

Proof Complexity of Constraint Satisfaction Problems

joint work with Albert Atserias

Joanna Ochremiak

Université Paris Diderot - Paris 7

Finite and Algorithmic Model Theory
Dagstuhl, 7th September 2017

(CSP problem)

\mathcal{P}

(proof system)

\mathcal{S}

“Succinct” proofs in \mathcal{S} of the fact that an instance of \mathcal{P} is unsatisfiable?

(CSP problem)

\mathcal{P}

2-SAT

(proof system)

\mathcal{S}

resolution

“Succinct” proofs in \mathcal{S} of the fact that an instance of \mathcal{P} is unsatisfiable?

Every unsatisfiable instance has a small refutation.

(CSP problem)

\mathcal{P}

3-SAT

(proof system)

\mathcal{S}

resolution

“Succinct” proofs in \mathcal{S} of the fact that an instance of \mathcal{P} is unsatisfiable?

There exist unsatisfiable instances that require big refutations.

(CSP problem)

\mathcal{P}

(proof system)

\mathcal{S}

“Succinct” proofs in \mathcal{S} of the fact that an instance of \mathcal{P} is unsatisfiable?

Standard CSP reductions.

Constraint Satisfaction Problems

 template

$\mathbb{B} = (B; R_1, R_2, \dots, R_n)$ - a fixed finite relational structure

Problem: $\text{CSP}(\mathbb{B})$

Input: a finite relational structure \mathbb{A}

Decide: Is there a homomorphism from \mathbb{A} to \mathbb{B} ?

Examples

$\mathbb{B} = (\{0, 1\}; R_1, R_0)$ - linear equations mod 2

$$R_1 = \{(x, y, z) \in \{0, 1\}^3 \mid x + y + z = 1 \pmod{2}\}$$

$$R_0 = \{(x, y, z) \in \{0, 1\}^3 \mid x + y + z = 0 \pmod{2}\}$$

$\mathbb{A} = (\{a, b, c\}; R_0(a, b, c), R_1(a, a, b), R_1(a, c, c))$

$$a + b + c = 0$$

$$a + a + b = 1$$

$$a + c + c = 1$$

Examples

- $\mathbb{B} = (\{0, 1, 2\}; \neq)$ - three-colorability
- $\mathbb{B} = (\{0, 1\}; R_0, R_1, R_2, R_3)$ - 3-SAT
 $R_2 = \{0, 1\}^3 \setminus \{(1, 1, 0)\}$, etc...

Propositional Proof Systems

\mathcal{C} - a set of propositional formulas

E - a propositional formula

A **proof** of E from the set \mathcal{C} is a sequence of formulas:

- from \mathcal{C} or
- obtained from previous formulas using some rules.

Resolution

\mathcal{C} - a set of clauses (disjunctions of literals, e.g. $p \vee q \vee r$)

E - a clause

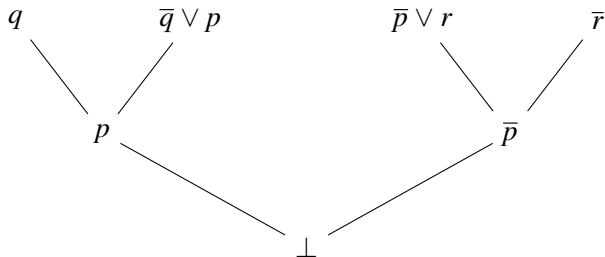
A **resolution proof** of E from the set \mathcal{C} is a sequence of clauses:

- from \mathcal{C} or
- obtained from previous formulas using the rules:

$$\frac{C \vee p \quad D \vee \bar{p}}{C \vee D} \qquad \frac{C}{C \vee p}$$

Example

$$\mathcal{C} = \{q, \bar{q} \vee p, \bar{p} \vee r, \bar{r}\}$$



refutation - ends with a contradiction (proof of unsatisfiability)

“Succinct” resolution refutations

A template \mathbb{B} admits “succinct” resolution refutations:

Take any instance \mathbb{A} of $\text{CSP}(\mathbb{B})$ such that $\mathbb{A} \not\rightarrow \mathbb{B}$.

↓

$\text{CNF}(\mathbb{A}, \mathbb{B})$ satisfiable iff $\mathbb{A} \rightarrow \mathbb{B}$ (fixed encoding)

↓

$\text{CNF}(\mathbb{A}, \mathbb{B})$ has a “succinct” resolution refutation $\ddot{\smile}$

“succinct” \rightsquigarrow only clauses with at most k variables (Ptime algorithm)

Sum-of-Squares

Positivstellensatz [Krivine'64, Stengle'74].

$q_1(\bar{x}) = 0, \dots, q_n(\bar{x}) = 0, p_1(\bar{x}) \geq 0, \dots, p_m(\bar{x}) \geq 0$ unsat. in \mathbb{R}

\Updownarrow

$\sum t_i(\bar{x})q_i(\bar{x}) + \sum s_j(\bar{x})p_j(\bar{x}) + s(\bar{x}) = -1$, where s and s_j 's are sos

Example.

$$q(x, y) = y + x^2 + 2 = 0, \quad p(x, y) = x - y^2 + 3 \geq 0$$

$$tq + s_1p + s = -1$$

$$t = -6, \quad s_1 = 2, \quad s = \frac{1}{3} + 2\left(y + \frac{3}{2}\right)^2 + 6\left(x - \frac{1}{6}\right)^2$$

“Succinct” SOS refutations

A template \mathbb{B} admits “succinct” SOS refutations:

Take any instance \mathbb{A} of $\text{CSP}(\mathbb{B})$ such that $\mathbb{A} \not\rightarrow \mathbb{B}$.

↓

$\text{INEQ}(\mathbb{A}, \mathbb{B})$ satisfiable iff $\mathbb{A} \rightarrow \mathbb{B}$ (fixed encoding)

↓

$\text{INEQ}(\mathbb{A}, \mathbb{B})$ has a “succinct” resolution refutation ☺

“succinct” \rightsquigarrow degree at most d (Ptime algorithm)

Reductions

$\mathcal{P}' \leq_{CSP} \mathcal{P}$ - “classical” reduction preserving the complexity of CSP

Theorem. If $\mathcal{P}' \leq_{CSP} \mathcal{P}$ then “succinct” refutations for \mathcal{P} imply “succinct” refutations for \mathcal{P}' .

DNF-resolution

bounded-depth Frege

Frege

Sherali-Adams

Sum-of-Squares

bounded-degree Lovász-Schrijver

Lovász-Schrijver

Reductions

$\mathcal{P}' \leq_{CSP} \mathcal{P}$ - “classical” reduction preserving the complexity of CSP

Theorem. If $\mathcal{P}' \leq_{CSP} \mathcal{P}$ then “succinct” refutations for \mathcal{P} imply “succinct” refutations for \mathcal{P}' .

DNF-resolution

bounded-depth Frege

Sherali-Adams

Sum-of-Squares

Reductions

$\mathcal{P}' \leq_{CSP} \mathcal{P}$ - “classical” reduction preserving the complexity of CSP

Theorem. If $\mathcal{P}' \leq_{CSP} \mathcal{P}$ then “succinct” refutations for \mathcal{P} imply “succinct” refutations for \mathcal{P}' .

DNF-resolution

bounded-depth Frege

Sherali-Adams

Sum-of-Squares

solvable by Datalog



bounded width



definable in LFP+C

Lower Bounds

Theorem [Chan]. Linear SOS degree lower bound for $3LIN(G)$.

Theorem [Ben-Sasson $+\epsilon$]. Exponential size lower bound for $3LIN(G)$, for bounded-depth Frege.

Reductions

$\mathcal{P}' \leq_{CSP} \mathcal{P}$ - “classical” reduction preserving the complexity of CSP

Theorem. If $\mathcal{P}' \leq_{CSP} \mathcal{P}$ then “succinct” refutations for \mathcal{P} imply “succinct” refutations for \mathcal{P}' .

DNF-resolution

bounded-depth Frege

Sherali-Adams

Sum-of-Squares

solvable by Datalog

bounded width

definable in LFP+C



Homomorphic Equivalence

\mathbb{B}, \mathbb{C} - templates

$$\begin{array}{l} h: B \rightarrow C \\ g: C \rightarrow B \end{array} \quad \text{homomorphisms}$$

\mathbb{A} maps homomorphically to \mathbb{B} iff \mathbb{A} maps homomorphically to \mathbb{C}

$$\mathbb{A} \longrightarrow \mathbb{B} \xrightarrow{h} \mathbb{C}$$

Fact: CSPs of homomorphically equivalent structures are the same.

Pp-definability

$\mathbb{B} = (B; R_1, R_2, \dots, R_n)$ - a template

R'_1, \dots, R'_m - defined using $\exists, \wedge, =$ (**pp-definition**)

$\mathbb{C} = (B; R'_1, \dots, R'_m)$ - **pp-definable** from \mathbb{B}

Fact: There is a polynomial time reduction from $\text{CSP}(\mathbb{C})$ to $\text{CSP}(\mathbb{B})$.

$\mathcal{P}' \leq_{CSP} \mathcal{P}$ - “classical” reduction preserving the complexity of CSP:

- homomorphic equivalence
- pp-interpretability
- adding constants to a core

Theorem. If $\mathcal{P}' \leq_{CSP} \mathcal{P}$ then “succinct” refutations for \mathcal{P} imply “succinct” refutations for \mathcal{P}' .

Theorem [Jeavons et al.; Barto, Opršal, Pinsker]. Class of CSP templates closed under \leq_{CSP} has an algebraic characterisation.

Theorem [Bulatov; Zhuk]. CSPs solvable in PTime are characterised by $f(y, x, y, z) = f(x, y, z, x)$.

Classes of CSPs with succinct refutations in:

DNF-resolution

bounded-depth Frege

Sherali-Adams

Lasserre/SOS

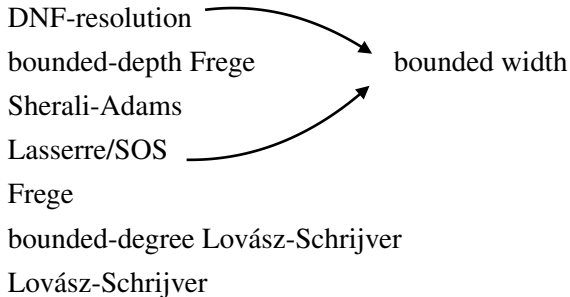
Frege

bounded-degree Lovász-Schrijver

Lovász-Schrijver

have algebraic characterisations.

Classes of CSPs with succinct refutations in:



have algebraic characterisations.

Classes of CSPs with succinct refutations in:

DNF-resolution

bounded-depth Frege $f_3(x, x, y) = f_4(x, x, x, y)$ (WNU)

Sherali-Adams [Kozik, Krokhin, Valeriotte, Willard]

Lasserre/SOS

Frege

bounded-degree Lovász-Schrijver

Lovász-Schrijver

have algebraic characterisations.

Classes of CSPs with succinct refutations in:

bounded-width resolution

DNF-resolution

bounded-depth Frege $f_3(x, x, y) = f_4(x, x, x, y)$ (WNU)

Sherali-Adams [Kozik, Krokhin, Valeriote, Willard]

Lasserre/SOS

Frege

bounded-degree Lovász-Schrijver

Lovász-Schrijver

have algebraic characterisations.

Classes of CSPs with succinct refutations in:

bounded-width resolution

DNF-resolution

bounded-depth Frege

Sherali-Adams

Lasserre/SOS

Frege

bounded-degree Lovász-Schrijver

Lovász-Schrijver

have algebraic characterisations.

Theorem [Grigoriev, Hirsch, Pasechnik; Atserias]. Unsatisfiable system of linear equations mod 2 with n variables and m equations has an LS refutation of degree 6 and size polynomial in n and m .

(CSP problem)

\mathcal{P}

(proof system)

\mathcal{S}

“Succinct” proofs in \mathcal{S} of the fact that an instance of \mathcal{P} is unsatisfiable?

Standard CSP reductions.