A Universal Algebra Primer for CSP

Benoit Larose 1 2

¹Department of Mathematics and Statistics Concordia University, Montréal

²Department of Mathematics Champlain Regional College, St-Lambert

UA, Logic and CSP American Institute of Mathematics, March 2008



The Paradigm

- Every Constraint Satisfaction Problem = a homomorphism problem CSP(B) for some relational structure B;
- to each structure **B** is associated an algebra A(**B**);
- the equational properties of A(B) control the descriptive and algorithmic complexity of the decision problem CSP(B).

Constraint Satisfaction Problems

Let $\Gamma = \{\theta_1, \dots, \theta_r\}$ be a constraint language, i.e. a set of relations on a finite set A.

The decision problem $CSP(\Gamma)$:

- Instance: variables x_1, \ldots, x_s and constraints $[(x_{i_1}, x_{i_2}, \ldots, x_{i_k}), \theta_i], [(x_{l_1}, x_{l_2}, \ldots, x_{l_m}), \theta_v], \ldots$
- **Question**: can one assign values a_1, \ldots, a_s to x_1, \ldots, x_s such that all constraints are satisfied, i.e.

$(a_{i_1},a_{i_2},\dots,a_{i_k}) \in \theta_j, (a_{l_1},a_{l_2},\dots,a_{l_m}) \in \theta_v,\dots \ ?$

Our goal:

to determine the algorithmic/descriptive complexity of $CSP(\Gamma)$.

Homomorphism Problems

Convenient to view $CSP(\Gamma)$ as follows:

Let $\mathbf{B} = \langle A; \theta_1, \dots, \theta_r \rangle$ be the relational structure on A whose basic relations are those in Γ ;

$$CSP(B) = \{C : C \rightarrow B\}$$

 ${f C} o {f B}$ means "there exists a homomorphism from ${f C}$ to ${f B}$ " i.e.

if $\mathbf{C} = \langle X; \rho_1, \dots, \rho_r \rangle$, there is a map $f : X \to A$ such that $f(\rho_i) \subseteq \theta_i$ for all i.

Both formulations are equivalent (Feder, Vardi)

Core structures

If ${\bf B}$ and ${\bf B}_0$ are homomorphically equivalent, i.e. if ${\bf B}_0 \to {\bf B}$ and ${\bf B} \to {\bf B}_0$, then

$$CSP(\mathbf{B}_0) = CSP(\mathbf{B}).$$

Hence we may always assume **B** is a core, i.e.

B has no proper retracts,

i.e.

every homomorphism from ${\bf B}$ to ${\bf B}$ is onto,

i.e.

of all structures equivalent to B, B has smallest universe.



The Dichotomy Conjecture

Dichotomy Conjecture (Feder-Vardi, 1993)

Every $CSP(\mathbf{B})$ is either in P or NP-complete.

Part 1: the Algebra associated to a CSP

Relational structure **B**↓

set of relations

↓

set of operations

↓

algebra A(**B**)

A Fundamental Duality

Relational structure \mathbf{B} \downarrow set of relations \uparrow set of operations \downarrow algebra $\mathbb{A}(\mathbf{B})$

A Fundamental Duality, cont'd

Let A be a finite set.

- Let $f: A^n \to A$ be an *n*-ary operation on A;
- Let $\theta \subseteq A^k$ be a k-ary relation on A.

A Fundamental Duality, cont'd

Let A be a finite set.

- Let $f: A^n \to A$ be an *n*-ary operation on A;
- Let $\theta \subseteq A^k$ be a k-ary relation on A.
- The operation f preserves the relation θ , or θ is invariant under f, if the following holds:

$$\begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \cdots & \vdots \\ a_{k,1} & \cdots & a_{k,n} \end{bmatrix} \xrightarrow{f} \begin{bmatrix} b_1 \\ \vdots \\ b_k \end{bmatrix}$$

Applying f to the rows of the matrix with columns in θ yields a tuple of θ .

A Fundamental Duality, cont'd

Example

On $\{0,1\}$ let \leq denote the usual ordering $\{(0,0),(0,1),(1,1)\}$. An operation f preserves \leq iff it is *monotonic*, i.e. $f(x_1,\ldots,x_n)\leq f(y_1,\ldots,y_n)$ whenever $x_i\leq y_i$ for all $1\leq i\leq n$.

$$\begin{bmatrix} x_1 & \cdots & x_n \\ | \wedge & \cdots & | \wedge \\ y_1 & \cdots & y_n \end{bmatrix} \xrightarrow{f} \begin{bmatrix} f(x_1, \dots, x_n) \\ | \wedge \\ f(y_1, \dots, y_n) \end{bmatrix}$$

Clones and Relational Clones

Let Γ be a set of relations on A.

$$Pol(\Gamma) = \{f : f \text{ preserves every } \theta \in \Gamma\};$$
 sets of operations of this form are clones.

Clones and Relational Clones

Let Γ be a set of relations on A.

$$Pol(\Gamma) = \{f : f \text{ preserves every } \theta \in \Gamma\};$$
 sets of operations of this form are clones.

• Let *F* be a set of operations on *A*.

$$Inv(F) = \{\theta : \theta \text{ is invariant under every } f \in F\};$$
 sets of relations of this form are relational clones.

Clones and Relational Clones

• Let Γ be a set of relations on A.

$$Pol(\Gamma) = \{f : f \text{ preserves every } \theta \in \Gamma\};$$
 sets of operations of this form are clones.

Let F be a set of operations on A.

$$Inv(F) = \{\theta : \theta \text{ is invariant under every } f \in F\};$$
 sets of relations of this form are relational clones.

Pol(Inv(F)) is the clone generated by F;
 Inv(Pol(Γ)) is the relational clone generated by Γ.

Clones ...

A constructive view of clones:

 g is in the clone generated by F iff it is obtained from members of F and projections by composition:

$$g(x, y, z, t) = f_1(x, f_2(y, x), f_3(f_2(t, z), y))$$

Clones ...

A constructive view of clones:

 g is in the clone generated by F iff it is obtained from members of F and projections by composition:

$$g(x, y, z, t) = f_1(x, f_2(y, x), f_3(f_2(t, z), y))$$

Example

On $\{0,1\}$, the clone of monotonic functions $Pol(\leq)$ is generated by $\{\vee, \wedge, 0, 1\}$: any non-constant monotonic function is of the form

$$f(\mathbf{x}_1,\ldots,\mathbf{x}_n)=(\mathbf{x}_{i_1}\vee\mathbf{x}_{i_2}\cdots\vee\mathbf{x}_{i_s})\wedge(\cdots)\wedge\cdots$$

... and Relational Clones

A constructive view of relational clones:

 ρ is in the relational clone generated by Γ iff it is (primitive positive) PP-definable from relations in Γ:

$$\rho = \{(\mathbf{x}, \mathbf{y}, \mathbf{z}) : \exists \mathbf{u} \,\exists \mathbf{v} \,\Phi(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{u}, \mathbf{v})\}$$

 Φ is a conjunct of atomic formulas from relations in Γ ,

$$\Phi(x,y,z,u,v) \equiv (x,u) \in \gamma_1 \land (y,v,z,z) \in \gamma_2.$$

... and Relational Clones

A constructive view of relational clones:

• ρ is in the relational clone generated by Γ iff it is (primitive positive) PP-definable from relations in Γ :

$$\rho = \{(x, y, z) : \exists u \,\exists v \,\Phi(x, y, z, u, v)\}$$

 Φ is a conjunct of atomic formulas from relations in Γ ,

$$\Phi(x,y,z,u,v) \equiv (x,u) \in \gamma_1 \land (y,v,z,z) \in \gamma_2.$$

Example

On $\{0,1\}$, the relational clone generated by < consists of all relations of the form

$$\theta = \{(x_1, \ldots, x_k) : x_{i_1} \leq x_{i_1}, \ldots, x_{i_s} \leq x_{i_s}\}.$$

The Definition of the Algebra $\mathbb{A}(\mathbf{B})$

Relational structure **B**set of relations

set of operations

algebra A(**B**)



definition of

Algebras

Let A be a non-void set.

 A (non-indexed) algebra is a pair A = ⟨A; F⟩ where F is a set of operations on A, the basic or fundamental operations of A.

Algebras

Let A be a non-void set.

- A (non-indexed) algebra is a pair A = ⟨A; F⟩ where F is a set of operations on A, the basic or fundamental operations of A.
- The members of the clone generated by F are called the term operations of A.
- If we also allow the use of constant operations, we obtain the polynomial operations of A.
- Algebras on the same universe with the same term (polynomial) operations are term (polynomially) equivalent.



Term equivalent Algebras

Example

Let \mathcal{O} denote the set of all operations on $\{0,1\}$.

 $\mathbb{A} = \langle \{0,1\}; \wedge, \vee, \neg \rangle$ and $\mathbb{B} = \langle \{0,1\}; \mathcal{O} \rangle$ are term equivalent.

Term equivalent Algebras

Example

Let \mathcal{O} denote the set of all operations on $\{0,1\}$.

 $\mathbb{A} = \langle \{0,1\}; \wedge, \vee, \neg \rangle$ and $\mathbb{B} = \langle \{0,1\}; \mathcal{O} \rangle$ are term equivalent.

Example

- Let $m(x, y, z) = (x \land y) \lor (x \land z) \lor (y \land z)$, the *majority* operation on $\{0, 1\}$.
- $\mathbb{A} = \langle \{0,1\}; \wedge, \vee \rangle$ and $\mathbb{B} = \langle \{0,1\}; m \rangle$ are *not* term equivalent, but they are polynomially equivalent.

The Algebra A(**B**)

Let $\mathbf{B} = \langle A; \Gamma \rangle$ be a relational structure.

The algebra associated to B is

$$\mathbb{A}(\mathbf{B}) = \langle A; Pol(\Gamma) \rangle.$$

The Algebra $\mathbb{A}(\mathbf{B})$, cont'd

Example

- Let $\mathbf{B} = \langle \{0, 1\}; \leq, \{0\}, \{1\} \rangle$.
- $\mathbb{A}(\mathbf{B}) = \langle \{0,1\}; Pol(\leq,\{0\},\{1\}) \rangle.$
- The term (basic) operations of $\mathbb{A}(\mathbf{B})$ are all monotonic Boolean operations f such that f(0, ..., 0) = 0 and f(1, ..., 1) = 1.

Idempotent Algebras

 It is convenient to consider idempotent algebras, i.e. algebras whose basic operations satisfy

$$f(x,\ldots,x)=x$$
 for all x ;

- f is idempotent iff it preserves every one-element unary relation {a};
- The full idempotent reduct of the algebra
 A(B) = ⟨A; Pol(Γ)⟩ is the algebra
 ⟨A; Pol(Γ ∪ {{a} : a ∈ A})⟩;
- The term operations of the full idempotent reduct are precisely the *idempotent* term operations of A(B).



Part 2: The Equational Properties of $\mathbb{A}(\mathbf{B})$

Relational structure **B**↓

set of relations

↓

set of operations

↓

algebra A(**B**)

Part 2: The Equational Properties of $\mathbb{A}(\mathbf{B})$

Relational structure \mathbf{B} \downarrow set of relations \downarrow set of operations \downarrow algebra $\mathbb{A}(\mathbf{B})$ \downarrow variety $\mathcal{V}(\mathbb{A}(\mathbf{B}))$

Similar Algebras; Identities

- Let I be a set of operation symbols, each with a given arity;
- $\mathbb{A} = \langle A; q^{\mathbb{A}}(q \in I) \rangle$ is an indexed algebra;
- $q^{\mathbb{A}}$ is the *interpretation* of q in \mathbb{A} , and arities match.
- An algebra $\mathbb{C} = \langle C; q^{\mathbb{C}}(q \in I) \rangle$ is *similar* to \mathbb{A} .

Similar Algebras; Identities, cont'd

An identity is an expression of the form

$$s(x_1,\ldots,x_n)\approx t(x_1,\ldots,x_n)$$

where s, t are terms, e.g.

$$F(x, G(y, z), t) \approx F_1(x, F_2(y, x), F_3(F_2(t, z), y))$$

where F, G, F₁, F₂, F₃ are operation symbols.

 Identities interpret in A: if the resulting term operations are equal, the identity holds in A, or A models the identity.

Equational classes

A class of similar algebras is equational if it consists of all algebras that model some set of identities.

Equational classes

A class of similar algebras is equational if it consists of all algebras that model some set of identities.

Example

The class of all algebras $\mathbb{S} = \langle S; \wedge^{\mathbb{S}} \rangle$ satisfying the identities

$$x \wedge (y \wedge z) \approx (x \wedge y) \wedge z,$$

 $x \wedge y \approx y \wedge x,$
 $x \wedge x \approx x.$

is the (equational) class of semilattices.

Varieties

Theorem (G. Birkhoff)

A class of similar algebras is an equational class iff it is a variety, i.e. if it is closed under the formation of products, subalgebras and homomorphic images.

H, S, and P

• (P) $\mathbb{A} \times \mathbb{C} = \langle A \times C; q^{\mathbb{A} \times \mathbb{C}} (q \in I) \rangle$ where $q^{\mathbb{A} \times \mathbb{C}}$ acts coordinatewise as $q^{\mathbb{A}}$ and $q^{\mathbb{C}}$.

H, S, and P

- (P) $\mathbb{A} \times \mathbb{C} = \langle A \times C; q^{\mathbb{A} \times \mathbb{C}} (q \in I) \rangle$ where $q^{\mathbb{A} \times \mathbb{C}}$ acts coordinatewise as $q^{\mathbb{A}}$ and $q^{\mathbb{C}}$.
- (S) Ø ≠ C ⊆ A is a subuniverse if it invariant under the basic operations of A:
 C = ⟨C; q^C (q ∈ I)⟩ where q^C is the restriction of q^A to C;

H, S, and P

- (P) $\mathbb{A} \times \mathbb{C} = \langle A \times C; q^{\mathbb{A} \times \mathbb{C}} (q \in I) \rangle$ where $q^{\mathbb{A} \times \mathbb{C}}$ acts coordinatewise as $q^{\mathbb{A}}$ and $q^{\mathbb{C}}$.
- (S) $\emptyset \neq C \subseteq A$ is a *subuniverse* if it invariant under the basic operations of A:
 - $\mathbb{C}=\langle \textit{\textbf{C}};\textit{\textbf{q}}^{\mathbb{C}}\,(\textit{\textbf{q}}\in\textit{\textbf{I}})
 angle$ where $\textit{\textbf{q}}^{\mathbb{C}}$ is the restriction of $\textit{\textbf{q}}^{\mathbb{A}}$ to $\textit{\textbf{C}};$
- (H) if α is a congruence of A, i.e. a partition of A invariant under the operations of A:
 - $\mathbb{A}/\alpha = \langle A/\alpha \, ; \, q^{\mathbb{A}/\alpha} \, (q \in I) \rangle$ where $q^{\mathbb{A}/\alpha}$ is the action of $q^{\mathbb{A}}$ on the α -blocks.
 - (Every image of the algebra $\mathbb A$ under a homomorphism is of this form: α is the *kernel* of the homomorphism.)

HSP

Theorem (Tarski)

Let V(A) denote the variety generated by the class of algebras A. Then V(A) = HSP(A).

HSP

Theorem (Tarski)

Let V(A) denote the variety generated by the class of algebras A. Then V(A) = HSP(A).

Example

Let $\mathbb{S} = \langle \{0,1\}; \wedge \rangle$ denote the 2-element (meet) semilattice. $HSP(\mathbb{S})$ is the variety of semilattices, i.e. every semilattice is a homomorphic image of a subalgebra of a power of \mathbb{S} .

Core relational structure \mathbf{B} \downarrow algebra $\mathbb{A}(\mathbf{B})$ \downarrow full idempotent reduct \mathbb{A} of $\mathbb{A}(\mathbf{B})$ \downarrow variety $\mathcal{V}(\mathbb{A})$

Core relational structure \mathbf{B} $\downarrow \\ \text{algebra } \mathbb{A}(\mathbf{B}) \\ \downarrow \\ \text{full idempotent reduct } \mathbb{A} \text{ of } \mathbb{A}(\mathbf{B}) \\ \downarrow \\ \text{variety } \mathcal{V}(\mathbb{A}) \\ \bullet \text{ Let } \mathbb{C} = \langle \textit{\textbf{C}}; \textit{\textbf{G}} \rangle \in \mathcal{V}(\mathbb{A}) \text{ be finite.}$

Core relational structure \mathbf{B} \downarrow algebra $\mathbb{A}(\mathbf{B})$ \downarrow full idempotent reduct \mathbb{A} of $\mathbb{A}(\mathbf{B})$ \downarrow variety $\mathcal{V}(\mathbb{A})$ • Let $\mathbb{C} = \langle C; G \rangle \in \mathcal{V}(\mathbb{A})$ be finite.

• Let $\mathbf{B}_0 = \langle C; \Gamma_0 \rangle$ such that $\Gamma_0 \subseteq Inv(G)$.

Core relational structure \mathbf{B} \downarrow algebra $\mathbb{A}(\mathbf{B})$ \downarrow full idempotent reduct \mathbb{A} of $\mathbb{A}(\mathbf{B})$ \downarrow variety $\mathcal{V}(\mathbb{A})$

- Let $\mathbb{C} = \langle C; G \rangle \in \mathcal{V}(\mathbb{A})$ be finite.
- Let $\mathbf{B}_0 = \langle C; \Gamma_0 \rangle$ such that $\Gamma_0 \subseteq Inv(G)$.
- How are CSP(B₀) and CSP(B) related ?



Algebraic Reductions: Algorithmic Complexity

Theorem (Jea + Bul-Jea-Kro + Ats-Bul-Daw + Lar-Tes)

Let **B** be a core relational structure. Let \mathbb{A} denote the full idempotent reduct of $\mathbb{A}(\mathbf{B})$.

- Let \mathbb{C} be a finite algebra in $\mathcal{V}(\mathbb{A})$, and let \mathbf{B}_0 be a relational structure whose relations are invariant under the basic operations of \mathbb{C} . Then there exists a logspace many-one reduction of $CSP(\mathbf{B}_0)$ to $CSP(\mathbf{B})$.
- If furthermore $\mathbb{C} \in HS(\mathbb{A})$ and the relations of \mathbf{B}_0 are irredundant, then the above reduction is first-order and without ordering.

Algebraic Reductions: Descriptive Complexity

Theorem (Ats-Bul-Daw + Lar-Zád + Lar-Tes)

Let **B** be a core relational structure. Let \mathbb{A} denote the full idempotent reduct of $\mathbb{A}(\mathbf{B})$.

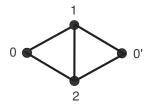
• Let \mathbb{C} be a finite algebra in $\mathcal{V}(\mathbb{A})$, and let \mathbf{B}_0 be a relational structure whose relations are invariant under the basic operations of \mathbb{C} .

If $\neg CSP(\mathbf{B})$ is expressible in (linear, symmetric) Datalog, then so is $\neg CSP(\mathbf{B}_0)$.

(Datalog: see Phokion Kolaitis' talk)

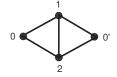
Algebraic Reductions: an Illustration

A graph on $A = \{0, 0', 1, 2\}$ with (irreflexive, symmetric) edge relation θ :



Let **B** =
$$\langle A; \theta, \{0\}, \{0'\}, \{1\}, \{2\} \rangle$$
.

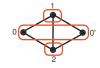




- $\mathbb{A} = \mathbb{A}(\mathbf{B})$ is an idempotent algebra.
- It has the following proper subuniverses:

$$\{0,0'\} = \{x : (x,1) \in \theta \land (x,2) \in \theta\},\$$
$$\{1,2\} = \{x : (x,0) \in \theta \land (x,0') \in \theta\}.$$





The following is a congruence of A:

$$\alpha = \{(\mathbf{x}, \mathbf{y}) : \exists \mathbf{u}, \, \mathbf{v}, \, \Phi(\mathbf{x}, \mathbf{y}, \mathbf{u}, \mathbf{v})\},\$$

where Φ is given by:





The operations of \mathbb{A}/α preserve $\overline{\theta}$ induced by θ :



If $\mathbf{B}_0 = \langle \{\overline{0}, \overline{1}, \overline{2}\}; \overline{\theta} \rangle$, then $CSP(\mathbf{B}_0)$ reduces to $CSP(\mathbf{B})$.

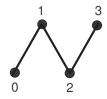




Since $CSP(\mathbf{B}_0)$ is 3-colouring, we conclude that $CSP(\mathbf{B})$ is NP-complete.

Algebraic Reductions: another Illustration

A *reflexive* graph on $A = \{0, 1, 2, 3\}$ with symmetric edge relation θ :



Let **B** = $\langle A; \theta, \text{ all subsets of } A \rangle$. (A *list-homomorphism problem*.)





- $\mathbb{A} = \mathbb{A}(\mathbf{B})$ is a conservative algebra, i.e. every subset is a subuniverse.
- The algebra A has a majority term (Feder, Hell, Huang) and hence CSP(B) is in NL (Dalmau, Krokhin).
- Can we do better?





The operations of the subalgebra $\mathbb C$ with universe $\{1,3\}$ preserve

$$\rho = \{(\mathbf{x}, \mathbf{y}) : \exists \mathbf{u}, \ \mathbf{v}, \ \Phi(\mathbf{x}, \mathbf{y}, \mathbf{u}, \mathbf{v})\},\$$

where Φ is given by:





- We have $\rho = \{(1,1), (1,3), (3,3)\}$, i.e. the natural order on $\{1,3\}$;
- if $\mathbf{B}_0 = \langle \{1,3\}; \rho, \{1\}, \{3\} \rangle$ then $CSP(\mathbf{B}_0)$ reduces to $CSP(\mathbf{B});$
- Since CSP(B₀) is (essentially) directed unreachability, we conclude that CSP(B) is NL-complete.



The Dichotomy Conjecture(s)

Core relational structure \mathbf{B} \downarrow full idempotent reduct \mathbb{A} of $\mathbb{A}(\mathbf{B})$ \downarrow variety $\mathcal{V}(\mathbb{A})$

The Dichotomy Conjecture(s)

Core relational structure ${\bf B}$ \downarrow full idempotent reduct ${\mathbb A}$ of ${\mathbb A}({\bf B})$ \downarrow variety ${\mathcal V}({\mathbb A})$

- If $\mathbb{C} \in \mathcal{V}(\mathbb{A})$ is "NP-hard", then $CSP(\mathbf{B})$ is NP-hard.
- All known hardness results for CSP's are of this form ...
- ... so what happens if $\mathcal{V}(\mathbb{A})$ contains *no* "bad algebra"?



The Dichotomy Conjecture(s), cont'd

Dichotomy Conjecture (Feder-Vardi, 1993)

Every $CSP(\mathbf{B})$ is either in P or NP-complete.

The Dichotomy Conjecture(s), cont'd

Dichotomy Conjecture (Feder-Vardi, 1993)

Every $CSP(\mathbf{B})$ is either in P or NP-complete.

An algebra \mathbb{C} is a *set* if its basic operations are projections.

Tractability Conjecture (Bulatov-Jeavons-Krokhin, 2000)

Let **B** be a core structure and let \mathbb{A} be the full idempotent reduct of $\mathbb{A}(\mathbf{B})$. If $\mathcal{V}(\mathbb{A})$ contains no set, then $CSP(\mathbf{B})$ is in P, otherwise it is NP-complete.

Miscellaneous Remarks

- In the examples: "bad algebra" in $\mathcal{V}(\mathbb{A})$ actually in $HS(\mathbb{A})$: true in general (Bul-Jea for sets, Valeriote for general case)
- NP-hardness, NL-hardness and P-hardness are detected by certain 2-element algebras in HS(A);
- preventing "bad algebras" in the variety means "nice equations" ...
- hence: do "nice equations" imply tractability (etc.) ?
- Some evidence: nuf, CD(4), 2-semilattices, TSI, few subpowers, etc.
- See Matt Valeriote's talk.

