Universal algebra for CSP
Lecture 1

Ross Willard

University of Waterloo

Fields Institute Summer School
June 26–30, 2011
Toronto, Canada

Outline

Lecture 1 Basic universal algebra

Lecture 2 Basic CSP reductions and algorithms

Lecture 3 Omitting types and the Classification conjectures

Lecture 4 Looking under the hood: examples of algebra in action

Clones of operations

(Finitary) *operation* on A: any total function

$$f : \underbrace{A \times \cdots \times A}_{n} \to A, \quad n \geq 1.$$

Definition

A *clone* on the set A is any set $\mathcal{C}$ of operations on A which

- Is *closed under composition*, and
- Contains all the *projections* $\mathrm{pr}^A_{n,i} : A^n \to A$ (where $\mathrm{pr}^A_{n,i}(\mathbf{x}) = \mathbf{x}[i]$).

Notation: $\mathcal{C}_{[n]}$ denotes the set of n-ary members of $\mathcal{C}$.

Closure under composition means the following: $\forall n, k \geq 1$, $\forall f \in \mathcal{C}_{[k]}$, $\forall g_1, \ldots, g_k \in \mathcal{C}_{[n]}$, the n-ary operation $f \circ (g_1, \ldots, g_k)$ defined by

$$(f \circ (g_1, \ldots, g_k))(\mathbf{a}) \;:=\; f(g_1(\mathbf{a}), \ldots, g_k(\mathbf{a}))$$

is in $\mathcal{C}_{[n]}$.

Easy fact

If $\mathcal{C}$ is a clone and $f \in \mathcal{C}_{[n]}$, then other members of $\mathcal{C}$ include:

1. The $2n$-ary operation $g : A^{2n} \to A$ given by

$$(x_1, x_2, \ldots, x_{2n}) \longmapsto f(x_1, x_3, \ldots, x_{2n-1})$$

   Proof: factor g as

$$\begin{array}{ccccc} A^{2n} & \xrightarrow{\text{proj's}} & A^n & \xrightarrow{f} & A \\ (x_1, x_2 \ldots, x_{2n}) & \longmapsto & (x_1, x_3, \ldots, x_{2n-1}) & \longmapsto & f(x_1, x_3, \ldots, x_{2n-1}). \end{array}$$

   Thus $g = f \circ (\mathrm{pr}^A_{2n,1}, \mathrm{pr}^A_{2n,3}, \ldots, \mathrm{pr}^A_{2n,2n-1})$.

2. The 2-ary operation $h(x, y) := f(x, \ldots, x, y)$.

   Proof: $h = f \circ (\mathrm{pr}^A_{2,1}, \ldots, \mathrm{pr}^A_{2,1}, \mathrm{pr}^A_{2,2})$.

3. Any function obtained by permuting the variables of f.

Examples of clones

1. The set of *all* operations on A.
2. $\mathcal{C} = \bigcup_n \{\mathrm{pr}^A_{n,i} : 1 \leq i \leq n\}$.
3. $A = \{0,1\}$, $\mathcal{C} = \{\text{all } \textit{monotone} \text{ boolean functions}\}$.
4. Let $(A,+)$ be a (real) vector space. For $n \geq 1$ put

$$\mathcal{C}_{[n]} \quad = \quad \{r_1x_1 + \cdots + r_nx_n \ : \ r_i \in \mathbb{R},\ r_i \geq 0, \text{ and } \sum_{i=1}^{n} r_i = 1\},$$

and $\mathcal{C} = \bigcup_n \mathcal{C}_{[n]}$, the clone of *convex linear combination functions* on A.

5. Given any set $\mathcal{F}$ of operations on A, there is a clone *generated* by $\mathcal{F}$.

Algebras

Definition

A (*universal*) *algebra* is any structure of the form $\mathbf{A} = (A; \mathcal{C})$ where $A \neq \varnothing$ and $\mathcal{C}$ is a clone of operations on A.

- A is the *domain* (or *universe*, *underlying set*) of $\mathbf{A}$.
- $\mathcal{C}$ is the *clone of* $\mathbf{A}$.

Caveats:

1. This defines an *unsigned* (or *non-indexed*) algebra.
2. For a *signed* (or *indexed*) algebra, must add a *signature*:
    1. Roughly speaking, a scheme for "naming" the operations in $\mathcal{C}$.
    2. Permits us to coordinate operations of a signed algebra with those of any other algebra having the same signature.

(More caveats)

2. Historically (and in practice), we consider $(A;\mathcal{F})$ to be an algebra whenever $\mathcal{F}$ is a *set* (not necessarily a clone) of operations.
3. When doing so, the *proper* algebra we have in mind is $(A;\mathrm{Clo}(\mathcal{F}))$, where $\mathrm{Clo}(\mathcal{F})$ is the clone of operations generated by $\mathcal{F}$.

Example: Let $A = \{0,1\}$ and $\mathcal{F} = \{\min(x,y), \max(x,y), \underline{0}(x), \underline{1}(x)\}$.

- $\mathrm{Clo}(\mathcal{F}) = \{$all monotone boolean functions$\}$.
- $(A;\mathcal{F})$ is a "presentation" of $(A;\mathrm{Clo}(\mathcal{F}))$.

If $\mathbf{A} = (A;\mathcal{F})$ and/or $\mathbf{B} = (B;\mathcal{G})$ are improper, we say that $\mathbf{A}$ and $\mathbf{B}$ are *clone-equivalent* (or *term-equivalent*) if they present the same algebra: i.e., $A = B$ and $\mathrm{Clo}(\mathcal{F}) = \mathrm{Clo}(\mathcal{G})$.

Subalgebras

Let $\mathbf{A} = (A; \mathcal{C})$ be an algebra and $B \subseteq A$.

Definition

1. B is *compatible with* (or *closed under*) $\mathcal{C}$ if $\forall n \geq 1$, $\forall f \in \mathcal{C}_{[n]}$,

$$b_1, \ldots, b_n \in B \;\Rightarrow\; f(b_1, \ldots, b_n) \in B.$$

2. If also $B \neq \varnothing$, then $\mathbf{B} := (B; \{f{\restriction}_B : f \in \mathcal{C}\})$ is a *subalgebra* of $\mathbf{A}$.

Given $\varnothing \neq X \subseteq A$, we can speak of the subalgebra of $\mathbf{A}$ *generated* by X.

"Generation X" Lemma

Let $\mathbf{A} = (A; \mathcal{C})$ be an algebra and $X = \{b_1, \ldots, b_n\} \subseteq A$. The domain of the subalgebra of $\mathbf{A}$ generated by X is

$$\{f(b_1, \ldots, b_n) : f \in \mathcal{C}_{[n]}\}.$$

Powers and subpowers

Let $\mathbf{A} = (A; \mathcal{C})$ be an algebra.

Power $\mathbf{A}^2$ is the algebra with domain $A \times A = \{(a,b) : a,b \in A\}$ and, corresponding to each $f \in \mathcal{C}_{[n]}$, the operation

$$f^{[2]}((a_1,b_1),\ldots,(a_n,b_n)) \ := \ (f(\mathbf{a}), f(\mathbf{b})).$$

Define $\mathbf{A}^m$ $(m \geq 3)$, $\mathbf{A}^X$ $(X \neq \varnothing)$ similarly.

Product …of two or more signed algebras with common signature is defined in a similar way:

$$f^{\mathbf{A}\times\mathbf{B}}((a_1,b_1),\ldots,(a_n,b_n)) \ := \ (f^{\mathbf{A}}(\mathbf{a}), f^{\mathbf{B}}(\mathbf{b})).$$

Subpower = any subalgebra of a power.

Congruences and quotient algebras

Suppose $\mathbf{A} = (A; \mathcal{C})$ is an algebra and $E \subseteq A \times A$.

Definition

E is *compatible with* (or *invariant under*) $\mathcal{C}$ if $\forall n \geq 1$, $\forall f \in \mathcal{C}_{[n]}$,

$$(a_1, b_1), \ldots, (a_n, b_n) \in E \text{ implies } (f(\mathbf{a}), f(\mathbf{b})) \in E.$$

Definition

A *congruence* of $\mathbf{A}$ is any equivalence relation on A which is compatible with $\mathcal{C}$.

Every congruence E supports the construction of a *quotient algebra* $\mathbf{A}/E$ on the set $A/E := \{[a]_E \,:\, a \in A\}$ of E-blocks:

$$f^{\mathbf{A}/E}([a_1]_E, \ldots, [a_n]_E) := [f(\mathbf{a})]_E.$$

Homomorphic images

If $\mathbf{A}, \mathbf{B}$ are signed algebras with common signature, we can discuss *isomorphisms* and *homomorphisms* between them. (The obvious thing.)

Suppose $\alpha : A \to B$ is a function. The *kernel* of α is the relation on A given by

$$\ker(\alpha) := \{(a, a') \in A^2 \, : \, \alpha(a) = \alpha(a')\}.$$

Lemma

If $\alpha : \mathbf{A} \to \mathbf{B}$ is a homomorphism, then:

1. $\ker(\alpha)$ *is a congruence of* $\mathbf{A}$.
2. *If α is surjective, then* $\mathbf{B} \cong \mathbf{A}/\ker(\alpha)$.

Hence the homomorphic images of $\mathbf{A}$ are, up to isomorphism, exactly the quotient algebras $\mathbf{A}/E$ (E a congruence of $\mathbf{A}$).

Varieties

Definition

A *variety* is any class $\mathcal{V}$ of signed algebras with common signature which is closed under forming subalgebras, products, and homomorphic images.

Examples

1. Any class of signed algebras axiomatized by *identities*, e.g.,

$$x * (y * z) \approx (x * y) * z, \quad g(x, x, y) \approx y, \quad \text{etc}$$

2. For any fixed **A**, the variety *generated by* **A** is

$$\mathrm{HSP}(\mathbf{A}) = \{\text{all homomorphic images of subpowers of } \mathbf{A}\}.$$

Free algebras

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

Fact: For every n there exists $\mathbf{F} \in \mathcal{V}$ and $c_1, \ldots, c_n \in F$ such that

1. $\{c_1, \ldots, c_n\}$ generates $\mathbf{F}$.
2. (Universal Mapping Property): for any $\mathbf{B} \in \mathcal{V}$, every map $\alpha : \{c_1, \ldots, c_n\} \to B$ extends to a homomorphism $\mathbf{F} \to \mathbf{B}$.
3. An identity $LHS(\mathbf{x}) \approx RHS(\mathbf{x})$ in n variables holds universally in $\mathcal{V}$ iff it is true in $\mathbf{F}$ at $x_1 = c_1, \ldots, x_n = c_n$.

$\mathbf{F}$ and $(c_1, \ldots, c_n)$ are determined up to isomorphism by $\mathcal{V}$ and n.
Any such $\mathbf{F}$ is denoted $\mathbf{F}_{\mathcal{V}}(n)$.

Example: If $\mathbf{A} = (A; \mathcal{C})$ and $\mathcal{V} = \mathrm{HSP}(\mathbf{A})$, then:

- $\mathbf{F}_{\mathcal{V}}(n)$ may be taken to be the subalgebra of $\mathbf{A}^{A^n}$ with universe $\mathcal{C}_{[n]}$.
- The free generators are $\mathrm{pr}^A_{n,1}, \ldots, \mathrm{pr}^A_{n,n}$.

Relational structures

(Finitary) *relation* on A: any subset $R \subseteq A^n$, $n \geq 1$.

- I always assume $R \neq \varnothing$.

Definition

A *relational structure* is any $\mathbb{G} = (G; \mathcal{R})$ where $G \neq \varnothing$ and $\mathcal{R}$ is a set of relations on G.

- G is the *domain* (or *universe*, or *vertex set*).
- Relational structures are also called *templates*, *databases*, etc.

Of particular interest to CSP: the case when both G and $\mathcal{R}$ are *finite*.

Examples:

- (Simple) graphs $\mathbb{G} = (G; \{E\})$.
  Here $G = V(\mathbb{G})$ and E is a symmetric, irreflexive binary relation on G.
- Digraphs, edge-colored graphs, etc.

Compatible relations of an algebra

Let $\mathbf{A} = (A; \mathcal{C})$ be an algebra. Recall that:

1. A subset $B \subseteq A$ is compatible with $\mathcal{C}$ iff $\forall n \geq 1$, $\forall f \in \mathcal{C}_{[n]}$,
$$a_1, \ldots, a_n \in B \text{ implies } f(\mathbf{a}) \in B.$$
2. A subset $E \subseteq A^2$ is compatible with $\mathcal{C}$ iff $\forall n \geq 1$, $\forall f \in \mathcal{C}_{[n]}$,
$$(a_1, b_1), \ldots, (a_n, b_n) \in E \text{ implies } (f(\mathbf{a}), f(\mathbf{b})) \in E.$$

In preparation for a generalization,

Definition

Suppose f is an n-ary operation and R is a k-ary relation on the same set. We say that f *preserves* R if

$$\underbrace{(\underbrace{a_1, \ldots, z_1}_{k}), \ldots, (\underbrace{a_n, \ldots, z_n}_{k})}_{n} \in R \text{ implies } (f(\mathbf{a}), \ldots, f(\mathbf{z})) \in R.$$

Let $\mathbf{A} = (A; \mathcal{C})$ be an algebra.

Definition

A relation $R \subseteq A^k$ is *compatible with* $\mathbf{A}$ if it is preserved by every operation of $\mathbf{A}$.

- [Equivalently, iff R is (the domain of) a subalgebra of $\mathbf{A}^k$.]

Dually:

Let $\mathbb{G} = (A; \mathcal{R})$ be a relational structure.

Definition

An operation $f : A^n \to A$ is a *polymorphism* of $\mathbb{G}$ if it preserves every relation of $\mathbb{G}$.

- [Equivalently, iff f is a homomorphism from $\mathbb{G}^n$ to $\mathbb{G}$.]

Compatible structures

Definition

Let $\mathbf{A} = (A, \mathcal{C})$ be an algebra and let $\mathbb{G} = (A, \mathcal{R})$ be a relational structure having the same domain as $\mathbf{A}$.

We say that $\mathbb{G}$ is *compatible with* $\mathbf{A}$ if either of the following equivalent conditions hold:

- Every relation $R \in \mathcal{R}$ is compatible with $\mathbf{A}$.
- Every operation $f \in \mathcal{C}$ is a polymorphism of $\mathbb{G}$.

Example: let $\mathbf{A}$ be the 2-element lattice $(A; \max, \min)$ where $A = \{0, 1\}$.

- $\mathbf{A}$ is improper; I really mean $(A; \mathrm{Clo}(\{\max, \min\}))$.

Let $\mathbb{G} = (A; E)$ be the digraph pictured below:

[Note that $E = \{(0,0), (0,1), (1,1)\}$ is the usual order relation on $\{0, 1\}$.]

- Both max and min preserve E.
- [Thus every operation in the clone of $\mathbf{A}$ preserves E.]

Hence $\mathbb{G}$ is a compatible digraph of the algebra $\mathbf{A}$.

Algebraic dichotomies – a preview

Definition

A digraph $(V; E)$ is *reflexive* if $(a, a) \in E$ for all $a \in V$.

Theorem (Maltsev 1954)

Suppose $\mathbf{A} = (A; \mathcal{C})$ *is an algebra. Exactly one of the following conditions holds:*

1. *There exists a reflexive not-symmetric digraph* $\mathbb{G}$ *which is compatible with some member of* $\mathrm{HSP}(\mathbf{A})$*; or*
2. *There exists* $f \in \mathcal{C}_{[3]}$ *which satisfies* $f(x, x, y) \approx y$ *and* $f(x, y, y) \approx x$*.*

Equivalently: the clone of $\mathbf{A}$ contains an operation satisfying (2) iff *every* compatible reflexive digraph of a member of $\mathrm{HSP}(\mathbf{A})$ is symmetric.

(An operation satisfying the identities in (2) is called a *Maltsev operation*.)

(Proof, $\Rightarrow$):

Assume $\exists f \in \mathcal{C}_{[3]}$ satisfying the identities

$$f(x,x,y) \approx y \quad \text{and} \quad f(x,y,y) \approx x. \tag{2}$$

Let $\mathbb{G} = (B; E)$ be a reflexive digraph. Assume $\mathbb{G}$ is compatible with some $\mathbf{B} \in \mathrm{HSP}(\mathbf{A})$. (Must show E is symmetric.)

Assume $(a,b) \in E$.

Also know $(a,a),(b,b) \in E$.

As identities are preserved by subpowers and homomorphic images, the operation $f^{\mathbf{B}}$ of $\mathbf{B}$ corresponding to f also satisfies the identities (2).

E is compatible with $\mathbf{B}$ by assumption. In particular, E is preserved by $f^{\mathbf{B}}$.

As $(a,a),(a,b),(b,b) \in E$, this implies $(f^{\mathbf{B}}(a,a,b), f^{\mathbf{B}}(a,b,b)) \in E$.

I.e., $(b,a) \in E$. □

(Proof, $\Leftarrow$):

Assume that every reflexive digraph compatible with some member of $\mathrm{HSP}(\mathbf{A})$ is symmetric.

Let $\mathcal{V} = \mathrm{HSP}(\mathbf{A})$ and $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(2)$ with free generators c, d.

Let $\mathbf{E}$ be the subalgebra of $\mathbf{F}^2$ generated by $\{(c,c),(c,d),(d,d)\}$.

Claim: E is reflexive (as a binary relation on F)

Proof: Let $u \in F$. (Must show $(u,u) \in E$.)

By the "Gen X" Lemma, there exists $g \in \mathcal{C}_{[2]}$ with $g^{\mathbf{F}}(c,d) = u$.

As E is (the domain of) a subalgebra of $\mathbf{F}^2$, E is compatible with $\mathbf{F}$.

Hence E is preserved by $g^{\mathbf{F}}$.

As $(c,c),(d,d) \in E$ we get $(g^{\mathbf{F}}(c,d), g^{\mathbf{F}}(c,d)) \in E$, i.e., $(u,u) \in E$. □

Conclusion: $(F;E)$ is a reflexive digraph.

(Proof, $\Leftarrow$, continued)

So far: $\mathcal{V} = \mathrm{HSP}(\mathbf{A})$ and $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(2)$ with free generators c, d.

$\mathbf{E}$ is the subalgebra of $\mathbf{F}^2$ generated by $\{(c,c),(c,d),(d,d)\}$.

$(F;E)$ is a reflexive digraph compatible with $\mathbf{F} \in \mathrm{HSP}(\mathbf{A})$.

Using the assumption, we deduce E is symmetric.

As $(c,d) \in E$, this implies $(d,c) \in E$.

By the "Gen X" Lemma, there exists $f \in \mathcal{C}_{[3]}$ with

$$\begin{aligned} f^{\mathbf{F}^2}((c,c),(c,d),(d,d)) &= (d,c), \\ \text{i.e.,} \quad (f^{\mathbf{F}}(c,c,d), f^{\mathbf{F}}(c,d,d)) &= (d,c), \\ \text{i.e.,} \quad f^{\mathbf{F}}(c,c,d) = d \quad \text{and} \quad f^{\mathbf{F}}(c,d,d) &= c. \end{aligned}$$

By a property of free algebras, $f(x,x,y) \approx y$ and $f(x,y,y) \approx x$. $\square$