# A Polynomial-time Algorithm for 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 A in a finite language, can we efficiently decide whether the variety generated by A has a difference term? We answer this question affirmatively in the idempotent case by using recent work of Valeriote and Willard as a guide and defining a "local difference term. " We use this idea to prove a new theorem that we use as the basis of a polynomial-time algorithm for deciding, given finite idempotent algebra, whether the variety it generates 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 $\mathbf{A} = \langle A, \dots \rangle \in \mathcal{V}$ and $a, b \in A$ we have

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

where $\theta$ is any congruence containing $(a, b)$ and $[\cdot, \cdot]$ denotes the (term condition) commutator. (See [3] or [5] 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, [3], [4], [5], [6], [7], [8].) 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 ([2]) or congruence-$n$-permutable ([10])—and to do so efficiently. In the present paper we add to the algorithmic arsenal by solving the following:

**Problem.** 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?

Let $\mathbf{p} = (p_0, p_1, \dots, p_n)$ be an $(n + 1)$-tuple of ternary terms, where $p_0(x, y, z) \approx x$ and $p_n(x, y, z) \approx z$, the first and third ternary projections, respectively. Let $\mathbf{A} = \langle A, \dots \rangle$ be an algebra. In [10], Valeriote and Willard define an $\mathbf{A}$*-triple for* $\mathbf{p}$ to be a triple $(a, b, i)$ such that $a, b \in A$ and $p_i(a, b, b) = p_{i+1}(a, a, b)$. They use this to define a "local Hagemann-Mitschke sequence" on which they base an efficient algorithm for deciding for a given $n$ whether an idempotent variety is $n$-permutable. Taking this as our inspiration, we devise a similar construct, which we call a "local difference term," and use it to develop a polynomial-time algorithm for deciding the existence of a (global) difference term.

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

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

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

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

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

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. [10, 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 $S = \{(a_0, b_0, \chi_0), (a_1, b_1, \chi_1), \dots, (a_n, b_n, \chi_n)\} \subseteq \mathcal{S}$, so that $|S| = n + 1$. We prove $S$ has a local difference term.

Since $|S| \geqslant 3$ and $\chi_i \in \{0, 1\}$ for all $i$, there must exist indices $i \neq j$ such that $\chi_i = \chi_j$. Assume without loss of generality that one of these indices is $j = 0$. Define the set $S' = S \setminus \{(a_0, b_0, \chi_0)\}$. Since $|S'| < |S|$, the set $S'$ has a local difference term $p$. We split the remainder of the proof into two cases. 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 $T = \{(a_0, p(a_0, b_0, b_0), 0), (a_1, b_1, 1), (a_2, b_2, 1), \dots, (a_k, b_k, 1)\}$, and note that $|T| < |S|$. Let $t$ be a local difference term for $T$. Define

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

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 $\tau$ 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

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

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

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

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

If $1 \leqslant i \leqslant k$, then $\chi_i = 0$, so for these indices we 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

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

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. $\square$

**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 $(a, b, 1)$. $\square$

**Corollary II.3.** There is a polynomial-time algorithm that takes as input any finite idempotent algebra $\mathbf{A}$ and decides whether the variety $\mathbb{V}(\mathbf{A})$ that it generates has a difference term.

*Proof.* Let $\mathbf{A}$ be a finite idempotent algebra and let $\mathcal{V} = \mathbb{V}(\mathbf{A})$. We describe a polynomial-time algorithm for deciding whether the hypothesis of Corollary II.2 holds for $\mathbf{A}$, thereby proving that we can decide in polynomial-time whether there is a difference term operation for $\mathbf{A}$. We will then complete the proof by explaining why $\mathbf{A}$ has a difference term operation iff the variety it generates has a difference term.

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

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

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

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

where $\delta = [\theta(a, b), \theta(a, b)]$ and $a/\delta$ denotes the $\delta$-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.

Finally, we observe that if $\mathbf{A}$ has a difference term operation, then the variety it generates has a difference term. $\square$

TODO: justify the last sentence of the last proof.

## Acknowledgment

The author would like to thank Ralph Freese for proposing this project and for recommending 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. Their 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] 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.

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

[10] 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.