Maltsev constraints

Ross Willard

University of Waterloo, CAN

Open Problems in Universal Algebra
Vanderbilt University
May 28, 2015

(2,3)-systems over a finite algebra

Let **A** be a finite algebra. A **(2,3)-system over A** is a triple

$$\mathcal{I} = (V, (P_x : x \in V), (R_{x,y} : x, y \in V))$$

where

- V is a finite nonempty set.
- Each "potato" P_x is a nonempty subuniverse of **A**.
- Each "edge relation" $R_{x,y} \leq_{sd} \mathbf{P}_x \times \mathbf{P}_y$.
- $R_{y,x} = (R_{x,y})^{-1}$ and $R_{x,x} = 0_{P_x}$.
- $R_{x,z} \subseteq R_{x,y} \circ R_{y,z}$ for all $x, y, z \in V$.

$\mathrm{Sol}(\mathcal{I}) = \{$all solutions to $\mathcal{I}\}$, where a **solution** is a function $s : V \to A$ satisfying $(s(x), s(y)) \in R_{x,y}$ for all $x, y \in V$.

CSP($\mathbf{A}$, 2)

Fix a finite algebra **A**.

CSP(A,2)

Input: a (2,3)-system $\mathcal{I}$ over **A**.
Question: Is $\mathrm{Sol}(\mathcal{I}) \neq \varnothing$?

Holy Grail

Prove that CSP($\mathbf{A}$, 2) is in P whenever **A** belongs to a Taylor variety.

Bulatov's theorem and improvements

Theorem (Bulatov 2002)

If $\mathbf{A}$ *is in a Maltsev variety, then* $\mathrm{CSP}(\mathbf{A}, 2)$ *is in P.*

Theorem (Bulatov, Dalmau 2006)

Same result, (much) simpler algorithm.

Improvements, generalizations:

- Dalmau 2006
- Idziak *et al* 2007
- Barto (submitted)

Theorem

A version of the Bulatov-Dalmau algorithm solves $\mathrm{CSP}(\mathbf{A}, 2)$ *whenever* $\mathbf{A}$ *belongs to a congruence modular variety.*

The Bulatov-Dalmau algorithm

Main idea:

- Find a generating set for the algebra of solutions of one constraint R_{x_1,y_1}, then of two constraints $R_{x_1,y_1}, R_{x_2,y_2}, \ldots$

Positive features:

- Correctly solves $\mathrm{CSP}(\mathbf{A}, 2)$ in polynomial time.
- No algebra required.

Negative features:

- No hope of extending beyond the congruence modular setting.
- No algebra required.

Challenge

Challenge

Find a new algorithm solving CSP($\mathbf{A}, 2$) when $\mathbf{A}$ is in a Maltsev variety ...

- With the possibility of generalization beyond the CM case.
- Exploiting algebraic knowledge of Maltsev varieties.

Intuition

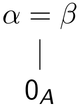
- Propagation, search for inconsistency
- Local consistency + Gaussian elimination should be enough.

Abelian atoms in finite Taylor algebras

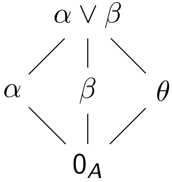
Let $\mathbf{A}$ be a finite algebra in a Taylor variety.

Definition

1. $\mathrm{At}(\mathbf{A}) := \{\alpha \in \mathrm{Con}(\mathbf{A}) : 0_A \prec \alpha$, α is abelian$\}$.
2. For $\alpha, \beta \in \mathrm{At}(\mathbf{A})$, define $\alpha \Bumpeq \beta$ iff $\alpha = \beta$ or α, β are two of the three middle elements in an M_3 in $\mathrm{Con}(\mathbf{A})$.



or



Geometrical congruences

Let **A** be a finite algebra in a Taylor variety.

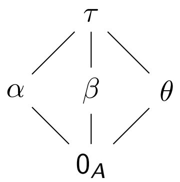
Lemma

$\Bumpeq$ is an equivalence relation on $\mathrm{At}(\mathbf{A})$.

Definition

$\tau \in \mathrm{Con}(\mathbf{A})$ is **geometrical** if there exists $\Phi \subseteq \mathrm{At}(\mathbf{A})$ such that $\Phi \subseteq$ a single $\Bumpeq$-class, **and** $\tau = \bigvee \Phi$.

E.g.,



$\mathrm{Geom}(\mathbf{A}) := \{\tau \in \mathrm{Con}(\mathbf{A}) \,:\, \tau \text{ is geometrical}\}$.

Coordinatization

Lemma

Suppose **A** *is a finite algebra in a Taylor variety. TFAE:*

1. τ *is geometrical.*
2. *The interval* $I[0_A, \tau]$ *is isomorphic to the lattice of subspaces of a fin. dim. vector space* V *over some finite field* $\mathbb{F}_q$*.*

When (2) holds, each τ*-block can be "coordinatized" as a matrix power of* V*.*

Corollary

For each $\tau \in \mathrm{Geom}(\mathbf{A}) \setminus \{0_A\}$ *there exists a unique prime* p *such that* $|a/\tau| = p^{n_a}$ *for all* $a \in A$*.*

Definition

$\mathrm{char}(\tau) =$ this prime p.

Application to (2,3)-systems

Suppose that, in a (2,3)-system $\mathcal{I} = (V, \ldots)$ over $\mathbf{A}$, we have

- A collection $\{\mathbf{P}_x : x \in C\}$ of potatoes ($C \subseteq V$).
- For each $x \in C$, $\tau_x \in \mathrm{Geom}(\mathbf{P}_x)$

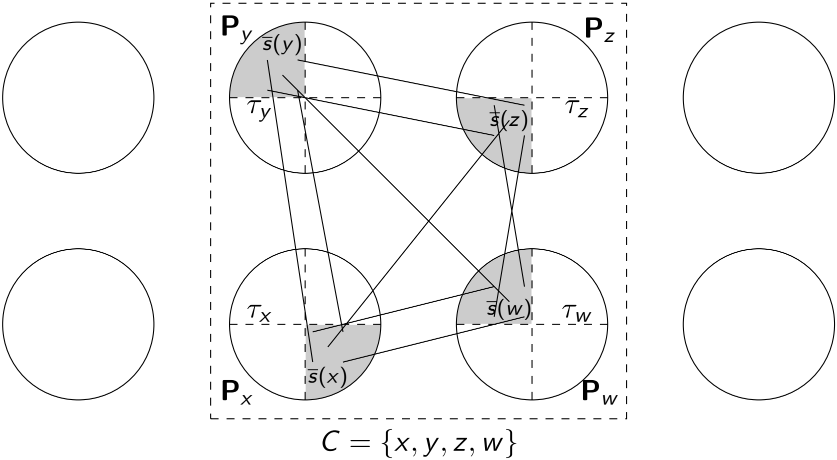
with $\mathrm{char}(\tau_x) = \mathrm{char}(\tau_y) =: p$ for all $x, y \in C$.

Notation

1. $\mathcal{I}|_C$ is the restriction of $\mathcal{I}$ to potatoes from C.
2. $(\mathcal{I}|_C)/\tau$ is the (2,3)-system with potatoes $\mathbf{P}_x/\tau_x$ ($x \in C$) and constraints $\overline{\mathbf{R}}_{x,y} := \{(a/\tau_x, b/\tau_y) : (a, b) \in R_{x,y}\}$.

(Thus if $\bar{s} \in \mathrm{Sol}((\mathcal{I}|_C)/\tau)$ then $\bar{s}$ names a τ_x-block for each $x \in C$.)

3. $\mathcal{I}[\bar{s}]$ is the restriction of $\mathcal{I}|_C$ to the τ_x-blocks named by $\bar{s}$.



$\mathcal{I}[\overline{s}] =$ the restriction of $\mathcal{I}|_C$ to the shaded regions given by $\overline{s}$.

Easy Fact

Each $\mathcal{I}[\overline{s}]$ can be encoded as a system of linear equations over $\mathbb{F}_p$.

Issues

On their own, such coordinatizations aren't particularly helpful.

1. $(\mathcal{I}|_C)/\tau$ may have exponentially many distinct solutions $\bar{s}$.
   In the worst case we must solve every linear system $\mathcal{I}[\bar{s}]$.
2. Focussing on C for which $|\mathrm{Sol}((\mathcal{I}|_C)/\tau)|$ is small (e.g., "following strands") may fail to capture inconsistency.

In the remainder of this lecture I discuss one response to these issues which can be formulated in **difference term varieties**.

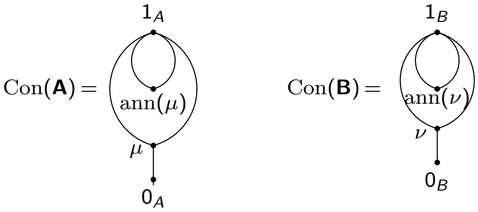
Similarity

(Freese 1982; also Freese & McKenzie 1987; cf. H. Neumann 1967)

Let $\mathcal{V}$ be a CM variety.

There is an equivalence relation $\sim$ between SI members of $\mathcal{V}$.

Let $\mathbf{A}, \mathbf{B}$ be SIs with <u>abelian</u> monoliths μ, ν. Let $\mathrm{ann}(\mu) = (0_A : \mu)$ and $\mathrm{ann}(\nu) = (0_B : \nu)$.



Rough Definition

$\mathbf{A} \sim \mathbf{B}$ means $\exists h : \mathbf{A}/\mathrm{ann}(\mu) \cong \mathbf{B}/\mathrm{ann}(\nu)$ such that

- The "module actions" of $\mathbf{A}/\mathrm{ann}(\mu)$ on μ-blocks, and of $\mathbf{B}/\mathrm{ann}(\nu)$ on ν-blocks, are compatible with h.

Generalizing similarity

We can generalize $\sim$:

- From SIs to pairs $(\mathbf{A}, \alpha)$ where $\alpha \in \mathrm{At}(\mathbf{A})$.
- From CM varieties to Difference Term (DT) varieties

Moreover, the generalization plays nicely with (2,3)-systems.

Congruence Completeness

Let $\mathcal{I} = (V, \dots)$ be a (2,3)-system.

Definition

If $x, y \in V$ and $\theta \in \mathrm{Con}(\mathbf{P}_x)$, write

$$\mathbf{P}_y \equiv (\mathbf{P}_x \mod \theta) \qquad (\text{also} \quad h : \mathbf{P}_y \equiv (\mathbf{P}_x \mod \theta)\ )$$

to mean $R_{x,y} = \mathrm{graph}(h)$ where $h : \mathbf{P}_x \twoheadrightarrow \mathbf{P}_y$ and $\ker(h) = \theta$.

Definition

$\mathcal{I}$ is **congruence complete** if for all $x \in V$ and $\theta \in \mathrm{Con}(\mathbf{P}_x)$ there exists $y \in V$ such that $\mathbf{P}_y \equiv (\mathbf{P}_x \mod \theta)$.

Remark. We can always assume that $\mathcal{I}$ is congruence complete.

Difference term varieties

Definition

$\mathcal{V}$ is a **difference term** (DT) variety if it has a term $d(x, y, z)$ such that

- $d(x, x, y) \approx y$
- $d(a, b, b) = a$ whenever (a, b) belongs to an abelian congruence of a member of $\mathcal{V}$.

Recall

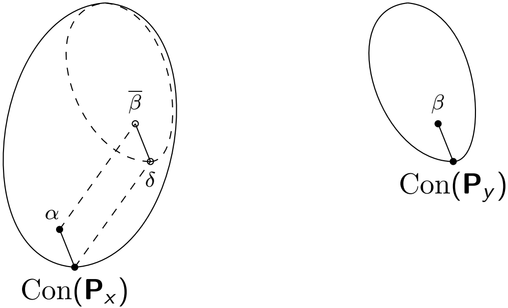
1. There is an idempotent linear Maltsev characterization.
2. CM $\Rightarrow$ DT $\Rightarrow$ Taylor.

Fix $\mathcal{I} = (V, \ldots)$, cong. comp. (2,3)-system over **A** in a DT variety.

Definition

1. $\mathrm{At}(\mathcal{I}) := \{(x, \alpha) \,:\, x \in V,\, \alpha \in \mathrm{At}(\mathbf{P}_x)\}$.
2. Given $(x, \alpha), (y, \beta) \in \mathrm{At}(\mathcal{I})$, we write $(x, \alpha) \to (y, \beta)$ iff $h : \mathbf{P}_y \equiv (\mathbf{P}_x \bmod \delta)$ and $(0_A, \alpha) \nearrow (\delta, \overline{\beta})$ where $\overline{\beta} = h^{-1}(\beta)$.

$\mathbf{P}_x \xrightarrow{R_{x,y}} \mathbf{P}_y$ and



3. Let $\approx$ be the smallest equiv. relation on $\mathrm{At}(\mathcal{I})$ containing $\to$. Call this **quasi-similarity**.

Components

$\mathcal{J} = (V, \ldots)$, a cong. comp. (2,3)-system over **A** in a DT variety.

Lemma

$(x, \alpha) \approx (x, \beta)$ iff $\alpha \Bumpeq \beta$ in $\mathrm{At}(\mathbf{P}_x)$.

Let C be a $\approx$-block and put $C_1 := \mathrm{proj}_1(C)$.

Corollary

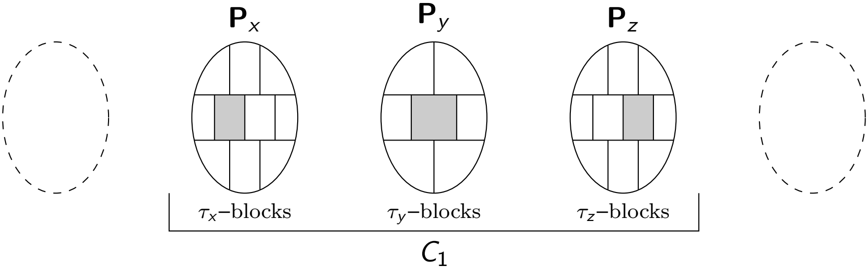
If $x \in C_1$, then $\{\alpha : (x, \alpha) \in C\}$ is a $\Bumpeq$-block in $\mathrm{At}(\mathbf{P}_x)$.

Definition

For $x \in C_1$, let $\tau_x := \bigvee\{\alpha : (x, \alpha) \in C\}$. $\quad (\tau_x \in \mathrm{Geom}(\mathbf{P}_x)$.)

Call C_1 a **component** of $\mathcal{J}$, with corresponding τ_x $(x \in C_1)$.

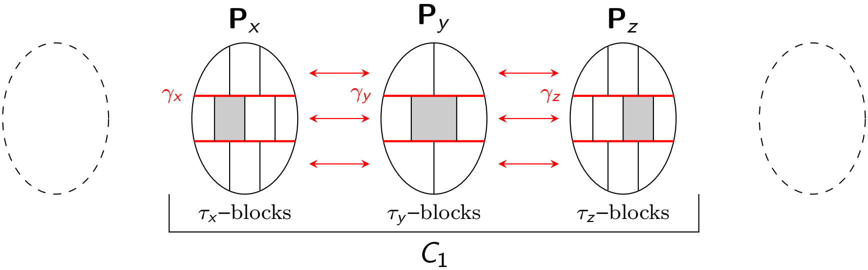
Summary: each $\approx$-block C gives a component C_1 and a family of geometric congruences τ_x.



Easy Fact

$\mathrm{char}(\tau_x) = \mathrm{char}(\tau_y)$ for all $x, y \in C_1$.

Hence each $\mathcal{I}[\bar{s}]$ encodes a linear system, $\bar{s} \in \mathrm{Sol}((\mathcal{I}|_{C_1})/\tau)$.



Fix a component C_1 with $(\tau_x : x \in C_1)$.

For $x \in C_1$ define $\gamma_x := \mathrm{ann}(\tau_x)$. (Blocks shown in red.)

Lemma

$\overline{R}_{x,y} : \mathbf{P}_x/\gamma_x \cong \mathbf{P}_y/\gamma_y \quad \forall x, y \in C_1.$

Conjecture

Suppose $\overline{s}, \overline{s}'$ are solutions to $(\mathcal{I}|_{C_1})/\tau$ belonging to the same γ-blocks. Then $\mathrm{Sol}(\mathcal{I}[\overline{s}]) \neq \varnothing$ iff $\mathrm{Sol}(\mathcal{I}[\overline{s}']) \neq \varnothing$.

Algorithm?

If the previous conjecture is true, then we can always reduce $\mathcal{I}$ to a (2,3)-subsystem which is congruence complete and satisfies:

- For every component C_1 and all $x, y \in C_1$,

$$\mathrm{proj}_{x,y}(\mathrm{Sol}(\mathcal{I}|_{C_1})) = R_{x,y}.$$

Definition

Say that $\mathcal{I}$ is **full on components** if it has this property.

Wild Conjecture (DT)

If $\mathcal{I}$ is congruence complete, full on components and nonempty, then $\mathrm{Sol}(\mathcal{I}) \neq \varnothing$.

I have a plan to prove this in the Maltsev case. The plan requires overcoming an obstacle.

Obstacle

Suppose $\mathcal{I}$ is congruence complete (2,3)-system over a Maltsev template, is full on components, and nonempty. If:

1. $X \subseteq V$ and $u \in V$.
2. $\mathbf{P}_u$ is subdirectly irreducible.
3. X "determines" u in the following sense: for all $s, t \in \mathrm{Sol}(\mathcal{I}|_{X \cup \{u\}})$, if $s|_X = t|_X$ then $s(u) = t(u)$.
4. X is "minimal" with respect to item (3) in the following sense: for each $x \in X$, if $[x] = \{y \in V : \mathbf{P}_y \equiv (\mathbf{P}_x \bmod \theta) \text{ with } \theta \neq 0\}$ and $X' = (X \setminus \{x\}) \cup [x]$, then X' fails to determine u.
5. $|X| > 1$.

Prove that $X \cup \{u\}$ is contained in some component.

OK, I'd better stop ...