Tutorial on the Constraint Satisfaction Problem

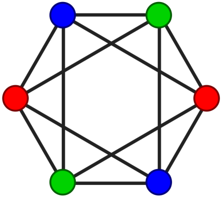
Miklós Maróti

Vanderbilt University and University of Szeged

Nový Smokovec, 2012. September 2–7.

Motivation

- **Constraint satisfaction problem**: natural way to express many combinatorical, mathematical and real world problems



$$3x + 2y - z - 2u = 1$$
$$2x - 2y + 4z + u = -2$$
$$-x + \frac{1}{2}y - z - u = 0$$
$$x + y - 3u = 1$$

1	6					3		
		9	7	1				
		3			8			9
7				4				5
			8		2			
6				3				8
9			2			7		
				9	1	4		
		5					6	1

- **Real benefits** from understanding limitations and better algorithms
- Fruitful **collaboration** between computer science, logic, graph theory and universal algebra, **new research directions**

Goals

- Computational complexity theory
  - Basic defitions and methods only
  - **P**, **NP** and **NP**-complete complexity classes
- Constraint satisfaction problem
  - Introduced for relational structures
  - Basic reduction theorems
  - Connection with relational clones
- Algebraic approach
  - Polymorphisms and compatible algebras,
  - Bounded width algorithm
  - Few subpowers algorithm
  - Applications in universal algebra
- Theory of absorption (ask Libor Barto)

Polynomial time computability

$W = \bigcup_{n=0}^{\infty} \{0,1\}^n$ is the set of **words** over the **alphabet** $\{0,1\}$. The **length** of a word $x \in W$ is $|x|$.

Definition

$f\colon W \to W$ is **computable in polynomial time** if there exist an algorithm and $c, d \in \mathbb{N}$ such that for any word $x \in W$ the algorithm stops in at most $|x|^c + d$ steps and computes $f(x)$.

- **algorithm**: computer program with infinite memory (Turing machine)
- **encoding of mathematical objects**: binary or ASCII text
- **polynomial bound**: masks all differences between various machines and encodings
- **examples**: basic arithmetic of natural numbers, factoring of polynomials over $\mathbb{Q}$, linear programming over finite fields

Decision problems, the complexity class **P**

Definition

Decision problem or **membership problem** is a non-empty proper set $L \subset W$ of words. The problem $L \subset W$ is **solvable in polynomial time** if its characteristic function

$$f(x) = \begin{cases} 1 & \text{if } x \in L, \\ 0 & \text{otherwise} \end{cases}$$

is computable in polynomial time. **P** is the class of polynomial time solvable decision problems.

- "PRIMES is in P" by M. Agrawal, N. Kayal and N. Saxena
- **examples**: class of bipartite graphs, solvable sets of linear equations

The complexity class **NP**

Definition

A decision problem $L \subset W$ is **solvable in nondeterministic polynomial time** if there is a polynomial time computable map $f\colon W \times W \to \{0,1\}$ and $c, d \in \mathbb{N}$ such that

1. if $x \in L$, then there is $y \in W$ so that $|y| \leq |x|^c + d$ and $f(x,y) = 1$,
2. if $x \notin L$, then for all $y \in W$ we have $f(x,y) = 0$.

NP is the class of nondeterministic poly time solvable decision problems.

- f is the **verifier**, y is the **certificate**
- **informally**: $x \in L$ iff there exists a short certificate $y \in W$ that can be verified by a polynomial time algorihm
- **example**: $L = \{\text{3-colorable graphs}\}$, certificate is $g\colon \mathbb{G} \to \{0,1,2\}$, verifier checks if adjacent vertices are assigned different colors

P versus **NP** problem

- **P** $\subseteq$ **NP**, but we do not know if **P** $=$ **NP**
- **P versus NP problem:** one of the Millennium Prize Problems proposed by the Clay Mathematics Institute, One million dollar prize

- We do not know if **NP** $=$ **coNP** where **coNP** $= \{ W \setminus L \mid L \in$ **NP** $\}$
- **Integer factorization**: in **NP** $\cap$ **coNP** but probably not in **P**, decision problem encoded as "does n have a prime factor smaller than k?"

Polynomial time reduction, the **NP**-complete class

Definition

$K \subset W$ is **polynomial time reducible** to $L \subset W$ if there is a polynomial time computable map $f\colon W \to W$ so that $x \in K \iff f(x) \in L$. They are **polynomial time equivalent**, if mutually reducible to each other.

- polynomial time reducibility is a quasi order
- factoring out by polynomial time equivalence we get a poset
- minial element is **P**, we have joins, (what are the exact properties?)

Definition

$L \subset W$ is **NP**-complete if every **NP**-problem is poly time reducible to L.

- Boolean formula satisfiability (SAT, 3-SAT)
- graph 3-coloring, solvable sudoku, graphs with Hamiltonian path, etc.
- Ladner's theorem: if $\mathbf{NP} \neq \mathbf{P}$, then there are intermediate classes.

Relational structures

Definition

$\mathbb{A} = (A; \mathcal{R})$ is a **relational structure**, where for each **relational symbol** $\varrho \in \mathcal{R}$ of **arity** $n \in \mathbb{N}$ we have a relation $\varrho^{\mathbb{A}} \subseteq A^n$. **Directed graph** is a relational structure $\mathbb{G} = (G; \rightarrow)$ with a single binary relation $\rightarrow^{\mathbb{G}} \subseteq G^2$.

Definition

A **homomorphism** from $\mathbb{A} = (A; \mathcal{R})$ to $\mathbb{B} = (B; \mathcal{R})$ is a map $f \colon A \rightarrow B$ that **preserves tuples**, i.e.

$$(a_1, \ldots, a_n) \in \varrho^{\mathbb{A}} \implies (f(a_1), \ldots, f(a_n)) \in \varrho^{\mathbb{B}}.$$

We write $\mathbb{A} \rightarrow \mathbb{B}$ if there is a homomorphism from $\mathbb{A}$ to $\mathbb{B}$.

- **isomorphism**: bijective and both f and f^{-1} are homomorphisms

Constraint satisfaction problem

Definition

For a finite relational structure $\mathbb{B}$ we define

$$\mathrm{CSP}(\mathbb{B}) = \{\, \mathbb{A} \mid \mathbb{A} \to \mathbb{B} \,\}.$$

- CSP() is the class of 3-colorable graphs
- CSP() is the class of bipartite graphs

Dichotomy Conjecture (T. Feder, M. Y. Vardi, 1993)

For every finite structure $\mathbb{B}$ the membership problem for CSP($\mathbb{B}$) is in **P** or **NP**-complete.

The dichotomy conjecture is proved for example when $\mathbb{B}$

- is an undirected graph (P. Hell, J. Nešetřil),
- has at most 3 elements (A. Bulatov)

Open for directed graphs.

Example: solving a system of equations

$$(\exists x, y, z \in \mathbf{Z}_5)(x + y = z \ \wedge \ x + x = y \ \wedge \ z = 1)$$

$$\Updownarrow$$

$$(\exists x, y, z \in \mathbf{Z}_5)((x, y, z) \in F_1 \ \wedge \ (x, x, y) \in F_1 \ \wedge \ z \in F_2),$$

where $F_1 = \{ (x, y, z) \in \mathbf{Z}_5^3 : x + y = z \}$ and $F_2 = \{1\}$.

$$\Updownarrow$$

$$(\exists f : \{1, 2, 3\} \to \mathbf{Z}_5)((f(1), f(2), f(3)) \in F_1 \ \wedge$$
$$(f(1), f(1), f(2)) \in F_1 \ \wedge \ f(3) \in F_2)$$

$$\Updownarrow$$

$$\exists f : \mathbb{A} \to \mathbb{B},$$

where $\mathbb{A} = (\{1, 2, 3\}; E_1, E_2)$, $\mathbb{B} = (\mathbf{Z}_5; F_1, F_2)$

$$E_1 = \{ (1, 2, 3), \ (1, 1, 2) \}, \ E_2 = \{3\}.$$

$$\Updownarrow$$

$$\mathbb{A} \in \mathrm{CSP}(\mathbb{B})$$

Example: solving a system of equations

$$(\exists x, y, z \in \mathbf{Z}_5)(x + y = z \ \wedge \ x + x = y \ \wedge \ z = 1)$$

$$\Updownarrow$$

$$(\exists x, y, z \in \mathbf{Z}_5)((x, y, z) \in F_1 \ \wedge \ (x, x, y) \in F_1 \ \wedge \ z \in F_2),$$

where $F_1 = \{ (x, y, z) \in \mathbf{Z}_5^3 : x + y = z \}$ and $F_2 = \{1\}$.

$$\Updownarrow$$

$$(\exists f : \{1, 2, 3\} \to \mathbf{Z}_5)((f(1), f(2), f(3)) \in F_1 \ \wedge$$
$$(f(1), f(1), f(2)) \in F_1 \ \wedge \ f(3) \in F_2)$$

$$\Updownarrow$$

$$\exists f : \mathbb{A} \to \mathbb{B},$$

where $\mathbb{A} = (\{1, 2, 3\}; E_1, E_2)$, $\mathbb{B} = (\mathbf{Z}_5; F_1, F_2)$

$$E_1 = \{ (1, 2, 3), \ (1, 1, 2) \}, \ E_2 = \{3\}.$$

$$\Updownarrow$$

$$\mathbb{A} \in \mathrm{CSP}(\mathbb{B})$$

Example: solving a system of equations

$$(\exists x, y, z \in \mathbf{Z}_5)(x + y = z \ \wedge \ x + x = y \ \wedge \ z = 1)$$

$$\Updownarrow$$

$$(\exists x, y, z \in \mathbf{Z}_5)((x, y, z) \in F_1 \ \wedge \ (x, x, y) \in F_1 \ \wedge \ z \in F_2),$$

where $F_1 = \{\, (x, y, z) \in \mathbf{Z}_5^3 : x + y = z \,\}$ and $F_2 = \{1\}$.

$$\Updownarrow$$

$$(\exists f : \{1, 2, 3\} \to \mathbf{Z}_5)((f(1), f(2), f(3)) \in F_1 \ \wedge \\ (f(1), f(1), f(2)) \in F_1 \ \wedge \ f(3) \in F_2)$$

$$\Updownarrow$$

$$\exists f : \mathbb{A} \to \mathbb{B},$$

where $\mathbb{A} = (\{1, 2, 3\}; E_1, E_2)$, $\mathbb{B} = (\mathbf{Z}_5; F_1, F_2)$

$E_1 = \{\, (1, 2, 3), \ (1, 1, 2) \,\}$, $E_2 = \{3\}$.

$$\Updownarrow$$

$$\mathbb{A} \in \mathrm{CSP}(\mathbb{B})$$

Example: solving a system of equations

$$(\exists x, y, z \in \mathbf{Z}_5)(x + y = z \ \wedge \ x + x = y \ \wedge \ z = 1)$$

$$\Updownarrow$$

$$(\exists x, y, z \in \mathbf{Z}_5)((x, y, z) \in F_1 \ \wedge \ (x, x, y) \in F_1 \ \wedge \ z \in F_2),$$

where $F_1 = \{\, (x, y, z) \in \mathbf{Z}_5^3 : x + y = z \,\}$ and $F_2 = \{1\}$.

$$\Updownarrow$$

$$(\exists f : \{1, 2, 3\} \to \mathbf{Z}_5)((f(1), f(2), f(3)) \in F_1 \ \wedge$$
$$(f(1), f(1), f(2)) \in F_1 \ \wedge \ f(3) \in F_2)$$

$$\Updownarrow$$

$$\exists f : \mathbb{A} \to \mathbb{B},$$

where $\mathbb{A} = (\{1, 2, 3\}; E_1, E_2)$, $\mathbb{B} = (\mathbf{Z}_5; F_1, F_2)$

$$E_1 = \{\, (1, 2, 3), \ (1, 1, 2) \,\}, \ E_2 = \{3\}.$$

$$\Updownarrow$$

$$\mathbb{A} \in \mathrm{CSP}(\mathbb{B})$$

Example: solving a system of equations

$$(\exists x, y, z \in \mathbf{Z}_5)(x + y = z \ \wedge \ x + x = y \ \wedge \ z = 1)$$

$$\Updownarrow$$

$$(\exists x, y, z \in \mathbf{Z}_5)((x, y, z) \in F_1 \ \wedge \ (x, x, y) \in F_1 \ \wedge \ z \in F_2),$$

where $F_1 = \{\, (x, y, z) \in \mathbf{Z}_5^3 : x + y = z \,\}$ and $F_2 = \{1\}$.

$$\Updownarrow$$

$$(\exists f : \{1, 2, 3\} \to \mathbf{Z}_5)((f(1), f(2), f(3)) \in F_1 \ \wedge$$
$$(f(1), f(1), f(2)) \in F_1 \ \wedge \ f(3) \in F_2)$$

$$\Updownarrow$$

$$\exists f : \mathbb{A} \to \mathbb{B},$$

where $\mathbb{A} = (\{1, 2, 3\}; E_1, E_2)$, $\mathbb{B} = (\mathbf{Z}_5; F_1, F_2)$

$$E_1 = \{\, (1, 2, 3),\ (1, 1, 2) \,\},\ E_2 = \{3\}.$$

$$\Updownarrow$$

$$\mathbb{A} \in \mathrm{CSP}(\mathbb{B})$$

Adding the equality relation

Lemma

Let $\mathbb{C} = (B; \mathcal{R} \cup \{\varepsilon\})$ *be the extension of* $\mathbb{B} = (B; \mathcal{R})$ *with the relation* $\varepsilon = \{\, (b, b) \mid b \in B \,\}$. *Then* $\mathrm{CSP}(\mathbb{B})$ *is poly time equivalent with* $\mathrm{CSP}(\mathbb{C})$.

Proof.

- $\mathrm{CSP}(\mathbb{B})$ is polynomial time reducible to $\mathrm{CSP}(\mathbb{C})$
  - for $\mathbb{A} = (A; \mathcal{R})$ we construct $\mathbb{A}' = (A'; \mathcal{R} \cup \{\varepsilon\})$ such that $\mathbb{A} \in \mathrm{CSP}(\mathbb{B}) \iff \mathbb{A}' \in \mathrm{CSP}(\mathbb{C})$
  - let $A' = A$ and $\varepsilon^{\mathbb{A}'} = \emptyset$
- $\mathrm{CSP}(\mathbb{C})$ is polynomial time reducible to $\mathrm{CSP}(\mathbb{B})$
  - for $\mathbb{A} = (A; \mathcal{R} \cup \{\varepsilon\})$ we construct $\mathbb{A}' = (A'; \mathcal{R})$ such that $\mathbb{A} \in \mathrm{CSP}(\mathbb{C}) \iff \mathbb{A}' \in \mathrm{CSP}(\mathbb{B})$
  - let ϑ be the equivalence relation generated by $\varepsilon^{\mathbb{A}}$
  - let $A' = A/\vartheta$ and $\varrho^{\mathbb{A}'} = (\varrho^{\mathbb{A}})/\vartheta$
  - if $f\colon \mathbb{A} \to \mathbb{C}$, then $\vartheta \subseteq \ker f$ and $f'\colon \mathbb{A}' \to \mathbb{B}$, $f'(x/\vartheta) = f(x)$ works
  - if $g\colon \mathbb{A}' \to \mathbb{B}$, then $g'\colon \mathbb{A} \to \mathbb{C}$, $g'(x) = g(x/\vartheta)$ works □

Adding projections and products (and intersections)

Lemma

Let $\mathbb{C} = (B; \mathcal{R} \cup \{\gamma\})$ be the extension of $\mathbb{B} = (B; \mathcal{R})$ with a relation γ that is a projection of $\beta \in \mathcal{R}^{\mathbb{B}}$. Then CSP($\mathbb{B}$) *is polynomial time equivalent with* CSP($\mathbb{C}$).

Idea: We let $\mathbb{A}' = (A'; \mathcal{R})$ be the same as $\mathbb{A} = (A; \mathcal{R} \cup \{\gamma\})$, except for each tuple $(a_1, \ldots, a_k) \in \gamma^{\mathbb{A}}$ we add $n - k$ new elements $x_{k+1}, \ldots, x_n$ to A' and add the tuple $(a_1, \ldots, a_k, x_{k+1}, \ldots, x_n)$ to the relation $\beta^{\mathbb{A}'}$.

Lemma

Let $\mathbb{C} = (B; \mathcal{R} \cup \{\gamma\})$ be the extension of $\mathbb{B} = (B; \mathcal{R})$ with a relation $\gamma = \alpha \times \beta$ for $\alpha, \beta \in \mathcal{R}^{\mathbb{B}}$. Then CSP($\mathbb{B}$) *is polynomial time equivalent with* CSP($\mathbb{C}$).

Idea: We let $\mathbb{A}' = (A'; \mathcal{R})$ be the same as $\mathbb{A} = (A; \mathcal{R} \cup \{\gamma\})$, except for each tuple $(a_1, \ldots, a_{n+m}) \in \gamma^{\mathbb{A}}$ we add the tuple $(a_1, \ldots, a_n)$ to $\alpha^{\mathbb{A}'}$ and the tuple $(a_{n+1}, \ldots, a_{n+m})$ to $\beta^{\mathbb{A}'}$.

Relational clones

Definition

A set Γ of relations over a fixed set is a **relational clone** if it contains the equality relation and is closed under intersections, projections, products. The relational clone generated by Γ is denoted by $\langle \Gamma \rangle$.

Theorem

Let $\mathbb{B} = (B; \mathcal{R})$ and $\mathbb{C} = (B; \mathcal{S})$ be finite relational structures on the same base set. If $\langle \mathcal{R}^{\mathbb{B}} \rangle \subseteq \langle \mathcal{S}^{\mathbb{C}} \rangle$, then $\mathrm{CSP}(\mathbb{B})$ poly time reducible to $\mathrm{CSP}(\mathbb{C})$.

Proof.

Let $\mathbb{D} = (B; \mathcal{R} \cup \mathcal{S})$ be the extension of both $\mathbb{B}$ and $\mathbb{C}$. Clearly, $\mathrm{CSP}(\mathbb{B})$ is polynomial time reducible to $\mathrm{CSP}(\mathbb{D})$. Since $\mathcal{R}^{\mathbb{B}} \subseteq \langle \mathcal{S}^{\mathbb{C}} \rangle$, we get by the previous lemmas, that $\mathrm{CSP}(\mathbb{D})$ is poly time equivalent with $\mathrm{CSP}(\mathbb{C})$. □

We can assign an algorithmic complexity class to finitely generated relational clones (or functional clones)!

Reduction to cores

- $\to$ is a quasi order on the set of finite structures of same signature

Lemma

If $\mathbb{B} \leftrightarrow \mathbb{C}$*, then* $\mathrm{CSP}(\mathbb{B}) = \mathrm{CSP}(\mathbb{C})$.

Lemma

Let $\mathbb{C}$ *be a minimal member of the* $\leftrightarrow$ *class of a finite structure* $\mathbb{B}$. *Then*

- *every endomorphism of* $\mathbb{C}$ *is an automorphism,*
- $\mathbb{C}$ *is uniquely determined up to isomorphism, and*
- $\mathbb{C}$ *is isomorphic to a substructure of* $\mathbb{B}$.

- We say that $\mathbb{C}$ is a **core** if it has no proper endomorphism

Theorem

Let $\mathbb{B}$ *be a finite relational structure and* $\mathbb{C}$ *be its core. Then* $\mathrm{CSP}(\mathbb{B}) = \mathrm{CSP}(\mathbb{C})$. □

Adding the singleton constant relations to cores

Lemma

Let $\mathbb{C} = (B; \mathcal{R} \cup \{\, \delta_b \mid b \in B \,\})$ *be the extension of a core* $\mathbb{B} = (B; \mathcal{R})$ *with* $\delta_b = \{b\}$ *for* $b \in B$. *Then* $\mathrm{CSP}(\mathbb{B})$ *is poly time equivalent with* $\mathrm{CSP}(\mathbb{C})$.

Sketch of proof.

Fix an ordering $B = \{b_1, \ldots, b_k\}$ and consider the k-ary relation

$$\sigma^{\mathbb{B}} = \{\, (f(b_1), \ldots, f(b_k)) \mid f \colon \mathbb{B} \to \mathbb{B} \,\}.$$

$\sigma^{\mathbb{B}}$ is in $\langle \mathcal{R}^{\mathbb{B}} \rangle$, so we may assume, that $\mathcal{R}$ already contains σ and the equality relation ε. For $\mathbb{A} = (A; \mathcal{R})$ define $\mathbb{A}' = (A \mathbin{\dot\cup} B; \mathcal{R})$ as

$$\varepsilon^{\mathbb{A}'} = \varepsilon^{\mathbb{A}} \cup \{\, (a, b) \mid b \in B, a \in \delta_b^{\mathbb{A}} \,\},$$

$$\sigma^{\mathbb{A}'} = \sigma^{\mathbb{A}} \cup \{(b_1, \ldots, b_k)\}, \text{ and}$$

$$\varrho^{\mathbb{A}'} = \varrho^{\mathbb{A}} \text{ for all } \varrho \in \mathcal{R} \setminus \{\sigma, \varepsilon\}.$$

□

Finding solutions, limiting the signature

Theorem

If CSP($\mathbb{B}$) *is in* **P**, *then there exists a polynomial time algorithm that, for a given* $\mathbb{A}$, *finds a homomorphism* $f : \mathbb{A} \to \mathbb{B}$ *or proves that no such homomorphism exists.*

Theorem (T. Feder, M. Y. Vardi, 1993)

For every finite relational structure $\mathbb{B}$ *there exists a directed graph* $\mathbb{G}$ *such that* CSP($\mathbb{B}$) *is polynomial time equivalent with* CSP($\mathbb{G}$).

Original proof "destroys algebraic structure", there is a new proof by J. Bulin, D. Delić, M. Jackson and T. Niven, that preserve most linear idempotent Maltsev conditions (but not Maltsev operations).

Theorem

For every finite relational structure $\mathbb{B}$ *there exists a structure* $\mathbb{C}$ *with only binary relations so that* CSP($\mathbb{B}$) *is poly time equivalent with* CSP($\mathbb{G}$).

Finite duality

- set of finite relational structures modulo $\leftrightarrow$ is a partially ordered set
- isomorphic to the set of core isomorphism types
- minimal [maximal] element: 1-element structure, with empty [full] relations
- join: disjoint union, meet: direct product,
- satisfies distributive laws, join irreducible = connected
- Heyting algebra (relatively pseudocomplemented)
- exponentiation: $\mathbb{B}^{\mathbb{A}}$ is defined on B^A as $(f_1, \dots, f_n) \in \varrho^{\mathbb{B}^{\mathbb{A}}}$ iff

$$(a_1, \dots, a_n) \in \varrho^{\mathbb{A}} \implies (f_1(a_1), \dots, f_n(a_n)) \in \varrho^{\mathbb{B}}.$$

- $\mathbb{B} \wedge \mathbb{A} \leq \mathbb{C} \iff \mathbb{C}^{\mathbb{B}\times\mathbb{A}} = (\mathbb{C}^{\mathbb{B}})^{\mathbb{A}}$ has a loop $\iff \mathbb{A} \leq \mathbb{C}^{\mathbb{B}}$
- if $\mathbb{B}$ is join irreducible with lower cover $\mathbb{C}$, then $(\mathbb{B}, \mathbb{C}^{\mathbb{B}})$ is a dual pair

Theorem (J. Nešetřil, C. Tardif, 2010)

Let $\mathbb{B}$ be a finite connected core structure. Then $\mathbb{B}$ has a dual pair $\mathbb{D}$, i.e. $\mathrm{CSP}(\mathbb{B}) = \{\, \mathbb{A} \mid \mathbb{D} \not\to \mathbb{A} \,\}$, if and only if $\mathbb{B}$ is a tree.

Algebraic approach: polymorphisms

Definition

A **polymorphism** of $\mathbb{B}$ is a homomorphism $p : \mathbb{B}^n \to \mathbb{B}$, that is an n-ary map that preserves the relations of $\mathbb{B}$, e.g. for a directed graph $\mathbb{B} = (B; \to)$

$$a_1 \to b_1, \dots, a_n \to b_n \implies p(a_1, \dots, a_n) \to p(b_1, \dots, b_n).$$

$\mathrm{Pol}(\mathbb{B}) = \{ p \mid p : \mathbb{B}^n \to \mathbb{B} \}$ is the **clone of polymorphisms**.

- if $\langle \mathbb{B} \rangle \subseteq \langle \mathbb{C} \rangle$ then $\mathrm{CSP}(\mathbb{B})$ is poly time reducible to $\mathrm{CSP}(\mathbb{C})$
- $\{ \langle \mathbb{B} \rangle \mid \mathrm{CSP}(\mathbb{B}) \in \mathbf{P} \}$ is a filter in the poset of finitely generated relational clones, $\{ \langle \mathbb{B} \rangle \mid \mathrm{CSP}(\mathbb{B}) \in \mathbf{NP}\text{-complete} \}$ is an ideal
- $\mathrm{CSP}(\mathbb{B})$ is in $\mathbf{P}$ if $\mathbb{B}$ has nice polymorphisms

Question

Which polymorphisms guarantee that $\mathrm{CSP}(\mathbb{B})$ is in $\mathbf{P}$?

Constraint satisfaction problem for algebras

Definition

Let $\mathbf{B} = (B; \mathcal{F})$ be a finite algebra. $(V, \mathcal{C})$ is an **instance for** $\mathrm{CSP}(\mathbf{B})$ if

- V is a finite set of **variables**,
- $\mathcal{C}$ is a finite set of **constraints**,
- where each constraint $(S, \mathbf{R}) \in \mathcal{C}$ has
  - a **scope** $S \subseteq V$, and
  - a **constraint relation** $\mathbf{R} \leq \mathbf{B}^S$.

A map $f \colon V \to B$ is a **solution** if $f|_S \in \mathbf{R}$ for all $(S, \mathbf{R}) \in \mathcal{C}$. We define $\mathrm{CSP}(\mathbf{B})$ to be the set of all solvable instances.

Theorem

$\mathrm{CSP}(\mathbb{B})$ *is polynomial time equivalent with a subproblem of* $\mathrm{CSP}(\mathbf{B})$ *where all constraint relations must be in* $\mathcal{R}^{\mathbb{B}}$ *(after suitable ordering of elements).*

Local and global reducibility

Definition

A relational structure $\mathbb{B} = (B; \mathcal{R})$ and an algebra $\mathbf{B} = (B; \mathcal{F})$ are **compatible** if $\mathcal{F}^{\mathbf{B}} \subseteq \mathrm{Pol}(\mathbb{B})$, or alternatively, $\mathcal{R}^{\mathbb{B}} \subseteq \mathrm{Inv}(\mathbf{B})$.

Definition

$\mathrm{CSP}(\mathbf{B})$ is **locally polynomial time reducible** to $\mathrm{CSP}(\mathbf{C})$ if for every relational structure $\mathbb{B}$ compatible with $\mathbf{B}$ there is a structure $\mathbb{C}$ compatible with $\mathbf{C}$ such that $\mathrm{CSP}(\mathbb{B})$ is polynomial time reducible to $\mathrm{CSP}(\mathbb{C})$.

Subtle difference between local and regular reducibility.

Theorem

Let $\mathbf{B}$ and $\mathbf{C}$ be finite algebras. If $\mathcal{V}(\mathbf{B}) \subseteq \mathcal{V}(\mathbf{C})$, then $\mathrm{CSP}(\mathbf{B})$ is locally polynomial time reducible to $\mathrm{CSP}(\mathbf{C})$.

Taylor terms

Theorem (D. Hobby, R. McKenzie)

For a locally finite variety $\mathcal{V}$ the followings are equivalent:

- *$\mathcal{V}$ omits type* **1** *(tame congruence theory),*
- *$\mathcal{V}$ has a* **Taylor** *term operation:*

$$
\begin{aligned}
t(x, x, \dots, x) &\approx x, \\
t(x, -, \dots, -) &\approx t(y, -, \dots, -), \\
t(-, x, \dots, -) &\approx t(-, y, \dots, -), \\
&\vdots \\
t(-, -, \dots, x) &\approx t(-, -, \dots, y).
\end{aligned}
$$

Theorem (W. Taylor, 1977)

Every idempotent, locally finite variety without a Taylor term contains a two-element algebra in which every operation is a projection.

The **NP**-complete case

Theorem (A. Bulatov, P. Jeavons, A. Krokhin)

If $\mathbb{B}$ is a finite core relational structure without a Taylor polymorphism, then CSP($\mathbb{B}$) *is* **NP***-complete.*

Proof.

- $\mathbb{B}$ is a core, so we may assume $\{b\}$ is a relation for all $b \in B$
- the algebra $\mathbf{B} = (B; \mathrm{Pol}(\mathbb{B}))$ is idempotent
- the variety $\mathcal{V}(\mathbf{B})$ contains a two-element trivial algebra $\mathbf{C}$
- 3-SAT is poly equivalent with CSP($\mathbb{C}$) for some $\mathbb{C}$ compatible with $\mathbf{C}$
- CSP($\mathbb{C}$) $\leq$ CSP($\mathbb{D}$) $\leq$ CSP($\mathbb{B}$) for some $\mathbb{D}$ compatible with $\mathbf{B}$ □

Algebraic Dichotomy Conjecture

If $\mathbb{B}$ is a core and has a Taylor polymorphism, then CSP($\mathbb{B}$) is in **P**.

CSP for semilattice algebras

Theorem

Let $\mathbf{B}$ *be a finite algebra with a semilattice term operation. Then* $\mathrm{CSP}(\mathbf{B})$ *is solvable in polynomial time.*

Sketch of proof.

- Take an instance $(V;\mathcal{C})$ for $\mathrm{CSP}(\mathbf{B})$
- Add the $(\{x\},\mathbf{B})$ constraint for each variable $x \in V$
- For each scope S create a single constraint relation $\mathbf{R}_S \leq \mathbf{B}^S$
- Modify the instance until $\pi_x(\mathbf{R}_S) = \mathbf{R}_{\{x\}}$ for all scope S and $x \in S$:
  - $\mathbf{R}'_{\{x\}} = \mathbf{R}_{\{x\}} \cap \pi_x(\mathbf{R}_S)$
  - $\mathbf{R}'_S = \{\, f \in \mathbf{R}_S \mid f(x) \in \mathbf{R}_{\{x\}} \,\}$.
- The new instance has the same set of solutions as the original
- Define $g\colon V \to B$, $g(x) = \bigwedge \mathbf{R}_{\{x\}} \in \mathbf{R}_{\{x\}}$
- For $(S,\mathbf{R}_S)$ and $x \in S$ we have $f_x \in \mathbf{R}_S$ with $f_x(x) = g(x)$
- Take $f = \bigwedge_{x\in S} f_x \in \mathbf{R}_S$ and verify that $g|_S = f$, so g is a solution □

Local consistency algorithm, CSP for NU algebras

Definition

An instance $(V;\mathcal{C})$ for CSP($\mathbf{B}$) is (k,l)-**consistent**, if

- for each scope S it has a unique constraint $(S;\mathbb{R}_S)$,
- it contains a constraint for each scope $S \subseteq V$, $|S| \leq l$, and
- $\pi_S(\mathbf{R}_T) = \mathbf{R}_S$ whenever $S \subseteq T$ are scopes and $|S| \leq k$.

Theorem

For every instance $(V;\mathcal{C})$ for CSP($\mathbf{B}$) a (k,l)-consistent instance $(V,\mathcal{C}')$ can be computed in polynomial time that has the same set of solutions.

Theorem

Let $\mathbf{B}$ be a finite algebra with a k-ary near-unanimity term operation. Then CSP($\mathbf{B}$) is solvable in polynomial time.

- apply the $(k-1,k)$ local consistency algorithm
- the instance has a solution iff all constraint relations are nonempty

Bounded width

Definition

A relational structure $\mathbb{B}$ has **bounded width** if there exist $k \leq l$ such that every nonempty (k, l)-consistent instance for $\mathrm{CSP}(\mathbb{B})$ has a solution.

If $\mathbb{B}$ has bounded width, then $\mathrm{CSP}(\mathbb{B})$ is solvable in polynomial time by the local consistency algorithm.

Theorem (B. Larose, L. Zádori, 2007)

If a core relational structure $\mathbb{B}$ has bounded width, then the corresponding algebra $\mathbf{B} = (B; \mathrm{Pol}(\mathbb{B}))$ generates congruence meet-semidistributive variety.

Theorem (L. Barto, M. Kozik, 2009)

A core relational structure $\mathbb{B}$ has bounded width if and only if the corresponding algebra $\mathbf{B} = (B; \mathrm{Pol}(\mathbb{B}))$ generates congruence meet-semidistributive variety.

CSP for Maltsev algebras

Definition

Let $\mathbf{B}$ be an algebra with a Maltsev term p, and $n \in \mathbb{N}$.

- **index** is an element of $\{1, \ldots, n\} \times B^2$,
- an index (i, a, b) is **witnessed** in $Q \subseteq B^n$ if there exist $f, g \in Q$ so that $f_1 = g_1, \ldots, f_{i-1} = g_{i-1}$ and $f_i = a$, $g_i = b$
- a **compact representation** of a subpower $\mathbf{R} \leq \mathbf{B}^n$ is a subset $Q \subseteq R$ that witnesses the same set of indices as $\mathbf{R}$ and $|Q| \leq 2|B|^2 \cdot n$.

Lemma

The compact representation Q of $\mathbf{R} \leq \mathbf{B}^n$ generates $\mathbf{R}$ as a subalgebra.

- Idea: take $f \in \mathbf{R}$ and its best approximation $g \in \mathrm{Sg}(Q)$
- let i be the smallest index where $f_i \neq g_i$
- take witnesses $f', g' \in Q$ for the index $(i, f(i), g(i))$
- but then $p(f', g', g)$ is a better approximation of f

CSP for Maltsev algebras

Lemma

The 2-projections of $\mathbf{R} \leq \mathbf{B}^n$ *are polynomial time computable from the compact representation of* $\mathbf{R}$*.*

- Idea: generate as usual, but keep track of representative tuples only

Lemma

For $c_1, \dots, c_k \in B$ *the compact representation of the subpower* $\mathbf{R}' = \{ f \in \mathbf{R} \mid f_1 = c_1, \dots, f_k = c_k \}$ *is poly time computable from that of* $\mathbf{R}$*.*

- Idea: we prove it for $k = 1$ and use induction
- take $f, g \in \mathbf{R}'$ witnesses for (i, a, b) in $\mathbf{R}'$
- then we have witnesses $f', g' \in Q$ for (i, a, b), and
- $h \in \mathrm{Sg}(Q)$ such that $h_1 = c$ and $h_i = a$
- thus $h, p(h, f', g') \in \mathrm{Sg}(Q)$ witness (i, a, b) in $\mathbf{R}'$

CSP for Maltsev algebras

Lemma

For $c \in B$ and $k \leq n$ the compact representation of the subpower $\mathbf{R}' = \{ f \in \mathbf{R} \mid f_k = c \}$ is polynomial time computable from that of $\mathbf{R}$.

Lemma

For $1 \leq k, l \leq n$ the compact representation of the subpower $\mathbf{R}' = \{ f \in R \mid f_k = f_l \}$ is polynomial time computable from that of $\mathbf{R}$.

Theorem

Let $\mathbf{B}$ be a finite Maltsev algebra. Then the compact representation of the product, projection and intersection of subpowers is computable in polynomial time from the compact representations of the arguments.

Theorem (A. Bulatov, V. Dalmau, 2006)

Let $\mathbf{B}$ be a finite algebra with a Maltsev term operation. Then $\mathrm{CSP}(\mathbf{B})$ *is solvable in polynomial time.*

CSP for few subpower algebras

Definition

A finite algebra $\mathbf{B}$ has **few subpowers**, if the number of subalgebras of $\mathbf{B}^n$ is bounded by 2^{n^a+b} for some fixed numbers $a, b \in \mathbb{N}$.

Theorem (Berman, Idziak, Marković, McKenzie, Valeriote, Willard)

A finite algebra $\mathbf{B}$ *has few subpowers iff it has a k-edge term operation*

$$\begin{aligned} p(y, y, x, x, \dots, x) &\approx x, \\ p(x, y, y, x, \dots, x) &\approx x, \\ p(x, x, x, y, \dots, x) &\approx x, \\ &\dots \\ p(x, x, x, x, \dots, y) &\approx x. \end{aligned}$$

Theorem (Idziak, Marković, McKenzie, Valeriote, Willard, 2010)

Let $\mathbf{B}$ *be a finite algebra with a k-edge term operation. Then* $\mathrm{CSP}(\mathbf{B})$ *can be solved in polynomial time.*

CSP for smooth digraphs

Theorem (McKenzie, Maróti, 2007)

For a locally finite variety has a Taylor term if and only if it has a **weak near-unanimity** *term operation:*

$$t(y, x, \dots, x) \approx \dots \approx t(x, \dots, x, y) \quad \text{and} \quad t(x, \dots, x) \approx x.$$

Theorem (L. Barto, M. Kozik, 2009)

Let $\mathbb{G}$ be a core directed graph with no sources and sinks. If $\mathbb{G}$ has a weak near-unanimity polymorphism, then it is a disjoint union of directed circles. So the dichotomy conjecture holds for digraphs with no sources and sinks.

The next classical theorem is now an easy corollary:

Theorem (P. Hell, J. Nešetřil, 1990)

Let $\mathbb{G}$ be an undirected graph. If $\mathbb{G}$ is bipartite, then CSP($\mathbb{G}$) *is in* **P**, *otherwise it is* **NP***-complete.*

Siggers term

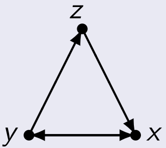
Theorem (M. Siggers, 2008; K. Kearnes, P. Markovic, R. McKenzie)

A locally finite variety has a Taylor term if and only if it has Siggers term

$$t(x,x,x,x) \approx x \quad \text{and} \quad t(x,y,z,y) \approx t(y,z,x,x).$$

Proof.

- let $\mathbf{G} = \mathbf{F}_3(\mathcal{V})$ be the 3-generated free algebra
- let $\mathbb{G} = (G; \to)$ be the digraph $\to^{\mathbb{G}} = \mathrm{Sg}(\{(x,y),(y,z),(z,x),(y,x)\})$ whose edge relation is generated by these edges



- no sources and sinks: $t(x,y,z) \to t(y,z,x) \to t(z,x,y) \to t(x,y,z)$
- because of the generating edges, the core of $\mathbb{G}$ must contain a loop
- the loop edge is $t((x,y),(y,z),(z,x),(x,z))$ for some term t. □

Further algebraic results

Theorem (E. Aichinger, P. Mayr, R. McKenzie, 2011)

There are countable many Maltsev clones on a finite set. The same holds for clones with an edge operation.

Theorem

A finite algebra generates a congruence meet-semidistributive variety if and only if it has a ternary and a 4-ary weak near-unanimity operation s and t such that $t(x, x, y) \approx s(x, x, x, y)$.

Theorem (L. Barto, 2011)

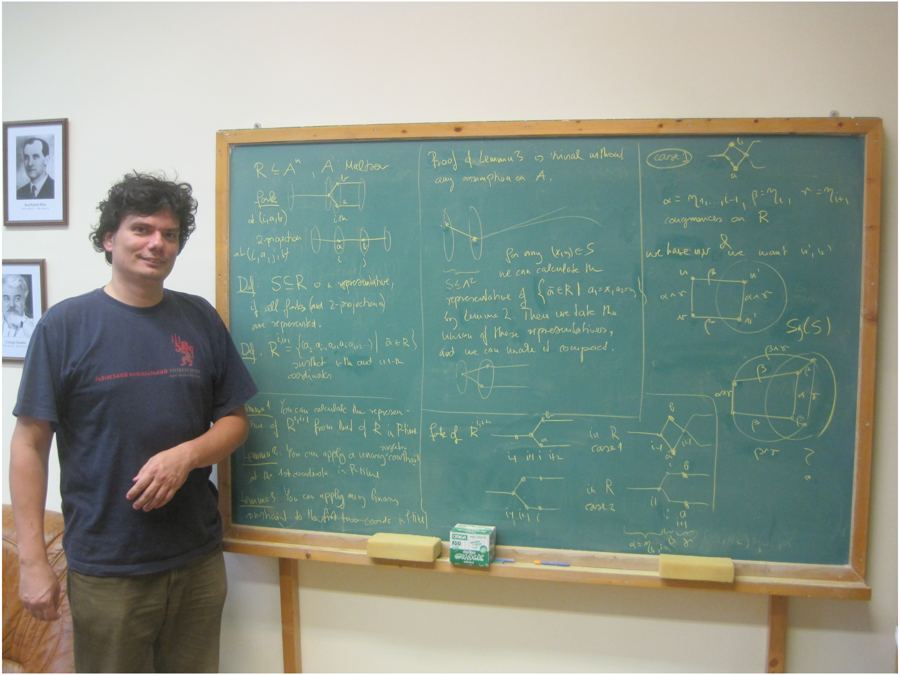
If a finite relational structure has Jónsson polymorphisms, then it has a near-unanimity polymorphism.

Theorem (L. Barto)

If a finite relational structure has Gumm polymorphisms (congruence modularity), then it has an edge polymorphism.

Thank you!


Sun Drop
CITRUS SODA
20 OZ SINGLE
99¢


Proof of Lemma 3 is trivial without any assumption on A.
Def. S ⊆ R is a representative, if all forks (and 2-projections) are represented.
case 1
case 2
Sg(S)

Maltsev on top Algorithm

Theorem (M. Maróti)

Suppose, that each algebra $\mathbf{B} \in \mathcal{B}$ *has a congruence* $\beta \in \mathrm{Con}(\mathbf{B})$ *such that* $\mathbf{B}/\beta$ *has few subpowers and each* β *block has bounded width. Then we can solve the constraint satisfaction problem over* $\mathcal{B}$ *in polynomial time.*

Proof Overview.

- Take an instance $\mathcal{A} = \{\, \mathbf{B}_i, \mathbf{R}_{ij} \mid i, j \in V \,\}$ and $\beta_i \in \mathrm{Con}(\mathbf{B}_i)$
- Consider **extended constraints** that not only limit the projection of the solution set to the $\{i, j\}$ coordinates, but also to $\prod_{v \in V} \mathbf{B}_v/\beta_v$
- Use extended (2,3)-consistency algorithm
- Obtain a solution modulo the β congruences so that the restriction of the problem to the selected congruence blocks is (2,3)-consistent.
- By the bounded width theorem there exists a solution. □