Proof Complexity Meets Algebra

joint work with Albert Atserias

Joanna Ochremiak

Université Paris Diderot - Paris 7

Logical Structures in Computation Reunion Workshop
Simons Institute, 13th December 2017

(CSP problem) $\mathcal{P}$

$\mathcal{S}$ (proof system)

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

(CSP problem) $\mathcal{P}$

2-SAT

$\mathcal{S}$ (proof system)

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

$\mathcal{S}$ (proof system)

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) $\mathcal{P}$

$\mathcal{S}$ (proof system)

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

(CSP problem) $\mathcal{P}$

$\mathcal{S}$ (proof system)

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

Standard CSP reductions.

Constraint Satisfaction Problems

template

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

Problem: CSP($\mathbb{B}$)
Input: a finite relational structure $\mathbb{A}$
Decide: Is there a homomorphism from $\mathbb{A}$ to $\mathbb{B}$?

Constraint Satisfaction Problems

template

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

Problem: CSP($\mathbb{B}$)
Input: a finite relational structure $\mathbb{A}$
Decide: Is there a homomorphism from $\mathbb{A}$ to $\mathbb{B}$?

$\mathbb{A} = (A; R_1^{\mathbb{A}}, R_2^{\mathbb{A}}, \ldots, R_n^{\mathbb{A}})$

$h\colon A \to B$ - homomorphism iff

$(a_1, \ldots, a_r) \in R_i^{\mathbb{A}} \;\; \Rightarrow \;\; (h(a_1), \ldots, h(a_r)) \in R_i$

Examples

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

$$R_1 = \{(x,y,z) \in \{0,1\}^3 \mid x+y+z = 1 \mod 2\}$$
$$R_0 = \{(x,y,z) \in \{0,1\}^3 \mid x+y+z = 0 \mod 2\}$$

Examples

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

$$R_1 = \{(x,y,z) \in \{0,1\}^3 \mid x+y+z = 1 \mod 2\}$$
$$R_0 = \{(x,y,z) \in \{0,1\}^3 \mid x+y+z = 0 \mod 2\}$$

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

$$a+b+c = 0$$
$$a+a+b = 1$$
$$a+c+c = 1$$

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...

Resolution

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

A resolution refutation of the set $\mathcal{C}$ is a sequence of clauses:

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

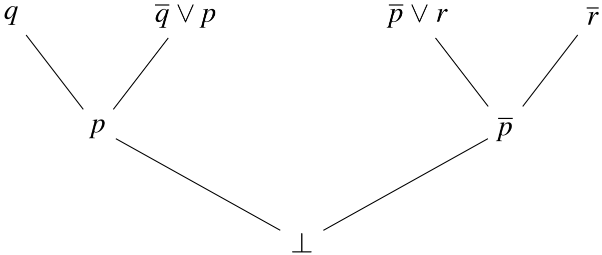
$$\frac{C \vee p \quad D \vee \overline{p}}{C \vee D}$$

negation

- finishing with a contradiction $\perp$

Example

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



“Succinct” resolution refutations

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

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

$\downarrow$

$E(\mathbb{A})$ satisfiable iff $\mathbb{A} \to \mathbb{B}$ (some fixed encoding for CSP($\mathbb{B}$))

$\downarrow$

$E(\mathbb{A})$ has a “succinct” resolution refutation ☺

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

Polynomial Calculus

$\mathcal{C} = \{q_1(\bar{x}) = 0, \ldots, q_n(\bar{x}) = 0\}$ - a system of polynomial equations

A PC refutation of $\mathcal{C}$ is a sequence of polynomial equations:

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

$$\frac{f(\bar{x}) = 0 \quad g(\bar{x}) = 0}{af(\bar{x}) + bg(\bar{x}) = 0} \qquad \frac{f(\bar{x}) = 0}{x_k f(\bar{x}) = 0}$$

- finishing with $-1 = 0$

“Succinct” PC refutations

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

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

$\downarrow$

$E(\mathbb{A})$ satisfiable iff $\mathbb{A} \to \mathbb{B}$ (some fixed encoding for CSP($\mathbb{B}$))

$\downarrow$

$E(\mathbb{A})$ has a “succinct” PC refutation :)

“succinct” $\rightsquigarrow$ degree at most d (Ptime - the Gröbner basis algorithm)

Sum-of-Squares

Positivstellensatz [Krivine'64, Stengle'74].

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

$$\Updownarrow$$

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

Sum-of-Squares

Positivstellensatz [Krivine'64, Stengle'74].

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

$$\Updownarrow$$

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

Example.

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

$$tq + s_1 p + s = -1$$

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

“Succinct” SOS refutations

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

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

$\downarrow$

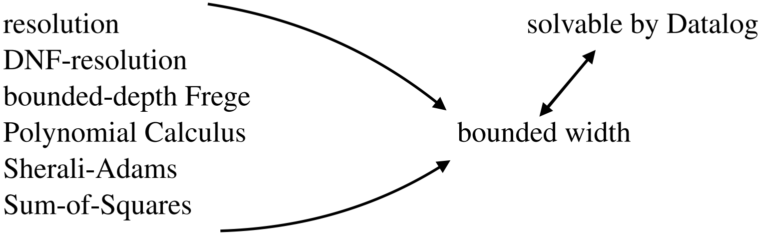
$E(\mathbb{A})$ satisfiable iff $\mathbb{A} \to \mathbb{B}$ (some fixed encoding for CSP($\mathbb{B}$))

$\downarrow$

$E(\mathbb{A})$ has a “succinct” resolution refutation :-)

“succinct” $\rightsquigarrow$ degree at most d (Ptime - Semidefinite programming)

“Succinct” refutations



Reductions

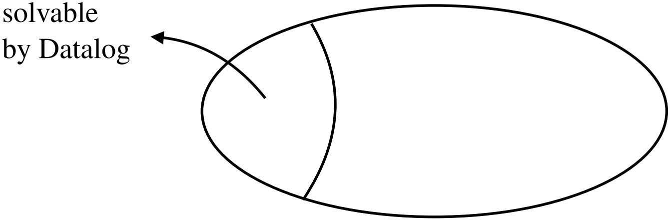
$\mathcal{P}' \leq_{CSP} \mathcal{P}$ - "classical" reduction preserving the complexity of CSP

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

Reductions

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

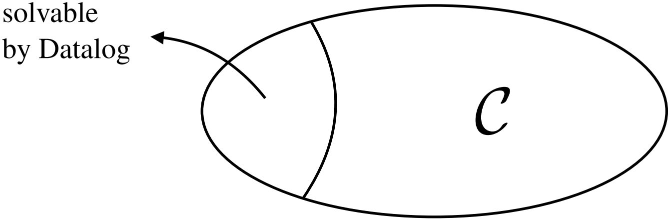
Theorem. If $\mathcal{P}' \leq_{CSP} \mathcal{P}$ then "succinct" refutations for $\mathcal{P}$ imply "succinct" refutations for $\mathcal{P}'$.



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 $\mathcal{P}'$.



Theorem [Barto, Kozik]. For every $\mathcal{P} \in \mathcal{C}$, there is a finite Abelian group G such that $3LIN(G) \leq_{CSP} \mathcal{P}$.

Lower bounds

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

Theorem [Buss, Grigoriev, Impagliazzo, Pitassi]. Linear PC degree lower bound for $3LIN(G)$.

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

“Succinct” refutations

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
Polynomial Calculus
Sherali-Adams
Sum-of-Squares

Polynomial Calculus over finite fields
Frege
bounded-degree Lovász-Schrijver
Lovász-Schrijver

“Succinct” refutations

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
Polynomial Calculus
Sherali-Adams
Sum-of-Squares

bounded width

Polynomial Calculus over finite fields
Frege
bounded-degree Lovász-Schrijver
Lovász-Schrijver

“Succinct” refutations

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
Polynomial Calculus
Sherali-Adams
Sum-of-Squares

bounded width

Polynomial Calculus over finite fields
Frege
bounded-degree Lovász-Schrijver
Lovász-Schrijver

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

Majority

identities

$m(x,x,y) = m(x,y,x) = m(y,x,x) = x$

$\mathbb{B} = (\{0,1\}; \neq) \; = \; (\{0,1\}; \{(0,1),(1,0)\})$ - two-colorability

$$\begin{array}{ccc} (0,1) & \in & \neq \\ (0,1) & \in & \neq \\ (1,0) & \in & \neq \\ \hline \end{array}$$

Majority

$m(x,x,y) = m(x,y,x) = m(y,x,x) = x$

$\mathbb{B} = (\{0,1\}; \neq) \; = \; (\{0,1\}; \{(0,1),(1,0)\})$ - two-colorability

$$\begin{array}{ccc} (0,1) & \in & \neq \\ (0,1) & \in & \neq \\ (1,0) & \in & \neq \\ \hline (0,1) & \in & \neq \end{array}$$

Majority

$m(x, x, y) = m(x, y, x) = m(y, x, x) = x$

$\mathbb{B} = (\{0, 1\}; \neq) = (\{0, 1\}; \{(0, 1), (1, 0)\})$ - two-colorability

$$\begin{array}{ccc} (0,1) & \in & \neq \\ (0,1) & \in & \neq \\ (1,0) & \in & \neq \\ \hline (0,1) & \in & \neq \end{array}$$

Fact. Every CSP whose all relations are preserved by majority is solvable in Ptime.

Algebra

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

There is a set of identities...

"$m(x,x,y) = m(x,y,x) = m(y,x,x) = x$"

such that $\mathbb{B}$ is in the class iff there are functions which:

- satisfy the identities
- preserve the relations of $\mathbb{B}$

Algebra

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

There is a set of identities...

"$m(x,x,y) = m(x,y,x) = m(y,x,x) = x$"

such that $\mathbb{B}$ is in the class iff there are functions which:

- satisfy the identities
- preserve the relations of $\mathbb{B}$

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

Algebraic characterisations

Classes of CSPs with succinct refutations in:

DNF-resolution
bounded-depth Frege
Polynomial Calculus
Sherali-Adams
Sum-of-Squares

$f_3(x,x,y) = f_4(x,x,x,y)$ (WNU)
[Kozik, Krokhin, Valeriote, Willard]

Polynomial Calculus over finite fields
Frege
bounded-degree Lovász-Schrijver
Lovász-Schrijver

have algebraic characterisations.

Beyond bounded-width

Fact. Polynomial Calculus over finite fields has succinct refutations beyond bounded-width.

Theorem. Frege, bounded-degree Lovász-Schrijver and Lovász-Schrijver have succinct refutations beyond bounded-width.

Questions

Characterise CSPs which admit succinct refutations in:

- Polynomial Calculus over finite fields
- Frege
- bounded-degree Lovász-Schrijver
- Lovász-Schrijver

(CSP problem) $\mathcal{P}$ $\mathcal{S}$ (proof system)

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

Standard CSP reductions.