Syntactic versus semantic cutting planes

Pavel Hrubeš

Institute of Mathematics, Prague

Based on work with Y. Filmus and M. Lauria

Semi-algebraic proof systems

- Systems based on integer linear programming, intended to prove that a set of linear equalities has no $0, 1$-solution.
- A CNF can be represented as a set of linear inequalities.

Cutting Planes

Cutting Planes

- Manipulates linear inequalities with integer coefficients, $a_1 x_1 + \cdots + a_n x_n \geq b$, with $a_1, \ldots, a_n, b \in \mathbb{Z}$
- Given a system $\mathcal{L}$ of linear inequalities with no $0, 1$-solution, CP derives the inequality $0 \geq 1$ from $\mathcal{L}$.

Cutting Planes

- Manipulates linear inequalities with integer coefficients, $a_1 x_1 + \cdots + a_n x_n \geq b$, with $a_1, \ldots, a_n, b \in \mathbb{Z}$
- Given a system $\mathcal{L}$ of linear inequalities with no $0,1$-solution, CP derives the inequality $0 \geq 1$ from $\mathcal{L}$.

Axioms are inequalities in $\mathcal{L}$ and the inequalities

$$x_i \geq 0\,,\;\; x_i \leq 1\,.$$

The rules are:

$$\frac{L \geq b}{cL \geq cb}\,,\;\; \text{if } c \geq 0\,,\;\; \frac{L_1 \geq b_1\,,\;\; L_2 \geq b_2}{L_1 + L_2 \geq b_1 + b_2}\,,$$

$$\frac{a_1 x_1 + \ldots a_n x_n \geq b}{(a_1/c)x_1 + \ldots (a_n/c)x_n \geq \lceil b/c \rceil}\,,\;\; \text{provided } c > 0 \text{ divides every } a_i\,.$$

The Lovász-Schrijver system

The Lovász-Schrijver system

- Refutes a set of linear inequalities, but the intermediary steps can have degree 2.
- We can add two inequalities and multiply by a positive number. The additional rules are

$$\frac{L \geq 0}{xL \geq 0}, \quad \frac{L \geq 0}{(1-x)L \geq 0}, \quad x \text{ a variable, } L \text{ degree one.}$$

The Lovász-Schrijver system

- Refutes a set of linear inequalities, but the intermediary steps can have degree 2.
- We can add two inequalities and multiply by a positive number. The additional rules are

$$\frac{L \geq 0}{xL \geq 0}, \quad \frac{L \geq 0}{(1-x)L \geq 0}, \quad x \text{ a variable, } L \text{ degree one.}$$

Degree-d semantic systems

The Lovász-Schrijver system

- Refutes a set of linear inequalities, but the intermediary steps can have degree 2.
- We can add two inequalities and multiply by a positive number. The additional rules are

$$\frac{L \geq 0}{xL \geq 0}, \quad \frac{L \geq 0}{(1-x)L \geq 0}, \; x \text{ a variable, } L \text{ degree one.}$$

Degree-d semantic systems

- Intermediate inequalities can have degree $\leq d$.
- Inference rule is *any* valid inference.

$$\frac{L_1 \geq 0, \quad L_2 \geq 0}{L \geq 0},$$

provided every $0, 1$-assignment which satisfies the assumption satisfies the conclusion.

- Exponential lower bound on Cutting Planes [Pudlák'97]
- A lower bound on Lovász-Schrijver system, assuming certain boolean circuit lower bounds [Pudlák'97].
  - Interpolation technique.
- Exponential lower bounds for *tree-like* degree-*d* semantic systems [Beame, Pitassi & Segerlind' 07].
  - Communication lower bounds on randomized multi-party communication complexity of DISJ [Lee& Shraibman'08, Sherstov'12,..].
- Exponential lower-bound for *non-commutative* Lovasz-Schrijver [Dasch'01].

- Exponential lower bound on Cutting Planes [Pudlák'97]
- A lower bound on Lovász-Schrijver system, assuming certain boolean circuit lower bounds [Pudlák'97].
  - Interpolation technique.
- Exponential lower bounds for *tree-like* degree-*d* semantic systems [Beame, Pitassi & Segerlind' 07].
  - Communication lower bounds on randomized multi-party communication complexity of DISJ [Lee& Shraibman'08, Sherstov'12,..].
- Exponential lower-bound for *non-commutative* Lovasz-Schrijver [Dasch'01].

- Exponential lower bound on Cutting Planes [Pudlák’97]
- A lower bound on Lovász-Schrijver system, assuming certain boolean circuit lower bounds [Pudlák’97].
  - Interpolation technique.
- Exponential lower bounds for *tree-like* degree-*d* semantic systems [Beame, Pitassi & Segerlind’ 07].
  - Communication lower bounds on randomized multi-party communication complexity of DISJ [Lee& Shraibman’08, Sherstov’12,..].
- Exponential lower-bound for *non-commutative* Lovasz-Schrijver [Dasch’01].

- Exponential lower bound on Cutting Planes [Pudlák'97]
- A lower bound on Lovász-Schrijver system, assuming certain boolean circuit lower bounds [Pudlák'97].
  - Interpolation technique.
- Exponential lower bounds for *tree-like* degree-*d* semantic systems [Beame, Pitassi & Segerlind' 07].
  - Communication lower bounds on randomized multi-party communication complexity of DISJ [Lee& Shraibman'08, Sherstov'12,..].
- Exponential lower-bound for *non-commutative* Lovasz-Schrijver [Dasch'01].

Open problem. Prove super-polynomial lower bound on the Lovász-Schrijver system, or the degree-2 semantic system.

Syntactic Cutting Planes: explicit inference rules

$$\frac{L \geq b}{cL \geq cb}, \text{ if } c \geq 0, \quad \frac{L_1 \geq b_1, \; L_2 \geq b_2}{L_1 + L_2 \geq b_1 + b_2},$$

$$\frac{a_1 x_1 + \ldots a_n x_n \geq b}{(a_1/c)x_1 + \ldots (a_n/c)x_n \geq \lceil b/c \rceil}, \text{ provided } c > 0 \text{ divides every } a_i .$$

Semantic Cutting Planes: Inference rule

$$\frac{L_1 \geq b_1, \; L_2 \geq b_2}{L \geq b}$$

whenever $L \geq b$ follows from $L_1 \geq b_1$, $L_2 \geq b_2$.

Theorem (Lower bound).

For every n, there exists an unsatisfiable CNF of polynomial size which requires semantic CP refutations with $2^{n^{\Omega(1)}}$ *proof lines.*

Theorem (Separation).

There exists an unsatisfiable CNF which has a semantic CP refutation of polynomial size but every syntactic CP refutation has an exponential size.

Theorem (Pudlák).

There exists an unsatisfiable CNF of polynomial size which requires syntactic CP refutations with exponentially many proof lines.

Theorem.

There exists an unsatisfiable CNF of polynomial size which requires semantic CP refutations with exponentially many proof lines.

Theorem.
There exists an unsatisfiable CNF of polynomial size which requires semantic CP refutations with exponentially many proof lines.

- Cutting Planes has feasible interpolation via monotone real circuits.

Monotone real circuit

- computes a monotone boolean function $f : \{0, 1\}^n \to \{0, 1\}$.
- the inputs as well as the output are in $\{0, 1\}$, but
- the intermediary gates can compute an *arbitrary* non-decreasing real function (in two variables).

Monotone real circuit

- computes a monotone boolean function $f : \{0,1\}^n \to \{0,1\}$.
- the inputs as well as the output are in $\{0,1\}$, but
- the intermediary gates can compute an *arbitrary* non-decreasing real function (in two variables).

Monotone real circuits are exponentially more powerful than monotone Boolean circuits [Rosenbloom'97].

$$\begin{aligned} \mathrm{Clique}_n^k &= \left\{ G \in \{0,1\}^{\binom{n}{2}} : G \text{ has a clique of size } k \right\}, \\ \mathrm{Color}_n^k &= \left\{ G \in \{0,1\}^{\binom{n}{2}} : G \text{ is } k\text{-colorable} \right\}. \end{aligned}$$

$$\begin{aligned} \text{Clique}_n^k &= \left\{ G \in \{0,1\}^{\binom{n}{2}} : G \text{ has a clique of size } k \right\}, \\ \text{Color}_n^k &= \left\{ G \in \{0,1\}^{\binom{n}{2}} : G \text{ is } k\text{-colorable} \right\}. \end{aligned}$$

- $\text{Clique}_n^{k+1} \cap \text{Color}_n^k = \emptyset$.
- Clique_n^k is closed upwards (and Color_n^k downwards).

$$\begin{aligned} \mathrm{Clique}_n^k &= \left\{ G \in \{0,1\}^{\binom{n}{2}} : G \text{ has a clique of size } k \right\}, \\ \mathrm{Color}_n^k &= \left\{ G \in \{0,1\}^{\binom{n}{2}} : G \text{ is } k\text{-colorable} \right\}. \end{aligned}$$

- $\mathrm{Clique}_n^{k+1} \cap \mathrm{Color}_n^k = \emptyset$.
- Clique_n^k is closed upwards (and Color_n^k downwards).

$$\begin{aligned}\text{Clique}_n^k &= \left\{G \in \{0,1\}^{\binom{n}{2}} : G \text{ has a clique of size } k\right\},\\ \text{Color}_n^k &= \left\{G \in \{0,1\}^{\binom{n}{2}} : G \text{ is } k\text{-colorable}\right\}.\end{aligned}$$

- $\text{Clique}_n^{k+1} \cap \text{Color}_n^k = \emptyset$.
- Clique_n^k is closed upwards (and Color_n^k downwards).

Theorem (Pudlák).

For a suitable k ($k \sim n^{2/3}$), every monotone real circuit which accepts on Clique_n^{k+1} and rejects on Color_n^k has exponential size.

$x = \{x_{i_1,i_2}, i_1 < i_2 \in [n]\}$ - represent a graph on vertices $[n]$.

$\text{CLIQUE}_n^k(x, y)$ - a CNF formula asserting that y defines a clique of size k in x.

$x = \{x_{i_1,i_2}, i_1 < i_2 \in [n]\}$ - represent a graph on vertices $[n]$.

$\text{CLIQUE}_n^k(x, y)$ - a CNF formula asserting that y defines a clique of size k in x.

E.g., the conjunction of the following:

1. $\bigvee_{i \in [n]} y_{j,i}$, for every $j \in [k]$,
2. $\neg y_{j_1,i} \vee \neg y_{j_2,i}$, for every $j_1 \neq j_2 \in [k]$, $i \in [n]$,
3. $\neg y_{j_1,i_1} \vee \neg y_{j_2,i_2} \vee x_{i_1,i_2}$, for every $j_1, j_2 \in [k], i_1 < i_2 \in [n]$.

$\text{CLIQUE}_n^k(x, y)$ - a CNF formula asserting that y defines a clique of size k in x.

$\text{COLOR}_n^k(x, z)$ - a CNF formula asserting that z defines a k-coloring of x.

Then: $\text{CLIQUE}_n^{k+1} \wedge \text{COLOR}_n^k$ is unsatisfiable.

$\mathrm{CLIQUE}_n^k(x, y)$ - a CNF formula asserting that y defines a clique of size k in x.

$\mathrm{COLOR}_n^k(x, z)$ - a CNF formula asserting that z defines a k-coloring of x.

Then: $\mathrm{CLIQUE}_n^{k+1} \wedge \mathrm{COLOR}_n^k$ is unsatisfiable.

Proposition.

Assume that $CLIQUE_n^{k+1} \wedge COLOR_n^k$ has a (semantic) CP refutation with s lines. Then there exists an f accepting on $Clique_n^{k+1}$, rejecting on $Color_n^k$, and which has a monotone real circuit of size $poly(s)$.

Corollary.

Every semantic CP refutation of $CLIQUE_n^{k+1} \wedge COLOR_n^k(x, z)$ requires exponential number of lines (for $k \sim n^{2/3}$).

How about semantic inferences with higher arity?

$$\frac{L_1 \geq 0, \ldots, L_k \geq 0}{L \geq 0}\,.$$

How about semantic inferences with higher arity?

$$\frac{L_1 \geq 0, \ldots, L_k \geq 0}{L \geq 0} \,.$$

- The lower-bound works for every fixed k.

How about semantic inferences with higher arity?

$$\frac{L_1 \geq 0, \ldots, L_k \geq 0}{L \geq 0} \,.$$

- The lower-bound works for every fixed k.

Open problem: Are k-ary semantic inferences more powerful than binary semantic inferences?

How about semantic inferences with higher arity?

$$\frac{L_1 \geq 0, \ldots, L_k \geq 0}{L \geq 0}.$$

- The lower-bound works for every fixed k.

Open problem: Are k-ary semantic inferences more powerful than binary semantic inferences?

Open problem: Can every multivariate non-decreasing real function be expressed as a composition of non-decreasing unary or binary functions?

Open problem: Can every multivariate non-decreasing real function be expressed as a composition of non-decreasing unary or binary functions?

- Kolmogorov-Arnold representation theorem: every real continuous function can be expressed in terms of unary continuous functions and addition. (A solution to Hilbert's 13th Problem.)
- Does not hold for, e.g., analytic functions.

Theorem (Separation).

There exists an unsatisfiable CNF which has a semantic CP refutation of polynomial size but every syntactic CP refutation has an exponential size.

Lemma 1.
If a set of m linear equations is unsatisfiable then it has a semantic cutting planes refutation with $O(m)$ lines.

Lemma 1.
If a set of m linear equations is unsatisfiable then it has a semantic cutting planes refutation with $O(m)$ lines.

Lemma 2.
Let

$$\begin{aligned} \mathcal{L} &= \mathcal{L}_0 \cup \{L \geq 0\} \cup \{L \leq 1\} \\ \mathcal{L}' &= \mathcal{L}_0 \cup \{L = z\}, \end{aligned}$$

where z is a fresh variable. In syntactic cutting planes, the lengths of the shortest refutations of $\mathcal{L}'$ and $\mathcal{L}$ differ at most by an additive constant term.

Open problem: Are semantic inferences with *polynomially bounded coefficients* more powerful than syntactic inferences?