On Deciding Existence of Difference Terms

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

***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 a related but easier question in the idempotent case. Using recent work of Valeriote and Willard as a guide, we define a "local difference term" and use this to prove a new theorem that yields a polynomial-time algorithm for deciding whether any finite idempotent algebra has a difference term operation. We hope this will lead to an efficient algorithm for determining whether the variety generated by such an algebra has a difference term.**

I. Introduction

Let $\mathcal{V}$ be a variety (equational class) of algebras. A ternary term d in the language of $\mathcal{V}$ is called a *difference term for* $\mathcal{V}$ if it satisfies the following: for all $\mathbf{A} = \langle A, \ldots \rangle \in \mathcal{V}$ and $a, b \in A$ we have

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

where θ is any congruence containing (a, b) and $[\cdot, \cdot]$ denotes the (term condition) commutator. (See [6] or [9] for definitions.) When the relations in (I.1) hold we will call $d^{\mathbf{A}}$ a *difference term operation* for $\mathbf{A}$.

Difference terms are studied extensively in the universal algebra literature. (See, for example, [6], [8], [9], [10], [11], [12].) There are many reasons to study difference terms, but one of the most obvious is that knowing a variety has a difference term allows us to deduce many useful properties of the algebras inhabiting that variety. (Very roughly speaking, having a difference term is slightly stronger than having a Taylor term and slightly weaker than having a Mal'tsev term. Note that if $\mathbf{A}$ is an *abelian* algebra—that is, $[1_A, 1_A] = 0_A$—then by the monotonicity of the commutator we have $[\theta, \theta] = 0_A$ for all $\theta \in \operatorname{Con} \mathbf{A}$, in which case (I.1) says that $d^{\mathbf{A}}$ is a Mal'tsev term operation.)

Digital computers have turned out to be invaluable tools for exploring and understanding algebras and the varieties they inhabit, and this is largely due to the fact that researchers have found ingenious ways to get computers to solve abstract decision problems—such as whether a variety is congruence-modular ([5]) or congruence-n-permutable ([14])—and to do so efficiently. The contribution of the present paper is to report progress toward a solution to the following:

Problem 1. Is there a polynomial-time algorithm that takes a finite idempotent algebra $\mathbf{A}$ as input and decides whether the variety generated by $\mathbf{A}$ has a difference term?

We solve the following easier problem:

Problem 2. Is there a polynomial-time algorithm that takes a finite idempotent algebra $\mathbf{A}$ as input and decides whether $\mathbf{A}$ has a difference term operation?

In [14], Valeriote and Willard define a "local Hagemann-Mitschke sequence" which they use as the basis of an efficient algorithm for deciding for a given n whether an idempotent variety is n-permutable. Inspired by that work, we devise a similar construct, called a "local difference term," that we use to develop a polynomial-time algorithm for deciding the existence of a (global) difference term operation.

II. Local Difference Terms

For the most part we use standard notation, definitions, and results of universal algebra, such as those found in [1]. However, we make a few exceptions for notational simplicity. For example, if $\mathbf{A} = \langle A, \ldots \rangle$ is an algebra with elements $a, b \in A$, then we use $\theta(a, b)$ to denote the congruence of $\mathbf{A}$ generated by a and b.

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

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

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

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

$$a_i\ [\theta(a_i, b_i), \theta(a_i, b_i)]\ p(a_i, b_i, b_i), \ \text{ if } \chi_i = 0, \text{ and} \tag{II.2}$$

$$p(a_i, a_i, b_i) = b_i, \ \text{ if } \chi_i = 1. \tag{II.3}$$

Under these hypothesis we will prove that every subset $S \subseteq \mathcal{S}$ has a local difference term. That is, there is a single term p that works (i.e., satisfies (II.2) and (II.3)) for all $(a_i, b_i, \chi_i) \in S$. The statement and proof of this new result follows.

Theorem II.1 (cf. [14, Theorem 2.2])**.** *Let $\mathcal{V}$ be an idempotent variety and $\mathbf{A} \in \mathcal{V}$. Define $\mathcal{S} = A \times A \times \{0, 1\}$ and suppose that every pair $((a_0, b_0, \chi_0), (a_1, b_1, \chi_1)) \in \mathcal{S}^2$ has a local difference term. Then every subset $S \subseteq \mathcal{S}$, has a local difference term.*

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

Since $|S| \geqslant 3$ and $\chi_i \in \{0, 1\}$ for all i, there must exist indices $i \neq j$ such that $\chi_i = \chi_j$. Assume without loss of generality that one of these indices is $j = 0$. Define the set $S' = S \setminus \{(a_0, b_0, \chi_0)\}$. Since $|S'| < |S|$, the set S' has a local difference term p. We split the remainder of the proof into two cases. In the first case $\chi_0 = 0$ and in the second $\chi_0 = 1$.

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

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

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

$$d(a_0, b_0, b_0) = t(a_0, p(a_0, b_0, b_0), p(a_0, b_0, b_0)) \; [\tau, \tau] \; a_0, \tag{II.4}$$

where we have used τ to denote $\theta(a_0, p(a_0, b_0, b_0))$. Note that $(a_0, p(a_0, b_0, b_0)) = (p(a_0, a_0, a_0), p(a_0, b_0, b_0))$ belongs to $\theta(a_0, b_0)$, so $\tau \leqslant \theta(a_0, b_0)$. Therefore, by monotonicity of the commutator, $[\tau, \tau] \leqslant [\theta(a_0, b_0), \theta(a_0, b_0)]$. It follows from this and (II.4) that

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

as desired.

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

$$\begin{aligned} d(a_i, a_i, b_i) &= t(a_i, p(a_i, a_i, a_i), p(a_i, a_i, b_i)) && \text{(II.5)} \\ &= t(a_i, a_i, b_i) && \text{(II.6)} \\ &= b_i. && \text{(II.7)} \end{aligned}$$

Equation (II.5) holds by definition of d, (II.6) because p is an idempotent local difference term for S', and (II.7) because t is a local difference term for T.

The remaining triples in our original set S have indices satisfying $k < j \leqslant n$ and $\chi_j = 0$. Thus, for these triples we want $d(a_j, b_j, b_j) \; [\theta(a_j, b_j), \theta(a_j, b_j)] \; a_j$. By definition,

$$d(a_j, b_j, b_j) = t(a_j, p(a_j, b_j, b_j), p(a_j, b_j, b_j)). \tag{II.8}$$

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

$$(p(a_j, b_j, b_j), a_j) \in [\theta(a_j, b_j), \theta(a_j, b_j)].$$

This and (II.8) imply that $(d(a_j, b_j, b_j), t(a_j, a_j, a_j))$ belongs to $[\theta(a_j, b_j), \theta(a_j, b_j)]$. Finally, by idempotence of t we have $d(a_j, b_j, b_j) \; [\theta(a_j, b_j), \theta(a_j, b_j)] \; a_j$, as desired.

Case 2: $\chi_0 = 1$. Without loss of generality, suppose $\chi_1 = \chi_2 = \cdots = \chi_k = 0$, and $\chi_{k+1} = \chi_{k+2} = \cdots = \chi_n = 1$. Define T to be the set

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

and note that $|T| < |S|$. Let t be a local difference term for T and define $d(x, y, z) = t(p(x, y, z), p(y, y, z), z)$. Since $\chi_0 = 1$, we want $d(a_0, a_0, b_0) = b_0$. By the definition of d,

$$d(a_0, a_0, b_0) = t(p(a_0, a_0, b_0), p(a_0, a_0, b_0), b_0) = b_0.$$

The last equality holds since t is a local difference term for T, thus, for $(p(a_0, a_0, b_0), b_0, 1)$.

If $1 \leqslant i \leqslant k$, then $\chi_i = 0$, so for these indices we want $d(a_i, b_i, b_i) \; [\theta(a_i, b_i), \theta(a_i, b_i)] \; a_i$. Again, starting from the definition of d and using idempotence of p, we have

$$\begin{aligned} d(a_i, b_i, b_i) &= t(p(a_i, b_i, b_i), p(b_i, b_i, b_i), b_i) \\ &= t(p(a_i, b_i, b_i), b_i, b_i). \end{aligned} \tag{II.9}$$

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

$$t(p(a_i, b_i, b_i), b_i, b_i) \; [\theta(a_i, b_i), \theta(a_i, b_i)] \; t(a_i, b_i, b_i). \tag{II.10}$$

Finally, since t is a local difference term for T, hence for (a_i, b_i, b_i), we have $t(a_i, b_i, b_i) \; [\theta(a_i, b_i), \theta(a_i, b_i)] \; a_i$. Combining this with (II.9) and (II.10) yields

$$d(a_i, b_i, b_i) \; [\theta(a_i, b_i), \theta(a_i, b_i)] \; a_i,$$

as desired.

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

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

as desired. □

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

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

III. The Algorithm

Corollary III.1. There is a polynomial-time algorithm that takes as input any finite idempotent algebra $\mathbf{A}$ and decides whether $\mathbf{A}$ has a difference term operation.

Proof. We describe an efficient algorithm for deciding, given a finite idempotent algebra $\mathbf{A}$, whether every pair $((a, b, i), (a', b', i')) \in (A \times A \times \{0, 1\})^2$ has a local difference term. By Corollary II.2, this will prove we can decide in polynomial-time whether $\mathbf{A}$ has a difference term operation.

Fix a pair $((a,b,i),(a',b',i'))$ in $(A\times A\times\{0,1\})^2$. If $i=i'=0$, then the first projection is a local difference term. If $i=i'=1$, then the third projection is a local difference term. The two remaining cases to consider are (1) $i=0$ and $i'=1$, and (2) $i=1$ and $i'=0$. Since these are completely symmetric, we only handle the first case. Assume the given pair of triples is $((a,b,0),(a',b',1))$. By definition, a term t is local difference term for this pair iff

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

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

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

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

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

Most of the operations carried out by this algorithm are well known to be polynomial-time. For example, that the running time of subalgebra generation is polynomial has been known for a long time (see [7]). The time complexity of congruence generation is also known to be polynomial (see [4]). The only operation whose tractability might be questionable is the commutator, but there is a straight-forward algorithm for computing it which, after the congruences have been computed, simply involves generating more subalgebras. □

More details on the complexity of operations carried out by the algorithm, as well as many other algebraic operations, can be found in the references mentioned, as well as [2], [3], [5].

ACKNOWLEDGMENT

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

REFERENCES

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

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

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

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

[5] 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.

[6] David Hobby and Ralph McKenzie. *The structure of finite algebras*, volume 76 of *Contemporary Mathematics*. American Mathematical Society, Providence, RI, 1988.

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

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

[13] 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.

[14] 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.