NOTES ON COMPLEXITY OF DECIDING EXISTENCE OF DIFFERENCE TERMS AND SEMILATTICE TERMS

DEMEO, FREESE, GUILLEN, HOLMES, LAMPE, AND NATION

Abstract. We consider the following practical question: given a finite algebra A in a finite language, can we efficiently decide whether the variety generated by A has a difference term? To help address this question we review some useful definitions and known facts about difference terms, prove some new results, and then discuss algorithms that exploit these result.

1. Introduction

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

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

where θ is any congruence containing (a, b) and $[\cdot, \cdot]$ denotes the *commutator* (see Section 2.1). 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 general algebra literature. (See, for example, [Kea95, KS98, KK13, KSW, KSW16].) There are many reasons to study difference terms, but one obvious reason is because if we know that a variety has a difference term, this fact allows us to deduce many useful properties of the algebras inhabiting that variety. Very roughly speaking, having a difference term is slightly stronger than having a Taylor term and slightly weaker than having a Mal'cev term. (Note that if $\mathbf{A}$ is an *abelian* algebra, which means that $[1_A, 1_A] = 0_A$, then, by the monotonicity of the commutator, $[\theta, \theta] = 0_A$ for all $\theta \in \operatorname{Con} \mathbf{A}$, 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, over the last three decades, researchers have found ingenious ways to get computers to solve challenging abstract decision problems—such as whether a variety is congruence n-permutable ([VW14]), or congruence modular ([FV09])—and to do so very quickly. This paper contributes to this effort by finding an efficient algorithm for deciding whether a locally finite idempotent variety has a difference term.

The central question motivating this project is the following:

Date: January 11, 2017.

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

Kearnes proved in [Kea95] that $\mathbf{A}$ has a difference term iff $\mathbb{V}(\mathbf{A})$ has a Taylor term and no type-2 tails (equivalently, $\mathbb{V}(\mathbf{A})$ has no 1's and no type-2 tails). No 1's is poly-time decidable by Valeriote's subtype theorem. In [FV09], Freese and Valeriote solved an analogous problem, by giving a positive answer to the following

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

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

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

Here is a related problem.

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

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

2. Background, definitions, and notation

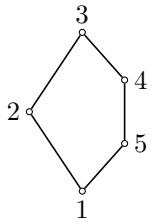
Our starting point is the set of lemmas at the beginning of Section 3 in the Freese-Valeriote paper [FV09]. We first review some of the basic tame congruence theory (TCT) that comes up in the proofs in that paper. (In fact, most of this section is copied from the nice presentation of TCT background that appears in [FV09, Sec. 2].)

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

(1) unary algebra whose basic operations are all permutations (unary type);

(2) one-dimensional vector space over some finite field (affine type);
(3) 2-element boolean algebra (boolean type);
(4) 2-element lattice (lattice type);
(5) 2-element semilattice (semilattice type).

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



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

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

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

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

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

In Section 3, the following result will be useful.

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

TABLE 1. [KKVW15].

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

2.1. **The centralizer, term condition, and abelian congruences.** We review some useful properties of centralizers and abelian algebras. In our previous work nonabelian algebras played the following role (see, e.g., [BD16]): a theorem would begin with the assumption that a particular algebra $\mathbf{A}$ is nonabelian and then proceed to show that if the result to be proved were false, then $\mathbf{A}$ would have to be abelian. Such arguments employ some basic facts about abelian algebras that we now review.

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

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

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

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

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

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

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

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

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

T is called *abelian* if $[T,T] = 0_A$. An algebra $\mathbf{A}$ is called *abelian* if 1_A is abelian (i.e., $[1_A, 1_A] = 0_A$).

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

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

It is sometimes useful to iterate the commutator, for example, $[[\alpha,\alpha],[\alpha,\alpha]]$, and for this purpose we define $[\alpha]^n$ recursively as follows: $[\alpha]^0 = \alpha$ and $[\alpha]^{n+1} = [[\alpha]^n, [\alpha]^n]$. A congruence α of $\mathbf{A}$ is called *solvable* if $[\alpha]^n = 0_A$ for some n.

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

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

The next two lemmas turn out to be very useful. The first identifies special conditions under which certain quotient congruences are abelian. The second gives fairly general conditions under which quotients of abelian congruences are abelian.

Lemma 2.4. *Let α_0, α_1, β be congruences of $\mathbf{A}$ and suppose $\alpha_0 \wedge \beta = \delta = \alpha_1 \wedge \beta$. Then $\mathsf{C}(\alpha_0 \vee \alpha_1, \beta; \delta)$. If, in addition, $\beta \leqslant \alpha_0 \vee \alpha_1$, then $\mathsf{C}(\beta, \beta; \delta)$, so β/δ is an abelian congruence of $\mathbf{A}/\delta$.*

Lemma 2.4 is an easy consequence of items (1), (3), (4), and (7) of Lemma 2.3.

Lemma 2.5. *Let $\mathcal{V}$ be a locally finite variety with a Taylor term and let $\mathbf{A} \in \mathcal{V}$. Then $\mathsf{C}(\beta, \beta; \gamma)$ for all $[\beta, \beta] \leqslant \gamma$.*

Lemma 2.5 can be proved by combining the next result, of David Hobby and Ralph McKenzie, with a result of Keith Kearnes and Emil Kiss.

Lemma 2.6 (cf. [HM88, Thm 7.12])**.** *A locally finite variety $\mathcal{V}$ has a Taylor term if and only if it has a so called weak difference term; that is, a term $d(x, y, z)$ satisfying the following conditions for all $\mathbf{A} \in \mathcal{V}$, all $a, b \in A$, and all $\beta \in \mathrm{Con}(\mathbf{A})$: $d^{\mathbf{A}}(a, a, b)$ $[\beta, \beta]$ b $[\beta, \beta]$ $d^{\mathbf{A}}(b, a, a)$, where $\beta = \mathrm{Cg}^{\mathbf{A}}(a, b)$.*

Lemma 2.7 ([KK13, Lem 6.8])**.** *If $\mathbf{A}$ belongs to a variety with a weak difference term and if β and γ are congruences of $\mathbf{A}$ satisfying $[\beta, \beta] \leqslant \gamma$, then $\mathsf{C}(\beta, \beta; \gamma)$.*

Remark. It follows immediately from Lemma 2.5 that in a locally finite Taylor variety, $\mathcal{V}$, quotients of abelian algebras are abelian, so the abelian members of $\mathcal{V}$ form a subvariety. But this can also be derived from Lemma 2.6, since $[\beta, \beta] = 0_A$ implies $d^{\mathbf{A}}$ is a Mal'tsev term operation on the blocks of β, so if $\mathbf{A}$ is abelian—i.e., if $\mathsf{C}(1_A, 1_A; 0_A)$—then Lemma 2.6, implies that $\mathbf{A}$ has a Mal'tsev term operation. It then follows that homomorphic images of $\mathbf{A}$ are abelian. (See [Ber12, Cor 7.28] for more details).

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

Lemma 2.8. *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 $\delta \in \mathrm{Con}\,\mathbf{A}$, $\mathsf{C}(\alpha', \beta'; \delta)$ 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 2.9. *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 2.8, $[\bigwedge \alpha_i, \bigwedge \beta_i] \leqslant [\alpha_i, \beta_i] \leqslant [\bigvee \alpha_i, \bigvee \beta_i]$, for all $i \in I$. □

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

Corollary 2.10. Let $\mathbf{A}$ be an algebra with congruences α, β, γ, δ. Then,

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

Lemma 2.11 ([Kea95, Theorem 2.10])**.** *Let $\mathbf{A}$ and $\mathbf{B}$ be algebras of the same signature and suppose $\phi : \mathbf{A} \to \mathbf{B}$ is a surjective homomorphism. If $\alpha, \beta \in \mathrm{Con}\,\mathbf{A}$, 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 $\rho, \sigma \in \mathrm{Con}\,\mathbf{B}$, then

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

2.3. **Necessary conditions for existence of difference terms.** In this subsection we recall some well known results about varieties that have difference terms.

Lemma 2.12 ([Kea95, Lemma 2.2]). *If $\mathcal{V}$ has a difference term, $\mathbf{A} \in \mathcal{V}$ and $\alpha, \beta \in \operatorname{Con}\mathbf{A}$, then $[\alpha, \beta] = [\beta, \alpha]$.*

Lemma 2.13 ([Kea95, Lemma 2.8]). *If $\mathcal{V}$ has a difference term, $\mathbf{A} \in \mathcal{V}$ and $\alpha_i \in \operatorname{Con}\mathbf{A}$ for $i \in I$, then*

$$\bigvee [\alpha_i, \alpha_i] = [\bigvee \alpha_i, \bigvee \alpha_i] \, .$$

Questions: Does the analog of Lemma 2.13 hold for complete meets? Does Lemma 2.13 hold for "mixed congruences?" That is, assuming also that $\beta_i \in \operatorname{Con}\mathbf{A}$, do we have

$$\bigvee [\alpha_i, \beta_i] = [\bigvee \alpha_i, \bigvee \beta_i] \, ?$$

Lemma 2.14 ([Kea95, Lemma 2.9]). *Assume $\mathcal{V}$ has a difference term d, that $\mathbf{A} \in \mathcal{V}$ and $\alpha \in \operatorname{Con}\mathbf{A}$. Then $[\alpha, \alpha] = 0_A$ iff*

(i) $d(b, b, a) = d(a, b, b) = a$ for all $(a, b) \in \alpha$ and
(ii) $d : \mathbf{A} \times_\alpha \mathbf{A} \times_\alpha \mathbf{A} \to \mathbf{A}$ is a homomorphism.

If α and β are congruences of $\mathbf{A}$, then we write $\alpha \overset{s}{\sim} \beta$ and say that α and β are *solvably related* if $[\alpha \vee \beta]^n \leqslant \alpha \wedge \beta$ for some n. For varieties with a difference term our definition of "solvably related" means that $\alpha \overset{s}{\sim} \beta$ iff $(\alpha \vee \beta)/(\alpha \wedge \beta)$ is a solvable congruence of $A/(\alpha \wedge \beta)$. (See [Kea95, Section 3].)

Lemma 2.15 ([Kea95, Lemma 3.2]). *Assume $\mathcal{V}$ has a difference term and $\mathbf{A} \in \mathcal{V}$. Then,*

(i) $\overset{s}{\sim}$ is a congruence of $\operatorname{Con}\mathbf{A}$.
(ii) if $\delta \leqslant \alpha, \beta$ then $\alpha \overset{s}{\sim} \beta$ iff $\alpha/\delta \overset{s}{\sim} \beta/\delta$ in $\operatorname{Con}\mathbf{A}/\delta$.
(iii) $\overset{s}{\sim}$-classes are convex sublattices of permuting congruences.
(iv) $\operatorname{Con}\mathbf{A}/\overset{s}{\sim}$ is meet-semidistributive.

Lemma 2.15 (ii) says that $\overset{s}{\sim}$ is preserved under homomorphisms.

Call a congruence $\alpha \in \operatorname{Con}\mathbf{A}$ *neutral relative to* δ if $[\alpha, \alpha]_\delta = \alpha$. (Recall $[\alpha, \alpha]_\delta$ denotes the smallest congruence $\theta \geqslant \delta$ such that $\mathsf{C}(\alpha, \alpha; \theta)$.) Call an interval $[\![\delta, \theta]\!]$ in a congruence lattice a *neutral interval* if every $\alpha \in [\![\delta, \theta]\!]$ is neutral relative to δ. This is equivalent to asserting that $[\alpha, \beta]_\delta = \alpha \wedge \beta$ holds for all $\alpha, \beta \in [\![\delta, \theta]\!]$. In particular, if α, β are solvably related congruences in a neutral interval then $\alpha = \beta$.

We write $\alpha \overset{n}{\sim} \beta$ and say that α and β are *neutrally related* if the interval $[\![\alpha \wedge \beta, \alpha \vee \beta]\!]$ is neutral.

Lemma 2.16 ([Kea95, Lemma 3.6]). *Assume that $\mathcal{V}$ has a difference term and $\mathbf{A} \in \mathcal{V}$. Then*

(i) $\overset{n}{\sim}$ *is a congruence of* $\operatorname{Con}\mathbf{A}$.
(ii) If $\delta \leqslant \alpha, \beta$, *then* $\alpha \overset{n}{\sim} \beta$ *iff* $\alpha/\delta \overset{n}{\sim} \beta/\delta$ *in* $\operatorname{Con}\mathbf{A}/\delta$.
(iii) $\overset{n}{\sim}$*-classes are convex, meet-semidistributive sublattices.*
(iv) $\operatorname{Con}\mathbf{A}/\overset{n}{\sim}$ *is modular.*

Hence $\operatorname{Con}\mathbf{A}$ *is a subdirect product of of a modular lattice and a meet-semidistributive lattice.*

2.4. **Equivalent conditions for existence of a difference term.** In this subsection we give an improved version of a well known result (Theorem 2.17).

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

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

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

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

Theorem 2.17. *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) ⇒ (ii) ⇒ (iii) are obvious. We prove (iii) ⇒ (i) by contraposition. Suppose $\mathcal{V}$ has no difference term. (We show $\mathbf{F}$ has no difference term operation.) Let $d(x, y, z)$ be a ternary term of $\mathcal{V}$. Let $\mathbf{A} \in \mathcal{V}$ be such that $d^{\mathbf{A}}(x, y, z)$ is not a difference term operation in $\mathbf{A}$. Choose $a, b \in A$ witnessing this fact. Then either

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

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

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

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 $\mathbf{B}$, it follows that $d^{\mathbf{F}}(x, y, z)$ cannot be a difference term operation for $\mathbf{F}$. Finally, recall that $d(x, y, z)$ was an arbitrary ternary term of $\mathcal{V}$, so $\mathbf{F}$ has no difference term operation whatsoever. $\square$

3. The Freese-Valeriote Lemmas Revisited

In [FV09], Corollary 2.2 is the starting point of the development of a polynomial-time algorithm that determines if a given finite idempotent algebra generates a CM variety.

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

It follows from Corollary 2.2 and Proposition 2.1 that if $\mathbf{A}$ is idempotent then one can test the first condition, on omitting types 1 and 5 (or 1, 2, and 5) by searching for a 2-generated subalgebra of $\mathbf{A}$ whose typeset is not contained in $\{2,3,4\}$ ($\{3,4\}$). It is proved in [FV09, Sec. 6] that this test can be performed in polynomial time—that is, the running time of the test is bounded by a polynomial function of the size of $\mathbf{A}$. In [FV09, Sec. 3], Freese and Valeriote prove a sequence of lemmas to establish that, if $\mathbf{A}$ is finite and idempotent, and if $\mathcal{V} = \mathbb{V}(\mathbf{A})$ omits types 1 and 5, then to test for the existence of tails in $\mathcal{V}$ it suffices to look for them in the 3-generated subalgebras of $\mathbf{A}^2$. In other words, either there are no non-empty tails or else there are non-empty tails that are easy to find (since they occur in 3-generated subalgebras of $\mathbf{A}^2$). It follows that Problem 2 has a positive answer: deciding whether or not a finite idempotent algebra generates a congruence modular variety is tractable.[1]

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

Throughout, we let $\underline{n}$ denote the set $\{0,1,\dots,n-1\}$ and (at least for the rest of this section) we let $\mathcal{S}$ be a finite set of finite, similar, idempotent algebras, closed under the taking of subalgebras, such that $\mathcal{V} = \mathbb{V}(\mathcal{S})$ omits 1 (but may include type 5). We will suppose that some finite algebra $\mathbf{B}$ in $\mathcal{V}$ has a prime quotient whose minimal sets have non-empty *type-2* tails and show that there is a 3-generated subalgebra of the product of two members of $\mathcal{S}$ with this property.

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

Since $\mathcal{S}$ is closed under the taking of subalgebras, we may assume that the algebra $\mathbf{B}$ from the previous paragraph is a subdirect product of a finite number of members of $\mathcal{S}$. Choose n minimal such that for some $\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_{n-1}$ in $\mathcal{S}$, there is a subdirect product $\mathbf{B} \leqslant_{\text{sd}} \prod_{\underline{n}} \mathbf{A}_i$ that has a prime quotient with non-empty type-2 tails. Under the assumption that $n > 1$ we will attempt to prove that $n = 2$.

For this n, select the $\mathbf{A}_i$ and $\mathbf{B}$ so that $|B|$ is as small as possible. Let $\alpha \prec \beta$ be a prime quotient of $\mathbf{B}$ with non-empty type-2 tails and choose β minimal with this property. Let U be an (α, β)-minimal set and let N be an (α, β)-trace of U. Let 0 and 1 be two distinct members of N with $(0, 1) \notin \alpha$.

Lemma 3.1 (Lem. 3.1 [FV09])**.** *Let t be a member of the tail of U. Then β is the congruence of $\mathbf{B}$ generated by the pair $(0, 1)$ and $\mathbf{B}$ is generated by $\{0, 1, t\}$.*

It seems the proof of [FV09, Lem. 3.1] goes through with only minor adjustments.

Proof. **TODO:** fill in proof of Lemma 3.1. □

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

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

Consequently,

$$\rho_{\underline{n}} = \bigwedge_{j \in \underline{n}} \rho_j = 0_B \quad \text{and} \quad \bigvee_{j \in \underline{n}} \rho_j = 1_B. \tag{3.1}$$

By minimality of n we know that the intersection of any proper subset of the ρ_i, $1 \leqslant i \leqslant n$ is strictly above 0_B. Thus, $0_B < \rho_\sigma < 1_B$ for all $\emptyset \subset \sigma \subset \underline{n}$. (N.B., $\subset$ means *proper* subset.)

wjd: I don't
why join in
is 1_B... it's
probably wr

Lemma 3.2 (Lem. 3.2 [FV09])**.** *If $\sigma \subset \underline{n}$, then either $\beta \leqslant \rho_\sigma$ or $\alpha \vee \rho_\sigma = 1_B$.*

Proof. **TODO:** fill in proof of Lemma 3.2. □

Lemma 3.3 (Lem. 3.3 [FV09])**.** *$\alpha \vee \rho_i < 1_B$ for at least one i and $\alpha \vee \rho_j = 1_B$ for at least one j.*

Proof. **TODO:** fill in proof of Lemma 3.3. □

Theorem 3.4 (Thm. 3.4 [FV09])**.** *Let $\mathcal{V}$ be the variety generated by some finite set $\mathcal{S}$ of finite, idempotent algebras that is closed under taking subalgebras. If $\mathcal{V}$ omits type 1 ~~and 5~~ and some finite member of $\mathcal{V}$ has a prime quotient whose minimal sets have non-empty type-2 tails then there is some 3-generated algebra B with this property that belongs to $\mathcal{S}$ or is a subdirect product of two algebras from $\mathcal{S}$.*

Proof. **TODO:** fill in proof of Theorem 3.4. □

4. Local difference terms

In [VW14], Valeriote and Willard define a "local Hagemann-Mitschke sequence" which they use as the basis of an efficient algorithm for deciding for a given n whether an idempotent variety is n-permutable. Inspired by that work, we devise a similar construct, called a "local difference term," that we use to develop a polynomial-time algorithm for deciding the existence of a (global) difference term operation.

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

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

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

If p satisfies (4.1) for all triples in some subset $S \subseteq A \times A \times \{0, 1\}$, then we call p a *local difference term for* S.

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

$$a_i \ [\theta(a_i, b_i), \theta(a_i, b_i)] \ p(a_i, b_i, b_i), \ \text{ if } \chi_i = 0, \text{ and} \tag{4.2}$$

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

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 p 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.

Theorem 4.1 (cf. [VW14, Theorem 2.2])**.** *Let $\mathcal{V}$ be an idempotent variety and $\mathbf{A} \in \mathcal{V}$. Define $\mathcal{S} = A \times A \times \{0, 1\}$ and suppose that every pair $((a_0, b_0, \chi_0), (a_1, b_1, \chi_1)) \in \mathcal{S}^2$ has a local difference term. Then every subset $S \subseteq \mathcal{S}$, has a local difference term.*

Proof. The proof is by induction on the size of S. In the base case, $|S| = 2$, the claim holds by assumption. Fix $n > 2$ and assume that every subset of $\mathcal{S}$ of size $2 \leqslant k \leqslant n$ has a local difference term. Let $S = \{(a_0, b_0, \chi_0), (a_1, b_1, \chi_1), \ldots, (a_n, b_n, \chi_n)\} \subseteq \mathcal{S}$, so that $|S| = n + 1$. We prove S has a local difference term.

Since $|S| \geqslant 3$ and $\chi_i \in \{0, 1\}$ for all i, there must exist indices $i \neq j$ such that $\chi_i = \chi_j$. Assume without loss of generality that one of these indices is $j = 0$. Define the set $S' =$

$S \setminus \{(a_0, b_0, \chi_0)\}$. Since $|S'| < |S|$, the set S' has a local difference term p. We split the remainder of the proof into two cases. In the first case $\chi_0 = 0$ and in the second $\chi_0 = 1$.

Case 1: $\chi_0 = 0$. Without loss of generality, suppose that $\chi_1 = \cdots = \chi_k = 1$, and $\chi_{k+1} = \cdots = \chi_n = 0$. Define $T = \{(a_0, p(a_0, b_0, b_0), 0), (a_1, b_1, 1), (a_2, b_2, 1), \ldots, (a_k, b_k, 1)\}$, and note that $|T| < |S|$. Let t be a local difference term for T. Define

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

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

$$d(a_0, b_0, b_0) = t(a_0, p(a_0, b_0, b_0), p(a_0, b_0, b_0))\ [\tau, \tau]\ a_0, \tag{4.4}$$

where we have used τ to denote $\theta(a_0, p(a_0, b_0, b_0))$. Note that $(a_0, p(a_0, b_0, b_0))$ is equal to $(p(a_0, a_0, a_0), p(a_0, b_0, b_0))$ which belongs to $\theta(a_0, b_0)$, so $\tau \leqslant \theta(a_0, b_0)$. Therefore, by monotonicity of the commutator, $[\tau, \tau] \leqslant [\theta(a_0, b_0), \theta(a_0, b_0)]$. It follows from this and (4.4) that

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

as desired.

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

$$d(a_i, a_i, b_i) = t(a_i, p(a_i, a_i, a_i), p(a_i, a_i, b_i)) \tag{4.5}$$

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

$$= b_i. \tag{4.7}$$

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 $d(a_j, b_j, b_j)\ [\theta(a_j, b_j), \theta(a_j, b_j)]\ a_j$. By definition,

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

Since p is a local difference term for S', we have $(p(a_j, b_j, b_j), a_j) \in [\theta(a_j, b_j), \theta(a_j, b_j)]$. This and (4.8) imply that $(d(a_j, b_j, b_j), t(a_j, a_j, a_j))$ belongs to $[\theta(a_j, b_j), \theta(a_j, b_j)]$. Finally, by idempotence of t we have $d(a_j, b_j, b_j)\ [\theta(a_j, b_j), \theta(a_j, b_j)]\ a_j$, as desired.

Case 2: $\chi_0 = 1$. 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 want $d(a_i, b_i, b_i)\ [\theta(a_i, b_i), \theta(a_i, b_i)]\ a_i$. 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

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

Finally, since t is a local difference term for T, hence for (a_i, b_i, b_i), we have $t(a_i, b_i, b_i)\ [\theta(a_i, b_i), \theta(a_i, b_i)]$ a_i. Combining this with (4.9) and (4.10) yields $d(a_i, b_i, b_i)\ [\theta(a_i, b_i), \theta(a_i, b_i)]\ a_i$, as desired.

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

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

as desired. □

Corollary 4.2. A finite idempotent algebra $\mathbf{A}$ has a difference term operation if and only if every pair $((a, b, i), (a', b', i')) \in (A \times A \times \{0, 1\})^2$ has a local difference term.

Proof. One direction is clear, since a difference term operation for $\mathbf{A}$ is obviously a local difference term for the whole set $A \times A \times \{0, 1\}$. For the converse, suppose each pair in $(A \times A \times \{0, 1\})^2$ has a local difference term. Then, by Theorem 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 $a\ [\theta(a, b), \theta(a, b)]\ d(a, b, b)$, since d is a local difference term for $(a, b, 0)$, and we have $d(a, a, b) = b$, since d is also a local difference term for $(a, b, 1)$. □

5. The Algorithm

Corollary 5.1. 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

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

We can rewrite this condition more compactly by considering $t^{\mathbf{A}\times\mathbf{A}}((a,a'),(b,a'),(b,b')) = (t^{\mathbf{A}}(a,b,b), t^{\mathbf{A}}(a',a',b'))$. Clearly t is a local difference term for $((a,b,0),(a',b',1))$ iff

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

where $\delta = [\theta(a,b), \theta(a,b)]$ and a/δ denotes the δ-class containing a. (Observe that $a/\delta \times \{b'\}$ is a subalgebra of $\mathbf{A} \times \mathbf{A}$ by idempotence.) It follows that the pair $((a,b,0),(a',b',1))$ has a local difference term iff the subuniverse of $\mathbf{A}\times\mathbf{A}$ generated by $\{(a,a'),(b,a'),(b,b')\}$ intersects nontrivially with the subuniverse $a/\delta \times \{b'\}$.

Thus, the algorithm takes as input $\mathbf{A}$ and, for each triple $((a,a'),(b,a'),(b,b'))$ in $(A \times A)^3$, computes $\delta = [\theta(a,b), \theta(a,b)]$, computes the subalgebra $\mathbf{S}$ of $\mathbf{A} \times \mathbf{A}$ generated by $\{(a,a'),(b,a'),(b,b')\}$, and then tests whether $S \cap (a/\delta \times \{b'\})$ is empty. If we find an empty intersection at any point, then the algorithm returns the answer "no difference term operation." Otherwise, $\mathbf{A}$ has a difference term operation.

Most of the operations carried out by this algorithm are well known to be polynomial-time. For example, that the running time of subalgebra generation is polynomial has been known for a long time (see [JL76]). The time complexity of congruence generation is also known to be polynomial (see [Fre08]). The only operation whose tractability might be questionable is the commutator, but there is a straight-forward algorithm for computing it which, after the congruences have been computed, simply involves generating more subalgebras. □

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

Appendix A. More About Abelian Algebras

Here are some additional facts about abelian algebras that are sometimes useful.

Lemma A.1. *If* $\mathsf{Clo}(\mathbf{A})$ *is trivial (i.e., generated by the projections), then* $\mathbf{A}$ *is abelian.*

In fact, it can be shown that $\mathbf{A}$ is *strongly abelian* in this case, but we won't prove this stronger result. The proof that $\mathbf{A}$ is abelian is elementary is a nice and easy example of a standard proof technique—induction on term height.[2]

Proof. We want to show $\mathsf{C}(1_A, 1_A)$. Equivalently, we must show that for all $t \in \mathsf{Clo}(\mathbf{A})$ (say, $(\ell + m)$-ary) and all $a, b \in A^\ell$, we have $\ker t(a, \cdot) = \ker t(b, \cdot)$. We prove this by induction on the height of the term t. Height-one terms are projections and the result is obvious for these. Let $n > 1$ and assume the result holds for all terms of height less than n. Let t be a term of height n, say, k-ary. Then for some terms $g_1, \dots, g_k$ of height less than n and for some $j \leqslant k$, we have $t = p^k_j[g_1, g_2, \dots, g_k] = g_j$ and since g_j has height less than n, we have

$$\ker t(a, \cdot) = \ker g_j(a, \cdot) = \ker g_j(b, \cdot) = \ker t(b, \cdot).$$

□

Lemma A.2. *An algebra* $\mathbf{A}$ *is abelian if and only if there is some* $\theta \in \mathrm{Con}(\mathbf{A}^2)$ *that has the diagonal* $D(A) := \{(a, a) : a \in A\}$ *as a congruence class.*

Proof. ($\Leftarrow$) Assume Θ is such a congruence. Fix $k < \omega$, $t^{\mathbf{A}} \in \mathsf{Clo}_{k+1}(\mathbf{A})$, $u, v \in A$, and $\mathbf{x}, \mathbf{y} \in A^k$. We will prove the implication (2.1), which in the present context is

$$t^{\mathbf{A}}(\mathbf{x}, u) = t^{\mathbf{A}}(\mathbf{y}, u) \quad \Longrightarrow \quad t^{\mathbf{A}}(\mathbf{x}, v) = t^{\mathbf{A}}(\mathbf{y}, v).$$

Since $D(A)$ is a class of Θ, we have $(u, u)\ \Theta\ (v, v)$, and since Θ is a reflexive relation, we have $(x_i, y_i)\ \Theta\ (x_i, y_i)$ for all i. Therefore,

$$t^{\mathbf{A}\times\mathbf{A}}((x_1, y_1), \dots, (x_k, y_k), (u, u))\ \Theta\ t^{\mathbf{A}\times\mathbf{A}}((x_1, y_1), \dots, (x_k, y_k), (v, v)). \tag{A.1}$$

since $t^{\mathbf{A}\times\mathbf{A}}$ is a term operation of $\mathbf{A} \times \mathbf{A}$. Note that (A.1) is equivalent to

$$(t^{\mathbf{A}}(\mathbf{x}, u), t^{\mathbf{A}}(\mathbf{y}, u))\ \Theta\ (t^{\mathbf{A}}(\mathbf{x}, v), t^{\mathbf{A}}(\mathbf{y}, v)). \tag{A.2}$$

If $t^{\mathbf{A}}(\mathbf{x}, u) = t^{\mathbf{A}}(\mathbf{y}, u)$ then the first pair in (A.2) belongs to the Θ-class $D(A)$, so the second pair must also belong this Θ-class. That is, $t^{\mathbf{A}}(\mathbf{x}, v) = t^{\mathbf{A}}(\mathbf{y}, v)$, as desired.

($\Rightarrow$) Assume $\mathbf{A}$ is abelian. We show $\mathrm{Cg}^{\mathbf{A}^2}(D(A)^2)$ has $D(A)$ as a block. Assume

$$((x, x), (c, c')) \in \mathrm{Cg}^{\mathbf{A}^2}(D(A)^2). \tag{A.3}$$

[2]This proof would be a good one to try in a proof assistant like Coq, since such tools excel at inductive arguments like this one.

It suffices to prove that $c = c'$. Recall, Mal'tsev's congruence generation theorem states that (A.3) holds iff

$$\begin{aligned}
&\exists\, (z_0, z_0'), (z_1, z_1'), \dots, (z_n, z_n') \in A^2 \\
&\exists\, ((x_0, x_0'), (y_0, y_0')), ((x_1, x_1'), (y_1, y_1')), \dots, ((x_{n-1}, x_{n-1}'), (y_{n-1}, y_{n-1}')) \in D(A)^2 \\
&\exists\, f_0, f_1, \dots, f_{n-1} \in F^*_{\mathbf{A}^2}
\end{aligned}$$

such that

$$\begin{aligned}
\{(x, x), (z_1, z_1')\} &= \{f_0(x_0, x_0'), f_0(y_0, y_0')\} \qquad \text{(A.4)} \\
\{(z_1, z_1'), (z_2, z_2')\} &= \{f_1(x_1, x_1'), f_1(y_1, y_1')\} \\
&\vdots \\
\{(z_{n-1}, z_{n-1}'), (c, c')\} &= \{f_{n-1}(x_{n-1}, x_{n-1}'), f_{n-1}(y_{n-1}, y_{n-1}')\} \qquad \text{(A.5)}
\end{aligned}$$

The notation $f_i \in F^*_{\mathbf{A}^2}$ means

$$\begin{aligned}
f_i(x, x') &= g_i^{\mathbf{A}^2}((a_1, a_1'), (a_2, a_2'), \dots, (a_k, a_k'), (x, x')) \\
&= (g_i^{\mathbf{A}}(a_1, a_2, \dots, a_k, x), g_i^{\mathbf{A}}(a_1', a_2', \dots, a_k', x')),
\end{aligned}$$

for some $g_i^{\mathbf{A}} \in \mathsf{Clo}_{k+1}(\mathbf{A})$ and some constants $\mathbf{a} = (a_1, \dots, a_k)$ and $\mathbf{a}' = (a_1', \dots, a_k')$ in A^k. Now, $((x_i, x_i'), (y_i, y_i')) \in D(A)^2$ implies $x_i = x_i'$, and $y_i = y_i'$, so in fact we have

$$\{(z_i, z_i'), (z_{i+1}, z_{i+1}')\} = \{f_i(x_i, x_i), f_i(y_i, y_i)\} \quad (0 \leqslant i < n).$$

Therefore, by Equation (A.4) we have either

$$(x, x) = (g_i^{\mathbf{A}}(\mathbf{a}, x_0), g_i^{\mathbf{A}}(\mathbf{a}', x_0)) \quad \text{or} \quad (x, x) = (g_i^{\mathbf{A}}(\mathbf{a}, y_0), g_i^{\mathbf{A}}(\mathbf{a}', y_0)).$$

Thus, either $g_i^{\mathbf{A}}(\mathbf{a}, x_0) = g_i^{\mathbf{A}}(\mathbf{a}', x_0)$ or $g_i^{\mathbf{A}}(\mathbf{a}, y_0) = g_i^{\mathbf{A}}(\mathbf{a}', y_0)$. By the abelian assumption, if one of these equations holds, then so does the other. This and and Equation (A.4) imply $z_1 = z_1'$. Applying the same argument inductively, we find that $z_i = z_i'$ for all $1 \leqslant i < n$ and so, by (A.5) and the abelian property, we have $c = c'$. □

Lemma A.3. *Suppose $\rho\colon A_1 \to A_2$ is a bijection and suppose the graph $\{(x, \rho x) \mid x \in A_1\}$ is a block of some congruence $\beta \in \mathrm{Con}(A_1 \times A_2)$. Then both $\mathbf{A}_1$ and $\mathbf{A}_2$ are abelian.*

Proof. Define the relation $\alpha \subseteq (A_1 \times A_1)^2$ as follows: for $((a, a'), (b, b')) \in (A_1 \times A_1)^2$,

$$(a, a')\ \alpha\ (b, b') \quad \iff \quad (a, \rho a')\ \beta\ (b, \rho b')$$

We prove that the diagonal $D(A_1)$ is a block of α by showing that $(a, a)\ \alpha\ (b, b')$ implies $b = b'$. Indeed, if $(a, a)\ \alpha\ (b, b')$, then $(a, \rho a)\ \beta\ (b, \rho b')$, which means that $(b, \rho b')$ belongs

to the block and $(a, \rho a)/\beta = \{(x, \rho x) : x \in A_1\}$. Therefore, $\rho b = \rho b'$, so $b = b'$ since ρ is injective. This proves that $\mathbf{A}_1$ is abelian.

To prove $\mathbf{A}_2$ is abelian, we reverse the roles of A_1 and A_2 in the foregoing argument. If $\{(x, \rho x) \mid x \in A_1\}$ is a block of β, then $\{(\rho^{-1}(\rho x), \rho x) \mid \rho x \in A_2\}$ is a block of β; that is, $\{(\rho^{-1} y, y) \mid y \in A_2\}$ is a block of β. Define the relation $\alpha \subseteq (A_2 \times A_2)^2$ as follows: for $((a, a'), (b, b')) \in (A_2 \times A_2)^2$,

$$(a, a') \; \alpha \; (b, b') \quad \iff \quad (\rho^{-1} a, \rho a') \; \beta \; (\rho^{-1} b, \rho b').$$

As above, we can prove that the diagonal $D(A_2)$ is a block of α by using the injectivity of ρ^{-1} to show that $(a, a) \; \alpha \; (b, b')$ implies $b = b'$. □

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

University of Hawaii

E-mail address: williamdemeo@gmail.com

E-mail address: ralph@math.hawaii.edu

E-mail address: guillena@math.hawaii.edu

E-mail address: tristanh@hawaii.edu

E-mail address: bill@math.hawaii.edu

E-mail address: jb@math.hawaii.edu