Promises Make Finite (Constraint Satisfaction) Problems Infinitary

Libor Barto

Department of Algebra, Charles University, Prague

LICS, Vancouver, 26 June 2019

European Research Council
Established by the European Commission

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)

Theorem

Efficiently solving
a specific computational problem over a two-element domain
requires an algorithm over an infinite domain.

Outline

- What problem?
- What "require" means?
- How to prove the theorem?
- What next?

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

$\mathbb{X} \to \mathbb{A}$ means that there exists a homomorphism from $\mathbb{X}$ to $\mathbb{A}$

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

Input: finite $\mathbb{X}$ of the same signature as $\mathbb{A}$
Answer Yes: $\mathbb{X} \to \mathbb{A}$
Answer No: $\mathbb{X} \not\to \mathbb{A}$

Search version: Find a homomorphism $\mathbb{X} \to \mathbb{A}$
Search looks harder, but it's not [Bulatov, Jeavons, Krokhin'05]

Fact: For finite $\mathbb{A}$, $\mathrm{CSP}(\mathbb{A})$ is always in NP.

- $\mathbb{K}_3 = (\{1,2,3\}; N)$, $N = \{1,2,3\}^2 \setminus \{(1,1),(2,2),(3,3)\}$
  $\mathrm{CSP}(\mathbb{K}_3)$ is the 3-coloring problem for graphs
- for a suitable $\mathbb{A}$, $\mathrm{CSP}(\mathbb{A})$ is the problem of solving systems of linear equations over a fixed field
- for a suitable $\mathbb{A}$, $\mathrm{CSP}(\mathbb{A})$ is 3-SAT
- $1\mathbb{IN}3 = (\{0,1\}, 1in3)$, $1in3 = \{(0,0,1),(0,1,0),(1,0,0)\}$
  $\mathrm{CSP}(1\mathbb{IN}3)$ is the positive 1-in-3-SAT
- $\mathbb{NAE} = (\{0,1\}, NAE)$, $NAE = \{0,1\}^3 \setminus \{(0,0,0),(1,1,1)\}$
  $\mathrm{CSP}(\mathbb{NAE})$ is the positive NAE-3-SAT
  $=$ 2-coloring problem for 3-uniform hypergraphs

$\mathrm{CSP}(\mathbb{A})$ is often NP-complete. What can we do?

1. **Approximation**: satisfy only some fraction of the constraints, eg.
   - for a satisfiable 3SAT instance,
     find an assignment satisfying at least 90% of the clauses
     (NP-complete [Håstad'01])
2. **Promise CSP**: satisfy a relaxed version of all constraints, eg.
   - for a 3-colorable graph,
     find a 37-coloring (conjecture: NP-c)
   - for a yes input of $\mathrm{CSP}(1\mathbb{IN}3)$,
     find a valid NAE-3-SAT assignment (in P!)

Fix two relational structures $\mathbb{A}, \mathbb{B}$ such that $\mathbb{A} \to \mathbb{B}$

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

Input: finite $\mathbb{X}$ of the same signature as $\mathbb{A}$ (and $\mathbb{B}$)
Answer Yes: $\mathbb{X} \to \mathbb{A}$
Answer No: $\mathbb{X} \not\to \mathbb{B}$

Search version: Find some $\mathbb{X} \to \mathbb{B}$
given $\mathbb{X}$ such that $\mathbb{X} \to \mathbb{A}$.
(it may be a harder problem, we don't know)

Example: $\mathrm{PCSP}(\mathbb{K}_3, \mathbb{K}_4) =$ 4-coloring a 3-colorable graph

CSP – complexity

- over two-element structures [Schaefer'78]
- over undirected graphs [Hell, Nešetřil'90]
- over finite structures [Bulatov'17], [Zhuk'17]

PCSP – complexity

- wide open for two-element structures, undirected graphs
- harder hardness proofs, use PCP theory, topology; known eg.
  - 137-coloring a 2-colorable 3-uniform hypergraph [Dinur,Regev,Smyth'05]
  - 4-coloring a 3-colorable graph [Brakensiek, Guruswami'16]
  - 5-coloring a 3-colorable graph [Bulín, Krokhin, Opršal'19]
  - $\mathrm{PCSP}(\mathbb{C}_{137}, \mathbb{K}_3)$ [Krokhin,Opršal]
- algorithmically richer – uses eg.
  systems of equations over $\mathbb{Z}$, linear programming

Recall:

- $1\mathbb{IN}3 = (\{0,1\}; \{(1,0,0),(0,1,0),(0,0,1)\})$
- $\mathbb{NAE} = (\{0,1\}; \{0,1\}^3 \setminus \{(0,0,0),(1,1,1)\})$

$\mathrm{PCSP}(1\mathbb{IN}3, \mathbb{NAE})$

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 [Brakensiek,Guruswami'18]

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 $x > 1/3$

Observation: If $\mathbb{A} \to \mathbb{C} \to \mathbb{B}$,
then $\mathrm{PCSP}(\mathbb{A}, \mathbb{B})$ reduces to $\mathrm{CSP}(\mathbb{C})$

For $\mathrm{PCSP}(1\mathbb{IN}3, \mathbb{NAE})$

- take $\mathbb{C} = (\mathbb{Q} \setminus \{1/3\}; R)$, $R = \{(x, y, z) : x + y + z = 1\}$
- $1\mathbb{IN}3 \to \mathbb{C}$ via $x \mapsto x$
- $\mathbb{C} \to \mathbb{NAE}$ via $x \mapsto 1$ iff $x > 1/3$

Remark: One can also use e.g. $\mathbb{C} = (\mathbb{Z}; x + y + z = 1)$

Theorem

If $1\mathbb{IN}3 \to \mathbb{C} \to \mathbb{NAE}$ *and* $\mathbb{C}$ *finite, then* $\mathrm{CSP}(\mathbb{C})$ *is NP-complete.*

Polymorphism of $\mathbb{C}$ = homomorphism $\mathbb{C}^n \to \mathbb{C}$

$f : C^n \to C$ is cyclic if $\forall x_i \;\; f(x_1, x_2, \ldots, x_n) = f(x_2, \ldots, x_n, x_1)$

Theorem ([Barto,Kozik'12])

Let $\mathbb{C} = (C; \ldots)$ be finite. If, for some prime $p > |C|$, $\mathbb{C}$ has no cyclic polymorphism of arity p, then $\mathrm{CSP}(\mathbb{C})$ is NP-complete.

Background in CSPs

- complexity is P or NP-c, and is tied to "closure properties" [Feder,Vardi'93]
- complexity depends only on polymorphisms [Jeavons'98]
- borderline between P and NP-c conjectured [Bulatov,Jeavons,Krokhin'05]
- borderline characterized in many ways (such as above)
- conjecture proved [Bulatov'17],[Zhuk'17]

- Assume $f : 1\mathbb{IN}3 \to \mathbb{C}$, $g : \mathbb{C} \to \mathbb{NAE}$, $\mathbb{C}$ finite
- WLOG f is the inclusion
- Take p large enough, assume $t : \mathbb{C}^p \to \mathbb{C}$ cyclic
- Take $s(x_{11}, \ldots, x_{pp}) = t(t(x_{11}, \ldots, x_{1p}), \ldots, t(x_{p1}, \ldots, x_{pp}))$, arity $n = p^2$
- Composition $g(s(f(x_1), \ldots, f(x_n)))$ is a homo $1\mathbb{IN}3 \to \mathbb{NAE}$.
- This (+cyclicity of t) gives for "nice" $\mathbf{x} \in \{0,1\}^n$ that $g(s(\mathbf{x})) = 1$ iff $\mathrm{ham}(\mathbf{x}) > n/3$
- Take $\mathbf{a}, \mathbf{b}$ such that $t(\mathbf{a}) = t(\mathbf{b})$ and $\mathrm{ham}(\mathbf{a}) \neq \mathrm{ham}(\mathbf{b})$
- Take suitable $\mathbf{x} = (\mathbf{a}, \ldots, \mathbf{a}, \mathbf{c}, \ldots, \mathbf{c})$, $\mathbf{y} = (\mathbf{b}, \ldots, \mathbf{b}, \mathbf{c}, \ldots, \mathbf{c})$
  - $\mathrm{ham}(\mathbf{x}) > n/3$ and $\mathrm{ham}(\mathbf{x}) < n/3$
  - both evaluations are nice for s, so $s(\mathbf{x}) \neq s(\mathbf{y})$
- But $s(\mathbf{x}) = t(t(\mathbf{a}, \ldots, t(\mathbf{a}), t(\mathbf{c}), \ldots, t(\mathbf{c}))$ $= t(t(\mathbf{b}, \ldots, t(\mathbf{b}), t(\mathbf{c}), \ldots, t(\mathbf{c})) = s(\mathbf{y})$, a contradiction

The main tool was an NP-hardness criterion for CSPs via cyclic polymorphisms.

Improvements/alternatives can

- simplify the proof of the presented result
- simplify the proof of the dichotomy theorem

Question

Assume a finite $\mathbb{C}$ has a cyclic polymorphism. Does $\mathbb{C}$ necessarily have a polymorphism s such that for any $a, b \in C$ and $\mathbf{x} \in \{a, b\}^n$, the value $s(\mathbf{x})$ depends only on the number of occurrences of a in $\mathbf{x}$?

Question

Assume $\mathrm{PCSP}(\mathbb{A}, \mathbb{B})$ *is in P. Is there always an infinite* $\mathbb{C}$ *such that* $\mathbb{A} \to \mathbb{C} \to \mathbb{B}$ *and* $\mathrm{CSP}(\mathbb{C})$ *is in P?*

(Such a family suggested in [Brakensiek,Guruswami'19] for PCSPs over two-element domains.)

If not, can $\mathrm{PCSP}(\mathbb{A}, \mathbb{B})$ *be reduced to a* $\mathrm{CSP}(\mathbb{C})$ *in P in a more complicated way?*

How to construct such a $\mathbb{C}$*?*

Question

Assume $1\mathbb{IN}3 \to \mathbb{C} \to \mathbb{NAE}$ *and* $\mathrm{CSP}(\mathbb{C})$ *is in P. Can* $\mathbb{C}$ *be*

- *reduct of a finitely bounded homogeneous structure?*
- ω*-categorical?*

In this sense we can measure the "level of finiteness" for PCSPs.

Question

For some classes of PCSPs, the complexity is known.

[Brakensiek,Guruswami'18],[Ficak,Kozik,Olšák,Stankiewicz'19]

Which PCSPs in P require infinite CSPs?

Question

Assume $1\mathbb{IN}3 \to \mathbb{C} \to \mathbb{NAE}$ *and* $\mathrm{CSP}(\mathbb{C})$ *is in P. Can* $\mathbb{C}$ *be*

- *reduct of a finitely bounded homogeneous structure?*
- ω*-categorical?*

In this sense we can measure the "level of finiteness" for PCSPs.

Question

For some classes of PCSPs, the complexity is known.

[Brakensiek,Guruswami'18],[Ficak,Kozik,Olšák,Stankiewicz'19]

Which PCSPs in P require infinite CSPs?

Thank you!