Universal algebra and CSP Tutorial

Ross Willard

University of Waterloo, CAN

Banff International Research Station
November 24, 2014

Outline

1. Basic objects
2. Avoiding structures
3. Maltsev conditions
4. Omitting types (Tame congruence theory)
5. Connection to CSP
6. Other buzzwords
   - Clones
   - Absorption

Basic Objects

Algebra: A structure $\mathbf{A} = (A, (f_i : i \in I))$ having functions, no relations.

Identity: Any sentence of the form $\forall \mathbf{x}[s(\mathbf{x}) = t(\mathbf{x})]$, s, t terms.

Equational class: Any class of algebras axiomatized by identities.

- Aka **variety**.
- Examples: {groups}, {abelian groups}, {R-modules}, etc.
- Varieties contain **free algebras**.

Special cases:

- **Idempotent** algebras/varieties: those for which every term s satisfies $s(x, x, \ldots, x) = x$ $(\forall x)$.
- **Finite** algebras (those with finite domain).
- $V(\mathbf{A}) = \mathrm{Mod}(\mathrm{Th}_{id}(\mathbf{A}))$, the variety **generated by A**.

Avoiding structures

Let $\mathbf{A} = (A, \ldots)$ be an algebra, and $\mathcal{V}$ a variety.

1. A relation $R \subseteq A^n$ is **compatible** with $\mathbf{A}$ if it is (the domain of) a subalgebra of $\mathbf{A}^n$.
2. A relational structure $\mathbb{A} = (A, (R_j : j \in J))$ is **compatible** with $\mathbf{A}$ if each of its relations R_j is compatible.
3. $\mathcal{V}$ **admits** a relational structure $\mathbb{B}$, if $\mathbb{B}$ is compatible with some $\mathbf{B} \in \mathcal{V}$; otherwise, $\mathcal{V}$ **avoids** $\mathbb{B}$.
4. $\mathcal{V}$ **avoids** a class $\mathcal{K}$ of relational structures if $\mathcal{V}$ avoids every $\mathbb{B} \in \mathcal{K}$.

Example

Example

The variety $\{\text{groups}\}$ avoids the class $\{\text{nontrivial posets}\}$.

Proof. Suppose $\mathbf{G}$ is a group and (G, E) is a poset compatible with $\mathbf{G}$.

This means E is a subgroup of $\mathbf{G}^2$.

Suppose $a, b \in G$ and aEb.

Then $(a, a), (a, b), (b, b) \in E$, so

$$(b, a) \;=\; (a, a)(a, b)^{-1}(b, b) \;\in\; E.$$

Thus aEb implies bEa.

Hence (G, E) is trivial. □

Theorem (Hagemann & Mitschke, 1973)

For any variety $\mathcal{V}$, tfae:

1. *$\mathcal{V}$ avoids $\mathcal{K} = \{$nontrivial posets$\}$.*
2. *For some $n \geq 1$, $\exists$ terms $p_1(x, y, z), \ldots, p_n(x, y, z)$ such that*

$$\mathcal{V} \models \forall xy \left[x = p_1(x, y, y) \;\&\; \bigwedge_{i=1}^{n-1} p_i(x, x, y) = p_{i+1}(x, y, y) \;\&\; p_n(x, x, y) = y \right].$$

Proof idea for (2) $\Rightarrow$ (1): Assuming $\mathbf{B} \in \mathcal{V}$, $\mathbf{E} \leq \mathbf{B}^2$, E is reflexive, and $(a, b) \in E$, evaluate the $p_i(x, y, z)$'s at $(a, a), (a, b), (b, b)$ to get

$$(b, c_1), (c_1, c_2), \ldots, (c_{n-1}, a) \in E.$$

The condition in (2) is an example of a **Maltsev condition**.

A **Maltsev condition** (on varieties) is a condition of the form

$$\bigvee_{n\in\omega} \underbrace{\left[\exists \underbrace{t_1, \ldots, t_{h(n)}}_{\text{terms}} \bigwedge_{i=1}^{k(n)} (\text{identities in the } t_j) \right]}_{C(n)}$$

Intuition: for "natural" classes $\mathcal{K}$, the varieties avoiding $\mathcal{K}$ "should" be characterized by a Maltsev condition, which "explains" why the varieties avoid $\mathcal{K}$.

Definition. A first-order sentence is a **finite product sentence** if it is true in $\mathbb{B}_1 \times \mathbb{B}_2$ whenever it is true in both factors.

Theorem (Taylor, 1973)

If $\mathcal{K}$ is definable by the negation of a finite product sentence, then "avoiding $\mathcal{K}$" is characterized by a Maltsev condition.

Many "classical" Maltsev conditions characterize the avoidance of "bad" configurations of compatible equivalence relations (aka **congruences**).

Example. $\mathcal{K}_{\neg DL}$ = the class of all structures $\mathbb{B} = (B, \alpha, \beta, \gamma)$ where

- α, β, γ are equivalence relations on B, and
- α, β, γ fail to satisfy the distributive law, i.e.,

$$\alpha \cap (\beta \vee \gamma) \neq (\alpha \cap \beta) \vee (\alpha \cap \gamma)$$

in the lattice of all equivalence relations on B.

Definition

A variety is **congruence distributive** (CD) if it avoids $\mathcal{K}_{\neg DL}$.

Theorem (Jónsson, 1967)

Being CD is characterized by a Maltsev condition.

Tame congruence theory

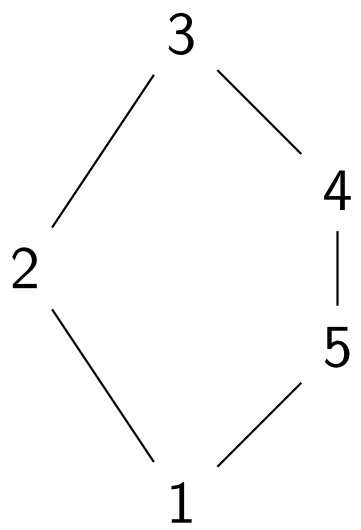
Developed by Hobby and McKenzie in the 1980s, about finite algebras.

- Discovers exactly 5 types of "local behaviour" of polynomial operations (i.e., terms with parameters).
- Called **type 1**, **type 2**,. . . ,**type 5**.
- If $\mathbf{A}$ is finite and $\mathcal{V} = V(\mathbf{A})$, can speak of $\mathcal{V}$ **omitting type i**.
- The types are naturally ordered:

For each **downset** S, it is natural to consider such $\mathcal{V}$ which omit S. E.g.,

- Omit $\{1\}$
- Omit $\{1, 2\}$
- Omit $\{1, 5\}$
- Omit $\{1, 2, 5\}$

etc.



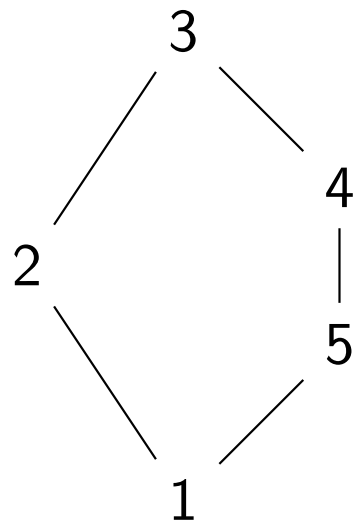
Theorem (Hobby & McKenzie, 1988)

For each downset S, among all varieties of the form $\mathcal{V} = V(\mathbf{A})$ with $\mathbf{A}$ finite, the varieties which omit S are characterized by a Maltsev condition.

- In each case, omitting S is characterized by avoiding a class of equivalence structures (i.e., by a condition on congruences).

  For example:

  - Omitting $\{1, 2\} \equiv$ "congruence meet semi-distributivity."
  - Omitting $\{1, 4, 5\} \equiv$ "congruence k-permutability for some k."



- If we restrict to **idempotent** $\mathcal{V}$, much simpler avoidance classes are known.

  (More later.)

Connection to CSP

Fix $\mathbb{A}$ – a finite relational structure in a finite signature.

The complexity of CSP($\mathbb{A}$) is governed by the $\mathbb{B}$ which pp-interpret in $\mathbb{A}$.

For example: let

$$\begin{aligned}
\mathbb{B}_{3SAT} &= (\{0,1\},\ \text{all 3-ary relations}) \\
\mathbb{B}_{Horn} &= (\{0,1\},\ \text{all 3-ary Horn relations}) \\
&= (\{0,1\},\ \text{all subalgebras of } (2,\wedge)^3) \\
\mathbb{B}_{\leq} &= (\{0,1\},\ \leq, \{0\}, \{1\}) \\
\mathbb{B}_{\mathbb{Z}_p,1} &= (\mathbb{Z}_p,\ \text{“}x+y=z\text{”},\ \{1\}).
\end{aligned}$$

1. If $\mathbb{B}_{3SAT}$ is pp-interpretable in $\mathbb{A}$, then CSP($\mathbb{A}$) is NP-complete.
2. If $\mathbb{B}_{Horn}$ is pp-interpretable in $\mathbb{A}$, then CSP($\mathbb{A}$) is P-hard.
3. If $\mathbb{B}_{\leq}$ is pp-interpretable in $\mathbb{A}$, then CSP($\mathbb{A}$) is NL-hard.
4. If $\mathbb{B}_{\mathbb{Z}_p,1}$ is pp-interpretable in $\mathbb{A}$, then CSP($\mathbb{A}$) is Mod$_p$-hard.

Characterizing pp-interpretability

Fix $\mathbb{A}$ – a finite relational structure in a finite signature.

Let $\mathbf{Pol}(\mathbb{A})$ be the "richest" algebra compatible with $\mathbb{A}$.

- $=$ "the polymorphism algebra of $\mathbb{A}$"

Theorem ($\approx$ Bodnarčuk *et al*, 1969)

For any finite structure $\mathbb{B}$,

$$\mathbb{B} \text{ is pp-interpretable in } \mathbb{A} \iff \mathbb{B} \text{ is compatible with some } \mathbf{B} \in V(\mathbf{Pol}(\mathbb{A})).$$

$$\iff V(\mathbf{Pol}(\mathbb{A})) \text{ admits } \mathbb{B}.$$

Hence the complexity of CSP($\mathbb{A}$) is determined by the structures which $V(\mathbf{Pol}(\mathbb{A}))$ admits/avoids.

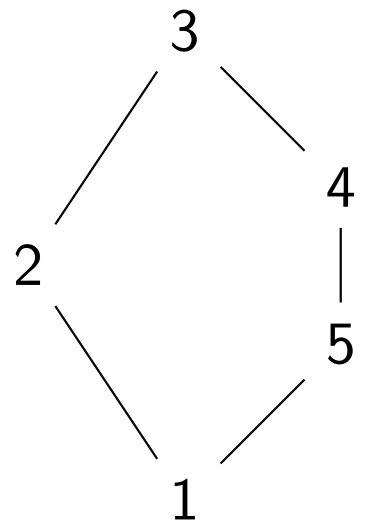
The idempotent case

Standard CSP assumption: $\mathbb{A}$ "has all constants" (as unary relations).

Hence $V(\mathbf{Pol}(\mathbb{A}))$ is **idempotent**: every f satisfies $f(x, x, \ldots, x) = x$.

Returning to Tame Congruence Theory: in the idempotent case,

1. $\mathcal{V}$ omits $\{1\}$ iff $\mathcal{V}$ avoids $\mathbb{B}_{3SAT}$.
2. $\mathcal{V}$ omits $\{1, 5\}$ iff $\mathcal{V}$ avoids $\mathbb{B}_{Horn}$.
3. $\mathcal{V}$ omits $\{1, 4, 5\}$ iff $\mathcal{V}$ avoids $\mathbb{B}_{\leq}$, iff $\mathcal{V}$ avoids {nontrivial posets}.
4. $\mathcal{V}$ omits $\{1, 2\}$ iff $\mathcal{V}$ avoids $\mathcal{K}_{Ab}$ where



$\mathcal{K}_{Ab} = \{\mathbb{B}_{G,b} : (G, +)$ an abelian group, $b \neq 0\}$.

The bad structures coincide with the (known) hard structures for CSP!

Algebraic Dichotomy Conjecture

Assume that $\mathbb{A}$ "has constants." Let $\mathcal{V} = V(\mathbf{Pol}(\mathbb{A}))$. $\mathcal{V}$ is idempotent.

$$\begin{array}{lcl} \text{CSP}(\mathbb{A}) \text{ is hard (NP-complete)} & \text{if} & \mathbb{B}_{3SAT} \text{ is pp-interpretable in } \mathbb{A} \\ & \iff & \mathcal{V} \text{ admits } \mathbb{B}_{3SAT} \\ & \iff & \mathcal{V} \text{ does not omit } \{1\}. \end{array}$$

We can't think of any other reason for $\text{CSP}(\mathbb{A})$ to be hard.

Algebraic Dichotomy Conjecture (Bulatov, Krokhin & Jeavons, 2005)

For finite $\mathbb{A}$ with constants, if $\mathcal{V}$ omits $\{1\}$, then $\text{CSP}(\mathbb{A})$ is in P.

Related conjectures:

1. If $\mathcal{V}$ omits $\{1, 2, 5\}$, then $\text{CSP}(\mathbb{A})$ is in NL.
2. If $\mathcal{V}$ omits $\{1, 2, 4, 5\}$, then $\text{CSP}(\mathbb{A})$ is in L.

Maltsev conditions for "omitting $\{1\}$"

Suppose $\mathcal{V} = V(\mathbf{A})$ with $\mathbf{A}$ finite. $\mathcal{V}$ omits $\{1\}$ iff $\mathcal{V}$ has ...

1. (Taylor) For some $n \geq 2$, a **Taylor** term $T(x_1, \ldots, x_n)$: idempotent and satisfies identities incompatible with T being a projection.
2. (Hobby, McKenzie) For some $n \geq 0$, terms $f_1(x, y, z), \ldots, f_n(x, y, z)$, $d(x, y, z)$ satisfying identities implying that $d(x, y, z)$ looks like $x - y + z$ on any block of any "abelian" congruence (in any member of the variety).
3. (Maróti, McKenzie) For some $n \geq 2$, a **weak near unanimity** (WNU) term $w(x_1, \ldots, x_n)$: idempotent and

$$w(y, x, x, \ldots, x) = w(x, y, x, \ldots, x) = \cdots = w(x, \ldots, x, y).$$

4. (Barto, Kozik) For some $n \geq 2$, a **cyclic** term operation of arity n.
5. (Siggers, with improvements) A 4-ary idempotent term $s(x, y, z, w)$ satisfying $\forall xyz[s(x, y, z, x) = s(y, x, y, z)]$.

Clones

Fix an algebra **A** (finite or infinite).

For $n \geq 1$ let $\mathrm{Clo}_n(\mathbf{A}) = \{\text{all term functions of } \mathbf{A} \text{ of arity } n\} \subseteq A^{A^n}$.

Definition

The **clone algebra** of **A** is the many-sorted algebra **Clo**(**A**), having

- Sorts $S_1, S_2, \ldots, S_n, \ldots$ where $S_n = \mathrm{Clo}_n(\mathbf{A})$.
- For $m, n \geq 1$, a "composition operation"

$$C_m^n : \; S_n \times \underbrace{S_m \times \cdots \times S_m}_{n} \to S_m.$$

- For $n \geq 1$, constants $e_1^n, \ldots, e_n^n \in S_n$ naming the n projection maps.

Fact: $\mathrm{Clo}(\mathbf{A}) \to \mathrm{Clo}(\mathbf{B})$ iff $V(\mathbf{B})$ satisfies every Maltsev condition satisfied by $V(\mathbf{A})$.

Prague Absorption

Prehistory: Bulatov (2006), Kiss & Valeriote (2007).
Godfathers: Barto & Kozik (2009, 2010, 2012, 2014).

The idea, roughly:

- Take your favourite idempotent linear Maltsev condition $\mathcal{C} = \bigvee_n C(n)$, whose identities include some of the form $f(x, \ldots, x, y, x, \ldots, x) = x$.
- Given a finite idempotent algebra $\mathbf{A}$ and subalgebra $\mathbf{B} \leq \mathbf{A}$: say $\mathbf{B}$ $\underline{\mathcal{C}\text{-absorbs}}$ $\mathbf{A}$ if for some n, $\mathbf{A}$ has terms which "satisfy $C(n)$ modulo B" in the following sense:
  - Identities not of the above form are satisfied in the usual sense.
  - For each identity of the form $f(x, \ldots, x, y, x, \ldots, x) = x$, require only that $f(B, \ldots, B, A, B, \ldots, B) \subseteq B$.
- Existence of proper absorbing algebras typically allows badness to be "shrunk." Absence of proper absorbing algebras imply some of the consequences of satisfying $\mathcal{C}$.

See e.g. Barto, Kozik & Stanowsky (2015) for some recent magic.

In closing

I was offered two tuturial hours.

You're welcome!