero labels of $\overline{\mathscr{L}}_r^i$ by label$(\overline{\mathscr{L}}_r^i)$.

For $x \in \{1,2,3\}$, define

$$S_x := \{x, c_x, d_{x,*}, c_{x,*}, c_{*,x}, e_*\} \subset A.$$

Notationally, $d_{2,1}$ is the element $d_{1,2}$, $d_{3,1}$ is the element $d_{1,3}$, and $d_{3,2}$ is the element $d_{2,3}$. Note that S_x satisfies the following properties, which can be verified by Table 3.1:

$$\text{If } u \in S_x \text{ and } v \in A, \text{ then } u + v \in S_x \cup \{a\}. \tag{‡}$$

$$\text{If } u, v \in S_x, \text{ then } u + v \neq a \text{ iff } u = v. \tag{⋆}$$

Lemma 3.8. *Let r be a subterm of s in f-form. Then $x \in \text{label}(\overline{\mathscr{L}}^i_r)$ if and only if $r(a_0, \ldots, a_n)|_i \in S_x$.*

Proof. $\Rightarrow$ We induct on $c_i(r)$. Since $\text{label}(\overline{\mathscr{L}}^i_r)$ is the set of non-zero labels of $\overline{\mathscr{L}}^i_r$, $c_i(r) \geq 1$. So the base case of our induction is $c_i(r) = 1$. If $c_i(r) = 1$, then there is exactly one leaf labeled x in $\overline{\mathfrak{T}}^i_r$, and all other leaves of $\overline{\mathfrak{T}}^i_r$ are labeled 0. Thus, $r(a_0, \ldots, a_n)|_i \in \{x, c_x\} \subset S_x$.

Now suppose $c_i(r) > 1$, and $r'(a_0, \ldots, a_n)|_i \in S_x$ whenever $x \in \text{label}(\overline{\mathscr{L}}^i_{r'})$ and $0 < c_i(r') < c_i(r)$. By Proposition 3.5(1), we may write

$$r(x_0, \ldots, x_n) = r_1(x_0, \ldots, x_n) + r_2(x_0, \ldots, x_n),$$

where we may assume $0 < c_i(r_1) \leq c_i(r_2) < c_i(r)$. Since $x \in \text{label}(\overline{\mathscr{L}}^i_r)$, we must have that $x \in \text{label}(\overline{\mathscr{L}}^i_{r_j})$ for at least one $j \in \{1, 2\}$. WLOG, we assume $x \in \text{label}(\overline{\mathscr{L}}^i_{r_1})$. Then we have that

$$r_1(a_0, \ldots, a_n)|_i, \in S_x$$

by the induction hypothesis. Since $r(a_0, \ldots, a_n)|_i \neq a$, property (‡) implies $r(a_0, \ldots, a_n)|_i = r_1(a_0, \ldots, a_n)|_i + r_2(a_0, \ldots, a_n)|_i \in S_x$.

$\Leftarrow$ Assume $x \notin \text{label}(\overline{\mathscr{L}}^i_r)$. If $\text{label}(\overline{\mathscr{L}}^i_r) = \{y\}$ $(y \neq x)$, then $r(a_0, \ldots, a_n)|_i \in \{y, c_y\}$, so $r(a_0, \ldots, a_n)|_i \notin S_x$. So suppose $\text{label}(\overline{\mathscr{L}}^i_r) = \{y, z\}$ $(z \neq x)$. By the forward direction of the proof of this Lemma, we have that

$$r(a_0, \ldots, a_n)|_i \in S_y \cap S_z = \{d_{y,z}, c_{y,z}, c_{z,y}, e_*\},$$

of which only the elements e_* are in S_x. But no two elements in $\{1, 2, 3\}$ can generate an element of the form e_*, so $r(a_0, \ldots, a_n)|_i \in \{d_{y,z}, c_{y,z}, c_{z,y}\}$, implying $r(a_0, \ldots, a_n)|_i \notin S_x$. □

Corollary 3.9. *Let r be a subterm of s in f-form such that $r(x_0,\ldots,x_n) = r_1(x_0,\ldots,x_n) + r_2(x_0,\ldots,x_n)$. Then $r_1(a_0,\ldots,a_n)|_i = r_2(a_0,\ldots,a_n)|_i \neq 0$ if and only if* $\mathrm{label}(\overline{\mathscr{L}}^i_{r_1}) = \mathrm{label}(\overline{\mathscr{L}}^i_{r_2}) \neq \emptyset$.

Proof. $\Rightarrow$ Note that

$$r_1(a_0,\ldots,a_n)|_i, r_2(a_0,\ldots,a_n)|_i \in A \setminus \{0,a\} = S_1 \cup S_2 \cup S_3.$$

Since $r_1(a_0,\ldots,a_n)|_i \in S_x$ if and only if $r_2(a_0,\ldots,a_n)|_i \in S_x$, Lemma 3.8 implies that $x \in \mathrm{label}(\overline{\mathscr{L}}^i_{r_1})$ if and only if $x \in \mathrm{label}(\overline{\mathscr{L}}^i_{r_2})$.

$\Leftarrow$ Let $x \in \mathrm{label}(\overline{\mathscr{L}}^i_{r_1}) = \mathrm{label}(\overline{\mathscr{L}}^i_{r_2})$. By Lemma 3.8, we have

$$r_1(a_0,\ldots,a_n)|_i, r_2(a_0,\ldots,a_n)|_i \in S_x.$$

By property $(\star)$, $r_1(a_0,\ldots,a_n)|_i = r_2(a_0,\ldots,a_n)|_i \neq 0$. □

Lemma 3.10. *If r is a subterm of s in f-form such that*

$$r(x_0,\ldots,x_n) = r_1(x_0,\ldots,x_n) + r_2(x_0,\ldots,x_n),$$

then for every $1 \leq i \leq m$, we have

$$\mathrm{label}(\overline{\mathscr{L}}^i_{r_1}) \cap \mathrm{label}(\overline{\mathscr{L}}^i_{r_2}) = \emptyset.$$

Proof. We will assume the statement is false, and construct a term $\overline{r}(x_0,\ldots,x_n)$ such that $r(a_0,\ldots,a_n) = \overline{r}(a_0,\ldots,a_n)$ and $|\mathfrak{T}_{\overline{r}}| + \sum_{i=1}^m c_i(\overline{r}) < |\mathfrak{T}_r| + \sum_{i=1}^m c_i(r)$. Replacing r with $\overline{r}$ in p contradicts that p is the shortest term of minimal conflict satisfying $p(a_0,\ldots,a_n) = b$.

Define the sets of coordinates

$$I_= = \{1 \leq i \leq m \mid \mathrm{label}(\overline{\mathscr{L}}^i_{r_1}) = \mathrm{label}(\overline{\mathscr{L}}^i_{r_2}) \neq \emptyset\}, \text{ and}$$
$$I_\cap = \{1 \leq i \leq m \mid \mathrm{label}(\overline{\mathscr{L}}^i_{r_1}) \cap \mathrm{label}(\overline{\mathscr{L}}^i_{r_2}) \neq \emptyset\}.$$

Claim 3.11. $I_= = I_\cap$.

Proof of Claim 3.11. It is clear that $I_= \subseteq I_\cap$. We show $I_\cap \subseteq I_=$. Let $i \in I_\cap$, and $x \in \text{label}(\overline{\mathscr{L}}^i_{r_1}) \cap \text{label}(\overline{\mathscr{L}}^i_{r_2})$. By Lemma 3.8, we have $r_j(a_0, \ldots, a_n)|_i \in S_x$ for $j \in \{1, 2\}$. Then using property $(\star)$, we see $r_1(a_0, \ldots, a_n)|_i = r_2(a_0, \ldots, a_n)|_i \neq 0$. By Corollary 3.9, this implies $\text{label}(\overline{\mathscr{L}}^i_{r_1}) = \text{label}(\overline{\mathscr{L}}^i_{r_2}) \neq \emptyset$, so $i \in I_=$. ■

In what remains, we will refer to these equal sets of coordinates as the set I. Since we are assuming $\text{label}(\overline{\mathscr{L}}^i_{r_1}) \cap \text{label}(\overline{\mathscr{L}}^i_{r_2}) \neq \emptyset$ for some i, we know I is nonempty.

For $i \in I$, let $\{\overline{\ell}^i_1, \ldots, \overline{\ell}^i_j\} \subseteq \overline{\mathscr{L}}^i_{r_1}$ be the subset of leaves whose labels are in $\text{label}(\overline{\mathscr{L}}^i_{r_1})$, and let $L_i = \{\ell_1, \ldots, \ell_j\}$ be the corresponding subset of leaves of $\mathscr{L}_{r_1}$. Then define $L = \bigcup_{i \in I} L_i$. We define $\overline{r}(x_0, \ldots, x_n)$ to be the term $\overline{r}_1(x_0, \ldots, x_n) + \overline{r}_2(x_0, \ldots, x_n)$, where $\overline{r}_1(x_0, \ldots, x_n)$ is obtained from $r_1(x_0, \ldots, x_n)$ by replacing $\text{label}(\ell)$ with x_0 for each $\ell \in L$, and $\overline{r}_2(x_0, \ldots, x_n) = r_2(x_0, \ldots, x_n)$. Recall that $a_0 = (0, \ldots, 0)$. Thus for all $i \in I$, all leaves of $\overline{\mathfrak{T}}^i_{\overline{r}_1}$ are labeled 0, so that $\overline{r}(a_0, \ldots, a_n)|_i = \overline{r}_2(a_0, \ldots, a_n)|_i = r_2(a_0, \ldots, a_n)|_i$ for all $i \in I$.

Note $c_i(\overline{r}) < c_i(r)$ for $i \in I$ and $c_i(\overline{r}) \leq c_i(r)$ for $i \notin I$. Thus, we have $\sum_{i=1}^m c_i(\overline{r}) < \sum_{i=1}^m c_i(r)$. Further, we obtained $\overline{r}$ from r by changing labels of leaves, so $|\mathfrak{T}_{\overline{r}}| = |\mathfrak{T}_r|$. Hence, $|\mathfrak{T}_{\overline{r}}| + \sum_{i=1}^m c_i(\overline{r}) < |\mathfrak{T}_r| + \sum_{i=1}^m c_i(r)$. It remains to show that $r(a_0, \ldots, a_n) = \overline{r}(a_0, \ldots, a_n)$. We use two claims:

Claim 3.12. *If $i \in I$, then $r_1(a_0, \ldots, a_n)|_i = r_2(a_0, \ldots, a_n)|_i$. Thus,*

$$r(a_0, \ldots, a_n)|_i = r_2(a_0, \ldots, a_n)|_i$$

for all $i \in I$.

Proof of Claim 3.12. Let $i \in I = I_\cap$. We showed in the proof of Claim 3.11 that if $i \in I_\cap$, then $r_1(a_0, \ldots, a_n)|_i = r_2(a_0, \ldots, a_n)|_i$. Then using the fact that $+$ is idempotent, we compute

$$\begin{aligned} r(a_0, \ldots, a_n)|_i &= r_1(a_0, \ldots, a_n)|_i + r_2(a_0, \ldots, a_n)|_i \\ &= r_2(a_0, \ldots, a_n)|_i. \end{aligned}$$

■

Claim 3.13. *If $i \notin I$, then* $\text{label}(\overline{\ell}^i) = 0$ *for all $\ell \in L$. Thus, $\overline{r}(a_0, \ldots, a_n)|_i = (r_1 + r_2)(a_0, \ldots, a_n)|_i$ for all $i \notin I$.*

Proof of Claim 3.13. For the first statement, we prove the contrapositive. Let $\ell \in L$ and i be a coordinate such that $\text{label}(\overline{\ell}^i) \in \{1, 2, 3\}$. The label of ℓ in $\mathfrak{T}_{r_1}$ is a variable x_j, and $\text{label}(\overline{\ell}^i) \in \{1, 2, 3\}$ implies that the variable x_j is in clause C_i. Since $\ell \in L$, we know $\ell \in L_k$ for some $k \in I$. Thus $\overline{\ell}^k$ has a non-zero label $c \in \{1, 2, 3\}$ in $\overline{\mathfrak{T}}^k_{r_1}$ (so x_j is in clause C_k), and since $k \in I$, $\overline{\mathfrak{T}}^k_{r_2}$ also has a leaf $\overline{\ell}^k_*$ labeled c. Since exactly one variable is labeled c in clause C_k, this means that the label of the leaf ℓ_* in $\mathfrak{T}_{r_2}$ is also the variable x_j. But then $\overline{\ell}^i_*$ in $\overline{\mathfrak{T}}^i_{r_2}$ has the same non-zero label as $\overline{\ell}^i$ in $\overline{\mathfrak{T}}^i_{r_1}$, so $i \in I_\cap = I$.

Thus, if $i \notin I$ and $\ell \in L$, the labels of $\overline{\ell}^i$ in $\overline{\mathfrak{T}}^i_{r_1}$ being replaced by 0 labels to obtain $\overline{\mathfrak{T}}^i_{\overline{r}_1}$ were already 0. Hence, $\overline{r}_1(a_0, \ldots, a_n)|_i = r_1(a_0, \ldots, a_n)|_i$, so that

$$\begin{aligned}\overline{r}(a_0, \ldots, a_n)|_i &= \overline{r}_1(a_0, \ldots, a_n)|_i + \overline{r}_2(a_0, \ldots, a_n)|_i \\ &= (r_1 + r_2)(a_0, \ldots, a_n)|_i\end{aligned}$$

for all $i \notin I$. ■

Then we compute

$$\begin{aligned}r(a_0, \ldots, a_n) &\overset{\text{Claim 3.12}}{=} \begin{cases} r_2(a_0, \ldots, a_n)|_i & \text{if } i \in I \\ (r_1 + r_2)(a_0, \ldots, a_n)|_i & \text{if } i \notin I \end{cases} \\ &\overset{\text{Claim 3.13}}{=} \overline{r}(a_0, \ldots, a_n),\end{aligned}$$

which completes the proof. □

Definition 3.14. Let $r(x_0, \ldots, x_n)$ be any term.

(a) $\overline{\mathfrak{T}}^i_r$ is **monochromatic of size** q for $q \geq 1$ if each leaf has color in $\{0, k\}$, for some $k \in \{1, 2, 3\}$, and there are q leaves colored k.

(b) A **monochromatic subtree of size** q (≥ 1) is a subtree of $\overline{\mathfrak{T}}^i_r$ which corresponds to a subterm of r, and is monochromatic of size q.

(c) A term r is **simplified** if for every $1 \leq i \leq m$, $\overline{\mathfrak{T}}^i_r$ has no monochromatic subtree of size $q \geq 2$.

We use Lemma 3.10 to show that every subterm of s in f-form is simplified.

Corollary 3.15. *If r is a subterm of s in f-form, then r is simplified.*

Proof. Suppose the statement is false. Then there exists a coordinate i and a monochromatic subtree $\overline{\mathfrak{T}}^i_{r'}$ of $\overline{\mathfrak{T}}^i_r$ of size $q \geq 2$. Assume $\overline{\mathfrak{T}}^i_{r'}$ is a minimal monochromatic subtree of size $q \geq 2$. Since $\overline{\mathfrak{T}}^i_{r'}$ is monochromatic of size $q \geq 2$, we know $\mathcal{C}(r') \geq 2$. By Proposition 3.5, the root of r' is $+$ so we may write $r'(x_0, \ldots, x_n) = r'_1(x_0, \ldots, x_n) + r'_2(x_0, \ldots, x_n)$. Since $\overline{\mathfrak{T}}^i_{r'}$ is a minimal monochromatic subtree of size $q \geq 2$, we must have that $c_i(r'_1) = c_i(r'_2) = 1$, so that $\overline{\mathfrak{T}}^i_{r'}$ is monochromatic of size 2 and is minimal with this property.

Now $\overline{\mathfrak{T}}^i_{r'}$ being a minimal monochromatic subtree of size 2 implies the two leaves, ℓ_1 and ℓ_2, of $\overline{\mathfrak{T}}^i_{r'}$ colored $k \in \{1, 2, 3\}$ satisfy that (WLOG) ℓ_1 belongs to $\overline{\mathfrak{T}}^i_{r'_1}$ and ℓ_2 belongs to $\overline{\mathfrak{T}}^i_{r'_2}$. That is, $\text{label}(\overline{\mathscr{L}}^i_{r_1}) \cap \text{label}(\overline{\mathscr{L}}^i_{r_2}) \neq \emptyset$, which contradicts Lemma 3.10. Thus, r must be simplified. □

Corollary 3.16. *If r is a subterm of s in f-form and $\mathcal{C}(r) \leq 3$, then the non-zero labels of $\overline{\mathfrak{T}}^i_r$ are distinct for all $1 \leq i \leq m$.*

Proof. Choose a coordinate i, and recall that r is simplified by Corollary 3.15. If $c_i(r) \in \{0, 1\}$, the result is clear. If $c_i(r) = 2$, then the result follows since otherwise $\overline{\mathfrak{T}}^i_r$ is monochromatic of size 2.

Finally, suppose $c_i(r) = 3$. Then $\mathcal{C}(r) \geq 3$, so by Proposition 3.5, the root of r is $+$. Thus, we may write $r(x_0, \ldots, x_n) = r_1(x_0, \ldots, x_n) + r_2(x_0, \ldots, x_n)$ (and assume $c_i(r_j) > 0$ for each $j \in \{1, 2\}$). Then WLOG, $c_i(r_1) = 2$. Since r is simplified, the non-zero labels of $\overline{\mathfrak{T}}^i_{r_1}$ are distinct. By Lemma 3.10, $\text{label}(\overline{\mathscr{L}}^i_{r_1}) \cap \text{label}(\overline{\mathscr{L}}^i_{r_2}) = \emptyset$, so all non-zero labels of $\overline{\mathfrak{T}}^i_r$ are distinct. □

Lemma 3.17. *The term s is in f-form.*

Proof. Suppose the statement is false. Recall, we are assuming that every subterm of p of the form $f(r(x_0, \ldots, x_n))$, where the subterm r is g-free, f-free, and satisfies $\mathcal{C}(r) = 1$, is an f-term. Thus, if s is not in f-form there exists a subterm $f(r(x_0, \ldots, x_n))$ such that either the subterm r is not f-free, or $\mathcal{C}(r) > 1$.

Suppose first that the subterm r is not f-free. Let r' be a subterm of r whose root is a maximal occurrence of f in $\mathfrak{T}_r$. Choose a coordinate i such that $\overline{\mathfrak{T}}^i_{r'}$ has at least one leaf with a non-zero label. Then $r'(a_0, \ldots, a_n)|_i \in \{c_*, a\}$, and since the root of r' is a maximal occurrence of f in $\mathfrak{T}_r$, Table 3.1 can be used to verify that $r(a_0, \ldots, a_n)|_i \in \{a, c_*, c_{*,*}, e_*\}$. But then $f(r(a_0, \ldots, a_n))|_i = a$, a contradiction. Thus we assume r is an f-free subterm.

Now suppose $\mathcal{C}(r) > 1$. We begin with a claim.

Claim 3.18. *If u is a subterm of s in f-form and $\mathcal{C}(u) > 1$, then $u(a_0, \ldots, a_n)|_i \notin \{0, 1, 2, 3\}$ for some coordinate i.*

Proof of Claim 3.18. We induct on $\mathcal{C}(u)$. For the base case, assume $\mathcal{C}(u) = 2$. Let i be a coordinate such that $c_i(u) = 2$. Then $|\text{label}(\overline{\mathscr{L}}^i_u)| = 2$, for otherwise $\overline{\mathfrak{T}}^i_u$ would be monochromatic of size 2, contradicting that u is simplified (Corollary 3.15). Thus if $\text{label}(\overline{\mathscr{L}}^i_u) = \{x, y\}$, then by Lemma 3.8 we have that

$$u(a_0, \ldots, a_n)|_i \in S_x \cap S_y = \{d_{x,y}, c_{x,y}, c_{y,x}, e_*\} \notin \{0, 1, 2, 3\}.$$

Now suppose $\mathcal{C}(u) > 2$, and if $1 < \mathcal{C}(u') < \mathcal{C}(u)$, then we have that $u'(a_0, \ldots, a_n)|_i \notin \{0, 1, 2, 3\}$ for some coordinate i. By Proposition 3.5, we may write $u(x_0, \ldots, x_n) = u_1(x_0, \ldots, x_n) + u_2(x_0, \ldots, x_n)$, and assume $1 \leq \mathcal{C}(u_j) < \mathcal{C}(u)$ for $j \in \{1, 2\}$. If $\mathcal{C}(u_1) = \mathcal{C}(u_2) = 1$, then $\mathcal{C}(u) \leq 2$. Hence we must have that (WLOG) $1 < \mathcal{C}(u_1) < \mathcal{C}(u)$. Then by the induction hypothesis, $u_1(a_0, \ldots, a_n)|_i \notin \{0, 1, 2, 3\}$ for some coordinate i. It is clear from Table 3.1 that if $x + y \in \{0, 1, 2, 3\}$, then $x, y \in \{0, 1, 2, 3\}$. Since $u_1(a_0, \ldots, a_n)|_i \notin \{0, 1, 2, 3\}$, it must be that $u(a_0, \ldots, a_n)|_i \notin \{0, 1, 2, 3\}$. ∎

Now since r is an f-free subterm by the first part of this lemma, r is trivially in f-form. By

the claim, $r(a_0,\dots,a_n)|_i \notin \{0,1,2,3\}$ for some coordinate i. But then $f(r(a_0,\dots,a_n))|_i = a$, a contradiction.

Thus, every subterm of the form $f(r(x_0,\dots,x_n))$ must satisfy that r is an f-free subterm and $\mathcal{C}(r) = 1$, which means s is in f-form. □

Lemma 3.19. *The term s satisfies $\mathcal{C}(s) \leq 3$.*

Proof. We show that if h is the height of $\mathfrak{T}_s$ and $0 \leq k \leq h$, then any subterm r of s whose root has height k in $\mathfrak{T}_s$ satisfies $\mathcal{C}(r) \leq 3$. We proceed by induction on the height k of the root of a subterm r of s in $\mathfrak{T}_s$.

If $k = 0$, then r is a variable. Thus, $\mathcal{C}(r) = 1$, and the base case is proven.

So let $k \geq 1$ be the height of the root of r in $\mathfrak{T}_s$ and assume any subterm r' whose root has height less than k satisfies $\mathcal{C}(r') \leq 3$.

Since s is in f-form, r is in f-form. Thus, if the root of r is f, then r is an f-term so $\mathcal{C}(r) = 1$. So we may assume the root of r is $+$. Then $r(x_0,\dots,x_n) = r_1(x_0,\dots,x_n) + r_2(x_0,\dots,x_n)$, where $\mathcal{C}(r_1) \leq 3$ and $\mathcal{C}(r_2) \leq 3$ by the induction hypothesis. Further, the non-zero labels of each of $\overline{\mathfrak{T}}^i_{r_1}$ and $\overline{\mathfrak{T}}^i_{r_2}$ are distinct for all i by Corollary 3.16.

We'd like to describe the range of r_j ($j \in \{1,2\}$) at the coordinate level based on $c_i(r_j)$. If $c_i(r_j) = 0$, then all leaves of $\overline{\mathfrak{T}}^i_{r_j}$ are labeled 0, so the range is $\{0\}$. If $c_i(r_j) = 1$, then there is exactly one leaf of $\overline{\mathfrak{T}}^i_{r_j}$ with a non-zero label. Thus, the range is $\{1,2,3,c_*\}$. If $c_i(r_j) = 2$, then $\mathcal{C}(r_j) \geq 2$, so the root of r_j is $+$ by Proposition 3.5. Thus we may write $r_j(x_0,\dots,x_n) = r_{j,1}(x_0,\dots,x_n) + r_{j,2}(x_0,\dots,x_n)$, where we assume $c_i(r_{j,1}) = c_i(r_{j,2}) = 1$. Thus the range of both $r_{j,1}$ and $r_{j,2}$ in the i^{th} coordinate is $\{1,2,3,c_*\}$. Since the non-zero labels of $\overline{\mathfrak{T}}_{r_j}$ are distinct and $r_j(a_0,\dots,a_n) \neq a$, the range in the case that $c_i(r_j) = 2$ is $\{d_{*,*}, c_{*,*}\}$. If $c_i(r_j) = 3$, since r_j is in f-form and $\overline{\mathfrak{T}}^i_{r_j}$ has 3 distinctly colored leaves, by Lemma 3.7 the range is $\{e_*\}$. We summarize our conclusions in Table 3.2.

From Table 3.2 we see that for all $1 \leq i \leq m$,

$$c_i(r_1 + r_2) = c_i(r_1) + c_i(r_2) \neq 5,$$

$c_i(r_j)$	Range
0	$\{0\}$
1	$\{1, 2, 3, c_*\}$
2	$\{d_{*,*}, c_{*,*}\}$
3	$\{e_*\}$

Table 3.2: The range of values at the coordinate level for r_1 and r_2 depending on conflict.

as adding any element from the range corresponding with conflict 2 to any element from the range corresponding with conflict 3 results in a. Further, if $c_i(r_1+r_2) \in \{4, 6\}$, then $c_i(r_1) = c_i(r_2) = 2$ or $c_i(r_1) = c_i(r_2) = 3$. In both cases, we see from Table 3.2 that $r_1(a_0, \ldots, a_n)|_i = r_2(a_0, \ldots, a_n)|_i \neq 0$. Thus label$(\overline{\mathscr{L}}^i_{r_1})$ = label$(\overline{\mathscr{L}}^i_{r_2}) \neq \emptyset$ by Corollary 3.9, contradicting Lemma 3.10.

Thus we have shown that $c_i(r_1 + r_2) \leq 3$ for all i, which means $\mathcal{C}(r) \leq 3$ as desired. By induction, we have that the term s satisfies $\mathcal{C}(s) \leq 3$. □

Corollary 3.20. *The term s satisfies $c_i(s) = 3$ for all $1 \leq i \leq m$.*

Proof. By the Lemma 3.19, $c_i(s) \leq 3$ for all $1 \leq i \leq m$. But no two elements of the set $\{1, 2, 3\}$ can generate an element of the form e_*, so we also have $c_i(s) \geq 3$ for all $1 \leq i \leq m$. Hence, $c_i(s) = 3$ for all $1 \leq i \leq m$. □

Now $p(a_0, \ldots, a_n) = b$ by assumption, and Corollaries 3.20 and 3.16 imply that each variable $x_i \in \{x_1, \ldots, x_n\}$ labels exactly one leaf in $\mathfrak{T}_p$. Finally, Lemma 3.7 implies that for all $1 \leq i \leq m$, exactly one variable in C_i belongs to a subterm of p whose root is f. We thus have proven Theorem 3.2.

Chapter 4

The SMP and strong linear Maltsev conditions

In the previous chapter, we constructed an algebra with a Taylor term whose subpower membership problem is NP-hard. The existence of a Taylor term is a consistent strong linear Maltsev condition which does not imply the existence of a cube term. In this chapter, we prove in Theorem 4.1 that this property of a consistent strong linear Maltsev condition $\mathcal{M}$ is sufficient to produce finite algebras which satisfy $\mathcal{M}$ and have a subpower membership problem which is EXPTIME-complete. We will then discuss consequences of Theorem 4.1.

4.1 The main result

Theorem 4.1. *Let $\mathcal{M} = (\mathcal{H}, \Sigma)$ be a consistent strong linear Maltsev condition such that Σ does not entail cube identities for any $h \in \mathcal{H}$.*

(i) *For any finite algebra $\mathbb{A}$, there exists a finite algebra $\mathbb{A}_\mathcal{M}$ such that the language of $\mathbb{A}_\mathcal{M}$ contains $\mathcal{H}$, $\mathbb{A}_\mathcal{M} \models \Sigma$, and* SMP($\mathbb{A}$) *has a polynomial time reduction to* SMP($\mathbb{A}_\mathcal{M}$).

(ii) *In particular, there exists a finite algebra $\mathbb{B}_\mathcal{M}$ such that the language of $\mathbb{B}_\mathcal{M}$ contains $\mathcal{H}$, $\mathbb{B}_\mathcal{M} \models \Sigma$, and* SMP($\mathbb{B}_\mathcal{M}$) *is* EXPTIME*-complete.*

Proof. (i) Let $\mathbb{A} = \langle A; \mathcal{F} \rangle$ be a finite algebra. We assume the languages $\mathcal{F}$ and $\mathcal{H}$ are disjoint, and now define $\mathbb{A}_\mathcal{M}$. We define the element set of $\mathbb{A}_\mathcal{M}$ to be the set $A \cup \{0\}$, where the element 0 is distinct from all elements of A. The language of $\mathbb{A}_\mathcal{M}$ will be $\mathcal{F} \cup \mathcal{H}$, which we must interpret in $\mathbb{A}_\mathcal{M}$. For k-ary $f \in \mathcal{F}$ and $(a_1, \ldots, a_k) \in (A \cup \{0\})^k$, we define $f^{\mathbb{A}_\mathcal{M}}(a_1, \ldots, a_k) = f^\mathbb{A}(a_1, \ldots, a_k)$ if

$a_i \neq 0$ for all $1 \leq i \leq k$, and $f^{\mathbb{A}_\mathcal{M}}(a_1, \ldots, a_k) = 0$ otherwise. Thus, 0 is an absorbing element with respect to the operations $f^{\mathbb{A}_\mathcal{M}}$ for $f \in \mathcal{F}$.

To interpret the operation symbols of $\mathcal{H}$ in $\mathbb{A}_\mathcal{M}$, we need to introduce some terminology and notation. Let X be a variable set which is large enough for Σ. Since $\mathcal{M}$ is consistent, we know Σ does not entail $x \approx y$ for distinct $x, y \in X$. For any positive integer k, we will say that $(x_1, \ldots, x_k) \in X^k$ and $(a_1, \ldots, a_k) \in A^k$ have the **same equality pattern** if, for all $1 \leq i, j \leq k$, the tuples have the property that $x_i = x_j$ if and only if $a_i = a_j$. For $\overline{a} \in A^k$, define

$$P_{\overline{a}} = \{\overline{x} \in X^k \mid \overline{x} \text{ and } \overline{a} \text{ have the same equality pattern}\}.$$

We are now ready to describe the interpretation of the symbols in $\mathcal{H}$. For k-ary $h \in \mathcal{H}$ and $\overline{a} = (a_1, \ldots, a_k) \in (A \cup \{0\})^k$, define

$$h^{\mathbb{A}_\mathcal{M}}(a_1, \ldots, a_k) = \begin{cases} a_i & \text{if there exist } (x_1, \ldots, x_k) \in P_{\overline{a}} \text{ and } 1 \leq i \leq k \\ & \text{such that } \Sigma \vdash h(x_1, \ldots, x_k) \approx x_i \\ 0 & \text{otherwise.} \end{cases}$$

Note that if h is 0-ary, then $h^{\mathbb{A}_\mathcal{M}} = 0$.

We first show $h^{\mathbb{A}_\mathcal{M}}$ is well-defined for each $h \in \mathcal{H}$. We must show that if

$$(y_1, \ldots, y_k), (z_1, \ldots, z_k) \in P_{\overline{a}},$$

and

$$\Sigma \vdash h(y_1, \ldots, y_k) \approx y_r \text{ and } \Sigma \vdash h(z_1, \ldots, z_k) \approx z_q,\ 1 \leq r, q \leq k,$$

then $a_r = a_q$. To see this is the case, note that $(y_1, \ldots, y_k), (z_1, \ldots, z_k) \in P_{\overline{a}}$ implies that $y_i = y_j$ if and only if $z_i = z_j$ for all $1 \leq i, j \leq k$. Thus, the map $\gamma \colon \{y_1, \ldots, y_k\} \to \{z_1, \ldots, z_k\}$, $y_i \mapsto z_i$, is well-defined, and by entailment property (4) we have that $\Sigma \vdash h(z_1, \ldots, z_k) \approx z_r$. Thus, by entailment properties (2) and (3), $\Sigma \vdash z_r \approx z_q$. Since Σ is consistent, it must be that $z_r = z_q$, hence $(z_1, \ldots, z_k) \in P_{\overline{a}}$ implies that $a_r = a_q$. This completes the definition of $\mathbb{A}_\mathcal{M} = \langle A \cup \{0\}; \mathcal{F} \cup \mathcal{H} \rangle$.

Next we show $\mathbb{A}_\mathcal{M} \models \Sigma$. In order to show this, we will first discuss how to evaluate, in $\mathbb{A}_\mathcal{M}$, an arbitrary linear term in the language $\mathcal{H}$. In the following, we use "=" to denote equality

of terms. Let $w(y_1, \ldots, y_\ell)$ be any linear term with distinct variables $y_1, \ldots, y_\ell$, where $\ell \leq |X|$ and w need not depend on all variables. If $w(y_1, \ldots, y_\ell) = y_i$ for some $1 \leq i \leq \ell$, then for any $(a_1, \ldots, a_\ell) \in (A \cup \{0\})^\ell$, we have that $w^{\mathbb{A}_\mathcal{M}}(a_1, \ldots, a_\ell) = a_i$. Otherwise, since w is a linear term, $w(y_1, \ldots, y_\ell) = h(y_{t(1)}, \ldots, y_{t(k)})$ for some k-ary $h \in \mathcal{H}$ and some map $t\colon \{1, \ldots, k\} \to \{1, \ldots, \ell\}$. The following claim establishes how we evaluate $w(y_1, \ldots, y_\ell)$ in $\mathbb{A}_\mathcal{M}$.

Claim 4.2. *Let $w(y_1, \ldots, y_\ell) = h(y_{t(1)}, \ldots, y_{t(k)})$ be a linear term in the language $\mathcal{H}$ ($\ell \leq |X|$). If $\overline{a} = (a_1, \ldots, a_\ell) \in (A \cup \{0\})^\ell$, then*

$$w^{\mathbb{A}_\mathcal{M}}(a_1, \ldots, a_\ell) = \begin{cases} a_j & \text{if there exist } (x_1, \ldots, x_\ell) \in P_{\overline{a}} \text{ and } 1 \leq j \leq \ell \\ & \text{such that } \Sigma \vdash w(x_1, \ldots, x_\ell) \approx x_j \\ 0 & \text{otherwise.} \end{cases}$$

Proof of Claim 4.2. Let $\overline{a} = (a_1, \ldots, a_\ell) \in (A \cup \{0\})^\ell$, and let $\overline{a}_t = (a_{t(1)}, \ldots, a_{t(k)}) \in (A \cup \{0\})^k$. We first show that the following two conditions on $\overline{a}$ and $\overline{a}_t$ are equivalent:

(a) There exist $(x_1, \ldots, x_\ell) \in P_{\overline{a}}$ and $1 \leq j \leq \ell$ such that

$$\Sigma \vdash w(x_1, \ldots, x_\ell) \approx x_j.$$

(b) There exist $(x_{t(1)}, \ldots, x_{t(k)}) \in P_{\overline{a}_t}$ and $1 \leq i \leq k$ such that

$$\Sigma \vdash h(x_{t(1)}, \ldots, x_{t(k)}) \approx x_{t(i)}.$$

(a) $\Rightarrow$ (b) If $(x_1, \ldots, x_\ell) \in P_{\overline{a}}$, then $(x_{t(1)}, \ldots, x_{t(k)}) \in P_{\overline{a}_t}$. Further,

$$\Sigma \vdash x_j \approx w(x_1, \ldots, x_\ell) \text{ by assumption and entailment property (2), and}$$

$$w(x_1, \ldots, x_\ell) = h(x_{t(1)}, \ldots, x_{t(k)}).$$

Thus, $\Sigma \vdash h(x_{t(1)}, \ldots, x_{t(k)}) \approx x_j$ by entailment property (2). Since Σ is consistent, $j = t(i)$ for some $1 \leq i \leq k$.

(b) $\Rightarrow$ (a) Let $\equiv$ denote the equivalence relation on the set $\{1,\dots,\ell\}$ defined by $r \equiv q$ if and only if $a_r = a_q$, and denote the $\equiv$-class of $r \in \{1,\dots,\ell\}$ by $[r]$. Let T be the set of $\equiv$-classes. Since $|T| \leq \ell \leq |X|$ and

$$t(q) \equiv t(r) \iff a_{t(q)} = a_{t(r)} \iff x_{t(q)} = x_{t(r)},$$

there is a well-defined and one-to-one map $\psi\colon T \to X$ such that $\psi([t(r)]) = x_{t(r)}$ for all numbers of the form $t(r)$ $(1 \leq r \leq k)$. For each $s \in \{1,\dots,\ell\}$, define $z_s := \psi([s])$. Then $(z_1,\dots,z_\ell) \in P_{\overline{a}}$, and $x_{t(r)} = \psi([t(r)]) = z_{t(r)}$ for all $1 \leq r \leq k$. We compute

$$\Sigma \vdash x_{t(i)} \approx h(x_{t(1)},\dots,x_{t(k)}) \text{ by assumption and entailment property (2), and}$$

$$\begin{aligned} h(x_{t(1)},\dots,x_{t(k)}) &= h(z_{t(1)},\dots,z_{t(k)}) \\ &= w(z_1,\dots,z_\ell). \end{aligned}$$

By entailment property (2), we have $\Sigma \vdash w(z_1,\dots,z_\ell) \approx x_{t(i)}$. Since $x_{t(i)} = z_{t(i)}$, we have $\Sigma \vdash w(z_1,\dots,z_\ell) \approx z_{t(i)}$, where $1 \leq t(i) \leq \ell$. This completes the argument that (a) and (b) are equivalent.

Now we compute

$$w^{\mathbb{A}_{\mathcal{M}}}(a_1,\dots,a_\ell) = h^{\mathbb{A}_{\mathcal{M}}}(a_{t(1)},\dots,a_{t(k)})$$

$$= \begin{cases} a_{t(i)} & \text{if there exist } (x_{t(1)},\dots,x_{t(k)}) \in P_{\overline{a}_t} \text{ and } 1 \leq i \leq k \\ & \text{such that } \Sigma \vdash h(x_{t(1)},\dots,x_{t(k)}) \approx x_{t(i)} \\ 0 & \text{otherwise} \end{cases}$$

$$= \begin{cases} a_j & \text{if there exist } (x_1,\dots,x_\ell) \in P_{\overline{a}} \text{ and } 1 \leq j \leq \ell \\ & \text{such that } \Sigma \vdash w(x_1,\dots,x_\ell) \approx x_j \\ 0 & \text{otherwise,} \end{cases}$$

where the last equality follows from the equivalence of (a) and (b). ■

We now finish the argument that $\mathbb{A}_{\mathcal{M}} \models \Sigma$. Let $u \approx v \in \Sigma$, where u and v are linear terms in the language $\mathcal{H}$. Since X is large enough for Σ, we may write $u(y_1,\dots,y_\ell) \approx v(y_1,\dots,y_\ell)$,

where $y_1, \ldots, y_\ell$ are distinct variables ($\ell \leq |X|$) and u and v need not depend on every variable. If $\overline{a} = (a_1, \ldots, a_\ell) \in (A \cup \{0\})^\ell$, entailment properties (2), (3), and (4) imply that if $(x_1, \ldots, x_\ell) \in P_{\overline{a}}$ and $1 \leq j \leq \ell$, then $\Sigma \vdash u(x_1, \ldots, x_\ell) \approx x_j$ if and only if $\Sigma \vdash v(x_1, \ldots, x_\ell) \approx x_j$. Thus by Claim 4.2, $u^{\mathbb{A}_\mathcal{M}}(a_1, \ldots, a_\ell) = v^{\mathbb{A}_\mathcal{M}}(a_1, \ldots, a_\ell)$, so $\mathbb{A}_\mathcal{M} \models u \approx v$.

To show that SMP($\mathbb{A}_\mathcal{M}$) is at least as hard as SMP($\mathbb{A}$), we will transform any instance of SMP($\mathbb{A}$) to a corresponding instance of SMP($\mathbb{A}_\mathcal{M}$) in polynomial time such that the SMP($\mathbb{A}$) instance has a 'yes' answer if and only if the corresponding SMP($\mathbb{A}_\mathcal{M}$) instance has a 'yes' answer.

Fix an instance $a_1, \ldots, a_n, b \in A^m$ of SMP($\mathbb{A}$). This is also an instance of SMP($\mathbb{A}_\mathcal{M}$), and we will use this same instance in our reduction. Since we have not changed the instance, this reduction can be done in constant time.

The main goal now is to show that b is in the subalgebra of $\mathbb{A}^m$ generated by $a_1, \ldots, a_n$ if and only if b is in the subalgebra of $\mathbb{A}^m_\mathcal{M}$ generated by $a_1, \ldots, a_n$. To distinguish generated subalgebras of $\mathbb{A}^m$ and generated subalgebras of $\mathbb{A}^m_\mathcal{M}$, we will denote the subalgebra $\langle a_1, \ldots, a_n \rangle$ of $\mathbb{B} \in \{\mathbb{A}^m, \mathbb{A}^m_\mathcal{M}\}$ by $\langle a_1, \ldots, a_n \rangle_\mathbb{B}$.

Suppose first that the SMP($\mathbb{A}$) instance has a 'yes' answer. That is, $b \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m}$. Let $p(x_1, \ldots, x_n)$ be a term in the language $\mathcal{F}$ such that $p^{\mathbb{A}^m}(a_1, \ldots, a_n) = b$. Then $p(x_1, \ldots, x_n)$ is also a term in the language $\mathcal{F} \cup \mathcal{H}$ and $p^{\mathbb{A}^m}(a_1, \ldots, a_n) = p^{\mathbb{A}^m_\mathcal{M}}(a_1, \ldots, a_n)$, so $b \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_\mathcal{M}}$. Thus the SMP($\mathbb{A}_\mathcal{M}$) instance also has a 'yes' answer.

For the converse direction, we will show that if $u_1, \ldots, u_n \in (A \cup \{0\})^m$, $w \in A^m$, and $w \in \langle u_1, \ldots, u_n \rangle_{\mathbb{A}^m_\mathcal{M}}$, then there exists a term $p(x_1, \ldots, x_n)$ in the language $\mathcal{F}$ such that $p^{\mathbb{A}^m_\mathcal{M}}(u_1, \ldots, u_n) = w$. Since $a_1, \ldots, a_n, b \in A^m \subseteq (A \cup \{0\})^m$, this will show that $b \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_\mathcal{M}}$ implies $b \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m}$.

Claim 4.3. *If $u_1, \ldots, u_n \in (A \cup \{0\})^m$, $w \in A^m$, and $w \in \langle u_1, \ldots, u_n \rangle_{\mathbb{A}^m_\mathcal{M}}$, then there exists a term $p(x_1, \ldots, x_n)$ in the language $\mathcal{F}$ such that*

$$p^{\mathbb{A}^m_\mathcal{M}}(u_1, \ldots, u_n) = w.$$

Proof of Claim 4.3. Let $u_1, \ldots, u_n \in (A \cup \{0\})^m$ and $w \in A^m$. Let $p(x_1, \ldots, x_n)$ be a term in the

language $\mathcal{F} \cup \mathcal{H}$ such that $p^{\mathbb{A}_{\mathcal{M}}^m}(u_1, \ldots, u_n) = w$. We assume $p(x_1, \ldots, x_n)$ was chosen so that the term tree $\mathfrak{T}_p$ has the minimum number of vertices with labels from $\mathcal{H}$ and satisfies $p^{\mathbb{A}_{\mathcal{M}}^m}(u_1, \ldots, u_n) = w$. If $\mathfrak{T}_p$ has no label from $\mathcal{H}$, then the claim is proven. So we assume $\mathfrak{T}_p$ has at least one vertex with label from $\mathcal{H}$. We will analyze the term $p(x_1, \ldots, x_n)$ in parallel with the evaluation of p at $u_1, \ldots, u_n$, as illustrated in Figure 4.1.

Choose a maximal vertex with respect to height with label from $\mathcal{H}$, and say the label is $h \in \mathcal{H}$. Call this vertex ν. The subtree of $\mathfrak{T}_p$ whose root is ν corresponds to a subterm q of p. If h is k-ary, the vertex ν has k edges corresponding to k subterms of q, which we will denote as $s_1, \ldots, s_k$. For $1 \leq i \leq k$, we define $c_i := s_i^{\mathbb{A}_{\mathcal{M}}^m}(u_1, \ldots, u_n)$. Set $z := h^{\mathbb{A}_{\mathcal{M}}^m}(c_1, \ldots, c_k)$. For $1 \leq j \leq m$, we write $z|_j$ to denote the j^{th} coordinate of the m-tuple z. Since ν is a maximal vertex in $\mathfrak{T}_p$ with label from

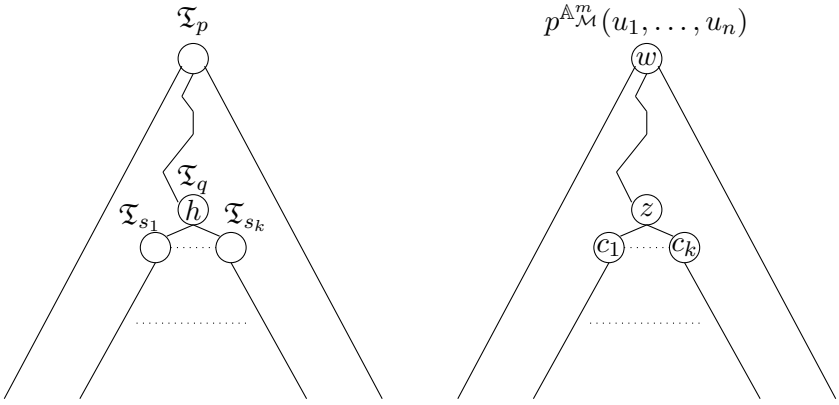

Figure 4.1: The term tree $\mathfrak{T}_p$ for the term $p(x_1, \ldots, x_n)$ in the language $\mathcal{F} \cup \mathcal{H}$ (left), and the evaluation of p at $(u_1, \ldots, u_n)$ (right).

$\mathcal{H}$, the term p has the form $t(\ldots, q(x_1, \ldots, x_n), \ldots)$, where t is a term in the language $\mathcal{F}$. Since 0 is an absorbing element with respect to the operations $f^{\mathbb{A}_{\mathcal{M}}}$ for $f \in \mathcal{F}$, and $w|_j \neq 0$ for all $1 \leq j \leq m$, we must have that

$$h^{\mathbb{A}_{\mathcal{M}}^m}(c_1, \ldots, c_k)|_j = z|_j = q^{\mathbb{A}_{\mathcal{M}}^m}(u_1, \ldots, u_n)|_j \neq 0$$

for all $1 \leq j \leq m$. For $1 \leq j \leq m$, define

$$B_j = \{i \in \{1, \ldots, k\} \mid h^{\mathbb{A}_{\mathcal{M}}^m}(c_1, \ldots, c_k)|_j = c_i|_j\}.$$

If $\bigcap_{j=1}^m B_j \neq \emptyset$, we choose $i \in \bigcap_{j=1}^m B_j$ and form a new term p' by replacing the subterm $q(x_1, \ldots, x_n) = h(s_1(x_1, \ldots, x_n), \ldots, s_k(x_1, \ldots, x_n))$ of p with $s_i(x_1, \ldots, x_n)$. Since $i \in \bigcap_{j=1}^m B_j$, we have $q^{\mathbb{A}_{\mathcal{M}}^m}(u_1, \ldots, u_n) = h^{\mathbb{A}_{\mathcal{M}}^m}(c_1, \ldots, c_k) = c_i$, so

$$\begin{aligned} p^{\mathbb{A}_{\mathcal{M}}^m}(u_1, \ldots, u_n) &= t^{\mathbb{A}_{\mathcal{M}}^m}(\ldots, q^{\mathbb{A}_{\mathcal{M}}^m}(u_1, \ldots, u_n), \ldots) \\ &= t^{\mathbb{A}_{\mathcal{M}}^m}(\ldots, c_i, \ldots) \\ &= t^{\mathbb{A}_{\mathcal{M}}^m}(\ldots, s_i^{\mathbb{A}_{\mathcal{M}}^m}(u_1, \ldots, u_n), \ldots) \\ &= p'^{\mathbb{A}_{\mathcal{M}}^m}(u_1, \ldots, u_n). \end{aligned}$$

Thus, $p'^{\mathbb{A}_{\mathcal{M}}^m}(u_1, \ldots, u_n) = w$. Further, $\mathfrak{T}_{p'}$ has fewer vertices with labels from $\mathcal{H}$ than $\mathfrak{T}_p$, which contradicts the choice of the term p.

Thus, it must be that $\bigcap_{j=1}^m B_j = \emptyset$. For each $1 \leq j \leq m$, let $\overline{c}|_j = (c_1, \ldots, c_k)|_j$. Since $h^{\mathbb{A}_{\mathcal{M}}^m}(c_1, \ldots, c_k)|_j \neq 0$, there exist $(x_1^j, \ldots, x_k^j) \in P_{\overline{c}|_j}$ and $1 \leq \ell \leq k$ such that $\Sigma \vdash h(x_1^j, \ldots, x_k^j) \approx x_\ell^j$. In particular, $\ell \in B_j$. Define $\gamma_j \colon \{x_1^j, \ldots, x_k^j\} \to \{x, y\}$, for distinct variables $x, y \in X$, by

$$\gamma_j(x_i^j) = \begin{cases} y & \text{if } i \in B_j \\ x & \text{otherwise.} \end{cases}$$

This map is well-defined since $x_r^j = x_s^j$ if and only if $c_r|_j = c_s|_j$, which implies $(r \in B_j \iff s \in B_j)$. Then computing $h[\gamma_j]$ for all $1 \leq j \leq m$ and using entailment property (4), we have that

$$\Sigma \vdash h \begin{pmatrix} \gamma_1(x_1^1) & \gamma_1(x_2^1) & \ldots & \gamma_1(x_k^1) \\ \gamma_2(x_1^2) & \gamma_2(x_2^2) & \ldots & \gamma_2(x_k^2) \\ & & \vdots & \\ \gamma_m(x_1^m) & \gamma_m(x_2^m) & \ldots & \gamma_m(x_k^m) \end{pmatrix} \approx \begin{pmatrix} y \\ y \\ \vdots \\ y \end{pmatrix}.$$

Since $\bigcap_{j=1}^m B_j = \emptyset$, no column in the above matrix on the left hand side is the tuple $(y, \ldots, y)$. Thus, Σ entails cube identities for h. This is also a contradiction, so we must have that p is a term in the language $\mathcal{F}$. ■

Thus, if $b \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}_{\mathcal{M}}^m}$, then there is a term $p(x_1, \ldots, x_n)$ in the language $\mathcal{F}$ such that $p^{\mathbb{A}_{\mathcal{M}}^m}(a_1, \ldots, a_n) = b$. Since $a_1, \ldots, a_n \in A^m$, we have $p^{\mathbb{A}_{\mathcal{M}}^m}(a_1, \ldots, a_n) = p^{\mathbb{A}^m}(a_1, \ldots, a_n)$, so

$b \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m}$. We have thus shown that SMP($\mathbb{A}_{\mathcal{M}}$) is at least as hard as SMP($\mathbb{A}$), which completes the proof of statement (i) of Theorem 4.1.

(ii) Let $\mathbb{B}$ be the finite algebra of Kozik [17] for which SMP($\mathbb{B}$) is EXPTIME-complete. Then by statement (i) of the theorem, there exists a finite algebra $\mathbb{B}_{\mathcal{M}}$ such that $\mathbb{B}_{\mathcal{M}} \models \Sigma$ and SMP($\mathbb{B}_{\mathcal{M}}$) is at least as hard as SMP($\mathbb{B}$). Since the subpower membership problem can always be answered in EXPTIME, it follows that SMP($\mathbb{B}_{\mathcal{M}}$) is EXPTIME-complete. □

4.2 Applications

We discuss some consequences of Theorem 4.1. We will prove a characterization of consistent strong linear Maltsev conditions which do not imply the existence of a cube term, similar to the results of Opršal [21] and Moore and McKenzie [19]. We will use this characterization along with Theorem 4.1 to show there exist examples of finite algebras which generate congruence distributive and congruence k-permutable ($k \geq 3$) varieties whose SMP is EXPTIME-complete. Before stating and proving the corollaries, we first recall some definitions and notation.

Let $\mathcal{V}$ and $\mathcal{W}$ be two varieties, and let $\{f_i\}_{i \in I}$ be the language of $\mathcal{V}$. We recall that $\mathcal{V}$ **is interpretable in** $\mathcal{W}$ if for every operation symbol f_i, there is a term t_i (of the same arity) in the language of $\mathcal{W}$ such that for all $\mathbb{A} \in \mathcal{W}$, the algebra $\langle A; \{t_i^{\mathbb{A}}\}_{i \in I} \rangle$ is a member of $\mathcal{V}$. If $\mathcal{V}$ is interpretable in $\mathcal{W}$, we write $\mathcal{V} \leq \mathcal{W}$. For a strong Maltsev condition $\mathcal{M} = (\mathcal{H}, \Sigma)$, we denote the variety determined by Σ by $\mathcal{V}_{\mathcal{M}}$.

The **dual algebra** of the 2-element implication algebra (with a constant) $\mathbb{I} = \langle \{0,1\}; \{\to, \mathbf{1}\} \rangle$ is the algebra $\mathbb{I}^{\mathrm{d}} = \langle \{0,1\}; \{\to^{\mathrm{d}}, \mathbf{0}\} \rangle$, where the operation $\to^{\mathrm{d}}$ is binary and is obtained from the operation table of $\to$ by permuting 0 and 1 (see Table 4.1), and $\mathbf{0}$ is the constant 0 operation.

$\to^{\mathrm{d}}$	0	1
0	0	1
1	0	0

Table 4.1: The operation table for $\to^{\mathrm{d}}$.

Corollary 4.4. *If $\mathcal{M} = (\mathcal{H}, \Sigma)$ is a strong linear Maltsev condition, then the following are equivalent:*

(i) *$\mathcal{M}$ is consistent and Σ does not entail the existence of cube identities for any $h \in \mathcal{H}$.*

(ii) $\mathcal{V}_{\mathcal{M}} \leq \mathcal{V}(\mathbb{I}^{\mathrm{d}})$.

Proof. (i) $\Rightarrow$ (ii) Let $\mathbb{A} = \langle \{1\}; \emptyset \rangle$ be the 1-element algebra whose language is the empty set. Let $\mathbb{A}_{\mathcal{M}} = \langle \{0,1\}; \mathcal{H} \rangle$ be the constructed algebra of Theorem 4.1. For any positive integer m and tuples $a_1, \ldots, a_n \in \{0,1\}^m$, by Claim 4.3 we see that if $(1, \ldots, 1) \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}_{\mathcal{M}}^m}$, then there is a term p in the language $\emptyset$ such that $p^{\mathbb{A}_{\mathcal{M}}^m}(a_1, \ldots a_n) = (1, \ldots, 1)$; that is, $a_i = (1, \ldots, 1)$ for some $1 \leq i \leq n$. Thus, the operations of $\mathbb{A}_{\mathcal{M}}$ preserve the relation $R_m = \{0,1\}^m \setminus (1, \ldots, 1)$ for all $m \geq 1$.

Let $\mathbf{R}$ be the relational structure $\langle \{0,1\}; \{R_m\}_{m \geq 1} \rangle$. Let $\mathrm{Pol}(\mathbf{R})$ denote the set of all operations of arity at least one which preserve the relations of $\mathbf{R}$, and define $\mathrm{Pol}^{\mathbf{0}}(\mathbf{R}) = \mathrm{Pol}(\mathbf{R}) \cup \{\mathbf{0}\}$. Let $\mathrm{Clo}(\mathbb{I}^{\mathrm{d}})$ denote the clone of term operations of $\mathbb{I}^{\mathrm{d}}$. Since the operations of $\mathbb{A}_{\mathcal{M}}$ are a subset of $\mathrm{Pol}^{\mathbf{0}}(\mathbf{R})$ and $\mathrm{Pol}^{\mathbf{0}}(\mathbf{R}) = \mathrm{Clo}(\mathbb{I}^{\mathrm{d}})$ [23], for every $h \in \mathcal{H}$ of arity k, there is a term t_h of arity k in the language of $\mathbb{I}^{\mathrm{d}}$ such that $h^{\mathbb{A}_{\mathcal{M}}}(c_1, \ldots, c_k) = t_h^{\mathbb{I}^{\mathrm{d}}}(c_1, \ldots, c_k)$ for all $(c_1, \ldots, c_k) \in \{0,1\}^k$. Note that we required $\mathbf{0}$ be an operation of $\mathbb{I}^{\mathrm{d}}$ so that if $h \in \mathcal{H}$ is 0-ary, then t_h can be taken to be $\mathbf{0}$. Thus, $\langle \{0,1\}; \{t_h^{\mathbb{I}^{\mathrm{d}}}\}_{h \in \mathcal{H}} \rangle \models \Sigma$. If $\mathbb{B} \in \mathcal{V}(\mathbb{I}^{\mathrm{d}})$, then $\mathbb{B}$ satisfies all identities satisfied by $\mathbb{I}^{\mathrm{d}}$, so $\langle B; \{t_h^{\mathbb{B}}\}_{h \in \mathcal{H}} \rangle \models \Sigma$. This implies that $\langle B; \{t_h^{\mathbb{B}}\}_{h \in \mathcal{H}} \rangle \in \mathcal{V}_{\mathcal{M}}$. Hence, $\mathcal{V}_{\mathcal{M}} \leq \mathcal{V}(\mathbb{I}^{\mathrm{d}})$.

(ii) $\Rightarrow$ (i) If $\mathcal{V}_{\mathcal{M}} \leq \mathcal{V}(\mathbb{I}^{\mathrm{d}})$, then for each operation symbol $h \in \mathcal{H}$ there is a term t_h in the language of $\mathbb{I}^{\mathrm{d}}$ such that the algebra $\mathbb{A} = \langle \{0,1\}; \{t_h^{\mathbb{I}^{\mathrm{d}}}\}_{h \in \mathcal{H}} \rangle$ is a member of $\mathcal{V}_{\mathcal{M}}$. Thus $\mathcal{M}$ is consistent. Since $\mathrm{Pol}^{\mathbf{0}}(\mathbf{R}) = \mathrm{Clo}(\mathbb{I}^{\mathrm{d}})$ [23], the tuples $\{0,1\}^m \setminus (1, \ldots, 1)$ are the element set of a subalgebra of $(\mathbb{I}^{\mathrm{d}})^m$ for all $m \geq 1$. Thus, $\mathbb{I}^{\mathrm{d}}$ does not have a cube term, so $\mathbb{A}$ cannot have a cube term. Thus, Σ does not entail the existence of cube identities for any $h \in \mathcal{H}$. □

We may quasi-order strong linear Maltsev conditions by interpretability. That is, we say $\mathcal{M}_1 \leq \mathcal{M}_2$ if and only if $\mathcal{V}_{\mathcal{M}_1} \leq \mathcal{V}_{\mathcal{M}_2}$. By identifying varieties which interpret into each other, this becomes a partial order. If $\mathcal{M}_1 \leq \mathcal{M}_2$, we say $\mathcal{M}_2$ is **stronger** than $\mathcal{M}_1$.

Given a finite index set J and finitely many strong linear Maltsev conditions indexed by J, $\mathcal{M}_j = (\mathcal{H}_j, \Sigma_j)$, we may form a new strong linear Maltsev condition $\mathcal{M} = (\bigcup_{j\in J} \mathcal{H}_j, \bigcup_{j\in J} \Sigma_j)$.

Lemma 4.5. *If $\mathcal{H}_i \cap \mathcal{H}_j = \emptyset$ for all $i \neq j$, then the following are equivalent:*

(i) *For all $j \in J$, $\mathcal{M}_j$ is consistent and Σ_j does not entail the existence of cube identities for any $h \in \mathcal{H}_j$.*

(ii) *For all $j \in J$, $\mathcal{V}_{\mathcal{M}_j} \leq \mathcal{V}(\mathbb{I}^{\mathrm{d}})$.*

(iii) $\mathcal{V}_{\mathcal{M}} \leq \mathcal{V}(\mathbb{I}^{\mathrm{d}})$.

(iv) *$\mathcal{M}$ is consistent and $\bigcup_{j\in J} \Sigma_j$ does not entail the existence of cube identities for any $h \in \bigcup_{j\in J} \mathcal{H}_j$.*

Proof. The equivalences (i) $\iff$ (ii) and (iii) $\iff$ (iv) follow from Corollary 4.4. We now show (ii) $\iff$ (iii).

If we assume, for all $j \in J$, there is a map from $\mathcal{H}_j$ to terms in the language of $\mathcal{V}(\mathbb{I}^{\mathrm{d}})$, then we have an induced map from $\bigcup_{j\in J} \mathcal{H}_j$ to terms in the language of $\mathbb{I}^{\mathrm{d}}$. The induced map is well-defined since $\mathcal{H}_i \cap \mathcal{H}_j = \emptyset$ for all $i \neq j$. If we assume there is a map from $\bigcup_{j\in J} \mathcal{H}_j$ to terms in the language of $\mathbb{I}^{\mathrm{d}}$, then for all $j \in J$ we have an induced map from $\mathcal{H}_j$ to terms in the language of $\mathbb{I}^{\mathrm{d}}$ by restriction.

Let $\mathbb{A} \in \mathcal{V}(\mathbb{I}^{\mathrm{d}})$. The algebra $\langle A; \{t_h^{\mathbb{A}}\}_{h\in\mathcal{H}_j}\rangle$ satisfies the identities in Σ_j for all $j \in J$ if and only if the algebra $\langle A; \{t_h^{\mathbb{A}}\}_{h\in\bigcup_{j\in J}\mathcal{H}_j}\rangle$ satisfies the identities in $\bigcup_{j\in J} \Sigma_j$. Thus

$$\langle A; \{t_h^{\mathbb{A}}\}_{h\in\mathcal{H}_j}\rangle \in \mathcal{V}_{\mathcal{M}_j} \text{ for all } j \in J \iff \langle A; \{t_h^{\mathbb{A}}\}_{h\in\bigcup_{j\in J}\mathcal{H}_j}\rangle \in \mathcal{V}_{\mathcal{M}},$$

which shows $\mathcal{V}_{\mathcal{M}_j} \leq \mathcal{V}(\mathbb{I}^{\mathrm{d}})$ for all $j \in J$ if and only if $\mathcal{V}_{\mathcal{M}} \leq \mathcal{V}(\mathbb{I}^{\mathrm{d}})$. □

Thus from finitely many strong linear Maltsev conditions for which Theorem 4.1 applies, we may produce a stronger strong linear Maltsev condition for which Theorem 4.1 applies. We will use this strategy to obtain examples of finite algebras in varieties that are congruence distributive and congruence k-permutable ($k \geq 3$) whose subpower membership problem is EXPTIME-complete.

We first recall several important facts from Examples 2.4 and 2.5. B. Jónsson [14] characterized congruence distributive varieties by the existence of an integer $k \geq 1$ and ternary terms $d_0, \ldots, d_k$ which satisfy the set of identities from Example 2.4. Recall that the terms $d_0, \ldots, d_k$ are referred to as **Jónsson terms**, and $\mathrm{CD}(k)$ is often used to refer to the class of algebras which have Jónsson terms $d_0, \ldots, d_k$.

J. Hagemann and A. Mitschke [12] characterized congruence k-permutable varieties by the existence of ternary terms $p_0, \ldots, p_k$ which satisfy the set of identities from Example 2.5. Recall that the terms $p_0, \ldots, p_k$ are referred to as **Hagemann–Mitschke terms**, and $\mathrm{CP}(k)$ is often used to refer to the class of algebras which have Hagemann–Mitschke terms $p_0, \ldots, p_k$.

The sequence of the classes $\mathrm{CD}(k)$ (respectively, $\mathrm{CP}(k)$) is an increasing sequence; that is, if $\mathbb{A}$ is a member of $\mathrm{CD}(k)$ (respectively, $\mathrm{CP}(k)$), $\mathbb{A}$ is also a member of $\mathrm{CD}(\ell)$ (respectively, $\mathrm{CP}(\ell)$) for all $\ell > k$.

An algebra is in $\mathrm{CD}(1)$ if and only if it is trivial, and is in $\mathrm{CD}(2)$ if and only if it has a majority term operation. If an algebra is in $\mathrm{CP}(2)$ and is also in a congruence distributive variety, then the algebra has a majority term operation [22]. Thus, every finite algebra which satisfies one of these properties has a subpower membership problem in P by the Baker–Pixley theorem [1].

Corollary 4.6. *If $k \geq 3$ and $\ell \geq 3$, then there exists a finite algebra $\mathbb{A} \in \mathrm{CD}(k) \cap \mathrm{CP}(\ell)$ such that* $\mathrm{SMP}(\mathbb{A})$ *is* EXPTIME*-complete.*

Proof. Let $\mathcal{M}_1 = (\mathcal{H}_1, \Sigma_1)$ be the strong linear Maltsev condition for $\mathrm{CD}(3)$. Note that the boolean operation $\wedge$ is a term operation of $\mathbb{I}^{\mathrm{d}}$ given by $x \wedge y = (x \to^{\mathrm{d}} y) \to^{\mathrm{d}} y$. It is straightforward to check that the term operations

$$d_1(x, y, z) = ((y \to^{\mathrm{d}} x) \wedge (z \to^{\mathrm{d}} x)) \to^{\mathrm{d}} x,$$
$$d_2(x, y, z) = (x \to^{\mathrm{d}} y) \to^{\mathrm{d}} z,$$

and the projections d_0 and d_3 satisfy the identities of $\mathrm{CD}(3)$, and so $\mathcal{V}_{\mathcal{M}_1} \leq \mathcal{V}(\mathbb{I}^{\mathrm{d}})$. By Corollary 4.4, $\mathcal{M}_1$ is consistent and Σ_1 does not entail the existence of cube identities for any $h \in \mathcal{H}_1$.

Let $\mathcal{M}_2 = (\mathcal{H}_2, \Sigma_2)$ be the strong linear Maltsev condition for CP(3). It is straightforward to check that the term operations

$$p_1(x, y, z) = (z \to^{\mathrm{d}} y) \to^{\mathrm{d}} x,$$

$$p_2(x, y, z) = (x \to^{\mathrm{d}} y) \to^{\mathrm{d}} z,$$

and the projections p_0 and p_3 satisfy the identities of CP(3), and so $\mathcal{V}_{\mathcal{M}_2} \leq \mathcal{V}(\mathbb{I}^{\mathrm{d}})$. By Corollary 4.4, $\mathcal{M}_2$ is consistent and Σ_2 does not entail the existence of cube identities for any $h \in \mathcal{H}_2$.

By Lemma 4.5, $\mathcal{M} = (\mathcal{H}_1 \cup \mathcal{H}_2, \Sigma_1 \cup \Sigma_2)$ is consistent and $\Sigma_1 \cup \Sigma_2$ does not entail the existence of cube identities for any $h \in \mathcal{H}_1 \cup \mathcal{H}_2$. Then by Theorem 4.1(ii), there exists $\mathbb{B}_{\mathcal{M}} \in \mathrm{CD}(3) \cap \mathrm{CP}(3)$ (thus in $\mathrm{CD}(k) \cap \mathrm{CP}(\ell)$ for $k, \ell \geq 3$) such that $\mathrm{SMP}(\mathbb{B}_{\mathcal{M}})$ is EXPTIME-complete. □

Chapter 5

An upper bound for the complexity of SMP($\mathbb{A}_{\mathcal{M}}$)

For any finite algebra $\mathbb{A}$, we know from Theorem 4.1(i) that if we expand $\mathbb{A}$ to the algebra $\mathbb{A}_{\mathcal{M}}$ that satisfies a strong linear Maltsev condition $\mathcal{M}$ which does not imply the existence of a cube term, the subpower membership problem for the expanded algebra is at least as hard as the subpower membership problem for the original algebra. It is natural to ask about the upper bound for the complexity of the problem SMP($\mathbb{A}_{\mathcal{M}}$). In this chapter, we prove the following theorem:

Theorem 5.1. *Let $\mathbb{A} = \langle A; \mathcal{F} \rangle$ be any finite algebra, and $\mathcal{M} = (\mathcal{H}, \Sigma)$ be a consistent strong linear Maltsev condition such that Σ does not entail cube identities for any $h \in \mathcal{H}$. If $\mathcal{H}$ has a 0-ary operation symbol $\mathbf{0}$ and a ternary operation symbol d such that*

- $\Sigma \vdash d(x, x, y) \approx x$,
- $\Sigma \vdash d(x, y, x) \approx x$, *and*
- $\Sigma \nvdash d(x, y, y) \approx x$,

then the problem SMP($\mathbb{A}$) *is polynomial time equivalent to the problem* SMP($\mathbb{A}_{\mathcal{M}}$).

From Theorem 4.1, we know SMP($\mathbb{A}_{\mathcal{M}}$) is at least as hard as SMP($\mathbb{A}$). We will now turn our attention to proving that SMP($\mathbb{A}$) is at least as hard SMP($\mathbb{A}_{\mathcal{M}}$).

We will be computing with a 0-ary symbol and a ternary symbol in $\mathbb{A}_{\mathcal{M}}$ or a direct power of $\mathbb{A}_{\mathcal{M}}$, so we record the interpretation of these symbols in $\mathbb{A}_{\mathcal{M}}$ according to the construction in Theorem 4.1:

Lemma 5.2. *Let* $\mathbf{0}$ *be a* 0*-ary operation symbol and* d *a ternary operation symbol which satisfies the conditions of Theorem 5.1. In* $\mathbb{A}_{\mathcal{M}}$*, we have* $\mathbf{0}^{\mathbb{A}_{\mathcal{M}}} = 0$ *and*

$$d^{\mathbb{A}_{\mathcal{M}}}(x_1, x_2, x_3) = \begin{cases} x_1 & \text{if } x_1 = x_2 \text{ or } x_1 = x_3 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. All 0-ary operation symbols are mapped to 0 according to the construction in Theorem 4.1, so $\mathbf{0}^{\mathbb{A}_{\mathcal{M}}} = 0$. Since $\Sigma \vdash d(x, x, y) \approx x$ and $\Sigma \vdash d(x, y, x) \approx x$ by assumption, we have that $d^{\mathbb{A}_{\mathcal{M}}}(x_1, x_2, x_3) = x_1$ if $x_1 = x_2$ or $x_1 = x_3$. Finally, $\Sigma \nvdash d(x, y, y) \approx x$ by assumption, $\Sigma \nvdash d(x, y, y) \approx y$ since Σ does not entail cube identities for d, and $\Sigma \nvdash d(x, y, y) \approx z$ for any other variable z since $\mathcal{M}$ is consistent. Thus, Σ also does not entail that $d(x, y, z)$ equals a variable for distinct variables x, y, z, so $d^{\mathbb{A}_{\mathcal{M}}}(x_1, x_2, x_3) = 0$ if $x_1 \neq x_2 = x_3$ or $x_1 \neq x_2 \neq x_3$. □

The algebra in which we are performing computations will be clear from context, so we will simply write d instead of $d^{\mathbb{A}_{\mathcal{M}}}$ or $d^{\mathbb{A}^m_{\mathcal{M}}}$. Recall that to finish the proof that SMP($\mathbb{A}$) is polynomial time equivalent to SMP($\mathbb{A}_{\mathcal{M}}$), we must show that SMP($\mathbb{A}$) is at least as hard as SMP($\mathbb{A}_{\mathcal{M}}$). To achieve this, we will prove Theorem 5.3 stated below. This characterization will be used to construct a polynomial time reduction from SMP($\mathbb{A}_{\mathcal{M}}$) to SMP($\mathbb{A}$).

Theorem 5.3. *Let* $\mathbb{A}$ *be any finite algebra, and* $\mathcal{M}$ *a consistent strong linear Maltsev condition which satisfies the conditions of Theorem 5.1. Let* $a_1, \ldots, a_n, b \in (A \cup \{0\})^m$ *be an* SMP($\mathbb{A}_{\mathcal{M}}$) *instance. Let* $[m]$ *denote the set* $\{1, \ldots, m\}$*, and define* $J = \{i \in [m] \mid b|_i = 0\}$*. Let* $\{i_1, \ldots i_\ell\} \subseteq \{1, \ldots, n\}$ *be the set of all subscripts such that* $a_{i_1}|_{[m]\setminus J}, \ldots, a_{i_\ell}|_{[m]\setminus J} \in A^{|[m]\setminus J|}$*. The following are equivalent:*

(1) $b \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$.

(2) *The projection* $b|_{[m]\setminus J}$ *satisfies* $b|_{[m]\setminus J} \in \langle a_{i_1}|_{[m]\setminus J}, \ldots, a_{i_\ell}|_{[m]\setminus J} \rangle_{\mathbb{A}^{|[m]\setminus J|}}$*, and for all* $i \in [m]\setminus J$ *and* $j \in J$*, the projection* $b|_{\{i,j\}}$ *satisfies* $b|_{\{i,j\}} \in \langle a_1|_{\{i,j\}}, \ldots, a_n|_{\{i,j\}} \rangle_{\mathbb{A}^2_{\mathcal{M}}}$.

Proof. (1) ⇒ (2) If $b \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$, then we must have that for all $i \in [m] \setminus J$ and $j \in J$, the projection $b|_{\{i,j\}}$ satisfies $b|_{\{i,j\}} \in \langle a_1|_{\{i,j\}}, \ldots, a_n|_{\{i,j\}} \rangle_{\mathbb{A}^2_{\mathcal{M}}}$. Further, since $a_1|_{[m]\setminus J}, \ldots, a_n|_{[m]\setminus J} \in$

$(A \cup \{0\})^{|[m]\setminus J|}$, $b|_{[m]\setminus J} \in A^{|[m]\setminus J|}$, and $b|_{[m]\setminus J} \in \langle a_1|_{[m]\setminus J}, \ldots, a_n|_{[m]\setminus J}\rangle_{\mathbb{A}_{\mathcal{M}}^{|[m]\setminus J|}}$, by Claim 4.3, there is a term $p(x_1, \ldots, x_n)$ in the language $\mathcal{F}$ such that $p^{\mathbb{A}_{\mathcal{M}}^{|[m]\setminus J|}}(a_1|_{[m]\setminus J}, \ldots, a_n|_{[m]\setminus J}) = b|_{[m]\setminus J}$. But since 0 is an absorbing element for all $f \in \mathcal{F}$ and $b|_{[m]\setminus J} \in A^{|[m]\setminus J|}$, the term p must only depend on the variables in $\{x_{i_1}, \ldots, x_{i_\ell}\}$. Thus, there is a term $p'(x_1, \ldots, x_\ell)$ in the language $\mathcal{F}$ such that $p'^{\mathbb{A}_{\mathcal{M}}^{|[m]\setminus J|}}(a_{i_1}|_{[m]\setminus J}, \ldots, a_{i_\ell}|_{[m]\setminus J}) = b|_{[m]\setminus J}$, so $b|_{[m]\setminus J} \in \langle a_{i_1}|_{[m]\setminus J}, \ldots, a_{i_\ell}|_{[m]\setminus J}\rangle_{\mathbb{A}^{|[m]\setminus J|}}$ as desired.

(2) $\Rightarrow$ (1) If $J = [m]$ (that is, b is the all 0-tuple), then $b \in \langle a_1, \ldots, a_n\rangle_{\mathbb{A}_{\mathcal{M}}^m}$ since $\mathbf{0}$ (the constant 0 operation) is an operation of $\mathbb{A}_{\mathcal{M}}$. If $J = \emptyset$, then $b|_{[m]\setminus J} = b$, so $b \in \langle a_1, \ldots, a_n\rangle_{\mathbb{A}_{\mathcal{M}}^m}$ by assumption. So we assume J is nonempty and $J \neq [m]$. We first present a method of generating m-tuples which approximate b. Specifically, for every $j \in J$, we will show there is an m-tuple $c_j \in \langle a_1, \ldots, a_n\rangle_{\mathbb{A}_{\mathcal{M}}^m}$ for which $c_j|_j = 0$ and c_j agrees with b in all coordinates of $[m] \setminus J$. We will do this by induction on the size of subsets of $[m] \setminus J$.

Claim 5.4. *For every $j \in J$, there is an m-tuple $c_j \in \langle a_1, \ldots, a_n\rangle_{\mathbb{A}_{\mathcal{M}}^m}$ such that*

- $c_j|_i = b|_i$ *if* $i \in [m] \setminus J$, *and*
- $c_j|_j = 0$.

Proof of Claim 5.4. To prove the claim, we prove the following stronger statement:

> For every $j \in J$ and for every nonempty subset $K \subseteq [m] \setminus J$, there is an m-tuple $c_j \in \langle a_1, \ldots, a_n\rangle_{\mathbb{A}_{\mathcal{M}}^m}$ such that
>
> - $c_j|_i = b|_i$ if $i \in K$, and
> - $c_j|_j = 0$.
>
> (†)

We will prove (†) by induction on $|K|$, and the claim will follow by letting $K = [m] \setminus J$.

For the base case, let $j \in J$ and $i \in [m] \setminus J$. By assumption, $b|_{\{i,j\}} \in \langle a_1|_{\{i,j\}}, \ldots, a_n|_{\{i,j\}}\rangle_{\mathbb{A}_{\mathcal{M}}^2}$. Thus, there exists $c_j \in \langle a_1, \ldots, a_n\rangle_{\mathbb{A}_{\mathcal{M}}^m}$ such that $c_j|_{\{i,j\}} = b|_{\{i,j\}}$. That is,

$$c_j|_i = b|_i$$

and

$$c_j|_j = b|_j = 0.$$

This completes the proof of the base case.

Let $j \in J$ and $|K| > 1$. We assume that for any nonempty subset K' of $[m] \setminus J$ of size strictly smaller than $|K|$, there is an m-tuple in $\langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$ satisfying the conditions of (†). Choose $k \in K$. Using the induction hypothesis on the sets $\{k\}$ and $K \setminus \{k\}$, we know

- there is an m-tuple $s_j \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$ satisfying $s_j|_k = b|_k$ and $s_j|_j = 0$, and
- there is an m-tuple $r_j \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$ satisfying $r_j|_i = b|_i$ for $i \in K \setminus \{k\}$ and $r_j|_j = 0$.

By assumption, $b|_{[m]\setminus J} \in \langle a_{i_1}|_{[m]\setminus J}, \ldots, a_{i_\ell}|_{[m]\setminus J} \rangle_{\mathbb{A}^{|[m]\setminus J|}}$. Thus, there is an m-tuple $b' \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$ such that $b'|_i = b|_i$ for all $i \in [m] \setminus J$. Then we set $c_j = d(b', s_j, r_j)$ and compute

$$\begin{aligned} c_j|_k &= d(b'|_k, s_j|_k, r_j|_k) = d(b|_k, b|_k, *) = b|_k, \\ c_j|_i &= d(b'|_i, s_j|_i, r_j|_i) = d(b|_i, *, b|_i) = b|_i \text{ if } i \in K \setminus \{k\}, \text{ and} \\ c_j|_j &= d(b'|_j, s_j|_j, r_j|_j) = d(*, 0, 0) = 0. \end{aligned}$$

Thus, $c_j \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$ and satisfies the properties of (†). ■

To prove that $b \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$, we prove the following stronger statement:

> For every nonempty subset $K \subseteq J$, there is an m-tuple $t_K \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$ such that
>
> - $t_K|_i = b|_i$ if $i \in [m] \setminus J$, and
> - $t_K|_i = 0$ if $i \in K$.
>
> (‡)

We will prove (‡) by induction on $|K|$, and $b \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$ will follow by letting $K = J$.

For the base case, let $\{j\} \subseteq J$. By Claim 5.4, there an m-tuple $c_j \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$ satisfying $c_j|_i = b_i$ if $i \in [m] \setminus J$ and $c_j|_j = 0$. Setting $t_{\{j\}} = c_j$ completes the base case.

So assume $|K| > 1$, and for every nonempty subset K' of J of size strictly less than $|K|$ there is an m-tuple $t_{K'} \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$ satisfying the conditions of (‡). Choose $k \in K$. Using the induction hypothesis on the sets $\{k\}$ and $K \setminus \{k\}$, we know

- there is an m-tuple $t_{\{k\}} \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$ satisfying $t_{\{k\}}|_i = b|_i$ if $i \in [m] \setminus J$ and $t_{\{k\}}|_k = 0$, and
- there is an m-tuple $t_{K\setminus\{k\}} \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$ satisfying $t_{K\setminus\{k\}}|_i = b|_i$ if $i \in [m] \setminus J$ and $t_{K\setminus\{k\}}|_i = 0$ if $i \in K \setminus \{k\}$.

Then we set $t_K = d(t_{K\setminus\{k\}}, t_{\{k\}}, \mathbf{0})$ and compute

$$t_K|_i = d(t_{K\setminus\{k\}}|_i, t_{\{k\}}|_i, \mathbf{0}|_i) = d(b|_i, b|_i, 0) = b|_i \text{ if } i \in [m] \setminus J,$$
$$t_K|_k = d(t_{K\setminus\{k\}}|_k, t_{\{k\}}|_k, \mathbf{0}|_k) = d(*, 0, 0) = 0, \text{ and}$$
$$t_K|_i = d(t_{K\setminus\{k\}}|_i, t_{\{k\}}|_i, \mathbf{0}|_i) = d(0, *, 0) = 0 \text{ if } i \in K \setminus \{k\}.$$

Thus, $t_K \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$ and satisfies the properties of (‡). □

We are now ready to prove Theorem 5.1.

Proof of Theorem 5.1. From Theorem 4.1, we know SMP($\mathbb{A}_{\mathcal{M}}$) is at least as hard as SMP($\mathbb{A}$). We will now show that SMP($\mathbb{A}$) is at least as hard as SMP($\mathbb{A}_{\mathcal{M}}$) by giving a polynomial time reduction from SMP($\mathbb{A}_{\mathcal{M}}$) to SMP($\mathbb{A}$).

Let $a_1, \ldots, a_n, b \in (A \cup \{0\})^m$ be an instance of SMP($\mathbb{A}_{\mathcal{M}}$). If b is the all 0-tuple, then we conclude that $b \in \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$ since $\mathbf{0}$ (the constant 0 operation) is an operation of $\mathbb{A}_{\mathcal{M}}$. Let $[m]$ denote the set $\{1, \ldots, m\}$, and define $J = \{i \in [m] \mid b|_i = 0\}$. We generate, for all $i \in [m] \setminus J$ and $j \in J$, the full subalgebra $\langle a_1|_{\{i,j\}}, \ldots, a_n|_{\{i,j\}} \rangle_{\mathbb{A}^2_{\mathcal{M}}}$ with a closure algorithm, and check if the projection $b|_{\{i,j\}}$ satisfies $b|_{\{i,j\}} \in \langle a_1|_{\{i,j\}}, \ldots, a_n|_{\{i,j\}} \rangle_{\mathbb{A}^2_{\mathcal{M}}}$. If this condition fails for some $i \in [m] \setminus J$ and $j \in J$, then we conclude $b \notin \langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$. Otherwise, we know for all $i \in [m] \setminus J$ and $j \in J$, the projection $b|_{\{i,j\}}$ satisfies $b|_{\{i,j\}} \in \langle a_1|_{\{i,j\}}, \ldots, a_n|_{\{i,j\}} \rangle_{\mathbb{A}^2_{\mathcal{M}}}$. Each subalgebra of $\mathbb{A}^2_{\mathcal{M}}$ can be generated in constant time $\mathcal{O}((|A| + 1)^2)$, and the number of subalgebras we must generate is bounded by m^2. Thus, this step may be completed in time $\mathcal{O}(m^2)$.

Let $\{i_1, \ldots i_\ell\} \subseteq \{1, \ldots, n\}$ be the set of all subscripts such that $a_{i_1}|_{[m]\setminus J}, \ldots, a_{i_\ell}|_{[m]\setminus J} \in A^{|[m]\setminus J|}$. To determine if b is in the subalgebra $\langle a_1, \ldots, a_n \rangle_{\mathbb{A}^m_{\mathcal{M}}}$, we form a corresponding instance

$a_{i_1}|_{[m]\setminus J}, \ldots, a_{i_\ell}|_{[m]\setminus J}, b|_{[m]\setminus J} \in A^{|[m]\setminus J|}$ of SMP($\mathbb{A}$). To form this instance, we run through the m coordinates of the tuple b and determine the nonempty set $[m]\setminus J$. Then for each of the n generators, we run through the coordinates in $[m] \setminus J$ to determine the tuples $a_{i_1}|_{[m]\setminus J}, \ldots, a_{i_\ell}|_{[m]\setminus J}$. This can be done in time $\mathcal{O}((n+1)m)$. We check the answer of the instance $a_{i_1}|_{[m]\setminus J}, \ldots, a_{i_\ell}|_{[m]\setminus J}, b|_{[m]\setminus J} \in A^{|[m]\setminus J|}$ of SMP($\mathbb{A}$). Since the input passed the tests described in the preceding paragraph, we know from Theorem 5.3 that $b \in \langle a_1, \ldots, a_n\rangle_{\mathbb{A}_{\mathcal{M}}^m}$ if and only if $b|_{[m]\setminus J} \in \langle a_{i_1}|_{[m]\setminus J}, \ldots, a_{i_\ell}|_{[m]\setminus J}\rangle_{\mathbb{A}^{|[m]\setminus J|}}$.

Since the size of the instance of SMP($\mathbb{A}_{\mathcal{M}}$) is $\mathcal{O}((n+1)m)$, we have provided a polynomial time algorithm for either answering the instance of SMP($\mathbb{A}_{\mathcal{M}}$), or transforming the instance of SMP($\mathbb{A}_{\mathcal{M}}$) to a corresponding instance of SMP($\mathbb{A}$). In the latter case, the SMP($\mathbb{A}_{\mathcal{M}}$) instance satisfies that for all $i \in [m] \setminus J$ and $j \in J$, the projection $b|_{\{i,j\}}$ satisfies $b|_{\{i,j\}} \in \langle a_1|_{\{i,j\}}, \ldots, a_n|_{\{i,j\}}\rangle_{\mathbb{A}_{\mathcal{M}}^2}$, so we know from Theorem 5.3 that the SMP($\mathbb{A}_{\mathcal{M}}$) instance has a 'yes' answer if and only if the corresponding SMP($\mathbb{A}$) instance has a 'yes' answer. Thus, SMP($\mathbb{A}$) is at least as hard as SMP($\mathbb{A}_{\mathcal{M}}$). □

Let $\mathcal{M}$ be the strong linear Malstev condition for CD(3) ∩ CP(3) expanded by a new 0-ary operation symbol. It is easy to verify that the ternary symbol d_1 from Example 2.4 satisfies the conditions of Theorem 5.1. We obtain the following corollary as an immediate consequence of Theorems 4.1 and 5.1:

Corollary 5.5. *For every finite algebra $\mathbb{A}$, there exists a finite algebra $\mathbb{A}_{\mathcal{M}} \in$ CD(3) ∩ CP(3) such that* SMP($\mathbb{A}$) *and* SMP($\mathbb{A}_{\mathcal{M}}$) *are polynomial time equivalent.* □

Further, there exists a finite semigroup $\mathbb{S}$ such that SMP($\mathbb{S}$) is NP-complete and a finite semigroup $\mathbb{T}$ such that SMP($\mathbb{T}$) is PSPACE-complete [3]. We obtain the following corollary as an immediate consequence of Corollary 5.5:

Corollary 5.6. *There exist finite algebras $\mathbb{S}_{\mathcal{M}}, \mathbb{T}_{\mathcal{M}} \in$ CD(3) ∩ CP(3) such that*

(1) SMP($\mathbb{S}_{\mathcal{M}}$) *is* NP*-complete, and*

(2) SMP($\mathbb{T}_{\mathcal{M}}$) *is* PSPACE*-complete.* □

Bibliography

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

[2] Joel Berman, Pawel Idziak, Petar Marković, Ralph McKenzie, Matthew Valeriote, and Ross Willard. Varieties with few subalgebras of powers. Transactions of the Amer. Math. Soc., 362(3):1445–1473, 2010.

[3] Andrei Bulatov, Marcin Kozik, Peter Mayr, and Markus Steindl. The subpower membership problem for semigroups. Internat. J. Algebra Comput., 26(7):1435–1451, 2016.

[4] Andrei Bulatov, Peter Mayr, and Ágnes Szendrei. The subpower membership problem for finite algebras with cube terms. In preparation.

[5] S. Burris and H.P. Sankappanavar. A Course in Universal Algebra. The Millenium Edition, 2012.

[6] Victor Dalmau and Peter Jeavons. Learnability of quantified formulas. Theoret. Comput. Sci., 306:485–511, 2003.

[7] A. Day. A characterization of modularity for congruence lattices of algebras. Canad. Math. Bull., 12:167–173, 1969.

[8] Ralph Freese, Emil Kiss, and Matthew Valeriote. Universal Algebra Calculator, 2011. Available at: `www.uacalc.org`.

[9] Merrick Furst, John Hopcroft, and Eugene Luks. Polynomial-time algorithms for permutation groups. In 21st Annual Symposium on Foundations of Computer Science, pages 36–41, Syracuse, N.Y., 1980. IEEE.

[10] O.C. Garcia and W. Taylor. The lattice of interpretability types of varieties. Mem. Amer. Math. Soc., 305, 1984.

[11] Michael Garey and David S. Johnson. Computers and Intractability: A Guide to the Theory of NP-Completeness. W.H. Freeman & Co., New York, NY, 1979.

[12] J. Hagemann and A. Mitschke. On n-permutable congruences. Algebra Universalis, 3:8–12, 1973.

[13] Pawel Idziak, Petar Marković, Ralph McKenzie, Matthew Valeriote, and Ross Willard. Tractability and learnability arising from algebras with few subpowers. SIAM J. Comput., 39(7):3023–3037, 2010.

[14] Bjarni Jónsson. Algebras whose congruence lattices are distributive. Math. Scandinavica, 21:110–121, 1967.

[15] Keith A. Kearnes, Emil W. Kiss, and Ágnes Szendrei. Growth rates of algebras, I: Pointed cube terms. J. Austral. Math. Soc., 101:56–94, 2016.

[16] David Kelly. Basic equations: word problems and Mal'cev conditions. Notices Amer. Math. Soc., 20:A–54, 1973. Abstract 701-08-4.

[17] Marcin Kozik. A finite set of functions with an EXPTIME-complete composition problem. Theoret. Comput. Sci., 407:330–341, 2008.

[18] Peter Mayr. The subpower membership problem for Mal'cev algebras. Internat. J. Algebra Comput., 22(07):1250075, 2012.

[19] Ralph McKenzie and Matthew Moore. Coloring and blockers. In preparation.

[20] M. Olšák. The weakest nontrivial idempotent equations. Bull. London Math. Soc., 49:1028–1047, 2017.

[21] Jakub Opršal. Taylor's modularity conjecture and related problems for idempotent varieties. Order, 2017. https://doi.org/10.1007/s11083-017-9441-4.

[22] Alden F. Pixley. Distributivity and permutability of congruence relations in equational classes of algebras. Proc. Amer. Math. Soc., 14:105–109, 1963.

[23] Emil L. Post. The two-valued iterative systems of mathematical logic. In Annals of Mathematics Studies, volume 5. Princeton University Press, Princeton, N.J., 1941.

[24] Michael Sipser. Introduction to the theory of computation. Thomson Course Technology, Boston, MA, 2006.

[25] Markus Steindl. On semigroups with PSPACE-complete subpower membership problem. arXiv:1604.01757 [math.GR], submitted.

[26] Markus Steindl. The subpower membership problem for bands. J. Algebra, 489:529–551, 2017.

[27] Ross Willard. Four unsolved problems in congruence permutable varieties. In Conference on Order, Algebra, and Logics, Nashville, TN, 2007.