The Undecidability of Definable Principal Subcongruences

Part I

Matthew Moore

The University of Colorado at Boulder

October 23, 2012

A. Tarski's Problem

Tarski's Problem (1960's)

Is there an algorithm which takes as input a finite algebra $\mathbb{A}$, and determines whether or not $\mathbb{A}$ has a finite equational basis?

Understanding it:

- An algorithm is a program which can run on a universal Turing machine.
- An algebra is a set with operations and relations, $\mathbb{A} = \langle A; F; R \rangle$. For example, $\mathbb{G} = \left\langle G; \cdot, \ ^{-1}, 1 \right\rangle$ might be a group.
- Algebras satisfy certain equations. For instance, abelian groups satisfy $xy = yx$. The set of equations an algebra satisfies (the *equational theory*) is usually infinite, but it may happen that a finite subset of equations implies the rest of them. In this case, the algebra is said to have a finite equational basis.

Passing to $\mathcal{V}(\mathbb{A})$

Let **T** be the set of all true equations in $\mathbb{A}$ and $\mathcal{V}(\mathbb{A})$ the class of models of **T** ($\mathcal{V}$ is the variety generated by $\mathbb{A}$).

Tarski's Problem is equivalent to

Tarski's Problem, v2

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

Why is this better?

- $\mathcal{V}(\mathbb{A}) = \mathsf{HSP}(\mathbb{A})$, which is somewhat easier to work with than $\mathbb{A}$.
- First-order sentences true in $\mathcal{V}(\mathbb{A})$ (the axioms of $\mathcal{V}(\mathbb{A})$) are more flexible than equations.

Approaching Tarski's Problem

An algebra is said to be *subdirectly irreducible (SI)* if it has a least nonzero congruence.

Lemma (Jònsson)

If $\mathcal{V}$ is a variety contained in a class $\mathcal{K}$ such that $\mathcal{K}$ and $\mathcal{K}_{SI}$ are both finitely axiomatizable, then $\mathcal{V}$ and $\mathcal{V}_{SI}$ are both finitely axiomatizable or both not finitely axiomatizable.

This suggests the following approach: given a finite algebra $\mathbb{A}$, let $\mathcal{V} = \mathcal{V}(\mathbb{A})$, and show

- $\mathcal{V}_{SI}$ is finitely axiomatizable, say by **S**, and
- there is a first-order sentence Ψ expressing "if I am SI, then I satisfy **S**".

Let $\mathcal{K}$ be the class of models of Ψ, so that both $\mathcal{K}$ and $\mathcal{K}_{SI}$ are finitely axiomatizable and $\mathcal{V} \subseteq \mathcal{K}$. Since $\mathcal{V}_{SI}$ is finitely axiomatizable, so is $\mathcal{V}$.

Difficulties

We would like

- $\mathcal{V}_{SI}$ is finitely axiomatizable, say by $\mathbf{S}$, and
- there is a first-order sentence Ψ expressing "if I am SI, then I satisfy $\mathbf{S}$".

The first item is manageable, but the second item is problematic. The statement that an algebra has a least congruence (i.e. it is SI) is not first-order. Further, the statement "$(c, d) \in \mathrm{Cg}(a, b)$" is not first-order either.

A Solution: insist that the varieties we study possess a first-order sentence $\Gamma(w, x, y, z)$ such that for all $\mathbb{B} \in \mathcal{V}(\mathbb{A})$,

$$\mathbb{B} \models \Gamma(c, d, a, b) \iff (c, d) \in \mathrm{Cg}^{\mathbb{B}}(a, b)$$

This property is called *definable principal congruences (DPC)*.

Making SI First-Order

If $\mathcal{V}$ is a variety with DPC witnessed by $\Gamma(w, x, y, z)$, then the formula

$$\Psi = \exists a, b\, [a \neq b \wedge \forall c, d\, [c \neq d \rightarrow \Gamma(a, b, c, d)]]$$

is satisfied by an algebra in $\mathcal{V}$ if and only if that algebra has a least nonzero congruence (i.e. it is SI).

Thus, we have reduced our problem to analyzing when $\mathcal{V}_{SI}$ is finitely axiomatizable. If we insist that there only be finitely many SI's in $\mathcal{V}$, all finite (in this case $\mathcal{V}$ is said to be residually finite), then we arrive at the following theorem.

Theorem (McKenzie)

If $\mathcal{V}$ is a residually finite variety with definable principal congruences, then $\mathcal{V}$ is finitely axiomatizable.

DPSC

For a variety to have DPC is quite rare, and equivalent properties written in the language of the variety are often quite awkward.

Is there a more general property than DPC that still allows us to detect SI's?

Definition

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

In this case, $\mathbb{B} \in \mathcal{V}$ is SI if and only if

$$\mathbb{B} \models \exists r, s\, [r \neq s \wedge \forall a, b\, [a \neq b \rightarrow \exists c, d\, [\Gamma(c, d, a, b) \wedge \psi(r, s, c, d)]]]$$

DPC vs. DPSC

Varieties of semilattices have both DPC and DPSC, because the polynomials are so simple ($f(x) = x \wedge a$ for some a).

A variety generated by a finite group $\mathbb{G}$ has DPC if and only if

$$\mathbb{G} \models [x, y, x] \approx 1.$$

On the other hand, the variety has DPSC if and only if $\mathbb{G}$ is nilpotent. In particular, if $\mathbb{G}$ has nilpotency class 3 or greater, then it will not satisfy $[x, y, x] \approx 1$ and thus has DPSC but not DPC.

Proving Things Have DPSC (or DPC)

Theorem (Maltsev's Lemma)

$(c, d) \in Cg^{\mathbb{B}}(a, b)$ if and only if there is a sequence of elements $c = e_1, e_2, \ldots, e_{n-1}, e_n = d$ and polynomials $\lambda_1(x), \ldots, \lambda_{n-1}(x)$ such that

$$\{\lambda_i(a), \lambda_i(b)\} = \{e_i, e_{i+1}\}$$

The general method to show something has DPC is to show that Maltsev chains are bounded in length and that there is a bound on the complexity of polynomials.

The general method to show that something has DPSC is to show that there is a bounded complexity way to reduce any principal congruence to a definable principal subcongruence. This usually involves performing some kind of polynomial operations on the larger congruence in order to produce a subcongruence which is small enough to be easily definable.

What Does it Mean for Something to be Undecidable?

A general decision problem is a computability problem of the form:

Input:	Object A,
Output:	"Y" if A has property P, "N" otherwise.

The property P is said to be *undecidable* if there is no algorithm that has the above input and output for all objects A.

Algebraic decidability problems have as input a finite algebra, and involve an algebraic property. In general, the decidability or undecidability of certain properties can be thought of as measures of the complexity of the algebra.

Saying "definable principal subcongruences is undecidable" is the same as saying that the there is no algorithm with

Input:	finite algebra $\mathbb{A}$,
Output:	"Y" if $\mathcal{V}(\mathbb{A})$ has DPSC, "N" otherwise.

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

A decision problem related to Tarski's Problem is whether or not the property of having a finite residual bound is decidable.

McKenzie addressed both this problem and Tarski's Problem by exhibiting constructions which associated to each Turing machine an algebra, $\mathbb{A}(\mathcal{T})$, in such a way that the halting status of the machine exactly determined properties of the algebra, thus showing that these properties are undecidable.

Theorem

The following are equivalent:

- $\mathcal{T}$ *halts,*
- $\mathcal{V}(\mathbb{A}(\mathcal{T}))$ *has finite residual bound,*
- $\mathcal{V}(\mathbb{A}(\mathcal{T}))$ *is finitely axiomatizable.*

Modifying $\mathbb{A}(\mathcal{T})$

Since DPC and DPSC are so closely related to finite axiomatizability, it is natural to ask whether the failure of $\mathcal{V}(\mathbb{A}(\mathcal{T}))$ to be finitely axiomatizable is the result of a failure of DPC or DPSC.

I modify McKenzie's $\mathbb{A}(\mathcal{T})$ to an algebra $\mathbb{A}^*(\mathcal{T})$ in such a way that $\mathcal{V}(\mathbb{A}^*(\mathcal{T}))$ has DPSC if and only if $\mathcal{T}$ halts.The modification is also such that the variety is residually finite if and only if $\mathcal{T}$ halts. It follows easily from this that $\mathbb{A}^*(\mathcal{T})$ is finitely based if and only if $\mathcal{T}$ halts.

Next Time

- an outline of the construction of $\mathbb{A}(\mathcal{T})$
- a description of the modifications to $\mathbb{A}(\mathcal{T})$ which are necessary
- a rough outline of the proof that DPSC is undecidable
- a quick negative answer to Tarski's Problem

Thank you.