International Journal of Algebra and Computation

ON THE COMPLEXITY OF DIFFERENCE TERM EXISTENCE

WILLIAM DEMEO

Department of Mathematics, University of Hawaii
Honolulu, Hawaii, 96822 USA
williamdemeo@gmail.com

RALPH FREESE

Department of Mathematics, University of Hawaii
Honolulu, Hawaii, 96822 USA
ralph@math.hawaii.edu

Received (Day Month Year)
Accepted (Day Month Year)

Communicated by [editor]

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? In [4] "local difference terms" were defined and used to solve a related but easier problem—namely, it was shown that there is a polynomial-time algorithm for deciding whether any finite idempotent algebra has a difference term operation. In the present paper, we continue to build on the ideas in [14] and complete the project started [4]. More specifically, we define "global-local difference terms" which we use to devise an efficient algorithm for deciding whether the variety generated by a finite idempotent algebra has a difference term.

Keywords: difference term; finite idempotent algebra; polynomial-time algorithm

Mathematics Subject Classification 2000: 08B05, 08B10, 68Q25, 03C05

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 $\mathbf{A} = \langle A, \dots \rangle \in \mathcal{V}$ 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 defined in Section 2 below (see also [7] or [12]). When the relations in (1.1) hold we call $d^{\mathbf{A}}$ a *difference term operation* for $\mathbf{A}$.

Difference terms are studied extensively in the universal algebra literature. (See, for example, [7,9,10,11,12,13].) There are many reasons to study difference terms, but perhaps the most obvious is that knowing a variety has a difference term allows us to deduce many useful properties of the algebras in 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 ([6]) or congruence-n-permutable ([14])—and to do so efficiently. The contribution of the present paper is to present a solution to the following:

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 [4]; in the latter, 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?

The rest of the paper is organized as follows: Section 2 introduces notation and definitions and some of the background that we expect the reader to have. In [11] it was shown that a locally finite idempotent variety $\mathcal{V}$ has a difference term if and only if $\mathsf{HSP}(\mathbf{F}_{\mathcal{V}}(2))$ has a difference term (where $\mathbf{F}_{\mathcal{V}}(2)$ denotes the 2-generated free algebra in $\mathcal{V}$). In Section 3 we extend this result by showing that this is also equivalent to the free algebra $\mathbf{F}_{\mathcal{V}}(2)$ itself having a difference term operation. In [14], 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. In Section 4 we devise a similar construct, called a "local difference term," that we use, in Section 4.3, to give a polynomial-time algorithm for deciding the existence of a difference term operation for $\mathbf{A}$. In Section 5.2 we extend local difference terms from points to universes and then, in Section 5.3, we devise a polynomial-time algorithm for deciding whether the variety generated by a finite idempotent algebra has a difference term. We conclude with a brief description of our software implementation of the main algorithm, and then briefly discuss some related problems that remain open.

2. Background, Notation, 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 [1]. The set of all congruences of $\mathbf{A}$ is denoted $\mathrm{Con}(\mathbf{A})$. The subalgebra of $\mathbf{A}$ generated by a set $X \subseteq A$ is denoted $\mathrm{Sg}^{\mathbf{A}}(X)$, but if X is finite, say, $X = \{a, b\}$, then we often write $\mathrm{Sg}^{\mathbf{A}}(a, b)$ instead of $\mathrm{Sg}^{\mathbf{A}}(\{a, b\})$.

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 $0 \leqslant i < m$. 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., $[1_A, 1_A] = 0_A$).

Here are some properties of the centralizer relation that are well-known and not too hard to prove (see [7, Prop 3.4] or [12, Thm 2.19]).

Lemma 2.1. *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 2.2. 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 are sometimes useful when reasoning about difference terms.

Lemma 2.3. *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 2.4. *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 2.3, $[\bigwedge \alpha_i, \bigwedge \beta_i] \leqslant [\alpha_i, \beta_i] \leqslant [\bigvee \alpha_i, \bigvee \beta_i]$, for all $i \in I$. □

Lemma 2.5 ([11, Theorem 2.10]). *Let* $\mathbf{A}$ *and* $\mathbf{B}$ *be algebras of the same similarity type 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* $\psi^{-1}\{[\psi(\rho), \psi(\sigma)]\} = \phi\big([\psi(\rho), \psi(\sigma)]\big) = [\rho, \sigma]$.

We conclude this section by describing a very convenient notational convention. The commutator, $[\theta, \theta]$, of a congruence with itself, appears so often in the sequel that we will abbreviate it as follows:[a]

$$[\![\theta]\!] := [\theta, \theta].$$

3. Equivalent conditions for existence of a difference term

The main result proved in this section is Theorem 3.1, which is a slightly improved version of the observation in [11] stating that a variety $\mathcal{V}$ has a difference term if and only if $\mathsf{HSP}(\mathbf{F}_{\mathcal{V}}(2))$ 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 $\mathbf{B} = \operatorname{Sg}^{\mathbf{A}}(\{a, b\})$. 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,

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

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

[a]This is similar to the standard notational convention for the iterated commutator:

$$[\theta]^0 = \theta, \quad [\theta]^1 = [\theta, \theta], \quad [\theta]^2 = \big[[\theta, \theta], [\theta, \theta]\big],\ \ldots,\ [\theta]^n = \big[[\theta]^{n-1}, [\theta]^{n-1}\big],\ \ldots.$$

Considering the goal of our project, it seems natural to begin by trying to prove that the existence of a difference term for $\mathcal{V}$ is equivalent to the existence of a difference term operation for a specific algebra in $\mathcal{V}$. This is achieved in Theorem 3.1, which will play a key role in our main complexity argument in Section 5.2.

Theorem 3.1. *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 for $\mathbf{A}$. Choose $a, b \in A$ witnessing this fact. Then either

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

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 $[\![\mathrm{Cg}^{\mathbf{A}}(a, b)]\!]$. But $[\![\mathrm{Cg}^{\mathbf{B}}(a, b)]\!] \subseteq [\![\mathrm{Cg}^{\mathbf{A}}(a, b)]\!]$, so

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

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 $\mathbf{B}$, Lemma 2.5 implies that $d^{\mathbf{F}}(x, y, z)$ is not a difference term operation for $\mathbf{F}$. Finally, recall that we chose $d(x, y, z)$ to be an arbitrary ternary term of $\mathcal{V}$, so $\mathbf{F}$ has no difference term operation whatsoever. $\square$

4. Local difference terms

In [14], 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 difference term operation.

4.1. *Definitions*

Let $\mathbf{A} = \langle A, \dots \rangle$ 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 d satisfying the following:

$$\begin{aligned} &\text{if } i = 0, \text{ then } a \; [\![\mathrm{Cg}(a, b)]\!] \; d(a, b, b); \\ &\text{if } i = 1, \text{ then } d(a, a, b) = b. \end{aligned} \tag{4.1}$$

If d satisfies (4.1) for all triples in some subset $S \subseteq A \times A \times \{0, 1\}$, then we call d 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 d such that for each $i \in \{0, 1\}$ we have

$$a_i \; [\![\mathrm{Cg}(a_i, b_i)]\!] \; d(a_i, b_i, b_i), \ \text{ if } \chi_i = 0, \text{ and} \tag{4.2}$$

$$d(a_i, a_i, b_i) = b_i, \ \text{ if } \chi_i = 1. \tag{4.3}$$

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 d that works (i.e., satisfies (4.2) and (4.3)) for all $(a_i, b_i, \chi_i) \in S$. The statement and proof of this new result follows.

4.2. *Main Results*

Theorem 4.1. *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

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

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

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

We show that d is a local difference term for S. Since $\chi_0 = 0$, we first verify that $(a_0, d(a_0, b_0, b_0))$ belongs to $[\![\mathrm{Cg}(a_0, b_0)]\!]$. Indeed,

$$d(a_0, b_0, b_0) = t(a_0, p(a_0, b_0, b_0), p(a_0, b_0, b_0)) \; [\![\mathrm{Cg}(a_0, p(a_0, b_0, b_0))]\!] \; a_0. \tag{4.4}$$

Note that

$$(a_0, p(a_0, b_0, b_0)) = (p(a_0, a_0, a_0), p(a_0, b_0, b_0)) \in \mathrm{Cg}(a_0, b_0),$$

so $\mathrm{Cg}(a_0, p(a_0, b_0, b_0)) \leqslant \mathrm{Cg}(a_0, b_0)$. Therefore, by monotonicity of the commutator we have $[\![\mathrm{Cg}(a_0, p(a_0, b_0, b_0))]\!] \leqslant [\![\mathrm{Cg}(a_0, b_0)]\!]$. It follows from this and (4.4) that

$$d(a_0, b_0, b_0) \; [\![\mathrm{Cg}(a_0, b_0)]\!] \; a_0,$$

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,

$$\begin{aligned} d(a_i, a_i, b_i) &= t(a_i, p(a_i, a_i, a_i), p(a_i, a_i, b_i)) && (4.5)\\ &= t(a_i, a_i, b_i) && (4.6)\\ &= b_i. && (4.7) \end{aligned}$$

Equation (4.5) holds by definition of d, (4.6) because p is an idempotent local difference term for S', and (4.7) 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 $d(a_j, b_j, b_j) \; [\![\mathrm{Cg}(a_j, b_j)]\!] \; a_j$. By definition,

$$d(a_j, b_j, b_j) = t(a_j, p(a_j, b_j, b_j), p(a_j, b_j, b_j)). \tag{4.8}$$

Since p is a local difference term for S', the pair $(p(a_j, b_j, b_j), a_j)$ belongs to $[\mathrm{Cg}(a_j, b_j), \mathrm{Cg}(a_j, b_j)]$. This and (4.8) imply that $(d(a_j, b_j, b_j), t(a_j, a_j, a_j))$ belongs to $[\![\mathrm{Cg}(a_j, b_j)]\!]$. Finally, by idempotence of t we have

$$d(a_j, b_j, b_j) \; [\![\mathrm{Cg}(a_j, b_j)]\!] \; a_j,$$

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 $[\![\mathrm{Cg}(a_i, b_i)]\!]$. Again, starting from the definition of d and using idempotence of p, we have

$$\begin{aligned} d(a_i, b_i, b_i) &= t(p(a_i, b_i, b_i), p(b_i, b_i, b_i), b_i) \\ &= t(p(a_i, b_i, b_i), b_i, b_i). \end{aligned} \tag{4.9}$$

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

$$t(p(a_i, b_i, b_i), b_i, b_i)\ [\![\mathrm{Cg}(a_i, b_i)]\!]\ t(a_i, b_i, b_i). \tag{4.10}$$

Since t is a local difference term for T, hence for (a_i, b_i, b_i), we see that $t(a_i, b_i, b_i)\ [\![\mathrm{Cg}(a_i, b_i)]\!]\ a_i$. Combining this with (4.9) and (4.10) yields $d(a_i, b_i, b_i)\ [\![\mathrm{Cg}(a_i, b_i)]\!]\ a_i$, 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 4.2. *A finite idempotent algebra* $\mathbf{A}$ *has a difference term operation if and only if each 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 4.1, 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 $a\ [\![\mathrm{Cg}(a, b)]\!]\ d(a, b, b)$, 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 $(a, b, 1)$. □

4.3. *Algorithm 1: existence of a difference term operation*

Corollary 4.3. *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 4.2, 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

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

We can rewrite this condition more compactly by considering

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

Clearly t 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 $\delta = [\![\mathrm{Cg}(a,b)]\!]$ 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 $\delta = [\![\mathrm{Cg}(a,b)]\!]$, 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 [8]). The time complexity of congruence generation is also known to be polynomial (see [5]). 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.

$\square$

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 [3,2,6].

5. Extensions and Generalizations

5.1. *Mixed local difference terms*

In this section, we observe that the proofs in the previous section did not hinge on the fact that we only considered a single algebra. Let $\mathcal{V}$ be a variety and let $\mathbf{A}_0 = \langle A_0, \dots \rangle$ and $\mathbf{A}_1 = \langle A_1, \dots \rangle$ be algebras in $\mathcal{V}$. The direct sum (or coproduct) of $\mathbf{A}_0$ and $\mathbf{A}_1$ is denoted by $\mathbf{A}_0 + \mathbf{A}_1$ (or by $\coprod_{i=0}^{1} \mathbf{A}_i$, especially when there are more than two factors). An element of (the universe of) $\mathbf{A}_0 + \mathbf{A}_1$ is often denoted by $\langle a, i \rangle$, where $i \in \{0,1\}$ and $a \in A_i$. The (universe of the) coproduct $\mathbf{A}_0^2 + \mathbf{A}_1^2$ has elements $\langle (a,b), i \rangle$ where $i \in \{0,1\}$ and $(a,b) \in A_i^2$. An element of the set $(A_0^2 + A_1^2) \times \{0,1\}$—and now the notation has already become a bit unwieldy—has the form $(\langle (a,b), i \rangle, \chi)$, where $i \in \{0,1\}$, $(a,b) \in A_i^2$, and $\chi \in \{0,1\}$.

Fix two elements $(\langle (a,b), i \rangle, \chi)$ and $(\langle (a',b'), i' \rangle, \chi')$ of the set $(A_0^2 + A_1^2) \times \{0,1\}$. By a *mixed local difference term* for this pair we mean a ternary term d satisfying both

$$\begin{aligned} &\text{if } \chi = 0, \text{ then } a \; [\![\mathrm{Cg}^{\mathbf{A}_i}(a,b)]\!] \; d^{\mathbf{A}_i}(a,b,b); \\ &\text{if } \chi = 1, \text{ then } d^{\mathbf{A}_i}(a,a,b) = b; \end{aligned} \tag{5.1}$$

and the same set of relations with a, b, i, χ replaced by a', b', i', χ', respectively.

Let S be a sequence of triples drawn from the set

$$\mathcal{U}(A_0, A_1) := (A_0^2 + A_1^2) \times \{0,1\}.$$

If d satisfies (5.1) for all triples in S. then we call d is a *mixed local difference term for* S. We may use $\mathcal{U}$ to denote the set $\mathcal{U}(A_0, A_1)$ when the context renders the universes involved obvious or immaterial.

Now, suppose that all pairs of triples in $\mathcal{U}$ have mixed local difference terms. Under this hypothesis the same argument that we used to prove Theorem 4.1 above can be used to prove that, for every n, every sequence $S \in \mathcal{U}^n$ has a mixed local difference term. That is, there is a single term d that works (i.e., satisfies the relations (5.1)) for all $(\langle (a,b), i \rangle, \chi)$ in S. Here is the full statement of this slightly more general version of Theorem 4.1. From now on we drop the "mixed" qualifier since it is inconsequential.

Theorem 5.1. *Let $\mathcal{V}$ be an idempotent variety and let $\mathbf{A}_0 = \langle A_0, \dots \rangle$ and $\mathbf{A}_1 = \langle A_1, \dots \rangle$ be algebras in $\mathcal{V}$. Define $\mathcal{U} = (A_0^2 + A_1^2) \times \{0,1\}$ and suppose that every pair $((\langle (a,b), i \rangle, \chi), (\langle (a',b'), i' \rangle \chi')) \in \mathcal{U}^2$ has a local difference term. Then, for every n, every sequence $S \in \mathcal{U}^n$ has a local difference term.*

Corollary 4.2 also generalizes, as follows:

Corollary 5.2. *Let $\mathcal{V}$ be an idempotent variety and let $\mathbf{A}_0 = \langle A_0, \dots\rangle$ and $\mathbf{A}_1 = \langle A_1, \dots\rangle$ be algebras in $\mathcal{V}$. Define $\mathcal{U} = (A_0^2 + A_1^2) \times \{0,1\}$ and suppose that every pair $((\langle(a,b),i\rangle,\chi),(\langle(a',b'),i'\rangle\chi')) \in \mathcal{U}^2$ has a local difference term. Then, there is a term d that interprets as a difference term operation for both $\mathbf{A}_0$ and $\mathbf{A}_1$.*

5.2. *Local difference terms on universes*

The methods from earlier sections can be lifted up to work globally—that is, on universes rather than elements—as we now explain. Let $\mathcal{V}$ be a variety, let $\mathbf{A} = \langle A, \dots\rangle \in \mathcal{V}$ and $i \in \{0,1\}$. We call a term d a *local difference term for* (A,i) provided d is a local difference term for every triple $(a,b,i) \in A \times A \times \{i\}$. That is, for all $a, b \in A$,

$$\text{if } i = 0, \text{ then } \; a \,[\![\mathrm{Cg}^{\mathbf{A}}(a,b)]\!]\, d^{\mathbf{A}}(a,b,b); \tag{5.2}$$

$$\text{if } i = 1, \text{ then } \; d^{\mathbf{A}}(a,a,b) = b. \tag{5.3}$$

Let $\mathcal{V}$ be a variety and let $\mathcal{A}$ be a collection of algebras that belong to $\mathcal{V}$. Let $\mathcal{S}(\mathcal{A})$ be the collection of all pairs (A,i) where A is the universe of some algebra in $\mathcal{A}$ and $i \in \{0,1\}$. That is,

$$\mathcal{S}(\mathcal{A}) = \{(A,i) \mid \langle A, \dots\rangle \in \mathcal{A} \text{ and } i \in \{0,1\}\}.$$

Given a sequence

$$S = ((A_0,\chi_0),(A_1,\chi_1),\dots,(A_{n-1},\chi_{n-1})) \in \mathcal{S}(\mathcal{A})^n,$$

(or a subset $S \subseteq \mathcal{S}(\mathcal{A})$), a term d is called a *local difference term for S* if it is a local difference term for every pair (A_i,χ_i) in S. In addition to these definitions, in the proof of the next theorem we use $|S|$ to denote the *length of the sequence S* (or, in case S is a set, then $|S|$ denotes the cardinality of S, as usual).

Theorem 5.3. *Let $\mathcal{V}$ be a variety. Let $\mathcal{A}$ be a collection of finite idempotent algebras in $\mathcal{V}$. Fix $n \geqslant 2$ and let $S = ((A_0,\chi_0),(A_1,\chi_1),\dots,(A_{n-1},\chi_{n-1})) \in \mathcal{S}(\mathcal{A})^n$. Then there exists a term that is a local difference term for S if and only if each 2-element subsequence $((A_i,\chi_i),(A_j,\chi_j))$ of S has a local difference term.*

We relegate the proof of Theorem 5.3 to the appendix (see Section A.1), since the argument is nearly identical to the one used to prove Theorem 4.1.

Corollary 5.4. *Let $\mathcal{V}$ be a variety. Let $\mathcal{A}$ be a collection of finite idempotent algebras in $\mathcal{V}$. Then there exists a term d that interprets as a difference term operation for every algebra in $\mathcal{A}$ if and only if each pair $((A,i),(B,j)) \in \mathcal{S}(\mathcal{A})^2$ has a local difference term.*

Since the proof of Corollary 5.4 is easy and similar to the proof of Corollary 4.2, we consign it to appendix Section A.2.

Before proceeding, recall the following fairly standard notation: if $\alpha \in \mathrm{Con}(\mathbf{A})$ and $\beta \in \mathrm{Con}(\mathbf{B})$, then $\alpha \times \beta$ denotes the set of pairs $((a,b),(a',b')) \in (A \times B)^2$ satisfying $a \,\alpha\, a'$ and $b \,\beta\, b'$. The relation $\alpha \times \beta$ is clearly a congruence of $\mathbf{A} \times \mathbf{B}$.

Lemma 5.5. *Let $\mathcal{V}$ be a variety and let* $\mathbf{A}$ *and* $\mathbf{B}$ *be finite idempotent algebras in* $\mathcal{V}$. *Suppose the term* d *interprets as a difference term operation for* $\mathbf{A} \times \mathbf{B}$. *Then* $d^{\mathbf{A}}$ *(resp.,* $d^{\mathbf{B}}$*) is a difference term operation for* $\mathbf{A}$ *(resp.,* $\mathbf{B}$*).*

Proof. Assume that for all (a, b) and (a', b') in $A \times B$, the term d satisfies

$$d^{\mathbf{A}\times\mathbf{B}}((a,b),(a,b),(a',b')) = (a',b'), \quad \text{and} \tag{5.4}$$

$$d^{\mathbf{A}\times\mathbf{B}}((a,b),(a',b'),(a',b')) \;[\![\mathrm{Cg}^{\mathbf{A}\times\mathbf{B}}((a,b),(a',b'))]\!]\; (a,b). \tag{5.5}$$

We prove that $d^{\mathbf{A}}$ is a difference term operation for $\mathbf{A}$. (Obviously, the proof for $\mathbf{B}$ is identical.) Thus, fixing $a, a' \in A$, we will show

$$d^{\mathbf{A}}(a,a,a') = a', \quad \text{and} \tag{5.6}$$

$$d^{\mathbf{A}}(a,a',a') \;[\![\mathrm{Cg}^{\mathbf{A}}(a,a')]\!]\; a. \tag{5.7}$$

Equation (5.6) is obvious by (5.4), so we proceed to (5.7). Observe that

$$(d^{\mathbf{A}}(a,a',a'), d^{\mathbf{B}}(b,b',b')) \;[\![\mathrm{Cg}^{\mathbf{A}\times\mathbf{B}}((a,b),(a',b'))]\!]\; (a,b),$$

by (5.5). Therefore, Lemma 2.5 implies[b]

$$(d^{\mathbf{A}}(a,a',a'),a) \in \pi_A\big([\![\mathrm{Cg}^{\mathbf{A}\times\mathbf{B}}((a,b),(a',b'))]\!]\big) \subseteq [\![\pi_A\big(\mathrm{Cg}^{\mathbf{A}\times\mathbf{B}}((a,b),(a',b'))\big)]\!].$$

Next, observe that $\mathrm{Cg}^{\mathbf{A}}(a,a') \times \mathrm{Cg}^{\mathbf{B}}(b,b')$ is a product of two congruences, one in $\mathrm{Con}(\mathbf{A})$ and the other in $\mathrm{Con}(\mathbf{B})$, so it is a congruence of $\mathbf{A} \times \mathbf{B}$. Moreover, it contains the pair $((a,b),(a',b'))$, so

$$\mathrm{Cg}^{\mathbf{A}\times\mathbf{B}}((a,b),(a',b')) \leqslant \mathrm{Cg}^{\mathbf{A}}(a,a') \times \mathrm{Cg}^{\mathbf{B}}(b,b').$$

Therefore,

$$\pi_A\big(\mathrm{Cg}^{\mathbf{A}\times\mathbf{B}}((a,b),(a',b'))\big) \leqslant \pi_A\big(\mathrm{Cg}^{\mathbf{A}}(a,a') \times \mathrm{Cg}^{\mathbf{B}}(b,b')\big) = \mathrm{Cg}^{\mathbf{A}}(a,a').$$

Pulling all of these observations together and applying monotonicity of the commutator, we arrive at $d^{\mathbf{A}}(a,a',a') \;[\![\mathrm{Cg}^{\mathbf{A}}(a,a')]\!]\; a$, as desired. □

The converse of Lemma 5.5 is harder to prove.

Lemma 5.6. *Let $\mathcal{V}$ be a variety and let* $\mathbf{A}$ *and* $\mathbf{B}$ *be finite idempotent algebras in* $\mathcal{V}$. *Suppose there is a single term* d *that interprets as a difference term operation for* $\mathbf{A}$ *and for* $\mathbf{B}$. *Then* $d^{\mathbf{A}\times\mathbf{B}}$ *is a difference term operation for the product* $\mathbf{A} \times \mathbf{B}$.

Proof. Fix (a, b) and (a', b') in $A \times B$. We must prove

$$d^{\mathbf{A}\times\mathbf{B}}((a,b),(a,b),(a',b')) = (a',b'), \quad \text{and} \tag{5.8}$$

$$d^{\mathbf{A}\times\mathbf{B}}((a,b),(a',b'),(a',b')) \;[\![\mathrm{Cg}^{\mathbf{A}\times\mathbf{B}}((a,b),(a',b'))]\!]\; (a,b). \tag{5.9}$$

[b]The first projection $\pi_A : \mathbf{A} \times \mathbf{B} \to \mathbf{A}$ is a surjective homomorphism, so $\pi_A([\![\theta]\!]) \subseteq [\![\pi_A(\theta)]\!]$ for all $\theta \in \mathrm{Con}(\mathbf{A} \times \mathbf{B})$, by Lemma 2.5. Recall, that π_A is defined on a congruence $\theta \in \mathrm{Con}(\mathbf{A} \times \mathbf{B})$ as follows: $\pi_A(\theta) := \{(a,a') \in A^2 \mid ((a,b),(a',b')) \in \theta \text{ for some } (b,b') \in B^2\}$.

Since $d^{\mathbf{A}}$ and $d^{\mathbf{B}}$ are difference term operations for $\mathbf{A}$ and $\mathbf{B}$, respectively, it's easy to see that (5.8) is satisfied:

$$d^{\mathbf{A}\times\mathbf{B}}((a,b),(a,b),(a',b')) = (d^{\mathbf{A}}(a,a,a'), d^{\mathbf{B}}(b,b,b')) = (a',b').$$

It remains to check (5.9). Again, since $d^{\mathbf{A}}$ and $d^{\mathbf{B}}$ are difference term operations,

$$d^{\mathbf{A}}(a,a',a') \; [\![\mathrm{Cg}^{\mathbf{A}}(a,a')]\!] \; a$$
$$d^{\mathbf{B}}(b,b',b') \; [\![\mathrm{Cg}^{\mathbf{B}}(b,b')]\!] \; b.$$

Therefore, the pair $\big((d^{\mathbf{A}}(a,a',a'), d^{\mathbf{B}}(b,b',b')),(a,b)\big)$ belongs to the relation

$$[\![\mathrm{Cg}^{\mathbf{A}}(a,a')]\!] \times [\![\mathrm{Cg}^{\mathbf{B}}(b,b')]\!].$$

We claim that the latter is equal to $[\![\mathrm{Cg}^{\mathbf{A}}(a,a') \times \mathrm{Cg}^{\mathbf{B}}(b,b')]\!]$. Recall from above that

$$\mathrm{Cg}^{\mathbf{A}\times\mathbf{B}}((a,b),(a',b')) \leqslant \mathrm{Cg}^{\mathbf{A}}(a,a') \times \mathrm{Cg}^{\mathbf{B}}(b,b').$$

Therefore, if we prove that

$$[\![\mathrm{Cg}^{\mathbf{A}}(a,a')]\!] \times [\![\mathrm{Cg}^{\mathbf{B}}(b,b')]\!] = [\![\mathrm{Cg}^{\mathbf{A}}(a,a') \times \mathrm{Cg}^{\mathbf{B}}(b,b')]\!],$$

then we could complete the proof by showing that

$$\mathrm{Cg}^{\mathbf{A}\times\mathbf{B}}((a,b),(a',b')) \geqslant \mathrm{Cg}^{\mathbf{A}}(a,a') \times \mathrm{Cg}^{\mathbf{B}}(b,b'). \tag{5.10}$$

TODO: (5.10) is false in general; maybe false here too; then we need a new idea.

TODO: Prove Lemma 5.6 somehow!!! □

5.3. *Algorithm 2: existence of a difference term*

Corollary 5.7. *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. Let $\mathcal{V} = \mathbb{V}(\mathbf{A})$ and let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x,y)$ be the free algebra in $\mathcal{V}$ generated by x and y. By Theorem 3.1, deciding whether $\mathcal{V}$ has a difference term is equivalent to deciding whether $\mathbf{F}$ has a difference term operation. We can assume $\mathbf{F}$ is a subdirect product of $\mathbf{A}_0 \times \mathbf{A}_1 \times \cdots \times \mathbf{A}_{n-1}$, where $n \leqslant |A|^2$ and where each $\mathbf{A}_i$ is a 2-generated subalgebra of $\mathbf{A}$.. Let $\mathcal{A} = \{A_0, A_1, \ldots, A_{n-1}\}$ and (as above) let $\mathcal{S}(\mathcal{A})$ denote all pairs (A,i) such that $\mathbf{A} = \langle A, \ldots \rangle \in \mathcal{A}$ and $i \in \{0,1\}$.

We begin by proving that we can check in polynomial time (in $|A|$) whether or not the product $\mathbf{A}_0 \times \mathbf{A}_1 \times \cdots \times \mathbf{A}_{n-1}$ has a difference term operation. By Corollary 5.4 and Lemma 5.6, it suffices to check that each of the n^2 pairs in $\mathcal{S}(\mathcal{A})^2$ has a local difference term. Fix a pair $((A_i,\chi_i),(A_j,\chi_j)) \in \mathcal{S}(\mathcal{A})^2$, and let $\mathcal{U} = (A_i^2 + A_j^2) \times \{0,1\}$. By Theorem 5.1, to prove that every sequence $S \in \mathcal{U}^n$ has a local difference term, it suffices to check that every pair

$\big((\langle(a,b),i\rangle,\chi),(\langle(a',b'),i'\rangle,\chi')\big) \in \mathcal{U}^2$ has a local difference term. It follows from the argument given in the proof of Corollary 4.3 that the number of operations required to check whether $\big((\langle(a,b),i\rangle,\chi),(\langle(a',b'),i'\rangle,\chi')\big)$ has a local difference term is bounded by a polynomial in $|A_i||A_j| \leqslant |A|^2$. Since there are $4|A_i|^2|A_j|^2 \leqslant 4|A|^4$ pairs in $\mathcal{U}^2$, it still takes only a polynomial in $|A|$ number of steps to test whether the pair $((A_i,\chi_i),(A_j,\chi_j))$ has a local difference term. There are $n^2 \leqslant |A|^4$ such pairs to test, so the number of steps required to test whether $\mathbf{A}_0 \times \mathbf{A}_1 \times \cdots \times \mathbf{A}_{n-1}$ has a difference term operation is bounded by a constant times a power of $|A|$.

TODO: complete the proof by showing that if the product $\mathbf{A}_0 \times \mathbf{A}_1 \times \cdots \times \mathbf{A}_{n-1}$ has a difference term operation, then so does the subdirect product $\mathbf{F}$. $\square$

Acknowledgments

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

References

[1] C. Bergman, *Universal algebra*, **301** of *Pure and Applied Mathematics (Boca Raton)* (CRC Press, Boca Raton, FL, 2012). Fundamentals and selected topics.
[2] C. Bergman, D. Juedes and G. Slutzki, Computational complexity of term-equivalence, *Internat. J. Algebra Comput.* **9**(1) (1999) 113–128.
[3] C. Bergman and G. Slutzki, Computational complexity of some problems involving congruences on algebras, *Theoret. Comput. Sci.* **270**(1-2) (2002) 591–608.
[4] W. DeMeo, On deciding existence of difference terms to appear.
[5] R. Freese, Computing congruences efficiently, *Algebra Universalis* **59**(3-4) (2008) 337–343.
[6] R. Freese and M. A. Valeriote, On the complexity of some Maltsev conditions, *Internat. J. Algebra Comput.* **19**(1) (2009) 41–77.
[7] D. Hobby and R. McKenzie, *The structure of finite algebras*, **76** of *Contemporary Mathematics* (American Mathematical Society, Providence, RI, 1988). Available from: math.hawaii.edu.
[8] N. D. Jones and W. T. Laaser, Complete problems for deterministic polynomial time, *Theoret. Comput. Sci.* **3**(1) (1976) 105–117 (1977).
[9] K. Kearnes, A. Szendrei and R. Willard, Simpler maltsev conditions for (weak) difference terms in locally finite varieties to appear.
[10] K. Kearnes, Á. Szendrei and R. Willard, A finite basis theorem for difference-term varieties with a finite residual bound, *Trans. Amer. Math. Soc.* **368**(3) (2016) 2115–2143.
[11] K. A. Kearnes, Varieties with a difference term, *J. Algebra* **177**(3) (1995) 926–960.
[12] K. A. Kearnes and E. W. Kiss, The shape of congruence lattices, *Mem. Amer. Math. Soc.* **222**(1046) (2013) viii+169.
[13] K. A. Kearnes and Á. Szendrei, The relationship between two commutators, *Internat. J. Algebra Comput.* **8**(4) (1998) 497–531.
[14] M. Valeriote and R. Willard, Idempotent n-permutable varieties, *Bull. Lond. Math. Soc.* **46**(4) (2014) 870–880.

Appendix A. Miscellaneous Proofs

A.1. *Proof of Theorem 5.3*

Theorem Appendix A.1 (5.3). *Let $\mathcal{V}$ be a variety. Let $\mathcal{A}$ be a collection of finite idempotent algebras in $\mathcal{V}$. Fix $n \geqslant 2$ and let $S = ((A_0, \chi_0), (A_1, \chi_1), \ldots, (A_{n-1}, \chi_{n-1})) \in \mathcal{S}(\mathcal{A})^n$. Then there exists a term that is a local difference term for S if and only if each 2-element subsequence $((A_i, \chi_i), (A_j, \chi_j))$ of S has a local difference term.*

Proof. One direction is clear; if d is a local difference term for every element (A_i, χ_i) of S, then every pair $((A_i, \chi_i), (A_j, \chi_j))$ of elements of S also has a local difference term—namely, d.

For the converse, suppose that for each pair $((A_i, \chi_i), (A_j, \chi_j))$ of elements of S there exists a term p_{ij} that is a local difference term for both (A_i, χ_i) and (A_j, χ_j). We will prove by induction on the length of S that there exists a term d that is a local difference term for every (A_i, χ_i) in S.

In the base case, $n = |S| = 2$, the claim holds by assumption. Fix $n \geqslant 2$ and assume for every $2 \leqslant k \leqslant n$ that every sequence in $\mathcal{S}(\mathcal{A})^k$ has a local difference term. Let $S = ((A_0, \chi_0), (A_1, \chi_1), \ldots, (A_n, \chi_n)) \in \mathcal{S}(\mathcal{A})^{n+1}$. 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 subsequence $S' = ((A_1, \chi_1), \ldots, (A_n, \chi_n))$ of S. Since $|S'| = n$, the sequence S' has a local difference term p. Thus, for all $1 \leqslant i \leqslant n$, for all $a, b \in A_i$ we have

$$\text{if } \chi_i = 0, \text{ then } a \; [\![\mathrm{Cg}(a,b)]\!] \; d(a,b,b);$$
$$\text{if } \chi_i = 1, \text{ then } d(a,a,b) = b.$$

We split the remainder of the proof into two cases.

<u>Case $\chi_0 = 0$:</u> 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

$$T = ((A_0, 0), (A_1, 1), (A_2, 1), \ldots, (A_k, 1)).$$

Note that $|T| < |S|$. Let t be a 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 local difference term for S.

The first element of S is $(A_0, 0)$, so we need to show for all a, $b \in A_0$ that

$$d(a,b,b) \; [\![\mathrm{Cg}(a,b)]\!] \; a.$$

Fix $a, b \in A_0$. By definition of d, and since t is a local difference term for $(A_0, 0)$, we have

$$d(a,b,b) = t(a,c,c) \; [\![\mathrm{Cg}(a,c)]\!] \; a, \tag{A.1}$$

where $c = p(a,b,b)$. Now, $(a,c) = (p(a,a,a), p(a,b,b)) \in \mathrm{Cg}(a,b)$, therefore, $\mathrm{Cg}(a,c) \leqslant \mathrm{Cg}(a,b')$. It follows from this and monotonicity of the commutator that $[\![\mathrm{Cg}(a,c)]\!] \leqslant [\![\mathrm{Cg}(a,b)]\!]$, This and (A.1) imply $d(a,b,b)\ [\![\mathrm{Cg}(a,b)]\!]\ a$, as desired.

Next, consider the (possibly empty) set of indices $\{i \mid 1 \leqslant i \leqslant k\}$. For such indices $\chi_i = 1$, so we will prove for all a, $b \in A_i$ that $d(a,a,b) = b$. Fix $a, b \in A_i$ and observe that

$$\begin{aligned} d(a,a,b) &= t(a, p(a,a,a), p(a,a,b)) && \text{(A.2)}\\ &= t(a,a,b) && \text{(A.3)}\\ &= b. && \text{(A.4)} \end{aligned}$$

Equation (A.2) holds by definition of d, (A.3) because p is an idempotent local difference term for S', and (A.4) because t is a local difference term for T.

The indices of the remaining elements of S belong to the set $\{j \mid k < j \leqslant n\}$ (which is nonempty since we assumed $\chi_0 = \chi_i = 0$ for some $i > 0$). For such indices we have $\chi_j = 0$. Thus, fixing $a, b \in A_j$, we check that $d(a,b,b)\ [\![\mathrm{Cg}(a,b)]\!]\ a$. By definition,

$$d(a,b,b) = t(a, p(a,b,b), p(a,b,b)). \tag{A.5}$$

Also, $p(a,b,b)\ [\![\mathrm{Cg}(a,b)]\!]\ a$, since p is a local difference term for S'. This and (A.5) imply that $d(a,b,b)\ [\![\mathrm{Cg}(a,b)]\!]\ t(a,a,a))$. Finally, by idempotence of t we have $d(a,b,b)\ [\![\mathrm{Cg}(a,b)]\!]\ a$, as desired.

<u>Case $\chi_0 = 1$:</u> 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

$$T = ((A_0, 1), (A_1, 0), (A_2, 0), \ldots, (A_k, 0)).$$

and note that $|T| < |S|$, so T has a 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 local difference term for S.

The first pair in S is $(A_0, 1)$, so we want to show for all a, $b \in A_0$ that $d(a,a,b) = b$. Fix a, $b \in A_0$. By definition of d, we have $d(a,a,b) = t(p(a,a,b), p(a,a,b), b) = b$. The last equality holds since t is a local difference term for T, in particular, for $(A_0, 1)$.

Next, consider the (possibly empty) set of indices $\{i \mid 1 \leqslant i \leqslant k\}$. For such indices $\chi_i = 0$, so we will prove for all a, $b \in A_i$ that

$$d(a,b,b)\ [\![\mathrm{Cg}(a,b)]\!]\ a.$$

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

$$\begin{aligned} d(a,b,b) &= t(p(a,b,b), p(b,b,b), b) && \text{(A.6)}\\ &= t(p(a,b,b), b, b). \end{aligned}$$

Next, since p is a local difference term for S', hence for $(A_i, 0)$, we have

$$t(p(a,b,b), b, b)\ [\![\mathrm{Cg}(a,b)]\!]\ t(a,b,b). \tag{A.7}$$

Finally, since t is a local difference term for T, hence for $(A_i, 0)$, we have

$$t(a, b, b) \, [\![\mathrm{Cg}(a, b)]\!] \, a.$$

Combining this with (A.6) and (A.7) yields $d(a, b, b) \, [\![\mathrm{Cg}(a, b)]\!] \, a$, as desired.

The indices of the remaining elements of S belong to the set $\{j \mid k < j \leqslant n\}$ (which is nonempty since we assumed $\chi_0 = \chi_i = 1$ for some $i > 0$). For such indices we have $\chi_j = 1$. Thus, fixing $a, b \in A_j$, we check that $d(a, a, b) = b$. Indeed, $p(a, a, b) = b$, since p is a local difference term for S'; this, along with idempotence of t, yields $d(a, a, b) = t(p(a, a, b), p(a, a, b), b) = t(b, b, b) = b$. □

A.2. *Proof of Corollary 5.4*

Corollary Appendix A.2 (5.4). *Let $\mathcal{V}$ be a variety. Let $\mathcal{A}$ be a collection of finite idempotent algebras in $\mathcal{V}$. Then there exists a term d that interprets as a difference term operation for every algebra in $\mathcal{A}$ if and only if each pair $((A, i), (B, j)) \in \mathcal{S}(\mathcal{A})^2$ has a local difference term.*

The proof of this result is also easy and very similar to the proof of 4.2; nevertheless, it appears in the appendix (see Section A.1).

Proof. One direction is clear, since a term that is a difference term operation for every $\mathbf{A} \in \mathcal{A}$ is obviously a local difference term for every $(A, i) \in \mathcal{S}(\mathcal{A})$. For the converse, suppose each pair in $\mathcal{S}(\mathcal{A})^2$ has a local difference term. Then, by Theorem 5.3, there is a single term d that is a local difference term for every $(A, i) \in \mathcal{S}(\mathcal{A})$, and therefore d interprets as a difference term operation for every $\mathbf{A} \in \mathcal{A}$. To see this, choose an arbitrary $\mathbf{A} = \langle A, \dots \rangle \in \mathcal{A}$ and fix $a, b \in A$. Then $a \, [\![\mathrm{Cg}(a, b)]\!] \, d^{\mathbf{A}}(a, b, b)$, since d is a local difference term for $(A, 0)$, and $d^{\mathbf{A}}(a, a, b) = b$, since d is a local difference term for $(A, 1)$. □