Four Unsolved Problems in Congruence Permutable Varieties

Ross Willard

University of Waterloo, Canada

Nashville, June 2007

Congruence permutable varieties

Definition

A variety $\mathcal{V}$ is **congruence permutable** (or **CP**) if for each $\mathbf{A} \in \mathcal{V}$, $\mathrm{Con}\,\mathbf{A}$ is a lattice of *permuting* equivalence relations.

θ, φ **permute** if $\theta \vee \varphi = \theta \circ \varphi = \varphi \circ \theta$.

Examples of CP varieties: Any variety of ...

- groups
- expansions of groups (e.g., rings, modules, non-associative rings, near rings, boolean algebras, etc.)
- quasi-groups in the language $\{\cdot, /, \backslash\}$

But not:

- lattices, semilattices, semigroups, unary algebras.

Basic facts about CP varieties

Fact 1

CP $\Rightarrow$ congruence modularity.

Fact 2 (Mal'tsev, 1954)

For a variety $\mathcal{V}$, TFAE:

- $\mathcal{V}$ is CP.
- $\mathcal{V}$ has a term $m(x, y, z)$ satisfying, in all $\mathbf{A} \in \mathcal{V}$,

$$m(x, x, z) = z \quad \text{and} \quad m(x, z, z) = x \qquad (*)$$

Definitions

- **Mal'tsev term**: a term $m(x, y, z)$ satisfying $(*)$.
- **Mal'tsev algebra**: an algebra having a Mal'tsev term.
- **Mal'tsev variety**: a variety having a common Mal'tsev term.

Fact 2 (restated)

CP varieties = Mal'tsev varieties.

Aim of lecture

Mal'tsev algebras and varieties are ...

- not "far" removed from groups, rings, near-rings, quasi-groups, etc...
- "old-fashioned," "solved."

Aim of this lecture: to correct this perception, by stating some open problems that:

- are general
- are of current interest
- are open
- are ripe for study in Mal'tsev algebras and varieties.

1. Subpower membership problem

Fix a finite algebra **A**.

Subpower membership problem for A

Input: $X \subseteq A^n$ and $f \in A^n$ $(n \geq 1)$

Question: is $f \in \mathrm{Sg}_{\mathbf{A}^n}(X)$?

How hard can it be?

HARD:

- Naive algorithm is **EXPTIME**
- There is no better algorithm (Friedman 1982; Bergman *et al* 1999. ADDED IN PROOF: Kozik, announced 2007).

However, for groups and rings the problem is solvable in polynomial time.

Subpower membership problem for groups

(adapted from Sims 1971; Furst, Hopcroft, Luks 1980)

Fix a finite group $\mathbf{G}$. Suppose $H \leq \mathbf{G}^n$.

Consider

$$H = H^{(0)} \geq H^{(1)} \geq \cdots \geq H^{(n)} = \{e\}$$

where

$$H^{(i)} = \{g \in H : g = (\underbrace{e, \ldots, e}_{i}, *, \ldots, *)\}.$$

Let M_i be a transversal for the cosets of $H^{(i)}$ in $H^{(i-1)}$, including $\widehat{e}$. Concretely:

1. $g \in M_i \quad \Rightarrow \quad g = (\underbrace{e, \ldots, e}_{i-1}, a, *, \ldots, *) \in H.$
2. Every such form witnessed in H is represented in M_i exactly once.

Put $M = \bigcup_{i=1}^{n} M_i$.

Facts:

1. M is small ($|M| = O(n)$)
2. $\langle M \rangle = H$. In fact,
   - $H = M_1 M_2 \cdots M_n$
   - every element $h \in H$ is uniquely expressible in the form $h = g_1 g_2 \cdots g_n$ with each $g_i \in M_i$. ("Canonical form")
3. Given $h \in H$, we can find $g_i \in M_i$ recursively, efficiently (knowing M).
4. Same algorithm tests arbitrary $f \in G^n$ for membership in H.
5. Thus the subpower membership problem for **G** is solvable in polynomial time **if**, given $X \subseteq G^n$, we can find such an M for $H = \langle X \rangle$.

Finding M.

Rough idea. Given $X \subseteq G^n$:

- Start with $M_i = \{\widehat{e}\}$ for each i (so $M = \{\widehat{e}\}$).
- For each $g \in X$, attempt to find the canonical form for g relative to M. (Will fail.)
- Each failure suggests an addition to some M_i.
    - The addition is always from $\langle X \rangle$.
    - **Action**: increment this M_i by the suggested addition.
- Repeat until each $g \in X$ passes; i.e., $X \subseteq M_1 M_2 \cdots M_n$.
- Next, for each $g, h \in M$, attempt to find the canonical form for gh.
    - Make additions to appropriate M_i upon each failure.
    - Loop until $g, h \in M \Rightarrow gh$ passes.

When to stop:

Lemma

$M_1 M_2 \cdots M_n = \langle X \rangle$ as soon as $g, h \in M \Rightarrow gh \in M_1 M_2 \cdots M_n$.

Corollary

The subpower membership problem is solvable in polynomial time for any finite group **G**.

Remark. Similar technique works for any expansion of a group by multilinear operations (e.g., rings, modules, nonassociative rings).

Corollary

The subpower membership problem is solvable in polynomial time for any finite ring or module.

Partial generalization to Mal'tsev algebras

(Adapted from A. Bulatov and V. Dalmau, A simple algorithm for Mal'tsev constraints, *SIAM J. Comput*. **36** (2006), 16–27.)

Fix a finite algebra $\mathbf{A}$ with Mal'tsev term $m(x, y, z)$.

Definition

An *index* for A^n is a triple $(i, a, b) \in \{1, 2, \ldots, n\} \times A \times A$.

Definition

A pair $(g, h) \in A^n \times A^n$ *witnesses* (i, a, b) if

$$\begin{aligned} g &= (x_1, \ldots, x_{i-1}, a, *, \ldots, *) \\ h &= (x_1, \ldots, x_{i-1}, b, *, \ldots, *) \end{aligned}$$

Consider $\mathbf{B} \leq \mathbf{A}^n$.

Definition

A **structured signature** for $\mathbf{B}$ is an n-tuple $(M_1, \ldots, M_n)$ where

1. $(i = 1)$:
   - $M_1 \subseteq B$
   - Each form $(a, *, \ldots, *) \in B$ is represented exactly once in M_1.
2. $(2 \leq i \leq n)$:
   - $M_i \subseteq B^2$
   - Each $(g, h) \in M_i$ witnesses some index (i, a, b).
   - Each index (i, a, b) witnessed in B is represented exactly once in M_i

'

Suppose $(M_1, \dots, M_n)$ is a structured signature for $\mathbf{B} \le \mathbf{A}^n$.
Let M be the set of all $g \in A^n$ mentioned in $(M_1, \dots, M_n)$.

Facts:

1. $(M_1, \dots, M_n)$ and M are small ($|M| = O(n)$)
2. $\mathrm{Sg}_{\mathbf{A}^n}(M) = \mathbf{B}$.
3. In fact, every element $h \in B$ is expressible in the "canonical form"

$$h = m(m(\cdots m(m(f_1, g_2, h_2), g_3, h_3), \cdots), g_n, h_n)$$

   with $f_1 \in M_1$ and $(g_i, h_i) \in M_i$ for $2 \le i \le n$.

   - **Note**: can also require

$$\begin{aligned} g_2(2) &= f_1(2) \\ g_3(3) &= m(f_1, g_2, h_2)(3), \text{ etc.} \end{aligned}$$

4. $f_1, g_2, h_2, \dots, g_n, h_n$ as above are unique for h and can be found recursively and efficiently.
5. Same algorithm tests arbitrary $f \in A^n$ for membership in B.

This was enough for Bulatov and Dalmau to give a simple polynomial-time solution to the "CSP problem with Mal'tsev constraints."

Question: What about the subpower membership problem?

Suppose $X \subseteq A^n$ and put $\mathbf{B} = \mathrm{Sg}_{\mathbf{A}^n}(X)$.

We can mimic the group algorithm by attempting to "grow" a structured signature for **B**.

Sticking point: knowing when to stop.

Problem 1

Using structured signatures or otherwise, is the Subpower Membership Problem for finite Mal'tsev algebras solvable in polynomial time?

2. The Pixley Problem

Recall: An algebra is *subdirectly irreducible* (or s.i.) if it cannot be embedding in a direct product of proper homomorphic images. (Equivalently, if its congruence lattice is monolithic.)

Definition

A variety $\mathcal{V}$ is a **Pixley variety** if:

- its language is finite
- every s.i. in $\mathcal{V}$ is finite (i.e., $\mathcal{V}$ is residually finite)
- $\mathcal{V}$ has arbitrarily large (finite) s.i.'s.

Question (Pixley, 1984): Is there a congruence distributive Pixley variety?

Answer (Kearnes, W., 1999): No.

Problem: Generalize.

What is the situation for groups, rings, etc.?

1. Commutative rings with 1.
   - No Pixley varieties here, since principal ideals are first-order definable.
2. Groups.
   - Ol'shanskii (1969) described all residually finite varieties of groups.
   - None are Pixley varieties.
3. Rings (with or without 1).
   - McKenzie (1982) analyzed all residually small varieties of rings.
   - None are Pixley varieties.
4. Modules.
   - Goodearl (priv. comm.): if R is an infinite, f.g. prime ring for which all nonzero ideals have finite index, then all nonzero injective left R-modules are infinite.
   - Kearnes (unpubl.): hence no variety of modules is Pixley.

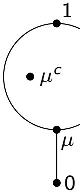
Commutator Theory

Mal'tsev varieties (and congruence modular varieties) have a well-behaved theory of abelianness, solvability, centralizers and nilpotency.

Fundamental notions:

- "θ centralizes φ" ($\theta, \varphi \in \mathrm{Con}\,\mathbf{A}$), i.e., $[\theta, \varphi] = 0$.
- φ^c = largest θ which centralizes φ.

Frequently important: if **A** is s.i.:

$\mathrm{Con}\,\mathbf{A} =$ 

Fact: if $\mathcal{V}$ is a CM Pixley variety, then (by the Freese-McKenzie theorem) for every s.i. in $\mathcal{V}$, μ^c is abelian.

An argument

Suppose $\mathcal{V}$ is a congruence modular variety in a finite language and having arbitrarily large finite s.i.'s.

Case 1: There exist arbitrarily large finite s.i.'s $\mathbf{A} \in \mathcal{V}$ with $|A/\mu^c|$ bounded.

- Use the module result to get an infinite s.i. $\mathbf{A} \in \mathcal{V}$ with $|A/\mu^c|$ bounded.

Case 2: Else.

- Define $C(x,y,z,w) \leftrightarrow$ "$\mathrm{Cg}(x,y)$ centralizes $\mathrm{Cg}(z,w)$."
- Assume $C(x,y,z,w)$ is first-order definable in $\mathcal{V}$. Then use compactness to get an s.i. $\mathbf{A} \in \mathcal{V}$ with $|A/\mu^c|$ infinite.

Hence:

Theorem (Kearnes, W., unpubl.)

If $\mathcal{V}$ is congruence modular and $C(x,y,z,w)$ is definable in $\mathcal{V}$, then $\mathcal{V}$ is **not** *a Pixley variety.*

Notes:

- Previous theorem handles all varieties of groups, rings and modules.
- Doesn't handle varieties of non-associative rings.

Problem 2

Does there exist a congruence permutable Pixley variety?

- What about varieties of non-associative rings?

3. McNulty's Problem

Definition

A variety $\mathcal{V}$ is **strange** if

- its language is finite.
- $\mathcal{V}$ is locally finite.
- $\mathcal{V}$ is not finitely based.
- There exists a finitely based variety $\mathcal{W}$ having exactly the same finite members as $\mathcal{V}$.

Definition

A finite algebra is strange if the variety it generates is.

Question (Eilenberg, Schützenberger, 1976): Does there exist a strange finite algebra?

McNulty has asked the same question for varieties.

Lemma (Cacioppo, 1993)

If **A** is strange, then it is inherently nonfinitely based (INFB).

Theorem (McNulty, Székely, W., 2007?)

If **A** can be shown to be INFB by the "shift automorphism method," then **A** is **not** strange.

Examples of algebras known to be INFB but not by the shift automorphism method:

1. (ADDED IN PROOF – thank you, George): INFB Semigroups. Characterized by Sapir; George has checked that none are strange.
2. Isaev's non-associative ring (1989).

That's it!

Problem 3

1. Is Isaev's algebra strange?
2. Find more INFB algebras that are expansions of groups. Are any of them strange?

4. Dualizability

Definition

A finite algebra ~~**A**~~ $\underline{\mathbf{M}}$ is **dualizable** if

- there exists an "alter ego" $\underset{\sim}{\mathbf{M}}$ ...
- ... partial operations ... relations ... discrete topology ...
- ... $\mathbb{ISP}$ and $\mathbb{IS}_c\mathbb{P}^+$ ...
- ... contravariant hom-functors ...
- ... dual adjunction (D, E, e, ε) ...
- **AARRRGGHH!!! STOP THE INSANITY!!**

Dualizability

All that you need to know about dualizability (but were afraid to ask):

- "Dualizability" is a property that a finite algebra may, or may not, have.
- In practice, "dualizability" coincides with an apparently stronger property, called "finite dualizability."
- By a theorem of Zádori and myself, "finite dualizability" can be characterized in purely clone-theoretic terms.

Classical clone theory

Fix a finite algebra $\mathbf{A}$.

Recall that:

1. $Inv(\mathbf{A}) := \{r \subseteq A^n \; : \; \mathbf{r} \leq \mathbf{A}^n, \, n \geq 1\}$.
2. $Inv(\mathbf{A})$ **determines** $\mathrm{Clo}(\mathbf{A})$, in the sense that

   $$\forall f : A^n \to A, \; f \in \mathrm{Clo}(\mathbf{A}) \text{ iff } f \text{ preserves every } r \in Inv(\mathbf{A}).$$

3. Can speak of
   - a subset $\mathcal{R} \subseteq Inv(\mathbf{A})$ **determining** $\mathrm{Clo}(\mathbf{A})$
   - $\mathrm{Clo}(\mathbf{A})$ being **finitely determined**.

Old Theorem

The following are equivalent:

- $\mathcal{R}$ determines $\mathrm{Clo}(\mathbf{A})$
- Every $r \in Inv(\mathbf{A})$ can be defined from $\mathcal{R}$ by a $\exists\&$*atomic* formula.

Partial operations with c.a.d. domains

Fix **A**.

A subset $D \subseteq A^n$ is **c.a.d.** (*conjunction-atomic-definable*) if it is definable in **A** by a &*atomic* formula.

Definition

$\mathrm{Clo}|_{cad}(\mathbf{A}) := \{$all restrictions of term operations of **A** to c.a.d. domains$\}$.

Then:

1. $Inv(\mathbf{A})$ determines $\mathrm{Clo}|_{cad}(\mathbf{A})$, in the same sense:

   $\forall f : D \to A$ with c.a.d. domain, $f \in \mathrm{Clo}|_{cad}(\mathbf{A})$ iff f preserves every $r \in Inv(\mathbf{A})$.

2. Can speak of
   - a subset $\mathcal{R} \subseteq Inv(\mathbf{A})$ **determining** $\mathrm{Clo}|_{cad}(\mathbf{A})$
   - $\mathrm{Clo}|_{cad}(\mathbf{A})$ being **finitely determined**.

Lemma/Definition

The following are equivalent:

1. $\mathbf{A}$ is "*finitely dualizable*" ($\Rightarrow$ dualizable)
2. $\mathrm{Clo}|_{cad}(\mathbf{A})$ is finitely determined.
3. There is a finite set $\mathcal{R} \subseteq Inv(\mathbf{A})$ such that every "*hom-transparent*" $r \in Inv(\mathbf{A})$ is $\&$*atomic* definable from $\mathcal{R}$.

Def. $r \in Inv(\mathbf{A})$ is **hom-transparent** (or **balanced**) if

- Every homomorphism $h : \mathbf{r} \to \mathbf{A}$ is a coordinate projection, and
- No two coordinate projections are the same.

Dualizability problem: which finite **A** are (finitely) dualizable?

1. CD case:
   - (finitely) dualizable $\Leftrightarrow$ **A** has a near-unanimity term
     - $\Leftarrow$ by Baker-Pixley, $\Rightarrow$ by (Davey, Heindorf, McKenzie, 1995)
2. Commutative rings with 1:
   - (finitely) dualizable $\Leftrightarrow$ **R** generates a residually small variety.
     - (Clark, Idziak, Sabourin, Szabó, W., 2001)
3. Groups:
   - (finitely) dualizable $\Leftrightarrow$ **G** generates a residually small variety.
     - $\Rightarrow$ by (Quackenbush, Szabó, 2002), $\Leftarrow$ by (Nickodemus, 2007?)
4. Rings (with or without 1):
   - (finitely) dualizable $\overset{?}{\Leftrightarrow}$ **R** generates a residually small variety.
     - $\Rightarrow$ by (Szabó, 1999), $\Leftarrow$ by recent work of Kearnes, Szendrei?
5. But:
   - if $\mathbf{G} = S_3$, then $\mathbf{G}_G$ is *not* dualizable, yet generates a residually small variety (Idziak, unpubl., 1994)
   - $\exists$ expansion of $(\mathbb{Z}_4, +)$ that is (finitely) dualizable, yet generates a residually large variety (Davey, Pitkethly, W., 2007?)

Problem 4

1. Which finite Mal'tsev algebras are (finitely) dualizable?
    - Can we at least answer this for expansions of groups?
2. Is the answer to (1) decidable?