Finitely generated varieties which are finitely decidable are residually finite

Ralph McKenzie and Matthew Smedberg

Vanderbilt University
Department of Mathematics

7 June 2013

The Finite Decidability Problem

Let $\mathcal{V}$ be a variety (usually locally finite) in a finite language. We say $\mathcal{V}$ is *decidable* if its first-order theory is, and *finitely decidable* if the theory of $\mathcal{V}_{\text{fin}}$ is decidable.

The Finite Decidability Problem

Let $\mathcal{V}$ be a variety (usually locally finite) in a finite language. We say $\mathcal{V}$ is *decidable* if its first-order theory is, and *finitely decidable* if the theory of $\mathcal{V}_{\text{fin}}$ is decidable.

Decidable and finitely decidable varieties are rare and structurally constrained. For example,

The Finite Decidability Problem

Let $\mathcal{V}$ be a variety (usually locally finite) in a finite language. We say $\mathcal{V}$ is *decidable* if its first-order theory is, and *finitely decidable* if the theory of $\mathcal{V}_{\text{fin}}$ is decidable.

Decidable and finitely decidable varieties are rare and structurally constrained. For example,

Fact

- *If* $\mathbf{A}$ *has any congruence covers of the lattice or semilattice types, or*

then every variety containing $\mathbf{A}$ *is finitely undecidable.*

The Finite Decidability Problem

Let $\mathcal{V}$ be a variety (usually locally finite) in a finite language. We say $\mathcal{V}$ is *decidable* if its first-order theory is, and *finitely decidable* if the theory of $\mathcal{V}_{\text{fin}}$ is decidable.

Decidable and finitely decidable varieties are rare and structurally constrained. For example,

Fact

- *If* **A** *has any congruence covers of the lattice or semilattice types, or*
- *If any boolean- or affine-type minimal sets in* **A** *have nonempty tails, or*

then every variety containing **A** *is finitely undecidable.*

The Finite Decidability Problem

Let $\mathcal{V}$ be a variety (usually locally finite) in a finite language. We say $\mathcal{V}$ is *decidable* if its first-order theory is, and *finitely decidable* if the theory of $\mathcal{V}_{\text{fin}}$ is decidable.

Decidable and finitely decidable varieties are rare and structurally constrained. For example,

Fact

- *If* **A** *has any congruence covers of the lattice or semilattice types, or*
- *If any boolean- or affine-type minimal sets in* **A** *have nonempty tails, or*
- *If* **A** *is a subdirectly irreducible finite algebra with two incomparable nonabelian congruences,*

then every variety containing **A** *is finitely undecidable.*

Fact (continued)

If **A** *is a finite algebra*

- *and* **A** *has a solvable congruence which is nonabelian, or*

then every variety containing **A** *is finitely undecidable.*

Fact (continued)

If **A** *is a finite algebra*

- *and* **A** *has a solvable congruence which is nonabelian, or*
- **A** *is subdirectly irreducible with boolean monolith and also has a cover of type 1 or 2, or*

then every variety containing **A** *is finitely undecidable.*

Fact (continued)

If **A** *is a finite algebra*

- *and* **A** *has a solvable congruence which is nonabelian, or*
- **A** *is subdirectly irreducible with boolean monolith and also has a cover of type 1 or 2, or*
- **A** *is SI with type 2 monolith and has also a cover of type 1, or vice versa,*

then every variety containing **A** *is finitely undecidable.*

Fact (continued)

If **A** *is a finite algebra*

- *and* **A** *has a solvable congruence which is nonabelian, or*
- **A** *is subdirectly irreducible with boolean monolith and also has a cover of type 1 or 2, or*
- **A** *is SI with type 2 monolith and has also a cover of type 1, or vice versa,*

then every variety containing **A** *is finitely undecidable.*

These facts (and many of a similar nature) were established for modular varieties in the 90s (see [Idziak 1997]). The results for nonmodular varieties are in most cases new.

Bounding Subdirect Irreducibles in $\mathcal{V}$

Theorem

Let $\mathcal{K}$ be a finite set of finite algebras, and suppose $\mathcal{V} = \mathrm{HSP}(\mathcal{K})$ is finitely decidable. Then there is a finite bound on the cardinalities of SI algebras in $\mathcal{V}$.

Bounding Subdirect Irreducibles in $\mathcal{V}$

Theorem

Let $\mathcal{K}$ be a finite set of finite algebras, and suppose $\mathcal{V} = \mathrm{HSP}(\mathcal{K})$ is finitely decidable. Then there is a finite bound on the cardinalities of SI algebras in $\mathcal{V}$.

Using familiar methods from the congruence-modular case, we show that

- every SI with boolean-type monolith belongs to $\mathrm{HS}(\mathcal{K})$;

Bounding Subdirect Irreducibles in $\mathcal{V}$

Theorem

Let $\mathcal{K}$ be a finite set of finite algebras, and suppose $\mathcal{V} = \mathrm{HSP}(\mathcal{K})$ is finitely decidable. Then there is a finite bound on the cardinalities of SI algebras in $\mathcal{V}$.

Using familiar methods from the congruence-modular case, we show that

- every SI with boolean-type monolith belongs to $\mathrm{HS}(\mathcal{K})$;
- there is a bound ($\sim$ quadruply exponential) on the affine-type SIs.

Bounding unary-type SIs in $\mathcal{V}$

So let $\mathbf{S} \in \mathcal{V}$ have monolith $\perp \overset{1}{\prec} \mu$.

Lemma

$\mathrm{Rad}_u(\mathbf{S})$ *is comparable to all congruences of* $\mathbf{S}$.

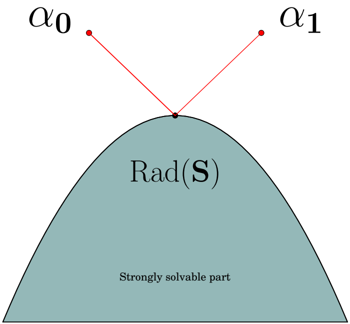
Lemma

$\mathrm{Rad}_u(\mathbf{S})$ *is meet-irreducible.*

Each of these is proved by contradiction: supposing the respective lemma were false, we construct a (relatively straightforward) interpretation of some finitely undecidable class into $\mathrm{HSP}(\mathbf{S})$.

Meet-irreducibility of the solvable radical

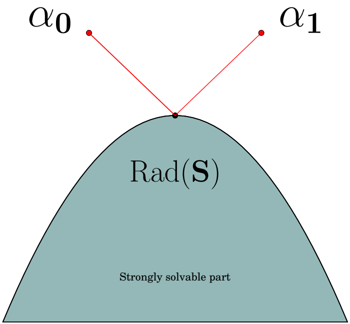
Goal: to semantically interprect a structure of the form $\langle I; E_0, E_1 \rangle$ (where the E_j are disjoint equivalence relations) into subpowers of $\mathbf{S}$.



Meet-irreducibility of the solvable radical

Goal: to semantically interprect a structure of the form $\langle I; E_0, E_1\rangle$ (where the E_j are disjoint equivalence relations) into subpowers of $\mathbf{S}$.

Let $\{0_j, 1_j\}$ be $(\mathrm{Rad}_u(\mathbf{S}), \alpha_j)$-minimal sets. Let $\mathbf{B} \leq \mathbf{S}^I$ consist of all $\mathbf{x}$ which are α_1-constant on E_1-blocks and vice versa.

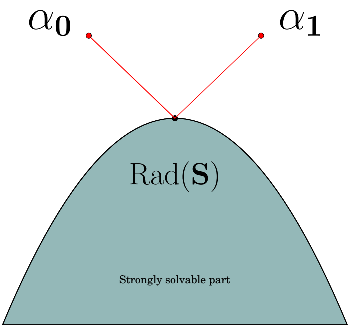


Meet-irreducibility of the solvable radical

Goal: to semantically interprect a structure of the form $\langle I; E_0, E_1\rangle$ (where the E_j are disjoint equivalence relations) into subpowers of $\mathbf{S}$.

Let $\{0_j, 1_j\}$ be $(\mathrm{Rad}_u(\mathbf{S}), \alpha_j)$-minimal sets. Let $\mathbf{B} \leq \mathbf{S}^I$ consist of all $\mathbf{x}$ which are α_1-constant on E_1-blocks and vice versa.

Using a failure of $\mathrm{C}(\mu, \{0_j, 1_j\}; \perp_S)$, and some tricks from tame congruence theory,



we reconstruct the original structure $\langle I; E_0, E_1\rangle$ in a first-order way from $\mathbf{B}$.

Since $\mathrm{Rad}_u(\mathbf{S})$ is meet-irreducible, we know that its index cannot exceed the maximum size of a boolean-type SI in $\mathcal{V}$.

Theorem

$\mathrm{Rad}_u(\mathbf{S})$ *is strongly abelian.*

Proof.

□

Since $\mathrm{Rad}_u(\mathbf{S})$ is meet-irreducible, we know that its index cannot exceed the maximum size of a boolean-type SI in $\mathcal{V}$.

Theorem

$\mathrm{Rad}_u(\mathbf{S})$ *is strongly abelian.*

Proof.

Long! □

Takeaway idea: Subalgebra generation (and congruence generation) can frequently be proven to be "sparse" in some useful sense, when the generators are chosen so that they are almost constant modulo a strongly abelian congruence (such as the monolith).

Sparse subalgebra generation: Example I

Suppose $\mathrm{C}(\theta_0, \mu_{|U}; \perp)$ holds in our subdirectly irreducible algebra, but $\mathrm{C}(\theta_1, \mu_{|U}; \perp)$ does not, where $\theta_0 \prec \theta_1$ are strongly solvable.

See Lemma 3.1 in our paper for more about this example.

Sparse subalgebra generation: Example I

Suppose $\mathrm{C}(\theta_0, \mu_{|U}; \perp)$ holds in our subdirectly irreducible algebra, but $\mathrm{C}(\theta_1, \mu_{|U}; \perp)$ does not, where $\theta_0 \prec \theta_1$ are strongly solvable.
Choose a witnessing package

$$t(a_0, \vec{b}_0) = t(a_0, \vec{b}_1)$$

but

$$t(a_1, \vec{b}_0) \neq t(a_1, \vec{b}_1)$$

where t takes values in some $\perp, \mu$-minimal set.

See Lemma 3.1 in our paper for more about this example.

Example I, continued

Now suppose $\mathbb{G} = \langle V, E \rangle$ is a graph we want to interpret into $\mathrm{HSP}(\mathbf{S})$. Generate $\mathbf{D} \leq \mathbf{S}^{V \sqcup \{\infty\}}$

Example I, continued

Now suppose $\mathbb{G} = \langle V, E\rangle$ is a graph we want to interpret into $\mathrm{HSP}(\mathbf{S})$. Generate $\mathbf{D} \leq \mathbf{S}^{V \sqcup \{\infty\}}$ using all the diagonal elements, plus all elements of the form

$$a_{1|\{v,\infty\}} \oplus a_{0|\text{else}} \quad (v \in V)$$
$$a_{1|\{v,w,\infty\}} \oplus a_{0|\text{else}} \quad (v \overset{E}{—} w)$$

plus one extra element $m_{0|V} \oplus m_{1|\{\infty\}}$ (m_0, m_1 belonging to some $(\perp, \mu)$-trace).

Example I, continued

Now suppose $\mathbb{G} = \langle V, E\rangle$ is a graph we want to interpret into $\mathrm{HSP}(\mathbf{S})$. Generate $\mathbf{D} \le \mathbf{S}^{V \sqcup \{\infty\}}$ using all the diagonal elements, plus all elements of the form

$$a_{1|\{v,\infty\}} \oplus a_{0|\text{else}} \quad (v \in V)$$

$$a_{1|\{v,w,\infty\}} \oplus a_{0|\text{else}} \quad (v \overset{E}{-\!\!-} w)$$

plus one extra element $m_{0|V} \oplus m_{1|\{\infty\}}$ (m_0, m_1 belonging to some $(\perp, \mu)$-trace).

Key Claim

Every point in $D \cap U$ attains at most two values (mod θ_0), and does so precisely in the pattern of one of the generators (i.e. one of these values occurs at a vertex and infinity, or at the endpoints of an edge and at infinity).

Sparse subalgebra generation: Example II

Fix a $(\perp, \mu)$-minimal set U, and say we are working to semantically interpret a graph $\langle V, E\rangle$ into a power of $\mathbf{S}$. Let $I = \{v^+, v^- : v \in V\}$. Define a subalgebra

$$\Delta \subseteq \mathbf{B} \leq \mathbf{S}^I$$

with generators those $\mathbf{x} \in U^I$ such that for some $v \in V$,

$$\begin{cases} x^{v^+} \equiv_\mu x^{v^-} \\ x^{w^+} = x^{w^-} \equiv_\mu x^{v^+} \quad \text{for all other } w \in V \end{cases}$$

Example II continued

Claim

$B \cap U^I$ consists of just the generators and no more.

Example II continued

Claim

$B \cap U^I$ consists of just the generators and no more.

Proof: write an arbitrary element $\mathbf{y} \in U^I$ as a product $\mathbf{f}(\mathbf{x}_1, \ldots, \mathbf{x}_k)$ of generators, where $\mathbf{f} = f^I$ for some polynomial operation $f : \mathbf{S} \to U$. Let C_j be the μ-class where $\mathbf{x}_j$ lives; then on $C_1 \times \cdots \times C_k$, f is essentially unary; say it depends on $\mathbf{x}_1$, which has its spike at $v_0 \in V$. Then $y^{v_0^+} \equiv_\mu y^{v_0^-}$, and for all $w \neq v_0$,

$$x_1^{w^+} = x_1^{w^-} \qquad \text{and} \qquad x_j^{w^+} \equiv_\mu x_j^{w^-}$$

so that

$$y^{w^+} = f(x_1^{w^+}, \ldots, x_k^{w^+}) = f(x_1^{w^-}, \ldots, x_k^{w^-}) = y^{w^-}$$

Sparse congruence generation: Example III

Assume that $\sigma = \mathrm{Rad}_u(\mathbf{S})$ is abelian over μ but not over $\bot$, and let $\mathbb{G} = \langle V, E \rangle$ be a graph. Fix the index set $I = V \times \{+, -\} \sqcup \{\infty\}$, and let $\mathbf{D} \leq \mathbf{S}^I$ be the subalgebra consisting of all σ-constant points.

See Lemma 3.6 in our paper for all the hypotheses of this example.

Sparse congruence generation: Example III

Assume that $\sigma = \mathrm{Rad}_u(\mathbf{S})$ is abelian over μ but not over $\perp$, and let $\mathbb{G} = \langle V, E \rangle$ be a graph. Fix the index set $I = V \times \{+, -\} \sqcup \{\infty\}$, and let $\mathbf{D} \leq \mathbf{S}^I$ be the subalgebra consisting of all σ-constant points.

Next, choose a $(\perp, \mu)$-subtrace $\{m_0, m_1\}$, and let Θ be the congruence on $\mathbf{D}$ generated by identifying all pairs

$$m_{1|v^+} \oplus m_{0|\text{else}} \equiv m_{1|v^-} \oplus m_{0|\text{else}} \qquad (v \in V)$$

$$m_{1|v^+,w^+} \oplus m_{0|\text{else}} \equiv m_{1|v^-,w^-} \oplus m_{0|\text{else}} \qquad (v \overset{E}{\text{---}} w)$$

See Lemma 3.6 in our paper for all the hypotheses of this example.

Key Claim

When restricted to a minimal set, Θ contains blocks of cardinality 1 and 2 only, and if $\mathbf{x} \equiv_\Theta \mathbf{y}$ then the set of coordinates where they differ is either empty, or $\{v^+, v^-\}$ for some $v \in V$, or $\{v^+, w^+, v^-, w^-\}$ for some $v \overset{E}{—} w$.

Bounding $\mathrm{Rad}_u(\mathbf{S})$-blocks

Say $\mathrm{Rad}_u(\mathbf{S})$ has index ℓ and some fixed monolith pair $c \neq d$.
Since $\mathrm{Rad}_u(\mathbf{S})$ is strongly abelian,

Lemma

For any polynomial $t(v_0, \vec{v}_1, \ldots, \vec{v}_\ell)$, there exist subsets of each variable set $\vec{v}_i$, of size no more than $\log |\mathbf{F}_{\mathcal{V}}(2+\ell)|$, such that for all $\mathrm{Rad}_u(\mathbf{S})$-blocks $B_1, \ldots, B_\ell$, the mapping

$$A \times \vec{B}_1 \times \cdots \times \vec{B}_\ell \to A$$

induced by t depends only on v_0 and the indicated subsets.

Because of the Lemma, terms $f(v_0) = t(v_0, \vec{s})$ of bounded arity suffice to send exactly one of any unequal elements $x_1 \neq x_2$ to c.

Bounding $\mathrm{Rad}_u(\mathbf{S})$-blocks, II

Consider a fixed $\mathrm{Rad}_u(\mathbf{S})$-block B, and to each $b \in B$ associate the set of terms $t(v_0, v_1, \ldots, v_k)$, with k bounded as described in the last slide, such that for some $p_1, \ldots, p_k$ from the appropriate $\mathrm{Rad}_u(\mathbf{S})$-blocks, $t(b, \vec{p}) = c$.

Claim

This is an injective map from B to subsets of $\mathbf{F}_{\mathcal{V}}(1 + k)$

For if not, we get a failure of the strong term condition

$$c = t(b_1, \vec{p}_1) = t(b_2, \vec{p}_2) \text{ but } t(b_2, \vec{p}_1) \neq c$$

This contradiction completes the proof.

Open Problems

Problem

Do finitely decidable, locally finite varieties have definable principal congruences? Definable principal subcongruences? Definable principal solvable congruences?

Open Problems

Problem

Do finitely decidable, locally finite varieties have definable principal congruences? Definable principal subcongruences? Definable principal solvable congruences?

Problem

In a finite algebra $\mathbf{A}$ *in a finitely decidable variety, must every congruence permute with* $\mathrm{Rad}(\mathbf{A})$*? With* $\mathrm{Rad}_u(\mathbf{A})$*?*

Open Problems

Problem

Do finitely decidable, locally finite varieties have definable principal congruences? Definable principal subcongruences? Definable principal solvable congruences?

Problem

In a finite algebra $\mathbf{A}$ *in a finitely decidable variety, must every congruence permute with* $\mathrm{Rad}(\mathbf{A})$*? With* $\mathrm{Rad}_u(\mathbf{A})$*?*

Problem

In all known cases, the set of finitely refutable sentences of a finitely generated variety is either decidable or Turing-complete. Do there exist varieties where this set has an intermediate complexity class?

Thank you!