Last updated: 6 April 2017

ON THE COMPLEXITY OF DIFFERENCE TERM EXISTENCE

William DeMeo[1] **and Ralph Freese**[2]

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 define "local difference terms" and used to solve a related but easier problem—namely, we show that there is a polynomial-time algorithm for deciding whether any finite idempotent algebra has a difference term operation. Thereafter, we define "global-local difference terms" which we use to make some progress toward an efficient algorithm for deciding whether the variety generated by a finite idempotent algebra has a difference term.

AMS Mathematics Subject Classification (2000): 08B05, 08B10, 68Q25

Key words: difference term, idempotent algebra, commutator

introduction

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 $\mathbf{A} = \langle A, \dots \rangle \in \mathcal{V}$, for all $a, b \in A$, for every congruence $\theta \in \operatorname{Con} \mathbf{A}$ containing (a, b), we have

eq:3

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

where $[\cdot, \cdot]$ denotes the (term condition) commutator defined in Section 2 below (see also [10] or [15]). (By the monotonicity of the commutator, we could replace θ in the definition by $\operatorname{Cg}^{\mathbf{A}}(a, b)$.) If for all $a, b \in A$ the relations in (1.1) hold with $\theta = \operatorname{Cg}^{\mathbf{A}}(a, b)$, then 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, [10, 12, 13, 14, 15, 16].) 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

[1] Department of Mathematics, University of Hawaii,
e-mail: williamdemeo@gmail.com

[2] Department of Mathematics, University of Hawaii,
e-mail: ralph@math.hawaii.edu

the fact that researchers have found ingenious ways to get computers to solve abstract decision problems—such as whether a variety is congruence-modular ([7]) or congruence-n-permutable ([19])—and to do so efficiently.

Consider the following problems:

prob:1 **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?

prob:2 **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 the present paper we solve Problem 2 and then discuss the progress we have made toward a solution to Problem 1.

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 [14] 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 observe that this is also equivalent to the free algebra $\mathbf{F}_{\mathcal{V}}(2)$ itself having a difference term operation. In [19], 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 4.1, 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 describe some recent progress toward 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 (TODO!!!), and mention some related problems that remain open (TODO!!!).

2. Background, Notation, Definitions

finitions

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].

Let A and B be sets and let $\alpha \subseteq A \times A$ and $\beta \subseteq B \times B$ be binary relations on A and B, respectively. We define the *pairwise product* of α and β by

r-product
$$\alpha * \beta = \{((a,b),(a',b')) \in (A \times B)^2 \mid a \; \alpha \; a' \text{ and } b \; \beta \; b'\}, \tag{2.1}$$

and we let $\alpha \times \beta$ denote the usual Cartesian product of sets; that is,

t-product
$$\alpha \times \beta = \{((a,a'),(b,b')) \in A^2 \times B^2 \mid a \; \alpha \; a' \text{ and } b \; \beta \; b'\}. \tag{2.2}$$

Notice that $\alpha * \beta$ defines an equivalence relation on $A \times B$, whereas in general $\alpha \times \beta$ is not even a binary relation on a single set. The equivalence class of $\alpha * \beta$ containing the pair (a, b) is denoted and defined by

$$(a,b)/(\alpha * \beta) = a/\alpha \times b/\beta = \{(a',b') \in A \times B \mid a \; \alpha \; a' \text{ and } b \; \beta \; b'\},$$

the Cartesian product of the sets a/α and b/β. The collection of all such equivalence classes is also a Cartesian product, namely,

$$(A \times B)/(\alpha * \beta) = A/\alpha \times B/\beta = \{(a,b)/(\alpha * \beta) \mid a \in A \text{ and } b \in B\}.$$

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 sometimes use the short-hand $\mathbf{u}\ \mathbf{T}\ \mathbf{v}$ to mean "$\mathbf{u}(i)\ T\ \mathbf{v}(i)$ for all $0 \leqslant i < m$."

The set of all tolerance relations of $\mathbf{A}$ is denoted $\operatorname{Tol}(\mathbf{A})$, and the set of all congruence relations is denoted $\operatorname{Con}(\mathbf{A})$. The subalgebra of $\mathbf{A}$ generated by a set $X \subseteq A$ is denoted by $\operatorname{Sg}^{\mathbf{A}}(X)$, and the congruence relation of $\mathbf{A}$ generated by a set $X \subseteq A \times A$ is denoted by $\operatorname{Cg}^{\mathbf{A}}(X)$. (We sometimes leave off the parentheses and write $\operatorname{Sg}^{\mathbf{A}} X$ or $\operatorname{Cg}^{\mathbf{A}} X$. If X is finite, say, $X = \{(a,b)\}$, we typically write $\operatorname{Cg}^{\mathbf{A}}(a,b)$ instead of $\operatorname{Cg}^{\mathbf{A}}\{(a,b)\}$.)

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

eq:22

$$t(\mathbf{a},\mathbf{u})\ \delta\ t(\mathbf{a},\mathbf{v}) \quad \Longleftrightarrow \quad t(\mathbf{b},\mathbf{u})\ \delta\ t(\mathbf{b},\mathbf{v}), \tag{2.3}$$

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 (2.3) 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 [10, Prop 3.4] or [15, Thm 2.19]).

centralizers **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:*

over_meet *1.* $\mathsf{C}(\alpha, \beta; \alpha \wedge \beta)$*;*

ver_meet2 *2. if* $\mathsf{C}(\alpha, \beta; \gamma_k)$ *for all* $k \in K$*, then* $\mathsf{C}(\alpha, \beta; \bigwedge_K \gamma_k)$*;*

ver_join1 *3. if* $\mathsf{C}(\alpha_i, \beta; \gamma)$ *for all* $i \in I$*, then* $\mathsf{C}(\bigvee_I \alpha_i, \beta; \gamma)$*;*

ralizers1 *4. if* $\mathsf{C}(\alpha, \beta; \gamma)$ *and* $\alpha' \leqslant \alpha$*, then* $\mathsf{C}(\alpha', \beta; \gamma)$*;*

ralizers2 *5. if* $\mathsf{C}(\alpha, \beta; \gamma)$ *and* $\beta' \leqslant \beta$*, then* $\mathsf{C}(\alpha, \beta'; \gamma)$*;*

er_subalg *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* $\mathbf{B}$*;*

g_factors *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, especially when reasoning about difference terms. The next two lemmas are easy consequences of Lemma 2.1, so we omit the proofs. (See Section B.1 of the extended version of this paper [5].)

tone-comm **Lemma 2.3** (Monotonicity of the Commutator)**.** *Let* $\mathbf{A}$ *be an algebra with congruences* α*,* α'*,* β*,* β' *satisfying* $\alpha \leqslant \alpha'$ *and* $\beta \leqslant \beta'$*. Then* $[\alpha, \beta] \leqslant [\alpha', \beta']$*.*

-monotone **Lemma 2.4.** *Let* $\mathbf{A}$ *be an algebra with congruences* α_i *and* β_i *for all* $i \in I$*. Then*

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

The next result is useful when considering a commutator computed with respect to a subalgebra $\mathbf{B} \leqslant \mathbf{A}$, rather than with respect to the whole algebra $\mathbf{A}$. In the statement of the lemma, we use shorthand notation that will come in handy below. The commutator of a congruence θ with itself, which appears so often in the sequel, will be abbreviated as follows:[3]

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

ebra-comm **Lemma 2.5.** *If* $\mathbf{B} \leqslant \mathbf{A}$ *and* $a, b \in B$*, then* $[\mathrm{Cg}^{\mathbf{B}}(a, b)] \subseteq [\mathrm{Cg}^{\mathbf{A}}(a, b)]$*.*

Proof. Let $\alpha = \mathrm{Cg}^{\mathbf{A}}(a, b)$, $\beta = \mathrm{Cg}^{\mathbf{B}}(a, b)$, and $\delta = [\mathrm{Cg}^{\mathbf{A}}(a, b)] \cap B^2$. To prove the lemma it suffices to show that $\mathsf{C}(\beta, \beta; \delta)$ holds, since this will give us the required $\leqslant$ relation in the following:

$$[\mathrm{Cg}^{\mathbf{B}}(a, b)] = [\beta, \beta] \leqslant \delta \subseteq [\mathrm{Cg}^{\mathbf{A}}(a, b)].$$

Let $\mathbf{r}$, $\mathbf{s} \in B^k$, $\mathbf{u}$, $\mathbf{v} \in B^\ell$, and $t \in \mathsf{Clo}_{k+\ell}(\mathbf{B})$. Assume $r_i \mathrel{\beta} s_i$ and $u_i \mathrel{\beta} v_i$ and $t(\mathbf{r}, \mathbf{u}) \mathrel{\delta} t(\mathbf{r}, \mathbf{v})$. We must prove $t(\mathbf{s}, \mathbf{u}) \mathrel{\delta} t(\mathbf{s}, \mathbf{v})$. Clearly, $\beta \subseteq \alpha$, so $r_i \mathrel{\beta} s_i$ and $u_i \mathrel{\beta} v_i$ imply $r_i \mathrel{\alpha} s_i$ and $u_i \mathrel{\alpha} v_i$. Therefore, $(t(\mathbf{r}, \mathbf{u}), t(\mathbf{r}, \mathbf{v})) \in \delta \subseteq [\alpha, \alpha]$ implies $(t(\mathbf{s}, \mathbf{u}), t(\mathbf{s}, \mathbf{v})) \in [\alpha, \alpha]$. Of course, $(t(\mathbf{s}, \mathbf{u}), t(\mathbf{s}, \mathbf{v})) \in B^2$, since $\mathbf{B}$ is a subalgebra. Therefore, $(t(\mathbf{s}, \mathbf{u}), t(\mathbf{s}, \mathbf{v})) \in [\alpha, \alpha] \cap B^2 = \delta$, as desired. □

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

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

Before stating the next result, we remind the reader of a standard notational convention. If $\varphi \in \mathrm{Hom}(\mathbf{A}, \mathbf{B})$ and $\theta \in \mathrm{Con}(\mathbf{A})$, then by $\varphi(\theta)$ we mean the set $\{(\varphi(x), \varphi(y)) \mid x \mathrel{\theta} y\}$.

ge-diff-term

Lemma 2.6 ([14, Theorem 2.10]). *Let* $\mathbf{A}$, $\mathbf{B}$ *be algebras of the same similarity type and suppose* $\varphi : \mathbf{A} \to \mathbf{B}$ *is a surjective homomorphism. If* $\alpha, \beta \in \mathrm{Con}\,\mathbf{A}$, *then* $\varphi([\alpha, \beta]) \subseteq [\varphi(\alpha), \varphi(\beta)]$. *Moreover, if there exists a homomorphism* $\psi : \mathbf{B} \to \mathbf{A}$ *such that* $\varphi \circ \psi = \mathrm{id}_B$ *and* $\rho, \sigma \in \mathrm{Con}\,\mathbf{B}$, *then*

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

In fact, this result holds even if φ is not surjective. (See the remark after the proof of [14, Theorem 2.10].)

lem:hom-cong

Lemma 2.7. *Let* $\mathbf{A}$, $\mathbf{B}$ *be algebras of the same similarity type and suppose* $\varphi : \mathbf{A} \to \mathbf{B}$ *is a surjective homomorphism. If* $a, a' \in A$, *then* $\varphi\big(\mathrm{Cg}^{\mathbf{A}}(a, a')\big) = \mathrm{Cg}^{\mathbf{B}}\big(\varphi(a), \varphi(a')\big)$.

Proof. We first let $(u, v) \in \varphi\big(\mathrm{Cg}^{\mathbf{A}}(a, a')\big)$—that is, $(u, v) = \big(\varphi(x), \varphi(y)\big)$ for some $(x, y) \in \mathrm{Cg}^{\mathbf{A}}(a, a')$— and we will show $(u, v) \in \mathrm{Cg}^{\mathbf{B}}\big(\varphi(a), \varphi(a')\big)$. By Malcev's theorem, $(x, y) \in \mathrm{Cg}^{\mathbf{A}}(a, a')$ iff there exist $c_i \in A$, $z_i \in \{a, a'\}$, and $f_i \in \mathrm{Pol}(\mathbf{A})$ such that

$$\{x, c_1\} = \{f_0(z_0), f_0(z_1)\}, \{c_1, c_2\} = \{f_1(z_1), f_1(z_2)\}, \dots$$
$$\dots, \{c_{n-1}, y\} = \{f_{n-1}(z_{n-1}), f_{n-1}(z_n)\}.$$

Now apply φ to all elements to get

$$\{\varphi(x), \varphi(c_1)\} = \{\varphi(f_0(z_0)), \varphi(f_0(z_1))\},$$
$$\{\varphi(c_1), \varphi(c_2)\} = \{\varphi(f_1(z_1)), \varphi(f_1(z_2))\}, \dots$$
$$\dots, \{\varphi(c_{n-1}), \varphi(y)\} = \{\varphi(f_{n-1}(z_{n-1})), \varphi(f_{n-1}(z_n))\};$$

that is,[4]

$$\{u, \varphi(c_1)\} = \{f_0(\varphi(z_0)), f_0(\varphi(z_1))\}, \{\varphi(c_1), \varphi(c_2)\} = \{f_1(\varphi(z_1)), f_1(\varphi(z_2))\}, \dots$$

eq:11111

$$\dots, \{\varphi(c_{n-1}), v\} = \{f_{n-1}(\varphi(z_{n-1})), f_{n-1}(\varphi(z_n))\}. \tag{2.4}$$

Now, again by Malcev's theorem, the relations in (2.4) hold iff (u, v) belongs to $\mathrm{Cg}^{\mathbf{B}}\big(\varphi(a), \varphi(a')\big)$, and the latter is what we set out to prove.

For the opposite inclusion, note that φ takes congruences to congruences, so $\varphi\big(\mathrm{Cg}^{\mathbf{A}}(a, a')\big)$ is a congruence of $\mathbf{B}$ that clearly contains $(\varphi(a), \varphi(a'))$. Therefore, $\mathrm{Cg}^{\mathbf{B}}\big(\varphi(a), \varphi(a')\big) \subseteq \varphi\big(\mathrm{Cg}^{\mathbf{A}}(a, a')\big)$. □

[4] Since φ is a homomorphism, to every polynomial $g^{\mathbf{A}} \in \mathrm{Pol}(\mathbf{A})$ there corresponds a polynomial $g^{\mathbf{B}} \in \mathrm{Pol}(\mathbf{B})$ satisfying $\varphi g^{\mathbf{A}} = g^{\mathbf{B}}\varphi$. This justifies equating $\varphi(f_i(z_i))$ with $f_i(\varphi(z_i))$ above.

ond-exist

3. Conditions for Existence of a Difference Term

The main result of this section is Theorem 3.3, which is essentially due to Keith Kearnes and is based on an observation in [14] asserting 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, $d^{\mathbf{A}}(a,b,b) = d^{\mathbf{B}}(a,b,b)\ [\operatorname{Cg}^{\mathbf{B}}(a,b)]\ a$. However, $[\operatorname{Cg}^{\mathbf{B}}(a,b)] \subseteq [\theta]$ for every congruence $\theta \in \operatorname{Con}\mathbf{A}$ containing (a,b). Consequently $d^{\mathbf{A}}(a,b,b)\ [\theta]\ a$ as desired.

Considering the goal of our project, it is natural to ask whether 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 3.3, which will play a key role in our main complexity argument in Section 5.2. First, the lemma that does the heavy lifting in the proof of Theorem 3.3 is the following:

d-exist-1 **Lemma 3.1.** *Let* $\mathbf{A}$ *be an algebra, let* $t(x,y,z)$ *be a ternary term in the language of* $\mathbf{A}$*, and let* $\mathbf{F} = \mathbf{F}_{\mathbb{V}(\mathbf{A})}(x,y)$*. Consider the following statements:*

item:6 *(A)* $t^{\mathbf{A}}$ *is not a difference term operation for* $\mathbf{A}$*.*

item:7 *(B) There exists a 2-generated subalgebra* $\mathbf{B} \leqslant \mathbf{A}$ *such that* $t^{\mathbf{B}}$ *is not a difference term operation for* $\mathbf{B}$*.*

item:8 *(C)* $t^{\mathbf{F}}$ *is not a difference term operation for* $\mathbf{F}$*.*

Then (A) implies (B) and (B) implies (C).

Proof. (A) ⇒ (B): Suppose $t^{\mathbf{A}}$ fails to be a difference term operation for $\mathbf{A}$ and let $a, b \in A$ witness this failure. That is, either

item:9 1. $d^{\mathbf{A}}(a,a,b) \neq b$, or

item:10 2. $(d^{\mathbf{A}}(a,b,b), a) \notin [\operatorname{Cg}^{\mathbf{A}}(a,b)]$.

Let $\mathbf{B} = \operatorname{Sg}^{\mathbf{A}}\{a,b\}$. 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 $(d^{\mathbf{B}}(a,b,b), a) = (d^{\mathbf{A}}(a,b,b), a) \notin [\operatorname{Cg}^{\mathbf{A}}(a,b)]$. By Lemma 2.5, $[\operatorname{Cg}^{\mathbf{B}}(a,b)] \subseteq [\operatorname{Cg}^{\mathbf{A}}(a,b)]$, from which it follow that $(d^{\mathbf{B}}(a,b,b), a) \notin [\operatorname{Cg}^{\mathbf{B}}(a,b)]$. Therefore, $d^{\mathbf{B}}(x,y,z)$ is not a difference term operation for $\mathbf{B}$.

(B) ⇒ (C): Since there is a surjective homomorphism from $\mathbf{F}$ to $\mathbf{B}$, Lemma 2.6 implies that $d^{\mathbf{F}}(x,y,z)$ is not a difference term operation for $\mathbf{F}$. □

Obviously, we could have stated 3.1 in the following positive form:

Corollary 3.2. *Let* $\mathbf{A}$ *be an algebra, let* $t(x,y,z)$ *be a ternary term in the language of* $\mathbf{A}$*, and let* $\mathbf{F} = \mathbf{F}_{\mathbb{V}(\mathbf{A})}(x,y)$*. Consider the following statements:*

item:6' *(A')* $t^{\mathbf{A}}$ *is a difference term operation for* $\mathbf{A}$*.*

item:7’ *(B’) for all 2-generated* $\mathbf{B} \leqslant \mathbf{A}$, $t^{\mathbf{B}}$ *is a difference term operation for* $\mathbf{B}$*;*

item:8’ *(C’)* $t^{\mathbf{F}}$ *is a difference term operation for* $\mathbf{F}$*;*

Then (C’) $\Rightarrow$ *(B’)* $\Rightarrow$ *(A’).*

thm:F **Theorem 3.3.** *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:*

item:1010 *(i)* $\mathcal{V}$ *has a difference term;*

item:2 *(ii)* $\mathsf{HSP}(\mathbf{F})$ *has a difference term;*

item:3 *(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 and let $d(x, y, z)$ be an arbitrary ternary term in the language 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 $\mathbf{A}$. Then by Lemma 3.1, $d^{\mathbf{F}}(x, y, z)$ is not a difference term operation for $\mathbf{F}$. □

4. Local Difference Terms

l-diff-terms

In [19], 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.

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:

:diff-triple

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

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

eq:d-trip-i1

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

eq:d-trip-i2

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

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.

iff-terms **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

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

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,

eq:100000
$$d(a_0, b_0, b_0) = t(a_0, p(a_0, b_0, b_0), p(a_0, b_0, b_0))\ [\mathrm{Cg}(a_0, p(a_0, b_0, b_0))]\ a_0. \tag{4.4}$$

Note that the pair $(a_0, p(a_0, b_0, b_0))$ is equal to $(p(a_0, a_0, a_0), p(a_0, b_0, b_0))$ (by idempotence) and belongs to $\mathrm{Cg}(a_0, b_0)$, 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 indices. Observe,

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

The first equation holds by definition of d, the second because p is an idempotent local difference term for S', and the third 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,

eq:450000
$$d(a_j, b_j, b_j) = t(a_j, p(a_j, b_j, b_j), p(a_j, b_j, b_j)). \tag{4.5}$$

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 (4.5) 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

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

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

eq:40000

$$d(a_i, b_i, b_i) = t(p(a_i, b_i, b_i), p(b_i, b_i, b_i), b_i) = t(p(a_i, b_i, b_i), b_i, b_i). \tag{4.6}$$

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

eq:50000

$$t(p(a_i, b_i, b_i), b_i, b_i)\ [\mathrm{Cg}(a_i, b_i)]\ t(a_i, b_i, b_i). \tag{4.7}$$

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. This plus (4.6) and (4.7) 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

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

as desired. □

oc-diff-term **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 $(a, b, 1)$. □

c:algor-1

4.1. Algorithm 1: existence of a difference term operation

r:algor-1

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 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, that the running time of subalgebra generation is polynomial has been known for a long time (see [11]). The time complexity of congruence generation is also known to be polynomial (see [6]). The only operation whose tractability might be called into question is the commutator, but we have a straight-forward algorithm for computing it that we describe in detail in Appendix Section A. □

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, 7].

5. Generalizations and Extensions

d-local-diff

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

-diff-triple

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

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.

l-diff-terms

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:

oc-diff-term

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 $\mathbf{A}_1$.*

ocal-diff

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 $a, b \in A$,

ff-triple

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

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

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).

iff-terms

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 B.2), since the argument is nearly identical to the one used to prove Theorem 4.1.

diff-term

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 B.3.

We now pause to fix some more notation. If $\alpha \in \mathrm{Con}(\mathbf{A})$ and $\beta \in \mathrm{Con}(\mathbf{B})$, then we let $\alpha * \beta$ denote the set of pairs $((a, b), (a', b')) \in (A \times B)^2$ satisfying $a\ \alpha\ a'$ and $b\ \beta\ b'$. The relation $\alpha * \beta$ is clearly a congruence of $\mathbf{A} \times \mathbf{B}$.

:products

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

eq:60002

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

eq:60003

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

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

eq:60004
eq:60005

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

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

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 2.6 implies[5]

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

Next, observe that $\mathrm{Cg}^{\mathbf{A}}(a, a') * \mathrm{Cg}^{\mathbf{B}}(b, b')$ 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

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

Therefore,

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

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.

roducts-conv

Question 1. 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 $\mathbf{B}$. Does it follow that $d^{\mathbf{A}\times\mathbf{B}}$ is a difference term operation for the product $\mathbf{A} \times \mathbf{B}$/

Fix (a, b) and (a', b') in $A \times B$. To answer Question 1 in the affirmative we must prove

eq:60000
eq:60001

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

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

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:

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

[5] 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 2.6. Recall, that π_A is defined on a congruence $\theta \in \mathrm{Con}(\mathbf{A}\times\mathbf{B})$ as follows: $\pi_A(\theta) = \{(a, a') \in A^2 \mid ((a, b), (a', b')) \in \theta \text{ for some } (b, b') \in B^2\}$.

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

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

Therefore, $(d^{\mathbf{A}}(a,a',a'), d^{\mathbf{B}}(b,b',b'))\ [\mathrm{Cg}^{\mathbf{A}}(a,a')] * [\mathrm{Cg}^{\mathbf{B}}(b,b')]\ (a,b)$. We claim that the latter is equal to $[\mathrm{Cg}^{\mathbf{A}}(a,a') * \mathrm{Cg}^{\mathbf{B}}(b,b')]$. 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

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

then we could complete the proof by showing that

eq:655
$$\mathrm{Cg}^{\mathbf{A}\times\mathbf{B}}((a,b),(a',b')) \geqslant \mathrm{Cg}^{\mathbf{A}}(a,a') * \mathrm{Cg}^{\mathbf{B}}(b,b'). \tag{5.10}$$

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

TODO: Prove Lemma **??** somehow!!!

c:algor-2

5.3. Algorithm 2: existence of a difference term

r:algor-2

Corollary 5.6. *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 3.3, 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 $\mathcal{A} = \{A_0, A_1, \dots, A_{n-1}\}$ and (as above) let $\mathcal{S}(\mathcal{A})$ denote all pairs (A,i) such that $\mathbf{A} = \langle A, \dots\rangle \in \mathcal{A}$ 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 **??**, 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 $\mathbf{F}$. □

Acknowledgments

The author would like to thank Ralph Freese for proposing this project and calling attention to the work of Valeriote and Willard. Other helpful suggestions came from Cliff Bergman and the following members of the *Hawaii Universal Algebra Seminar:* Alex Guillen, Tristan Holmes, Bill Lampe, and J. B. Nation. These contributions are gratefully acknowledged.

This work was partially supported by the National Science Foundation Grant No. 1500235.

A. An Easy Route to the Commutator

ude:-an-easy

For an algebra $\mathbf{A}$ with congruence relations α, $\beta \in \operatorname{Con}\mathbf{A}$, let $\boldsymbol{\beta}$ denote the subalgebra of $\mathbf{A} \times \mathbf{A}$ with universe β, and let 0_A denote the least equivalence relation on A. Thus, $0_A = \{(a, a) \mid a \in A\} \leqslant \beta$. Denote by D_α the following subset of $\beta \times \beta$:

eq:9009

$$D_\alpha = (\alpha * \alpha) \cap (0_A \times 0_A) = \{((a, a), (b, b)) \in (0_A \times 0_A) \mid a \; \alpha \; b\}. \tag{A.1}$$

Let $\Delta_{\beta,\alpha} = \operatorname{Cg}^{\boldsymbol{\beta}}(D_\alpha)$ denote the congruence relation of $\boldsymbol{\beta}$ generated by D_α. The condition $\mathsf{C}(\alpha, \beta; \gamma)$ holds iff for all $a \; \alpha \; b$, for all $u_i \; \beta \; v_i$ $(1 \leqslant i \leqslant n)$, and for all $t \in \operatorname{Pol}_{n+1}(\mathbf{A})$, we have $t(a, \mathbf{u}) \; \gamma \; t(a, \mathbf{v})$ iff $t(b, \mathbf{u}) \; \gamma \; t(b, \mathbf{v})$. There are a number of different ways to define a commutator. See, for example, [18, 9, 8, 4, 16, 17]. In this note, the commutator $[\alpha, \beta]$ is defined to be the least congruence γ such that $\mathsf{C}(\alpha, \beta; \gamma)$ holds.

We now describe an alternate way to express the commutator—specifically, it is the least fixed point of a certain closure operator. This description was inspired by the one that is mentioned in passing by Keith Kearnes in [14, p. 930]. Our objective here is to prove that the description we present is correct (i.e., describes the commutator) and to show that it leads to a simple, efficient procedure for computing the commutator.

Let $\operatorname{Tol}(A)$ denote the collection of all tolerances (reflexive symmetric relations) on the set A,[6] and let $\Psi_{\beta,\alpha}\colon \operatorname{Tol}(A) \to \operatorname{Tol}(A)$ be the function defined for each $T \in \operatorname{Tol}(A)$ follows:

eq:7

$$\Psi_{\beta,\alpha}(T) = \{(x, y) \in A \times A \mid (\exists\, (a, b) \in T)\, (a, b) \; \Delta_{\beta,\alpha} \; (x, y)\}, \tag{A.2}$$

where $\Delta_{\beta,\alpha} = \operatorname{Cg}^{\boldsymbol{\beta}}(D_\alpha)$ and $D_\alpha = (\alpha * \alpha) \cap (0_A \times 0_A)$ (as in (A.1)).

Remarks 1.

1. It's easy to see that $\Psi_{\beta,\alpha}(T)$ is reflexive and symmetric whenever T has these properties; similarly, $\Psi_{\beta,\alpha}(T)$ is compatible with the operations of $\mathbf{A}$ whenever T is. In other words $\Psi_{\beta,\alpha}$ maps tolerances of A ($\mathbf{A}$, resp.) to tolerances of A ($\mathbf{A}$, resp.).

[6] Actually, a *tolerance* of an algebra $\mathbf{A} = \langle A, \ldots\rangle$ is a reflexive symmetric subalgebra of $\mathbf{A} \times \mathbf{A}$. Therefore, the set of all tolerances of $\mathbf{A}$ forms an algebraic (hence complete) lattice. If we drop the operations and consider only the set A, then a tolerance relation on A is simply a reflexive symmetric binary relation.

2. Since $\Psi_{\beta,\alpha}$ is clearly a monotone increasing function on the complete lattice $\operatorname{Tol}(A)$, it is guaranteed to have a least fixed point—that is, there is a point $\tau \in \operatorname{Tol}(A)$ such that $\Psi_{\beta,\alpha}(\tau) = \tau$ and $\tau \leqslant T$, for every $T \in \operatorname{Tol}(A)$ satisfying $\Psi_{\beta,\alpha}(T) = T$.

3. Here are two ways the least fixed point of $\Psi_{\beta,\alpha}$ could be computed:

eq:4

$$\text{(A.3)} \quad \tau = \bigwedge \{T \in \operatorname{Tol}(A) \mid \Psi_{\beta,\alpha}(T) \leqslant T\} \quad \text{and} \quad \tau = \bigvee_{k \geqslant 0} \Psi^k_{\beta,\alpha}(0_A).$$

In Lemma A.1 we will show that the least fixed point of $\Psi_{\beta,\alpha}$ is, in fact, the commutator, $\tau = [\alpha, \beta]$, so either expression in (A.3) could potentially be used to compute it. However, Lemma A.1 also shows that $\Psi_{\beta,\alpha}$ is a closure operator; in particular, it is idempotent. Therefore, $\Psi^k_{\beta,\alpha}(0_A) = \Psi_{\beta,\alpha}(0_A)$ for all k, so we have the following simple description of the commutator:

$$\begin{aligned}[]
[\alpha, \beta] = \Psi_{\beta,\alpha}(0_A) &= \{(x, y) \in A \times A \mid (\exists\, (a, b) \in 0_A)\, (a, b)\ \Delta_{\beta,\alpha}\ (x, y)\} \\
&= \{(x, y) \in A \times A \mid (\exists a \in A)\, (a, a)\ \Delta_{\beta,\alpha}\ (x, y)\}.
\end{aligned}$$

A.1. Fixed Point Lemma

oint-comm

Lemma. *If α, $\beta \in \operatorname{Con}(\mathbf{A})$ and if $\Psi_{\beta,\alpha}$ is defined by (A.2), then*

(i) $\Psi_{\beta,\alpha}$ *is a closure operator on* $\operatorname{Tol}(A)$*;*

(ii) $[\alpha, \beta]$ *is the least fixed point of* $\Psi_{\beta,\alpha}$.

Proof.

(i) To prove (i) we verify that $\Psi_{\beta,\alpha}$ has the three properties that define a closure operator—namely for all T, $T' \in \operatorname{Tol}(A)$,

item:c1 (c.1) $T \leqslant \Psi_{\beta,\alpha}(T)$;

item:c2 (c.2) $T \leqslant T' \Rightarrow \Psi_{\beta,\alpha}(T) \leqslant \Psi_{\beta,\alpha}(T')$;

item:c3 (c.3) $\Psi_{\beta,\alpha}(\Psi_{\beta,\alpha}(T)) = \Psi_{\beta,\alpha}(T)$.

Proof of (c.1): $(a, b) \in T$ implies $(a, b) \in \Psi_{\beta,\alpha}(T)$ because $(a, b)\ \Delta_{\beta,\alpha}\ (a, b)$.

Proof of (c.2): $(x, y) \in \Psi_{\beta,\alpha}(T)$ iff there exists $(a, b) \in T \leqslant T'$ such that $(a, b)\ \Delta_{\beta,\alpha}\ (x, y)$; this and $(a, b) \in T'$ implies $(x, y) \in \Psi_{\beta,\alpha}(T')$.

Proof of (c.3): $(x, y) \in \Psi_{\beta,\alpha}(\Psi_{\beta,\alpha}(T))$ if and only if there exists $(a, b) \in \Psi_{\beta,\alpha}(T)$ such that $(a, b)\ \Delta_{\beta,\alpha}\ (x, y)$, and $(a, b) \in \Psi_{\beta,\alpha}(T)$ is in turn equivalent to the existence of $(c, d) \in T$ such that $(c, d)\ \Delta_{\beta,\alpha}\ (a, b)$. By transitivity of $\Delta_{\beta,\alpha}$, we have that $(c, d)\ \Delta_{\beta,\alpha}\ (a, b)\ \Delta_{\beta,\alpha}\ (x, y)$ implies $(c, d)\ \Delta_{\beta,\alpha}\ (x, y)$, proving that there exists $(c, d) \in T$ such that $(c, d)\ \Delta_{\beta,\alpha}\ (x, y)$; equivalently, $(x, y) \in T$.

(ii) As remarked above, from part (i) follows $\Psi^k_{\beta,\alpha}(0_A) = \Psi_{\beta,\alpha}(0_A)$ for all k, so the least fixed point of $\Psi_{\beta,\alpha}$ that appears in the formula on the right in (A.3) reduces to $\tau = \Psi_{\beta,\alpha}(0_A)$. Therefore, to complete the proof it suffices to show $[\alpha,\beta] = \Psi_{\beta,\alpha}(0_A)$.

We first prove $[\alpha,\beta] \leqslant \Psi_{\beta,\alpha}(0_A)$. Since $[\alpha,\beta]$ is the least congruence γ satisfying $\mathsf{C}(\alpha,\beta;\gamma)$, it suffices to prove $\mathsf{C}(\alpha,\beta;\Psi_{\beta,\alpha}(0_A))$ holds. Suppose $a\ \alpha\ a'$ and $b_i\ \beta\ b_i'$ and $t^{\mathbf{A}} \in \mathrm{Pol}_{k+1}(\mathbf{A})$ satisfy $t^{\mathbf{A}}(a,\mathbf{b})\ \Psi_{\beta,\alpha}(0_A)\ t^{\mathbf{A}}(a,\mathbf{b}')$, where $\mathbf{b} = (b_1,\dots,b_k)$ and $\mathbf{b}' = (b_1',\dots,b_k')$. We must show $t(a',\mathbf{b})\ \Psi_{\beta,\alpha}(0_A)\ t(a',\mathbf{b}')$. The antecedent $t^{\mathbf{A}}(a,\mathbf{b})\ \Psi_{\beta,\alpha}(0_A)\ t^{\mathbf{A}}(a,\mathbf{b}')$ is equivalent to $(\exists\, c \in A)\ (c,c)\ \Delta_{\beta,\alpha}\ (t^{\mathbf{A}}(a,\mathbf{b}), t^{\mathbf{A}}(a,\mathbf{b}'))$. Now

$$(t^{\mathbf{A}}(a,\mathbf{b}), t^{\mathbf{A}}(a,\mathbf{b}')) = t^{\boldsymbol{\beta}}((a,a),(b_1,b_1'),\dots,(b_k,b_k')),$$

and since $a\ \alpha\ a'$, we have

$$t^{\boldsymbol{\beta}}((a,a),(b_1,b_1'),\dots,(b_k,b_k'))\ \Delta_{\beta,\alpha}\ t^{\boldsymbol{\beta}}((a',a'),(b_1,b_1'),\dots,(b_k,b_k')).$$

The latter is equal to $(t^{\mathbf{A}}(a',\mathbf{b}), t^{\mathbf{A}}(a',\mathbf{b}'))$, and it follows by transitivity of $\Delta_{\beta,\alpha}$ that $(c,c)\ \Delta_{\beta,\alpha}\ (t^{\mathbf{A}}(a',\mathbf{b}), t^{\mathbf{A}}(a',\mathbf{b}'))$. Therefore, $t(a',\mathbf{b})\ \Psi_{\beta,\alpha}(0_A)\ t(a',\mathbf{b}')$, as desired.

We now prove $\Psi_{\beta,\alpha}(0_A) \leqslant [\alpha,\beta]$. If $(x,y) \in \Psi_{\beta,\alpha}(0_A)$ then there exists $a \in A$ such that

eq:1100

$$(a,a)\ \Delta_{\beta,\alpha}\ (x,y). \tag{A.4}$$

From the definition of $\Delta_{\beta,\alpha}$ and Mal'tsev's congruence generation theorem, (A.4) holds if and only if for there exist $(z_i,z_i') \in \beta$ $(0 \leqslant i \leqslant n+1)$, and $(u_i,v_i) \in \alpha$, $f_i \in \mathrm{Pol}_1(\boldsymbol{\beta})$ $(0 \leqslant i \leqslant n)$, such that $(a,a) = (z_0,z_0')$ and $(x,y) = (z_{n+1},z_{n+1}')$ hold, and so do the following equations of sets:

eq:001

eq:011

$$\{(a,a),(z_1,z_1')\} = \{f_0(u_0,u_0), f_0(v_0,v_0)\}, \tag{A.5}$$

$$\{(z_1,z_1'),(z_2,z_2')\} = \{f_1(u_1,u_1), f_1(v_1,v_1)\}, \tag{A.6}$$

$$\vdots$$

$$\{(z_n,z_n'),(x,y)\} = \{f_n(u_n,u_n), f_n(v_n,v_n)\}.$$

Now $f_i \in \mathrm{Pol}_1(\boldsymbol{\beta})$ for all i, so

$$f_i(c,c') = g_i^{\boldsymbol{\beta}}((c,c'),(b_1,b_1'),\dots,(b_k,b_k')) = (g_i^{\mathbf{A}}(c,\mathbf{b}), g_i^{\mathbf{A}}(c',\mathbf{b}')),$$

for some k, some $(k+1)$-ary term g_i, and some constant tuples $\mathbf{b} = (b_1,\dots,b_k)$ and $\mathbf{b}' = (b_1',\dots,b_k')$ satisfying $b_i\ \beta\ b_i'$ $(1 \leqslant i \leqslant k)$. By (A.5), either

$$(a,a) = \big(g_0(u_0,\mathbf{b}), g_0(u_0,\mathbf{b}')\big) \quad \text{and} \quad (z_1,z_1') = \big(g_0(v_0,\mathbf{b}), g_0(v_0,\mathbf{b}')\big),$$

or vice-versa. We assumed $u_0\ \alpha\ v_0$ and $b_i\ \beta\ b_i'$ $(1 \leqslant i \leqslant k)$, so the α,β-term condition entails $g_0(u_0,\mathbf{a})\ [\alpha,\beta]\ g_0(u_0,\mathbf{a}')$ iff $g_0(v_0,\mathbf{a})\ [\alpha,\beta]$

$g_0(v_0, \mathbf{a}')$. From this and (A.5) we deduce that $(a, a) \in [\alpha, \beta]$ iff $(z_1, z_1') \in [\alpha, \beta]$. Similarly (A.6) and $u_1 \ \alpha \ v_1$ imply $(z_1, z_1') \in [\alpha, \beta]$ iff $(z_2, z_2') \in [\alpha, \beta]$. Inductively, and by transitivity of $[\alpha, \beta]$, we conclude $(a, a) \in [\alpha, \beta]$ iff $(x, y) \in [\alpha, \beta]$. Since $(a, a) \in [\alpha, \beta]$, we have $(x, y) \in [\alpha, \beta]$, as desired.

□

A.2. Computing the Commutator

As a consequence of the description of the commutator given in the last section, we now have the following simple method for computing it.

Input A finite algebra $\mathbf{A} = \langle A, \dots \rangle$ and two congruences α, $\beta \in \operatorname{Con} \mathbf{A}$.

Procedure

- **Step 1** Compute the congruence relation

$$\Delta_{\beta,\alpha} = \mathrm{Cg}^{\boldsymbol{\beta}}\big\{((a, a), (b, b)) \mid a \ \alpha \ b\big\}.$$

- **Step 2** Compute the commutator

$$[\alpha, \beta] = \big\{(x, y) \in A \times A \mid (\exists a \in A)\, (a, a) \ \Delta_{\beta,\alpha} \ (x, y)\big\} = \bigcup_{a \in A} (a, a)/\Delta_{\beta,\alpha}$$

Note that $\Delta_{\beta,\alpha}$ is a subalgebra of $\mathbf{A}^2 \times \mathbf{A}^2$ and such a congruence can be computed in polynomial-time in the size of $\mathbf{A}$. (See [6].)

B. Proofs

ec:proofs

B.1. Proof of Lemmas 2.3 and 2.4

tone-comm

Lemma (Monotonicity of the Commutator)**.** *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*

$$\big[\bigwedge \alpha_i, \bigwedge \beta_i\big] \leqslant \bigwedge [\alpha_i, \beta_i] \quad \textit{and} \quad \bigvee [\alpha_i, \beta_i] \leqslant \big[\bigvee \alpha_i, \bigvee \beta_i\big].$$

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

oof-thm:glob

B.2. Proof of Theorem 5.3

Theorem. *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.*

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 $S = ((A_0, \chi_0), (A_1, \chi_1), \dots, (A_n, \chi_n)) \in \mathcal{S}(\mathcal{A})^{n+1}$. 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 $S' = ((A_1, \chi_1), \dots, (A_n, \chi_n))$ 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

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

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

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

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 $(A_0, 0)$,

eq:100100

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

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 (B.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

$$d(a, a, b) = t(a, p(a, a, a), p(a, a, b)) = t(a, a, b) = b.$$

The first equation holds by definition of d, the second because p is an idempotent local difference term for S', and the third 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,

eq:451
$$d(a, b, b) = t(a, p(a, b, b), p(a, b, b)). \tag{B.2}$$

Also, $p(a, b, b)$ $[\mathrm{Cg}(a, b)]$ a, since p is a local difference term for S'. This and (B.2) 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.

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

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

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,

eq:444
$$d(a, b, b) = t(p(a, b, b), p(b, b, b), b) = t(p(a, b, b), b, b). \tag{B.3}$$

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

eq:555
$$t(p(a, b, b), b, b)\ [\mathrm{Cg}(a, b)]\ t(a, b, b). \tag{B.4}$$

Finally, since t is a local difference term for T, hence for $(A_i, 0)$ $(1 \leqslant i \leqslant k)$, we have $t(a, b, b)$ $[\mathrm{Cg}(a, b)]$ a. This, (B.3), and (B.4) yield $d(a, b, b)$ $[\mathrm{Cg}(a, b)]$ 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 $d(a, a, b) = t(p(a, a, b), p(a, a, b), b) = t(b, b, b) = b$. □

oof-cor:glob

B.3. Proof of Corollary 5.4

Corollary. *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.*

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 $(A,1)$. □

References

MR2839398 [1] Clifford Bergman. *Universal algebra*, volume 301 of *Pure and Applied Mathematics (Boca Raton)*. CRC Press, Boca Raton, FL, 2012. Fundamentals and selected topics.

MR1695293 [2] 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`.

MR1871085 [3] 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`.

MR1145556 [4] A. Day and H. P. Gumm. Some characterizations of the commutator. *Algebra Universalis*, 29(1):61–78, 1992. URL: `http://dx.doi.org/10.1007/BF01190756`, `doi:10.1007/BF01190756`.

Meo:2017-ext [5] William DeMeo. On the complexity of difference term existence. 2017. This is a place-holder to be used after posting long version on arXiv. URL: `https://github.com/UniversalAlgebra/diff-term-existence`.

MR2470585 [6] 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`.

Freese:2009 [7] 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`.

MR590312 [8] H.-Peter Gumm. An easy way to the commutator in modular varieties. *Arch. Math. (Basel)*, 34(3):220–228, 1980. URL: `http://dx.doi.org/10.1007/BF01224955`, `doi:10.1007/BF01224955`.

MR541622 [9] Joachim Hagemann and Christian Herrmann. A concrete ideal multiplication for algebraic systems and its relation to congruence distributivity. *Arch. Math. (Basel)*, 32(3):234–245, 1979. URL: `http://dx.doi.org/10.1007/BF01238496`, `doi:10.1007/BF01238496`.

HM:1988 [10] 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.

MR0455543 [11] 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`.

KSW [12] Keith Kearnes, Ágnes Szendrei, and Ross Willard. Simpler maltsev conditions for (weak) difference terms in locally finite varieties. to appear.

MR3449235 [13] 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`.

MR1358491 [14] 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`.

MR3076179 [15] 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`.

MR1663558 [16] 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`.

MR1257643 [17] Paolo Lipparini. Commutator theory without join-distributivity. *Trans. Amer. Math. Soc.*, 346(1):177–202, 1994. URL: `http://dx.doi.org/10.2307/2154948`, `doi:10.2307/2154948`.

MR0432511 [18] Jonathan D. H. Smith. *Mal′cev varieties*. Lecture Notes in Mathematics, Vol. 554. Springer-Verlag, Berlin-New York, 1976.

MR3239624 [19] 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`.