The Complexity of Constraint Satisfaction Problems

Andrei Krokhin
Durham University

Tutorial, Part II - Here and Now

Recap from Yesterday's Lecture

- Three forms of CSP: Variable-Value, Sat, and Hom
- Parameterisation: CSP(Γ), CSP($\mathcal{B}$)
- Feder-Vardi (Dichotomy) Conjecture
- Three approaches: graphs, logic, and algebra
- Pol(Γ) determines the complexity of CSP(Γ)

Today

1. Constraints and Their Complexity: An introduction
2. Universal Algebra for CSP: A general theory
   - From clones to algebras
   - From algebras to varieties
   - Hardness results
   - Algebraic Dichotomy Conjecture
   - Some tractability results
3. UA (and a bit of logic) for CSP: A bigger picture

Reducing the Domain

For a unary operation f and a relation R on D, let $f(R) = \{(f(a_1), \ldots, f(a_n)) \mid (a_1, \ldots, a_n) \in R\}$.
For a constraint language Γ, let $f(\Gamma) = \{f(R) \mid R \in \Gamma\}$.

Theorem 1 (Jeavons, 1998) *Let Γ be finite, and let $f \in \mathrm{Pol}(\Gamma)$ be unary with minimal range. Then $\mathrm{CSP}(\Gamma)$ and $\mathrm{CSP}(f(\Gamma))$ are polynomial-time equivalent.*

Proof. Take an instance $\mathcal{P} = \bigwedge R_i(\overline{s}_i)$ of $\mathrm{CSP}(\Gamma)$ and consider the instance $\mathcal{P}' = \bigwedge f(R_i)(\overline{s}_i)$ of $\mathrm{CSP}(f(\Gamma))$.

Since $f(R_i) \subseteq R_i$, we have $Sol(\mathcal{P}') \subseteq Sol(\mathcal{P})$, and conversely, for each $\varphi \in Sol(\mathcal{P})$, $f \circ \varphi$ is a solution to $\mathcal{P}'$.

Mapping $\mathcal{P}' \mapsto \mathcal{P}$ is the reduction in the other direction.

Adding the Constants

By previous slide, assume that unary operations in $\mathrm{Pol}(\Gamma)$ form a permutation group G, i.e., Γ is a core.

Theorem 2 (Bulatov, Jeavons, K, 2005)
Let $\Gamma' = \Gamma \cup \{\{a\} \mid a \in D\}$. *Then* $\mathrm{CSP}(\Gamma)$ *and* $\mathrm{CSP}(\Gamma')$ *are polynomial-time equivalent.*

Proof. Obviously, $\mathrm{CSP}(\Gamma)$ reduces to $\mathrm{CSP}(\Gamma')$.

The other direction. Let $D = \{a_1, \ldots, a_n\}$. Then $R_G \in \langle \Gamma \rangle$ where

$$R_G = \{(g(a_1), \ldots, g(a_n)) \mid g \in G\}.$$

We may assume that $R_G \in \Gamma$ and $=_D \in \Gamma$.

Proof cont'd

Take an instance $\mathcal{P}'$ of CSP(Γ') over a set of variables V' and build an equivalent instance $\mathcal{P}$ of CSP(Γ) as follows.

- Include all constraints from $\mathcal{P}'$ to $\mathcal{P}$
- Introduce new variables $y_a, a \in D$
- Replace each constraint of the form $x = a$ with $x = y_a$
- Introduce new constraint $R_G(y_{a_1}, \ldots, y_{a_n})$

Any solution of $\mathcal{P}'$ extends to a solution of $\mathcal{P}$ by $y_{a_i} \mapsto a_i$.

If ϕ is a solution to $\mathcal{P}$ then we have
$\phi(y_{a_1}, \ldots, y_{a_n}) = (g(a_1), \ldots, g(a_n))$ for some $g \in G$.
Then $g^{-1} \circ \phi$ (restricted to V') is a solution to $\mathcal{P}'$.

Search Problem

Theorem 3 (Bulatov, Jeavons, K, 2005)
If the decision problem CSP(Γ) *is tractable then the corresponding search problem is tractable as well.*

Proof. Take an instance $\mathcal{P}$ of CSP(Γ) and build an equivalent instance $\mathcal{P}'$ of CSP($f(\Gamma)$) s.t. $Sol(\mathcal{P}') \subseteq Sol(\mathcal{P})$.

Remember: CSP($f(\Gamma) \cup \{\{a\} \mid a \in f(D)\}$) is tractable.

For all variables x (in order)
  for all values $a \in f(D)$
    if $\mathcal{P}' \wedge (x = a)$ is satisfiable
      set $\mathcal{P}' := \mathcal{P}' \wedge (x = a)$ and go to next variable

From CSP to Algebras

Definition 1 *A finite algebra is a pair* $\mathbf{A} = (D, F)$ *where* D *is a finite set and* F *is a family of operations on* D.

The clone $\langle F \rangle$ *is called the clone of term operations of* $\mathbf{A}$. *Two algebras* $\mathbf{A}_1 = (D, F_1)$ *and* $\mathbf{A}_2 = (D, F_2)$ *are said to be term equivalent if they have the same clone of term op's.*

Definition 2 *Let* $\mathbf{A} = (D, F)$ *be a finite algebra.*
Let $\mathrm{CSP}(\mathbf{A}) = \{\mathrm{CSP}(\Gamma) \mid \Gamma \subseteq \mathrm{Inv}(F), |\Gamma| < \infty\}$.
We say that $\mathbf{A}$ *is tractable if each problem in* $\mathrm{CSP}(\mathbf{A})$ *is tractable, and* $\mathbf{A}$ *is* **NP**-*complete if some problem in* $\mathrm{CSP}(\mathbf{A})$ *is* **NP**-*complete.*

Note: Term equivalent algebras have the same complexity.

A View on CSP(A)

Fact. Relations from $\mathrm{Inv}(F)$ are universes of algebras from $\mathsf{SP}_{fin}(\mathbf{A})$ (the so-called subpowers of $\mathbf{A}$).

Take an instance $\{(\overline{s}_1, R_1), \ldots, (\overline{s}_q, R_q)\}$ of a problem in CSP($\mathbf{A}$), over a set of variables $V = \{x_1, \ldots, x_n\}$.

For a constraint $(\overline{s}_i, R_i)$, consider the following subalgebra $\mathbf{A}_i$ of $\mathbf{A}^V$: $\{\overline{a} \in D^V \mid \mathrm{pr}_{\overline{s}_i}\, \overline{a} \in R_i\}$.

Solutions to the instance = elements in $\bigcap_{i=1}^q \mathbf{A}_i$.

Hence, CSP($\mathbf{A}$) = Subalgebra Intersection problem: "given" subalgebras $\mathbf{A}_1, \ldots, \mathbf{A}_q$ of $\mathbf{A}^k$, $k \geq 1$, is it true that $\bigcap_{i=1}^q \mathbf{A}_i \neq \emptyset$?

Varieties

Definition 3 *For a class $\mathcal{K}$ of similar algebras, let*

- $\mathsf{H}(\mathcal{K})$ *be the class of all hom images of algebras from* $\mathcal{K}$
- $\mathsf{S}(\mathcal{K})$ *be the class of all subalgebras of algebras from* $\mathcal{K}$
- $\mathsf{P}(\mathcal{K})$ *and* $\mathsf{P}_{fin}(\mathcal{K})$ *be the classes of all and all finite, respectively, direct products of algebras from* $\mathcal{K}$

A class of similar algebras that is closed under the operators H, S *and* P *is called a variety.*

For an algebra $\mathbf{A}$, *the class* $\mathsf{HSP}(\mathbf{A})$ *is the variety generated by* $\mathbf{A}$, *and is denoted* $\mathrm{var}(\mathbf{A})$.

From Algebras to Varieties

Theorem 4 (Bulatov, Jeavons, 2003) *If an algebra* $\mathbf{A}$ *is tractable then every finite algebra in* $\mathrm{var}(\mathbf{A})$ *is tractable. If* $\mathrm{var}(\mathbf{A})$ *contains a finite* **NP**-*complete algebra then* $\mathbf{A}$ *is* **NP**-*complete.*

Proof. We know $(\mathsf{HSP}(\mathbf{A}))_{fin} = \mathsf{HSP}_{fin}(\mathbf{A})$.

Let $\mathbf{B} = (B, F_B)$ be a subalgebra or a homomorphic image or a finite direct power of $\mathbf{A} = (D, F_A)$.

Take a finite $\Gamma \subseteq \mathrm{Inv}(F_B)$. We need to reduce $\mathrm{CSP}(\Gamma)$ to $\mathrm{CSP}(\Gamma')$ for some finite $\Gamma' \subseteq \mathrm{Inv}(F_A)$.

If $\mathbf{B}$ is a subalgebra of $\mathbf{A}$ then $\mathrm{Inv}(F_B) \subseteq \mathrm{Inv}(F_A)$, so we can take $\Gamma' = \Gamma$.

Proof: Homomorphic Images

Let $\psi : \mathbf{A} \twoheadrightarrow \mathbf{B}$ be a surjective homomorphism.

For a k-ary relation R on B, let

$$\psi^{-1}(R) = \{(a_1, \ldots, a_k) \in D^k \mid (\psi(a_1), \ldots, \psi(a_k)) \in R\}$$

Fact. If $R \in \mathrm{Inv}(F_B)$ then $\psi^{-1}(R) \in \mathrm{Inv}(F_A)$.

Take $\Gamma' = \{\psi^{-1}(R) \mid R \in \Gamma\}$.

The reduction from CSP(Γ) to CSP(Γ') is straightforward: an instance $\bigwedge R_i(\overline{s}_i)$ is transformed into $\bigwedge \psi^{-1}(R_i)(\overline{s}_i)$.

Proof: Finite Direct Powers

Let $\mathbf{B} = \mathbf{A}^k$.

Let R be an m-ary relation on D^k. Form an km-ary relation R' on D as follows: if $((a_{11}, \ldots, a_{1k}), \ldots, (a_{m1}, \ldots, a_{mk})) \in R$ then $(a_{11}, \ldots, a_{1k}, \ldots, a_{m1}, \ldots, a_{mk}) \in R'$.

Take $\Gamma' = \{R' \mid R \in \Gamma\}$. We have $\Gamma' \subseteq \text{Inv}(F_A)$.

Take instance $\bigwedge R_i(x_1, \ldots, x_{n_i})$ of CSP(Γ). For every variable x_i in it, introduce new variables $x_i^1, \ldots, x_i^k$.

Transform the instance into an equivalent instance

$$\bigwedge R_i'(x_1^1, \ldots, x_1^k, \ldots, x_{n_i}^1, \ldots, x_{n_i}^k).$$

Varieties and Identities

Definition 4 *An equational class is a class of all algebras (in a given signature) satisfying a given set of identities.*

Example 1

- *Mal'tsev* $f(x, y, y) = f(y, y, x) = x$
- *Semilattice* $x \cdot x = x,\ x \cdot y = y \cdot x,\ x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- *Near-unanimity (NU)*

$$f(y, x, \ldots, x) = f(x, y, \ldots, x) = \ldots = f(x, x, \ldots, y) = x$$

Theorem 5 (Birkhoff) *Varieties = equational classes.*

Thus, identities of $\mathbf{A}$ determine the complexity of CSP($\mathbf{A}$).

Idempotent Algebras

We have shown that we only need to consider constraint languages Γ which contain all constant relations $\{a\}$.

Then all polymorphisms of Γ are idempotent, that is, they satisfy the identity $f(x, \ldots, x) = x$.

Hence, we need to classify only idempotent algebras and idempotent varieties.

NP-complete Algebras: G-sets

For a permutation group G on D, a G-set is an algebra all whose operations are of the form $f(x_1, \ldots, x_n) = g(x_i)$ for some $g \in G$ and $1 \leq i \leq n$.
If a G-set is idempotent then $g = id$ and f is a projection.

Lemma 1 *If* $\mathbf{A} = (D, F)$ *is a non-trivial idempotent* G*-set then* $\mathbf{A}$ *is* **NP***-complete.*

Proof. Assume $0, 1 \in D$. $\mathrm{Inv}(F)$ is the set of all relations on D. Hence $R = \{0, 1\}^3 \setminus \{(0, 0, 0), (1, 1, 1)\} \in \mathrm{Inv}(F)$.
Recall that $\mathrm{CSP}(\{R\})$ is the NOT-ALL-EQUAL SAT problem, it's **NP**-complete.

NP-complete Algebras and Conjecture

Theorem 6 (Bulatov, Jeavons, K, 2005)
An idempotent algebra $\mathbf{A}$ *is* $\mathbf{NP}$*-complete if* $\mathbf{var}(\mathbf{A})$ *contains a G-set.*

Proposition 1 *For an idempotent algebra* $\mathbf{A}$, $\mathbf{var}(\mathbf{A})$ *contains a G-set iff* $\mathsf{HS}(\mathbf{A})$ *contains a G-set.*

All known **NP**-complete algebras satisfy this condition.

Conjecture 1 (BJK, 2005) *(Structure of Dichotomy)*
An idempotent algebra $\mathbf{A}$ *is* $\mathbf{NP}$*-complete if* $\mathsf{HS}(\mathbf{A})$ *contains a G-set, and it is tractable otherwise.*

The Mother and The Highlights

Theorem 7 (Schaefer'78)
The dichotomy conjecture holds for $D = \{0, 1\}$.

Schaefer's description perfectly aligns with Conjecture 1.
The theorem was one of main arguments for FV conjecture.

Definition 5 *An algebra is called conservative if every subset is a subalgebra.*

Theorem 8 (Bulatov'02-06)
The Structure of Dichotomy conjecture holds

1. *for all three-element algebras, and*
2. *for all conservative algebras.*

Taylor Operations

Theorem 9 (Taylor, 1977)
For any finite idempotent algebra $\mathbf{A}$, *TFAE*

1. *The variety* $\mathrm{var}(\mathbf{A})$ *does not contain a G-set.*
2. *The algebra* $\mathbf{A}$ *has an n-ary (Taylor) term operation* f *satisfying* n *identities of the form*

$$f(x_{i1},\ldots,x_{in}) = f(y_{i1},\ldots,y_{in}), \quad i = 1,\ldots,n$$

where all $x_{ij}, y_{ij} \in \{x, y\}$ *and* $x_{ii} \neq y_{ii}$.

Ex: Mal'tsev, semilattice, NU operations are all Taylor.

NB. For idempotent algebras, no Taylor term ⇒ **NPc** and, if the conjecture is true, then Taylor term ⇒ **P**.

WNU Operations

An idempotent operation is called weak NU operation if
$f(y, x, \ldots, x) = f(x, y, \ldots, x) = \ldots = f(x, x, \ldots, y)$.

Examples: $x_1 \vee \ldots \vee x_n, \quad x_1 + \ldots + x_n + x_{n+1} (\mathrm{mod}\ n)$.

NB. Any WNU operation is a Taylor operation.

Theorem 10 (Maróti, McKenzie, 2006)
For any finite idempotent algebra $\mathbf{A}$ *with a Taylor term has an WNU term operation* f *of some arity* ≥ 2.

NB. For idempotent algebras, no WNU term ⇒ **NPc**, and, if the conjecture is true, then WNU term ⇒ **P**.

WNU: Application in Graph Theory

Recall that, for a digraph $\mathcal{H}$, $\mathcal{H}$-COLOURING = CSP($\mathcal{H}$).

Assume wlog that $\mathcal{H}$ is a core. If H is a directed cycle then CSP($\mathcal{H}$) is tractable. Why?
Same if $\mathcal{H}$ is a disjoint union of directed cycles.

Conjecture 2 (Bang-Jensen,Hell, '90)
If $\mathcal{H}$ is a core digraph without sources or sinks that is not as above then CSP($\mathcal{H}$) *is* **NP***-complete.*

Theorem 11 (Barto, Kozik, Niven' 08) *Let $\mathcal{H}$ be a core digraph without sources or sinks. If $\mathcal{H}$ has a WNU polymorphism then it is a disjoint union of directed cycles.*

Corollary 1 *Conjecture 2 holds.*

How To Prove Tractability

Currently, the two main (systematic) methods are:

- via bounded width (k-minimality or Datalog)

  More on this in tomorrow's lecture

- via small generating sets

  More on this now

An Algorithm to Solve CSP($\mathbf{A}$)

Take a CSP instance $\{(\overline{s}_1, R_1), \ldots, (\overline{s}_q, R_q)\}$ of a problem in CSP($\mathbf{A}$), over a set of variables $V = \{x_1, \ldots, x_n\}$.

For a constraint $(\overline{s}_i, R_i)$, consider the following subalgebra $\mathbf{A}_i$ of $\mathbf{A}^V$: $\{\overline{a} \in D^V \mid \mathrm{pr}_{\overline{s}_i} \overline{a} \in R_i\}$.

Let $\mathbf{A}'_0 = \mathbf{A}^n$ and $\mathbf{A}'_r = \bigcap_{i=1}^r \mathbf{A}_i = \mathbf{A}'_{r-1} \cap \mathbf{A}_r$ for $r > 0$.

The solutions to the instance = the elements in $\mathbf{A}'_q$.

Assume that we know a way to represent subpowers of $\mathbf{A}$, a way to recognise $Rep(\emptyset)$, and an algorithm $\mathfrak{A}$ that takes $Rep(\mathbf{A}'_{r-1})$ and $C_r = (\overline{s}_i, R_i)$ and computes $Rep(\mathbf{A}'_r)$.

This algorithm solves any problem in CSP($\mathbf{A}$) !

Small generating sets

For $\mathfrak{A}$ to be polynomial, *Rep* must be "compact".

One way to represent a subpower is by a generating set.

For each n, let $g_{\mathbf{A}}(n)$ denote the smallest k such that each subalgebra of $\mathbf{A}^n$ has a generating set of size $\leq k$.

Assume $g_{\mathbf{A}}(n)$ is bounded by a polynomial function.
Can $\mathfrak{A}$ be made polynomial then?

Theorem 12 (Idziak,Marković,McKenzie,Valeriote,Willard)
Yes.

Details follow an algorithm that was first used by Dalmau for Mal'tsev algebras and then for GMM, a common generalisation of Mal'tsev and NU.

Few Subpowers

An algebra **A** is said to have few subpowers if the function $s_{\mathbf{A}}(n) = \log_2 |\{\mathbf{B} : \mathbf{B} \leq \mathbf{A}^n\}| \leq p(n)$ for some polynomial p.

Examples: NU algebras (Baker-Pixley'74), Mal'tsev alg's.

Non-Examples: semilattices.

Theorem 13 (Berman+IMMVW'07)
For any algebra $\mathbf{A}$*, the functions* $s_{\mathbf{A}}(n)$ *and* $g_{\mathbf{A}}(n)$ *are*

- *either both bounded by a polynomial from above,*
- *or both bounded by an exponential function from below.*

In particular, few subpowers $\Leftrightarrow$ small generating sets.

Few Subpowers: A Mal'tsev condition

Theorem 14 (Berman+IMMVW'07) *A finite algebra has few subpowers iff it has a k-edge term for some $k > 1$.*

A k-edge operation is a $(k+1)$-ary operation satisfying

$$
\begin{aligned}
t(x,x,y,y,y,\ldots,y,y) &= y \\
t(x,y,x,y,y,\ldots,y,y) &= y \\
t(y,y,y,x,y,\ldots,y,y) &= y \\
t(y,y,y,y,x,\ldots,y,y) &= y \\
&\vdots \\
t(y,y,y,y,y,\ldots,y,x) &= y
\end{aligned}
$$

NB. 2-edge = Mal'tsev.