Proof Complexity of Constraint Satisfaction Problems

joint work with Albert Atserias

Joanna Ochremiak

Université Paris Diderot - Paris 7

Aktuelle Themen in Logik und Datenbanktheorie,
Berlin, 3rd May 2017

Constraint Satisfaction Problem

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

$R_i \subseteq B^{r_i}$

Notation: $(x, y) \in R \;\Leftrightarrow\; R(x, y)$

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

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

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

Constraint Satisfaction Problem

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

Problem: CSP($\mathbb{B}$)
Input: a finite 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

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

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

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

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...

Homomorphic Equivalence

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

$$h\colon B \to C$$
$$g\colon C \to B$$

homomorphisms

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

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

Fact: CSPs of homomorphically equivalent structures are the same.

Pp-definability

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

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

$R(x,y) \Leftrightarrow \exists z\, R_0(z,z,z) \wedge R_0(x,y,z)$ - pp-definition

$$R = \{(x,y) \in \{0,1\}^2 \mid x+y = 0 \mod 2\}$$

$\mathbb{C} = (\{0,1\}; R_1, R_0, R)$ - pp-definable in $\mathbb{B}$

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

$\mathbb{A} = (\{a,b\}; R(a,b)\} \quad \rightsquigarrow \quad \mathbb{A}' = (\{a,b,\mathbf{c}\}; R_0(c,c,c), R_0(a,b,c)\}$

Formulas

Formulas: $(x \wedge \bar{y}) \vee z$ (negation normal form)

3-term: $x \wedge \bar{y} \wedge z$ (literals can repeat)

3-clause: $x \vee \bar{y} \vee z$ (literals can repeat)

k-DNF: disjunction of k-terms $(\Sigma_{1,k})$

k-CNF: conjunction of k-clauses $(\Pi_{1,k})$

$\Sigma_{t,k}$: disjunctions of formulas from $\Pi_{t-1,k}$

$\Pi_{t,k}$: conjunctions of formulas from $\Sigma_{t-1,k}$

Σ_t: sum of all $\Sigma_{t,k}$ (depth t)

Frege Proof System

Rules of Frege: axiom, cut, introduction of conjunction, weakening

$$\frac{}{A \vee \overline{A}} \qquad \frac{C \vee A \quad D \vee \overline{A}}{C \vee D} \qquad \frac{C \vee A \quad D \vee B}{C \vee D \vee (A \wedge B)} \qquad \frac{C}{C \vee A}$$

A proof of A from a set of formulas $\mathcal{C}$ - a sequence of formulas:

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

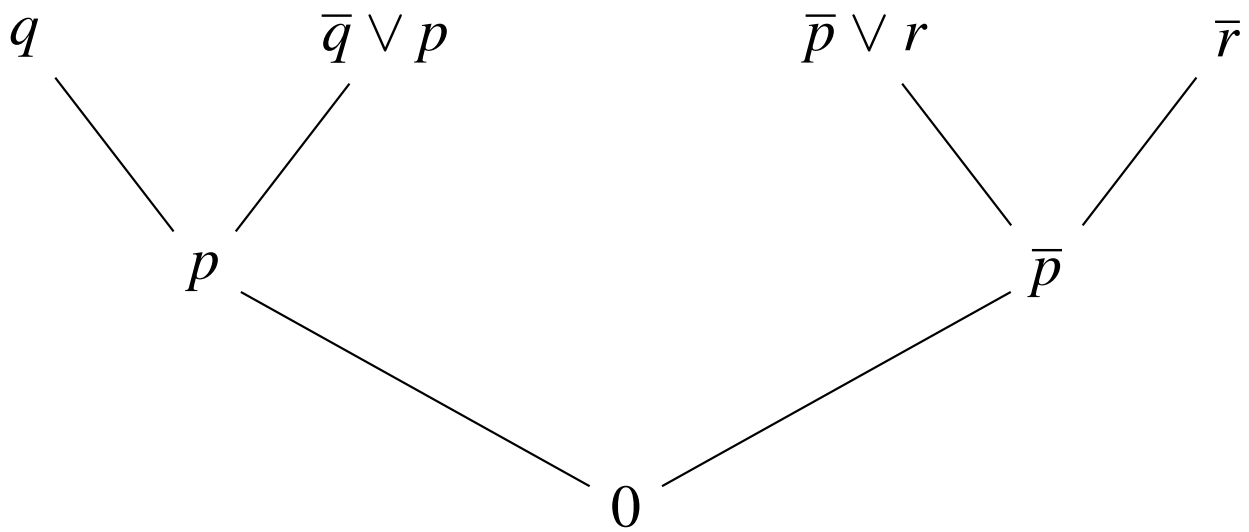
Fact. Frege is sound and implicationally complete.

Frege refutation - ends with an empty formula

size of a proof - number of symbols

Example Refutation

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



Proof Complexity of CSPs

CSP template $\mathbb{B}$

- Size of Frege proof that an instance $\mathbb{A}$ is unsatisfiable? Polynomial? Exponential?
- Size of Frege proofs using only formulas of depth d?
- Using only k-clauses? Possible?

$\mathbb{C}$ pp-definable/homomorphically equivalent to $\mathbb{B}$

- "Small" proofs for $\mathbb{B}$ imply "small" proofs for $\mathbb{C}$?

Encoding

$\mathbb{C} = (\{0,1\}; R_1, R_0, R)$

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

$\mathbb{A} = (\{a,b\}; R(a,b)\}$

CNF$(\mathbb{A}, \mathbb{C})$:

- $X(a,0) \vee X(a,1)$ $\quad X(b,0) \vee X(b,1)$
- $\overline{X(a,0)} \vee \overline{X(a,1)}$ $\quad \overline{X(b,0)} \vee \overline{X(b,1)}$
- $\overline{X(a,0)} \vee \overline{X(b,1)}$ $\quad \overline{X(a,1)} \vee \overline{X(b,0)}$

CNF$(\mathbb{A}, \mathbb{C})$ is satisfiable $\Leftrightarrow$ there is a homomorphism from $\mathbb{A}$ to $\mathbb{C}$

Encoding

$\mathbb{C} = (\{0,1\}; R_1, R_0, R)$

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

$\mathbb{A} = (\{a,b\}; R(a,b))$

CNF$(\mathbb{A}, \mathbb{C})$:

- $X(a,0) \vee X(a,1)$ $X(b,0) \vee X(b,1)$ $|C|$-clauses
- $\overline{X(a,0)} \vee \overline{X(a,1)}$ $\overline{X(b,0)} \vee \overline{X(b,1)}$ 2-clauses
- $\overline{X(a,0)} \vee \overline{X(b,1)}$ $\overline{X(a,1)} \vee \overline{X(b,0)}$ maxar$(\mathbb{C})$-clauses

CNF$(\mathbb{A}, \mathbb{C})$ is satisfiable $\Leftrightarrow$ there is a homomorphism from $\mathbb{A}$ to $\mathbb{C}$

Closure Under Reductions

Fix: $\mathbb{C}$ pp-definable in $\mathbb{B}$

Polynomial-time computable transformation maps instances $\mathbb{A}$ of $\mathrm{CSP}(\mathbb{C})$ to instances $\mathbb{A}'$ of $\mathrm{CSP}(\mathbb{B})$:

- $\mathbb{A}'$ is satisfiable $\Leftrightarrow$ $\mathbb{A}$ is satisfiable
- size of $\mathbb{A}'$ is linear in the size of $\mathbb{A}$

Theorem

Frege refutation of $\mathrm{CNF}(\mathbb{A}', \mathbb{B})$ *of size s using formulas from* $\Sigma_{t,k}$

$$\Downarrow$$

Frege refutation of $\mathrm{CNF}(\mathbb{A}, \mathbb{C})$ *of size polynomial in the size of* $\mathbb{A}'$ *and s using formulas from* $\Sigma_{t,l}$ *where l is polynomial in k*

Closure Under Reductions

Fix: $\mathbb{C}$ pp-definable in $\mathbb{B}$

Polynomial-time computable transformation maps instances $\mathbb{A}$ of CSP($\mathbb{C}$) to instances $\mathbb{A}'$ of CSP($\mathbb{B}$):

- $\mathbb{A}'$ is satisfiable $\Leftrightarrow$ $\mathbb{A}$ is satisfiable
- size of $\mathbb{A}'$ is linear in the size of $\mathbb{A}$

Corollary

Frege refutation of CNF($\mathbb{A}', \mathbb{B}$) *of size s using k-DNFs*

$\Downarrow$

Frege refutation of CNF($\mathbb{A}, \mathbb{C}$) *of size polynomial in the size of* $\mathbb{A}'$ *and s using l-DNFs where l is polynomial in k*

Example

$\mathbb{C} = (\{0,1\}; R_1, R_0, R) \quad \mathbb{B} = (\{0,1\}; R_1, R_0)$

$R(x,y) \Leftrightarrow \exists z\, R_0(z,z,z) \wedge R_0(x,y,z)$

$\mathbb{A} = (\{a,b\}; R(a,b)\} \quad \rightsquigarrow \quad \mathbb{A}' = (\{a,b,\mathbf{c}\}; R_0(c,c,c), R_0(a,b,c)\}$

$\Sigma_{t,k}$-Frege refutation of CNF$(\mathbb{A}', \mathbb{B})$ of size s

Substitution:

$$X(c,0) := (X(a,0) \wedge X(b,0)) \vee (X(a,1) \wedge X(b,1))$$
$$X(c,1) := 0$$

Lemma. Each formula from CNF$(\mathbb{A}', \mathbb{B})$ after substitution is a logical consequence of a bounded number of formulas from CNF$(\mathbb{A}, \mathbb{C})$.

Proof Complexity of CSPs

CSP template $\mathbb{B}$

- Size of Frege proof that an instance $\mathbb{A}$ is unsatisfiable? Polynomial? Exponential?
- Size of Frege proofs using only formulas of depth d?
- Using only k-clauses? Possible?

$\mathbb{C}$ pp-definable/homomorphically equivalent to $\mathbb{B}$

- "Small" proofs for $\mathbb{B}$ imply "small" proofs for $\mathbb{C}$?

Bounded-width

$\mathbb{B}$ has bounded width iff CSP($\mathbb{B}$) is solvable by local consistency

Lemma. If $\mathbb{B}$ has bounded width then CSP($\mathbb{B}$) has Frege refutations using only k-clauses.

- Polynomial size refutations.
- Polynomial time algorithm.

Theorem. Otherwise CSP($\mathbb{B}$) does not have Frege refutations of bounded depth and subexponential size.

Bounded-width

$\mathbb{B}$ has bounded width iff CSP($\mathbb{B}$) is solvable by local consistency

Lemma. If $\mathbb{B}$ has bounded width then CSP($\mathbb{B}$) has Frege refutations using only k-clauses.

- Polynomial size refutations.
- Polynomial time algorithm.

Theorem. Otherwise CSP($\mathbb{B}$) does not have Frege refutations of bounded depth and subexponential size.

For every t there exists δ such that for each big enough n there is an n-variable instance of CSP($\mathbb{B}$) whose Σ_t-Frege refutations require size at least 2^{n^δ}.

Linear Equations

G - non-trivial finite Abelian group

$\mathbb{B}(G,3) = (G; R_1, \ldots, R_n)$

$R_i = \{(g_1, g_2, g_3) \mid z_1 g_1 + z_2 g_2 + z_3 g_3 = g\}$

Theorem [Barto, Kozik, Bulatov]. The following are equivalent:

- $\mathbb{B}$ does not have bounded width,
- $\mathbb{B}(G,3)$ is pp-interpretable in $\mathbb{B}$.

Proof Idea

Theorem. $\mathbb{B}(G,3)$ has no Frege refutations of bounded depth and subexponential size.

- known for $G = \mathbb{Z}_2$ (Ben-Sasson 2002)
- Tseitin formulas based on expander graphs

$\mathbb{B}$ has no bounded width

$\Downarrow$

$\mathbb{B}(G,3)$ is pp-interpretable in $\mathbb{B}$

$\Downarrow$

refutations for CSP($\mathbb{B}$) translate to refutations for CSP($\mathbb{B}(G,3)$)

$\Downarrow$

CSP($\mathbb{B}$) cannot have "small size" refutations

Gap Theorem

Theorem

Exactly one of the following holds:

- *either $\mathbb{B}$ has Frege refutations using k-clauses,*
- *or $\mathbb{B}$ has no Frege refutations of bounded depth and subexponential size.*

Beyond Bounded Width

Theorem
$\mathrm{CSP}(\mathbb{B}(\mathbb{Z}_2, 3))$ *have Frege refutations of polynomial size.*

closed under "standard CSP reductions"

$\Downarrow$

has an algebraic characterization

Open Problem. Characterize the class of CSPs that have Frege refutations of polynomial size.

Conclusions

- for most propositional proof systems:

  polynomial size proofs $=$ bounded width;

- Frege goes beyond bounded width, how much?
- similar results for semi-algebraic proof systems;
- is proof complexity of approximating MAX CSP preserved by reductions?

  efficient proofs that $\mathbb{A}'$ is "far from satisfiable" transform into efficient proofs that $\mathbb{A}$ is "far from satisfiable"?

Thank you