A polynomial-time algorithm for deciding existence of difference terms

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 a related but easier question in the idempotent case. Using recent work of Valeriote and Willard as a guide, we define "local difference terms" and use these to find a polynomial-time algorithm for deciding whether any finite idempotent algebra has a difference term operation. Then we demonstrate that the notion of local difference term can be lifted up to a notion of "global-local difference terms" which enables us to devise an efficient algorithm for determining whether the variety generated by a finite idempotent algebra has a difference term.

1. Introduction

Let $\mathcal{V}$ be a variety (equational class) of algebras. A ternary term d in the language of $\mathcal{V}$ is called a *difference term for* $\mathcal{V}$ if it satisfies the following: for all $\mathbf{A} = \langle A, \ldots \rangle \in \mathcal{V}$ and $a, b \in A$ we have

$$d^{\mathbf{A}}(a, a, b) = b \quad \text{and} \quad d^{\mathbf{A}}(a, b, b) \; [\theta, \theta] \; a, \tag{1.1}$$

where θ is any congruence containing (a, b) and $[\cdot, \cdot]$ denotes the (term condition) commutator. (See [HM88] or [KK13] for definitions.) When the relations in (1.1) hold we will call $d^{\mathbf{A}}$ a *difference term operation* for $\mathbf{A}$.

Difference terms are studied extensively in the universal algebra literature. (See, for example, [HM88, Kea95, KK13, KS98, KSW16, KSW].) There are many reasons to study difference terms, but one of the most obvious is that knowing a variety has a difference term 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'tsev term. Note that if $\mathbf{A}$ is an *abelian* algebra—that is, $[1_A, 1_A] = 0_A$—then by the monotonicity of the commutator we have $[\theta, \theta] = 0_A$ for all $\theta \in \operatorname{Con} \mathbf{A}$, in which case (1.1) 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 researchers have found ingenious ways to get computers to solve abstract decision problems—such as whether a variety is congruence-modular ([FV09]) or congruence-n-permutable ([VW14])—and to do so efficiently. The contribution of the present paper is to present a solution to the following:

Presented by ...
Received ...; accepted in final form ...
Key words and phrases: difference terms.

Problem 1. Is there a polynomial-time algorithm that takes a finite idempotent algebra $\mathbf{A}$ as input and decides whether the variety generated by $\mathbf{A}$ has a difference term?

By solving Problem 1 we complete the project started in (TODO: insert LICS reference) where we solved the following easier problem:

Problem 2. Is there a polynomial-time algorithm that takes a finite idempotent algebra $\mathbf{A}$ as input and decides whether $\mathbf{A}$ has a difference term operation?

In [VW14], Valeriote and Willard 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. Inspired by that work, we devise a similar construct, called a "local difference term," that we use to develop a polynomial-time algorithm for deciding the existence of a (global) difference term operation.

2. Background, Notation, and Definitions

Our arguments depend on some basic results of universal algebra that we now review. For the most part we use standard notation such as those found in [Ber12]. However, we make the following exception for notational simplicity: if $\mathbf{A} = \langle A, \ldots \rangle$ is an algebra with elements $a, b \in A$, then we use $\theta(a, b)$ to denote the congruence of $\mathbf{A}$ generated by a and b.

Let $\mathbf{A} = \langle A, F^{\mathbf{A}} \rangle$ be an algebra. A reflexive, symmetric, compatible binary relation $T \subseteq A^2$ is called a *tolerance of* $\mathbf{A}$. Given a pair $(\mathbf{u}, \mathbf{v}) \in A^m \times A^m$ of m-tuples of A, we write $\mathbf{u}\ \mathbf{T}\ \mathbf{v}$ just in case $\mathbf{u}(i)\ T\ \mathbf{v}(i)$ for all $i \in \underline{m}$. We state a number of definitions in this section using tolerance relations, but the definitions don't change when the tolerance in question happens to be a congruence relation (i.e., a transitive tolerance).

Suppose S and T are tolerances on $\mathbf{A}$. An S, T-*matrix* is a 2×2 array of the form

$$\begin{bmatrix} t(\mathbf{a}, \mathbf{u}) & t(\mathbf{a}, \mathbf{v}) \\ t(\mathbf{b}, \mathbf{u}) & t(\mathbf{b}, \mathbf{v}) \end{bmatrix},$$

where t, $\mathbf{a}$, $\mathbf{b}$, $\mathbf{u}$, $\mathbf{v}$ have the following properties:

(i) $t \in \mathsf{Clo}_{\ell+m}(\mathbf{A})$,
(ii) $(\mathbf{a}, \mathbf{b}) \in A^\ell \times A^\ell$ and $\mathbf{a}\ \mathbf{S}\ \mathbf{b}$,
(iii) $(\mathbf{u}, \mathbf{v}) \in A^m \times A^m$ and $\mathbf{u}\ \mathbf{T}\ \mathbf{v}$.

Let δ be a congruence relation of $\mathbf{A}$. If the entries of every S, T-matrix satisfy

$$t(\mathbf{a}, \mathbf{u})\ \delta\ t(\mathbf{a}, \mathbf{v}) \quad \Longleftrightarrow \quad t(\mathbf{b}, \mathbf{u})\ \delta\ t(\mathbf{b}, \mathbf{v}), \tag{2.1}$$

then we say that S *centralizes* T *modulo* δ and we write $\mathsf{C}(S, T; \delta)$. That is, $\mathsf{C}(S, T; \delta)$ means that (2.1) holds *for all* ℓ, m, t, $\mathbf{a}$, $\mathbf{b}$, $\mathbf{u}$, $\mathbf{v}$ satisfying properties (i)–(iii).

The *commutator* of S and T, denoted by $[S,T]$, is the least congruence δ such that $\mathsf{C}(S,T;\delta)$ holds. Note that $\mathsf{C}(S,T;0_A)$ is equivalent to $[S,T]=0_A$, and this is sometimes called the S,T*-term condition*; when it holds we say that S *centralizes* T. A tolerance T is called *abelian* if $[T,T]=0_A$. An algebra $\mathbf{A}$ is called *abelian* if 1_A is abelian (i.e., $[1_A,1_A]=0_A$).

Remark 2.1. An algebra $\mathbf{A}$ is abelian iff

$$\forall \ell, m \in \mathbb{N}, \quad \forall t \in \mathsf{Clo}_{\ell+m}(\mathbf{A}), \quad \forall (\mathbf{a},\mathbf{b}) \in A^\ell \times A^\ell,$$
$$\ker t(\mathbf{a},\cdot) = \ker t(\mathbf{b},\cdot).$$

Here are some properties of the centralizer relation that are well-known and not too hard to prove (see [HM88, Prop 3.4] or [KK13, Thm 2.19]).

Lemma 2.2. *Let* $\mathbf{A}$ *be an algebra and suppose* $\mathbf{B}$ *is a subalgebra of* $\mathbf{A}$*. Let* α*,* β*,* γ*,* δ*,* α_i β_j*,* γ_k *be congruences of* $\mathbf{A}$*, for all* $i \in I$*,* $j \in J$*,* $k \in K$*. Then the following hold:*

(1) $\mathsf{C}(\alpha,\beta;\alpha\wedge\beta)$*;*
(2) if $\mathsf{C}(\alpha,\beta;\gamma_k)$ *for all* $k\in K$*, then* $\mathsf{C}(\alpha,\beta;\bigwedge_K \gamma_k)$*;*
(3) if $\mathsf{C}(\alpha_i,\beta;\gamma)$ *for all* $i\in I$*, then* $\mathsf{C}(\bigvee_I \alpha_i,\beta;\gamma)$*;*
(4) if $\mathsf{C}(\alpha,\beta;\gamma)$ *and* $\alpha'\leqslant\alpha$*, then* $\mathsf{C}(\alpha',\beta;\gamma)$*;*
(5) if $\mathsf{C}(\alpha,\beta;\gamma)$ *and* $\beta'\leqslant\beta$*, then* $\mathsf{C}(\alpha,\beta';\gamma)$*;*
(6) if $\mathsf{C}(\alpha,\beta;\gamma)$ *in* $\mathbf{A}$*, then* $\mathsf{C}(\alpha\cap B^2,\beta\cap B^2;\gamma\cap B^2)$ *in* $\mathbf{B}$*;*
(7) if $\gamma\leqslant\delta$*, then* $\mathsf{C}(\alpha,\beta;\delta)$ *in* $\mathbf{A}$ *if and only if* $\mathsf{C}(\alpha/\gamma,\beta/\gamma;\delta/\gamma)$ *in* $\mathbf{A}/\gamma$*.*

Remark 2.3. By (1), if $\alpha\wedge\beta=0_A$, then $[\beta,\alpha]=0_A=[\alpha,\beta]$.

Before proceeding, we collect some facts about the commutator that may be useful for reasoning about difference terms.

Lemma 2.4. *Let* $\mathbf{A}$ *be an algebra with congruences* α*,* α'*,* β*,* β' *satisfying* $\alpha\leqslant\alpha'$ *and* $\beta\leqslant\beta'$*. Then* $[\alpha,\beta]\leqslant[\alpha',\beta']$*.*

Proof. For every $\delta\in\operatorname{Con}\mathbf{A}$, $\mathsf{C}(\alpha',\beta';\delta)$ implies $\mathsf{C}(\alpha,\beta;\delta)$, since $\alpha\leqslant\alpha'$ and $\beta\leqslant\beta'$. In particular, $\mathsf{C}(\alpha',\beta';[\alpha',\beta'])$ implies $\mathsf{C}(\alpha,\beta;[\alpha',\beta'])$, so $[\alpha,\beta]\leqslant[\alpha',\beta']$. □

Lemma 2.5. *Let* $\mathbf{A}$ *be an algebra with congruences* α_i *and* β_i *for all* $i\in I$*. Then*

$$[\bigwedge\alpha_i,\bigwedge\beta_i]\leqslant\bigwedge[\alpha_i,\beta_i] \qquad \text{and} \qquad \bigvee[\alpha_i,\beta_i]\leqslant[\bigvee\alpha_i,\bigvee\beta_i]\,.$$

Proof. By Lemma 2.4, $[\bigwedge\alpha_i,\bigwedge\beta_i]\leqslant[\alpha_i,\beta_i]\leqslant[\bigvee\alpha_i,\bigvee\beta_i]$, for all $i\in I$. □

We will apply the preceding result in a simple special case involving just four congruences; we record this version of the result for convenience.

Corollary 2.6. *Let* $\mathbf{A}$ *be an algebra with congruences* α*,* β*,* γ*,* δ*. Then,*

$$[\alpha\wedge\gamma,\beta\wedge\delta]\leqslant[\alpha,\beta]\wedge[\gamma,\delta] \qquad \text{and} \qquad [\alpha,\beta]\vee[\gamma,\delta]\leqslant[\alpha\vee\gamma,\beta\vee\delta]\,.$$

Lemma 2.7 ([Kea95, Theorem 2.10])**.** *Let* $\mathbf{A}$ *and* $\mathbf{B}$ *be algebras of the same signature and suppose* $\phi : \mathbf{A} \to \mathbf{B}$ *is a surjective homomorphism. If* $\alpha, \beta \in \operatorname{Con}\mathbf{A}$*, then*

$$\phi([\alpha, \beta]) \subseteq [\phi(\alpha), \phi(\beta)].$$

Moreover, if there exists a homomorphism $\psi : \mathbf{B} \to \mathbf{A}$ *such that* $\phi \circ \psi = \mathrm{id}_B$ *and if* $\rho, \sigma \in \operatorname{Con}\mathbf{B}$*, then*

$$\psi^{-1}\{[\psi(\rho), \psi(\sigma)]\} = \phi\big([\psi(\rho), \psi(\sigma)]\big) = [\rho, \sigma]$$

2.1. Equivalent conditions for existence of a difference term. In this subsection we give an improved version of a well known result (Theorem 2.8).

In [Kea95] Kearnes proved that a locally finite variety has a difference term iff it has a Taylor term and no type-2 tails. Let $\mathcal{V}$ be a variety and let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(2)$ denote the 2-generated free algebra in $\mathcal{V}$. Then the assumption that $\mathcal{V}$ be locally finite can be weakened to the hypothesis that $\mathbf{F}$ is finite. This was observed in [Kea95] by showing that $\mathcal{V}$ has a difference term if and only if $\mathsf{HSP}(\mathbf{F})$ has a difference term. The forward implication of this claim is trivial. The argument for the converse goes as follows: assume that $d(x, y, z)$ is a difference term for $\mathsf{HSP}(\mathbf{F})$. Choose $\mathbf{A} \in \mathcal{V}$ and $a, b \in A$. Let $\mathbf{B} = \mathrm{Sg}^{\mathbf{A}}(\{a, b\})$. Since $\mathbf{B}$ is 2-generated, $B \in \mathsf{HSP}(\mathbf{F})$. Hence $d(x, y, z)$ interprets as a difference term in $\mathbf{B}$. This means that $d^{\mathbf{A}}(a, a, b) = d^{\mathbf{B}}(a, a, b) = b$. Furthermore,

$$d^{\mathbf{A}}(a, b, b) = d^{\mathbf{B}}(a, b, b)\ [\theta^{\mathbf{B}}(a, b), \theta^{\mathbf{B}}(a, b)]\ a.$$

But $[\theta^{\mathbf{B}}(a, b), \theta^{\mathbf{B}}(a, b)] \subseteq [\theta, \theta]$ for any congruence $\theta \in \operatorname{Con}\mathbf{A}$ for which $(a, b) \in \theta$. Consequently $d^{\mathbf{A}}(a, b, b)\ [\theta, \theta]\ a$ as desired.

For the purposes of the present project, it would be helpful if we could extend this observation and prove that the existence (or nonexistence) of a difference term in $\mathcal{V}$ is equivalent to the existence (or nonexistence) of a difference term operation for a specific algebra in $\mathcal{V}$. In fact, this is possible, as we now demonstrate.

Theorem 2.8. *Let* $\mathcal{V}$ *be a variety and* $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(2)$*, the 2-generated free algebra in* $\mathcal{V}$*. The following are equivalent:*

(i) $\mathcal{V}$ *has a difference term;*
(ii) $\mathsf{HSP}(\mathbf{F})$ *has a difference term;*
(iii) $\mathbf{F}$ *has a difference term operation.*

Proof. The implications (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) are obvious. We prove (iii) $\Rightarrow$ (i) by contraposition. Suppose $\mathcal{V}$ has no difference term. (We show $\mathbf{F}$ has no difference term operation.) Let $d(x, y, z)$ be a ternary term of $\mathcal{V}$. Let $\mathbf{A} \in \mathcal{V}$ be such that $d^{\mathbf{A}}(x, y, z)$ is not a difference term operation in $\mathbf{A}$. Choose $a, b \in A$ witnessing this fact. Then either

(1) $d^{\mathbf{A}}(a, a, b) \neq b$, or
(2) $(d^{\mathbf{A}}(a, b, b), a) \notin [\theta^{\mathbf{A}}(a, b), \theta^{\mathbf{A}}(a, b)]$.

Let $\mathbf{B} = \mathrm{Sg}^{\mathbf{A}}(\{a, b\})$. In case (1), $d^{\mathbf{B}}(a, a, b) = d^{\mathbf{A}}(a, a, b) \neq b$, so $d^{\mathbf{B}}(x, y, z)$ is not a difference term operation for $\mathbf{B}$. In case (2), observe that the pair $(d^{\mathbf{B}}(a, b, b), a)$ is equal to the pair $(d^{\mathbf{A}}(a, b, b), a)$ which does not belong to $[\theta^{\mathbf{A}}(a, b), \theta^{\mathbf{A}}(a, b)]$. But $[\theta^{\mathbf{B}}(a, b), \theta^{\mathbf{B}}(a, b)] \subseteq [\theta^{\mathbf{A}}(a, b), \theta^{\mathbf{A}}(a, b)]$, so

$$(d^{\mathbf{B}}(a, b, b), a) \notin [\theta^{\mathbf{B}}(a, b), \theta^{\mathbf{B}}(a, b)],$$

and again we conclude that $d^{\mathbf{B}}(x, y, z)$ is not a difference term operation for $\mathbf{B}$. Now, since there is a surjective homomorphism from $\mathbf{F}$ to $\mathbf{B}$, it follows that $d^{\mathbf{F}}(x, y, z)$ cannot be a difference term operation for $\mathbf{F}$. Finally, recall that $d(x, y, z)$ was an arbitrary ternary term of $\mathcal{V}$, so $\mathbf{F}$ has no difference term operation whatsoever. □

3. Local difference terms

In [VW14], Valeriote and Willard 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. Inspired by that work, we devise a similar construct, called a "local difference term," that we use to develop a polynomial-time algorithm for deciding the existence of a (global) difference term operation.

Let $\mathbf{A} = \langle A, \ldots \rangle$ be an algebra, fix $a, b \in A$ and $i \in \{0, 1\}$. A *local difference term for* (a, b, i) is a ternary term p satisfying the following:

$$\begin{aligned} &\text{if } i = 0, \text{ then } a\ [\theta(a, b), \theta(a, b)]\ p(a, b, b); \\ &\text{if } i = 1, \text{ then } p(a, a, b) = b. \end{aligned} \tag{3.1}$$

If p satisfies (3.1) for all triples in some subset $S \subseteq A \times A \times \{0, 1\}$, then we call p a *local difference term for* S.

Let $\mathcal{S} = A \times A \times \{0, 1\}$ and suppose that every pair $((a_0, b_0, \chi_0), (a_1, b_1, \chi_1))$ in $\mathcal{S}^2$ has a local difference term. That is, for each pair $((a_0, b_0, \chi_0), (a_1, b_1, \chi_1))$, there exists p such that for each $i \in \{0, 1\}$ we have

$$a_i\ [\theta(a_i, b_i), \theta(a_i, b_i)]\ p(a_i, b_i, b_i), \text{ if } \chi_i = 0, \text{ and} \tag{3.2}$$

$$p(a_i, a_i, b_i) = b_i, \text{ if } \chi_i = 1. \tag{3.3}$$

Under these hypothesis we will prove that every subset $S \subseteq \mathcal{S}$ has a local difference term. That is, there is a single term p that works (i.e., satisfies (3.2) and (3.3)) for all $(a_i, b_i, \chi_i) \in S$. The statement and proof of this new result follows.

Theorem 3.1 (cf. [VW14, Theorem 2.2])**.** *Let $\mathcal{V}$ be an idempotent variety and $\mathbf{A} \in \mathcal{V}$. Define $\mathcal{S} = A \times A \times \{0, 1\}$ and suppose that every pair $((a_0, b_0, \chi_0), (a_1, b_1, \chi_1)) \in \mathcal{S}^2$ has a local difference term. Then every subset $S \subseteq \mathcal{S}$, has a local difference term.*

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 $\mathcal{S}$ of size $2 \leqslant k \leqslant n$ has a local difference term. Let

$$S = \{(a_0, b_0, \chi_0), (a_1, b_1, \chi_1), \ldots, (a_n, b_n, \chi_n)\} \subseteq \mathcal{S},$$

so that $|S| = n + 1$. We prove S has a local difference 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 $j = 0$. Define the set $S' = S \setminus \{(a_0, b_0, \chi_0)\}$. Since $|S'| < |S|$, the set S' has a local difference term p. We split the remainder of the proof into two cases.

Case $\chi_0 = 0$: Without loss of generality, suppose that $\chi_1 = \cdots = \chi_k = 1$, and $\chi_{k+1} = \cdots = \chi_n = 0$. Define

$$T = \{(a_0, p(a_0, b_0, b_0), 0), (a_1, b_1, 1), (a_2, b_2, 1), \ldots, (a_k, b_k, 1)\},$$

and note that $|T| < |S|$. Let t be a local difference term for T. Define

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

Since $\chi_0 = 0$, we need to show $(a_0, d(a_0, b_0, b_0))$ belongs to $[\theta(a_0, b_0), \theta(a_0, b_0)]$. We have

$$d(a_0, b_0, b_0) = t(a_0, p(a_0, b_0, b_0), p(a_0, b_0, b_0)) \; [\tau, \tau] \; a_0, \tag{3.4}$$

where we have used τ to denote $\theta(a_0, p(a_0, b_0, b_0))$. Note that

$$(a_0, p(a_0, b_0, b_0)) = (p(a_0, a_0, a_0), p(a_0, b_0, b_0)) \in \theta(a_0, b_0),$$

so $\tau \leqslant \theta(a_0, b_0)$. Therefore, by monotonicity of the commutator we have $[\tau, \tau] \leqslant [\theta(a_0, b_0), \theta(a_0, b_0)]$. It follows from this and (3.4) that

$$d(a_0, b_0, b_0) \; [\theta(a_0, b_0), \theta(a_0, b_0)] \; a_0,$$

as desired.

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

$$\begin{aligned} d(a_i, a_i, b_i) &= t(a_i, p(a_i, a_i, a_i), p(a_i, a_i, b_i)) && (3.5)\\ &= t(a_i, a_i, b_i) && (3.6)\\ &= b_i. && (3.7) \end{aligned}$$

Equation (3.5) holds by definition of d, (3.6) because p is an idempotent local difference term for S', and (3.7) because t is a local difference term for T.

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

$$d(a_j, b_j, b_j) = t(a_j, p(a_j, b_j, b_j), p(a_j, b_j, b_j)). \tag{3.8}$$

Since p is a local difference term for S', the pair $(p(a_j, b_j, b_j), a_j)$ belongs to $[\theta(a_j, b_j), \theta(a_j, b_j)]$. This and (3.8) imply that $(d(a_j, b_j, b_j), t(a_j, a_j, a_j))$ belongs to $[\theta(a_j, b_j), \theta(a_j, b_j)]$. Finally, by idempotence of t we have

$$d(a_j, b_j, b_j)\ [\theta(a_j, b_j), \theta(a_j, b_j)]\ a_j,$$

as desired.

Case $\chi_0 = 1$: Without loss of generality, suppose $\chi_1 = \chi_2 = \cdots = \chi_k = 0$, and $\chi_{k+1} = \chi_{k+2} = \cdots = \chi_n = 1$. Define

$$T = \{(p(a_0, a_0, b_0), b_0, 1), (a_1, b_1, 0), (a_2, b_2 0), \ldots, (a_k, b_k, 0)\},$$

and note that $|T| < |S|$. Let t be a local difference term for T and define $d(x, y, z) = t(p(x, y, z), p(y, y, z), z)$. Since $\chi_0 = 1$, we want $d(a_0, a_0, b_0) = b_0$. By the definition of d,

$$d(a_0, a_0, b_0) = t(p(a_0, a_0, b_0), p(a_0, a_0, b_0), b_0) = b_0.$$

The last equality holds since t is a local difference term for T, thus, for $(p(a_0, a_0, b_0), b_0, 1)$.

If $1 \leqslant i \leqslant k$, then $\chi_i = 0$, so for these indices we prove that $(a_i, d(a_i, b_i, b_i))$ belongs to $[\theta(a_i, b_i), \theta(a_i, b_i)]$. Again, starting from the definition of d and using idempotence of p, we have

$$\begin{aligned} d(a_i, b_i, b_i) &= t(p(a_i, b_i, b_i), p(b_i, b_i, b_i), b_i) \\ &= t(p(a_i, b_i, b_i), b_i, b_i). \end{aligned} \tag{3.9}$$

Next, since p is a local difference term for S', we have

$$t(p(a_i, b_i, b_i), b_i, b_i)\ [\theta(a_i, b_i), \theta(a_i, b_i)]\ t(a_i, b_i, b_i). \tag{3.10}$$

Finally, since t is a local difference term for T, hence for (a_i, b_i, b_i), we have $t(a_i, b_i, b_i)\ [\theta(a_i, b_i), \theta(a_i, b_i)]\ a_i$. Combining this with (3.9) and (3.10) yields $d(a_i, b_i, b_i)\ [\theta(a_i, b_i), \theta(a_i, b_i)]\ a_i$, as desired.

The remaining elements of our original set S have indices j satisfying $k < j \leqslant n$ and $\chi_j = 1$. For these we want $d(a_j, a_j, b_j) = b_j$. Since p is a local difference term for S', we have $p(a_j, a_j, b_j) = b_j$, and this along with idempotence of t yields

$$\begin{aligned} d(a_j, a_j, b_j) &= t(p(a_j, a_j, b_j), p(a_j, a_j, b_j), b_j) \\ &= t(b_j, b_j, b_j) = b_j, \end{aligned}$$

as desired. □

Corollary 3.2. *A finite idempotent algebra* $\mathbf{A}$ *has a difference term operation if and only if every pair* $((a, b, i), (a', b', i')) \in (A \times A \times \{0, 1\})^2$ *has a local difference term.*

Proof. One direction is clear, since a difference term operation for $\mathbf{A}$ is obviously a local difference term for the whole set $A \times A \times \{0, 1\}$. For the converse, suppose each pair in $(A \times A \times \{0, 1\})^2$ has a local difference term.

Then, by Theorem 3.1, there is a single local difference term for the whole set $A \times A \times \{0,1\}$, and this is a difference term operation for $\mathbf{A}$. Indeed, if d is a local difference term for $A \times A \times \{0,1\}$, then for all $a, b \in A$, we have $a\ [\theta(a,b), \theta(a,b)]\ d(a,b,b)$, since d is a local difference term for $(a,b,0)$, and we have $d(a,a,b) = b$, since d is also a local difference term for $(a,b,1)$. □

3.1. Algorithm 1: existence of difference term operations. In this subsection we prove the following

Corollary 3.3. *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 $((a,b,i),(a',b',i')) \in (A \times A \times \{0,1\})^2$ has a local difference term. By Corollary 3.2, this will prove we can decide in polynomial-time whether $\mathbf{A}$ has a difference term operation.

Fix a pair $((a,b,i),(a',b',i'))$ in $(A \times A \times \{0,1\})^2$. If $i = i' = 0$, then the first projection is a local difference term. If $i = i' = 1$, then the third projection is a local difference term. The two remaining cases to consider are (1) $i = 0$ and $i' = 1$, and (2) $i = 1$ and $i' = 0$. Since these are completely symmetric, we only handle the first case. Assume the given pair of triples is $((a,b,0),(a',b',1))$. By definition, a term t is local difference term for this pair iff

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

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 is a local difference term for $((a,b,0),(a',b',1))$ iff

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

where $\delta = [\theta(a,b), \theta(a,b)]$ and a/δ denotes the δ-class containing a. (Observe that $a/\delta \times \{b'\}$ is a subalgebra of $\mathbf{A} \times \mathbf{A}$ by idempotence.) It follows that the pair $((a,b,0),(a',b',1))$ has a local difference 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, the algorithm takes as input $\mathbf{A}$ and, for each $((a,a'),(b,a'),(b,b'))$ in $(A \times A)^3$, computes $\delta = [\theta(a,b), \theta(a,b)]$, computes the subalgebra $\mathbf{S}$ of $\mathbf{A} \times \mathbf{A}$ generated by $\{(a,a'),(b,a'),(b,b')\}$, and then tests whether $S \cap (a/\delta \times \{b'\})$ is empty. If we find an empty intersection at any point, then $\mathbf{A}$ has a 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, 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 questionable is the commutator, but there is a straight-forward algorithm for computing it which, after the congruences have been computed, simply involves generating more subalgebras.

TODO: insert more details about complexity of commutator.

□

More details on the complexity of operations carried out by the algorithm, as well as many other algebraic operations, can be found in the references mentioned, as well as [BS02, BJS99, FV09].

4. Global-local difference terms

The methods from the previous section can be lifted up to subuniverses, as we now describe. Let $\mathcal{V}$ be a variety, let $\mathbf{A} = \langle A, \ldots \rangle$ and $\mathbf{B} = \langle B, \ldots \rangle$ be algebras in $\mathcal{V}$, and let $i \in \{0, 1\}$. We call a term d a *global-local difference term for* (A, B, i) provided for all $a, a' \in A$ and $b, b' \in B$ we have

$$\text{if } i = 0, \text{ then } a\ [\theta(a, a'), \theta(a, a')]\ d^{\mathbf{A}}(a, a', a'); \tag{4.1}$$

$$\text{if } i = 1, \text{ then } d^{\mathbf{B}}(b, b, b') = b'. \tag{4.2}$$

Let $\mathrm{Sub}(\mathbf{A})$ denote the set of all subuniverses of $\mathbf{A}$. In the next theorem we will use the following notation and terminology: $\mathcal{S}(\mathbf{A}) := \mathrm{Sub}(\mathbf{A}) \times \mathrm{Sub}(\mathbf{A}) \times \{0, 1\}$, and for any sequence

$$S = ((A_0, B_0, \chi_0), (A_1, B_1, \chi_1), \ldots, (A_{n-1}, B_{n-1}, \chi_{n-1})) \in \mathcal{S}(\mathbf{A})^n,$$

a term d is a *global-local difference term for* S if d is a global-local difference term for every triple in S.

Throughout this section $|S|$ denotes the *length of the sequence* S.

Theorem 4.1 (cf. [VW14, Theorem 2.2])**.** *Let $\mathcal{V}$ be an idempotent variety and $\mathbf{A} \in \mathcal{V}$. If every pair $((A_0, B_0, \chi_0), (A_1, B_1, \chi_1)) \in \mathcal{S}(\mathbf{A}) \times \mathcal{S}(\mathbf{A})$ has a global-local difference term, then, for all $n \geqslant 2$, every sequence $S \in \mathcal{S}(\mathbf{A})^n$ has a global-local difference term.*

Proof. The proof is by induction on $|S|$, the length of the sequence S.

In the base case, $|S| = 2$, the claim holds by assumption. Fix $n \geqslant 2$ and assume that every sequence in $\mathcal{S}(\mathbf{A})^k$ of length $2 \leqslant k \leqslant n$ has a global-local difference term. Let $S = ((A_0, B_0, \chi_0), (A_1, B_1, \chi_1), \ldots, (A_n, B_n, \chi_n)) \in \mathcal{S}(\mathbf{A})^{n+1}$. We will prove that S has a global-local difference 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 $j = 0$. Define the subsequence $S' = ((A_1, B_1, \chi_1), \ldots, (A_n, B_n, \chi_n))$ of S. Since $|S'| = n$, the sequence S' has a global-local difference term p. Thus, for

all $1 \leqslant i \leqslant n$, for all $a, a' \in A_i$ and $b, b' \in B_i$ we have

$$\begin{aligned} &\text{if } \chi_i = 0, \text{ then } a\ [\theta(a,a'), \theta(a,a')]\ d^{\mathbf{A}_i}(a,a',a');\\ &\text{if } \chi_i = 1, \text{ then } d^{\mathbf{B}_i}(b,b,b') = b'. \end{aligned}$$

We split the remainder of the proof into two cases.

Case $\chi_0 = 0$: Without loss of generality, suppose that $\chi_1 = \chi_2 = \cdots = \chi_k = 1$, and $\chi_{k+1} = \chi_{k+2} = \cdots = \chi_n = 0$. Define

$$T = ((A_0, B_0, 0), (A_1, B_1, 1), (A_2, B_2, 1), \ldots, (A_k, B_k, 1)).$$

Note that $|T| < |S|$. Let t be a global-local difference term for T. We will prove that the term $d(x,y,z) = t(x, p(x,y,y), p(x,y,z))$ is a global-local difference term for the sequence S.

The first triple in S is $(A_0, B_0, 0)$, so we need to show for all a, $a' \in A_0$ that

$$d^{\mathbf{A}_0}(a,a',a')\ [\theta(a,a'), \theta(a,a')]\ a.$$

Fix $a, a' \in A_0$. By definition of d, and since t is a global-local difference term for $(A_0, B_0, 0)$, we have

$$d^{\mathbf{A}_0}(a,a',a') = t^{\mathbf{A}_0}(a,a'',a'')\ [\theta(a,a''), \theta(a,a'')]\ a, \tag{4.3}$$

where $a'' = p^{\mathbf{A}_0}(a,a',a')$. Now, $(a,a'') = (p^{\mathbf{A}_0}(a,a,a), p^{\mathbf{A}_0}(a,a',a')) \in \theta(a,a')$, therefore, $\theta(a,a'') \leqslant \theta(a,a')$. It follows from this and monotonicity of the commutator that $[\theta(a,a''), \theta(a,a'')] \leqslant [\theta(a,a'), \theta(a,a')]$, This and (4.3) imply $d^{\mathbf{A}_0}(a,a',a')\ [\theta(a,a'), \theta(a,a')]\ a$, as desired.

For indices $1 \leqslant i \leqslant k$ we have $\chi_i = 1$, so we wish to prove that for all b, $b' \in B_i$ we have $d^{\mathbf{A}_i}(b,b,b') = b'$. Fix $b, b' \in B_i$ and observe that

$$\begin{aligned} d^{\mathbf{B}_i}(b,b,b') &= t(b, p^{\mathbf{B}_i}(b,b,b), p^{\mathbf{B}_i}(b,b,b')) &(4.4)\\ &= t^{\mathbf{B}_i}(b,b,b') &(4.5)\\ &= b'. &(4.6) \end{aligned}$$

Equation (4.4) holds by definition of d, (4.5) because p is an idempotent global-local difference term for S', and (4.6) because t is a global-local difference term for T.

The remaining triples in our original sequence S have indices satisfying $k < j \leqslant n$ and $\chi_j = 0$. Thus, for these triples we prove for all $a, a' \in A_j$ that $d^{\mathbf{A}_j}(a,a',a')\ [\theta(a,a'), \theta(a,a')]\ a$. Fix $a, a' \in A_j$. By definition,

$$d^{\mathbf{A}_j}(a,a',a') = t^{\mathbf{A}_j}(a, p^{\mathbf{A}_j}(a,a',a'), p^{\mathbf{A}_j}(a,a',a')). \tag{4.7}$$

Also, $p^{\mathbf{A}_j}(a,a',a')\ [\theta(a,a'), \theta(a,a')]\ a$, since p is a global-local difference term for S'. This and (4.7) imply that $d^{\mathbf{A}_j}(a,a',a')\ [\theta(a,a'), \theta(a,a')]\ t^{\mathbf{A}_j}(a,a,a))$. Finally, by idempotence of t we have $d^{\mathbf{A}_j}(a,a',a')\ [\theta(a,a'), \theta(a,a')]\ a$, as desired.

Case $\chi_0 = 1$: Without loss of generality, suppose $\chi_1 = \chi_2 = \cdots = \chi_k = 0$, and $\chi_{k+1} = \chi_{k+2} = \cdots = \chi_n = 1$. Define

$$T = ((A_0, B_0, 1), (A_0, B_1, 0), (A_2, B_2, 0), \ldots, (A_k, B_k, 0)),$$

and note that $|T| < |S|$, so T has a global-local difference term t. We will prove that the term $d(x, y, z) = t(p(x, y, z), p(y, y, z), z)$ is a global-local difference term for the sequence S.

The first triple in S is $(A_0, B_0, 1)$, so we want to show for all b, $b' \in B_0$ that $d(b, b, b') = b'$. Fix b, $b' \in B_0$. By definition of d, we have $d^{\mathbf{B}_0}(b, b, b') = t^{\mathbf{B}_0}(p^{\mathbf{B}_0}(b, b, b'), p^{\mathbf{B}_0}(b, b, b'), b') = b'$. The last equality holds since t is a global-local difference term for T, thus, for $(A_0, B_0, 1)$.

If $1 \leqslant i \leqslant k$, then $\chi_i = 0$, so for these indices we want for all $a, a' \in A_i$ that

$$d^{\mathbf{A}_i}(a, a', a') \; [\theta(a, a'), \theta(a, a')] \; a.$$

Fix $a, a' \in A_i$. By definition of d and idempotence of p, we have

$$\begin{aligned} d^{\mathbf{A}_i}(a, a', a') &= t^{\mathbf{A}_i}(p^{\mathbf{A}_i}(a, a', a'), p^{\mathbf{A}_i}(a', a', a'), a') \\ &= t^{\mathbf{A}_i}(p^{\mathbf{A}_i}(a, a', a'), a', a'). \end{aligned} \tag{4.8}$$

Next, since p is a global-local difference term for S', we have

$$t^{\mathbf{A}_i}(p^{\mathbf{A}_i}(a, a', a'), a', a') \; [\theta(a, a'), \theta(a, a')] \; t^{\mathbf{A}_i}(a, a', a'). \tag{4.9}$$

Finally, since t is a global-local difference term for T, hence for (a, a', a'), we have

$$t^{\mathbf{A}_i}(a, a', a') \; [\theta(a, a'), \theta(a, a')] \; a.$$

Combining this with (4.8) and (4.9) yields $d^{\mathbf{A}_i}(a, a', a') \; [\theta(a, a'), \theta(a, a')] \; a$, as desired.

The remaining elements of our original sequence S have indices j satisfying $k < j \leqslant n$ and $\chi_j = 1$. For these we want to prove for all $b, b' \in B_j$ that $d^{\mathbf{B}_j}(b, b, b') = b'$. Fix $b, b' \in B_j$. Since p is a global-local difference term for S', we have $p^{\mathbf{B}_j}(b, b, b') = b'$, and this along with idempotence of t yields

$$d^{\mathbf{B}_j}(b, b, b') = t^{\mathbf{B}_j}(p^{\mathbf{B}_j}(b, b, b'), p^{\mathbf{B}_j}(b, b, b'), b') = t^{\mathbf{B}_j}(b', b', b') = b'$$

as desired. □

If $\mathcal{A}$ be a collection of similar algebras, we will use the notation $\mathrm{Sub}(\mathcal{A})$ to denote the collection of all subuniverses of all algebras in $\mathcal{A}$. That is,

$$\mathrm{Sub}(\mathcal{A}) = \bigcup_{\mathbf{A} \in \mathcal{A}} \mathrm{Sub}(\mathbf{A}).$$

By further abuse of notation, we let

$$\mathcal{S}(\mathcal{A}) = \mathrm{Sub}(\mathcal{A}) \times \mathrm{Sub}(\mathcal{A}) \times \{0, 1\},$$

so $(A, B, i) \in \mathcal{S}(\mathcal{A})$ indicates that A is a subuniverse of some algebra in $\mathcal{A}$, and B is a subuniverse of some (possibly different) algebra in $\mathcal{A}$, and $i \in \{0, 1\}$.

Corollary 4.2. *Let $\mathcal{V}$ be a variety. Let $\mathcal{A}$ be a collection of finite idempotent algebras in $\mathcal{V}$ that is closed under the taking of subalgebras. Then there exists a term d that is a difference term operation for every algebra in $\mathcal{A}$ if and only if every $((A, B, i), (A', B', i')) \in \mathcal{S}(\mathcal{A})^2$ has a global-local difference term.*

Proof. One direction is clear, since a difference term for all of $\mathcal{A}$ is obviously a global-local difference term for the whole set $\mathcal{S}(\mathcal{A})$. For the converse, suppose each pair in $\mathcal{S}(\mathcal{A})^2$ has a global-local difference term. Then, by Theorem 4.1, there is a single global-local difference term for the whole set $\mathcal{S}(\mathcal{A})$ and this is a difference term for all of $\mathcal{A}$. Indeed, suppose d is a global-local difference term for $\mathcal{S}(\mathcal{A})$ and fix $\mathbf{A} \in \mathcal{A}$. We show that d is a difference term operation for $\mathbf{A}$. Indeed, so for all $a, a' \in A$ we have $a \; [\theta(a, a'), \theta(a, a')] \; d(a, a', a')$, since d is a global-local difference term for $(A, A, 0)$, and we have $d(a, a, a') = a'$, since d is a global-local difference term for $(A, A, 1)$. □

4.1. Algorithm 2: existence of difference terms. In this subsection we prove the following

Corollary 4.3. *There is a polynomial-time algorithm that takes as input any finite idempotent algebra $\mathbf{A}$ and decides whether the variety $\mathbb{V}(\mathbf{A})$ that it generates has a difference term operation.*

Proof. TODO: fill in proof!!! □

4.2. Algorithm 2: existence of difference terms. In this subsection we prove the following

Corollary 4.4. *There is a polynomial-time algorithm that takes as input any finite idempotent algebra $\mathbf{A}$ and decides whether the variety $\mathbb{V}(\mathbf{A})$ that it generates has a difference term operation.*

Proof. TODO: fill in proof!!! □

References

[BD16] Clifford Bergman and William DeMeo. Universal algebraic methods for constraint satisfaction problems: with applications to commutative idempotent binars. unpublished notes; soon to be available online, 2016. URL: `https://github.com/UniversalAlgebra/algebraic-csp`.

[Ber12] Clifford Bergman. *Universal algebra*, volume 301 of *Pure and Applied Mathematics (Boca Raton)*. CRC Press, Boca Raton, FL, 2012. Fundamentals and selected topics.

[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.

[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.

[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.

[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.

Department of Mathematics, University of Hawaii, Honolulu 96816, USA
e-mail: williamdemeo@gmail.com
URL: http://williamdemeo.org