Universal algebra for CSP
Lecture 2

Ross Willard

University of Waterloo

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

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 $f(x,y,y) \approx x$.

In case (1), the proof found such $\mathbb{G}$ compatible with $\mathbf{F} \leq \mathbf{A}^{|A|^2}$.

Question raised: do we really need to look that 'deeply" into $\mathrm{HSP}(\mathbf{A})$?

Example. For any finite set A, the *Słupecki clone* $\mathcal{S}_A$ on A is the union of:

- $\{$all operations that depend on at most one variable$\}$,
- $\{$all operations that are not surjective$\}$.

Let $\mathbf{A} = (A; \mathcal{S}_A)$. Clearly $\mathbf{A}$ is not in case (2).

Exercise: if $|A| > 2n$, show that no member of $\mathrm{HS}(\mathbf{A}^n)$ has a reflexive not-symmetric compatible digraph.

Fixed-Template Constraint Satisfaction Problems

Fix a relational structure $\mathbb{G} = (A; \mathcal{R})$ with A and $\mathcal{R}$ finite.

Definition

$\mathrm{CSP}(\mathbb{G})$ is either of the following equivalent decision problems:

Constraints version

Input: Set V of variables, "constraints" on tuples of variables (requiring them to belong to prescribed relations in $\mathcal{R}$).

Query: Is there an assignment $V \to A$ which satisfies all the constraints?

Homomorphism version

Input: a finite relational structure $\mathbb{H} = (B, \mathcal{S})$ of the same "signature" as $\mathbb{G}$.

Query: Does there exist a homomorphism $\mathbb{H} \to \mathbb{G}$?

Archetypal examples

$\mathbb{G}_1 = (\{0,1\}; \{R_{abc} : a,b,c \in \{0,1\}\})$ where

$$R_{abc} = \{0,1\}^3 \setminus \{(a,b,c)\}.$$

E.g., the constraint "$(x,y,z) \in R_{101}$" says "$\neg x$ or y or $\neg z$."

$\mathrm{CSP}(\mathbb{G}_1)$ is equivalent to 3-SAT, which is *NP*-complete.

$\mathbb{G}_2 = (\{0,1\}; \{S_0, S_1\})$ where

$$S_0 = \{(x,y,z) : x \oplus y \oplus z = 0\}$$
$$S_1 = \{(x,y,z) : x \oplus y \oplus z = 1\}.$$

Instances of $\mathrm{CSP}(\mathbb{G}_2)$ are systems of linear equations (each in 3 variables) over $\mathbb{Z}_2$.

Such systems can be checked for consistency by Gaussian elimination; thus $\mathrm{CSP}(\mathbb{G}_2)$ is in P.

$\mathbb{G}_4 = (\{0,1\}; \{LE, C_0, C_1\})$ where

$$\begin{aligned} LE &= \{(0,0),(0,1),(1,1)\} \\ C_0 &= \{0\} \\ C_1 &= \{1\}. \end{aligned}$$

Instances of $\mathrm{CSP}(\mathbb{G}_4)$ can only "say" $x \le y$, $x = 0$, or $x = 1$.

There is only one way to get a contradiction: by saying

$$x_1 = 1 \text{ and } x_n = 0 \text{ and } x_1 \le x_2 \text{ and } x_2 \le x_3 \text{ and } \ldots \text{and } x_{n-1} \le x_n.$$

$CSP(\mathbb{G}_4)$ is equivalent to REACHABILITY, which is in P (in fact, in NL).

$\mathbb{G}_3 = (\{0,1\}; \{=, C_0, C_1\})$.

Similar to $\mathbb{G}_4$, but "undirected."

$\mathrm{CSP}(\mathbb{G}_3)$ encodes Undirected REACHABILITY, which is in L (Reingold, 2005).

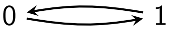
$\mathbb{G}_5 = (\{0,1\}; \{R_{110}, C_0, C_1\})$.

"$(x,y,z) \in R_{110}$" is equivalent to "(x and y) implies z."

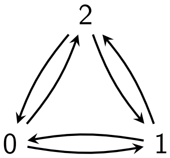
Similar to $\mathbb{G}_4$, but with directed paths replaced by directed binary trees.

$\mathrm{CSP}(\mathbb{G}_5)$ is equivalent to Horn 3-SAT, which is P-complete.

$\mathbb{K}_n = (A; \{\neq_A\})$ where $A = \{0,1,\ldots,n-1\}$.



$\mathbb{K}_2$

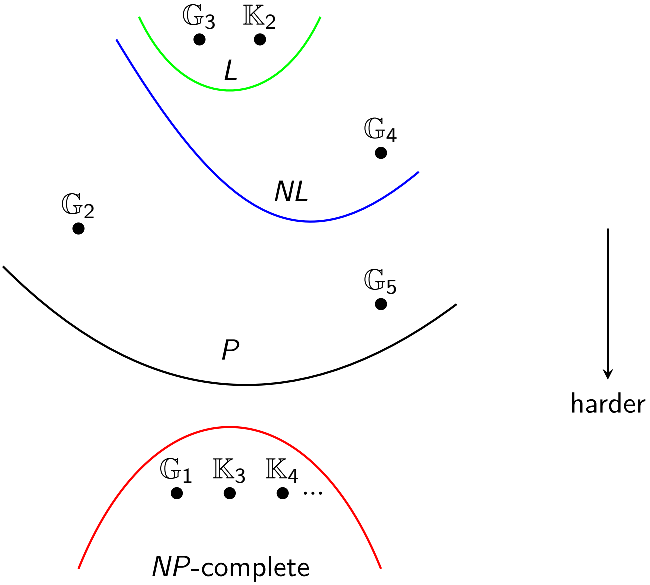


$\mathbb{K}_3$

$\mathrm{CSP}(\mathbb{K}_n)$ is equivalent to n-COLOURABILITY, which is

- NP-complete for $n \geq 3$, and
- In P (in fact, in L) if $n = 2$.

Summary:


$\mathbb{G}_3$ $\mathbb{K}_2$
L
$\mathbb{G}_4$
NL
$\mathbb{G}_2$
$\mathbb{G}_5$
P
harder
$\mathbb{G}_1$ $\mathbb{K}_3$ $\mathbb{K}_4$ ...
NP-complete

Comparing CSPs

We will use the following tools:

1. Simulations, pp-definitions
2. Polymorphisms
3. Reduction to the "idempotent case"
4. Algebraic substructures, Pp-constructions

Simulation

Consider again $\mathbb{G}_5 = (\{0,1\}; R_{110}, C_0, C_1)$.

Suppose we modify $\mathbb{G}_5$ by adding $R_{1110} = \{0,1\}^4 \setminus \{(1,1,1,0)\}$:

$$\mathbb{G}_5' \;=\; (\{0,1\}; R_{110}, C_0, C_1, R_{1110}).$$

Is $\mathrm{CSP}(\mathbb{G}_5')$ harder than $\mathrm{CSP}(\mathbb{G}_5)$?

NO! R_{110} can simulate R_{1110} as follows:

- "$(x,y,z,w) \in R_{1110}$" means "$(x \;\&\; y \;\&\; z) \Rightarrow w$."
- Given any constraint $(x \;\&\; y \;\&\; z) \Rightarrow w$, introduce a new variable t and replace the constraint with two new constraints

$$(x \;\&\; y) \Rightarrow t \quad \text{and} \quad (t \;\&\; z) \Rightarrow w.$$

Key: $R_{1110}(x,y,z,w)$ is <u>defined in $\mathbb{G}_5$</u> by $\exists t[R_{110}(x,y,t) \;\&\; R_{110}(t,z,w)]$.

Pp-definability

In general:

Definition

1. A *primitive positive* (*pp*) formula is any first-order formula of the form

$$\exists \cdots [\bigwedge_i atomic_i]$$

   where each $atomic_i$ is a basic relation or equality ($x = y$).
2. Given a relational structure $\mathbb{G} = (A; \mathcal{R})$ and a relation S on A, we say that S is *pp-definable in* $\mathbb{G}$ if there exist a pp-formula using relations from $\mathcal{R}$ whose set of solutions in $\mathbb{G}$ is S.

Theorem (Folklore; Larose & Tesson 2007)

Suppose $\mathbb{G}, \mathbb{H}$ *are finite relational structures with the same domain. If every relation of* $\mathbb{H}$ *is pp-definable in* $\mathbb{G}$*, then* $\mathrm{CSP}(\mathbb{H}) \leq_L \mathrm{CSP}(\mathbb{G})$.

Testing pp-definability

How can we test whether a relation is pp-definable in a structure?

Theorem (Bodnarčuk et al; Geiger 1968)

Let $\mathbb{G} = (A; \mathcal{R})$ with A finite, and let E be an n-ary relation on A. TFAE:

1. *E is pp-definable in $\mathbb{G}$.*
2. *E is compatible with every polymorphism of $\mathbb{G}$.*

Proof sketch (2) $\Rightarrow$ (1) . . .

Corollary

If $\mathbb{G}, \mathbb{H}$ are finite relational structures with the same domain and the same polymorphisms, then $\mathrm{CSP}(\mathbb{G})$ and $\mathrm{CSP}(\mathbb{H})$ have the same complexity.

Proof . . .

Polymorphism algebra of a structure

Definition

Given a finite relational structure $\mathbb{G} = (A; \mathcal{R})$, the *polymorphism algebra* of $\mathbb{G}$ is the algebra

$$\mathrm{PolAlg}(\mathbb{G}) \quad = \quad (A; \mathrm{Pol}(\mathbb{G}))$$

where $\mathrm{Pol}(\mathbb{G}) = \{$all polymorphisms of $\mathbb{G}\}$.

By previous slide, $\mathrm{PolAlg}(\mathbb{G})$ determines the complexity of $\mathrm{CSP}(\mathbb{G})$.

This is the first insight of the "Algebraic approach" to CSP.

Examples revisited

$\mathbb{G}_1 = (\{0,1\}; \{R_{abc} \ : \ a,b,c \in \{0,1\}\})$ where

$$R_{abc} \quad = \quad \{0,1\}^3 \setminus \{(a,b,c)\}.$$

$\mathrm{Pol}(\mathbb{G}_1) = \{\text{projections}\}$. (Exercise: prove it!)

$\mathrm{PolAlg}(\mathbb{G}_1) = (\{0,1\}; \{\text{proj's}\})$ "=" $(\{0,1\}; \varnothing)$ = the 2-element set!

$\mathbb{G}_2 = (\{0,1\}; \{\text{"}x \oplus y \oplus z = 0,\text{" "}x \oplus y \oplus z = 1\text{"}\})$.

$\mathrm{Pol}(\mathbb{G}_2) = \{\text{all boolean sums of an odd number of variables}\} =: \mathcal{C}_2$.

$\mathrm{PolAlg}(\mathbb{G}_2) = (\{0,1\}; \mathcal{C}_2)$ "=" $(\{0,1\}; x \oplus y \oplus z)$ = like a vector space!

$\mathbb{G}_4 = (\{0,1\}; \{LE, C_0, C_1\})$ where $LE = \{(0,0),(0,1),(1,1)\}$.

$\mathrm{Pol}(\mathbb{G}_4) = \{f : f \text{ is monotone and "idempotent"}\} =: \mathcal{C}_4$.

("Idempotent" means $f(0,0,\ldots,0) = 0$ and $f(1,1,\ldots,1) = 1$.)

$\mathrm{PolAlg}(\mathbb{G}_4) = (\{0,1\}; \mathcal{C}_4)$ "=" $(\{0,1\}; \max, \min)$ = the 2-element lattice!

$\mathbb{G}_3 = (\{0,1\}; \{=, C_0, C_1\})$.

$\mathrm{Pol}(\mathbb{G}_3) = \{\text{all idempotent boolean functions}\} =: \mathcal{C}_3$.

$\mathrm{PolAlg}(\mathbb{G}_3) = (\{0,1\}; \mathcal{C}_3)$ = almost a boolean algebra!

$\mathbb{G}_5 = (\{0,1\}; \{R_{110}, C_0, C_1\})$.

(Recall that $\mathrm{CSP}(\mathbb{G}_5)$ encodes Horn 3-SAT, which is in P.)

Exercise:

1. Every $f \in \mathrm{Pol}(\mathbb{G}_5)$ is monotone and idempotent.
2. $\min \in \mathrm{Pol}(\mathbb{G}_5)$ but $\max \notin \mathrm{Pol}(\mathbb{G}_5)$. (Exercise: prove it.)

$\mathrm{PolAlg}(\mathbb{G}_5)$ "$=$" $(\{0,1\}; \min) =$ the 2-element semi-lattice!

$\mathbb{K}_n$. For $n \geq 3$,

- $\mathrm{Pol}(\mathbb{K}_n) = \{$permutations (in a single variable)$\}$.
- I.e., $\mathrm{PolAlg}(\mathbb{K}_n)$ is a set with permutations.

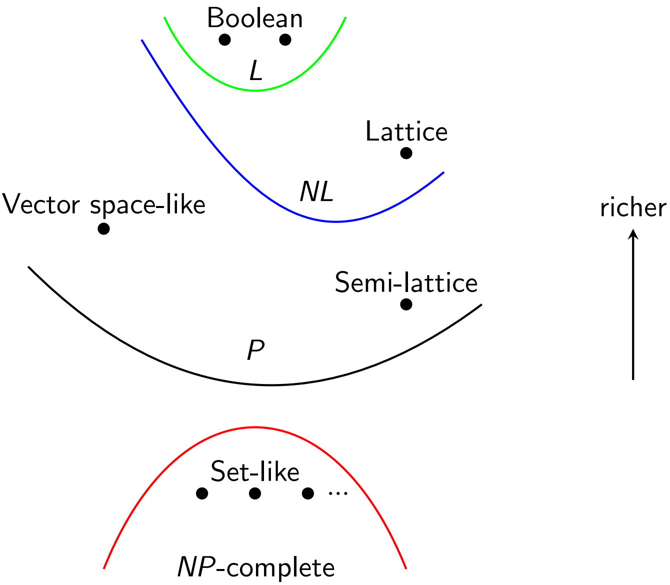
$\mathrm{Pol}(\mathbb{K}_2)$ is much richer:

1. Consists of all "self-dual" functions, i.e., functions f which satisfy

$$f(\neg x_1, \neg x_2, \ldots, \neg x_n) \approx \neg f(x_1, \ldots, x_n).$$

2. Includes $x \oplus y \oplus z$ (which is a "Maltsev" operation), $\mathrm{maj}(x,y,z)$, etc. Almost a boolean algebra!

Polymorphism algebras as measure of CSP:



Core and idempotent structures

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

Definition

1. $\mathbb{G}$ is *core* if every endomorphism $f : \mathbb{G} \to \mathbb{G}$ is a bijection.
2. $\mathbb{G}$ is *idempotent* if $\mathcal{R}$ contains the relation $C_a = \{a\}$ for every $a \in A$.

Remarks:

1. $\mathbb{G}$ is core iff all its 1-ary polymorphisms are permutations.
2. $\mathbb{G}$ is idempotent $\Rightarrow \mathrm{PolAlg}(\mathbb{G})$ is an idempotent algebra $\Leftrightarrow$ every C_a is pp-definable in $\mathbb{G} \Leftrightarrow$ the identity map is the only 1-ary polymorphism of $\mathbb{G}$.
3. For every finite $\mathbb{G}$ there exists an induced substructure $\mathbb{G}'$ which is core and for which there exists a *retract* mapping $\mathbb{G}$ onto $\mathbb{G}'$.
   - This $\mathbb{G}'$ is unique up to isomorphism, and is called *the core of* $\mathbb{G}$.
4. $\mathbb{G}^c := (A; \mathcal{R} \cup \{C_a \,:\, a \in A\})$; it is idempotent.

Lemma

If $\mathbb{G}$ is finite and $\mathrm{core}(\mathbb{G})$ is its core, then $\mathrm{CSP}(\mathbb{G}) \equiv \mathrm{CSP}(\mathrm{core}(\mathbb{G}))$.

Proof: An input maps homomorphically to $\mathbb{G}$ iff it maps homomorphically to $\mathrm{core}(\mathbb{G})$.

Lemma (???, Larose & Tesson 2007)

Suppose $\mathbb{G}$ is core. Then $\mathrm{CSP}(\mathbb{G}) \equiv_L \mathrm{CSP}(\mathbb{G}^c)$.

Proof: it suffices to reduce $\mathrm{CSP}(\mathbb{G}^c)$ to $\mathrm{CSP}(\mathbb{G})$. There is a trick to do this.

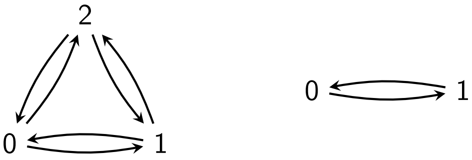
Conclusion: For CSP, we always assume the template $\mathbb{G}$ is idempotent.

Algebraic substructures

Definition

Let $\mathbb{G} = (A; \mathcal{R})$ be a finite structure and $\mathbb{H} = (B; \mathcal{R}\restriction_B)$ an induced substructure. We say that $\mathbb{H}$ is an *algebraic substructure* of $\mathbb{G}$ if B is (the domain of) a subalgebra of $\mathrm{PolAlg}(\mathbb{G})$.

Example:



$\mathbb{K}_3$ $\qquad$ $\mathbb{H} = \mathbb{K}_2$

$\mathbb{H}$ is **not** an algebraic substructure of $\mathbb{K}_3$.

Observe: if $\mathbb{H} = (B; \ldots)$ is an algebraic substructure of $\mathbb{G}$, then

- B is preserved by all polymorphisms of $\mathbb{G}$ …
- …so B is pp-definable in $\mathbb{G}$.

More generally, given $\mathbb{G}$ we will permit "substructures" whose:

- Domains are pp-definable subsets of G^2 (or G^3, etc.) …
- …modulo pp-definable equivalence relations …
- …and whose relations need not be induced, merely pp-definable.

Pp-constructible structures

Example: $\mathbb{K}_3$.

Let Δ be the 3-ary relation defined by the formula

$$\delta(x,y,z) \quad : \quad (x \to y) \ \& \ (y \to z) \ \& \ (z \to x).$$

So

$$\Delta = \{(0,1,2),(1,2,0),(2,0,1),(2,1,0),(0,2,1),(1,0,2)\}.$$

Let E be the 6-ary relation defined by the formula $\varepsilon(x,y,z,x',y',z')$:

$$\begin{aligned}\exists x'',y'',z'' \quad [\quad & \delta(x,y,z) \ \& \ \delta(x',y',z') \ \& \ \delta(x'',y'',z'') \ \& \\ & (x \to x'') \ \& \ (x'' \to x') \ \& \ (y \to y'') \ \& \ (y'' \to y') \\ & \& \ (z \to z'') \ \& \ (z'' \to z') \quad]\end{aligned}$$

$E = \{(0,1,2),(1,2,0),(2,0,1)\}^2 \cup \{(2,1,0),(0,2,1),(1,0,2)\}^2$, which is an equivalence relation on Δ (with two blocks).

Let R be the 6-ary relation defined by the formula

$$\begin{aligned}\exists x'', y'', z'' \quad [\quad & \delta(x,y,z) \;\&\; \delta(x',y',z') \;\&\; \delta(x'',y'',z'') \;\&\\ & \varepsilon(x,y,z,x'',y'',z'') \;\&\\ & (x' = x'') \;\&\; (y' = z'') \;\&\; (z' = y'') \quad].\end{aligned}$$

$$\begin{aligned} R \;=\; & \{(0,1,2),(1,2,0),(2,0,1)\} \times \{(2,1,0),(0,2,1),(1,0,2)\} \;\cup \\ & \{(2,1,0),(0,2,1),(1,0,2)\} \times \{(0,1,2),(1,2,0),(2,0,1)\}.\end{aligned}$$

So $(\Delta/E; R/E) \;\cong\; \mathbb{K}_2$.

We say that $\mathbb{K}_2$ is *pp-constructible* from $\mathbb{K}_3$ via the above pp-formulas.

(Note from the audience: a simpler formula can define R.)

Let $\mathbb{G}, \mathbb{H}$ be finite relational structures.

Write $\mathbb{G} = (A; \{\ldots\})$ and $\mathbb{H} = (B; \{R_1, R_2, \ldots\})$ with $\text{arity}(R_i) = n_i$.

General Definition

$\mathbb{H}$ is **pp-constructible from** $\mathbb{G}$ iff there exist:

- $k \geq 1$
- Pp-definable relations of $\mathbb{G}$:
  - $U \subseteq A^k$
  - $\Theta \subseteq U^2 \quad (\subseteq (A^k)^2 = A^{2k})$
  - $S_i \subseteq U^{n_i} \quad (\subseteq (A^k)^{n_i} = A^{n_i k})$ for $i = 1, 2, \ldots$

such that

- Θ is an equivalence relation on U.
- $\mathbb{H} \cong (U; S_1, S_2, \ldots)/\Theta$.

Notation: $\mathbb{H} \leq_{ppc} \mathbb{G}$.

Theorem (Bulatov, Jeavons, Krokhin 2005; Larose, Tesson (2007))

Suppose $\mathbb{G}, \mathbb{H}$ *are finite structures. If* $\mathbb{H}$ *is pp-constructible from* $\mathbb{G}$*, then* $\mathrm{CSP}(\mathbb{H}) \leq_L \mathrm{CSP}(\mathbb{G})$.

Proof: similar to the proof that pp-definable relations can be simulated.

Corollary

If $\mathbb{K}_3$ *(or* $\mathbb{G}_1 = (\{0,1\}; \{R_{abc} : abc \in \{0,1\}^3\})$*) is pp-constructible from* $\mathbb{G}$*, then* $\mathrm{CSP}(\mathbb{G})$ *is NP-complete.*

Theorem

Let $\mathbb{G}, \mathbb{H}$ be finite relational structures. TFAE:

1. *$\mathbb{H}$ is pp-constructible from $\mathbb{G}$.*
2. *$\mathbb{H}$ is compatible with some member of $\mathrm{HSP}(\mathrm{PolAlg}(\mathbb{G}))$.*

Proof sketch (2) $\Rightarrow$ (1). Write $\mathbb{G} = (A; \ldots)$, $\mathbb{H} = (B; \{R_1, R_2, \ldots,\})$.

Let $\mathbf{A} = \mathrm{PolAlg}(\mathbb{G})$. Assume $\mathbb{H}$ is compatible with $\mathbf{B} \in \mathrm{HSP}(\mathbf{A})$.

WLOG, $\mathbf{B} = \mathbf{U}/E$ for some $\mathbf{U} \in \mathrm{SP}(\mathbf{A})$ and some congruence E of $\mathbf{U}$.

Say $\mathbf{U} \leq \mathbf{A}^k$. We can view $E \subseteq A^{2k}$.

Similarly, we can "pull back" each n-ary relation R_i to a kn-ary relation R_i^* on A.

All of $U, E, R_1^*, R_2^*, \ldots$ are compatible with $\mathbf{A}$.

Hence they are all pp-definable in $\mathbb{G}$...

...and give a pp-construction of $\mathbb{H}$ from $\mathbb{G}$. □

Corollary

For a finite relational structure $\mathbb{G}$*, TFAE:*

1. $\mathbb{G}_1 = (\{0,1\}; \{R_{abc} : abc \in \{0,1\}^3\})$ *is pp-constructible from* $\mathbb{G}$.
2. $\mathrm{HSP}(\mathrm{PolAlg}(\mathbb{G}))$ *contains the 2-element set* $(\{0,1\}; \varnothing)$.

If either holds, $\mathrm{CSP}(\mathbb{G})$ *is NP-complete.*

The **Algebraic Dichotomy Conjecture**, due to Bulatov, Jeavons and Krokhin, states:

Conjecture: If $\mathbb{G}$ is *idempotent* and neither condition above holds, then $\mathrm{CSP}(\mathbb{G})$ is in P.