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

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

where θ is any congruence containing (a, b) and $[\cdot, \cdot]$ denotes the *commutator* (see Section 2.2). When the relations in (1.1) hold we call $d^{\mathbf{A}}$ a *difference term operation* for $\mathbf{A}$. 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 $\theta \in \text{Con}\,\mathbf{A}$, in which case (1.1) says that $d^{\mathbf{A}}$ is a Mal'cev term operation.

The question motivating this effort is the following:

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

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 notations

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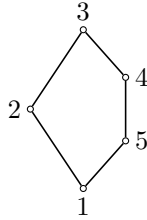
Whether or not $\mathbb{V}(\mathbf{A})$ omits one of the order ideals of the lattice of types can be determined locally. This is spelled out for us in the next proposition. (A *strictly simple* algebra is a simple algebra with no non-trivial subalgebras.)

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. [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

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.*

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

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

But $[\mathrm{Cg}^\mathbf{B}(a, b), \mathrm{Cg}^\mathbf{B}(a, b)] \subseteq [\theta, \theta]$ for any congruence $\theta \in \mathrm{Con}\,\mathbf{A}$ 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 2.3. *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:*

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

(iii) **F** *has a difference term operation.*

Proof. The implications (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) are obvious. We prove (iii) $\Rightarrow$ (i) by contraposition. Suppose $\mathcal{V}$ has no difference term. (We show **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 **A**. Choose $a, b \in A$ witnessing this fact. Then either

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

Let $\mathbf{B} = \mathrm{Sg}^{\mathbf{A}}(\{a, b\})$. In case (1), $d^{\mathbf{B}}(a, a, b) = d^{\mathbf{A}}(a, a, b) \neq b$, so $d^{\mathbf{B}}(x, y, z)$ is not a difference term operation for **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 **B**. Now, since there is a surjective homomorphism from **F** to **B**, it follows that $d^{\mathbf{F}}(x, y, z)$ cannot be a difference term operation for **F**. Finally, recall that $d(x, y, z)$ was an arbitrary ternary term of $\mathcal{V}$, so **F** has no difference term operation whatsoever. $\square$

2.2. **Definitions and other useful tools.** Before proceeding, we harvest some facts about the commutator which may be useful for reasoning about difference terms. Specifically, we review some properties of congruences, centralizers, and abelian algebras that we have recently found very useful (see [BD16]).

In previous work, nonabelian algebras played the following useful role: a theorem would begin with the assumption that a particular algebra **A** is nonabelian and then proceed to show that if the result to be proved were false, then **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* **A**. Given a pair $(\mathbf{u}, \mathbf{v}) \in A^m \times A^m$ of m-tuples of A, we write $\mathbf{u} \, T \, \mathbf{v}$ 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 **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

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

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

Remark. An algebra $\mathbf{A}$ is abelian iff $\mathsf{C}(1_A, 1_A)$ iff

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

$$\ker t(\mathbf{a}, \cdot) = \ker t(\mathbf{b}, \cdot).$$

2.2.1. *Facts about centralizers and abelian congruences.* We begin with a list of properties that are well-known and not too hard to prove (see [HM88, Prop 3.4] or [KK13, Thm 2.19]).

Lemma 2.4. *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 some $i \in I$, $j \in J$, $k \in K$. 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 $\mathsf{C}(\beta, \alpha)$ and $\mathsf{C}(\alpha, \beta)$.

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 2.5. *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 2.5 is an easy consequence of items (1), (3), (4), and (7) of Lemma 2.4.

Lemma 2.6. *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 2.6 can be proved by combining the next result, of David Hobby and Ralph McKenzie, with a result of Keith Kearnes and Emil Kiss.

Lemma 2.7 (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 2.8 ([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 2.6 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 2.7, 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 2.7, 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).

2.2.2. *Facts about the commutator.*

Lemma 2.9. *Let $\mathbf{A}$ be an algebra with congruences α, α', β, β', γ, δ, α_i β_j for some $i \in I$, and suppose $\alpha \leqslant \alpha'$ and $\beta \leqslant \beta'$. Then the following hold:*

(1) $[\alpha, \beta] \leqslant [\alpha', \beta']$;
(2) $[\alpha \wedge \gamma, \beta \wedge \delta] \leqslant [\alpha, \beta] \wedge [\gamma, \delta]$ and $[\alpha, \beta] \vee [\gamma, \delta] \leqslant [\alpha \vee \gamma, \beta \vee \delta]$; more generally,
(3) $[\bigwedge \alpha_i, \bigwedge \beta_i] \leqslant \bigwedge [\alpha_i, \beta_i]$ and $\bigvee [\alpha_i, \beta_i] \leqslant [\bigvee \alpha_i, \bigvee \beta_i]$.

Lemma 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

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

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 $\{0, 1, \ldots, n-1\}$ 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 $\mathbf{B} \leqslant_{\mathrm{sd}} \prod_{\underline{n}} \mathbf{A}_i$ 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. $\qquad\square$

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

Consequently,

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

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. $\qquad\square$

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. $\qquad\square$

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. $\qquad\square$

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 $g_1, \ldots, g_k$ of height less than n and for some $j \leqslant k$, we have $t = p_j^k[g_1, g_2, \ldots, g_k] = g_j$ and since g_j has height less than n, we have

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

$\square$

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,

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

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

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

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

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

---

[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

$$\exists\, (z_0, z_0'), (z_1, z_1'), \ldots, (z_n, z_n') \in A^2$$
$$\exists\, ((x_0, x_0'), (y_0, y_0')), ((x_1, x_1'), (y_1, y_1')), \ldots, ((x_{n-1}, x_{n-1}'), (y_{n-1}, y_{n-1}')) \in D(A)^2$$
$$\exists\, f_0, f_1, \ldots, f_{n-1} \in F_{\mathbf{A}^2}^*$$

such that

(A.4)
$$\{(x, x), (z_1, z_1')\} = \{f_0(x_0, x_0'), f_0(y_0, y_0')\}$$
$$\{(z_1, z_1'), (z_2, z_2')\} = \{f_1(x_1, x_1'), f_1(y_1, y_1')\}$$
$$\vdots$$

(A.5)
$$\{(z_{n-1}, z_{n-1}'), (c, c')\} = \{f_{n-1}(x_{n-1}, x_{n-1}'), f_{n-1}(y_{n-1}, y_{n-1}')\}$$

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

$$f_i(x, x') = g_i^{\mathbf{A}^2}((a_1, a_1'), (a_2, a_2'), \ldots, (a_k, a_k'), (x, x'))$$
$$= (g_i^{\mathbf{A}}(a_1, a_2, \ldots, a_k, x), g_i^{\mathbf{A}}(a_1', a_2', \ldots, a_k', x')),$$

for some $g_i^{\mathbf{A}} \in \mathsf{Clo}_{k+1}(\mathbf{A})$ and some constants $\mathbf{a} = (a_1, \ldots, a_k)$ and $\mathbf{a}' = (a_1', \ldots, a_k')$ 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 $c = c'$. $\qquad\square$

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 $((a, a'), (b, b')) \in (A_1 \times A_1)^2$,

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

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

11

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 $((a, a'), (b, b')) \in (A_2 \times A_2)^2$,

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

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 $b = b'$. $\qquad\square$

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.

[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.

[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`.

[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`.

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