Feasible Interpolation in Proof Systems based on Integer Linear Programming

Pavel Pudlák

Mathematical Institute, Academy of Sciences, Prague

Vienna 17.7.2014

Overview

1. Feasible interpolation
2. Linear programing
3. Cutting Planes
4. Lovász-Schrijver system
5. Semidefinite programing
6. Stronger Lovász-Schrijver systems

Feasible Interpolation

Theorem (Craig's Interpolation Theorem in Propositional Calculus)

Let $A(\bar{x}, \bar{y})$ and $B(\bar{x}, \bar{z})$ be propositions, where $\bar{x}, \bar{y}, \bar{z}$ are strings of propositional variables and $\bar{y}, \bar{z}$ are disjoint. If

$$\vdash A(\bar{x}, \bar{y}) \rightarrow B(\bar{x}, \bar{z}),$$

then there exists a proposition $C(\bar{x})$ such that

$$\vdash A(\bar{x}, \bar{y}) \rightarrow C(\bar{x}) \text{ and } \vdash C(\bar{x}) \rightarrow B(\bar{x}, \bar{z}).$$

Feasible Interpolation

Theorem (Craig's Interpolation Theorem in Propositional Calculus)

Let $A(\bar{x}, \bar{y})$ and $B(\bar{x}, \bar{z})$ be propositions, where $\bar{x}, \bar{y}, \bar{z}$ are strings of propositional variables and $\bar{y}, \bar{z}$ are disjoint. If

$$\vdash A(\bar{x}, \bar{y}) \rightarrow B(\bar{x}, \bar{z}),$$

then there exists a proposition $C(\bar{x})$ such that

$$\vdash A(\bar{x}, \bar{y}) \rightarrow C(\bar{x}) \text{ and } \vdash C(\bar{x}) \rightarrow B(\bar{x}, \bar{z}).$$

Krajíček's Idea:

If $A(\bar{x}, \bar{y}) \rightarrow B(\bar{x}, \bar{z})$ has a short proof, then C should be a small (circuit).

Reformulations

If $\vdash A(\bar{x}, \bar{y}) \vee B(\bar{x}, \bar{z})$, then there exists $C(\bar{x})$ such that

- $\vdash \neg C(\bar{x}) \rightarrow A(\bar{x}, \bar{y})$ and
- $\vdash C(\bar{x}) \rightarrow B(\bar{x}, \bar{z})$.

Reformulations

If $\vdash A(\bar{x}, \bar{y}) \vee B(\bar{x}, \bar{z})$, then there exists $C(\bar{x})$ such that

- $\vdash \neg C(\bar{x}) \rightarrow A(\bar{x}, \bar{y})$ and
- $\vdash C(\bar{x}) \rightarrow B(\bar{x}, \bar{z})$.

If $\vdash A(\bar{x}, \bar{y}) \vee B(\bar{x}, \bar{z})$, then there exists $C(\bar{x})$ such that for all assignments $\bar{x} \rightarrow \bar{a}$,

- if $C(\bar{a}) = 0$, then $\vdash A(\bar{a}, \bar{y})$, and
- if $C(\bar{a}) = 1$, then $\vdash A(\bar{a}, \bar{z})$

Reformulations

If $\vdash A(\bar{x},\bar{y}) \vee B(\bar{x},\bar{z})$, then there exists $C(\bar{x})$ such that

- $\vdash \neg C(\bar{x}) \rightarrow A(\bar{x},\bar{y})$ and
- $\vdash C(\bar{x}) \rightarrow B(\bar{x},\bar{z})$.

If $\vdash A(\bar{x},\bar{y}) \vee B(\bar{x},\bar{z})$, then there exists $C(\bar{x})$ such that for all assignments $\bar{x} \rightarrow \bar{a}$,

- if $C(\bar{a}) = 0$, then $\vdash A(\bar{a},\bar{y})$, and
- if $C(\bar{a}) = 1$, then $\vdash A(\bar{a},\bar{z})$

If $A(\bar{x},\bar{y}) \wedge B(\bar{x},\bar{z}) \vdash \bot$, then there exists $C(\bar{x})$ such that for all assignments $\bar{x} \rightarrow \bar{a}$,

- if $C(\bar{a}) = 0$, then $\vdash A(\bar{a},\bar{y}) \vdash \bot$, and
- if $C(\bar{a}) = 1$, then $\vdash A(\bar{a},\bar{z}) \vdash \bot$

The method of splitting proofs

Given a refutation $d : \{\alpha_j(\bar{x}, \bar{y})\} \cup \{\beta_k(\bar{x}, \bar{z})\} \vdash \bot$, and an assignment $\bar{x} \longrightarrow \bar{a}$, construct d_1 and d_2 such that

- either d_1 is a refutation of $\{\alpha_j(\bar{a}, \bar{y})\}$,
- or d_2 is a refutation of $\{\beta_k(\bar{a}, \bar{z})\}$

by splitting the proof into a y-part and a z-part:

The method of splitting proofs

Given a refutation $d : \{\alpha_j(\bar{x}, \bar{y})\} \cup \{\beta_k(\bar{x}, \bar{z})\} \vdash \bot$, and an assignment $\bar{x} \to \bar{a}$, construct d_1 and d_2 such that

- either d_1 is a refutation of $\{\alpha_j(\bar{a}, \bar{y})\}$,
- or d_2 is a refutation of $\{\beta_k(\bar{a}, \bar{z})\}$

by splitting the proof into a y-part and a z-part:

Procedure

1. substitute $d \mapsto d[\bar{x}/\bar{a}]$,
2. gradually replace $\phi(\bar{a}, \bar{y}, \bar{z}) \mapsto (\phi_1(\bar{a}, \bar{y}), \phi_2(\bar{a}, \bar{z}))$ so that

$$\phi_1(\bar{a}, \bar{y}) \wedge \phi_2(\bar{a}, \bar{z}) \Rightarrow \phi(\bar{a}, \bar{y}, \bar{z})$$

3. finally we get either $(\bot, \dots)$ or $(\dots, \bot)$

The transformation must preserve initial formulas and logical rules. In particular

$\alpha_j(\bar{a}, \bar{y}) \mapsto (\alpha_j(\bar{a}, \bar{y}), \top)$,

$\beta_k(\bar{a}, \bar{z}) \mapsto (\top, \beta_k(\bar{a}, \bar{z}))$

If this can be done done in polynomial time, we have feasible interpolation.

The transformation must preserve initial formulas and logical rules. In particular

$\alpha_j(\bar{a}, \bar{y}) \mapsto (\alpha_j(\bar{a}, \bar{y}), \top)$,

$\beta_k(\bar{a}, \bar{z}) \mapsto (\top, \beta_k(\bar{a}, \bar{z}))$

If this can be done done in polynomial time, we have feasible interpolation.

In Resolution

- $\phi(\bar{a}, \bar{y}, \bar{z}) \mapsto (\phi_1(\bar{a}, \bar{y}), \top)$ and $\phi_1(\bar{a}, \bar{y}) \subseteq \phi(\bar{a}, \bar{y}, \bar{z})$, or
- $\phi(\bar{a}, \bar{y}, \bar{z}) \mapsto (\top, \phi_2(\bar{a}, \bar{z}))$ and $\phi_2(\bar{a}, \bar{z}) \subseteq \phi(\bar{a}, \bar{y}, \bar{z})$

for all clauses in the proof.

Linear Programing

General problem

Given inequalities in $\mathbb{Q}$

$$\sum_{i=1}^{n} a_{ij} x_i \geq b_j, \qquad j = 1, \ldots, m, \tag{1}$$

and a vector $\vec{c}$, find

$$\max \sum c_i x_i$$

if it exists.

Linear Programing

General problem

Given inequalities in $\mathbb{Q}$

$$\sum_{i=1}^{n} a_{ij} x_i \geq b_j, \qquad j = 1, \ldots, m, \tag{1}$$

and a vector $\vec{c}$, find

$$\max \sum c_i x_i$$

if it exists.

Decision problem

Decide if (1) has any solution $\vec{x} \in \mathbb{Q}^n$.

Facts:

1. LP is solvable in polynomial time with exponential precision in general, hence precisely in $\mathbb{Q}$. In particular, the decision problem is in **P**.
2. (Farkas' Lemma) If (1) is unsolvable, then there exists a non-negative linear combination of the inequalities that gives
$$0 \geq 1$$
3. If an inequality E is a consequence of (1), then we can find in polynomial time a positive linear combination that gives E (by solving a dual problem).

Proof system for LP: use positive linear combinations to derive $0 \geq 1$.

Proof search is in polynomial time.

Integer Linear Programing

Find a solution of

$$\sum_i a_{ij} x_i \geq b_j, \qquad j = 1, \ldots, m,$$

in $\mathbb{Z}^n$.

- The decision problem is **NP**-complete.

Integer Linear Programing

Find a solution of

$$\sum_i a_{ij} x_i \geq b_j, \qquad j = 1, \ldots, m,$$

in $\mathbb{Z}^n$.

- The decision problem is **NP**-complete.

Two polytopes (or empty sets)

1. the polytope given by the inequalities,
2. the convex hull of the integral points.

Integer Linear Programing

Find a solution of

$$\sum_i a_{ij} x_i \geq b_j, \qquad j = 1, \ldots, m,$$

in $\mathbb{Z}^n$.

- The decision problem is **NP**-complete.

Two polytopes (or empty sets)

1. the polytope given by the inequalities,
2. the convex hull of the integral points.

We have to extend the LP proof system to obtain the smaller polytope.

Cutting Planes

The rounding up rule:

$$\frac{\sum_i c_i x_i \geq d}{\sum_i \lceil c_i \rceil x_i \geq \lceil d \rceil}$$

Cutting Planes

The rounding up rule:

$$\frac{\sum_i c_i x_i \geq d}{\sum_i \lceil c_i \rceil x_i \geq \lceil d \rceil}$$

Theorem (Gomory, Chvátal)

Applying the rounding rule a sufficient number of times we get the convex hull of the integral points (or the empty set if there are no such points).

The cutting plane proof system[1] CP

1. axioms $0 \leq x_i \leq 1 \qquad i = 1, \ldots, n$
2. positive linear combinations
3. the rounding rule

[1] Sometimes cutting planes is used as a generic name for all systems for ILP. Then one has to specify that it is Gomory-Chvátal cutting plane system.

The cutting plane proof system[1] CP

1. axioms $0 \leq x_i \leq 1 \qquad i = 1, \ldots, n$
2. positive linear combinations
3. the rounding rule

- simulates Resolution
- is stronger than Resolution (poly size proofs of PHP)
- has feasible interpolation

[1] Sometimes cutting planes is used as a generic name for all systems for ILP. Then one has to specify that it is Gomory-Chvátal cutting plane system.

Splitting a cutting plane proof

Apply the rules at each component separately:

$$
\begin{array}{ccccc}
\sum a_i y_i \geq c & \mapsto & \sum a_i y_i \geq c & | & 0 \geq 0 \\
\vdots & & & & \\
\sum b_j z_j \geq d & \mapsto & 0 \geq 0 & | & \sum b_j z_j \geq d \\
\vdots & & & & \\
\sum c_i y_i + \sum d_j z_j \geq e & \mapsto & \sum c_i y_i \geq e_1 & | & \sum d_j z_j \geq e_2 \\
\vdots & & & & \\
0 \geq 1 & \mapsto & 0 \geq f_1 & | & 0 \geq f_2
\end{array}
$$

where always $e \leq e_1 + e_2$; in particular $f_1 > 0$ or $f_2 > 0$.

Quadratic inequalities

It is difficult to split a quadratic inequality into two.

Eg. $y_1 z_1 + \cdots + y_n z_n \geq a$

Quadratic inequalities

It is difficult to split a quadratic inequality into two.

Eg. $y_1 z_1 + \cdots + y_n z_n \geq a$

We will write linear inequalities in the form

$$\sum a_i x_i - b \geq 0;$$

and call $\sum a_i x_i - b$ a *linear polynomial*.

Lovász-Schrijver system LS

- initial inequalities are linear
- axioms
  1. $0 \leq x_i \leq 1$
  2. $x_i^2 - x_i = 0$ (integrality)
- rules:
  1. positive linear combinations
  2. (multiplication) if $L(\bar{x}), K(\bar{x})$ are linear polynomials, then

$$\frac{L(\bar{x}) \geq 0 \quad K(\bar{x}) \geq 0}{L(\bar{x})K(\bar{x}) \geq 0}$$

Lovász-Schrijver system LS

- initial inequalities are linear
- axioms
  1. $0 \leq x_i \leq 1$
  2. $x_i^2 - x_i = 0$ (integrality)
- rules:
  1. positive linear combinations
  2. (multiplication) if $L(\bar{x}), K(\bar{x})$ are linear polynomials, then

$$\frac{L(\bar{x}) \geq 0 \quad K(\bar{x}) \geq 0}{L(\bar{x})K(\bar{x}) \geq 0}$$

Properties:

- sound and complete [Lovász-Schrijver, 1991]
- simulates Resolution
- stronger than Resolution

example

$x + y - \frac{1}{2} \geq 0$ given

example

$x + y - \frac{1}{2} \geq 0$ given

$x \geq 0,\ 1 - x \geq 0,\ y \geq 0,\ 1 - y \geq 0,\ x^2 - x = 0,\ y^2 - y = 0$ axioms

example

$x + y - \frac{1}{2} \geq 0$ given

$x \geq 0,\ 1 - x \geq 0,\ y \geq 0,\ 1 - y \geq 0,\ x^2 - x = 0,\ y^2 - y = 0$ axioms

$xy \geq 0$ by multiplication

example

$x + y - \frac{1}{2} \geq 0$ given

$x \geq 0,\ 1 - x \geq 0,\ y \geq 0,\ 1 - y \geq 0,\ x^2 - x = 0,\ y^2 - y = 0$ axioms

$xy \geq 0$ by multiplication

$x - x^2 + y - xy - \frac{1}{2} + \frac{1}{2}x \geq 0$ multiplication by $1 - x$

example

$x + y - \frac{1}{2} \geq 0$ given

$x \geq 0,\ 1 - x \geq 0,\ y \geq 0,\ 1 - y \geq 0,\ x^2 - x = 0,\ y^2 - y = 0$ axioms

$xy \geq 0$ by multiplication

$x - x^2 + y - xy - \frac{1}{2} + \frac{1}{2}x \geq 0$ multiplication by $1 - x$

$\frac{1}{2}x + y - \frac{1}{2} \geq 0$ using $x^2 - x = 0$ and $xy \geq 0$

example

$x + y - \frac{1}{2} \geq 0$ given

$x \geq 0,\ 1 - x \geq 0,\ y \geq 0,\ 1 - y \geq 0,\ x^2 - x = 0,\ y^2 - y = 0$ axioms

$xy \geq 0$ by multiplication

$x - x^2 + y - xy - \frac{1}{2} + \frac{1}{2}x \geq 0$ multiplication by $1 - x$

$\frac{1}{2}x + y - \frac{1}{2} \geq 0$ using $x^2 - x = 0$ and $xy \geq 0$

$\frac{1}{2}x - \frac{1}{2}xy + y - y^2 - \frac{1}{2} + \frac{1}{2}y \geq 0$ multiplication by $1 - y$

example

$x + y - \frac{1}{2} \geq 0$ given

$x \geq 0,\ 1 - x \geq 0,\ y \geq 0,\ 1 - y \geq 0,\ x^2 - x = 0,\ y^2 - y = 0$ axioms

$xy \geq 0$ by multiplication

$x - x^2 + y - xy - \frac{1}{2} + \frac{1}{2}x \geq 0$ multiplication by $1 - x$

$\frac{1}{2}x + y - \frac{1}{2} \geq 0$ using $x^2 - x = 0$ and $xy \geq 0$

$\frac{1}{2}x - \frac{1}{2}xy + y - y^2 - \frac{1}{2} + \frac{1}{2}y \geq 0$ multiplication by $1 - y$

$\frac{1}{2}x + \frac{1}{2}y - \frac{1}{2} \geq 0$

example

$x + y - \frac{1}{2} \geq 0$ given

$x \geq 0,\ 1 - x \geq 0,\ y \geq 0,\ 1 - y \geq 0,\ x^2 - x = 0,\ y^2 - y = 0$ axioms

$xy \geq 0$ by multiplication

$x - x^2 + y - xy - \frac{1}{2} + \frac{1}{2}x \geq 0$ multiplication by $1 - x$

$\frac{1}{2}x + y - \frac{1}{2} \geq 0$ using $x^2 - x = 0$ and $xy \geq 0$

$\frac{1}{2}x - \frac{1}{2}xy + y - y^2 - \frac{1}{2} + \frac{1}{2}y \geq 0$ multiplication by $1 - y$

$\frac{1}{2}x + \frac{1}{2}y - \frac{1}{2} \geq 0$

$x + y - 1 \geq 0$

Splitting an LS proof

We cannot split quadratic inequalities. Therefore we view segments between linear inequalities as single steps.

Splitting an LS proof

We cannot split quadratic inequalities. Therefore we view segments between linear inequalities as single steps.

We will gradually split the linear inequalities of a proof.

Assuming we have split the previous linear inequalities, we can express the next linear inequality as follows:

$$L_1(\bar{y})+$$

$$L_2(\bar{z})+$$

$$\sum_i a_i(y_i^2 - y_i) + \sum_k L_{3,k}(\bar{y})L_{4,k}(\bar{y})+$$

$$\sum_j b_j(z_i^2 - z_i) + \sum_l L_{5,l}(\bar{z})L_{6,l}(\bar{z})+$$

$$\sum_h L_{7,h}(\bar{y})L_{8,h}(\bar{z}) \geq 0$$

Assuming we have split the previous linear inequalities, we can express the next linear inequality as follows:

$$
\begin{gathered}
L_1(\bar{y})+ \\
L_2(\bar{z})+ \\
\sum_i a_i(y_i^2 - y_i) + \sum_k L_{3,k}(\bar{y})L_{4,k}(\bar{y})+ \\
\sum_j b_j(z_i^2 - z_i) + \sum_l L_{5,l}(\bar{z})L_{6,l}(\bar{z})+ \\
\sum_h L_{7,h}(\bar{y})L_{8,h}(\bar{z}) \geq 0
\end{gathered}
$$

Then all 5 parts are linear and the first 4 naturally split into a y-part and a z-part.

We only need to split

$$\sum_h L_{7,h}(\bar{y})L_{8,h}(\bar{z}) \geq 0$$

Note that after cancellations of terms it is a linear inequality that is a consequence of the inequalities $L_{7,h}(\bar{y}) \geq 0$ and $L_{8,h}(\bar{z}) \geq 0$. Hence it has form

$$\sum_h \alpha_h L_{7,h}(\bar{y}) + \sum_h \beta_h L_{8,h}(\bar{z}) \geq 0$$

To find α_hs and β_hs we use a polynomial algorithm for linear programing.

We only need to split

$$\sum_h L_{7,h}(\bar{y})L_{8,h}(\bar{z}) \geq 0$$

Note that after cancellations of terms it is a linear inequality that is a consequence of the inequalities $L_{7,h}(\bar{y}) \geq 0$ and $L_{8,h}(\bar{z}) \geq 0$. Hence it has form

$$\sum_h \alpha_h L_{7,h}(\bar{y}) + \sum_h \beta_h L_{8,h}(\bar{z}) \geq 0$$

To find α_hs and β_hs we use a polynomial algorithm for linear programing.

In fact, we only need the constant terms of $\sum_h \alpha_h L_{7,h}(\bar{y})$ and $\sum_h \beta_h L_{8,h}(\bar{z})$,
i.e., we need to split the constant term of $\sum_h L_{7,h}(\bar{y})L_{8,h}(\bar{z})$.

Semidefinite programing

A symmetric matrix $A \in \mathbb{R}^{n \times n}$ is positive semidefinite if for every vector $v \in \mathbb{R}^n$

$$v^\top A v \geq 0.$$

Equivalently, if there are vectors $v_1, \ldots, v_n$ such that

$$A_{ij} = v_i^\top v_j.$$

Semidefinite programing

A symmetric matrix $A \in \mathbb{R}^{n \times n}$ is positive semidefinite if for every vector $v \in \mathbb{R}^n$

$$v^\top A v \geq 0.$$

Equivalently, if there are vectors $v_1, \ldots, v_n$ such that

$$A_{ij} = v_i^\top v_j.$$

Another characterization: A quadratic form is semidefinite iff it is a sum of squares of linear forms:

$$\sum_{ij} A_{ij} x_i x_j = \sum_k (\sum_i b_{ik} x_i)^2$$

A semidefinite programing problem is given by a set of linear inequalities with variables x_{ij} and a linear function $L(\dots x_{ij} \dots)$.

We want to minimize $L(\dots x_{ij} \dots)$ subject to the inequalities and the condition that $\{x_{ij}\}$ is a positive semidefinite matrix.

A semidefinite programing problem is given by a set of linear inequalities with variables x_{ij} and a linear function $L(\dots x_{ij} \dots)$.

We want to minimize $L(\dots x_{ij} \dots)$ subject to the inequalities and the condition that $\{x_{ij}\}$ is a positive semidefinite matrix.

- SDP is solvable in polynomial time (by the ellipsoid method, or the interior point method)

A stronger Lovász-Schrijver system LS^+

- add axioms of the form
$$L(\bar{x})^2 \geq 0$$
for all linear polynomials L.

A stronger Lovász-Schrijver system LS^+

- add axioms of the form
$$L(\bar{x})^2 \geq 0$$
for all linear polynomials L.

Theorem (S. Dash 2001)

This system has feasible interpolation.

Splitting proofs in LS$^+$ (basic idea)

Given

$$\sum_j K_j(\bar{y}, \bar{z})^2$$

we need to write it in the form

$$\sum_j L_j(\bar{y})^2 + \sum_j M_j(\bar{z})^2 + \sum_j 2L_j(\bar{y})M_j(\bar{z})$$

so that the quadratic terms of $L_j(\bar{y})^2$, $M_j(\bar{z})^2$ and $L_j(\bar{y})M_j(\bar{z})$ are canceled by the terms from the multiplication rule and integrality axioms. The problem is how to split the constant terms in $K_j(\bar{y}, \bar{z})^2$.

Splitting proofs in LS$^+$ (basic idea)

Given

$$\sum_j K_j(\bar{y}, \bar{z})^2$$

we need to write it in the form

$$\sum_j L_j(\bar{y})^2 + \sum_j M_j(\bar{z})^2 + \sum_j 2L_j(\bar{y})M_j(\bar{z})$$

so that the quadratic terms of $L_j(\bar{y})^2$, $M_j(\bar{z})^2$ and $L_j(\bar{y})M_j(\bar{z})$ are canceled by the terms from the multiplication rule and integrality axioms. The problem is how to split the constant terms in $K_j(\bar{y}, \bar{z})^2$.

Finding such a representation of a quadratic polynomial in y_i's (resp. z_i's) is equivalent to finding a representation of a positive semidefinite matrix as a sum of rank 1 positive semidefinite matrices.

Splitting proofs in LS^+ (basic idea)

Given

$$\sum_j K_j(\bar{y}, \bar{z})^2$$

we need to write it in the form

$$\sum_j L_j(\bar{y})^2 + \sum_j M_j(\bar{z})^2 + \sum_j 2L_j(\bar{y})M_j(\bar{z})$$

so that the quadratic terms of $L_j(\bar{y})^2$, $M_j(\bar{z})^2$ and $L_j(\bar{y})M_j(\bar{z})$ are canceled by the terms from the multiplication rule and integrality axioms. The problem is how to split the constant terms in $K_j(\bar{y}, \bar{z})^2$.

Finding such a representation of a quadratic polynomial in y_i's (resp. z_i's) is equivalent to finding a representation of a positive semidefinite matrix as a sum of rank 1 positive semidefinite matrices.

Thus this representation can be found by semidefinite linear programing.

Recap

1. **CP** — elementary
2. **LS** — linear programing
3. **LS$^+$** — semidefinite linear programing

Applications

- May be easier to find an LS proof than a linear program, or semidefinite program for a given problem.
- Conditional lower bounds: if $\mathbf{P} \neq \mathbf{NP} \cap \mathbf{coNP}$, then there are tautologies that do not have polynomial length proofs.
- Unconditional lower bounds using monotone interpolation.

Monotone interpolation and lower bounds

Theorem (Krajíček)

Given a refutation of $d : \{\alpha_j(\bar{x}, \bar{y})\} \cup \{\beta_k(\bar{x}, \bar{z})\} \vdash \perp$ *where variables* $\bar{x}$ *occur in* $\{\alpha_j(\bar{x}, \bar{y})\}$ *only positively, one can construct a monotone Boolean circuit that interpolates these two sets and has size linear in the size of* d*.*

Monotone interpolation and lower bounds

Theorem (Krajíček)

Given a refutation of $d : \{\alpha_j(\bar{x}, \bar{y})\} \cup \{\beta_k(\bar{x}, \bar{z})\} \vdash \bot$ where variables $\bar{x}$ occur in $\{\alpha_j(\bar{x}, \bar{y})\}$ only positively, one can construct a monotone Boolean circuit that interpolates these two sets and has size linear in the size of d.

Theorem

The same for CP proofs and monotone real-valued circuits.

Using lower bounds on monotone Boolean and real-valued circuits for certain functions, we get exponential lower bounds on the lengths of Resolution and CP proofs.

Semantic CP

Fix $k \in \mathbb{N}$. Allow positive linear combinations and any valid rule with at most k assumptions.

Semantic CP

Fix $k \in \mathbb{N}$. Allow positive linear combinations and any valid rule with at most k assumptions.

Example For $a_i, b \in \mathbb{N}$, allow

$$\frac{\sum a_i x_i \geq b \qquad \sum a_i x_i \leq b}{0 \geq 1}$$

if $\sum a_i x_i = b$ has no solution. It is **NP**-hard to decide if it is a valid rule (knapsack!).

Semantic CP

Fix $k \in \mathbb{N}$. Allow positive linear combinations and any valid rule with at most k assumptions.

Example For $a_i, b \in \mathbb{N}$, allow

$$\frac{\sum a_i x_i \geq b \qquad \sum a_i x_i \leq b}{0 \geq 1}$$

if $\sum a_i x_i = b$ has no solution. It is **NP**-hard to decide if it is a valid rule (knapsack!).

[Hrubeš, 2014] An exponential lower bound based on monotone interpolation and real-valued circuits.

No lower bounds are known for LS.

[S. Dash, 2001] Exponential lower bounds on a weaker version of LS where $x_i x_j$ and $x_j x_i$ do not cancel each other and the multiplication rule has the form

$$\frac{L(\bar{x}) \geq 0}{xL(\bar{x}) \geq 0, \quad (1-x)L(\bar{x}) \geq 0}$$

No lower bounds are known for LS.

[S. Dash, 2001] Exponential lower bounds on a weaker version of LS where $x_i x_j$ and $x_j x_i$ do not cancel each other and the multiplication rule has the form

$$\frac{L(\bar{x}) \geq 0}{xL(\bar{x}) \geq 0, \quad (1-x)L(\bar{x}) \geq 0}$$

Conjecture

For proving lower bounds on LS proofs, we need lower bounds on a stronger model of monotone computations.

monotone Boolean circuits $\rightarrow$ monotone real circuits $\rightarrow$???

Monotone LP programs

P:

$$\sum_j a_{ij} z_j \leq \sum_k b_{ik} x_k + c_i$$

$a_{ij}, b_{ik}, c_i \in \mathbf{R}$ constants
$z_j \in \mathbf{R}^+$, $x_k \in \{0,1\}$ variables
$i = 1, \dots, l$, $j = 1, \dots, m$, $k = 1, \dots, n$.

P computes a Boolean function $f(\bar{x})$, if for every assignment $\bar{a}$ to $\bar{x}$

$$f(\bar{a}) = 1 \quad \equiv \quad P \text{ has a solution}$$

The size of P is $l + m + n$.

Monotone LP programs

P:

$$\sum_j a_{ij} z_j \leq \sum_k b_{ik} x_k + c_i$$

$a_{ij}, b_{ik}, c_i \in \mathbf{R}$ constants
$z_j \in \mathbf{R}^+$, $x_k \in \{0, 1\}$ variables
$i = 1, \ldots, l$, $j = 1, \ldots, m$, $k = 1, \ldots, n$.

P computes a Boolean function $f(\bar{x})$, if for every assignment $\bar{a}$ to $\bar{x}$

$$f(\bar{a}) = 1 \quad \equiv \quad P \text{ has a solution}$$

The size of P is $l + m + n$.

Problem

Prove lower bounds on the size of monotone LP programs computing a concrete Boolean functions.

THANK YOU