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 in the idempotent case and then describe possible 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 $\mathbf{A} = \langle A, \dots\rangle \in \mathcal{V}$, 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 θ 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 many useful properties of the algebras inhabiting that variety. Very roughly speaking, having a difference term is slightly stronger than having a Taylor term and slightly weaker than having a Mal'cev 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.)

Digital computers have turned out to be invaluable tools for exploring and understanding algebras and the varieties they inhabit, and this is largely due to the fact that, over the last three decades, researchers

Date: 2017/07/18.

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

have found ingenious ways to get computers to solve challenging abstract decision problems—such as whether a variety is congruence n-permutable ([VW14]), or congruence modular ([FV09])—and to do so very quickly. This paper contributes to this effort by finding an efficient algorithm for deciding whether a locally finite idempotent variety has a difference term.

The central question motivating this project 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?

In [Kea95] Kearnes proved the following theorem, which is basic for our studies.

Theorem 1. *The variety $\mathcal{V} = \mathbb{V}(\mathbf{A})$ generated by a finite algebra $\mathbf{A}$ has a difference if and only if it has a Taylor term and, for all finite algebras $\mathbf{B} \in \mathcal{V}$, the minimal sets of every type $\mathbf{2}$ prime interval in* $\operatorname{Con}(\mathbf{B})$ *have empty tails.*

No 1's is poly-time decidable by Valeriote's subtype theorem. In [FV09], Freese and Valeriote solved an analogous problem, by giving a positive answer to the following

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 (CM)?

Congruence modularity is characterized by no 1's, no 5's and no tails. Again no 1's and no 5's can be decided by the subtype theorem, and in [FV09] the authors prove that if there is a tail in $\mathbb{V}(\mathbf{A})$, there is a tail "near the bottom." More precisely, if $\mathbf{A}$ is finite and idempotent, and $\mathbb{V}(\mathbf{A})$ has no 1's and no 5's and has tails, then there is a tail in a 3-generated subalgebra of $\mathbf{A}^2$. Using this it is proved that deciding CM is polynomial-time.

But the proof of the no tails part uses that in a variety with no 1's or 5's, the congruence lattice modulo the *solvability congruence* (defined below) is (join) semidistributive. Now, restricting to just testing no type-$\mathbf{2}$ tails (vs no tails of any type) is not a problem. So, for example, there is a poly-time algorithm for testing if $\mathbb{V}(\mathbf{A})$ has no 1's, no 5's and no type-$\mathbf{2}$ tails.

Here is a related problem.

Problem 3. Is there an $\mathbf{A}$, idempotent and having a Taylor term, no type-2 tail in subalgebras of $\mathbf{A}^k$, for $k < n$, but having a type-$\mathbf{2}$ tail in a subalgebra of $\mathbf{A}^n$.

Perhaps we could construct such an algebra using congruence lattice representation techniques.

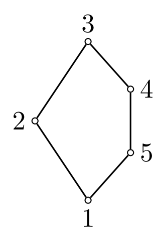
2. Background, definitions, and notation

Our starting point is the set of lemmas at the beginning of Section 3 in the Freese-Valeriote paper [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 copied from the nice presentation of TCT background that appears in [FV09, Sec. 2].)

The 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 β-classes is captured by the so-called (α, β)-traces [HM88, Def. 2.15]. Modulo α, the induced structure on the traces is limited to one of five possible types:

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

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



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

(1) $j = 1$ then $\mathbf{S}$ is term equivalent to a 2-element set;

TABLE 1. [KKVW15].

Omitting Class	Equivalent Property
$\mathcal{M}_{\{1\}}$	satisfies a nontrivial idempotent Mal'tsev condition
$\mathcal{M}_{\{1,5\}}$	satisfies a nontrivial congruence identity
$\mathcal{M}_{\{1,4,5\}}$	congruence n-permutable, for some $n > 1$
$\mathcal{M}_{\{1,2\}}$	congruence meet semidistributive
$\mathcal{M}_{\{1,2,5\}}$	congruence join semidistributive
$\mathcal{M}_{\{1,2,4,5\}}$	congruence n-permutable for some n and congruence join semidistributive

(2) $j = 2$ then $\mathbf{S}$ is term equivalent to the idempotent reduct of a module;
(3) $j = 3$ then $\mathbf{S}$ is functionally complete;
(4) $j = 4$ then $\mathbf{S}$ is polynomially equivalent to a 2-element lattice;
(5) $j = 5$ then $\mathbf{S}$ is term equivalent to a 2-element semilattice.

Proof. This is a combination of [Val09, Prop. 3.1] and [Sze92, Thm. 6.1]. □

Table 1 is from [KKVW15] and gives another characterization of omitting types.

In Section 3, the following result will be useful.

Corollary 3. *[cf. [FV09, Lem. 3.3]] [Cor. 2.2 [FV09]] 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. THE FREESE-VALERIOTE LEMMAS REVISITED

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 CM variety.

According to the characterization in [HM88, Ch. 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]. Note that 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, on omitting types $\mathbf{1}$ and $\mathbf{5}$ (or $\mathbf{1}$, $\mathbf{2}$, and **5**) by searching for a 2-generated subalgebra of $\mathbf{A}$ whose typeset is not contained in $\{\mathbf{2},\mathbf{3},\mathbf{4}\}$ ($\{\mathbf{3},\mathbf{4}\}$). It is proved in [FV09, Sec. 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 $\mathbf{A}$. In [FV09, Sec. 3], Freese and Valeriote prove a sequence of lemmas to establish that, 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 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 non-empty tails or else there are non-empty tails that are easy to find (since they occur in 3-generated subalgebras 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.[1]

Our goal is to use the same strategy to solve Problem 1. As such, we revisit each lemma in Section 3 of [FV09], and consider whether it can be proved under modified hypotheses. Specifically, we continue to assume that the type set of $\mathbb{V}(\mathbf{A})$ contains no **1**'s, but we will now drop the "no **5**'s" assumption. We will attempt to prove that 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 $\mathbf{A}^2$). We continue to quote [FV09] where possible, while modifying the assumptions and adjusting the arguments as necessary.

Throughout, we let $\underline{n}$ denote the set $\{0, 1, \dots, n-1\}$ and we let $\mathcal{S}$ be a finite set of finite, similar, idempotent algebras, closed under the taking of subalgebras, such that $\mathcal{V} = \mathbb{V}(\mathcal{S})$ omits type-**1** (but may include type-**5**). If there is a finite algebra in $\mathcal{V}$ having a type-**2** minimal set with a tail, then, by standard Tame Congruence Theory, there is such an algebra which is 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** whose minimal sets have non-empty 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 some $\mathbf{A}_0, \mathbf{A}_1, \dots, \mathbf{A}_{n-1}$ in $\mathcal{S}$, there is a subdirect product $\mathbf{B} \leqslant_{\mathrm{sd}} \prod_{\underline{n}} \mathbf{A}_i$

[1]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 $\mathbf{A}$.

that has a prime quotient of type **2** whose minimal sets have non-empty 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** such that its minimal sets have non-empty tails, and choose β minimal with this property. By [HM88, Lemma 6.2] this implies β is join irreducible and α is its unique subcover. Let U be an (α, β)-minimal set.

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

Proof. Since β is join irreducible with unique subcover α, any pair of elements in $\beta - \alpha$ generates β.

Let $\mathbf{C}$ be the subalgebra of $\mathbf{B}$ generated by $\{0, 1, t\}$. We will obtain a contradiction under the assumption that $|C| < |B|$ and the minimal sets of $\mathbf{C}$ which have type **2** all have empty tails. Let β' and α' be the restrictions of β and α 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 (α, β) is type **2**, β is abelian over α. This implies β' is abelian over α' by [KK13, Lemma 2.19(9)], which implies the types of the prime quotients occurring between α' and β' are **1** or **2**. But since we are assuming $\mathbf{B}$ has a Taylor term, they are all of type **2**. In particular, (δ, γ) has type **2**.

Suppose that $|C| < |B|$ and all $\langle \delta, \gamma \rangle$ minimal sets have empty 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 Theorem 2.8 of [HM88] 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 $\mathcal{V}$ and so 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 $(p'(0), p'(1)) \in \beta - \alpha$ and so p' must map the minimal set U onto a polynomially isomorphic set W.

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

For $i \leqslant n$, let ρ_i denote the kernel of the projection of $\mathbf{B}$ onto $\mathbf{A}_i$, so $\mathbf{B} \cong \mathbf{A}_i/\rho_i$. 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 ρ_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, Lem. 3.2])**.** *For every proper nonempty subset $\sigma \subset \underline{n}$, either $\beta \leqslant \rho_\sigma$ or $\alpha \vee \rho_\sigma = 1_B$.*

Proof. Let $\rho = \rho_\sigma$. Suppose that $\beta \nleqslant \rho$ (or equivalently $(0,1) \notin \rho$). Since β 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 $\mathbf{2}$ whose minimal sets have non-empty 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 Lemma 2.4 of [HM88], 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 α and β. 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 Maltsev 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 $\sigma \subset \underline{n}$, for all $v \in B$, and for all $c \in \mathrm{Body}(U)$, we have $(v, c) \in \beta \circ \rho_\sigma \cap \rho_\sigma \circ \beta$.*

Proof. Let $\rho = \rho_\sigma$. Note that $\beta \vee \rho = 1_B$ implies $\beta\big|_U \vee \rho\big|_U = 1_U$ 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 $a \in \mathrm{Body}(U)$ and $t \in \mathrm{Tail}(U)$ such that $a \mathrel{\rho} t$.

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.

Next, fix an arbitrary element $c \in \mathrm{Body}(U)$ and let $p(x) = d(x, a, c)$. Then (see [HM88, Lem. 4.20]) we have

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

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

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

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

and

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

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

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

(i) There exists $0 \leqslant i < n$ *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 $\alpha \vee \rho_\sigma = 1_B$ since otherwise, by Lemma 5, we have $\alpha \leqslant \beta \leqslant \rho_\sigma \leqslant \rho_i$ for $i \in \sigma$, so $\alpha \vee \rho_i = \rho_i < 1_B$, contradicting (2). Therefore, $\beta \vee \rho_\sigma = 1_B$.

Let $b \in \mathrm{Body}(U)$ and $t \in \mathrm{Tail}(U)$. 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, $(b, t) \in \beta \circ \rho$ so there is an element $a \in B$ with $b\ \beta\ a\ \rho_i\ t$. By applying the idempotent polynomial e with

$e(U) = U$ to this, we may assume $a \in U$ and, since $a \ \beta \ b$, $a \in \text{Body}(U)$. So

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

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

Theorem 8 (Thm. 3.4 [FV09]). *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 non-empty 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 $0 \le i \le n-1$ 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 $j \le n$ with $\beta \le \rho_i$ 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 $\beta \le \rho$ or $\alpha \vee \rho = 1_B$. This yields a contradiction as the former is not possible, since $\beta \not\le \rho_j$ and the latter can't hold since both α and ρ are below ρ_i.

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

The next theorem essentially gives an algorithm to decide if a finitely generated 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 $\langle \alpha, \beta \rangle$ minimal sets, where $\alpha \prec \beta$, having tails, and $\alpha \prec \beta$ being the critical interval of a pentagon. By Theorem 2.1 of [KK99], 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 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 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 θ is a congruence of $\mathbf{A}$, let $\theta_0 \in \text{Con}(\mathbf{B})$ be defined by $(x_0, x_1) \ \theta_0 \ (y_0, y_1)$ if $x_0 \ \theta \ y_0$. Of course θ_1 is defined similarly. In the case $\theta = 0_{\mathbf{A}}$ is the least congruence, we use the notation ρ_0 and ρ_1 instead of 0_0 and 0_1. Of course ρ_0 and ρ_1 are the kernels of the first and second projections of $\mathbf{B}$ onto $\mathbf{A}$.

Theorem 9. *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) $\mathbf{A}$ *has a Taylor term.*

(2) *There do not exist a, b and $c \in A$ such that, if* $\mathbf{B}$ *is the subalgebra of* $\mathbf{A}$ *generated by a, b and c, $\beta = \mathrm{Cg}^{\mathbf{B}}(a,b)$, and* $\mathbf{C}$ *is the subalgebra of* $\mathbf{B}^2$ *generated by (a,b), (a,c), (b,c) and the diagonal of B,*
 (a) *β is join irreducible with lower cover α,*
 (b) *$((a,b),(b,b)) \notin \delta$,*
 (c) *$[\beta,\beta] \leq \alpha$, and*
 where $\delta = (\alpha_0 \wedge \alpha_1) \vee \mathrm{Cg}^{\mathbf{C}}((a,c),(b,c))$.

(3) *There do not exist x_0, x_1, y_0, and $y_1 \in A$ satisfying the following conditions, 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 $t = (x_0,y_1)$, ρ_0 is the kernel of the first projection, and $\beta = \mathrm{Cg}^{\mathbf{B}}(0,1)$,*
 (a) *β is join irreducible with lower cover α,*
 (b) *$\rho_0 \vee \alpha = 1_{\mathbf{B}}$, and*
 (c) *the type of β over α 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. Let $\theta = \delta \vee \mathrm{Cg}^{\mathbf{C}}((a,b),(b,b))$. By its definition, $\delta \nleq \alpha_0$. So, by (2b), $\alpha_0 \wedge \alpha_1 < \delta < \theta \leq \beta_0$. Since C contains the diagonal of B, the coordinate projections are onto, and so, $\alpha_0 \prec \beta_0$ and has type **2**. From this it follows that $\alpha_0 \vee \delta = \beta_0$. Since $\theta \leq \alpha_1$, $\alpha_0 \wedge \theta = \alpha_0 \wedge \alpha_1$. 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 $[\theta,\theta] \leqslant \alpha_0 \wedge \alpha_1 < \delta$. Hence the is a congruence δ' such that $\delta \leqslant \delta' \prec \theta$ and this covering has type **2**. As mentioned in the discussion above, this implies the $\langle \delta', \theta \rangle$ minimal sets have tails, contradicting Theorem 1.

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 tppe **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 α such that the type of β over α 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 β over α is $\mathbf{2}$, (2c) holds and we already have (2a) holds. That (2b) holds is proved in Theorem 2.4 of [KK99]. 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,

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

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

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

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

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

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

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

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

where $\Delta_{\beta,\alpha}$ is the congruence on the subalgebra of $\mathbf{A}^2$ with universe β 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 11. *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 9 gives a three-step algorithm to test if $\mathbb{V}(\mathbf{A})$ has a difference term. The first step is to test if $\mathbf{A}$ has a Taylor term. By Theorem 6.3 of [FV09], this can be done in time crn^3m.

Looking now at part (3) of Theorem 9, there are several things that have to be constructed. By Proposition 10, all of 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 β over α is **2**. Since at this point in the algorithm we know that $\mathbf{A}$ has a Taylor term, we can test if the type is **2** by testing if $[\beta, \beta] \leq \alpha$. By Proposition 10 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.

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, locally finite) 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 11 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.

wjd 2017.6.12: We should insert an example of an algebra $\mathbf{A}$ that has a difference term operation and is such that $\mathbb{V}(\mathbf{A})$ has no difference term.

In this section we present solutions to problems (1) and (2) using methods that are entirely different to 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 algebra $\mathbf{A}$ has a difference term operation. In Subsection 5.3 we address problem (2) by presenting a (non-polynomial-time) algorithm for constructing a difference term operation. We suspect there is a polynomial-time algorithm for constructing a difference term when one is known to exist. However, we don't have such an algorithm yet.

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'cev 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.

Let $\mathbf{A} = \langle A, \dots \rangle$ be an algebra, fix $a, b \in A$ and denote by $\theta_{ab} := \mathrm{Cg}^{\mathbf{A}}(a, b)$ the congruence of $\mathbf{A}$ generated by a and b. Let $i \in \{0, 1\}$. A *local difference term operation for* (a, b, i) is a ternary term operation ℓ satisfying the following:

$$\begin{aligned} &\text{if } i = 0, \text{ then } a\, [\theta_{ab}, \theta_{ab}]\, \ell(a, b, b); \\ &\text{if } i = 1, \text{ then } \ell(a, a, b) = b. \end{aligned} \tag{3}$$

If ℓ satisfies (3) for all triples in some subset $S \subseteq A^2 \times \{0, 1\}$, then we call ℓ 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." One more bit of notation will come in handy below.

Given a subset $T \subseteq \mathsf{Clo}_3(\mathbf{A})$ of ternary term operations on $\mathbf{A}$, and a subset $S \subseteq A^2 \times \{0,1\}$, denote by $\bowtie$ the relation from T to S defined by $t \bowtie (a,b,i)$ iff the following conditions hold:

$$\begin{aligned} &\text{if } i = 0, \quad a\ [\theta_{ab}, \theta_{ab}]\ t(a,b,b); \\ &\text{if } i = 1, \qquad\quad t(a,a,b) = b. \end{aligned}$$

As a binary relation, $\bowtie$ induces an obvious *Galois connection* from subsets of $\mathsf{Clo}_3(\mathbf{A})$ to subsets of $A^2 \times \{0,1\}$ and back—namely,

$$\begin{aligned} &\widehat{\mathsf{LD}}\colon \mathcal{P}(\mathsf{Clo}_3(\mathbf{A})) \to \mathcal{P}(A^2 \times \{0,1\}), \text{ and} \\ &\mathsf{LD}\colon \mathcal{P}(A^2 \times \{0,1\}) \to \mathcal{P}(\mathsf{Clo}_3(\mathbf{A})), \end{aligned}$$

are defined as follows: for $T \subseteq \mathsf{Clo}_3(\mathbf{A})$ and $S \subseteq A^2 \times \{0,1\}$,

$$\begin{aligned} \widehat{\mathsf{LD}}(T) &= \{s \in A^2 \times \{0,1\} \mid t \bowtie s \text{ for all } t \in T\}, \\ \mathsf{LD}(S) &= \{t \in \mathsf{Clo}_3(\mathbf{A}) \mid t \bowtie s \text{ for all } s \in S\}. \end{aligned}$$

In other words, the set of local difference term operations for S is $\mathsf{LD}(S)$. We S is finite, say $S = ((a_0,b_0,\chi_0),\dots,(a_n,b_n,\chi_n)$, where usually write $\mathsf{LD}((a_0,b_0,\chi_0),\dots,(a_n,b_n,\chi_n))$.

The subset of $A^2 \times \{0,1\}$ for which every $t \in T$ is an LD term is denoted by $\widehat{\mathsf{LD}}(T)$

Now, suppose that every pair $(s_0,s_1) \in (A^2 \times \{0,1\})^2$ has an LD term. That is, suppose $\mathsf{LD}(s_0,s_1)$ is nonempty. Under this hypothesis we will prove that every subset $S \subseteq A^2 \times \{0,1\}$ has an LD term.

Theorem 12. *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 $2 \leqslant k \leqslant n$ has an LD term. Let

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

so that $|S| = n+1$. We prove S has an LD term.

Since $|S| \geqslant 3$ and $\chi_i \in \{0,1\}$ for all i, there must exist indices $i \neq j$ such that $\chi_i = \chi_j$. Assume without loss of generality that one of these indices is $j = n$. Define the set $S' = S - \{(a_n,b_n,\chi_n)\}$. Since $|S'| < |S|$, the set S' has an LD term p. We split the remainder of the proof into two cases.

<u>Case $\chi_n = 0$</u>: Without loss of generality, suppose that

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

Define

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

and note that $|S_1| < |S|$. Let q be an LD term for S_1. We show that

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

is an LD term for S.

Since $\chi_n = 0$, we first verify that $a_n\ [\theta_n, \theta_n]\ d(a_n, b_n, b_n)$. If we let $\gamma = \mathrm{Cg}(a_n, p(a_n, b_n, b_n))$, then

$$d(a_n, b_n, b_n) = q(a_n, p(a_n, b_n, b_n), p(a_n, b_n, b_n))\ [\gamma, \gamma]\ a_n. \tag{4}$$

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 $\theta_n := \mathrm{Cg}^{\mathbf{A}}(a_n, b_n)$. Therefore, $\gamma \leqslant \theta_n$, so $[\gamma, \gamma] \leqslant [\theta_n, \theta_n]$, by monotonicity of the commutator. It follows from this and (4) that $a_n\ [\theta_n, \theta_n]\ d(a_n, b_n, b_n)$, as desired.

For the indices $0 \leqslant i < k$ we have $\chi_i = 1$, so we prove $d(a_i, a_i, b_i) = b_i$ for these indices. 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 $q \in \mathsf{LD}(S_1)$.

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

$$d(a_j, b_j, b_j) = q(a_j, p(a_j, b_j, b_j), p(a_j, b_j, b_j)). \tag{5}$$

Since $p \in \mathsf{LD}(S')$, we have $a_j\ [\theta_j, \theta_j]\ p(a_j, b_j, b_j)$, so (5) 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

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

Define

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

and note that $|S_0| < |S|$. Let $q \in \mathsf{LD}(S_0)$ and define $d(x, y, z) = q(p(x, y, z), p(y, y, z), z)$. Since $\chi_n = 1$, we must show that $d(a_n, a_n, b_n) = b_n$. By the definition of d,

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

The last equality holds since $q \in \mathsf{LD}(S_0) \subseteq \mathsf{LD}(p(a_n, a_n, b_n), b_n, 1)$.

If $1 \leqslant i \leqslant k$, 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

$$d(a_i, b_i, b_i) = q(p(a_i, b_i, b_i), p(b_i, b_i, b_i), b_i) = q(p(a_i, b_i, b_i), b_i, b_i). \tag{6}$$

Next, since $p \in \mathsf{LD}(S')$,

$$q(p(a_i, b_i, b_i), b_i, b_i)\ [\theta_i, \theta_i]\ q(a_i, b_i, b_i). \tag{7}$$

Since $q \in \mathsf{LD}(S_0)$, we have $q(a_i, b_i, b_i)\ [\theta_i, \theta_i]\ a_i$, so (6) and (7) 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 $p \in \mathsf{LD}(S')$, $p(a_j, a_j, b_j) = b_j$; this plus idempotence of q yields

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

□

Here is an obvious corollary of Theorem 12.

Corollary 13. *Let* $\mathbf{A}$ *be a finite idempotent algebra. If* $\mathsf{LD}(s, s') \neq \emptyset$ *for all pairs* $(s, s') \in (A^2 \times \{0, 1\})^2$*, then* $\mathsf{LD}(A^2 \times \{0, 1\}) \neq \emptyset$*, and* $\mathbf{A}$ *has a difference term operation.*

Proof. If we let $S = A^2 \times \{0, 1\}$ in Theorem 12, then there exists a term operation $d \in \mathsf{LD}(A^2 \times \{0, 1\})$, so for all $a, b \in A$ we have $a\ [\mathrm{Cg}(a, b), \mathrm{Cg}(a, b)]\ d(a, b, b)$, (since $d \in \mathsf{LD}((a, b, 0))$) and $d(a, a, b) = b$ (since $d \in \mathsf{LD}((a, b, 1))$). □

5.2. Algorithm to test existence of difference term operation.

Here is the practical consequence of Theorem 12.

Corollary 14. *There is a polynomial-time algorithm that takes as input any finite idempotent algebra* $\mathbf{A}$ *and decides whether* $\mathbf{A}$ *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 13, 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 to consider are (1) $i = 0$ and $i' = 1$, and (2) $i = 1$ and $i' = 0$. Since these are symmetric, we only handle the first case. Assume the given pair of triples are $((a, b, 0), (a', b', 1))$. By definition, $t \in \mathsf{LD}\{(a, b, 0), (a', b', 1)\}$ iff

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

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 $t \in \mathsf{LD}\{(a,b,0),(a',b',1)\}$ iff

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

where $\delta = [\mathrm{Cg}(a,b), \mathrm{Cg}(a,b)]$ and a/δ denotes the δ-class containing a. It follows that the pair $((a,b,0),(a',b',1))$ has an LD term 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 $\delta = [\mathrm{Cg}(a,b), \mathrm{Cg}(a,b)]$,
(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.

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 there is a straight-forward algorithm for computing it (see [DeM17]). $\square$

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 $\mathbf{A} = \langle A, \dots\rangle$ 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). We build up the algorithm in stages. Subsection 5.3.1 gives a procedure (Algorithm 1) for finding an LD term for sets of size 2, and Subsection 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 operation for the set $\{(a_0, b_0, 0), (a_1, b_1, 0)\}$ is the first projection, $t(x, y, z) = x$. An LD term operation 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. (In the following algorithm descriptions, we continue to use the shorthand notations established above, such as $\theta_0 = \mathrm{Cg}^{\mathbf{A}}(a_0, b_0)$.)

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: $t \in \mathsf{LD}(S)$ (an LD term for 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

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.[2]

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

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

[2] 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.
(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).

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

$$\zeta_i = \mathrm{LD}(a_i, b_i, 0) \quad \text{and} \quad \zeta_{\underline{k}} = \bigcap_{0 \leqslant i < k} \zeta_i = \mathrm{LD}\{(a_i, b_i, 0) \mid 0 \leqslant i < k\},$$

$$\eta_i = \mathrm{LD}(a_i, b_i, 1) \quad \text{and} \quad \eta_{\underline{k}} = \bigcap_{0 \leqslant i < k} \eta_i = \mathrm{LD}\{(a_i, b_i, 1) \mid 0 \leqslant i < k\}.$$

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 $\mathbf{A}$.

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

Input : $\eta_{\underline{k}}$ and $s_{2k} \in \mathrm{LD}(\mathcal{A}_{2k})$
Output: $\eta_{\underline{k+1}}$ and $s_{2k+1} \in \mathrm{LD}(\mathcal{A}_{2k+1})$
compute $p \in \eta_{\underline{k}} \cap \mathrm{LD}(a_{k+1}, s_{2k}(a_{k+1}, b_{k+1}, b_{k+1}), 0)$
return $(s_{2k+1}, \eta_{\underline{k+1}})$ where
$s_{2k+1}(x, y, z) = p(x, s_{2k}(x, y, y), s_{2k}(x, y, z))$.

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 $s_{2k-1} \in \mathrm{LD}(\mathcal{A}_{2k-1})$
Output: $\zeta_{\underline{k}}$ and $s_{2k} \in \mathrm{LD}(\mathcal{A}_{2k})$
compute $p \in \zeta_{\underline{k-1}} \cap \mathrm{LD}(s_{2k-1}(a_k, a_k, b_k), b_k, 1)$;
return $(s_{2k}, \zeta_{\underline{k}})$ where
$s_{2k}(x, y, z) = p(s_{2k-1}(x, y, z), s_{2k-1}(y, y, z), z)$.

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.

[DeM17] W. DeMeo. The Commutator as Least Fixed Point of a Closure Operator. *ArXiv e-prints*, March 2017. arXiv:1703.02764.

[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.

[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.

[KKVW15] Marcin Kozik, Andrei Krokhin, Matt Valeriote, and Ross Willard. Characterizations of several Maltsev conditions. *Algebra Universalis*, 73(3-4):205–224, 2015. URL: http://dx.doi.org/10.1007/s00012-015-0327-2, doi:10.1007/s00012-015-0327-2.

[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.

(William DeMeo) Department of Mathematics, University of Hawaii, Honolulu, Hawaii, 96822 USA

E-mail address, William DeMeo: demeo@math.hawaii.edu

(Ralph Freese) Department of Mathematics, University of Hawaii, Honolulu, Hawaii, 96822 USA

E-mail address, Ralph Freese: ralph@math.hawaii.edu

(Matthew Valeriote) Department of Mathematics, McMaster University, Hamilton, Ontario, xxxxx Canada

E-mail address, Mathhew Valeriote: matt@math.mcmaster.ca