Algebraic theory of promise constraint satisfaction problems

Libor Barto

Department of Algebra, Charles University, Prague

PGL 2019, Praha, 10 May :

CoCoSym: Symmetry in Computational Complexity

This project has received funding from the European Research Council (ERC) under the European Unions Horizon 2020 research and innovation programme (grant agreement No 771005)

Constraint Satisfaction Problems (CSPs) over finite template

- class of computational problems
- goal: determine the computational complexity
- 3 step development of algebraic theory
- goal scored (two complexity classes: P, NP-complete)

Promise Constraint Satisfaction Problems (PCSPs)

- larger class of computational problems, goal not scored
- richer on both algorithmic and hardness side
  - algorithms need to be infinitary
  - hardness requires heavy tools
- algebraic theory for CSP generalizes
- 4th step: 2 Logical computational tasks are equivalent

(Barto), Bulín, Krokhin, Opršal: Algebraic approach to promise constraint satisfaction

General problem: Given a structure $\mathfrak{A}$ and 1st order sentence ϕ (the same language), decide whether $\mathfrak{A}$ satisfies ϕ.

CSP

- fix a finite relational structure
- restrict to primitive positive (pp-) sentences:
  $(\exists x_1 \exists x_2 \dots)\ R(x_1, x_3) \wedge S(x_5, x_2) \wedge R(x_3, x_3) \wedge \dots$

Another problem: Given a structure $\mathfrak{A}$ and 1st order sentence ϕ (different language), decide whether symbols in ϕ can be interpreted in $\mathfrak{A}$ so that $\mathfrak{A}$ satisfies ϕ.

Our case: solving functional equations over an algebra

- fix a finite algebraic structure
- restrict to universally quantified conjunction of equations
  $(\forall x_1 \forall x_2 \dots)(f(x_1, x_2) = f(x_2, x_1)) \wedge (g(x_3) = f(x_3, x_3)) \wedge \dots$

CSP

Fix $\mathbb{A} = (A; R, S, \dots)$ relational structure

Definition ($\mathrm{CSP}(\mathbb{A})$)

Input: pp-sentence ϕ, eg. $(\exists x_1 \exists x_2 \dots) R(x_1, x_3) \wedge S(x_5, x_2) \wedge \dots$
Answer Yes: ϕ satisfied in $\mathbb{A}$
Answer No: ϕ not satisfied in $\mathbb{A}$

Search version: Find a satisfying assignment.
Search looks harder, but it's not [Bulatov, Jeavons, Krokhin'05]

$\mathbb{K}_3 = (A; R)$ where

- $A = \{\textit{lilac}, \textit{mauve}, \textit{cyclamen}\}$
- $R =$ (binary) inequality relation on A

Input of $\mathrm{CSP}(\mathbb{K}_3)$ is, e.g.

$(\exists x_1 \exists x_2 \dots \exists x_4) R(x_1, x_2) \wedge R(x_1, x_3) \wedge R(x_1, x_4) \wedge R(x_2, x_3) \wedge R(x_2, x_4)$

Viewpoint

- variables = vertices
- clauses (constraints) = edges

$\mathrm{CSP}(\mathbb{K}_3)$ is the 3-coloring problem for graphs

Fact: It is NP-hard (7-coloring NP-hard, 2-coloring in P)

- $\mathbb{NAE}_2 = (\{0,1\}; \mathit{NAE}_2)$ where
  $\mathit{NAE}_2 =$ all but $\{(0,0,0),(1,1,1)\}$

  $\mathrm{CSP}(\mathbb{NAE}_2) =$ positive not-all-equal 3-SAT
  $=$ 2-coloring problem for 3-uniform hypergraphs

- $\mathbb{NAE}_4 = (\{0,1,2,3\}; \mathit{NAE}_4)$, where NAE_4 still ternary

  $\mathrm{CSP}(\mathbb{NAE}_4) =$ 4-coloring problem for 3-uniform hypergraphs

- $\mathbb{ONETHREE} = (\{0,1\}; 1\mathit{in}3)$ where
  $1\mathit{in}3 = \{(0,0,1),(0,1,0),(1,0,0)\}$

  $\mathrm{CSP}(\mathbb{ONETHREE}) =$ positive 1-in-3 SAT

Fact: All NP-hard

$\mathbb{EQ}_5 = (\mathbb{Z}_5; L_{0000}, L_{0001}, \ldots, L_{4444})$ where e.g.

$L_{1234} = \{(x, y, z) : \mathbb{Z}_5^3 : 1x + 2y + 3z = 4\}$

(note: relations are affine subspaces of $\mathbb{Z}_5^3$)

$\mathrm{CSP}(\mathbb{EQ}_5)$ = solving systems of linear equations in $\mathbb{Z}_5$

Fact: In P

polymorphism of $\mathbb{A}$: mapping $f : A^n \to A$
compatible with every relation

compatible with R: f applied component-wise to tuples in R
is a tuple in R

Example: $f(x_1, \ldots, x_4) = 2x_1 + 3x_2 + 3x_3 + 3x_4 \quad f : \mathbb{Z}_5^4 \to \mathbb{Z}_5$
is compatible with each L_{abcd}
because $f(\mathbf{v}_1, \ldots, \mathbf{v}_4)$ is an affine combination of these vectors (as $2 + 3 + 3 + 3 = 1$)
and L_{abcd} is an affine subspace

$\mathrm{Pol}(\mathbb{A})$: the set of all polymorphisms (it is a "clone")
$=$ set of (multivariable) symmetries of $\mathbb{A}$

Jeavons'98: On the algebraic structure of combinatorial problems

Theorem

Complexity of $\mathrm{CSP}(\mathbb{A})$ *is determined by* Pol$(\mathbb{A})$*:*

If Pol$(\mathbb{A}) \subseteq$ Pol$(\mathbb{B})$ *then* $\mathrm{CSP}(\mathbb{B})$ *is not harder than* $\mathrm{CSP}(\mathbb{A})$*.*

Proof.

If Pol$(\mathbb{A}) \subseteq$ Pol$(\mathbb{B})$, then relations in $\mathbb{B}$ can be defined from relations in $\mathbb{A}$ by a pp-formula.

[Geiger'69, Bondarčuk, Kalužnin, Kotov, Romov'60]

This gives a computational reduction of $\mathrm{CSP}(\mathbb{B})$ to $\mathrm{CSP}(\mathbb{A})$. $\square$

So: $\mathrm{CSP}(\mathbb{EQ}_5)$ is in P because $\mathbb{EQ}_5$ has a lot of polymorphisms

System of functional equations is, e.g.

$$f(g(x,y),z) = g(x,h(y,z))$$
$$m(y,x,x) = m(y,y,y)$$
$$m(x,x,y) = m(y,y,y)$$

Solvable in $\mathcal{M}$, where $\mathcal{M}$ is a set of functions:
symbols can be interpreted in $\mathcal{M}$ so that
each equality is (universally) satisfied

Example: The above system is solvable in $\mathrm{Pol}(\mathbb{EQ}_5)$:

- take $f(x,y) = g(x,y) = h(x,y) = x$
  (note: projections are always polymoprhisms)
- take $m(x,y,z) = x - y + z$

Bulatov, Jeavons, Krokhin'05: Classifying the complexity of constraints using finite algebras $+$ Bodirsky'08: PhD thesis

Theorem

Complexity of $\mathrm{CSP}(\mathbb{A})$ *is determined by*
systems of functional equations solvable in $\mathrm{Pol}(\mathbb{A})$*:*

If each system solvable in $\mathrm{Pol}(\mathbb{A})$ *is solvable in* $\mathrm{Pol}(\mathbb{B})$*,*
then $\mathrm{CSP}(\mathbb{B})$ *is not harder than* $\mathrm{CSP}(\mathbb{A})$*.*

Proof.

Previous theorem, pp-definitions $\to$ pp-interpretations,
the HSP theorem [Birkhoff'35] $\square$

So: $\mathrm{CSP}(\mathbb{EQ}_5)$ is in P because
$\mathrm{Pol}(\mathbb{EQ}_5)$ solves strong systems of functional equations.

Barto, Opršal, Pinsker'18: The wonderland of reflections

minor condition = system of functional equations, each of the form
symbol(*variables*) = *symbol*(*variables*),
e.g. $m(y,x,x) = m(y,y,y)$, $m(x,x,y) = m(y,y,y)$

Theorem

Complexity of $\mathrm{CSP}(\mathbb{A})$ *determined by*
minor conditions solvable in $\mathrm{Pol}(\mathbb{A})$*:*

If each minor condition solvable in $\mathrm{Pol}(\mathbb{A})$ *is solvable in* $\mathrm{Pol}(\mathbb{B})$*,*
then $\mathrm{CSP}(\mathbb{B})$ *is not harder than* $\mathrm{CSP}(\mathbb{A})$*.*

Proof.

pp-interpretation $\rightarrow$ pp-construction,
version of the HSP theorem. $\square$

Minor condition is trivial:
solvable in every Pol($\mathbb{A}$)
= solvable using projections

Corollary

If Pol($\mathbb{A}$) *solves only trivial minor conditions,*
then $\mathrm{CSP}(\mathbb{A})$ *is NP-hard.*

Theorem ([Bulatov'19], [Zhuk'19])

If Pol($\mathbb{A}$) *solves some non-trivial minor condition,*
then $\mathrm{CSP}(\mathbb{A})$ *is in P.*

PCSP

Fix 2 relational structures in the same language

- $\mathbb{A} = (A; R^{\mathbb{A}}, S^{\mathbb{A}}, \dots)$
- $\mathbb{B} = (B; R^{\mathbb{B}}, S^{\mathbb{B}}, \dots)$
- there is a homomorphism $\mathbb{A} \to \mathbb{B}$

Definition ($\mathrm{PCSP}(\mathbb{A}, \mathbb{B})$)

Input: pp-sentence ϕ, eg. $(\exists x_1 \exists x_2 \dots) R(x_1, x_3) \wedge S(x_5, x_2) \wedge \dots$
Answer Yes: ϕ satisfied in $\mathbb{A}$
Answer No: ϕ not satisfied in $\mathbb{B}$

Search version: Find a $\mathbb{B}$-satisfying assignment
given a $\mathbb{A}$-satisfiable input.
(it may be a harder problem, we don't know)

Recall: $\mathbb{K}_n = (\{1, 2, \ldots, n\}; \text{inequality})$

$\mathrm{PCSP}(\mathbb{K}_3, \mathbb{K}_4)$

Input: a graph
Answer Yes: it is 3-colorable
Answer No: it is not 4-colorable

Search version: Find a 4-coloring of a 3-colorable graph

Fun facts:

- **Theorem:** it is NP-hard [Brakensiek, Guruswami'16]
  (more generally $\mathrm{PCSP}(\mathbb{K}_n, \mathbb{K}_{2n-2})$ is NP-hard)
- 6-coloring 3-colorable graph: complexity not known
- **Conjecture**: k-coloring, l-colorable graph always NP-hard
  ($k \geq l \geq 3$)

Recall: $\mathbb{NAE}_k$ ternary not-all-equal relation on a k-element set

$\mathrm{PCSP}(\mathbb{NAE}_2, \mathbb{NAE}_{137})$

Input: a 3-uniform hypergraph
Answer Yes: it is 2-colorable
Answer No: it is not 137-colorable

Theorem: It is NP-hard [Dinur,Regev,Smyth'05]
(more generally $\mathrm{PCSP}(\mathbb{NAE}_l, \mathbb{NAE}_k)$ NP-hard for $k \geq l \geq 2$)

Proof uses the PCP theorem and
Lovász's thoerem on Kneser's graphs

Recall: $\mathbb{ONETHREE} = (\{0,1\}; \{(1,0,0),(0,1,0),(0,0,1)\})$

$\mathrm{PCSP}(\mathbb{ONETHREE}, \mathbb{NAE}_2)$

Input: a 3-uniform hypergraph

Answer Yes: there is a 2-coloring such that exactly one vertex in each hyperedge receives 1

Answer No: it is not 2-colorable

Fact: It is in P. Algorithm for finding a 2-coloring of a Yes input:

- for each hyperedge $\{x, y, z\}$ write $x + y + z = 1$
- solve the system over $\mathbb{Q} \setminus \{\frac{1}{3}\}$ (it is solvable in $\{0,1\}$)
- assign $x \mapsto 1$ iff $x > 1/3$

Note: algorithm uses infinite domain CSP

Theorem: infinity is necessary [Barto'19]

polymorphism of $(\mathbb{A}, \mathbb{B})$: mapping $f : A^n \to B$
compatible with every relation-pair

compatible with $(R^{\mathbb{A}}, R^{\mathbb{B}})$: f applied to tuples in $R^{\mathbb{A}}$
is a tuple in $R^{\mathbb{B}}$

Example: $f(x_1, \ldots, x_{97}) = 1$ iff $\frac{\sum x_i}{97} > \frac{1}{3}$ $\quad f : \{0,1\}^{97} \to \{0,1\}$
is compatible with $(1in3, NAE_2)$

$\mathrm{Pol}(\mathbb{A}, \mathbb{B})$: the set of all polymorphisms (it is a "minion")
$=$ set of (multivariable) symmetries of $(\mathbb{A}, \mathbb{B})$

1st step (polymorphisms):
can be generalized [Brakensiek, Guruswami'18]
using [Pippenger'02]

2nd step (systems of functional equations):
makes no sense
since polymorphisms can no longer be composed

3nd step (minor conditions):
can be generalized [Bulín, Opršal, Krokhin'19]
alternative proof (the 4th step)
interesting for several reasons, e.g.
- direct and simple, without Pippenger or Birhoff
- gives a link to the PCP theory

Theorem ([Bulín, Opršal, Krokhin'19])

Let $\mathcal{M} = \mathsf{Pol}(\mathbb{A}, \mathbb{B})$.
The following computational problems are equivalent.

(i) $\mathrm{PCSP}(\mathbb{A}, \mathbb{B})$.

(ii) *Given a minor condition, answer Yes if it's trivial, and answer No if it's not solvable in* $\mathcal{M}$

Consequence: Complexity of $\mathrm{PCSP}(\mathbb{A}, \mathbb{B})$ determined by minor conditions solvable in $\mathsf{Pol}(\mathbb{A}, \mathbb{B})$.

Consequence: $\mathrm{PCSP}(\mathbb{K}_3, \mathbb{K}_5)$ is NP-hard
(more generally $\mathrm{PCSP}(\mathbb{K}_n, \mathbb{K}_{2n-1})$)
Proof uses the above theorem,
hardness of hypergraph coloring,
and little extra work

Proof 1: Reduction from PCSP

Given input of $\mathrm{PCSP}(\mathbb{ONETHREE}, \mathbb{NAE}_2)$, eg.

$$(\exists a, b, c, d)\ R(c, a, b) \wedge R(a, d, c)$$

transform it to a minor condition, eg.

$$\begin{aligned} f_1(x_1, x_0, x_0) &= g_c(x_0, x_1) \\ f_1(x_0, x_1, x_0) &= g_a(x_0, x_1) \\ f_1(x_0, x_0, x_1) &= g_b(x_0, x_1) \end{aligned}$$

$$\begin{aligned} f_2(x_1, x_0, x_0) &= g_a(x_0, x_1) \\ f_2(x_0, x_1, x_0) &= g_d(x_0, x_1) \\ f_2(x_0, x_0, x_1) &= g_c(x_0, x_1) \end{aligned}$$

"Yes input $\to$ Yes input": easy
"No input $\to$ No input": for contrapositive use $y \mapsto g_y(0, 1)$.

Given a minor condition

we *formulate* it as an instance of $\mathrm{PCSP}(\mathbb{A}, \mathbb{B})$

This is abstract nonsense:

- look at functions as tuples (their tables)
- then "f is a polymorphism" *is* a pp-sentence
- equations are coded by merging variables

PCSP is cool and fun because

- complexity still determined by symmetry
- proving membership in P requires more algorithms
  than in CSP
- proving hardness seems to require interesting math
  (that did not show up in CSP):
  PCP theory, algebraic topology

Thank you!