# A POLYNOMIAL-TIME TEST FOR A DIFFERENCE TERM IN AN IDEMPOTENT VARIETY

WILLIAM DEMEO, RALPH FREESE, AND MATTHEW VALERIOTE

Abstract. We consider the following practical question: given a finite algebra $\mathbf{A}$ in a finite language, can we efficiently decide whether the variety generated by $\mathbf{A}$ has a difference term? We answer this question (positively) in the idempotent case and then describe algorithms for constructing difference terms.

## 1. Introduction

A *difference term* for a variety $\mathcal{V}$ is a ternary term $d$ in the language of $\mathcal{V}$ that satisfies the following: if $\mathbf{A} = \langle A, \ldots \rangle \in \mathcal{V}$, then for all $a, b \in A$ we have

$$d^{\mathbf{A}}(a, a, b) = b \quad \text{and} \quad d^{\mathbf{A}}(a, b, b)\ [\theta, \theta]\ a, \tag{1}$$

where $\theta$ is any congruence containing $(a, b)$ and $[\cdot, \cdot]$ denotes the *commutator*. When the relations in (1) hold we call $d^{\mathbf{A}}$ a *difference term operation* for $\mathbf{A}$.

Difference terms are studied extensively in the general algebra literature. (See, for example, [Kea95, KS98, KK13, KSW, KSW16].) There are many reasons to study difference terms, but one obvious reason is because if we know that a variety has a difference term, this fact allows us to deduce some useful properties of the algebras inhabiting that variety. Any variety that has a Mal'tsev term or for which the commutator operation satisfies $[\alpha, \beta] = \alpha \wedge \beta$ has a difference term. (Note that if $\mathbf{A}$ is an *abelian* algebra, which means that $[1_A, 1_A] = 0_A$, then, by the monotonicity of the commutator, $[\theta, \theta] = 0_A$ for all $\theta \in \mathbf{Con}\,\mathbf{A}$, in which case $\mathbf{A}$ (1) says that $d^{\mathbf{A}}$ is a Mal'tsev term operation.)

Difference terms also play a role in recent work of Keith Kearnes, Agnes Szendrei, and Ross Willard. In [KSW16] these authors give a positive answer Jónsson's famous question—whether a variety of finite

*Date*: 2017-11-17.

This research was supported by the National Science Foundation under Grant No. 1500235.



WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

residual bound must be finitely axiomatizable—for the special case in which the variety has a difference term.[1]

Computers have become invaluable as a research tool and have helped to broaden and deepen our understanding of algebraic structures and the varieties they inhabit. This is largely due to the efforts of researchers who, over the last three decades, have found ingenious ways to coax computers into solving challenging abstract algebraic decision problems, and to do so very quickly. To give a couple of examples related to our own work, it is proved in [VW14] (respectively, [FV09]) that deciding whether a finite idempotent algebra generates a variety that is congruence-$n$-permutable (respectively, congruence-modular) is *tractable*.[2] The present paper continues this effort by presenting an efficient algorithm for deciding whether a locally finite idempotent variety has a difference term.

The question that motivated us to begin this project, and whose solution is the main subject of this paper, is the following:

**Problem 1.** Is there a polynomial-time algorithm to decide for a finite, idempotent algebra $\mathbf{A}$ if $\mathbb{V}(\mathbf{A})$ has a difference term?

We note that for arbitrary finite algebras $\mathbf{A}$, the problem of deciding if $\mathbb{V}(\mathbf{A})$ has a difference term is an EXP-time complete problem. This follows from Theorem 9.2 of [FV09].

The remainder of this introduction uses the language of *tame congruence theory* TCT. Many of the terms we use are defined and explained in the next section. For others, see [HM88].

Our solution to Problem 1 exploits the connection between difference terms and TCT that was established by Keith Kearnes in [Kea95].

**Theorem 1** ([Kea95, Theorem 1.1])**.** *The variety $\mathcal{V} = \mathbb{V}(\mathbf{A})$ generated by a finite algebra $\mathbf{A}$ has a difference if and only if $\mathcal{V}$ omits TCT-type **1** and, for all finite algebras $\mathbf{B} \in \mathcal{V}$, the minimal sets of every type **2** prime interval in* $\mathrm{Con}(\mathbf{B})$ *have empty tails.*

It follows from an observation of Bulatov that the problem of deciding if a finite idempotent algebra generates a variety that omits TCT-type **1** is tractable (see Proposition 3.1 of [Val09]). In [FV09], the second and third authors solve an analogous problem by giving a positive answer to the following:

[1] To say a variety has *finite residual bound* is to say there is a finite bound on the size of the subdirectly irreducible members of the variety.

[2] To say that the decision problem is *tractable* is to say that there exists an algorithm for solvng the problem that "scales well" with respect to increasing input size, by which we mean that the number of operations required to reach a correct decision is bounded by a polynomial function of the input size.

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

**Problem 2.** Is there a polynomial-time algorithm to decide for a finite, idempotent algebra $\mathbf{A}$ if $\mathbb{V}(\mathbf{A})$ is congruence modular?

Congruence modularity is characterized by omitting tails and TCT-types **1** and **5**. Omitting **1**'s and **5**'s can be decided by the subtype theorem. The second and third authors also prove in [FV09] that if there is a nonempty tail in $\mathbb{V}(\mathbf{A})$, then there is a nonempty tail "near the bottom." More precisely, suppose $\mathbf{A}$ is a finite idempotent algebra, and suppose $\mathbb{V}(\mathbf{A})$ has nonempty tails but lacks **1**'s and **5**'s. Then a nonempty tail must occur in a 3-generated subalgebra of $\mathbf{A}^2$. The authors use this to prove that congruence modularity is polynomial-time decidable.

However, proving lack of tails uses the fact that a variety omitting **1**'s and **5**'s has a congruence lattice that—modulo the *solvability congruence* (defined below)—is (join) semidistributive. Now, restricting to just testing whether $\mathbb{V}(\mathbf{A})$ omits type-**2** tails is not a problem. So, for example, there is a polynomial-time algorithm for testing if $\mathbb{V}(\mathbf{A})$ omits **1**'s, **5**'s, and type-**2** tails.

## 2. Background, definitions, and notation

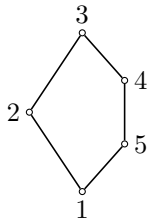
Our starting point is the set of lemmas at the beginning of Section 3 of [FV09]. We first review some of the basic tame congruence theory (TCT) that comes up in the proofs in that paper. (In fact, most of this section is lifted directly from [FV09, Section 2].)

The seminal reference for TCT is the book by Hobby and McKenzie [HM88], according to which, for each covering $\alpha \prec \beta$ in the congruence lattice of a finite algebra $\mathbf{A}$, the local behavior of the $\beta$-classes is captured by the so-called $(\alpha, \beta)$-traces [HM88, Def. 2.15]. Modulo $\alpha$, the induced structure on the traces is limited to one of five possible types:

**1** (unary type) an algebra whose basic operations are permutations;
**2** (affine type) a one-dimensional vector space over some finite field;
**3** (boolean type) a 2-element boolean algebra;
**4** (lattice type) a 2-element lattice;
**5** (semilattice type) a 2-element semilattice.

Thus to each covering $\alpha \prec \beta$ corresponds a "TCT type," denoted by $\mathrm{typ}(\alpha, \beta)$, belonging to the set $\{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}\}$ (see [HM88, Def. 5.1]). The set of all TCT types that are realized by covering pairs of congruences of a finite algebra $\mathbf{A}$ is denoted by $\mathrm{typ}\{\mathbf{A}\}$ and called the *typeset* of $\mathbf{A}$. If $\mathcal{K}$ is a class of algebras, then $\mathrm{typ}\{\mathcal{K}\}$ denotes the union of the typesets of all finite algebras in $\mathcal{K}$. TCT types are ordered according to the following "lattice of types:"

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)




Whether or not $\mathbb{V}(\mathbf{A})$ omits one of the order ideals of the lattice of types can be determined locally. This is spelled out for us in the next proposition. (A *strictly simple* algebra is a simple algebra with no non-trivial subalgebras.)

**Proposition 2** ([FV09, Proposition 2.1])**.** *If* $\mathbf{A}$ *is a finite idempotent algebra and* $\mathbf{i} \in \operatorname{typ}(\mathbb{V}(\mathbf{A}))$ *then there is a finite strictly simple algebra* $\mathbf{S}$ *of type* $\mathbf{j}$ *for some* $\mathbf{j} \leqslant \mathbf{i}$ *in* $\mathsf{HS}(\mathbf{A})$*. The possible cases are*

- $\mathbf{j} = 1 \Rightarrow \mathbf{S}$ *is term equivalent to a 2-element set*
- $\mathbf{j} = 2 \Rightarrow \mathbf{S}$ *is term equivalent to the idempotent reduct of a module*
- $\mathbf{j} = 3 \Rightarrow \mathbf{S}$ *is functionally complete*
- $\mathbf{j} = 4 \Rightarrow \mathbf{S}$ *is polynomially equivalent to a 2-element lattice*
- $\mathbf{j} = 5 \Rightarrow \mathbf{S}$ *is term equivalent to a 2-element semilattice.*

*Proof.* This is a combination of [Val09, Proposition 3.1] and [Sze92, Theorem 6.1]. □

We conclude this section with a result that will be useful in Section 3.

**Corollary 3** ([FV09, Corollary 2.2, Lemma 3.3])**.** *Let* $\mathbf{A}$ *be a finite idempotent algebra and* $T$ *an order ideal in the lattice of types. Then* $\mathbb{V}(\mathbf{A})$ *omits* $T$ *if and only if* $\mathsf{S}(\mathbf{A})$ *does.*

## 3. Prior Work

In [FV09], Corollary 3 is the starting point of the development of a polynomial-time algorithm that determines if a given finite idempotent algebra generates a congruence modular variety.

According to the characterization in [HM88, Chapter 8] of locally finite congruence modular (resp., distributive) varieties, a finite algebra $\mathbf{A}$ generates a congruence modular (resp., distributive) variety $\mathcal{V}$ if and only if the typeset of $\mathcal{V}$ is contained in $\{\mathbf{2}, \mathbf{3}, \mathbf{4}\}$ (resp., $\{\mathbf{3}, \mathbf{4}\}$) and all minimal sets of prime quotients of finite algebras in $\mathcal{V}$ have empty tails [HM88, Def. 2.15]. (In the distributive case the empty tails condition is equivalent to the minimal sets all having exactly two elements.)

It follows from Corollary 3 and Proposition 2 that if $\mathbf{A}$ is idempotent then one can test the first condition—omitting types $\mathbf{1}$, $\mathbf{5}$ (resp., $\mathbf{1}$,

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

**2**, **5**)—by searching for a 2-generated subalgebra of $\mathbf{A}$ whose typeset is not contained in $\{\mathbf{2}, \mathbf{3}, \mathbf{4}\}$ (resp., $\{\mathbf{3}, \mathbf{4}\}$). It is proved in [FV09, Section 6] that this test can be performed in polynomial-time—that is, the running time of the test is bounded by a polynomial function of the size of $\mathbf{A}$. The main tools developed to this end are presented in [FV09, Section 3] as a sequence of lemmas that enable the authors to prove the following: if $\mathbf{A}$ is finite and idempotent, and if $\mathcal{V} = \mathbb{V}(\mathbf{A})$ omits types **1** and **5**, then to test for the existence of nonempty tails in $\mathcal{V}$ it suffices to look for them in the 3-generated subalgebras of $\mathbf{A}^2$. In other words, either there are no nonempty tails or else there are nonempty tails that are easy to find (since they occur in a 3-generated subalgebra of $\mathbf{A}^2$). It follows that Problem 2 has a positive answer: deciding whether or not a finite idempotent algebra generates a congruence modular variety is tractable.[3]

Our goal is to use the same strategy to solve Problem 1. As such, we revisit each of the lemmas in Section 3 of [FV09], and consider whether an analogous result can be proved under modified hypotheses. Specifically, we retain the assumption that the type set of $\mathbb{V}(\mathbf{A})$ omits **1**, but we drop the assumption that it omits **5**. We will attempt to prove that, under these circumstances, either there are no type-**2** tails in $\mathbb{V}(\mathbf{A})$, or else type-**2** tails can be found "quickly," (e.g., in a 3-generated subalgebra of $\mathbf{A}^2$). Where possible, we will relate our new results to analogous results in [FV09].

3.1. **Notation.** Throughout we let $\underline{n}$ denote the set $\{0, 1, \dots, n-1\}$ and we take $\mathcal{S}$ to be a finite set of finite, similar, idempotent algebras that is closed under the taking of subalgebras, and we assume that the type set of $\mathcal{V} = \mathbb{V}(\mathcal{S})$ omits **1** (but may include **5**). If there exists a finite algebra in $\mathcal{V}$ having a type-**2** minimal set with a nonempty tail—in which case we say that "$\mathcal{V}$ has type-**2** tails"—then, by standard results in TCT (see [HM88]), at least one such algebra appears as a subalgebra of a product of elements in $\mathcal{S}$. So we suppose that some finite algebra $\mathbf{B}$ in $\mathcal{V}$ has a prime quotient of type **2** with minimal sets that have nonempty tails and show that there is a 3-generated subalgebra of the product of two members of $\mathcal{S}$ with this property.

Since $\mathcal{S}$ is closed under the taking of subalgebras, we may assume that the algebra $\mathbf{B}$ from the previous paragraph is a subdirect product of a finite number of members of $\mathcal{S}$. Choose $n$ minimal such that for

[3]That is, there are positive integers $C, n$, and an algorithm that takes a finite idempotent algebra $\mathbf{A}$ as input and decides in at most $C|\mathbf{A}|^n$ steps whether $\mathbb{V}(\mathbf{A})$ is congruence modular. Here $|\mathbf{A}|$ denotes the number of bits required to encode the algebra $\mathbf{A}$.

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

some $\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_{n-1}$ in $\mathcal{S}$, there is a subdirect product $\mathbf{B} \leqslant_{\text{sd}} \prod_{\underline{n}} \mathbf{A}_i$ that has a prime quotient of type **2** whose minimal sets have nonempty tails. Under the assumption that $n > 1$ we will prove that $n = 2$.

For this $n$, select the $\mathbf{A}_i$ and $\mathbf{B}$ so that $|B|$ is as small as possible. Let $\alpha \prec \beta$ be a prime quotient of $\mathbf{B}$ of type **2** whose minimal sets have nonempty tails, and choose $\beta$ minimal with respect to this property. By [HM88, Lemma 6.2], this implies $\beta$ is join irreducible and $\alpha$ is its unique subcover. Let $U$ be an $\langle \alpha, \beta \rangle$-minimal set.

**Lemma 4** (cf. [FV09, Lemma 3.1])**.** *If* $0, 1 \in U$*, if* $(0,1) \in \beta - \alpha$*, and if* $t$ *belongs to the tail of* $U$*, then* $\beta$ *is the congruence of* $\mathbf{B}$ *generated by the pair* $(0,1)$*, and* $\mathbf{B}$ *is generated by* $\{0,1,t\}$*.*

*Proof.* Since $\beta$ is join irreducible with unique subcover $\alpha$, any pair of elements in $\beta - \alpha$ generates $\beta$. Let $\mathbf{C}$ be the subalgebra of $\mathbf{B}$ generated by $\{0,1,t\}$. We will obtain a contradiction under the assumption that $|C| < |B|$.

Let $\beta'$ and $\alpha'$ be the restrictions of $\beta$ and $\alpha$ to $C$, respectively. Then $\alpha' < \beta'$ since $(0,1) \in \beta' - \alpha'$ and so there are $\delta \succ \gamma$ in $\operatorname{Con}\mathbf{C}$ with $\alpha' \leq \delta \prec \gamma \leq \beta'$ and such that $(0,1) \in \gamma - \delta$. Since $\langle \alpha, \beta \rangle$ is type **2**, $\beta$ is abelian over $\alpha$. This implies $\beta'$ is abelian over $\alpha'$ by [KK13, Lemma 2.19(9)], which implies the types of the prime quotients occurring between $\alpha'$ and $\beta'$ are **1** or **2**. But since we are assuming that $\mathcal{V}$ omits type **1** and $\mathbf{B} \in \mathcal{V}$ then they are all of type **2**. In particular, $\langle \delta, \gamma \rangle$ has type **2**.

Now, if $|C| < |B|$, then all $\langle \delta, \gamma \rangle$-minimal sets have empty tails (since $\mathbf{B}$ is minimal among algebras with nonempty type-**2** tails). Let $V$ be a $\langle \delta, \gamma \rangle$-minimal set and let $p(x)$ be some polynomial of $\mathbf{C}$ with range $V$ and with $(p(0), p(1)) \notin \delta$. Such a polynomial exists by [HM88, Theorem 2.8], since $(0,1) \in \gamma - \delta$.

The polynomial $p(x)$ can be expressed in the form $s^{\mathbf{C}}(x, 0, 1, t)$ for some term $s(x, y, z, w)$ of $\mathcal{V}$, so $p(x)$ extends to a polynomial $p'(x) = s^{\mathbf{B}}(x, 0, 1, t)$ of $\mathbf{B}$. Since $(p(0), p(1)) \in \gamma - \delta$, then $(p'(0), p'(1)) \in \beta - \alpha$, so $p'$ must map the minimal set $U$ onto a polynomially isomorphic set $W$. In particular, $\{p'(0), p'(1)\} \subseteq \operatorname{Body}(W)$ and $p'(t) \in \operatorname{Tail}(W)$.

Since the type of $\langle \delta, \gamma \rangle$ is **2** and $V$ has no tail, $\mathbf{C}|_V$ has a Mal'tsev polynomial. This polynomial has an extension to a polynomial of $\mathbf{B}$ and, since $\{p(0), p(1), p(t)\} \subseteq V$, it follows that there is a polynomial $f(x, y, z)$ of $\mathbf{B}$ that satisfies the Mal'tsev identities when restricted to the set $\{p'(0), p'(1), p'(t)\} \subseteq W$. This contradicts [HM88, Lemma 4.26], since $p'(0)$ and $p'(1)$ are in the body of $W$ and $p'(t)$ is in the tail. □

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

For $i \leqslant n$, let $\rho_i$ denote the kernel of the projection of $\mathbf{B}$ onto $\mathbf{A}_i$, so $\mathbf{B}/\rho_i \cong \mathbf{A}_i$. For a subset $\sigma \subseteq \underline{n}$, define

$$\rho_\sigma := \bigwedge_{j \in \sigma} \rho_j.$$

Consequently, $\rho_{\underline{n}} = \bigwedge_{j \in \underline{n}} \rho_j = 0_B$. By minimality of $n$ we know that the intersection of any proper subset of the $\rho_i$, $1 \leqslant i \leqslant n$ is strictly above $0_B$. Thus, $0_B < \rho_\sigma < 1_B$ for all $\emptyset \subset \sigma \subset \underline{n}$. (By $\subset$ we mean *proper* subset.)

**Lemma 5** (cf. [FV09, Lemma 3.2])**.** *For every proper nonempty subset $\sigma$ of $\underline{n}$, either $\beta \leqslant \rho_\sigma$ or $\alpha \vee \rho_\sigma = 1_B$.*

*Proof.* Let $\rho = \rho_\sigma$. Suppose that $\beta \not\leq \rho$ (or equivalently $(0,1) \notin \rho$). Since $\beta$ is join irreducible, $\beta \wedge \rho \leq \alpha$ and so $\beta \wedge \rho = \alpha \wedge \rho$. Furthermore, $\alpha \vee \rho = \beta \vee \rho$, or else we can find a prime quotient between these two congruences that is perspective with $\langle \alpha, \beta \rangle$. But then the algebra $\mathbf{B}/\rho$ has a prime quotient of type **2** whose minimal sets have nonempty tails. Since this algebra is isomorphic to a subdirect product of fewer than $n$ members of $\mathcal{S}$, we conclude, by the minimality of $n$, that indeed $\alpha \vee \rho = \beta \vee \rho$.

Thus the set

$$\mathcal{P} = \{\beta \wedge \rho, \rho, \alpha, \beta, \alpha \vee \rho\}$$

forms a pentagon in $\mathbf{Con}\,\mathbf{B}$. Let $C$ be the $(\alpha \vee \rho)$-class that contains 0 and let $M = C \cap U$. Note that $C$ contains 1 and, since $\mathbf{B}$ is idempotent, that $C$ is a subuniverse of $\mathbf{B}$. By [HM88, Lemma 2.4], we conclude that the restriction to $M$ is a surjective lattice homomorphism from the interval $I[0_B, \alpha \vee \rho]$ in $\mathbf{Con}\,\mathbf{B}$ to the interval $I[0_M, (\alpha \vee \rho)|_M]$ in $\mathbf{Con}\,\mathbf{B}|_M$. Note that since $(0,1) \in \beta|_M - \alpha|_M$, this restriction map separates $\alpha$ and $\beta$. Then, the image under the restriction map of the pentagon $\mathcal{P}$ is a pentagon in $\mathbf{Con}\,\mathbf{B}|_M$. This implies that $M$ contains some elements of the tail of $U$, since otherwise $\mathbf{Con}\,\mathbf{B}|_M$ has a Mal'tsev term operation and hence is modular. Thus, there is some $t$ in the tail of $U$ with $(0,t) \in \alpha \vee \rho$. Using Lemma 4 we conclude that $C = B$ since it contains $\{0,1,t\}$. Thus, $\alpha \vee \rho = 1_B$. □

**Lemma 6.** *For every proper nonempty subset $\sigma$ of $\underline{n}$, for all $v \in B$, and for all $b \in \mathrm{Body}(U)$, we have $(v,b) \in \beta \circ \rho_\sigma \cap \rho_\sigma \circ \beta$.*

*Proof.* Let $\rho = \rho_\sigma$. Note that $\beta \vee \rho = 1_B$ implies $\beta\big|_U \vee \rho\big|_U = 1_B\big|_U = 1_U$, since $U = e(B)$, for some idempotent unary polynomial $e$. Now, for all $x, y \in U$, if $x \in \mathrm{Body}(U)$ and $y \in \mathrm{Tail}(U)$, then $(x,y) \notin \beta$. Therefore, $(x,y) \in 1_U = \beta\big|_U \vee \rho\big|_U$ implies there must be some $b' \in \mathrm{Body}(U)$ and $t' \in \mathrm{Tail}(U)$ such that $b' \,\rho\, t'$.

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

Now, let $d(x, y, z)$ be a pseudo-Mal'tsev polynomial for $U$, which exists by [HM88, Lemma 4.20]. Thus,

- $d(B, B, B) = U$
- $d(x, x, x) = x$ for all $x \in U$
- $d(x, x, y) = y = d(y, x, x)$ for all $x \in \mathrm{Body}(U)$, $y \in U$.

Moreover, for all $c$, $d \in \mathrm{Body}(U)$, the unary polynomials $d(x, c, d)$, $d(c, x, d)$, and $d(c, d, x)$ are permutations on $U$. If we now fix an arbitrary element $b \in \mathrm{Body}(U)$ and let $p(x) = d(x, b', b)$, then (see [HM88, Lemma 4.20])

- $p(U) = U$, since $U$ is minimal,
- $p(b') = d(b', b', b) = b \in \mathrm{Body}(U)$, and
- $t := p(t') \in \mathrm{Tail}(U)$, since $t' \in \mathrm{Tail}(U)$.

Since $(b', t') \in \rho$, we have $(b, t) = (p(b'), p(t')) \in \rho$. Since $b$ is in the body, there is an element $b''$ in the body with $(b, b'') \in \beta - \alpha$. By Lemma 4, this implies $\mathbf{B} = \mathrm{Sg}^{\mathbf{B}}(\{b, b'', t'\})$.

Finally, if $v \in B$, then $v = s^{\mathbf{B}}(b, b'', t)$ for some (idempotent) term $s$, so

$$v = s^{\mathbf{B}}(b, b'', t)\ \rho\ s^{\mathbf{B}}(b, b'', b)\ \beta\ s^{\mathbf{B}}(b, b, b) = b,$$

and

$$v = s^{\mathbf{B}}(b, b'', t)\ \beta\ s^{\mathbf{B}}(b, b, t)\ \rho\ s^{\mathbf{B}}(b, b, b) = b.$$

Therefore, $(v, b) \in \beta \circ \rho \cap \rho \circ \beta$. Since $v \in B$ and $b \in \mathrm{Body}(U)$ were aribitrary, this completes the proof. □

**Lemma 7** (cf. [FV09, Lemma 3.3])**.**

*(i) There exists $i$ such that $\alpha \vee \rho_i = 1_B$*
*(ii) There exists $i$ such that $\alpha \vee \rho_i < 1_B$.*

*Proof.* If item (i) failed, then we would have $\beta \leqslant \rho_i$ for all $i$, and that would imply $\beta = 0_B$.

To see (ii), assume

$$\alpha \vee \rho_i = 1_B \quad \text{for all } i. \tag{2}$$

Take a nonempty proper subset $\sigma \subset \underline{n}$ of indices and let $\rho_\sigma = \bigwedge_{j \in \sigma} \rho_j$. Then $\beta \vee \rho_\sigma = 1_B$. (Otherwise, $\alpha \vee \rho_\sigma \leqslant \beta \vee \rho_\sigma < 1_B$, and it would follow from Lemma 5 that $\alpha \leqslant \beta \leqslant \rho_\sigma \leqslant \rho_i$ for all $i \in \sigma$, but then $\alpha \vee \rho_i = \rho_i < 1_B$, contradicting (2).)

Let $b \in \mathrm{Body}(U)$ and $t \in \mathrm{Tail}(U)$, and let $d(x, y, z)$ denote the pseudo-Mal'tsev operation introduced in the proof of Lemma 6. By [HM88, Lemma 4.25], $(b, d(b, t, t)) \notin \beta$. We will arrive at a contradiction by showing that $b = d(b, t, t)$. By Lemma 6, for any $i \in \underline{n}$, $(b, t) \in \beta \circ \rho_i$ so there is an element $a \in B$ satisfying $b\ \beta\ a\ \rho_i\ t$. By applying the idempotent polynomial $e$ with $e(U) = U$, we have

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

$b \ \beta \ e(a) \ \rho_i \ t$, so we may assume $a \in U$. But this puts $a \in \mathrm{Body}(U)$, since $a \ \beta \ b$. Therefore,

$$d(b,t,t) \ \rho_i \ d(b,a,a) = b.$$

Since this hold for every $i$, $d(b,t,t) = b$. □

**Theorem 8** (cf. [FV09, Theorem 3.4])**.** *Let $\mathcal{V}$ be the variety generated by some finite set $\mathcal{S}$ of finite, idempotent algebras that is closed under taking subalgebras. If $\mathcal{V}$ omits type **1** and some finite member of $\mathcal{V}$ has a prime quotient of type **2** whose minimal sets have nonempty tails, then there is some 3-generated algebra $\mathbf{B}$ with this property that belongs to $\mathcal{S}$ or is a subdirect product of two algebras from $\mathcal{S}$.*

*Proof.* Choose $n > 0$, $\mathbf{A}_i \in \mathcal{S}$, for $0 \leq i \leq n-1$ and $\mathbf{B}$ as above. From Lemma 4 we know that $\mathbf{B}$ is 3-generated. If $n > 1$ then by the previous lemma we can choose $i$ and $j < n$ with $\beta \leq \rho_i$ and $\alpha \vee \rho_j = 1_B$. If $n > 2$ then Lemma 5 applies to $\rho = \rho_i \wedge \rho_j$ and so we know that either $\beta \leq \rho$ or $\alpha \vee \rho = 1_B$. This yields a contradiction as the former is not possible, since $\beta \not\leq \rho_j$ and the latter can't hold since both $\alpha$ and $\rho$ are below $\rho_i$.

So, the minimality of $n$ forces $n \leq 2$ and the result follows. □

**Example 9.** Let $\mathbf{A}$ be the algebra with universe $\{0,1,2\}$ that has the ternary idempotent operation $f(x,y,z)$ such that on $\{0,1\}$ $f(x,y,z) = x \oplus y \oplus z$, on $\{0,2\}$, $f(x,y,z) = \min\{x,y,z\}$ and is equal to 0 otherwise. Then $f$ is a cyclic operation and so $\mathbf{A}$ generates a variety that omits type **1**. It can be checked that there is a 3 element subdirectly irreducible algebra in $\mathsf{HS}(\mathbf{A}^2)$ that has a prime quotient of type **2** whose minimal sets have nonempty tails and that no member of $\mathsf{HS}(\mathbf{A})$ has this property. This demonstrates that in general one must look for nonempty tails of minimal sets of type **2** in the square of a finite idempotent algebra.

The next theorem essentially gives an algorithm to decide if a finitely generated, idempotent variety has a difference term, which, in the next section, we will show is polynomial-time.

In [KK99], Kearnes and Kiss show there is a close connection between $\alpha \prec \beta$ being the critical interval of a pentagon and $\langle \alpha, \beta \rangle$-minimal sets having nonempty tails. By [KK99, Theorem 2.1], the minimal sets of a prime critical interval of a pentagon have nonempty tails, provided the type is not **1**. In the other direction, if the $\langle \alpha, \beta \rangle$-minimal sets have nonempty tails, then there is a pentagon in the congruence lattice of a subalgebra of $\mathbf{A}^2$ with a prime critical interval of the same type. This connection between minimal sets with tails and pentagons is important

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

for us: we do not have a polynomial time algorithm for finding an $\langle \alpha, \beta \rangle$-minimal set.

If $\mathbf{B}$ is a subalgebra of $\mathbf{A}^2$ and $\theta$ is a congruence of $\mathbf{A}$, then we define $\theta_0 \in \mathrm{Con}(\mathbf{B})$ by $(x_0, x_1)\ \theta_0\ (y_0, y_1)$ iff $x_0\ \theta\ y_0$. We define $\theta_1$ similarly. In case $\theta = 0_{\mathbf{A}}$, the least congruence, we use the notation $\rho_0$ and $\rho_1$ instead of $0_0$ and $0_1$. Of course $\rho_0$ and $\rho_1$ are the kernels of the first and second projections of $\mathbf{B}$ onto $\mathbf{A}$.

**Theorem 10.** *Let $\mathbf{A}$ be a finite idempotent algebra and let $\mathcal{V}$ be the variety it generates. Then $\mathcal{V}$ has a difference term if and only if the following conditions hold:*

*(1) $\mathcal{V}$ omits TCT-type **1**.*
*(2) There do not exist $a, b, c \in A$ satisfying the following, where $\mathbf{B} := \mathrm{Sg}^{\mathbf{A}}(a, b, c)$ and $\mathbf{C} := \mathrm{Sg}^{\mathbf{B}^2}\big(\{(a, b), (a, c), (b, c)\} \cup 0_{\mathbf{B}}\big)$:*
  *(a) $\beta := \mathrm{Cg}^{\mathbf{B}}(a, b)$ is join irreducible with lower cover $\alpha$,*
  *(b) $((a, b), (b, b)) \notin (\alpha_0 \wedge \alpha_1) \vee \mathrm{Cg}^{\mathbf{C}}((a, c), (b, c))$, and*
  *(c) $[\beta, \beta] \leq \alpha$.*
*(3) There do not exist $x_0$, $x_1$, $y_0$, $y_1 \in A$ satisfying the following, where $\mathbf{B}$ is the subalgebra of $\mathbf{A} \times \mathbf{A}$ generated by $0 := (x_0, x_1)$, $1 := (y_0, x_1)$, and $t := (x_0, y_1)$:*
  *(a) $\beta := \mathrm{Cg}^{\mathbf{B}}(0, 1)$ is join irreducible with lower cover $\alpha$,*
  *(b) $\rho_0 \vee \alpha = 1_{\mathbf{B}}$, and*
  *(c) the type of $\beta$ over $\alpha$ is **2**.*

*Proof.* First assume $\mathcal{V}$ has a difference term. Then (1) holds by Theorem 1. If (2) fails then there are $a$, $b$ and $c \in A$ such that the conditions specified in (2) hold. In particular, (2c) holds and implies that $\mathrm{typ}\langle \alpha, \beta \rangle \subseteq \{\mathbf{1}, \mathbf{2}\}$, so by (1) the type of $\langle \alpha, \beta \rangle$ is **2**. Let

$$\delta := (\alpha_0 \wedge \alpha_1) \vee \mathrm{Cg}^{\mathbf{C}}((a, c), (b, c)), \text{ and}$$
$$\theta := \delta \vee \mathrm{Cg}^{\mathbf{C}}((a, b), (b, b)).$$

By its definition, $\delta \not\leq \alpha_0$, so by (2b), $\alpha_0 \wedge \alpha_1 < \delta < \theta \leq \beta_0$. Since $C$ contains $0_B$, the diagonal of $B$, the coordinate projections are onto, so $\alpha_0 \prec \beta_0$ and this interval has type **2**. From this it follows that $\alpha_0 \vee \delta = \beta_0$. Since $\theta \leq \alpha_1$, we have $\alpha_0 \wedge \theta = \alpha_0 \wedge \alpha_1$. Hence

$$\{\alpha_0 \wedge \alpha_1, \delta, \theta, \alpha_0, \beta_0\}$$

forms a pentagon. Since $[\beta_0, \beta_0] \leqslant \alpha_0$, we have $[\theta, \theta] \leqslant \alpha_0 \wedge \alpha_1 < \delta$, so there is a congruence $\delta'$ such that $\delta \leqslant \delta' \prec \theta$ and $\langle \delta', \theta \rangle$ has type **2**. As mentioned in the discussion above, this implies the $\langle \delta', \theta \rangle$-minimal sets have tails, contradicting Theorem 1.

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

Now suppose that (3) fails. Then the conditions imply

$$\{0_{\mathbf{B}}, \alpha, \beta, \rho_0, 1_{\mathbf{B}}\}$$

is a pentagon whose critical prime interval has type **2**. This leads to a contradiction in the same manner as above.

For the converse assume that $\mathcal{V}$ does not have a difference term. We want to show that (1), (2) or (3) fails. Assume all three hold. By Theorem 1 there is a finite algebra $\mathbf{B} \in \mathcal{V}$ and a join irreducible $\beta \in \mathrm{Con}(\mathbf{B})$ with lower cover $\alpha$ such that the type of $\langle \alpha, \beta \rangle$ is **2** and the $\langle \alpha, \beta \rangle$-minimal sets have nonempty tails. Let $U$ be one of these minimal sets.

We may assume $\mathbf{B}$ is minimal in the same manner as with the above lemmas (with $\mathcal{S}$ being the subalgebras of $\mathbf{A}$). By Lemma 4 we have that $\mathbf{B}$ is generated by any 0, 1, and $t$ in $U$ such that $\beta = \mathrm{Cg}^{\mathbf{B}}(0, 1)$ and $t$ is in the tail. By Theorem 8, $\mathbf{B}$ is either in $\mathcal{S}$ or is a subdirect product of two members of $\mathcal{S}$.

Assume $\mathbf{B}$ is a subalgebra of $\mathbf{A}$. Taking $a = 0$, $b = 1$ and $c = t$, we claim the conditions specified in (2) hold. Since the type of $\beta$ over $\alpha$ is **2**, (2c) holds and we already have (2a) holds. (2b) holds by [KK99, Theorem 2.4]. So this choice of $a$, $b$, and $c$ witness that (2) fails.

Now assume $\mathbf{B}$ is not in $\mathcal{S}$ but is a subdirect product of two members of $\mathcal{S}$. Then by Lemma 7 we may assume $\rho_0 \vee \alpha = 1_{\mathbf{B}}$ and $\rho_1 \vee \alpha < 1_{\mathbf{B}}$. By Lemma 5 we have $\rho_1 \geq \beta$.

This implies that 0 and 1 have the same second coordinate; that is, $0 = (x_0, x_1)$ and $1 = (y_0, x_1)$ for some $x_0$, $y_0$ and $x_1 \in A$. By Lemma 6, $(0, t) \in \rho_0 \circ \beta$ so $0 \ \rho_0 \ t' \ \beta \ t$. Let $U = e(B)$ where $e$ is an idempotent polynomial. Then $0 \ \rho_0 \ e(t') \ \beta \ t$. This gives that $e(t')$ is in the tail of $U$ and $0 \ \rho_0 \ e(t')$. We can replace $t$ by $e(t')$, and so assume that $0 \ \rho_0 \ t$. Since $0 = (x_0, x_1)$, $t = (x_0, y_1)$ for some $y_1 \in A$. Now $x_0$, $y_0$, $x_1$ and $y_1$ witness that (3) fails. □

## 4. The Algorithm and its Time Complexity

If $\mathbf{A}$ is an algebra with underlying set (or universe) $A$, we let $|\mathbf{A}| = |A|$ be the cardinality of $A$ and $||\mathbf{A}||$ be the *input size*; that is,

$$||\mathbf{A}|| = \sum_{i=0}^{r} k_i n^i$$

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

where, $k_i$ is the number of basic operations of arity $i$ and $r$ is the largest arity. We let

$$n = |\mathbf{A}| \qquad m = ||\mathbf{A}||$$
$$r = \text{the largest arity of the operations of } \mathbf{A}$$

Throughout this section we let $c$ denote a constant independent of these parameters.

**Proposition 11.** *Let* $\mathbf{A}$ *be a finite algebra with the parameters above.*

*(1) If* $S$ *is a subset of* $A$*, then* $\mathrm{Sg}^{\mathbf{A}}(S)$ *can be computed in time*

$$c\,r\,||\,\mathrm{Sg}^{\mathbf{A}}(S)|| \leq c\,r\,||\mathbf{A}|| = crm$$

*(2) If* $a,\ b \in A$*, then* $\mathrm{Cg}^{\mathbf{A}}(a, b)$ *can be computed in* $c\,r\,||\mathbf{A}|| = crm$ *time.*

*(3) If* $\alpha$ *and* $\beta$ *are congruences of* $\mathbf{A}$*, then* $[\alpha, \beta]$ *can be computed in time* $crm^2$*.*

*Proof.* For the first two parts see [FV09, Proposition 6.1]. For the third part we use that

$$\begin{aligned}[\alpha, \beta] &= \bigcup_{a \in A} (a, a)/\Delta_{\beta,\alpha} \\ &= \left\{(x, y) \in A \times A : (\exists a \in A)\,(a, a)\ \Delta_{\beta,\alpha}\ (x, y)\right\}\end{aligned}$$

where $\Delta_{\beta,\alpha}$ is the congruence on the subalgebra of $\mathbf{A}^2$ with universe $\beta$ generated by the pairs $((u, u), (v, v))$ with $(u, v) \in \alpha$. By (2), $\Delta_{\beta,\alpha}$ can be calculated in time $crm^2$. Using the displayed formula above, it is easy to see that (3) holds. □

**Theorem 12.** *Let* $\mathbf{A}$ *be a finite idempotent algebra with parameters as above. Then one can determine if* $\mathbb{V}(\mathbf{A})$ *has a difference term in time* $crn^4m^4$*.*

*Proof.* Theorem 10 gives a three-step algorithm to test if $\mathbb{V}(\mathbf{A})$ has a difference term. The first step is to test if $\mathbb{V}(\mathbf{A})$ omits type **1**. This can be done in time $crn^3m$ by [FV09, Theorem 6.3].

Looking now at part (3) of Theorem 10, there are several things that have to be constructed. By Proposition 11, all of these things can be constructed in time $crm^2$ and parts (a) and (b) can be executed in this time or less. For part (c) we need to test if the type of $\beta$ over $\alpha$ is **2**. Since at this point in the algorithm we know that $\mathbf{A}$ omits type **1**, we can test if the type is **2** by testing if $[\beta, \beta] \leq \alpha$. By Proposition 11 this can be done in time $crm^4$. Since we need to do this for all $x_0$, $x_1$, $y_0$ and $y_1$, the total time for this step is at most $crn^4m^4$.

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

A similar analysis applies to part (2) and shows that it can be done in time $crn^3m^2$. Since $crn^4m^4$ dominates the other terms, the bound of the theorem holds. □

## 5. Difference Term Operations

Above we addressed the problem of deciding the existence of a difference term for a given (idempotent, finitely generated) variety. In this section we are concerned with the practical problem of finding a difference term *operation* for a given (finite, idempotent) algebra. We describe algorithms for

(1) deciding whether a given finite idempotent algebra has a difference term operation, and
(2) finding a difference term operation for a given finite idempotent algebra.

Note that Theorem 12 gives a polynomial-time algorithm for deciding whether or not the variety $\mathbb{V}(\mathbf{A})$ generated by a finite idempotent algebra $\mathbf{A}$ has a difference term. If we run that algorithm on input $\mathbf{A}$, and if the observed output is "Yes", then of course we have a positive answer to decision problem (1). However, a negative answer returned by the algorithm only tells us that $\mathbb{V}(\mathbf{A})$ has no difference term. It does not tell us whether or not $\mathbf{A}$ has a difference term operation.

**Example 13.** Let $\mathbf{A}$ be the idempotent algebra with universe $\{0, 1, 2\}$ with basic operation $x \cdot y$ defined by:

| $\cdot$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 |
| 2 | 0 | 2 | 2 |

Then $\mathbf{A}$ is a simple algebra of type **4** and so the ternary projection operation $p(x, y, z) = z$ is a difference term operation for $\mathbf{A}$. On the other hand, since $\{1, 2\}$ is a subuniverse of $\mathbf{A}$ and $x \cdot y = x$ on this subset then the variety generated by $\mathbf{A}$ cannot have a difference term.

In this section we present solutions to problems (1) and (2) using methods that are entirely different than the ones used in the previous sections. (For example, we make no use of tame congruence theory.) In Subsection 5.2 we give a polynomial-time algorithm for deciding whether a given idempotent algebra $\mathbf{A}$ has a difference term operation. In Subsection 5.3 we address problem (2) by presenting an algorithm for constructing a difference term operation. However, this algorithm does not run in polynomial-time and, at the time of this writing, we

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

do not know of a more efficient algorithm for constructing a difference term operation, even when such an operation is known to exist.

5.1. **Local Difference Terms.** In [VW14], Ross Willard and the third author define a "local Hagemann-Mitschke sequence" which they use as the basis of an efficient algorithm for deciding for a given $n$ whether an idempotent variety is $n$-permutable. In [Hor13], Jonah Horowitz introduced similar "local-to-global" methods for deciding when a given variety satisfies certain Mal'tsev conditions. Inspired by these works, we now define a "local difference term operation" and use it to develop a polynomial-time algorithm for deciding the existence of a difference term operation.

Start with a finite idempotent algebra, $\mathbf{A} = \langle A, \ldots \rangle$. For elements $a, b, a_j, b_j \in A$, the following are some shorthands we will use to denote the congruences generated by these elements:

$$\theta_{ab} := \mathrm{Cg}^{\mathbf{A}}(a, b) \qquad \theta_i := \mathrm{Cg}^{\mathbf{A}}(a_i, b_i).$$

Let $i \in \{0, 1\}$. By a *local difference term operation for* $(a, b, i)$ we mean a ternary term operation $t$ satisfying the following conditions:

$$\text{if } i = 0, \text{ then } a \; [\theta_{ab}, \theta_{ab}] \; t(a, b, b); \tag{3}$$

$$\text{if } i = 1, \text{ then } t(a, a, b) = b. \tag{4}$$

If $t$ satisfies conditions (3) and (4) for all triples in some subset $S \subseteq A^2 \times \{0, 1\}$, then we call $t$ a *local difference term operation for* $S$. Throughout the remainder of the paper, we will write "LD term" as shorthand for "local difference term operation."

Often we will take $S$ to be a finite list of elements of $A \times \{0, 1\}$, and $|S|$ will denote the length of the list. The definition above of a LD term for a set has an obvious analog for a list.

A few more notational conventions will come in handy below. We will use the symbol $\mathcal{D} \subseteq A^2 \times \{0, 1\} \times \mathsf{Clo}_3(\mathbf{A})$ to denote the relation that connects $(a, b, i) \in A^2 \times \{0, 1\}$ with terms in $\mathsf{Clo}_3(\mathbf{A})$ that are LD term for $(a, b, i)$. That is,

$$((a, b, i), t) \in \mathcal{D} \text{ iff conditions (3) and (4) are satisfied.}$$

The relation $\mathcal{D}$ induces an obvious Galois connection from subsets of $A^2 \times \{0, 1\}$ to subsets of $\mathsf{Clo}_3(\mathbf{A})$. If we permit ourselves to overload notation for the moment, then we could take

$$\mathcal{D} \colon \mathcal{P}(A^2 \times \{0, 1\}) \to \mathcal{P}(\mathsf{Clo}_3(\mathbf{A})) \text{ and}$$
$$\breve{\mathcal{D}} \colon \mathcal{P}(\mathsf{Clo}_3(\mathbf{A})) \to \mathcal{P}(A^2 \times \{0, 1\})$$

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

to denote the maps defined as follows:

$$\begin{aligned}&\text{for } S \subseteq A^2 \times \{0,1\} \text{ and } T \subseteq \mathsf{Clo}_3(\mathbf{A}), \text{ let}\\ &\mathcal{D}(S) = \{t \in \mathsf{Clo}_3(\mathbf{A}) \mid (s,t) \in \mathcal{D} \text{ for all } s \in S\}, \text{ and}\\ &\breve{\mathcal{D}}(T) = \{s \in A^2 \times \{0,1\} \mid (s,t) \in \mathcal{D} \text{ for all } t \in T\}.\end{aligned}$$

In other words, $\mathcal{D}(S)$ is the set of LD terms for $S$, and $\breve{\mathcal{D}}(T)$ is the set of triples for which every $t \in T$ is an LD term.

Now, suppose that every pair $(s_0, s_1) \in (A^2 \times \{0,1\})^2$ has an LD term. Then every subset $S \subseteq A^2 \times \{0,1\}$ has an LD term, as we now prove.

**Theorem 14.** *Let $\mathcal{V}$ be an idempotent variety and let $\mathbf{A} \in \mathcal{V}$. If every pair $(s_0, s_1) \in (A^2 \times \{0,1\})^2$ has a local difference term operation, then every subset $S \subseteq A^2 \times \{0,1\}$ has a local difference term operation.*

*Proof.* The proof is by induction on the size of $S$. In the base case, $|S| = 2$, the claim holds by assumption. Fix $n \geqslant 2$ and assume that every subset of $A^2 \times \{0,1\}$ of size $k \leqslant n$ has an LD term. Let

$$S := \{(a_0, b_0, \chi_0), (a_1, b_1, \chi_1), \ldots, (a_n, b_n, \chi_n)\} \subseteq A^2 \times \{0,1\},$$

so $|S| = n + 1$. We prove $S$ has an LD term (i.e., $\mathcal{D}(S)$ is nonempty).

Since $|S| \geqslant 3$, there exist indices $i \neq j$ such that $\chi_i = \chi_j$. Assume without loss of generality that one such index is $j = n$, and define the set

$$S' := S - \{(a_n, b_n, \chi_n)\}.$$

Since $|S'| < |S|$, there exists $p \in \mathcal{D}(S')$. We split the remainder of the proof into two cases.

Case $\chi_n = 0$: Without loss of generality, assume

$$\chi_0 = \cdots = \chi_{k-1} = 1 \quad \text{and} \quad \chi_k = \cdots = \chi_n = 0.$$

If we define

$$S_0 := \{(a_0, b_0, 1), (a_1, b_1, 1), \ldots, (a_{k-1}, b_{k-1}, 1), (a_n, p(a_n, b_n, b_n), 0)\},$$

then $|S_0| < |S|$, so $S_0$ has a LD term term, $q \in \mathcal{D}(S_0)$. We now show that

$$d(x, y, z) := q(x, p(x, y, y), p(x, y, z))$$

is a local difference term operation for $S$.

Since $\chi_n = 0$, we must first check that $a_n \ [\theta_n, \theta_n] \ d(a_n, b_n, b_n)$. If $\gamma_n := \mathrm{Cg}(a_n, p(a_n, b_n, b_n))$, then

$$d(a_n, b_n, b_n) = q(a_n, p(a_n, b_n, b_n), p(a_n, b_n, b_n)) \ [\gamma_n, \gamma_n] \ a_n. \tag{5}$$

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

The pair $(a_n, p(a_n, b_n, b_n))$ is equal to $(p(a_n, a_n, a_n), p(a_n, b_n, b_n))$ and so belongs to $\theta_n$. Therefore, $\gamma_n \leqslant \theta_n$, so $[\gamma_n, \gamma_n] \leqslant [\theta_n, \theta_n]$. It follows from this and (5) that $a_n \; [\theta_n, \theta_n] \; d(a_n, b_n, b_n)$, as desired.

For indices $i < k$, we have $\chi_i = 1$, so want to prove $d(a_i, a_i, b_i) = b_i$ for such $i$. Observe,

$$d(a_i, a_i, b_i) = q(a_i, p(a_i, a_i, a_i), p(a_i, a_i, b_i)) = q(a_i, a_i, b_i) = b_i.$$

The first equation holds by definition of $d$, the second because $p$ is an idempotent LD term for $S'$, and the third because $q \in \mathcal{D}(S_0)$.

The remaining triples in our original set $S$ have indices satisfying $k \leqslant j < n$ and $\chi_j = 0$. For these we want $a_j \; [\theta_j, \theta_j] \; d(a_j, b_j, b_j)$. By definition,

$$d(a_j, b_j, b_j) = q(a_j, p(a_j, b_j, b_j), p(a_j, b_j, b_j)). \tag{6}$$

Since $p \in \mathcal{D}(S')$, we have $a_j \; [\theta_j, \theta_j] \; p(a_j, b_j, b_j)$, so (6) implies that $a_j = q(a_j, a_j, a_j) \; [\theta_j, \theta_j] \; d(a_j, b_j, b_j)$.

Case $\chi_n = 1$: Without loss of generality, suppose

$$\chi_0 = \cdots = \chi_{k-1} = 0 \quad \text{and} \quad \chi_k = \cdots = \chi_n = 1.$$

If

$$S_1 := \{(a_0, b_0, 0), (a_1, b_1 0), \ldots, (a_{k-1}, b_{k-1}, 0), (p(a_n, a_n, b_n), b_n, 1)\},$$

then $|S_1| < |S|$, so there exists $q \in \mathcal{D}(S_1)$. We claim that

$$d(x, y, z) := q(p(x, y, z), p(y, y, z), z)$$

is an LD term for $S$. For $(a_n, b_n, \chi_n) \in S$ we have that

$$d(a_n, a_n, b_n) = q(p(a_n, a_n, b_n), p(a_n, a_n, b_n), b_n) = b_n.$$

The last equality holds since $q$ is LD term for $(p(a_n, a_n, b_n), b_n, 1)$.

If $1 \leqslant i < k$, then $\chi_i = 0$. For these indices we must prove that $a_i$ is congruent to $d(a_i, b_i, b_i)$ modulo $[\theta_i, \theta_i]$. Again, starting from the definition of $d$ and using idempotence of $p$, we have

$$d(a_i, b_i, b_i) = q(p(a_i, b_i, b_i), p(b_i, b_i, b_i), b_i) = q(p(a_i, b_i, b_i), b_i, b_i). \tag{7}$$

Next, since $p \in \mathcal{D}(S')$,

$$q(p(a_i, b_i, b_i), b_i, b_i) \; [\theta_i, \theta_i] \; q(a_i, b_i, b_i). \tag{8}$$

Since $q \in \mathcal{D}(S_1)$, we have $q(a_i, b_i, b_i) \; [\theta_i, \theta_i] \; a_i$, so (7) and (8) imply $d(a_i, b_i, b_i) \; [\theta_i, \theta_i] \; a_i$, as desired.

The remaining elements of $S$ have indices satisfying $k \leqslant j < n$ and $\chi_j = 1$. For these we want $d(a_j, a_j, b_j) = b_j$. Since $p \in \mathcal{D}(S')$, we have $p(a_j, a_j, b_j) = b_j$, and this plus idempotence of $q$ yields

$$d(a_j, a_j, b_j) = q(p(a_j, a_j, b_j), p(a_j, a_j, b_j), b_j) = q(b_j, b_j, b_j) = b_j,$$

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

as desired. □

**Corollary 15.** *Let* $\mathbf{A}$ *be a finite idempotent algebra and suppose that every pair* $(s, s') \in (A^2 \times \{0,1\})^2$ *has a local difference term operation. Then* $\mathcal{D}(A^2 \times \{0,1\}) \neq \emptyset$*, so* $\mathbf{A}$ *has a difference term operation.*

*Proof.* Letting $S := A^2 \times \{0,1\}$ in Theorem 14 establishes the existence of a term operation $d \in \mathcal{D}(S)$. Thus, for all $a, b \in A$, we have that $a\ [\theta_{ab}, \theta_{ab}]\ d(a,b,b)$, since $d$ is LD term for $(a,b,0)$, and $d(a,a,b) = b$, since $d$ is LD term for $(a,b,1)$. □

5.2. **Algorithm to test for existence of a difference term operation.** Here is a practical consequence of Theorem 14.

**Corollary 16.** *There is a polynomial-time algorithm that takes as input any finite idempotent algebra* $\mathbf{A}$ *and decides if* $\mathbf{A}$ *has a difference term operation.*

*Proof.* We describe an efficient algorithm for deciding, given a finite idempotent algebra $\mathbf{A}$, whether every pair in $(A^2 \times \{0,1\})^2$ has an LD term. By Corollary 15, this will prove we can decide in polynomial-time whether $\mathbf{A}$ has an difference term operation.

Fix a pair $((a,b,i),(a',b',i'))$ in $(A^2 \times \{0,1\})^2$. If $i = i' = 0$, then the first projection is an LD term. If $i = i' = 1$, then the third projection is an LD term. The two remaining cases occur when $i \neq i'$. Without loss of generality, assume $i = 0$ and $i' = 1$, so the given pair of triples are of the form $((a,b,0),(a',b',1))$. By definition, $t \in \mathcal{D}(\{(a,b,0),(a',b',1)\})$ iff

$$a\ [\theta_{ab}, \theta_{ab}]\ t^{\mathbf{A}}(a,b,b) \quad \text{and} \quad t^{\mathbf{A}}(a',a',b') = b'.$$

We can rewrite this condition more compactly by considering

$$t^{\mathbf{A}\times\mathbf{A}}((a,a'),(b,a'),(b,b')) = (t^{\mathbf{A}}(a,b,b), t^{\mathbf{A}}(a',a',b')).$$

Clearly $t \in \mathcal{D}(\{(a,b,0),(a',b',1)\})$ iff

$$t^{\mathbf{A}\times\mathbf{A}}((a,a'),(b,a'),(b,b')) \in a/\delta \times \{b'\},$$

where $\delta = [\theta_{ab}, \theta_{ab}]$ and $a/\delta$ denotes the $\delta$-class containing $a$. It follows that $\mathcal{D}(\{(a,b,0),(a',b',1)\}) \neq \emptyset$ iff the subuniverse of $\mathbf{A} \times \mathbf{A}$ generated by $\{(a,a'),(b,a'),(b,b')\}$ intersects nontrivially with the subuniverse $a/\delta \times \{b'\}$.

Thus, we take as input a finite idempotent algebra $\mathbf{A}$ and, for each element $((a,a'),(b,a'),(b,b'))$ of $(A \times A)^3$,

(1) compute $\delta = [\theta_{ab}, \theta_{ab}]$,
(2) compute $\mathbf{S} = \mathrm{Sg}^{\mathbf{A}\times\mathbf{A}}\{(a,a'),(b,a'),(b,b')\}$,
(3) test whether $S \cap (a/\delta \times \{b'\})$ is empty.

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

If ever we find an empty intersection in step (3), then $\mathbf{A}$ has no difference term operation. Otherwise the algorithm halts without witnessing an empty intersection, in which case $\mathbf{A}$ has a difference term operation.

Most of the operations carried out by this algorithm are well known to be polynomial-time. For example, the fact that the running time of subalgebra generation is polynomial has been known for a long time (see [JL76]). The time complexity of congruence generation is also known to be polynomial (see [Fre08]). The only operation whose tractability might be called into question is the commutator, but, as we saw in the proof of Proposition 11 above, there is a straight-forward polynomial-time algorithm for computing it. □

More details on the complexity of operations carried out by the algorithm, and many other algebraic operations, can be found in the references mentioned in the preceding paragraph, but see also [BS02, BJS99, FV09]. It is also worth remarking that the algorithm above is "embarrassingly parallel" since each pair of triples can be tested in isolation, on a single thread, without communicating with processes testing other triples.

5.3. **Computing a difference term operation.** Let $\mathbf{A} = \langle A, \ldots \rangle$ be a finite idempotent algebra and suppose we know that a difference term operation for $\mathbf{A}$ exists. In this section we describe an algorithm for constructing a difference term operation (given that we know such an operation exists).

**wjd** 2017-11-17: Does the alg ever use the fact that an LD term exists?

We build up the algorithm in stages. Section 5.3.1 gives a procedure (Algorithm 1) for finding an LD term for sets of size 2, and Section 5.3.2 gives two inductive steps (Algorithms 2 and 3) for producing LD terms on successively larger subsets of $A^2 \times \{0, 1\}$.

5.3.1. *Base case.* An LD term for $((a_0, b_0, 0), (a_1, b_1, 0))$ is the first projection, $t(x, y, z) = x$. An LD term for the set $((a_0, b_0, 1), (a_1, b_1, 1))$ is the third projection, $t(x, y, z) = z$.

The remaining sets of size 2 have the form $((a_0, b_0, 0), (a_1, b_1, 1))$, and an LD term for such sets can be computed by Algorithm 1, as described in the box below.

In practice, there are a number of different ways we could structure this algorithm when implementing it in software, and it should be obvious that the ordering of the first three steps is inconsequential.[4]

[4] For instance, we might structure the algorithm in one of the following ways:

(1) Compute $\delta_0 = [\theta_0, \theta_0]$, then present $\mathrm{Sg}^{\mathbf{A}\times\mathbf{A}}((a_0, a_1), (b_0, a_1), (b_0, b_1))$ as a (call-by-need) stream $S_0$; filter $S_0$ against the predicate $s \in (a_0/\delta_0) \times \{b_1\}$; the result is a stream from which we take (compute) the first element.

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

**Algorithm 1:** Return an LD term for $((a_0, b_0, 0), (a_1, b_1, 1))$

**Input** : $S = ((a_0, b_0, 0), (a_1, b_1, 1))$
**Output:** $t \in \mathcal{D}(S)$

1 compute $\delta_0 = [\theta_0, \theta_0]$;
2 form $C_0 = (a_0/\delta_0) \times \{b_1\}$;
3 compute $S_0 = \mathrm{Sg}^{\mathbf{A}\times\mathbf{A}}((a_0, a_1), (b_0, a_1), (b_0, b_1))$;
4 find a term $t$ such that $(t^{\mathbf{A}}(a_0, b_0, b_0), t^{\mathbf{A}}(a_1, a_1, b_1)) \in C_0 \cap S_0$;
5 return $t$

5.3.2. *Induction step.* Here are some notational conventions we use in this section.

$$\begin{aligned}
\mathcal{A}_0 &:= \{(a_0, b_0, 0), (a_0, b_0, 1)\},\\
\mathcal{A}_1 &:= \{(a_0, b_0, 0), (a_0, b_0, 1), (a_1, b_1, 0)\},\\
\mathcal{A}_2 &:= \{(a_0, b_0, 0), (a_0, b_0, 1), (a_1, b_1, 0), (a_1, b_1, 1)\},\\
&\vdots\\
\mathcal{A}_{2k} &:= \{(a_0, b_0, 0), (a_0, b_0, 1), \dots, (a_k, b_k, 0), (a_k, b_k, 1)\}.
\end{aligned}$$

That is, $\mathcal{A}_{2k} := \mathcal{A}_{2k-1} \cup \{(a_k, b_k, 1)\}$ and $\mathcal{A}_{2k+1} := \mathcal{A}_{2k} \cup \{(a_{k+1}, b_{k+1}, 0)\}$. Let

$$\begin{aligned}
\zeta_i &:= \mathcal{D}(\{(a_i, b_i, 0)\}),\\
\zeta_{\underline{k}} &:= \bigcap_{0\leqslant i<k} \zeta_i = \mathcal{D}(\{(a_0, b_0, 0), \dots, (a_{k-1}, b_{k-1}, 0)\}),\\
\eta_i &:= \mathcal{D}(\{(a_i, b_i, 1)\}),\\
\eta_{\underline{k}} &:= \bigcap_{0\leqslant i<k} \eta_i = \mathcal{D}(\{(a_0, b_0, 1), \dots, (a_{k-1}, b_{k-1}, 1)\}).
\end{aligned}$$

Algorithm 1 serves as a base case, giving an LD term for $\mathcal{A}_0$ that we will use as input to Algorithm 2, the output of which is an LD term for $\mathcal{A}_1$. That output will serve in turn as input to Algorithm 3 the result of which is an LD term for $\mathcal{A}_2$. Thereafter, this process alternates between Algorithms 2 and 3. Inductively, we obtain a single LD term for all of $A^2 \times \{0, 1\}$, which is a difference term operation for $\mathbf{A}$.

(2) Alternatively, while generating elements of $S_0$ in Step 3 of Algorithm 1, we simultaneously check whether any of these elements belongs to $C_0$. If so, the algorithm halts (without necessarily computing all of $S_0$).

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

**Algorithm 2:** Return LD term for $\mathcal{A}_{2k+1}$, given $\eta_{\underline{k}}$ and LD term for $\mathcal{A}_{2k}$.

**Input** : $\eta_{\underline{k}}$ and $s_{2k} \in \mathcal{D}(\mathcal{A}_{2k})$
**Output:** $\eta_{\underline{k+1}}$ and $s_{2k+1} \in \mathcal{D}(\mathcal{A}_{2k+1})$

1 construct $p \in \eta_{\underline{k}} \cap \mathcal{D}(\{(a_{k+1}, s_{2k}(a_{k+1}, b_{k+1}, b_{k+1}), 0)\})$
2 construct $s_{2k+1}(x, y, z) = p(x, s_{2k}(x, y, y), s_{2k}(x, y, z))$;
3 construct $\eta_{\underline{k+1}} = \eta_{\underline{k}} \cap \eta_k$;
4 return $(s_{2k+1}, \eta_{\underline{k+1}})$.

**Algorithm 3:** Return an LD term for $\mathcal{A}_{2k}$ given $\zeta_{\underline{k}}$ and an LD term for $\mathcal{A}_{2k-1}$.

**Input** : $\zeta_{\underline{k-1}}$ and $s_{2k-1} \in \mathcal{D}(\mathcal{A}_{2k-1})$
**Output:** $\zeta_{\underline{k}}$ and $s_{2k} \in \mathcal{D}(\mathcal{A}_{2k})$

1 construct $p \in \zeta_{\underline{k-1}} \cap \mathcal{D}(\{(s_{2k-1}(a_k, a_k, b_k), b_k, 1)\})$;
2 construct $s_{2k}(x, y, z) = p(s_{2k-1}(x, y, z), s_{2k-1}(y, y, z), z)$;
3 construct $\zeta_{\underline{k}} = \zeta_{\underline{k-1}} \cap \zeta_{k-1}$
4 return $(s_{2k}, \zeta_{\underline{k}})$.

## References


[BJS99] Clifford Bergman, David Juedes, and Giora Slutzki. Computational complexity of term-equivalence. *Internat. J. Algebra Comput.*, 9(1):113–128, 1999. URL: http://dx.doi.org/10.1142/S0218196799000084, doi:10.1142/S0218196799000084.

[BS02] Clifford Bergman and Giora Slutzki. Computational complexity of some problems involving congruences on algebras. *Theoret. Comput. Sci.*, 270(1-2):591–608, 2002. URL: http://dx.doi.org/10.1016/S0304-3975(01)00009-3, doi:10.1016/S0304-3975(01)00009-3.

[Fre08] Ralph Freese. Computing congruences efficiently. *Algebra Universalis*, 59(3-4):337–343, 2008. URL: http://dx.doi.org/10.1007/s00012-008-2073-1, doi:10.1007/s00012-008-2073-1.

[FV09] Ralph Freese and Matthew A. Valeriote. On the complexity of some Maltsev conditions. *Internat. J. Algebra Comput.*, 19(1):41–77, 2009. URL: http://dx.doi.org/10.1142/S0218196709004956, doi:10.1142/S0218196709004956.

[HM88] David Hobby and Ralph McKenzie. *The structure of finite algebras*, volume 76 of *Contemporary Mathematics*. American Mathematical Society, Providence, RI, 1988. Available from: math.hawaii.edu.

[Hor13] Jonah Horowitz. Computational complexity of various Mal'cev conditions. *Internat. J. Algebra Comput.*, 23(6):1521–1531, 2013. URL: http://dx.doi.org/10.1142/S0218196713500343, doi:10.1142/S0218196713500343.


WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)

[JL76] Neil D. Jones and William T. Laaser. Complete problems for deterministic polynomial time. *Theoret. Comput. Sci.*, 3(1):105–117 (1977), 1976. URL: http://dx.doi.org/10.1016/0304-3975(76)90068-2, doi:10.1016/0304-3975(76)90068-2.

[Kea95] Keith A. Kearnes. Varieties with a difference term. *J. Algebra*, 177(3):926–960, 1995. URL: http://dx.doi.org/10.1006/jabr.1995.1334, doi:10.1006/jabr.1995.1334.

[KK99] Keith A. Kearnes and Emil W. Kiss. Modularity prevents tails. *Proc. Amer. Math. Soc.*, 127(1):11–19, 1999.

[KK13] Keith A. Kearnes and Emil W. Kiss. The shape of congruence lattices. *Mem. Amer. Math. Soc.*, 222(1046):viii+169, 2013. URL: http://dx.doi.org/10.1090/S0065-9266-2012-00667-8, doi:10.1090/S0065-9266-2012-00667-8.

[KS98] Keith A. Kearnes and Ágnes Szendrei. The relationship between two commutators. *Internat. J. Algebra Comput.*, 8(4):497–531, 1998. URL: http://dx.doi.org/10.1142/S0218196798000247, doi:10.1142/S0218196798000247.

[KSW] Keith Kearnes, Ágnes Szendrei, and Ross Willard. Simpler Maltsev conditions for (weak) difference terms in locally finite varieties. to appear.

[KSW16] Keith Kearnes, Ágnes Szendrei, and Ross Willard. A finite basis theorem for difference-term varieties with a finite residual bound. *Trans. Amer. Math. Soc.*, 368(3):2115–2143, 2016. URL: http://dx.doi.org/10.1090/tran/6509, doi:10.1090/tran/6509.

[Sze92] Ágnes. Szendrei. A survey on strictly simple algebras and minimal varieties. In *Universal algebra and quasigroup theory (Jadwisin, 1989)*, volume 19 of *Res. Exp. Math.*, pages 209–239. Heldermann, Berlin, 1992.

[Val09] Matthew A. Valeriote. A subalgebra intersection property for congruence distributive varieties. *Canad. J. Math.*, 61(2):451–464, 2009. URL: http://dx.doi.org/10.4153/CJM-2009-023-2, doi:10.4153/CJM-2009-023-2.

[VW14] M. Valeriote and R. Willard. Idempotent $n$-permutable varieties. *Bull. Lond. Math. Soc.*, 46(4):870–880, 2014. URL: http://dx.doi.org/10.1112/blms/bdu044, doi:10.1112/blms/bdu044.

*E-mail address*: williamdemeo@gmail.com
*URL*: http://williamdemeo.github.io

University of Colorado, Mathematics Dept, Boulder 80309, USA

*E-mail address*: ralph@math.hawaii.edu
*URL*: http://www.math.hawaii.edu/~ralph/

University of Hawaii, Mathematics Dept, Honolulu 96822, USA

*E-mail address*: matt@math.mcmaster.ca
*URL*: http://ms.mcmaster.ca/~matt/

McMaster University, Mathematics Dept, Hamilton L8S 4K1, CAN

WORK IN PROGRESS. DO NOT DISTRIBUTE. (compiled on 2017-11-17 at 15:45:46)