A POLYNOMIAL-TIME TEST FOR A DIFFERENCE TERM IN AN IDEMPOTENT VARIETY

WILLIAM DEMEO, RALPH FREESE, AND MATTHEW VALERIOTE

Abstract. We consider the following practical question: given a finite algebra $\mathbf{A}$ in a finite language, can we efficiently decide whether the variety generated by $\mathbf{A}$ has a difference term? We answer this question (positively) in the idempotent case and then describe algorithms for constructing difference terms.

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

$$d^{\mathbf{A}}(a, a, b) = b \quad \text{and} \quad d^{\mathbf{A}}(a, b, b)\ [\theta, \theta]\ a, \tag{1}$$

where θ is any congruence containing (a, b) and $[\cdot, \cdot]$ denotes the *commutator*. When the relations in (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 some useful properties of the algebras inhabiting that variety. Any variety that has a Mal'tsev term or for which the commutator operation satisfies $[\alpha, \beta] = \alpha \wedge \beta$ has a difference 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 $\theta \in \mathbf{Con}\,\mathbf{A}$, in which case $\mathbf{A}$ (1) says that $d^{\mathbf{A}}$ is a Mal'tsev term operation.)

Difference terms also play a role in recent work of Keith Kearnes, Agnes Szendrei, and Ross Willard. In [KSW16] these authors give a positive answer Jónsson's famous question—whether a variety of finite

Date: 2018-08-13.

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

residual bound must be finitely axiomatizable—for the special case in which the variety has a difference term.[1]

Computers have become invaluable as a research tool and have helped to broaden and deepen our understanding of algebraic structures and the varieties they inhabit. This is largely due to the efforts of researchers who, over the last three decades, have found ingenious ways to coax computers into solving challenging abstract algebraic decision problems, and to do so very quickly. To give a couple of examples related to our own work, it is proved in [VW14] (respectively, [FV09]) that deciding whether a finite idempotent algebra generates a variety that is congruence-n-permutable (respectively, congruence-modular) is *tractable*.[2] The present paper continues this effort by presenting an efficient algorithm for deciding whether a locally finite idempotent variety has a difference term.

The question that motivated us to begin this project, and whose solution is the main subject of this paper, 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?

We note that for arbitrary finite algebras $\mathbf{A}$, the problem of deciding if $\mathbb{V}(\mathbf{A})$ has a difference term is an EXP-time complete problem. This follows from Theorem 9.2 of [FV09].

The remainder of this introduction uses the language of *tame congruence theory* TCT. Many of the terms we use are defined and explained in the next section. For others, see [HM88].

Our solution to Problem 1 exploits the connection between difference terms and TCT that was established by Keith Kearnes in [Kea95].

Theorem 1 ([Kea95, Theorem 1.1])**.** *The variety $\mathcal{V} = \mathbb{V}(\mathbf{A})$ generated by a finite algebra $\mathbf{A}$ has a difference if and only if $\mathcal{V}$ omits TCT-type **1** and, for all finite algebras $\mathbf{B} \in \mathcal{V}$, the minimal sets of every type **2** prime interval in* $\mathrm{Con}(\mathbf{B})$ *have empty tails.*

It follows from an observation of Bulatov that the problem of deciding if a finite idempotent algebra generates a variety that omits TCT-type **1** is tractable (see Proposition 3.1 of [Val09]). In [FV09], the second and third authors solve an analogous problem by giving a positive answer to the following:

[1] To say a variety has *finite residual bound* is to say there is a finite bound on the size of the subdirectly irreducible members of the variety.

[2] To say that the decision problem is *tractable* is to say that there exists an algorithm for solvng the problem that "scales well" with respect to increasing input size, by which we mean that the number of operations required to reach a correct decision is bounded by a polynomial function of the input size.

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?

Congruence modularity is characterized by omitting tails and TCT-types **1** and **5**. Omitting **1**'s and **5**'s can be decided by the subtype theorem. The second and third authors also prove in [FV09] that if there is a nonempty tail in $\mathbb{V}(\mathbf{A})$, then there is a nonempty tail "near the bottom." More precisely, suppose $\mathbf{A}$ is a finite idempotent algebra, and suppose $\mathbb{V}(\mathbf{A})$ has nonempty tails but lacks **1**'s and **5**'s. Then a nonempty tail must occur in a 3-generated subalgebra of $\mathbf{A}^2$. The authors use this to prove that congruence modularity is polynomial-time decidable.

However, proving lack of tails uses the fact that a variety omitting **1**'s and **5**'s has a congruence lattice that—modulo the *solvability congruence* (defined below)—is (join) semidistributive. Now, restricting to just testing whether $\mathbb{V}(\mathbf{A})$ omits type-**2** tails is not a problem. So, for example, there is a polynomial-time algorithm for testing if $\mathbb{V}(\mathbf{A})$ omits **1**'s, **5**'s, and type-**2** tails.

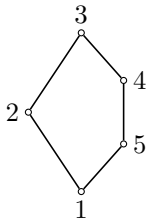
2. Background, definitions, and notation

Our starting point is the set of lemmas at the beginning of Section 3 of [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 lifted directly from [FV09, Section 2].)

The seminal 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 type) an algebra whose basic operations are permutations;
2 (affine type) a one-dimensional vector space over some finite field;
3 (boolean type) a 2-element boolean algebra;
4 (lattice type) a 2-element lattice;
5 (semilattice type) a 2-element semilattice.

Thus to each covering $\alpha \prec \beta$ corresponds a "TCT type," denoted by $\mathrm{typ}(\alpha, \beta)$, belonging to the set $\{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}\}$ (see [HM88, Def. 5.1]). 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 called the *typeset* of $\mathbf{A}$. 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 ([FV09, Proposition 2.1])**.** *If* $\mathbf{A}$ *is a finite idempotent algebra and* $\mathbf{i} \in \operatorname{typ}(\mathbb{V}(\mathbf{A}))$ *then there is a finite strictly simple algebra* $\mathbf{S}$ *of type* $\mathbf{j}$ *for some* $\mathbf{j} \leqslant \mathbf{i}$ *in* $\mathsf{HS}(\mathbf{A})$*. The possible cases are*

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

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

We conclude this section with a result that will be useful in Section 3.

rsf 2018-08-13: did not see how FV 09 lemma 3.3 was used; eliminating it

Corollary 3 ([FV09, Corollary 2.2])**.** *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.*

3. The Characterization

In [FV09], Corollary 3 is the starting point of the development of a polynomial-time algorithm that determines if a given finite idempotent algebra generates a congruence modular variety.

According to the characterization in [HM88, Chapter 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 $\{\mathbf{2}, \mathbf{3}, \mathbf{4}\}$ (resp., $\{\mathbf{3}, \mathbf{4}\}$) and all minimal sets of prime quotients of finite algebras in $\mathcal{V}$ have empty tails [HM88, Def. 2.15]. (In the distributive case the empty tails condition is equivalent to the minimal sets all having exactly two elements.)

It follows from Corollary 3 and Proposition 2 that if $\mathbf{A}$ is idempotent then one can test the first condition—omitting types **1**, **5** (resp., **1**, **2**, **5**)—by searching for a 2-generated subalgebra of $\mathbf{A}$ whose typeset is not contained in $\{\mathbf{2}, \mathbf{3}, \mathbf{4}\}$ (resp., $\{\mathbf{3}, \mathbf{4}\}$). It is proved in [FV09, Section 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 $\mathbf{A}$. The main tools developed to this end are presented in [FV09, Section 3] as a sequence of lemmas that enable the authors to prove the following: 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 nonempty 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 nonempty tails or else there are nonempty tails that are easy to find (since they occur in a 3-generated subalgebra 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.

Our goal is to use the same strategy to solve Problem 1. As such, we revisit each of the lemmas in Section 3 of [FV09], and consider whether an analogous result can be proved under modified hypotheses. Specifically, we retain the assumption that the type set of $\mathbb{V}(\mathbf{A})$ omits **1**, but we drop the assumption that it omits **5**. We will prove that, under these circumstances, either there are no type-**2** tails in $\mathbb{V}(\mathbf{A})$ (so the latter has a difference term), or else type-**2** tails can be found "quickly," (e.g., in a 3-generated subalgebra of $\mathbf{A}^2$). Where possible, we will relate our new results to analogous results in [FV09].

3.1. **Notation.** Throughout we let $\underline{n}$ denote the set $\{0, 1, \dots, n-1\}$ and we take $\mathcal{S}$ to be a finite set of finite, similar, idempotent algebras that is closed under the taking of subalgebras, and we assume that the type set of $\mathcal{V} = \mathbb{V}(\mathcal{S})$ omits **1** (but may include **5**). If there exists a finite algebra in $\mathcal{V}$ having a type-**2** minimal set with a nonempty tail—in which case we say that "$\mathcal{V}$ has type-**2** tails"—then, by standard results in TCT (see [HM88]), at least one such algebra appears as a subalgebra of a product of elements in $\mathcal{S}$. So we suppose that some finite algebra $\mathbf{B}$ in $\mathcal{V}$ has a prime quotient of type **2** with minimal sets that have nonempty tails and show that there is a 3-generated subalgebra of the product of two members of $\mathcal{S}$ with this property (which can be found "quickly").

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 $\mathbf{A}_0, \mathbf{A}_1, \dots, \mathbf{A}_{n-1}$ in $\mathcal{S}$, there is a subdirect product $\mathbf{B} \leqslant_{\text{sd}} \prod_{\underline{n}} \mathbf{A}_i$

that has a prime quotient of type **2** whose minimal sets have nonempty tails. Under the assumption that $n > 1$ we will 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 $\mathbf{B}$ of type **2** whose minimal sets have nonempty tails, and choose β minimal with respect to this property. By [HM88, Lemma 6.2], this implies β is join irreducible and α is its unique subcover. Let U be an $\langle \alpha, \beta \rangle$-minimal set.

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

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

Consequently, $\rho_{\underline{n}} = \bigwedge_{j \in \underline{n}} \rho_j = 0_B$. 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 $\emptyset \subset \sigma \subset \underline{n}$. (By $\subset$ we mean *proper* subset.)

The next four lemmas assume the context above, which for convenience we will denote by Γ; that is, "*Assume* Γ" will mean "Assume $\mathcal{S}$, $\mathbf{B}$, n, $\{\mathbf{A}_i \colon i < n\}$, α, β, U, and ρ_σ are as described above."

Lemma 4 (cf. [FV09, Lemma 3.1])**.** *Assume* Γ. *If* $0, 1 \in U$, *if* $(0,1) \in \beta - \alpha$, *and if* t *belongs to the tail of* U, *then* β *is the congruence of* $\mathbf{B}$ *generated by the pair* $(0,1)$, *and* $\mathbf{B}$ *is generated by* $\{0,1,t\}$.

This follows from the same argument used to prove [FV09, Lemma 3.1], using the fact that since β is abelian over α it follows that γ over δ that appears in the proof will also have type 2.

Lemma 5 (cf. [FV09, Lemma 3.2])**.** *Assume* Γ. *For every proper nonempty subset* σ *of* $\underline{n}$, *either* $\beta \leqslant \rho_\sigma$ *or* $\alpha \vee \rho_\sigma = 1_B$.

This follows from the proof [FV09, Lemma 3.2].

Lemma 6. *Assume* Γ. *For every proper nonempty subset* σ *of* $\underline{n}$, *for all* $v \in B$, *and for all* $b \in \mathrm{Body}(U)$, *we have* $(v, b) \in \beta \circ \rho_\sigma \cap \rho_\sigma \circ \beta$.

Proof. Let $\rho = \rho_\sigma$. Note that $\beta \vee \rho = 1_B$ implies $\beta\big|_U \vee \rho\big|_U = 1_B\big|_U = 1_U$, since $U = e(B)$, for some idempotent unary polynomial e. Now, for all $x, y \in U$, if $x \in \mathrm{Body}(U)$ and $y \in \mathrm{Tail}(U)$, then $(x, y) \notin \beta$. Therefore, $(x, y) \in 1_U = \beta\big|_U \vee \rho\big|_U$ implies there must be some $b' \in \mathrm{Body}(U)$ and $t' \in \mathrm{Tail}(U)$ such that $b' \; \rho \; t'$.

Now, let $d(x, y, z)$ be a pseudo-Mal'tsev polynomial for U, which exists by [HM88, Lemma 4.20]. Thus,

- $d(B, B, B) = U$
- $d(x, x, x) = x$ for all $x \in U$

- $d(x,x,y) = y = d(y,x,x)$ for all $x \in \mathrm{Body}(U)$, $y \in U$.

Moreover, for all c, $d \in \mathrm{Body}(U)$, the unary polynomials $d(x,c,d)$, $d(c,x,d)$, and $d(c,d,x)$ are permutations on U. If we now fix an arbitrary element $b \in \mathrm{Body}(U)$ and let $p(x) = d(x,b',b)$, then (see [HM88, Lemma 4.20])

- $p(U) = U$, since U is minimal,
- $p(b') = d(b',b',b) = b \in \mathrm{Body}(U)$, and
- $t := p(t') \in \mathrm{Tail}(U)$, since $t' \in \mathrm{Tail}(U)$.

Since $(b',t') \in \rho$, we have $(b,t) = (p(b'),p(t')) \in \rho$. Since b is in the body, there is an element b'' in the body with $(b,b'') \in \beta - \alpha$. By Lemma 4, this implies $\mathbf{B} = \mathrm{Sg}^{\mathbf{B}}(\{b,b'',t\})$.

Finally, if $v \in B$, then $v = s^{\mathbf{B}}(b,b'',t)$ for some (idempotent) term s, so

$$v = s^{\mathbf{B}}(b,b'',t)\ \rho\ s^{\mathbf{B}}(b,b'',b)\ \beta\ s^{\mathbf{B}}(b,b,b) = b,$$

and

$$v = s^{\mathbf{B}}(b,b'',t)\ \beta\ s^{\mathbf{B}}(b,b,t)\ \rho\ s^{\mathbf{B}}(b,b,b) = b.$$

Therefore, $(v,b) \in \beta \circ \rho \cap \rho \circ \beta$. Since $v \in B$ and $b \in \mathrm{Body}(U)$ were aribitrary, this completes the proof. □

Lemma 7 (cf. [FV09, Lemma 3.3])**.** *Assume* Γ.

(i) There exists i such that $\alpha \vee \rho_i = 1_B$
(ii) There exists i such that $\alpha \vee \rho_i < 1_B$.

Proof. If item (i) failed, then by Lemma 5 we would have $\beta \leqslant \rho_i$ for all i, and that would imply $\beta = 0_B$.

To see (ii), assume

$$\alpha \vee \rho_i = 1_B \quad \text{for all } i. \tag{2}$$

Take a nonempty proper subset $\sigma \subset \underline{n}$ of indices and let $\rho_\sigma = \bigwedge_{j\in\sigma} \rho_j$. Then $\beta \vee \rho_\sigma = 1_B$. (Otherwise, $\alpha \vee \rho_\sigma \leqslant \beta \vee \rho_\sigma < 1_B$, and it would follow from Lemma 5 that $\alpha \leqslant \beta \leqslant \rho_\sigma \leqslant \rho_i$ for all $i \in \sigma$, but then $\alpha \vee \rho_i = \rho_i < 1_B$, contradicting (2).)

Let $b \in \mathrm{Body}(U)$ and $t \in \mathrm{Tail}(U)$, and let $d(x,y,z)$ denote the pseudo-Mal'tsev operation introduced in the proof of Lemma 6. By [HM88, Lemma 4.25], $(b,d(b,t,t)) \notin \beta$. We will arrive at a contradiction by showing that $b = d(b,t,t)$. By Lemma 6, for every $i \in \underline{n}$, $(b,t) \in \beta \circ \rho_i$ so there is an element $a \in B$ satisfying $b\ \beta\ a\ \rho_i\ t$. By applying the idempotent polynomial e with $e(U) = U$, we have $b\ \beta\ e(a)\ \rho_i\ t$, so we may assume $a \in U$. But this puts $a \in \mathrm{Body}(U)$, since $a\ \beta\ b$. Therefore,

$$d(b,t,t)\ \rho_i\ d(b,a,a) = b.$$

Since this hold for every i, $d(b,t,t) = b$. □

Theorem 8 (cf. [FV09, Theorem 3.4])**.** *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 some finite member of $\mathcal{V}$ has a prime quotient of type **2** whose minimal sets have nonempty tails, then there is some 3-generated algebra $\mathbf{B}$ with this property that belongs to $\mathcal{S}$ or is a subdirect product of two algebras from $\mathcal{S}$.*

Proof. Choose $n > 0$, $\mathbf{A}_i \in \mathcal{S}$, for $0 \leq i \leq n-1$ and $\mathbf{B}$ as above. From Lemma 4 we know that $\mathbf{B}$ is 3-generated. If $n > 1$ then by the previous lemma we can choose i and $j < n$ with $\beta \leq \rho_i$ and $\alpha \vee \rho_j = 1_B$. If $n > 2$ then Lemma 5 applies to $\rho = \rho_i \wedge \rho_j$ and so we know that either $\beta \leq \rho$ or $\alpha \vee \rho = 1_B$. This yields a contradiction as the former is not possible, since $\beta \not\leq \rho_j$ and the latter can't hold since both α and ρ are below ρ_i.

So, the minimality of n forces $n \leq 2$ and the result follows. □

Example 9. Let $\mathbf{A}$ be the (idempotent) algebra with universe $\{0,1,2,3\}$ with basic operation $x \cdot y$ defined by:

$\cdot$	0	1	2	3
0	0	2	1	3
1	2	1	0	3
2	1	0	2	3
3	3	0	0	3

It can be checked that $\mathbf{A}$ is a simple algebra of type **3** and that no subalgebra of $\mathbf{A}$ has a prime quotient of type **2** whose minimal sets have nonempty tails. It can also be checked that the subalgebra of $\mathbf{A}^2$ generated by $\{(0,0),(1,0),(0,3)\}$ does have such a prime quotient. This demonstrates that in general one must look for nonempty tails of minimal sets of type **2** in the square of a finite idempotent algebra and not just in the subalgebras of the algebra itself.

We note that, since $\mathbf{A}$ is simple of type **3**, the ternary projection operation $p(x,y,z) = z$ is a difference term operation for $\mathbf{A}$. We also note that the term operation $(x \cdot y) \cdot (y \cdot x)$ of $\mathbf{A}$ is commutative and so the variety generated by $\mathbf{A}$ omits type **1**. So, this example also demonstrates that for finite idempotent algebras, having a difference term operation and generating a variety that omits type **1** does not guarantee the existence of a difference term for the variety.

mav 2018-08-13: added so that it can be cited later on.

Corollary 10. *Let $\mathbf{A}$ be a finite idempotent algebra. Then $\mathbb{V}(\mathbf{A})$ has a difference term if and only if*

- $\mathsf{HS}(\mathbf{A})$ *does not contain an algebra that is term equivalent to the 2-element set and*
- *no 3-generated subalgebra of* $\mathbf{A}^2$ *has a prime quotient of type* ***2*** *whose minimal sets have nonempty tails.*

Proof. This is just a combination of Proposition 2 and Theorems 1 and 8. □

The next theorem essentially gives an algorithm to decide if a finitely generated, idempotent variety has a difference term. In the next section, we will show that the algorithm runs in polynomial-time.

In [KK99], Kearnes and Kiss show there is a close connection between $\alpha \prec \beta$ being the critical interval of a pentagon and $\langle \alpha, \beta \rangle$-minimal sets having nonempty tails. By [KK99, Theorem 2.1], the minimal sets of a prime critical interval of a pentagon have nonempty tails, provided the type is not **1**. In the other direction, if the $\langle \alpha, \beta \rangle$-minimal sets have nonempty tails, then there is a pentagon in the congruence lattice of a subalgebra of $\mathbf{A}^2$ with a prime critical interval of the same type. This connection between minimal sets with tails and pentagons is important for us: we do not have a polynomial time algorithm for finding an $\langle \alpha, \beta \rangle$-minimal set.

If $\mathbf{B}$ is a subalgebra of $\mathbf{A}^2$ and θ is a congruence of $\mathbf{A}$, then we define $\theta_0 \in \mathrm{Con}(\mathbf{B})$ by $(x_0, x_1)\ \theta_0\ (y_0, y_1)$ iff $x_0\ \theta\ y_0$. We define θ_1 similarly. In case $\theta = 0_{\mathbf{A}}$, the least congruence, we use the notation ρ_0 and ρ_1 instead of 0_0 and 0_1. Of course ρ_0 and ρ_1 are the kernels of the first and second projections of $\mathbf{B}$ onto $\mathbf{A}$.

Theorem 11. *Let* $\mathbf{A}$ *be a finite idempotent algebra and let* $\mathcal{V}$ *be the variety it generates. Then* $\mathcal{V}$ *has a difference term if and only if the following conditions hold:*

(1) $\mathcal{V}$ *omits TCT-type* ***1****.*
(2) There do not exist a, b, $c \in A$ *satisfying the following, where* $\mathbf{B} := \mathrm{Sg}^{\mathbf{A}}(a, b, c)$ *and* $\mathbf{C} := \mathrm{Sg}^{\mathbf{B}^2}\big(\{(a, b), (a, c), (b, c)\} \cup 0_{\mathbf{B}}\big)$*:*
  (a) $\beta := \mathrm{Cg}^{\mathbf{B}}(a, b)$ *is join irreducible with lower cover* α*,*
  (b) $((a, b), (b, b)) \notin (\alpha_0 \wedge \alpha_1) \vee \mathrm{Cg}^{\mathbf{C}}((a, c), (b, c))$*, and*
  (c) $[\beta, \beta] \leq \alpha$*.*
(3) There do not exist x_0, x_1, y_0, $y_1 \in A$ *satisfying the following, where* $\mathbf{B}$ *is the subalgebra of* $\mathbf{A} \times \mathbf{A}$ *generated by* $0 := (x_0, x_1)$, $1 := (y_0, x_1)$*, and* $t := (x_0, y_1)$*:*
  (a) $\beta := \mathrm{Cg}^{\mathbf{B}}(0, 1)$ *is join irreducible with lower cover* α*,*
  (b) $\rho_0 \vee \alpha = 1_{\mathbf{B}}$*, and*
  (c) the type of β *over* α *is* ***2****.*

Proof. First assume $\mathcal{V}$ has a difference term. Then (1) holds by Theorem 1. If (2) fails then there are a, b and $c \in A$ such that the conditions specified in (2) hold. In particular, (2c) holds and implies that $\operatorname{typ}\langle\alpha,\beta\rangle \subseteq \{\mathbf{1},\mathbf{2}\}$, so by (1) the type of $\langle\alpha,\beta\rangle$ is $\mathbf{2}$. Let

$$\delta := (\alpha_0 \wedge \alpha_1) \vee \operatorname{Cg}^{\mathbf{C}}((a,c),(b,c)), \text{ and}$$
$$\theta := \delta \vee \operatorname{Cg}^{\mathbf{C}}((a,b),(b,b)).$$

By its definition, $\delta \not\leqslant \alpha_0$, so by (2b), $\alpha_0 \wedge \alpha_1 < \delta < \theta \leq \beta_0$. Since C contains 0_B, the diagonal of B, the coordinate projections are onto, so $\alpha_0 \prec \beta_0$ and this interval has type $\mathbf{2}$. From this it follows that $\alpha_0 \vee \delta = \beta_0$. Since $\theta \leq \alpha_1$, we have $\alpha_0 \wedge \theta = \alpha_0 \wedge \alpha_1$. Hence

$$\{\alpha_0 \wedge \alpha_1, \delta, \theta, \alpha_0, \beta_0\}$$

forms a pentagon. Since $[\beta_0,\beta_0] \leqslant \alpha_0$, we have $[\theta,\theta] \leqslant \alpha_0 \wedge \alpha_1 < \delta$, so there is a congruence δ' such that $\delta \leqslant \delta' \prec \theta$ and $\langle\delta',\theta\rangle$ has type $\mathbf{2}$. As mentioned in the discussion above, this implies the $\langle\delta',\theta\rangle$-minimal sets have tails, contradicting Theorem 1.

Now suppose that (3) fails. Then the conditions imply

$$\{0_{\mathbf{B}}, \alpha, \beta, \rho_0, 1_{\mathbf{B}}\}$$

is a pentagon whose critical prime interval has type $\mathbf{2}$. This leads to a contradiction in the same manner as above.

For the converse assume that $\mathcal{V}$ does not have a difference term. We want to show that (1), (2) or (3) fails. Assume all three hold. By Theorem 1 there is a finite algebra $\mathbf{B} \in \mathcal{V}$ and a join irreducible $\beta \in \operatorname{Con}(\mathbf{B})$ with lower cover α such that the type of $\langle\alpha,\beta\rangle$ is $\mathbf{2}$ and the $\langle\alpha,\beta\rangle$-minimal sets have nonempty tails. Let U be one of these minimal sets.

We may assume $\mathbf{B}$ is minimal in the same manner as with the above lemmas (with $\mathcal{S}$ being the subalgebras of $\mathbf{A}$). By Lemma 4 we have that $\mathbf{B}$ is generated by any 0, 1, and t in U such that $\beta = \operatorname{Cg}^{\mathbf{B}}(0,1)$ and t is in the tail. By Theorem 8, $\mathbf{B}$ is either in $\mathcal{S}$ or is a subdirect product of two members of $\mathcal{S}$.

Assume $\mathbf{B}$ is a subalgebra of $\mathbf{A}$. Taking $a = 0$, $b = 1$ and $c = t$, we claim the conditions specified in (2) hold. Since the type of β over α is $\mathbf{2}$, (2c) holds and we already have (2a) holds. (2b) holds by [KK99, Theorem 2.4]. So this choice of a, b, and c witness that (2) fails.

Now assume $\mathbf{B}$ is not in $\mathcal{S}$ but is a subdirect product of two members of $\mathcal{S}$. Then by Lemma 7 we may assume $\rho_0 \vee \alpha = 1_{\mathbf{B}}$ and $\rho_1 \vee \alpha < 1_{\mathbf{B}}$. By Lemma 5 we have $\rho_1 \geq \beta$.

This implies that 0 and 1 have the same second coordinate; that is, $0 = (x_0, x_1)$ and $1 = (y_0, x_1)$ for some x_0, y_0 and $x_1 \in A$. By Lemma 6,

$(0,t) \in \rho_0 \circ \beta$ so $0\ \rho_0\ t'\ \beta\ t$. Let $U = e(B)$ where e is an idempotent polynomial. Then $0\ \rho_0\ e(t')\ \beta\ t$. This gives that $e(t')$ is in the tail of U and $0\ \rho_0\ e(t')$. We can replace t by $e(t')$, and so assume that $0\ \rho_0\ t$. Since $0 = (x_0, x_1)$, $t = (x_0, y_1)$ for some $y_1 \in A$. Now x_0, y_0, x_1 and y_1 witness that (3) fails. □

4. The Algorithm and its Time Complexity

If $\mathbf{A}$ is an algebra with underlying set (or universe) A, we let $|\mathbf{A}| = |A|$ be the cardinality of A and $||\mathbf{A}||$ be the *input size*; that is,

$$||\mathbf{A}|| = \sum_{i=0}^{r} k_i n^i$$

where, k_i is the number of basic operations of arity i and r is the largest arity. We let

$$n = |\mathbf{A}| \qquad m = ||\mathbf{A}||$$
$$r = \text{the largest arity of the operations of } \mathbf{A}$$

Proposition 12. *Let $\mathbf{A}$ be a finite algebra with the parameters above. Then there is a constant c independent of these parameters such that:*

(1) If S is a subset of A, then $\mathrm{Sg}^{\mathbf{A}}(S)$ can be computed in time

$$c\,r\,||\,\mathrm{Sg}^{\mathbf{A}}(S)|| \leq c\,r\,||\mathbf{A}|| = crm$$

(2) If a, $b \in A$, then $\mathrm{Cg}^{\mathbf{A}}(a,b)$ can be computed in $c\,r\,||\mathbf{A}|| = crm$ time.

(3) If α and β are congruences of $\mathbf{A}$, then $[\alpha,\beta]$ can be computed in time crm^4. If $\mathbf{A}$ has a Taylor term and $[\alpha,\beta] = [\beta,\alpha]$, then $[\alpha,\beta]$ can be computed in time $c(rm^2+n^5)$. In particular, $[\beta,\beta]$ can be computed in this time.

Proof. For the first two parts see [FV09, Proposition 6.1]. To see the third part we first describe a method to compute $[\alpha,\beta]$.

Following the notation of [FM87], we write elements of $\mathbf{A}^4$ as 2×2 matrices, and let $M(\alpha,\beta)$ be the subalgebra of $\mathbf{A}^4$ generated by the elements of the form

$$\begin{bmatrix} a & a \\ a' & a' \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} b & b' \\ b & b' \end{bmatrix}$$

where $a\ \alpha\ a'$ and $b\ \beta\ b'$. Then by definition $[\alpha,\beta]$ is the least congruence γ such that

$$\text{if } \begin{bmatrix} x & y \\ u & v \end{bmatrix} \text{ is in } M(\alpha,\beta) \text{ and } x\ \gamma\ y, \text{ then } u\ \gamma\ v. \tag{3}$$

Let $\delta = [\alpha, \beta]$. Clearly, if $\begin{bmatrix} x & x \\ u & v \end{bmatrix}$ is in $M(\alpha, \beta)$, then $u \; \delta \; v$. Let δ_1 be the congruence generated by the (u, v)'s so obtained. Then $\delta_1 \leq \delta$.

We can now define δ_2 as the congruence generated by the pairs (u, v) arising as the second row of members of $M(\alpha, \beta)$, where the elements of the first row are δ_1 related. More precisely, we inductively define $\delta_0 = 0_{\mathbf{A}}$ and

$$\delta_{i+1} = \mathrm{Cg}^{\mathbf{A}}\left(\left\{(u, v) : \begin{bmatrix} x & y \\ u & v \end{bmatrix} \in M(\alpha, \beta) \text{ and } (x, y) \in \delta_i\right\}\right) \tag{4}$$

Clearly, $\delta_1 \leq \delta_2 \leq \cdots \leq \delta$ and so $\bigvee_i \delta_i \leq \delta$.

Now $\bigvee_i \delta_i$ has the property (3) of the definition of $[\alpha, \beta]$, and hence $\delta \leq \bigvee_i \delta_i$, and thus they are equal.

So to find $[\alpha, \beta]$ when $\mathbf{A}$ is finite, we find $M(\alpha, \beta)$ and then compute the δ_i's, stoping when $\delta_i = \delta_{i+1}$, which will be $[\alpha, \beta]$ of course. The time to compute $M(\alpha, \beta)$ is bounded by crm^4 by part (1). Suppose we have computed δ_i. To compute δ_{i+1} we run through the at most n^4 matrices in $\begin{bmatrix} x & y \\ u & v \end{bmatrix} \in M(\alpha, \beta)$. If x and y are in the same block, we join the block containing u and the one containing v into a single block. By the techniques of [Fre08], this can be done in constant time. Now we take the congruence generated by this partition. So, by (2) the time to compute δ_{i+1} from δ_i is $c(n^4 + rm)$. Since the congruence lattice of $\mathbf{A}$ has length at most $n - 1$, there are at most n passes. So the total time is at most a constant times $rm^4 + n(n^4 + rm) = rm^4 + n^5 + nrm$. But since the commutator is trivial in unary algebras, we may assume $m \geq n^2$, and thus the time is bounded by a constant times rm^4, proving the first part of (3). This procedure for calculating the commutator is part of Ross Willard's thesis [Wil89].

To see the other part, let $\mathbf{A}(\alpha)$ the subalgebra of $\mathbf{A} \times \mathbf{A}$ whose components are α related. If we view the elements of $\mathbf{A}(\alpha)$ as column vectors, then the elements of $M(\alpha, \beta)$ can be thought of as pairs of elements of $\mathbf{A}(\alpha)$, that is, as a binary relation on $\mathbf{A}(\alpha)$. Define $\Delta_{\alpha,\beta}$ to be the congruence on $\mathbf{A}(\alpha)$ generated by this relation, that is, the transitive closure of this relation. Clearly $M(\alpha, \beta) \subseteq \Delta_{\alpha,\beta}$. So, if in the algorithm above we used $\Delta_{\alpha,\beta}$ in place of $M(\alpha, \beta)$, the result would be at least $\delta = [\alpha, \beta]$. So, if we knew that

$$\text{whenever } \begin{bmatrix} x & y \\ u & v \end{bmatrix} \in \Delta_{\alpha,\beta} \text{ and } (x, y) \in \delta, \text{ then } (u, v) \in \delta, \tag{5}$$

then this modified procedure would also compute δ.

While (5) is not true in general even if $\mathbf{A}$ has a Taylor term, it is true when $\mathbf{A}$ has a Taylor term and $[\alpha, \beta] = [\beta, \alpha]$. So assume $\mathbf{A}$ has a Taylor term and $[\alpha, \beta] = [\beta, \alpha]$. Under these conditions the commutator agrees with the linear commutator, that is, $[\alpha, \beta] = [\alpha, \beta]_\ell$ by Corollary 4.5 of [KS98]. Suppose $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Delta_{\alpha,\beta}$ and $(a, b) \in \delta$. Then, since $\Delta_{\alpha,\beta}$ is the transitive closure of $M(\alpha, \beta)$, there are elements a_i and c_i in A, $i = 0, \dots, k$, with $a_0 = a$, $c_0 = c$, $a_k = b$ and $c_k = d$, such that $\begin{bmatrix} a_i & a_{i+1} \\ c_i & c_{i+1} \end{bmatrix} \in M(\alpha, \beta)$.

Now the linear commutator is $[\alpha^*, \beta^*]\big|_A$, where α^* and β^* are congruences on an expansion $\mathbf{A}^*$ of $\mathbf{A}$ such that $\alpha \subseteq \alpha^*$ and $\beta \subseteq \beta^*$; see Lemma 2.4 of [KS98] and the surrounding discussion.

Moreover $M(\alpha, \beta) \subseteq M(\alpha^*, \beta^*)$, the latter calculated in $\mathbf{A}^*$, because the generating matrices of $M(\alpha^*, \beta^*)$ contain those of $M(\alpha, \beta)$, and the operations of $\mathbf{A}$ are contained in the operations of $\mathbf{A}^*$. So $\begin{bmatrix} a_i & a_{i+1} \\ c_i & c_{i+1} \end{bmatrix} \in M(\alpha^*, \beta^*)$. By its definition $\mathbf{A}^*$ has a Maltsev term, and consequently $M(\alpha^*, \beta^*)$ is transitive as a relation on $\mathbf{A}(\alpha^*)$. Thus $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M(\alpha^*, \beta^*)$, and hence, $(c, d) \in [\alpha^*, \beta^*]\big|_A = [\alpha, \beta]$.

Now, since $\Delta_{\alpha,\beta}$ is a congruence on $\mathbf{A}(\alpha)$, it can be computed in time crm^2 by part (2). The result follows. □

Theorem 13. *Let* $\mathbf{A}$ *be a finite idempotent algebra with parameters as above. Then one can determine if* $\mathbb{V}(\mathbf{A})$ *has a difference term in time* $c(rn^4m^4 + n^{14})$.

rsf 2018-08-13: See if we can omit n^{14}.

Proof. Theorem 11 gives a three-step algorithm to test if $\mathbb{V}(\mathbf{A})$ has a difference term. The first step is to test if $\mathbb{V}(\mathbf{A})$ omits type **1**. This can be done in time crn^3m by [FV09, Theorem 6.3].

Looking now at part (3) of Theorem 11, there are several things that have to be constructed. By Proposition 12, all of these things can be constructed in time crm^2 and parts (a) and (b) can be executed in this time or less. For part (c) we need to test if the type of β over α is **2**. Since at this point in the algorithm we know that $\mathbf{A}$ omits type **1**, we can test if the type is **2** by testing if $[\beta, \beta] \leq \alpha$. By Proposition 12 this can be done in time $c(rm^4 + n^{10})$. Since we need to do this for all x_0, x_1, y_0 and y_1, the total time for this step is at most $crn^4m^4 + n^{14}$.

A similar analysis applies to part (2) and shows that it can be done in time crn^3m^2. Since crn^4m^4 dominates the other terms, the bound of the theorem holds. □

5. Difference Term Operations

Above we addressed the problem of deciding the existence of a difference term for a given (idempotent, finitely generated) variety. In this section we are concerned with the practical problem of finding a difference term *operation* for a given (finite, idempotent) algebra. We describe algorithms for

(1) deciding whether a given finite idempotent algebra has a difference term operation, and
(2) finding a difference term operation for a given finite idempotent algebra.

Note that Theorem 13 gives a polynomial-time algorithm for deciding whether or not the variety $\mathbb{V}(\mathbf{A})$ generated by a finite idempotent algebra $\mathbf{A}$ has a difference term. If we run that algorithm on input $\mathbf{A}$, and if the observed output is "Yes", then of course we have a positive answer to decision problem (1). However, a negative answer returned by the algorithm only tells us that $\mathbb{V}(\mathbf{A})$ has no difference term. It does not tell us whether or not $\mathbf{A}$ has a difference term operation. Example 9 provides a finite idempotent algebra that has a difference term operation such that the variety that it generates does not have a difference term.

In this section we present solutions to problems (1) and (2) using different methods than those of the previous sections. In Subsection 5.2 we give a polynomial-time algorithm for deciding whether a given idempotent algebra $\mathbf{A}$ has a difference term operation. In Subsection 6 we address problem (2) by presenting an algorithm for constructing a difference term operation.

5.1. Local Difference Terms.

In [VW14], Ross Willard and the third author 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 [Hor13], Jonah Horowitz introduced similar local methods for deciding when a given variety satisfies certain Mal'tsev conditions. Inspired by these works, we now define a "local difference term operation" and use it to develop a polynomial-time algorithm for deciding the existence of a difference term operation.

Start with a finite idempotent algebra, $\mathbf{A} = \langle A, \ldots \rangle$. For elements $a, b, a_j, b_j \in A$, the following are some shorthands we will use to denote

the congruences generated by these elements:

$$\theta_{ab} := \mathrm{Cg}^{\mathbf{A}}(a, b) \qquad \theta_i := \mathrm{Cg}^{\mathbf{A}}(a_i, b_i).$$

Let $i \in \{0, 1\}$. By a *local difference term operation for* (a, b, i) we mean a ternary term operation t satisfying the following conditions:

$$\text{if } i = 0, \text{ then } a \; [\theta_{ab}, \theta_{ab}] \; t(a, b, b); \tag{6}$$

$$\text{if } i = 1, \text{ then } t(a, a, b) = b. \tag{7}$$

If t satisfies conditions (6) and (7) for all triples in some subset $S \subseteq A^2 \times \{0, 1\}$, then we call t a *local difference term operation for* S. Throughout the remainder of the paper, we will write "LDT operation" as a shorthand for "local difference term operation."

A few more notational conventions will come in handy below. Let $\mathsf{Clo}_3(\mathbf{A})$ denote the set of all ternary term operations of $\mathbf{A}$, and let $\mathcal{D} \subseteq \big(A^2 \times \{0, 1\}\big) \times \mathsf{Clo}_3(\mathbf{A})$ denote the relation that associates (a, b, i) with the operations in $\mathsf{Clo}_3(\mathbf{A})$ that are LDT operations for (a, b, i). That is, $((a, b, i), t) \in \mathcal{D}$ iff conditions (6) and (7) are satisfied. The relation $\mathcal{D}$ induces an obvious Galois connection from subsets of $A^2 \times \{0, 1\}$ to subsets of $\mathsf{Clo}_3(\mathbf{A})$. Overloading the symbol $\mathcal{D}$, we take

$$\mathcal{D} \colon \mathcal{P}(A^2 \times \{0, 1\}) \to \mathcal{P}(\mathsf{Clo}_3(\mathbf{A})) \text{ and}$$

$$\breve{\mathcal{D}} \colon \mathcal{P}(\mathsf{Clo}_3(\mathbf{A})) \to \mathcal{P}(A^2 \times \{0, 1\})$$

to be the maps defined as follows:

$$\begin{aligned} &\text{for } \; S \subseteq A^2 \times \{0, 1\} \; \text{ and } \; T \subseteq \mathsf{Clo}_3(\mathbf{A}), \text{ let} \\ &\mathcal{D}S = \{t \in \mathsf{Clo}_3(\mathbf{A}) \colon (s, t) \in \mathcal{D} \text{ for all } s \in S\}, \text{ and} \\ &\breve{\mathcal{D}}T = \{s \in A^2 \times \{0, 1\} \colon (s, t) \in \mathcal{D} \text{ for all } t \in T\}. \end{aligned}$$

In other words, $\mathcal{D}S$ is the set of LDT operations for S, and $\breve{\mathcal{D}}T$ is the set of triples for which every $t \in T$ is a LDT operation. When the set S is just a singleton, we write $\mathcal{D}(a, b, \chi)$ instead of $\mathcal{D}\{(a, b, \chi)\}$.

Now, suppose that every pair $(s_0, s_1) \in (A^2 \times \{0, 1\})^2$ has a LDT operation. Then every subset $S \subseteq A^2 \times \{0, 1\}$ has a LDT operation, as we now prove.

Theorem 14. *Let $\mathcal{V}$ be an idempotent variety and let $\mathbf{A} \in \mathcal{V}$. If every pair $(s_0, s_1) \in (A^2 \times \{0, 1\})^2$ has a local difference term operation, then every subset $S \subseteq A^2 \times \{0, 1\}$ has a local difference term operation.*

Proof. The proof is by induction on the size of S. In the base case, $|S| = 2$, the claim holds by assumption. Fix $\ell \geqslant 2$ and assume that every subset of $A^2 \times \{0, 1\}$ of size $k \leqslant \ell$ has a LDT operation. Let

$$S := \{(a_0, b_0, \chi_0), (a_1, b_1, \chi_1), \ldots, (a_\ell, b_\ell, \chi_\ell)\} \subseteq A^2 \times \{0, 1\},$$

so $|S| = \ell + 1$. We prove S has a LDT operation.

Since $|S| \geqslant 3$, there exist indices $k \neq j$ such that $\chi_k = \chi_j$. Assume without loss of generality that one such index is $j = \ell$, and define the set

$$S' := S - \{(a_\ell, b_\ell, \chi_\ell)\}.$$

Since $|S'| < |S|$, there exists $p \in \mathcal{D}S'$. We split the remainder of the proof into two cases.

Case $\chi_\ell = 0$: Without loss of generality, assume

$$\chi_0 = \cdots = \chi_{k-1} = 1 \quad \text{and} \quad \chi_k = \cdots = \chi_\ell = 0.$$

If we define

$$S_0 := \{(a_0, b_0, 1), (a_1, b_1, 1), \ldots, (a_{k-1}, b_{k-1}, 1), (a_\ell, p(a_\ell, b_\ell, b_\ell), 0)\},$$

then $|S_0| < |S|$, so S_0 has a LDT operation, $q \in \mathcal{D}S_0$. We now show that

$$d(x, y, z) := q(x, p(x, y, y), p(x, y, z))$$

is a local difference term operation for S.

Since $\chi_\ell = 0$, we must check that $a_\ell \ [\theta_\ell, \theta_\ell] \ d(a_\ell, b_\ell, b_\ell)$. If $\gamma := \mathrm{Cg}(a_\ell, p(a_\ell, b_\ell, b_\ell))$, then

$$d(a_\ell, b_\ell, b_n\ell) = q(a_\ell, p(a_\ell, b_\ell, b_\ell), p(a_\ell, b_\ell, b_\ell)) \ [\gamma, \gamma] \ a_\ell. \tag{8}$$

The pair $(a_\ell, p(a_\ell, b_\ell, b_\ell))$ is equal to $(p(a_\ell, a_\ell, a_\ell), p(a_\ell, b_\ell, b_\ell))$ and so belongs to θ_ℓ. Therefore, $\gamma \leqslant \theta_\ell$, so $[\gamma, \gamma] \leqslant [\theta_\ell, \theta_\ell]$. It follows from this and (8) that $a_\ell \ [\theta_\ell, \theta_\ell] \ d(a_\ell, b_\ell, b_\ell)$, as desired.

For indices $i < k$, we have $\chi_i = 1$, so $d(a_i, a_i, b_i) = b_i$ for such i. Indeed,

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

The first equation holds by definition of d, the second because p is an idempotent LDT operation for S', and the third because $q \in \mathcal{D}S_0$.

The remaining triples in our original set S have indices satisfying $k \leqslant j < \ell$ and $\chi_j = 0$. Here, we have $a_j \ [\theta_j, \theta_j] \ d(a_j, b_j, b_j)$. Indeed, by definition,

$$d(a_j, b_j, b_j) = q(a_j, p(a_j, b_j, b_j), p(a_j, b_j, b_j)), \tag{9}$$

and, since $p \in \mathcal{D}S'$, we have $a_j \ [\theta_j, \theta_j] \ p(a_j, b_j, b_j)$, so (9) implies that $a_j = q(a_j, a_j, a_j) \ [\theta_j, \theta_j] \ d(a_j, b_j, b_j)$.

Case $\chi_\ell = 1$: Without loss of generality, assume

$$\chi_0 = \cdots = \chi_{k-1} = 0 \quad \text{and} \quad \chi_k = \cdots = \chi_\ell = 1.$$

If $S_1 := \{(a_0, b_0, 0), (a_1, b_1 0), \ldots, (a_{k-1}, b_{k-1}, 0), (p(a_\ell, a_\ell, b_\ell), b_\ell, 1)\}$,

then $|S_1| < |S|$, so there exists $q \in \mathcal{D}S_1$. We claim that

$$d(x, y, z) := q(p(x, y, z), p(y, y, z), z)$$

is a LDT operation for S. For $(a_\ell, b_\ell, \chi_\ell) \in S$ we have that

$$d(a_\ell, a_\ell, b_\ell) = q(p(a_\ell, a_\ell, b_\ell), p(a_\ell, a_\ell, b_\ell), b_\ell) = b_\ell.$$

The last equality holds since $q \in \mathcal{D}S_1$.

If $i < k$, then $\chi_i = 0$. For these indices we must prove that a_i is congruent to $d(a_i, b_i, b_i)$ modulo $[\theta_i, \theta_i]$. Again, starting from the definition of d and using idempotence of p, we have

$$d(a_i, b_i, b_i) = q(p(a_i, b_i, b_i), p(b_i, b_i, b_i), b_i) = q(p(a_i, b_i, b_i), b_i, b_i). \tag{10}$$

Next, since $p \in \mathcal{D}S'$,

$$q(p(a_i, b_i, b_i), b_i, b_i) \; [\theta_i, \theta_i] \; q(a_i, b_i, b_i). \tag{11}$$

Since $q \in \mathcal{D}S_1$, we have $q(a_i, b_i, b_i) \; [\theta_i, \theta_i] \; a_i$, so (10) and (11) imply $d(a_i, b_i, b_i) \; [\theta_i, \theta_i] \; a_i$, as desired.

The remaining elements of S have indices satisfying $k \leqslant j < \ell$ and $\chi_j = 1$. For these we want $d(a_j, a_j, b_j) = b_j$. Since $p \in \mathcal{D}S'$, we have $p(a_j, a_j, b_j) = b_j$, and this plus idempotence of q yields

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

as desired. □

Corollary 15. *Let* $\mathbf{A}$ *be a finite idempotent algebra and suppose that every pair* $(s, s') \in (A^2 \times \{0, 1\})^2$ *has a local difference term operation. Then* $\mathcal{D}(A^2 \times \{0, 1\}) \neq \emptyset$*, so* $\mathbf{A}$ *has a difference term operation.*

Proof. Letting $S := A^2 \times \{0, 1\}$ in Theorem 14 establishes the existence of a LDT operation d for S. That is, $d \in \mathcal{D}S$. It follows that d is a difference term operation for A. Indeed, for all $a, b \in A$, we have that $a \; [\theta_{ab}, \theta_{ab}] \; d(a, b, b)$, since $d \in \mathcal{D}S \subseteq \mathcal{D}(a, b, 0)$, and $d(a, a, b) = b$, since $d \in \mathcal{D}S \subseteq \mathcal{D}(a, b, 1)$. □

5.2. **Test for existence of a difference term operation.** Here is a practical consequence of Theorem 14.

Corollary 16. *There is a polynomial-time algorithm that takes as input any finite idempotent algebra* $\mathbf{A}$ *and decides if* $\mathbf{A}$ *has a difference term operation.*

Proof. We describe an efficient algorithm for deciding, given a finite idempotent algebra $\mathbf{A}$, whether every pair in $(A^2 \times \{0, 1\})^2$ has a LDT operation. By Corollary 15, 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 $(A^2\times\{0,1\})^2$. If $i=i'=0$, then the first projection is a LDT operation. If $i=i'=1$, then the third projection is a LDT operation. The two remaining cases occur when $i\neq i'$. Without loss of generality, assume $i=0$ and $i'=1$, so the given pair of triples is of the form $((a,b,0),(a',b',1))$. By definition, $t\in\mathcal{D}\{(a,b,0),(a',b',1)\}$ iff

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

We can rewrite this condition more compactly by noting that

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

and that $t\in\mathcal{D}\{(a,b,0),(a',b',1)\}$ if and only if

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

where $\delta=[\theta_{ab},\theta_{ab}]$ and a/δ denotes the δ-class containing a. It follows that $\mathcal{D}\{(a,b,0),(a',b',1)\}\neq\emptyset$ 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, we take as input a finite idempotent algebra $\mathbf{A}$ and, for each element $((a,a'),(b,a'),(b,b'))$ of $(A\times A)^3$,

(1) compute θ_{ab},
(2) compute $\delta=[\theta_{ab},\theta_{ab}]$,
(3) compute $\mathbf{S}=\mathrm{Sg}^{\mathbf{A}\times\mathbf{A}}\{(a,a'),(b,a'),(b,b')\}$,
(4) test whether $S\cap(a/\delta\times\{b'\})$ is empty.

If ever we find an empty intersection in step (4), 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.

Finally, we analyze the time-complexity of the procedure just described, using the same notation and complexity bounds as those appearing in Section 4. Recall, $n=|A|$, and $m=\|\mathbf{A}\|=\sum_{i=0}^{r}k_in^i$, where k_i is the number of basic operations of arity i, and r is the largest arity of the basic operations of $\mathbf{A}$. The following assertions are consequences of (the proof of) Proposition 12: θ_{ab}, δ, and S are computable in time $O(rm)$, $O(rm^2+n^5)$, and $O(rm^2)$, respectively; θ_{ab} and δ are computed for each pair $(a,b)\in A^2$; S is computed for each triple of the form $((a,a'),(b,a'),(b,b'))\in(A\times A)^3$, and there are n^4 such triples. Thus, the computational complexity of the above procedure is $O(rm^2n^4+n^7)$. □

5.3. **Test for existence of a difference term.** The following proposition provides another avenue for constructing a polynomial-time algorithm to decide if a finite idempotent algebra generates a variety that has a difference term (cf. Theorem 13).

Proposition 17. *Let* $\mathbf{A}$ *be a finite idempotent algebra. Then* $\mathbb{V}(\mathbf{A})$ *has a difference term if and only if each 3-generated subalgebra of* $\mathbf{A}^2$ *has a difference term operation.*

Proof. Of course if $\mathbb{V}(\mathbf{A})$ has a difference term then each 3-generated subalgebra of $\mathbf{A}^2$ has a difference term operation. For the converse, we refer to the proof of Theorem 1 [Kea95, Theorem 3.8]. One part of this theorem establishes that if an algebra $\mathbf{B}$ is in a variety that has a difference term, then all type **2** minimal sets of $\mathbf{B}$ have empty tails. A careful reading of the proof of this fact shows that a weaker hypothesis will suffice, namely that all quotients of $\mathbf{B}$ have difference term operations. This is equivalent to just $\mathbf{B}$ having a difference term operation, since this property is preserved under taking quotients.

To complete the proof of this proposition, we use Corollary 10. Suppose that each 3-generated subalgebra of $\mathbf{A}^2$ has a difference term operation. Then, in particular, each 2-generated subalgebra of $\mathbf{A}$ does. This rules out that $\mathsf{HS}(\mathbf{A})$ contains an algebra that is term equivalent to the 2-element set. It also follows, from the previous paragraph, that no 3-generated subalgebra of $\mathbf{A}^2$ has a prime quotient of type **2** whose minimal sets have nonempty tails. □

mav 2018-08-13: This is true, I think. Should it be mentioned somewhere, as part of a general discussion of difference term operations?

Corollary 18. *There is a polynomial-time algorithm to decide if a finite idempotent algebra* $\mathbf{A}$ *generates a variety that has a difference term.*

Proof. By the previous proposition, it suffices to check whether each 3-generated subalgebra of $\mathbf{A}^2$ has a difference term operation. This can be decided by applying the algorithm from Corollary 16 at most $\binom{n^2}{3}$ ($\approx n^6$) times, so the total running time of this decision procedure is $O(rm^2n^{10} + n^{13})$ (cf. $O(rn^4m^4 + n^{14})$, the complexity of the difference term existence test of Theorem 13). □

6. Efficiently computing difference term tables

In this section we present a polynomial-time algorithm that takes a finite idempotent algebra $\mathbf{A}$ and constructs the Cayley table of a difference term operation for $\mathbf{A}$, if such a term exists.

The method consists of three subroutines. Algorithm 1 finds Cayley tables of LDT operations for sets of size 2, and Algorithm 2 calls Algorithm 1 repeatedly to find tables of LDT operations for larger and larger

sets up to size $n^2 + 1$. Finally, Algorithm 3 calls these subroutines in order to produce LDT operations for larger subsets of $A^2 \times \{0, 1\}$.

Some new notation will be helpful here. Suppose that $u \in \mathrm{Sg}^{\mathbf{A}}(X)$. Then there is a term t of some arity k that, when applied to a certain tuple of generators $(x_1, \dots, x_k)$, produces u. In this situation, we may ask for the operation table (or "Cayley table") for $t^{\mathbf{A}}$, which is an A^k-dimensional array whose $(a_1, \dots, a_k)$-entry is the value $t^{\mathbf{A}}(a_1, \dots, a_k)$. If $\mathtt{t}$ is such a table, we will denote the entry at position $(a_1, \dots, a_k)$ of the table by $\mathtt{t}[a_1, \dots, a_k]$. Alternatively, if we wish to emphasize the means by which we arrived at the term that the table represents, we may use $\mathtt{t}_{x_1,\dots,x_k|u}$ to denote the table.

6.1. **Base step.** The first step of our method finds a ternary operation on $\mathbf{A} \times \mathbf{A}$ that maps the element $((a, a'), (b, a'), (b, b'))$ into the set $a/[\theta_{ab}, \theta_{ab}] \times \{b'\}$. In other words, the first step finds a LDT operation for $\{(a, b, 0), (a', b', 1)\}$. When such an operation is found, its Cayley table—a 3-dimensional array $\mathtt{t}$ satisfying $\mathtt{t}[a, b, b] \ \delta \ a$ and $\mathtt{t}[a', a', b'] = b'$—is returned.

Algorithm 1: Generate the Cayley table of a LDT operation for $\{(a, b, 0), (a', b', 1)\}$

Input: $S = \{(a, b, 0), (a', b', 1)\}$
Output: Cayley table of an operation in $\mathcal{D}S$
compute $\delta = [\theta_{ab}, \theta_{ab}]$ and form $C = (a/\delta) \times \{b'\}$;
compute $S = \mathrm{Sg}^{\mathbf{A}\times\mathbf{A}}((a, a'), (b, a'), (b, b'))$;
forall $(u, v) \in S$ **do**
  compute the table $\mathtt{t}_{(a,a'),(b,a'),(b,b')|(u,v)}$;
  if $(u, v) \in C$ **then**
    return $\mathtt{t}_{(a,a'),(b,a'),(b,b')|(u,v)}$;
  end
end

Note that the subalgebra S in Algorithm 1 need not be computed in its entirety before the condition inside the **forall** loop is tested. Naturally, we test $(u, v) \in C$ as soon as the new element $(u, v) \in S$ is generated.

Let us now consider the computational complexity of Algorithm 1. Recall the notation introduced in Section 4;

$$n = |A|, \quad m = \|\mathbf{A}\| = \sum_{i=0}^{r} k_i n^i,$$
$$k_i = \text{ the number of basic operations of arity } i,$$
$$r = \text{ the largest arity of the basic operations of } \mathbf{A}.$$

Also, $\mathsf{t}_{(a,a'),(b,a'),(b,b')|(u,v)}$ denotes the Cayley table of a term operation that generates (u, v) from the set $\{(a, a'), (b, a'), (b, b')\}$.

Algorithm 1 can be implemented as follows:

(1) compute θ_{ab}, in time $O(rm)$;
(2) compute $C = a/[\theta_{ab}, \theta_{ab}] \times \{b'\}$, in time $O(rm^2 + n^5)$;
(3) generate $S = \mathrm{Sg}^{\mathbf{A}\times\mathbf{A}}\{(a, a'), (b, a'), (b, b')\}$, in time $O(rm^2)$;
for each newly generated $(u, v) \in S$,
- construct and store the table $\mathsf{t}_{(a,a'),(b,a'),(b,b')|(u,v)}$;
- if $(u, v) \in C$, then return $\mathsf{t}_{(a,a'),(b,a'),(b,b')|(u,v)}$;

Each element $(u, v) \in S$ is the result of applying some (say, k-ary) basic operation f to previously generated pairs (u_1, v_1), ..., (u_k, v_k) from S, and the operation tables generating these pairs were already stored (the first bullet of Step 3). Thus, to compute the table for the operation that produced $(u, v) = f((u_1, v_1), \dots, (u_k, v_k))$ we simply compose f with previously stored operation tables. Since all tables represent ternary operations, the time-complexity of this composition is $|A|^3$-steps multiplied by k reads per step; that is, $kn^3 \leqslant rn^3$. All told, the time-complexity of Algorithm 1 is $O(r^2m^2n^3 + n^5)$.

6.2. **Inductive stages.** The method is based on the proof of Theorem 14 and consists of n^2 stages, each of which makes n^2 calls to Algorithm 1.

Let $\ell := n^2 - 1$ and let $\{(a_0, b_0), (a_1, b_1), (a_2, b_2), \dots, (a_\ell, b_\ell)\}$ be an enumeration of the set A^2. For all $1 \leqslant k \leqslant n^2$, define

$$Z_k := \{(a_0, b_0, 0), (a_1, b_1, 0), \dots, (a_{k-1}, b_{k-1}, 0)\},$$
$$U_k := \{(a_0, b_0, 1), (a_1, b_1, 1), \dots, (a_{k-1}, b_{k-1}, 1)\}.$$

So $Z_{n^2} \cup U_{n^2} = A^2 \times \{0, 1\}$. The first stage of our procedure computes the Cayley table of a LDT operation for $Z_1 \cup U_{n^2} := \{(a_0, b_0, 0)\} \cup A^2 \times \{1\}$. The second stage does the same for $Z_2 \cup U_{n^2} := Z_1 \cup U_\ell \cup \{(a_1, b_1, 0)\}$. This continues for n^2 stages, after which we obtain a Cayley table of a LDT operation for $Z_{n^2} \cup U_{n^2} = A^2 \times \{0, 1\}$. There are n^2 stages, each stage consisting of n^2 steps (described below), and each step requiring a single call to Algorithm 1. Thus, the procedure makes

n^4 calls to Algorithm 1, and the total running-time is on the order of $r^2m^2n^7 + n^9$.

Here are the steps that Stage 1 takes in order to compute a LDT operation for $\{(a_0, b_0, 0), (a_0, b_0, 1), (a_1, b_1, 1), \dots, (a_\ell, b_\ell, 1)\}$.

(1) Compute the table t_1 of a LDT op for $\{(a_0, b_0, 0), (a_0, b_0, 1)\}$;

(2) compute the table s_1 of a LDT op for $\{(a_0, b_0, 0), (\mathsf{t}_1[a_1, a_1, b_1], b_1, 1)\}$; form the table $\mathsf{t}_2[x, y, z] = \mathsf{s}_1\big[\mathsf{t}_1[x, y, z], \mathsf{t}_1[y, y, z], z\big]$ $(\forall x, y, z)$;

(3) compute the table s_2 of a LDT op for $\{(a_0, b_0, 0), (\mathsf{t}_2[a_2, a_2, b_2], b_2, 1)\}$; form the table $\mathsf{t}_3[x, y, z] = \mathsf{s}_2\big[\mathsf{t}_2[x, y, z], \mathsf{t}_2[y, y, z], z\big]$ $(\forall x, y, z)$;

$\vdots$

(n^2) compute a table s_ℓ of a LDT op for $\{(a_0, b_0, 0), (\mathsf{t}_\ell[a_\ell, a_\ell, b_\ell], b_\ell, 1)\}$; form the table $\mathsf{t}_{n^2}[x, y, z] = \mathsf{s}_\ell\big[\mathsf{t}_\ell[x, y, z], \mathsf{t}_\ell[y, y, z], z\big]$ $(\forall x, y, z)$.

Let $\mathsf{d}_1 := \mathsf{t}_{n^2}$ denote the final result of Stage 1. It is not hard to check that d_1 is the table of a LDT operation for $Z_1 \cup U_{n^2}$. (See the proof of Theorem 14.)

Stage 2 is very similar to Stage 1; however, we first produce the table, d'_2, of a LDT operation for $\{(a_1, \mathsf{d}_1[a_1, b_1, b_1], 0)\} \cup U_{n^2}$, and then form the table $\mathsf{d}_2[x, y, z] := \mathsf{d}'_2\big[x, \mathsf{d}_1[x, y, y], \mathsf{d}_1[x, y, z]\big]$ $(\forall x, y, z \in A)$, which will be the table of a LDT operation for $Z_2 \cup U_{n^2}$. We continue in this way for n^2 stages of n^2 steps each, until we reach our goal: $\mathsf{d} := \mathsf{d}_{n^2}$, the Cayley table of a LDT operation for $Z_{n^2} \cup U_{n^2}$.

Without further ado, here is a precise description of an algorithm that carries out any one of the n^2 stages; the argument (a, b) determines which stage is executed.

Algorithm 2: Return the Cayley table of a LDT operation for $\{(a, b, 0)\} \cup U_{n^2}$

Input: A pair $(a, b) \in A^2$
Output: The Cayley table of a LDT op for $\{(a, b, 0)\} \cup U_{n^2}$.
Use Alg. 1 to compute the table t_1 of a LDT operation for $\{(a, b, 0), (a_0, b_0, 1)\}$;
forall $1 \leqslant i < n^2$ **do**
  Use Alg. 1 to compute the table s_i of a LDT operation for $\{(a, b, 0), (\mathsf{t}_i[a_i, a_i, b_i], b_i, 1)\}$
  Form the table t_{i+1}, defined as follows: $\forall x, y, z$, $\mathsf{t}_{i+1}[x, y, z] = \mathsf{s}_i\big[\mathsf{t}_i[x, y, z], \mathsf{t}_i[y, y, z], z\big]$;
end
return t_{n^2}

Lemma 19. *The output of Algorithm 2 is the Cayley table of a LDT operation for* $Z_1 \cup U_{n^2} := \{(a, b, 0), (a_0, b_0, 1), (a_1, b_1, 1), \dots, (a_\ell, b_\ell, 1)\}$.

Proof. This follows from the proof of Theorem 14. □

Algorithm 3: Return the Cayley table of a difference term operation for **A**

Output: d_{n^2}, the Cayley table of a LDT op for $A^2 \times \{0, 1\}$
Use Alg. 2 to compute the table d_0 of a LDT op for $Z_0 \cup U_{n^2}$;
forall $1 \leqslant k < n^2$ **do**
  Use Alg. 2 compute the table d'_{k+1} of a LDT operation for $\{(a_k, \mathsf{d}_k[a_k, b_k, b_k], 0)\} \cup U_{n^2}$;
  Form the table d_{k+1}, defined as follows: $\forall x, y, z$, $\mathsf{d}_{k+1}[x, y, z] := \mathsf{d}'_{k+1}\big[x, \mathsf{d}_k[x, y, y], \mathsf{d}_k[x, y, z]\big]$;
end
return d_{n^2}

Proposition 20. *The output of Algorithm 3 is the Cayley table of a LDT operation for* $A^2 \times \{0, 1\}$*, hence a difference term operation for* **A**.

Proof. This follows from Lemma 19 and the proof of Theorem 14. □

References

[FM87] Ralph Freese and Ralph McKenzie. *Commutator theory for congruence modular varieties*, volume 125 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1987. Online version available at: http://www.math.hawaii.edu/~ralph/papers.html.

[Fre08] Ralph Freese. Computing congruences efficiently. *Alg. Univ.*, 59:337–343, 2008.

[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.

[Hor13] Jonah Horowitz. Computational complexity of various Mal'cev conditions. *Internat. J. Algebra Comput.*, 23(6):1521–1531, 2013. URL: http://dx.doi.org/10.1142/S0218196713500343, doi:10.1142/S0218196713500343.

[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.

[KK99] Keith A. Kearnes and Emil W. Kiss. Modularity prevents tails. *Proc. Amer. Math. Soc.*, 127(1):11–19, 1999.

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

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

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

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

[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.

[Wil89] Ross David Willard. *Varieties having Boolean factor congruences*. ProQuest LLC, Ann Arbor, MI, 1989. Thesis (Ph.D.)–University of Waterloo (Canada).

Email address: williamdemeo@gmail.com
URL: http://williamdemeo.github.io

University of Colorado, Mathematics Dept, Boulder 80309, USA

Email address: ralph@math.hawaii.edu
URL: http://www.math.hawaii.edu/~ralph/

University of Hawaii, Mathematics Dept, Honolulu 96822, USA

Email address: matt@math.mcmaster.ca
URL: http://ms.mcmaster.ca/~matt/

McMaster University, Mathematics Dept, Hamilton L8S 4K1, CAN