Decidability in Universal Algebra

Matthew Moore

McMaster University

March 10, 2017

Decidability

Definition

The **decision problem** for property $P(\cdot)$ is the computational problem

Input: some finite object A.

Output: whether $P(A)$ is true.

If there is an algorithm which solves this problem, then $P(\cdot)$ is **decidable**. Otherwise $P(\cdot)$ is otherwise is **undecidable**.

Example

The **halting problem** is the decision problem

Input: a program P.

Output: whether P eventually halts.

The halting problem is famously undecidable.

General strategy: encode the halting problem into $P(\cdot)$.

Known results (in Universal Algebra)

The following are known to be undecidable for finite algebra $\mathbb{A}$:

- Whether $\mathbb{A}$ has a finite residual bound [McKenzie].
  - strategy: encode Turing machine $\mathcal{T}$ into special $\mathbb{A}(\mathcal{T})$.
- Whether $\mathbb{A}$ has a finite equational base [McKenzie; Willard].
  - McKenzie: new algebra $\mathbb{F}(\mathcal{T})$.
  - Willard: $\mathbb{A}(\mathcal{T})$ above works!
- Whether $\mathbb{A}$ has definable principal subcongruences [M].
  - variation on McKenzie's $\mathbb{A}(\mathcal{T})$.
- Whether $\operatorname{typ}(\mathcal{V}(\mathbb{A}))$ contains i for $i \in \{\mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}\}$ [Wood, McKenzie].
  - variation on McKenzie's $\mathbb{A}(\mathcal{T})$.
- Whether $\mathbb{A}$ has an NU term on $A - \{p, q\}$ [Maroti].
  - encode Minsky machine into a special $\mathbb{B}(\mathcal{M})$.

Conjectures

The following are **conjectured** to be undecidable for finite $\mathbb{A}$:

- **(1)** Whether $\mathbb{A}$ is finitely related.
- **(2)** Whether $\mathbb{A}$ is naturally dualizable.
- $+$ **many** more problems from clone theory.

If $\mathcal{V}(\mathbb{A})$...

- is congruence distributive, then we can decide **(1)** and **(2)**.
- is congruence modular, then we can decide **(1)** and (sort of) **(2)**.
- is congruence SD($\wedge$), we have no strong results.
- has a compatible semilattice term, then we can decide both ('yes').

Entailment

Let...

- $\mathbb{A}$ be a finite algebra,
- $\mathbb{R}$ an m-ary relation of $\mathbb{A}$ $(\mathbb{R} \leq \mathbb{A}^m)$,
- $\mathcal{R}$ be a set of finite arity relations of $\mathbb{A}$ $\left(\mathcal{R} \subseteq \bigcup_{n=1}^{N} \mathbf{S}(\mathbb{A}^n)\right)$,

$\mathcal{R}$ **entails** $\mathbb{R}$ $(\mathcal{R} \models \mathbb{R})$ if $\mathbb{R}$ is obtained by applying the operations below to members of $\mathcal{R} \cup \{=\}$.

- intersection
- product
- permutation of coordinates
- projection onto a subset of coordinates

$\mathcal{R}$ **duality entails** $\mathbb{R}$ $(\mathcal{R} \models_d \mathbb{R})$ if $\mathbb{R}$ is obtained by applying the operations below to members of $\mathcal{R} \cup \{=\}$.

- intersection
- product
- permutation of coordinates
- bijective projection onto coordinates

Entailment

Definition

Let $\mathbb{A}$ be a finite algebra, and let $\mathcal{R}_n = \bigcup_{k \leq n} \mathbf{S}(\mathbb{A}^k)$.

- $\mathbb{A}$ is **finitely related** if $\mathcal{R}_n \models \mathcal{R}_\omega$ for some n.
- $\mathbb{A}$ is **finitely duality related** if $\mathcal{R}_n \models_d \mathcal{R}_\omega$ for some n.

Problem (Relational entailment)

Input: *finite algebra* $\mathbb{A}$*.*

Output: *whether* $\mathbb{A}$ *is finitely related.*

Problem (Relational duality entailment)

Input: *finite algebra* $\mathbb{A}$*.*

Output: *whether* $\mathbb{A}$ *is finitely duality related.*

Minsky machines

The Minsky machine is a simple model of computation.

A Minsky machine has...

- states $0, 1, \ldots, N$ (state 1 is starting state, 0 is halting),
- registers A and B that have integer values ≥ 0,
- instructions of the form (i, R, j), meaning
  "in state i, increase register R by 1 and enter j".
- instructions of the form (i, R, j, k), meaning
  "in state i, if R is 0 enter j, otherwise decrease R by 1 and enter k".

A Minsky machine

Let $\mathcal{M}$ have instructions

$$(1,B,3,2), \qquad (2,A,1), \qquad (3,A,4), \qquad (4,A,0).$$

Start the machine with register contents $A = 3$, $B = 2$.

Step	State	A	B
0	1	3	2
1	2	3	1
2	1	4	1
3	2	4	0

Step	State	A	B
4	1	5	0
5	3	5	0
6	4	6	0
7	0	7	0

$\mathcal{M}$ computes $A + B + 2$ and stores the result in A.

Minsky machines more useful for us than Turing machines:

- no tape,
- no machine head,
- instructions are more condensed,
- "equivalent" to Turing machines,
- the Halting Problem for Minsky machines is undecidable.

$A(\mathcal{M})$

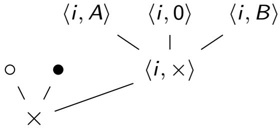
Let $\mathcal{M}$ be a Minsky machine with states $0, 1, \ldots, N$. Let

- $\Sigma = \{\circ, \bullet, \times\}$,
- for each state i, $M_i = \Big\{ \langle i, c \rangle \mid c \in \{0, A, B, \times\} \Big\}$.

$\mathbb{A}(\mathcal{M})$ has underlying set $A(\mathcal{M}) = \Sigma \cup \bigcup_{i=0}^{N} M_i$.

$\mathbb{A}(\mathcal{M})$ has the following operations, plus some more:

- a semilattice operation $\wedge$:



- $\langle 1, 0 \rangle$ as a constant
- machine operations $M(x, y)$, $M'(x)$

$$M(x,y) = \begin{cases} \langle j, R\rangle & \text{if } (i,R,j)\in\mathcal{M}, \\ & \quad y=\bullet, x=\langle i,0\rangle\,; \\ \langle j, 0\rangle & \text{if } (i,R,k,j)\in\mathcal{M}, \\ & \quad y=\bullet, x=\langle i,R\rangle\,; \\ \langle j, c\rangle & \text{if } (i,R,j) \text{ or } (i,R,k,j)\in\mathcal{M}, \\ & \quad y=\circ, x=\langle i,c\rangle\,; \\ \vdots & \end{cases} \qquad M'(x) = \begin{cases} \langle k, c\rangle & \text{if } (i,R,k,j)\in\mathcal{M}, \\ & \quad x=\langle i,c\rangle, c\neq R; \\ \vdots & \end{cases}$$

Let $\mathcal{M} = \big\{(1,B,3,2),(2,A,1),(3,A,4),(4,A,0)\big\}$. ($A+B+2$ from before)

1: $M\begin{pmatrix}\langle 1,0\rangle,\circ\\ \langle 1,A\rangle,\circ\\ \langle 1,B\rangle,\bullet\\ \langle 1,0\rangle,\circ\end{pmatrix} = \begin{pmatrix}\langle 2,0\rangle\\ \langle 2,A\rangle\\ \langle 2,0\rangle\\ \langle 2,0\rangle\end{pmatrix}$

2: $M\begin{pmatrix}\langle 2,0\rangle,\circ\\ \langle 2,A\rangle,\circ\\ \langle 2,0\rangle,\circ\\ \langle 2,0\rangle,\bullet\end{pmatrix} = \begin{pmatrix}\langle 1,0\rangle\\ \langle 1,A\rangle\\ \langle 1,0\rangle\\ \langle 1,A\rangle\end{pmatrix}$

3: $M'\begin{pmatrix}\langle 1,0\rangle\\ \langle 1,A\rangle\\ \langle 1,0\rangle\\ \langle 1,A\rangle\end{pmatrix} = \begin{pmatrix}\langle 3,0\rangle\\ \langle 3,A\rangle\\ \langle 3,0\rangle\\ \langle 3,A\rangle\end{pmatrix}$

4: $M\begin{pmatrix}\langle 3,0\rangle,\bullet\\ \langle 3,A\rangle,\circ\\ \langle 3,0\rangle,\circ\\ \langle 3,A\rangle,\circ\end{pmatrix} = \begin{pmatrix}\langle 4,A\rangle\\ \langle 4,A\rangle\\ \langle 4,0\rangle\\ \langle 4,A\rangle\end{pmatrix}$

5: $M\begin{pmatrix}\langle 4,A\rangle,\circ\\ \langle 4,A\rangle,\circ\\ \langle 4,0\rangle,\bullet\\ \langle 4,A\rangle,\circ\end{pmatrix} = \begin{pmatrix}\langle 0,A\rangle\\ \langle 0,A\rangle\\ \langle 0,A\rangle\\ \langle 0,A\rangle\end{pmatrix}$

Step	State	A	B
0	1	1	1
1	2	1	0
2	1	2	0
3	3	2	0
4	4	3	0
5	0	4	0

Computational relations

Let $\mathbb{S}_n = \mathrm{Sg}_{\mathbb{A}(\mathcal{M})^n} \left\{ \begin{pmatrix} \bullet \\ \circ \\ \vdots \\ \circ \end{pmatrix}, \begin{pmatrix} \circ \\ \bullet \\ \vdots \\ \circ \end{pmatrix}, \dots, \begin{pmatrix} \circ \\ \circ \\ \vdots \\ \bullet \end{pmatrix} \right\}$.

- $\langle 1, 0 \rangle$ is a constant, so every relation of $\mathbb{A}(\mathcal{M})$ contains $\begin{pmatrix} \langle 1, 0 \rangle \\ \vdots \\ \langle 1, 0 \rangle \end{pmatrix}$.
- This represents a configuration in state 1, with A and B registers 0.
- The generators allow for simulated computation inside the relation.

Theorem

$\mathcal{M}$ halts if and only if eventually $(M_0 \setminus \{\langle 0, \times \rangle\})^n \cap S_n \neq \emptyset$.

Theorem

Let $\mathcal{M}$ be a Minksky machine, $\mathcal{R}_n = \bigcup_{k=1}^{n} \mathbf{S}(\mathbb{A}(\mathcal{M})^k)$, and $\mathbb{S}_m$ be as before. The following are equivalent:

- *$\mathcal{M}$ halts,*
- *eventually $\mathcal{R}_n \models \mathbb{S}_m$ for all $m \geq n$,*
- *eventually $\mathcal{R}_n \models_d \mathbb{S}_m$ for all $m \geq n$.*

$\mathbb{A}(\mathcal{M})$ is not finitely (duality) related if $\mathcal{M}$ does not halt.

Make $\mathbb{A}(\mathcal{M})$ into a partial algebra (call it $\mathbb{A}^*(\mathcal{M})$)
$\rightsquigarrow$ fewer relations $\rightsquigarrow$ finitely (duality) related?

Theorem

Let $\mathcal{R}_n^* = \bigcup_{k=1}^{n} \mathbf{S}(\mathbb{A}^*(\mathcal{M})^k)$. The following are equivalent:

- *$\mathcal{M}$ halts,*
- *eventually $\mathcal{R}_n^* \models \mathcal{R}_\omega^*$,*
- *eventually $\mathcal{R}_n^* \models_d \mathcal{R}_\omega^*$.*

Coding theorem

Theorem

$\mathcal{M}$ halts if and only if eventually $(M_0 \setminus \{\langle 0, \times\rangle\})^n \cap S_n \neq \emptyset$.

Define another operation of $\mathbb{A}(\mathcal{M})$:

$$N(u,x,y,z) = \begin{cases} m & \text{if } u \in M_0 \setminus \{\langle 0,\times\rangle\}, \\ & \quad (x,y,z) \text{ is NU with majority} = m; \\ (x \wedge y) \vee (x \wedge z) & \text{elif } u \in M_0 \setminus \{\langle 0,\times\rangle\}; \\ w & \text{else, where } w = \langle i, \times\rangle \text{ if } x \in M_i \\ & \qquad \text{and } w = \times \text{ otherwise.} \end{cases}$$

It follows that if $(M_0 \setminus \{\langle 0, \times\rangle\})^n \cap S_n \neq \emptyset$, then $\mathbb{S}_n$ has an NU polynomial.

Theorem

Let $\mathcal{M}$ be a Minsky machine. The following are equivalent:

- *$\mathcal{M}$ halts,*
- *eventually $\mathbb{S}_n$ has an NU polynomial,*
- *eventually $(\circ, \circ, \ldots, \circ) \in S_n$,*

If $\mathcal{M}$ does not halt

If $\mathcal{R}_n \models \mathbb{R}$, then $\mathbb{R} = \pi\left(\bigcap_{i\in I}\mu_i\Big(\prod_{j\in J}\mathbb{R}_{ij}\Big)\right)$

for some $\mathbb{R}_{ij} \in \mathcal{R}_n$, finite sets I, J, permutations μ_i, and projection π.

Lemma

If

$$m\left\{\begin{pmatrix}\bullet\\ \circ\\ \vdots\\ \circ\end{pmatrix}, \begin{pmatrix}\circ\\ \bullet\\ \vdots\\ \circ\end{pmatrix}, \dots, \begin{pmatrix}\circ\\ \circ\\ \vdots\\ \bullet\end{pmatrix}\right. \in \pi\left(\bigcap_{i\in I}\mu_i\Big(\prod_{j\in J}\mathbb{R}_{ij}\Big)\right) = \mathbb{T}$$

where $m > n$ and $\mathbb{R}_{ij} \in \mathcal{R}_n$, then $(\circ, \circ, \dots, \circ) \in T$.

In particular, if $\mathcal{R}_n \models \mathbb{S}_m$ for some $m > n$, then $(\circ, \dots, \circ) \in S_m$.

From the coding theorem, this holds if and only if $\mathcal{M}$ halts.

$\mathcal{M}$ does not halt $\Rightarrow \mathcal{R}_n \not\models \mathbb{S}_m \Rightarrow \mathbb{A}(\mathcal{M})$ is not finitely (duality) related.

If $\mathcal{M}$ halts

The coding theorem:
if $\mathcal{M}$ halts, then eventually $\mathbb{S}_n$ has a 3-ary NU polynomial.

Let $m(x, y, z)$ be the NU polynomial and define

$$\mathbb{S}_n^i = \left\{ (s_1, \ldots, \overset{i}{\hat{a}_i}, \ldots, s_n) \mid \exists s_i (s_1, \ldots, \overset{i}{\hat{s}_i}, \ldots, s_n) \in S_n \right\}, \qquad \hat{\mathbb{S}}_n = \bigcap_{i=1}^{n} \mathbb{S}_n^i.$$

Each $\mathbb{S}_n^i$ is a permutation of $\mathbb{A}(\mathcal{M}) \times \mathbb{S}_{n-1}$. Thus, $\mathcal{R}_{n-1} \models_d \hat{\mathbb{S}}_n$.

$S_n \subseteq S_n^i$, so $S_n \subseteq \hat{S}_n$. If $(a_1, \ldots, a_n) \in \hat{S}_n \setminus S_n$, then there are b_i such that

$$\begin{pmatrix} b_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} a_1 \\ b_2 \\ \vdots \\ a_n \end{pmatrix}, \ldots, \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ b_n \end{pmatrix} \in S_n.$$

Since $m(x, y, z)$ is a polynomial of $\mathbb{S}_n$, applying $m(x, y, z)$ to any 3 yields $(a_1, \ldots, a_n) \in S_n$.

If $\mathcal{M}$ halts

- We have that eventually $\mathcal{R}_n \models \mathbb{S}_m$, $m > n$.

  What about other relations $\mathbb{R} \leq \mathbb{A}(\mathcal{M})^m$?

- If $\mathbb{R}$ contains a member of $(M_0 \setminus \{\langle 0, \times \rangle\})^m$ then it has an NU polynomial (call $\mathbb{R}$ **halting**).

- $\mathbb{A}(\mathcal{M})$ has operation

$$P(u, v, x, y) = \begin{cases} x & \text{if } u, v \in M_i \text{ or } u, v \in \Sigma, \\ y & \text{otherwise.} \end{cases}$$

  If $\mathbb{R}$ is not a subset of $\Sigma^m \cup M_0^m \cup \cdots \cup M_N^m$, then $\mathbb{R}$ directly decomposes (call $\mathbb{R}$ **non-synchronized**).

- Thus, the problematic relations are the non-halting, synchronized, $\cap$-irreducible relations.

  In the partial algebra construction, these are very easy to understand.

Decidability in universal algebra

Other directions

Question

If $\mathcal{M}$ halts, is $\mathbb{A}(\mathcal{M})$ finitely related?

(tentative yes, but **very** complicated)

$\mathbb{A}(\mathcal{M})$ has a semilattice operation, so it is SD($\wedge$).

Question

What are the connections between SD($\wedge$), residual size, finite axiomatizability, and dualizability?

Is $\mathbb{A}(\mathcal{M})$ finitely axiomatizable? Is $\mathbb{A}(\mathcal{M})$ residually small?

Conclusion

Theorem

Let $\mathcal{M}$ be a Minsky machine.

Let $\mathcal{R}_n = \bigcup_{k=1}^{n} \mathbf{S}(\mathbb{A}(\mathcal{M})^k)$*, and* $\mathbb{S}_m$ *be as before.*

Let $\mathcal{R}_n^* = \bigcup_{k=1}^{n} \mathbf{S}(\mathbb{A}^*(\mathcal{M})^k)$*. (*$\mathbb{A}^*(\mathcal{M})$ *is the partial algebra)*

The following are equivalent:

- $\mathcal{M}$ *halts,*
- *for some* n*,* $\mathcal{R}_n \models \mathbb{S}_m$ *for all* $m \geq n$*,*
- *for some* n*,* $\mathcal{R}_n \models_d \mathbb{S}_m$ *for all* $m \geq n$*,*
- *for some* n*,* $\mathcal{R}_n^* \models \mathcal{R}_\omega^*$*,*
- *for some* n*,* $\mathcal{R}_n^* \models_d \mathcal{R}_\omega^*$*.*

Thank you.