Complexity of testing for a difference term in idempotent algebras

William DeMeo, Ralph Freese, Matt Valeriote

http://math.hawaii.edu/∼ralph/

http://uacalc.org/

https://github.com/UACalc/

Algebras and Algorithms, University of Hawaii, May 18–20, 2018

Difference Terms

Definition

A *difference term* for a variety $\mathcal{V}$ is a ternary term d in the language of $\mathcal{V}$ that satisfies the following: if $\mathbf{A} \in \mathcal{V}$, 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*.

Difference Terms

Definition

A *difference term* for a variety $\mathcal{V}$ is a ternary term d in the language of $\mathcal{V}$ that satisfies the following: if $\mathbf{A} \in \mathcal{V}$, 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*.

Theorem (Kearnes)

*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.*

Difference Terms

Definition

A *difference term* for a variety $\mathcal{V}$ is a ternary term d in the language of $\mathcal{V}$ that satisfies the following: if $\mathbf{A} \in \mathcal{V}$, 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*.

Theorem (Kearnes, short version)

*The variety $\mathcal{V} = \mathbb{V}(\mathbf{A})$ generated by a finite algebra $\mathbf{A}$ has a difference if and only if $\mathcal{V}$ has no **1**'s and no type **2** tails.*

Congruence Modularity (CM)

Theorem (Hobby-McKenzie, short version)

*The variety $\mathcal{V} = \mathbb{V}(\mathbf{A})$ generated by a finite algebra $\mathbf{A}$ is CM if and only if $\mathcal{V}$ has no **1**'s, no **5**'s, and no tails.*

Congruence Modularity (CM)

Theorem (Hobby-McKenzie, short version)

The variety $\mathcal{V} = \mathbb{V}(\mathbf{A})$ generated by a finite algebra $\mathbf{A}$ is CM if and only if $\mathcal{V}$ has no ***1****'s, no* ***5****'s, and no tails.*

Given $\mathbf{A}$ finite, how hard is it to decide if $\mathbb{V}(\mathbf{A})$ is CM?

Congruence Modularity (CM)

Theorem (Hobby-McKenzie, short version)

*The variety $\mathcal{V} = \mathbb{V}(\mathbf{A})$ generated by a finite algebra $\mathbf{A}$ is CM if and only if $\mathcal{V}$ has no **1**'s, no **5**'s, and no tails.*

Given $\mathbf{A}$ finite, how hard is it to decide if $\mathbb{V}(\mathbf{A})$ is CM?

Answer: EXPTIME-complete.

Congruence Modularity (CM)

Theorem (Hobby-McKenzie, short version)

*The variety $\mathcal{V} = \mathbb{V}(\mathbf{A})$ generated by a finite algebra $\mathbf{A}$ is CM if and only if $\mathcal{V}$ has no **1**'s, no **5**'s, and no tails.*

Given $\mathbf{A}$ finite, how hard is it to decide if $\mathbb{V}(\mathbf{A})$ is CM?

Answer: EXPTIME-complete.

But if $\mathbf{A}$ is idempotent, it is Polynomial time.

Congruence Modularity (CM)

Theorem (Hobby-McKenzie, short version)

The variety $\mathcal{V} = \mathbb{V}(\mathbf{A})$ generated by a finite algebra **A** *is CM if and only if $\mathcal{V}$ has no* ***1****'s, no* ***5****'s, and no tails.*

Given **A** finite, how hard is it to decide if $\mathbb{V}(\mathbf{A})$ is CM?

Answer: EXPTIME-complete.

But if **A** is idempotent, it is Polynomial time.

Do these results hold for testing if $\mathbb{V}(\mathbf{A})$ has a difference term?

Congruence Modularity (CM)

Theorem (Hobby-McKenzie, short version)

*The variety $\mathcal{V} = \mathbb{V}(\mathbf{A})$ generated by a finite algebra $\mathbf{A}$ is CM if and only if $\mathcal{V}$ has no **1**'s, no **5**'s, and no tails.*

Given $\mathbf{A}$ finite, how hard is it to decide if $\mathbb{V}(\mathbf{A})$ is CM?

Answer: EXPTIME-complete.

But if $\mathbf{A}$ is idempotent, it is Polynomial time.

Do these results hold for testing if $\mathbb{V}(\mathbf{A})$ has a difference term?
Yes.

Difference Term

Theorem

Let **A** *finite and idempotent,* $\mathcal{V} = \mathbb{V}(\mathbf{A})$*. Then* $\mathcal{V}$ *has a difference term if and only if the following conditions hold:*

1. $\mathcal{V}$ *omits TCT-type* ***1****.*

Difference Term

Theorem

Let $\mathbf{A}$ *finite and idempotent,* $\mathcal{V} = \mathbb{V}(\mathbf{A})$*. 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* $\mathbf{B} := \operatorname{Sg}^{\mathbf{A}}(a, b, c)$ *and* $\mathbf{C} := \operatorname{Sg}^{\mathbf{B}^2}\left(\{(a, b), (a, c), (b, c)\} \cup 0_{\mathbf{B}}\right)$*:*
    1. $\beta := \operatorname{Cg}^{\mathbf{B}}(a, b)$ *is join irreducible with lower cover* α*,*
    2. $((a, b), (b, b)) \notin (\alpha_0 \wedge \alpha_1) \vee \operatorname{Cg}^{\mathbf{C}}((a, c), (b, c))$*, and*
    3. $[\beta, \beta] \leq \alpha$*.*

Difference Term

Theorem

Let $\mathbf{A}$ *finite and idempotent,* $\mathcal{V} = \mathbb{V}(\mathbf{A})$*. 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* $\mathbf{C} := \mathrm{Sg}^{\mathbf{B}^2}\left(\{(a, b), (a, c), (b, c)\} \cup 0_{\mathbf{B}}\right)$*:*
    1. $\beta := \mathrm{Cg}^{\mathbf{B}}(a, b)$ *is join irreducible with lower cover* α*,*
    2. $((a, b), (b, b)) \notin (\alpha_0 \wedge \alpha_1) \vee \mathrm{Cg}^{\mathbf{C}}((a, c), (b, c))$*, and*
    3. $[\beta, \beta] \leq \alpha$*.*
3. *Next slide.*

The third item

- 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 $t := (x_0, y_1)$:
  1. $\beta := \mathrm{Cg}^{\mathbf{B}}(0, 1)$ is join irreducible with lower cover α,
  2. $\rho_0 \vee \alpha = 1_{\mathbf{B}}$, and
  3. the type of β over α is **2**.

Complexity

If **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

$$n = |\mathbf{A}| \qquad m = ||\mathbf{A}||$$

$$r = \text{the largest arity of the operations of } \mathbf{A}$$

Complexity

Theorem (F-V + B-K-P-S)

Let $\mathcal{V}$ be the variety generated by a finite, idempotent algebra $\mathbf{A}$. The time needed to test:

- *if $\mathcal{V}$ has a Taylor term is at most crn^3m;*
- *if $\mathcal{V}$ is CM is at most crn^4m^2;*
- *if a prime interval in $\mathbf{Con}(\mathbf{A})$ has type $\mathbf{2}$ is at most crm^3.*

Corollary

Testing for a difference term takes time at most crn^4m^6.

Question: Can we the commutator to speed up the third item?

Complexity

Theorem

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* $\operatorname{Sg}^{\mathbf{A}}(S)$ *can be computed in time*

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

Complexity

Theorem

Let **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 time*

$$c\,r\,||\mathbf{A}|| = crm.$$

Complexity of Computing $[\alpha, \beta]$

$M(\alpha, \beta)$ is 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

$$\text{if } \begin{bmatrix} x & y \\ u & v \end{bmatrix} \text{ is in } M(\alpha, \beta) \text{ and } x \, \gamma \, y, \text{ then } u \, \gamma \, v. \tag{2}$$

Complexity of Computing $[\alpha, \beta]$

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 $\delta_1 \leq \delta$.

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

Clearly, $\delta_1 \leq \delta_2 \leq \cdots \leq \delta$ and so $\bigvee_i \delta_i \leq \delta$. In fact, they are equal.

Complexity of Computing $[\alpha, \beta]$

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 $\delta_1 \leq \delta$.

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

Clearly, $\delta_1 \leq \delta_2 \leq \cdots \leq \delta$ and so $\bigvee_i \delta_i \leq \delta$. In fact, they are equal.
Time: a constant time

$$rm^4 + n(n^4 + rm)$$

Complexity of Computing $[\alpha, \beta]$

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 $\delta_1 \leq \delta$.

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

Clearly, $\delta_1 \leq \delta_2 \leq \cdots \leq \delta$ and so $\bigvee_i \delta_i \leq \delta$. In fact, they are equal.

Time: a constant time

$$rm^4 + n(n^4 + rm)$$

We can assume **A** is not unary. So the time is a constant times

$$rm^4.$$

Complexity of Computing $[\alpha, \beta]$

The columns of $M(\alpha, \beta)$ are elements of $\mathbf{A}(\alpha)$, the subalgebra of $\mathbf{A} \times \mathbf{A}$ whose coordinates are α-related.

Complexity of Computing $[\alpha, \beta]$

The columns of $M(\alpha, \beta)$ are elements of $\mathbf{A}(\alpha)$, the subalgebra of $\mathbf{A} \times \mathbf{A}$ whose coordinates are α-related.
Viewing $M(\alpha, \beta)$ as a relation on $\mathbf{A}(\alpha)$, Let

$$\Delta_{\alpha,\beta}$$

be the congruence generated by it.
Can we use $\Delta_{\alpha,\beta}$ in place of $M(\alpha, \beta)$ in the algorithm?

Complexity of Computing $[\alpha, \beta]$

The columns of $M(\alpha, \beta)$ are elements of $\mathbf{A}(\alpha)$, the subalgebra of $\mathbf{A} \times \mathbf{A}$ whose coordinates are α-related.
Viewing $M(\alpha, \beta)$ as a relation on $\mathbf{A}(\alpha)$, Let

$$\Delta_{\alpha,\beta}$$

be the congruence generated by it.
Can we use $\Delta_{\alpha,\beta}$ in place of $M(\alpha, \beta)$ in the algorithm?
No.

Complexity of Computing $[\alpha, \beta]$

The columns of $M(\alpha, \beta)$ are elements of $\mathbf{A}(\alpha)$, the subalgebra of $\mathbf{A} \times \mathbf{A}$ whose coordinates are α-related.
Viewing $M(\alpha, \beta)$ as a relation on $\mathbf{A}(\alpha)$, Let

$$\Delta_{\alpha,\beta}$$

be the congruence generated by it.
Can we use $\Delta_{\alpha,\beta}$ in place of $M(\alpha, \beta)$ in the algorithm?
No. But **yes** if **A** has a Taylor term and $[\alpha, \beta] = [\beta, \alpha]$.

Theorem (Kearnes-Szendrei)

If **A** *has a Taylor term, then* $[\alpha, \beta]_s = [\alpha, \beta]_\ell$.

Complexity of Computing $[\alpha, \beta]$

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, $i = 0, \ldots, k$, 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 $\beta \subseteq \beta^*$.

Complexity of Computing $[\alpha, \beta]$

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, $(c, d) \in [\alpha^*, \beta^*]\big|_A = [\alpha, \beta]$.

Complexity of Computing $[\alpha, \beta]$

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, $(c, d) \in [\alpha^*, \beta^*]\big|_A = [\alpha, \beta]$.

Corollary

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.*