The Undecidability of the Definability of Principal Subcongruences

Matthew Moore

The University of Colorado at Boulder

April 13, 2013

Tarski's Problem

A. Tarski's Problem [1960's]

Is there an algorithm which takes as input a finite algebra and outputs whether or not the algebra has a finite equational basis?

A. Tarski's Problem, v2

Is there an algorithm which takes as input a finite algebra $\mathbb{A}$ *and outputs whether or not* $\mathcal{V}(\mathbb{A})$ *is finitely axiomatizable?*

Proving Finite Axiomatizability

Theorem (Jónsson)

Suppose that $\mathcal{V}$ is a variety, $\mathcal{V} \subseteq \mathcal{K}$, and both $\mathcal{K}$ and $\mathcal{K}_{SI}$ are finitely axiomatizable. Then $\mathcal{V}$ and $\mathcal{V}_{SI}$ are either both finitely axiomatizable or both not.

An Idea:

- Carefully choose some class $\mathcal{K}$ that is finitely axiomatizable.
- Make sure that $\mathcal{K}_{SI}$ is finitely axiomatized.
- Restrict consideration to those $\mathcal{V} \subseteq \mathcal{K}$ with finitely many SI's, all finite.

For instance, if $\mathcal{K}$ is the class of abelian groups of exponent m, then the sentence

$$\bigvee_{p^n | m} \left(\quad \forall x \left[x^{p^n} = 1 \right] \quad \right) \wedge \left(\qquad \exists_{=p} y \left[y^p = 1 \right] \qquad \right)$$

axiomatizes $\mathcal{K}_{SI}$. If $\mathcal{V}$ is a variety contained in $\mathcal{K}$ with only finitely many SI's, all finite, then $\mathcal{V}$ is finitely axiomatizable.

Proving Finite Axiomatizability

Theorem (Jónsson)

Suppose that $\mathcal{V}$ is a variety, $\mathcal{V} \subseteq \mathcal{K}$, and both $\mathcal{K}$ and $\mathcal{K}_{SI}$ are finitely axiomatizable. Then $\mathcal{V}$ and $\mathcal{V}_{SI}$ are either both finitely axiomatizable or both not.

An Idea:

- Carefully choose some class $\mathcal{K}$ that is finitely axiomatizable.
- Make sure that $\mathcal{K}_{SI}$ is finitely axiomatized.
- Restrict consideration to those $\mathcal{V} \subseteq \mathcal{K}$ with finitely many SI's, all finite.

For instance, if $\mathcal{K}$ is the class of abelian groups of exponent m, then the sentence

$$\bigvee_{p^n | m} (\text{“I am a } p^n \text{ group”}) \wedge (\text{“exactly } p-1 \text{ order } p \text{ elements”})$$

axiomatizes $\mathcal{K}_{SI}$. If $\mathcal{V}$ is a variety contained in $\mathcal{K}$ with only finitely many SI's, all finite, then $\mathcal{V}$ is finitely axiomatizable.

Proving Finite Axiomatizability

Theorem (Jónsson)

Suppose that $\mathcal{V}$ is a variety, $\mathcal{V} \subseteq \mathcal{K}$, and both $\mathcal{K}$ and $\mathcal{K}_{SI}$ are finitely axiomatizable. Then $\mathcal{V}$ and $\mathcal{V}_{SI}$ are either both finitely axiomatizable or both not.

An Idea:

- Carefully choose some class $\mathcal{K}$ that is finitely axiomatizable.
- Make sure that $\mathcal{K}_{SI}$ is finitely axiomatized.
- Restrict consideration to those $\mathcal{V} \subseteq \mathcal{K}$ with finitely many SI's, all finite.

For instance, if $\mathcal{K}$ is the class of abelian groups of exponent m, then the sentence

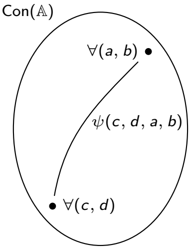
$$\bigvee_{p^n | m} \text{"I am an order } p^n \text{ cyclic } p\text{-group"}$$

axiomatizes $\mathcal{K}_{SI}$. If $\mathcal{V}$ is a variety contained in $\mathcal{K}$ with only finitely many SI's, all finite, then $\mathcal{V}$ is finitely axiomatizable.

Choosing the class $\mathcal{K}$: DPC

Definition

A variety $\mathcal{V}$ is said to have **definable principal congruences (DPC)** if there is a congruence formula $\psi(w, x, y, z)$ such that for all $\mathbb{A} \in \mathcal{V}$ and all $a, b \in A$, $\mathrm{Cg}^{\mathbb{A}}(a, b)$ is defined by $\psi(-, -, a, b)$.



In this case, take $\mathcal{K}$ to be the class of algebras with DPC witnessed by ψ (this is finitely axiomatizable).

$\mathcal{K}_{SI}$ is axiomatized by

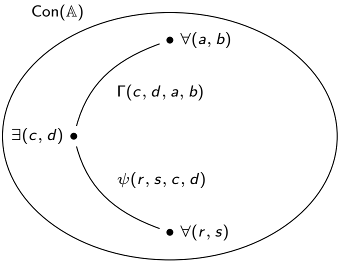
$$\exists u, v \left[u \neq v \wedge \forall a, b \left[a \neq b \rightarrow \psi(u, v, a, b) \right] \right].$$

If $\mathcal{V} \subseteq \mathcal{K}$ and $\mathcal{V}_{SI}$ is finite and contains only finite algebras then $\mathcal{V}$ is finitely axiomatizable.

Choosing the class $\mathcal{K}$: DPSC

Definition

A variety $\mathcal{V}$ is said to have **definable principal subcongruences (DPSC)** if there are congruence formulas Γ and $\psi(w, x, y, z)$ such that for all $\mathbb{A} \in \mathcal{V}$ and all $a, b \in A$ there exist $c, d \in A$ such that $\Gamma(c, d, a, b)$ witnesses $(c, d) \in \mathrm{Cg}^{\mathbb{A}}(a, b)$ and $\psi(-, -, c, d)$ defines $\mathrm{Cg}^{\mathbb{A}}(c, d)$.



Let $\mathcal{K}$ be the class of algebras with DPSC via Γ and ψ (this is finitely axiomatizable).

$\mathcal{K}_{SI}$ is axiomatized by

$$\exists u, v \, [u \neq v \wedge \forall a, b \, [a \neq b \rightarrow \exists c, d \, [\Gamma(c, d, a, b) \wedge \psi(u, v, c, d)]]] .$$

If $\mathcal{V} \subseteq \mathcal{K}$ and $\mathcal{V}_{SI}$ is finite and contains only finite algebras then $\mathcal{V}$ is finitely axiomatizable.

A Question

- For each Turing machine $\mathcal{T}$ McKenzie constructed an algebra associated to it, $\mathbb{A}(\mathcal{T})$, such that $\mathcal{V}(\mathbb{A}(\mathcal{T}))$ has finitely many SI's, all finite, if and only if $\mathcal{T}$ halts.
- Willard showed that $\mathcal{V}(\mathbb{A}(\mathcal{T}))$ is finitely axiomatizable if and only if $\mathcal{T}$ halts.

In the case where there are only finitely many SI's, all finite, DPC and DPSC are closely related to finite axiomatizability. This leads naturally to the question:

Question

1. *Is the undecidability of finite axiomatizability in $\mathcal{V}(\mathbb{A}(\mathcal{T}))$ due to a more primitive result about the undecidability of DPSC for $\mathcal{V}(\mathbb{A}(\mathcal{T}))$?*
2. *Is it true that $\mathcal{V}(\mathbb{A}(\mathcal{T}))$ has DPSC if and only if $\mathcal{T}$ halts?*

A Theorem

In order to connect the halting status of $\mathcal{T}$ with DPSC, the algebra $\mathbb{A}(\mathcal{T})$ is modified by adding a new operation. The modified algebra is called $\mathbb{A}'(\mathcal{T})$ and still possesses many of the same important properties that $\mathbb{A}(\mathcal{T})$ does.

Theorem

The following are equivalent:

- $\mathcal{T}$ *halts.*
- $\mathcal{V}(\mathbb{A}'(\mathcal{T}))$ *has finitely many SI's, all finite.*

Since the problem of determining when a Turing machine halts is undecidable, this shows that the other property is also undecidable.

$\mathbb{A}'(\mathcal{T})$

For a Turing machine $\mathcal{T}$ with n states, the underlying set of $\mathbb{A}'(\mathcal{T})$ has $(20n + 16)$ elements:

$$A'(\mathcal{T}) = \{0, 1, 2, H, C, D, \partial C, \partial D, \\ C_{ir}^{s}, D_{ir}^{s}, M_{i}^{r}, \partial C_{ir}^{s}, \partial D_{ir}^{s}, \partial M_{i}^{r} \mid 0 \leq i \leq n \text{ and } r, s \in \{0, 1\}\}.$$

$\mathbb{A}'(\mathcal{T})$ has operations to emulate computation on certain tuples of the indexed elements:

$$\mathcal{L} = \{L_{irt} \mid \mathcal{T} \text{ has instruction } (\mu_i, r, s, L, \mu_j) \text{ and } t \in \{0, 1\}\},$$
$$\mathcal{R} = \{R_{irt} \mid \mathcal{T} \text{ has instruction } (\mu_i, r, s, R, \mu_j) \text{ and } t \in \{0, 1\}\}.$$

The operations of $\mathbb{A}'(\mathcal{T})$ are

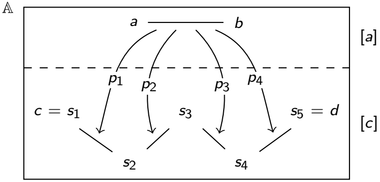
$$\left\{0, \wedge, (\cdot), J, J', K, S_0, S_1, S_2, T, I, F, U_F^0, U_F^1 \mid F \in \mathcal{L} \cup \mathcal{R}\right\}.$$

How do we approach proving that $\mathcal{V}(\mathbb{A}'(\mathcal{T}))$ has DPSC?

Maltsev Chains

The unary polynomials of an algebra $\mathbb{A}$ are

$$\mathrm{Pol}_1(\mathbb{A}) = \left\{ p(x) = t(\overline{y}, x) \mid t(x_1, \ldots, x_n) \text{ a term}, \overline{y} \in A^{n-1} \right\}$$



$(c, d) \in \mathrm{Cg}^{\mathbb{A}}(a, b)$ iff there are
$p_1, \ldots, p_{n-1} \in \mathrm{Pol}_1(\mathbb{A})$ and
$c = s_1, s_2, \ldots, s_n = d \in A$ with
$\{s_i, s_{i+1}\} = \{t_i(a), t_i(b)\}$

Such chains are called **Maltsev chains**.

DPSC in General

1. Produce (c, d) from (a, b) in a way that is bounded in complexity. This means Maltsev chains of uniformly bounded length, whose associated polynomials are uniformly bounded in complexity.

2. The (c, d) thus produced should be made to have some special properties so that the congruence generated by (c, d) is uniformly definable.

3. This means that the Maltsev chains for **any** $(r, s) \in \text{Cg}^{\mathbb{B}}(c, d)$ should be uniformly bounded in length and have associated polynomials that are uniformly bounded in complexity.

DPSC for $\mathbb{A}'(\mathcal{T})$ (when $\mathcal{T}$ halts)

For $\mathbb{B} \in \mathcal{V}(\mathbb{A}'(\mathcal{T}))$ and $a, b \in B$, we want a uniform way to produce (c, d) from (a, b) such that (c, d) generates a congruence that is uniformly definable.

DPSC for $\mathbb{A}'(\mathcal{T})$ (when $\mathcal{T}$ halts)

Take a subdirect representation of $\mathbb{B}$ by SI's:

$$\mathbb{B} \leq \prod_{l \in L} \mathbb{C}_l \qquad \text{such that} \qquad \pi_l(B) = C_l.$$

We will try to understand congruences in $\mathbb{B}$ by carefully analyzing the $\mathbb{C}_l$.

The $\mathbb{C}_l$ come in 4 different flavors:

- **Flavor S:** These SI's are all contained in $\mathbf{HS}(\mathbb{A}'(\mathcal{T}))$ and satisfy a certain identity involving the S_i operation.
- **Flavor Seq:** These SI's all have a certain nice structure based on the $(\cdot)$ operation. These are called sequential type.
- **Flavor M:** These SI's all have a certain nice structure based on the machine operations, $\mathcal{L} \cup \mathcal{R}$. These are called machine type.
- **Flavor X:** These SI's are all contained in $\mathbf{HS}(\mathbb{A}'(\mathcal{T}))$, but don't fit into Flavor S.

The Case Distinction

For $\mathbb{B} \in \mathcal{V}(\mathbb{A}'(\mathcal{T}))$ with $\mathbb{B} \leq \prod_{l \in L} \mathbb{C}_l$ and distinct $a, b \in B$, let

$$K = \{l \in L \mid a(l) \neq b(l)\}.$$

The 4 flavors of SI's give rise to 4 cases to consider:

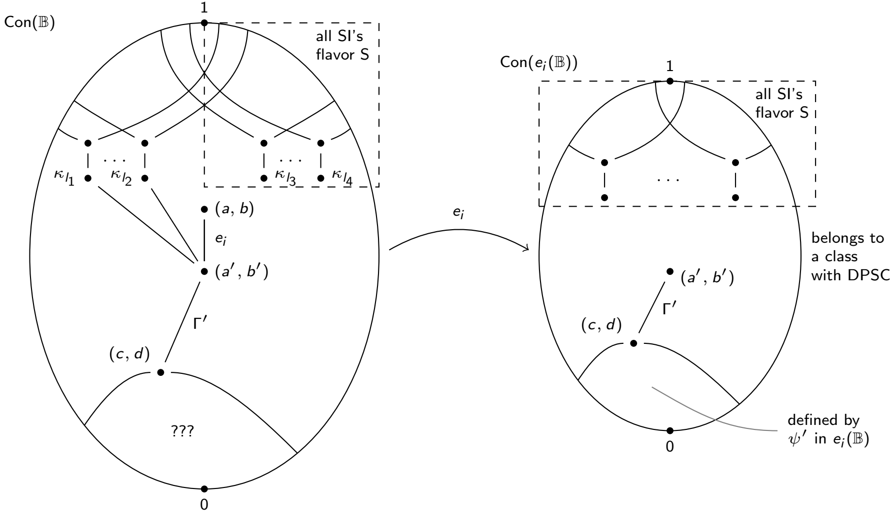
1. **Case S:** There is $k \in K$ such that $\mathbb{C}_k$ is flavor S.
2. **Case Seq:** Case S does not hold, and there is $k \in K$ such that $\mathbb{C}_k$ is flavor Seq.
3. **Case M:** Cases S and Seq. don't hold, and there is $k \in K$ such that $\mathbb{C}_k$ is flavor M.
4. **Case X:** Cases S, Seq., and M do not hold, so there must be $k \in K$ such that $\mathbb{C}_k$ is flavor X.

DPSC in $\mathcal{V}(\mathbb{A}'(\mathcal{T}))$ (when $\mathcal{T}$ halts)

1. In cases Seq., M, and X, Maltsev chains are short (length 1), and polynomials will be bounded in complexity when $\mathcal{T}$ halts.

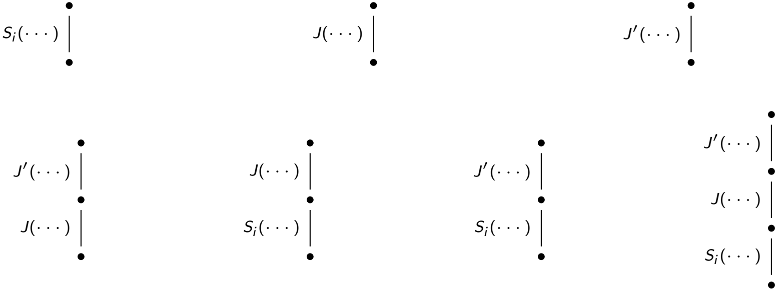
2. Case S is quite involved, and requires a fine analysis of the polynomials and extensive calculations using $\mathbb{A}'(\mathcal{T})$ arithmetic.

Case S: An Overview



Case S: Reducing a Maltsev Chain

In Case S membership in $\mathrm{Cg}^{\mathbb{B}}(c, d)$ is witnessed by one of the 15 chains below



(the $\cdots$ is uniformly bounded in complexity). In Case S, this demonstrates a uniform way to produce (c, d) from (a, b) such that $\mathrm{Cg}^{\mathbb{B}}(c, d)$ is uniformly definable.

If $\mathcal{T}$ Halts, Then...

Working through cases S, Seq., M, and X proves the following theorem.

Theorem

If $\mathcal{T}$ halts, then $\mathcal{V}(\mathbb{A}'(\mathcal{T}))$ has DSPC.

If $\mathcal{T}$ Does Not Halt

Suppose that there is a first-order sentence Φ expressing "I am SI".

- If $\mathcal{T}$ does not halt, then $\mathcal{V}(\mathbb{A}'(\mathcal{T}))$ has a countably infinite SI, call it $\mathbb{S}$.
- $\mathbb{S}$ satisfies the sentence Φ.
- Any ultrapower of $\mathbb{S}$ satisfies Φ, so any ultrapower of $\mathbb{S}$ is also SI.
- Under close examination, the ultrapower cannot be SI if it is uncountable.
- Therefore, if $\mathcal{T}$ does not halt then no such Φ can exist.

If $\mathcal{V}(\mathbb{A}'(\mathcal{T}))$ has DPSC, then there **is** a first-order sentence expressing "I am SI". Therefore $\mathcal{V}(\mathbb{A}'(\mathcal{T}))$ cannot have DPSC if $\mathcal{T}$ does not halt.

If $\mathcal{T}$ Does Not Halt

Lemma

If $\mathcal{T}$ does not halt, then $\mathcal{V}(\mathbb{A}'(\mathcal{T}))$ does not have DPSC.

The Theorem

Combining everything, we have the following theorem.

Theorem

The following are equivalent:

- $\mathcal{T}$ *halts.*
- $\mathcal{V}(\mathbb{A}'(\mathcal{T}))$ *has finitely many SI's, all finite.*
- $\mathcal{V}(\mathbb{A}'(\mathcal{T}))$ *has DPSC.*
- $\mathcal{V}(\mathbb{A}'(\mathcal{T}))$ *is finitely axiomatizable.*

Since the problem of determining when a Turing machine halts is undecidable, this shows that other stated properties are also undecidable.

Bibliography

- Kirby A. Baker and Ju Wang, **Definable principal subcongruences**, Algebra Universalis **47** (2002), no. 2, 145–151. MR 1916612 (2003c:08002)
- Ralph McKenzie, **The residual bound of a finite algebra is not computable**, Internat. J. Algebra Comput. **6** (1996), no. 1, 29–48. MR 1371733 (97e:08002b)
- ______, **Tarski's finite basis problem is undecidable**, Internat. J. Algebra Comput. **6** (1996), no. 1, 49–104. MR 1371734 (97e:08002c)
- Ross Willard, **Tarski's finite basis problem via $A(\mathcal{T})$**, Trans. Amer. Math. Soc. **349** (1997), no. 7, 2755–2774. MR 1389791 (97i:03019)