Deciding Maltsev Conditions

Matt Valeriote

McMaster University

30 May 2015

Maltsev Conditions

Definition

- A strong Maltsev condition $\mathcal{S}$ consists of a finite set of function symbols $\{f_i\}_{i \in I}$ of various arities along with a finite set of equations Σ involving terms over the f_i.
- An algebra $\mathbf{A}$ satisfies $\mathcal{M}$ if it has terms $\{t_i\}_{i \in I}$ such that

$$\langle A, \{t_i^{\mathbf{A}}\}_{i \in I} \rangle \models \Sigma.$$

- A Maltsev condition $\mathcal{M}$ consists of a sequence $\mathcal{S}_i$, $i \geq 1$, of strong Maltsev conditions such that for all i, the condition $\mathcal{S}_i$ is stronger than the condition $\mathcal{S}_{i+1}$. An algebra satisfies $\mathcal{M}$ if it satisfies $\mathcal{S}_i$ for some i.
- A Maltsev condition is linear if none of the equations used to define it involve compositions.
- A Maltsev condition is idempotent if the equations defining it imply that all of the functions that appear in the definition are idempotent.
- A Maltsev condition is special if it is strong, idempotent, and linear.

Congruence Distributivity

Definition

For $k > 1$, let $CD(k)$ be the special Maltsev condition defined by the equations:

$$\begin{aligned}
p_0(x, y, z) &\approx x \\
p_i(x, y, x) &\approx x \text{ for all } i \\
p_i(x, x, y) &\approx p_{i+1}(x, x, y) \text{ for all } i \text{ even} \\
p_i(x, y, y) &\approx p_{i+1}(x, y, y) \text{ for all } i \text{ odd} \\
p_k(x, y, z) &\approx z
\end{aligned}$$

Theorem (Jónsson)

$\mathcal{V}$ is congruence distributive (CD) if and only if it satisfies $CD(k)$ for some $k > 1$.

Testing for Maltsev conditions

Three decision problems

Let $\mathcal{M}$ be a Maltsev condition.

- ($\mathrm{SAT}_{\mathcal{M}}$) **Instance**: A finite algebra $\mathbf{A}$.
  Question: Does $\mathbf{A}$ satisfy $\mathcal{M}$?
- ($\text{Id-Sat}_{\mathcal{M}}$) **Instance**: A finite idempotent algebra $\mathbf{A}$.
  Question: Does $\mathbf{A}$ satisfy $\mathcal{M}$?
- ($\text{Rel-Sat}_{\mathcal{M}}$) **Instance**: A finite relational structure $\mathbb{B}$.
  Question: Does $\langle B, \mathrm{Pol}(\mathbb{B})\rangle$ satisfy $\mathcal{M}$?

Related questions

For a Maltsev condition $\mathcal{M}$, what are the computational complexities of the three decision problems $\mathrm{SAT}_{\mathcal{M}}$, $\text{Id-Sat}_{\mathcal{M}}$, and $\text{Rel-Sat}_{\mathcal{M}}$?

Back to congruence distributivity

Remark

There is a straightforward algorithm that demonstrates that for any $k > 1$, $SAT_{CD(k)}$ and SAT_{CD} are in EXP-TIME: Compute the free algebra in $\mathbf{V}(\mathbf{A})$ generated by $\{x, y, z\}$ and look for a sequence of terms that satisfy the condition.

Theorem (Freese-Val., Horowitz ($k = 3$ case))

- *SAT_{CD} is EXP-TIME complete.*
- *For a fixed $k > 2$, $SAT_{CD(k)}$ is EXP-TIME complete*

The Clone Membership Problem

Remark

The principle tool that we use to establish hardness is the following EXP-TIME complete problem (shown by Bergman, Juedes, and Slutzki and also by H. Friedman).

Theorem (Clone Membership Problem)

The following decision problem is EXP-TIME complete:

- **Instance:** *A finite algebra* $\mathbf{A} = (A, f_1, \dots, f_k)$ *and a function* g *on* A.
- **Question:** *Is* g *in the clone of operations on* A *generated by* $\{f_1, \dots, f_k\}$*, i.e., can* g *be obtained by composing the* f_i *in some fashion?*

A general purpose construction

Remark

We came up with a construction that takes an instance I of the Clone Membership Problem and builds a finite algebra $\mathbf{A}_I$ such that:

- *If I is a* **no** *instance, then $\mathbf{A}_I$ has no non-trivial idempotent term operations, and*
- *If I is a* **yes** *instance, then $\mathbf{A}_I$ has a flat semi-lattice term operation and also the operation $(x \wedge y) \vee (x \wedge z)$.*

Theorem

Testing for any of the following conditions is an EXP-TIME complete: Given a finite algebra $\mathbf{A}$:

- *Does $\mathbf{A}$ have a nontrivial idempotent term operation or a Taylor (or Siggers) term?*
- *Does $\mathbf{A}$ have a (flat) semi-lattice term operation?*
- *Does $\mathbf{A}$ generate a variety that is CD or CM or SD($\vee$) or SD($\wedge$)?*

Is SAT$_{\mathcal{M}}$ always hard?

Remarks

- *For any strong Maltsev condition $\mathcal{M}$, SAT$_{\mathcal{M}}$ is in EXP-TIME (just look for suitable terms by building the appropriate free algebras).*
- *Challenge: Find some strong, idempotent, non-trivial Maltsev condition $\mathcal{M}$ such that SAT$_{\mathcal{M}}$ is* **not** *EXP-TIME complete.*

Problems

- What is the complexity of testing for a Maltsev term or a majority term or a Pixley term?
- If $\mathcal{M}$ is a non-trivial special Maltsev condition, is SAT$_{\mathcal{M}}$ EXP-TIME complete?

The idempotent case

Remark

It turns out that for many familiar idempotent linear Maltsev conditions $\mathcal{M}$, it can be shown that Id-SAT$_{\mathcal{M}}$ is in **P**.

Theorem

Id-SAT$_{\mathcal{M}}$ is in **P** *for $\mathcal{M}$ any one of the following Maltsev conditions:*

- *(Bulatov) Having a Taylor term (or omitting the unary type),*
- *(Freese, Val.) one of the other five "type omitting" conditions from tame congruence theory,*
- *(Freese, Val.) CM, CD, having a majority or Maltsev term,*
- *(Val., Willard) for a fixed $k > 2$, congruence k-permutability,*
- *(Kazda, Val.) for a fixed $k > 1$, CD(k) and CM(k),*
- *(BKMMN) for a fixed $k > 1$, having a cyclic term of arity k,*
- *(Horowitz) for a fixed $k > 1$, having a k-edge term.*

The Idempotent Case

Remarks

- *A number of the results from the previous theorem can be proved by "localizing" a failure of the condition in a small subalgebra of a small power of the given idempotent algebra.*
- *For example, a finite idempotent algebra* $\mathbf{A}$ *generates a* $CD(k)$ *variety if and only if every 3-generated subalgebra of* $\mathbf{A}^{2k-1}$ *is congruence distributive.*

Theorem (Bulatov)

If $\mathbf{A}$ *is a finite idempotent algebra, then* $\mathbf{A}$ *has a Taylor term if and only if the class* $\mathbf{HS}(\mathbf{A})$ *does not contain a 2-element set.*

Omitting the unary type

Proof.

- By Taylor's result, if $\mathbf{A}$ fails to have a Taylor term then $\mathbf{V}(\mathbf{A})$ contains an algebra that is essentially a set, so it contains a 2-element set T, considered as an algebra.
- Choose n minimal so that T is isomorphic to a quotient of a subalgebra of $\mathbf{A}^n$, say $T \approx \mathbf{S}/\theta$ for some $\theta \in \mathrm{Con}\,(\mathbf{S})$ and $\mathbf{S} \leq \mathbf{A}^n$.
- For $a \in A$, let $S_a = \{(a_1, a_2, \ldots, a_n) \in S \,:\, a_1 = a\} \leq S$.
- If for some $a \in A$, S_a is not contained in a θ-class, then $\mathbf{S}_a/\theta \approx T$, and we can reduce n by 1.
- Otherwise, $\pi_1 \subseteq \theta$ and so $\mathbf{T}$ is isomorphic to a quotient of $\mathbf{A}$.

$\square$

Testing for Maltsev Conditions: An Example

Cyclic Terms

A term t is cyclic if it is idempotent and satisfies the identity $t(x_1, x_2, \ldots, x_n) \approx t(x_2, x_3, \ldots, x_n, x_1)$.

Theorem (BKMMN)

For $n > 1$ there is a polynomial time algorithm to determine if a given finite idempotent algebra has an n-ary cyclic term.

The case $n = 4$

Remark

We need to determine if our finite idempotent algebra $\mathbf{A}$ *has a 4-ary term operation* $c(x, y, z, w)$ *such that for all* $\vec{a} = (a_1, a_2, a_3, a_4) \in A^4$,

$$c(a_1, a_2, a_3, a_4) = c(a_2, a_3, a_4, a_1) = \cdots = c(a_4, a_1, a_2, a_3).$$

Definition

- A 4-ary term operation c is cyclic for a tuple $\vec{a} = (a_1, a_2, a_3, a_4) \in A^4$, if $c(a_1, a_2, a_3, a_4) = c(a_2, a_3, a_4, a_1) = \cdots = c(a_4, a_1, a_2, a_3)$.
- For $S \subseteq A^4$, the term operation c is cyclic for S if it is cyclic for each member of S.

Remark

So, $\mathbf{A}$ *has a cyclic term if and only if it has a term that is cyclic for* A^4.

The case $n = 4$

Lemma

If for each $\vec{a} \in A^4$, $\mathbf{A}$ has a term that is cyclic for $\vec{a}$ then it has a cyclic term.

Proof.

- We show by induction on $|S|$, for $S \subseteq A^4$, that $\mathbf{A}$ has a term that is cyclic for S. The case $|S| = 1$ is given.
- Suppose that $S' = S \cup \{\vec{a}\}$ and c_S is cyclic for S.
- Set $b_1 = c_S(a_1, a_2, a_3, a_4)$, $b_2 = c_S(a_2, a_3, a_4, a_1)$, $b_3 = c_S(a_3, a_4, a_1, a_2)$, and $b_4 = c_S(a_4, a_1, a_2, a_3)$.
- Let $c_{\vec{b}}$ be cyclic for $\vec{b}$ and set $c(x_1, x_2, x_3, x_4)$ to be the term operation

$$c_{\vec{b}}(c_S(x_1, x_2, x_3, x_4), c_S(x_2, x_3, x_4, x_1), \ldots, c_S(x_4, x_1, x_2, x_3)).$$

- Then c is cyclic for S'.

$\square$

The case $n = 4$

Remark

So, to determine if $\mathbf{A}$ *has a 4-ary cyclic term operation, it suffices to determine if, for each* $\vec{a} \in A^4$*, it has a term operation that is cyclic for* $\vec{a}$*.*

Lemma

For $\vec{a} \in A^4$*,* $\mathbf{A}$ *has a term that is cyclic for* $\vec{a}$ *if and only if the subalgebra of* $\mathbf{A}^4$ *generated by*

$$\{(a_1, a_2, a_3, a_4), (a_2, a_3, a_4, a_1), \ldots, (a_4, a_1, a_2, a_3)\}$$

contains a constant 4-tuple.

Corollary

There is a polynomial time algorithm to determine if a given finite idempotent algebra has a 4-ary cyclic term operation.

Is Id-SAT$_{\mathcal{M}}$ always easy?

Remarks

- *There is a lot of evidence to support the claim (conjecture!!!) that if $\mathcal{M}$ is a special Maltsev condition, then Id-SAT$_{\mathcal{M}}$ is in* **P**, *but,*
- *there are a lot of gaps in our knowledge.*
- *Challenge: Find some special Maltsev condition $\mathcal{M}$ such that Id-SAT$_{\mathcal{M}}$ is* **not** *in* **P**.

Problems

For **A** a finite idempotent algebra,

- what is the complexity of testing for a minority term?
- what is the complexity of testing, for a fixed $k > 2$, for a k-ary totally symmetric term?

A non-linear example

Remarks

- *One of the simplest strong, idempotent non-linear Maltsev conditions is that of having a semi-lattice term.*
- *What is the complexity of testing for this condition?*
- *Recall that in general, this is an EXP-TIME complete problem, and even checking for a flat semi-lattice operation is EXP-TIME complete.*

Guess

Even for idempotent algebras, this problem is EXP-TIME complete.

Wild Guess

If $\mathcal{M}$ is a strong idempotent non-linear Maltsev condition that is not equivalent to a special Maltsev condition, then Id-SAT$_{\mathcal{M}}$ is EXP-TIME complete.

The semi-lattice case

Example (Freese, Nation, Val.)

For each $n > 1$, we build an idempotent (conservative!) algebra $\mathbf{A}_n$ of size $2n$ such that for each subset $S \subset A_n$ of size $2n-1$ there is a term $b_S(x, y)$ of $\mathbf{A}_n$ such that when restricted to S, b_S is a semi-lattice operation with respect to a linear ordering on S, **but** $\mathbf{A}_n$ does not have a semi-lattice term operation.

Partial Results

- The problem of deciding if a finite idempotent algebra has a flat semi-lattice term operation is in $\mathbf{P}$.
- The problem of deciding if a finite idempotent algebra has an "M_n" semi-lattice operation is EXP-TIME complete.

The Relational case

Remarks

- *For $\mathcal{M}$ a strong Maltsev condition, the problem Rel-Sat$_{\mathcal{M}}$ is always in* **NP**.
- *For some special Maltsev conditions, there is a close association with the* CSP.

Theorem

Let $\mathcal{M}$ be a special Maltsev condition that implies $SD(\wedge)$. Then Rel-Sat$_{\mathcal{M}}$ is in **P**.

Corollary

For relational structures, testing for a majority polymorphism, or, for a fixed $k > 2$, a k-ary near unanimity polymorphism, is in **P**.

Special Maltsev conditions that imply SD($\wedge$)

Proof of the majority case

- Given a finite relational structure $\mathbb{A}$, we may assume that it contains, for each $a \in A$, the singleton unary relation $\{a\}$.
- Let I be the instance of CSP($\mathbb{A}$) with variables A^3 and with the following constraints:
  - for a, $b \in A$, $\langle((a,a,b)),\{a\}\rangle$, $\langle((a,b,a)),\{a\}\rangle$, $\langle((b,a,a)),\{a\}\rangle$,
  - for each k-ary relation R of $\mathbb{A}$ and tuples $\vec{u}_1$, $\vec{u}_2$, $\vec{u}_3 \in R$, $\langle((u_1^1,u_2^1,u_3^1),\dots,(u_1^k,u_2^k,u_3^k)),R\rangle$.
- Then $\mathbb{A}$ has a majority term polymorphism if and only if I has a solution.
- Now, we run the SD($\wedge$) CSP algorithm on I.
- If the algorithm determines that I doesn't have a solution, then $\mathbb{A}$ doesn't have a majority term polymorphism.

Special Maltsev conditions that imply SD($\wedge$)

Proof of the majority case

- If the algorithm determines that there is a solution, this may not be true, if $\mathbb{A}$ doesn't have an SD($\wedge$) polymorphism.
- Choose some triple $\vec{u} \in A^3$ and some $d \in A$ and add the constraint $\langle (\vec{u}), \{d\} \rangle$ to I. Then rerun the CSP algorithm on I.
- If it determines that there is no solution, then choose some other element in place of d and rerun the algorithm.
- If no choice of d yields a positive result, then we conclude that $\mathbb{A}$ has no majority polymorphism.
- If some value of d works, then move on to another triple $\vec{u}'$ from A^3 and augment I with a constraint $\langle (\vec{u}), \{d\} \rangle$ for some $d \in A$ and rerun the algorithm.
- In the end, after all triples have been considered, we will end up with a ternary function on A that will be a majority operation on A that is a polymorphism of $\mathbb{A}$ if and only if $\mathbb{A}$ has one.

The Relational case

Remark

Any special Maltsev condition can be coded up as a particular instance of CSP($\mathbb{A}$) *but this appears to break down for conditions that are not linear.*

Maltsev polymorphism

- If there is a uniform, polynomial-time algorithm to solve instances of the CSP over Maltsev templates (Willard, 2016???) then the above ideas can be used to prove that the problem of deciding if a finite relational structure has a Maltsev polymorphism is in **P**.
- Conversely, if there is an algorithm which, given a finite relational structure, produces a Maltsev polymorphism of it, if it has one, then there is a uniform polynomial-time algorithm to solve instances of the CSP over Maltsev templates.

More Problems

Problems

- For $\mathcal{M} =$ omitting the unary type, what is the complexity of Rel-Sat$_{\mathcal{M}}$?
- If $\mathcal{M}$ is a special Maltsev condition, is Rel-Sat$_{\mathcal{M}}$ in **P**?
- What about when $\mathcal{M}$ is not linear?
- When $\mathcal{M} =$ having a semi-lattice term?

UACALC

Remarks

- *Over the past 20 years a package of computational tools for investigating finite algebras and the varieties that they generate has been developed.*
- *It is currently being maintained by Ralph Freese and William DeMeo and can be freely downloaded from the website http://uacalc.org.*
- *In addition to the program, a large library of java code is also available.*
- *Contributions and suggestions from the community are always welcome.*