Constraints in Universal Algebra

Ross Willard

University of Waterloo, CAN

SSAOS 2014
September 7, 2014
Lecture 1

Outline

Lecture 1: Intersection problems and congruence SD($\wedge$) varieties

Lecture 2: Constraint problems in ternary groups (and generalizations)

Lecture 3: Constraint problems in Taylor varieties

Almost all algebras will be finite.

Quiz!

Fix an algebra **A**. Suppose

- $\mathbf{C}, \mathbf{D} \leq \mathbf{A}^n$ for some $n \geq 3$
- $\mathrm{proj}_{i,j}(C) = \mathrm{proj}_{i,j}(D)$ for all $1 \leq i < j \leq n$.

Question: Does it follow that $C \cap D \neq \varnothing$?

Answer: No, of course not!

- Let **A** be the set $\{0,1\}$ (with no operations – ha ha!).
- Let $n = 3$ and put

$$\begin{aligned} C &= \{\mathbf{x} \in \{0,1\}^3 : x_1 + x_2 + x_3 = 0 \pmod{2}\} \\ D &= \{\mathbf{x} \in \{0,1\}^3 : x_1 + x_2 + x_3 = 1 \pmod{2}\} \end{aligned}$$

- $\mathbf{C}, \mathbf{D} \leq \mathbf{A}^3$ and $\mathrm{proj}_{i,j}(C) = \mathrm{proj}_{i,j}(D) = \{0,1\}^2$ for all $i < j$, yet $C \cap D = \varnothing$.

Apology

I'm sorry. Choosing $\mathbf{A}$ to be a set with no operations is pathetic.

Better example: $\mathbf{A} = (\{0,1\}; x{+}y{+}z \pmod 2)$ with the same $\mathbf{C},\mathbf{D} \leq \mathbf{A}^3$.

More generally, for any R-module ${}_RA$, take the associated **affine** R**-module**

$$\mathbf{A} \; = \; (\, A\,;\, x{-}y{+}z,\, \{r\,x{+}(1{-}r)y \;:\; r \in R\}\,)$$

and let C, D be different cosets of $\{(x,y,z) \,:\, x+y+z=0\} \leq \mathbf{A}^3$.

Harder Quiz

Bonus Problem: For which $\mathbf{A}$ is the answer "Yes"?

(The question: if $\mathbf{C}, \mathbf{D} \leq \mathbf{A}^n$ and $\mathrm{proj}_{i,j}(C) = \mathrm{proj}_{i,j}(D)$ for all $i < j$, does it follow that $C \cap D \neq \varnothing$?)

Subproblem: are there any $\mathbf{A}$ for which the answer is "Yes"?

Answer: Of course!

- Any algebra $\mathbf{A}$ having a constant term operation has this property. (So any group, ring, module, ...)
  - This is cheating.
  - We can forbid cheating by requiring that $\mathbf{A}$ be **idempotent**, i.e., all 1-element subsets must be subalgebras.

Problem: are there any idempotent $\mathbf{A}$ for which the the answer is "Yes"?

The k-intersection property

Definition (Valeriote). Let **A** be an algebra.

1. If $C, D \subseteq A^n$ and $0 < k \leq n$, we write $C \overset{k}{=} D$ to mean $\mathrm{proj}_J(C) = \mathrm{proj}_J(D)$ for all $J \subseteq \{1, \ldots, n\}$ satisfying $|J| = k$.
2. For example:
   - $C \overset{1}{=} D$ iff $\mathrm{proj}_i(C) = \mathrm{proj}_i(D)$ for all i.
   - $C \overset{2}{=} D$ iff $\mathrm{proj}_{i,j}(C) = \mathrm{proj}_{i,j}(D)$ for all $i < j$.
   - $C \overset{n}{=} D$ iff $C = D$.
3. We say that **A** has the **k-intersection property** (or k-**IP**) if for all $n > k$ and every family $\{\mathbf{C}_t \leq \mathbf{A}^n \,:\, t \in T\}$,

$$\left(C_s \overset{k}{=} C_t \text{ for all } s, t \in T\right) \;\Rightarrow\; \bigcap_{t \in T} C_t \neq \varnothing.$$

Note: 1-IP $\Rightarrow$ 2-IP $\Rightarrow$ 3-IP $\Rightarrow$ 4-IP $\Rightarrow \cdots$

Problem (modified): are there any idempotent algebras with 2-IP? What about 1-IP? Or k-IP for some k?

Theorem

1. Every lattice (or lattice expansion) has 2-IP.
2. Every finite semilattice (or expansion) has 1-IP.

Proof.
(1) Every lattice (or lattice expansion) $\mathbf{L}$ has a *majority term*

$$m(x,x,y) = m(x,y,x) = m(y,x,x) = x \qquad \text{for all } x,y \in L.$$

Hence for any $\mathbf{C} \leq \mathbf{L}^n$, C is determined by $(\mathrm{proj}_{i,j}(C) : 1 \leq i < j \leq n)$ (Baker-Pixley 1975).

Thus if $\{\mathbf{C}_t \leq \mathbf{L}^n \ : \ t \in T\}$ satisfies $C_s \overset{2}{=} C_t$ $\forall s,t$, then $C_s = C_t$ $\forall s,t$.

So $\bigcap C_t \neq \varnothing$.

Generalization. If $\mathbf{A}$ has a $(k+1)$-ary **near unanimity** (**NU**) term, then $\mathbf{A}$ has k-IP. (Again by Baker-Pixley)

Theorem

1. Every lattice (or lattice expansion) has 2-IP.
2. Every finite semilattice (or expansion) has 1-IP.

Proof.
(2) Suppose $\mathbf{L}$ is finite and has a semilattice term $\wedge$.

For any $\mathbf{C} \leq \mathbf{L}^n$, the $\wedge$-least element of $\mathbf{C}$ is determined by $(\mathrm{proj}_i(C) : 1 \leq i \leq n)$.

Thus if $\{\mathbf{C}_t \leq \mathbf{L}^n \,:\, t \in T\}$ satisfies $C_s \stackrel{1}{=} C_t$ $\forall s, t$, then all the $\mathbf{C}_s$ have the same $\wedge$-least element.

So $\bigcap C_t \neq \varnothing$. □

Summary

Idempotent algebras that have k-IP for some k:

- Lattices
- NU algebras
- Finite semilattices

Idempotent algebras that do not have k-IP for any k:

- Sets (pathetic, but true)
- Affine R-modules

Question: What *algebraic* property separates "lattices, NU algebras and semilattices" from "sets and affine R-modules"?

Answer: Congruence meet semi-distributivity

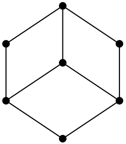
Meet Semi-Distributivity (SD(∧))

Definition. A lattice **L** is **meet semi-distributive** (or **SD(∧)**) if it satisfies the implication

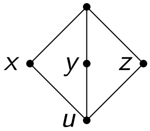
$$x \wedge y = x \wedge z =: u \quad \Rightarrow \quad x \wedge (y \vee z) = u.$$

Basic facts:

1. Every distributive lattice is SD(∧).
2. There exist SD(∧) lattices that are not modular. E.g.,



3. $\mathbf{M}_3$ is **not** SD(∧):



Congruence SD($\wedge$)

Definition.

1. An algebra is **congruence SD($\wedge$)** if its congruence lattice is SD($\wedge$).
2. A variety is **congruence SD($\wedge$)** if every algebra in the variety is congruence SD($\wedge$).

Theorem (Lipparini 1998; Kearnes, Szendrei 1998; Kearnes, Kiss 2013; cf. Hobby, McKenzie 1988)

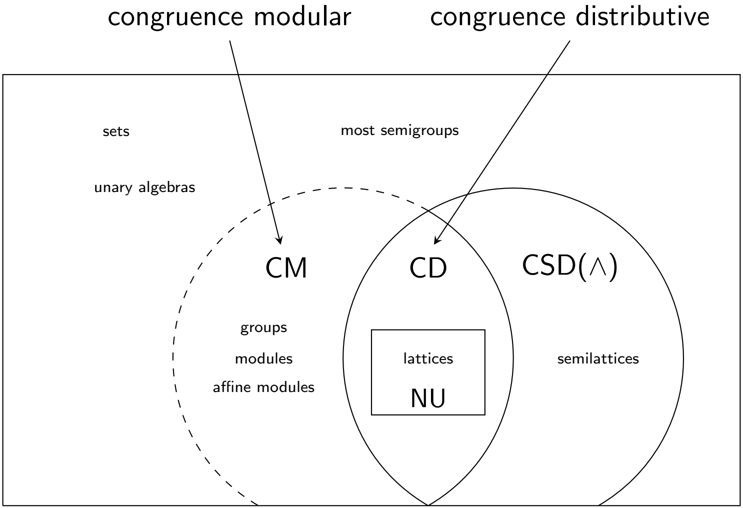
For a variety $\mathcal{V}$, the following are equivalent:

1. $\mathcal{V}$ is congruence SD($\wedge$).
2. $\mathbf{M}_3$ does not embed into $\mathrm{Con}(\mathbf{B})$, for any $\mathbf{B} \in \mathcal{V}$.

If $\mathcal{V}$ is idempotent, then we can add

3. No nontrivial algebra $\mathbf{B} \in \mathcal{V}$ is a term reduct of an affine R-module.

Congruence SD(∧) varieties



Valeriote's observation

Theorem (Valeriote 2009)

Assume $\mathbf{A}$ is finite and idempotent.

If $\mathbf{A}$ has k-IP for some k, then $\mathbf{HSP}(\mathbf{A})$ is CSD($\wedge$).

Proof.

- Assume $\mathbf{HSP}(\mathbf{A})$ is not CSD($\wedge$).
- By the previous theorem, there exists a nontrivial $\mathbf{B} \in \mathcal{V}$ which is a term reduct of an affine R-module $\mathbf{M}$.
- We can assume $\mathbf{B} \in \mathbf{HSP}_{fin}(\mathbf{A})$.
- Assume $\mathbf{A}$ has k-IP; then so does every algebra in $\mathbf{HSP}_{fin}(\mathbf{A})$.
- Hence $\mathbf{B}$ has k-IP.
- Hence $\mathbf{M}$ has k-IP, but we can show this is impossible. □

Valeriote's conjecture

Conjecture (Valeriote 2009)

And conversely.

That is, if **A** is finite, idempotent, and **HSP**(**A**) is CSD($\wedge$), then **A** has k-IP for some k.

Theorem (Barto 2014 ms)

Valeriote's conjecture is true.

In fact, if **A** is finite and **HSP**(**A**) is CSD($\wedge$), then **A** has 2-IP.

This is a surprising result with a beautiful proof.

Constraint Satisfaction Problem (CSP)

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

An **instance of CSP(A)** of degree n is a list

$$(s_1, C_1), (s_2, C_2), \ldots, (s_p, C_p)$$

of "specifications" of subalgebras of $\mathbf{A}^n$ (of a certain kind).

- Each s_i is a non-empty subset of $\{1, 2, \ldots, n\}$.
- Each C_i is a non-empty subuniverse of $\mathbf{A}^{s_i}$.
- (s_i, C_i) "specifies" the subalgebra $\{\mathbf{a} \in A^n : \mathrm{proj}_{s_i}(\mathbf{a}) \in C_i\}$ of $\mathbf{A}^n$.
  - I denote this subalgebra by $[\![s_i, C_i]\!]$.

Computer Science jargon:

- $\{1, 2, \ldots, n\}$ is the **set of variables**.
- Each (s_i, C_i) is a **constraint**.
- s_i is the **scope** of (s_i, C_i). C_i is the **constraint relation**.

Example

Let $\mathbf{A} = (\{0,1\}, \wedge)$. (The 2-element semilattice)

With $n = 4$, define

$$\begin{aligned} s_1 &= \{2,3,4\} \\ C_1 &= \{\mathbf{a} \in A^{\{2,3,4\}} : a_2 \leq a_3 \leq a_4\} \\ &= \{(0,0,0), (0,0,1), (0,1,1), (1,1,1)\}. \end{aligned}$$

The subalgebra of $\mathbf{A}^4$ "specified" by (s_1, C_1) is

$$[\![s_1, C_1]\!] := \{(a_1, a_2, a_3, a_4) \in A^4 : a_2 \leq a_3 \leq a_4\}.$$

Similarly define $(s_2, C_2), (s_3, C_3)$ by

$$\begin{aligned} s_2 &= \{1,3,4\}, \qquad C_2 = \{\mathbf{a} \in A^{\{1,3,4\}} : a_3 \leq a_4 \leq a_1\} \\ s_3 &= \{1,2,4\}, \qquad C_3 = \{\mathbf{a} \in A^{\{1,2,4\}} : a_4 \leq a_1 \leq a_2\}. \end{aligned}$$

$(s_1, C_1), (s_2, C_2), (s_3, C_3)$ is an instance of CSP($\mathbf{A}$).

Solutions

In general, given a CSP($\mathbf{A}$) instance $(s_1, C_1), \ldots, (s_p, C_p)$, we ask whether

$$[\![s_1, C_1]\!] \cap \cdots \cap [\![s_p, C_p]\!] \neq \varnothing.$$

The elements of $[\![s_1, C_1]\!] \cap \cdots \cap [\![s_p, C_p]\!]$ (if any) are called **solutions**.

In the previous example, the subalgebras of $(\{0,1\}, \wedge)^4$ "specified" by the constraints are:

$$\begin{aligned} [\![s_1, C_1]\!] &:= \{\mathbf{a} \in \{0,1\}^4 : a_2 \leq a_3 \leq a_4\} \\ [\![s_2, C_2]\!] &:= \{\mathbf{a} \in \{0,1\}^4 : a_3 \leq a_4 \leq a_1\} \\ [\![s_3, C_3]\!] &:= \{\mathbf{a} \in \{0,1\}^4 : a_4 \leq a_1 \leq a_2\} \end{aligned}$$

This instance has two solutions, since

$$[\![s_1, C_1]\!] \cap [\![s_2, C_2]\!] \cap [\![s_3, C_3]\!] = \{\mathbf{a} \in \{0,1\}^4 : a_1 = a_2 = a_3 = a_4\}.$$

(2,3)-minimal instances

Definition

An instance $(s_1, C_1), \ldots, (s_p, C_p)$ of CSP($\mathbf{A}$) (say of degree n) is **(2,3)-minimal** if:

- For any two constraints $(s_i, C_i), (s_j, C_j)$, if

  $$J \subseteq s_i \cap s_j \quad \text{and} \quad 1 \leq |J| \leq 2$$

  then $\mathrm{proj}_J(C_i) = \mathrm{proj}_J(C_j)$.
- For every 3-element subset $J \subseteq \{1, \ldots, n\}$ there exists a constraint (s_i, C_i) such that $J \subseteq s_i$.

Remark. The first requirement is like $[\![s_i, C_i]\!] \stackrel{2}{=} [\![s_j, C_j]\!]$, but only requiring it on coordinates in their common scopes.

With $\mathbf{A} = (\{0,1\}, \wedge)$, recall the instance with three constraints:

$$\begin{aligned} s_1 &= \{2,3,4\}, \qquad C_1 = \{\mathbf{a} \in A^{\{2,3,4\}} : a_2 \le a_3 \le a_4\} \\ s_2 &= \{1,3,4\}, \qquad C_2 = \{\mathbf{a} \in A^{\{1,3,4\}} : a_3 \le a_4 \le a_1\} \\ s_3 &= \{1,2,4\}, \qquad C_3 = \{\mathbf{a} \in A^{\{1,2,4\}} : a_4 \le a_1 \le a_2\}. \end{aligned}$$

Surprise Quiz: is this instance (2,3)-minimal?

- For any two constraints $(s_i, C_i), (s_j, C_j)$, if $J \subseteq s_i \cap s_j$ and $|J| \le 2$, then $\mathrm{proj}_J(C_i) = \mathrm{proj}_J(C_j)$.
- For every 3-element subset $J \subseteq \{1, \ldots, n\}$ there exists a constraint (s_i, C_i) such that $J \subseteq s_i$.

Answers

- **No**: $\mathrm{proj}_{2,4}(C_1) \neq \mathrm{proj}_{2,4}(C_3)$.
- **No**: $\{1,2,3\}$ is not contained in the scope of any constraint.

Main Theorem

Theorem (Barto 2014 ms, improving Barto, Kozik 2009; Bulatov ms)

Suppose $\mathbf{A}$ is finite and $\mathbf{HSP}(\mathbf{A})$ is CSD($\wedge$). Then every (2,3)-minimal instance of CSP($\mathbf{A}$) has a solution.

Proof: Prague absorption.

Corollary (Barto)

If $\mathbf{A}$ is finite and $\mathbf{HSP}(\mathbf{A})$ is CSD($\wedge$), then $\mathbf{A}$ has 2-IP.

Proof. Given $\{\mathbf{C}_t \leq \mathbf{A}^n : 1 \leq t \leq p\}$ with $C_s \stackrel{2}{=} C_t$ for all s, t, consider the CSP($\mathbf{A}$) instance

$$(\{1,\ldots,n\}, C_1),\ (\{1,\ldots,n\}, C_2),\ \ldots\ ,\ (\{1,\ldots,n\}, C_p).$$

It is (2,3)-minimal. □

Application (if time)

Definition. Let **A** be an algebra. A **weak majority term** for **A** is a term $t(x, y, z)$ satisfying the idempotent law $t(x, x, x) = x$ and

$$t(x, x, y) \ = \ t(x, y, x) \ = \ t(y, x, x) \qquad \text{for all } x, y \in A.$$

Similarly, for any $k \geq 2$ we can define a k-ary **weak NU** term (**WNU**).

Examples of WNUs

- For semilattices (or lattices) we can take $t(x_1, \ldots, x_n) = x_1 \wedge \cdots \wedge x_n$.
- For $(\mathbb{Z}_2, +)$ we have $t(x_1, \ldots, x_n) = x_1 + \cdots + x_n$ (for any **odd** $n \geq 3$).

Theorem (Kozik; in Kozik *et al* 2014?)

Let **A** be a finite algebra. The following are equivalent:

1. HSP(**A**) is congruence SD($\wedge$).
2. **A** has 3-ary and 4-ary WNU terms $t_1(x, y, z)$ and $t_2(x, y, z, w)$ satisfying $t_1(x, x, y) = t_2(x, x, x, y)$ for all $x, y \in A$.

Let **A** be a finite algebra. The following are equivalent:

1. HSP(**A**) is congruence SD($\wedge$).
2. **A** has 3-ary and 4-ary WNU terms $t_1(x, y, z)$ and $t_2(x, y, z, w)$ satisfying $t_1(x, x, y) = t_2(x, x, x, y)$ for all $x, y \in A$.

Proof sketch. We can assume **A** is idempotent.

(2) $\Rightarrow$ (1). Assume **A** has such WNUs but CSP(**A**) is **not** CSD($\wedge$).

Then $\exists$**B** $\in$ **HSP**(**A**) such that $|B| > 1$ and **B** is a term reduct of an affine R-module **M**.

B also has such WNUs, so **M** has such WNUs, contradiction.

(1) $\Rightarrow$ (2). (Variation of an argument due to E. W. Kiss)

Let $\mathbf{F}_2$ be the free algebra of rank 2 in **HSP**(**A**). Let $n = 3|F_2| + 1$.

One can define a (2,3)-minimal instance of CSP($\mathbf{F}_2$) of degree n, any solution of which will give the desired WNUs. (Details in Kozik *et al.*)

By Barto's theorem, a solution to the instance exists. □

Bibliography

K. A. Baker and A. F. Pixley, Polynomial interpolation and the Chinese remainder theorem for algebraic systems, *Math. Z.* **143** (1975), 165–174.

A. A. Bulatov, Bounded relational width, manuscript, 2009.

L. Barto, The collapse of the bounded width hierarchy, manuscript, 2014.

L. Barto and M. Kozik, Constraint satisfaction problems of bounded width, *FOCS 2009*, IEEE, 595–603.

D. Hobby and R. McKenzie, *The Structure of Finite Algebras*, Contemporary Mathematics **76**, Amer. Math. Soc., 1988.

K. A. Kearnes and E. W. Kiss, The shape of congruence lattices, *Mem. Amer. Math. Soc.* **222** (2013), no. 1046.

K. A. Kearnes and Á. Szendrei, The relationship between two commutators, *Internat. J. Algebra Comput.* **8** (1998), 497–531.

M. Kozik, A. Krokhin, M. Valeriote and R. Willard, Characterizations of several Maltsev conditions, *Algebra Universalis*, to appear.

P. Lipparini, A characterization of varieties with a difference term, II: neutral = meet semi-distributive, *Canad. Math. Bull.* **41** (1998), 318–327.

M. Valeriote, A subalgebra intersection property for congruence distributive varieties, *Canad. J. Math*. **61** (2009), 451–464.