CSE 599S Proof Complexity

Lecture 10 2 Nov 2020

Semi-Algebraic Proofs

inequalities vs equalities vs logic

Cutting Planes

Integer Programming

deg 1 in original vars

Sherali-Adams

~LP lifts

linear programming

Nullstellensatz style

SoS Sum of Squares

~SDP lifts

semi-definite programming

high degree or extra vars

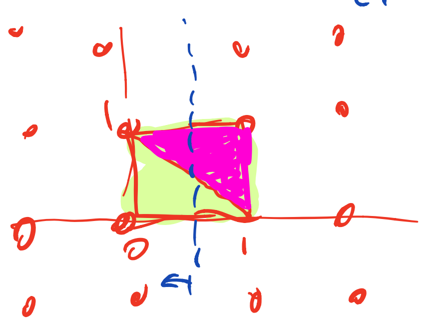
Clause C $x \vee y \vee \bar{z} \vee \bar{w}$

L_C: $x + y + 1-z + 1-w \geq 1$

$+ \quad 0 \leq x \leq 1 \quad 0 \leq y \leq 1 \quad 0 \leq z \leq 1 \quad 0 \leq w \leq 1$

$1-x \geq 0$

$x \geq 0$



$x \vee y$

$2x \leq 1$

$x + y \geq 1$

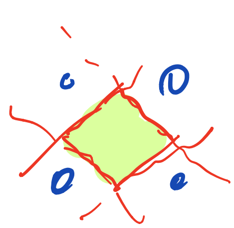
Cutting Planes Proofs

Work over arbitrary Integer Programs

each line is a linear inequality

$a_1 x_1 + \cdots + a_n x_n \geq c$

c, a_i integers



Rules of inference:

Addition

$$\begin{array}{l} a_1x_1 + \cdots + a_nx_n \geq c \\ b_1x_1 + \cdots + b_nx_n \geq d \\ \hline \therefore (a_1+b_1)x_1 + \cdots (a_n+b_n)x_n \geq c+d \end{array}$$

sound rules over $\mathbb{R}$

Multiplication

$$a_1x_1 + \cdots + a_nx_n \geq b$$

and $c \geq 0$

then $ca_1x_1 + \cdots + ca_nx_n \geq cb$

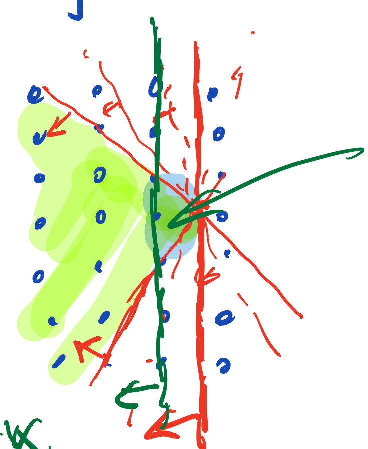
Division $c > 0$ integer

$$\begin{array}{l} ca_1x_1 + \cdots + ca_nx_n \geq b \\ \hline \therefore a_1x_1 + \cdots + a_nx_n \geq \lceil \frac{b}{c} \rceil \end{array}$$

Sound over $\mathbb{Z}$

not sound over $\mathbb{R}$.

e.g. $2x \geq 1 \Rightarrow x \geq 1$



cuts off this part of the region of $\mathbb{R}$ satisfying constraints

A $m \times n$ matrix

$Ax \leq b$

$x \geq 0$

polyhedra

polytopes

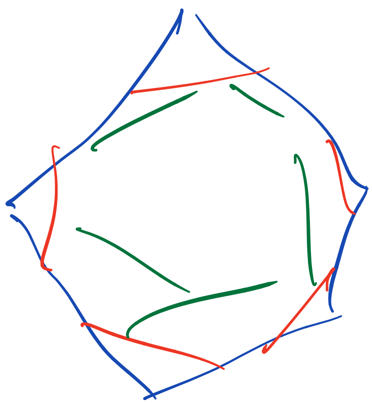
Rational Hull — P

Integer Hull — Convex hull of integer points in P

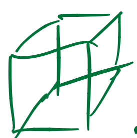
Gomory 1958 Chvátal 1983 Proof system for deriving integer hull from Rational Hull

- n dimension

depth n inference is enough to derive integer hull.



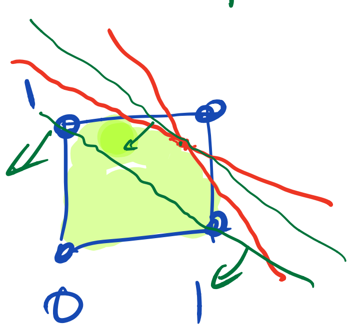
Integer Hull may have exponential # of faces (compare to polysize # of constraints for P.



$2n$ faces

+ M. Refutation System

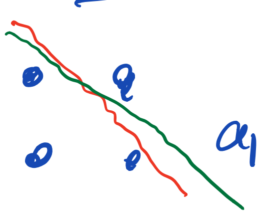
Goal: Derive $0 \geq 1$



Coefficient size
- arbitrary integers.

0,1-vars

Muroga: Coefficient size n^{n+1} enough for $\{0,1\}^n$



$a_1x_1 \cdots + a_nx_n \geq b$
$a'_1x_1 + \cdots + a'_nx_n \geq b'$ → same integer points.

Coulthard et al same idea works for Cutting Planes proofs

big coeffs $\Rightarrow$ small coeffs

$O(n \log n)$ bits long

Size : # lines

Depth of inferences

CP

Special subclass of CP: CP^*

$n^{O(1)}$ all coefficients are polysize

$n^{O(n)}$ not just poly # of bits.

Open: CP^* vs CP ?

Thm CP^* poly simulates Resolution

Proof line-by-line $C \longrightarrow L_C$

$x \vee y \vee \bar{z}$ $\qquad$ $x + y + (1 - z) \geq 1$

Resolution

$$\frac{(a \vee b \vee \bar{c} \vee d) \quad (\bar{a} \vee b \vee \bar{c} \vee \bar{e})}{b \vee \bar{c} \vee d \vee \bar{e}}$$

$$
\begin{array}{r}
a + b + 1-c + d \geq 1 \\
1-a + b + 1-c + 1-e \geq 1 \\
d \geq 0 \\
1-e \geq 0 \\
\hline
1 + 2b + 2(1-c) + 2d + 2(1-e) \geq 2
\end{array}
$$

$$\Downarrow$$

$$2b + 2(1-c) + 2d + 2(1-e) \geq 1$$

$$\boxed{b + (1-c) + d + (1-e) \geq \left\lceil \tfrac{1}{2} \right\rceil = 1}$$

Thm (Buss & Clote) division by 2 is enough (can keep proof length the same)

$O(\text{coeff \# bits})$ # of steps to simulate

Thm CP^* has an efficient proof of PHP^m_n $m > n$

Proof PHP^m_n: Pigeon: $x_{i1} + \cdots + x_{in} \geq 1$

Hole: $x_{ij} + x_{i'j} \leq 1$

Claim For $2 \leq k \leq m$ there is a k^2-line CP^* derivation of $\sum_{i \in [k]} x_{ij} \leq 1$

Proof $k=2$ $\quad x_{1j}+x_{2j}\le 1$ axiom ✓

Ind-Step ⓪ $x_{1j}+\cdots+x_{kj}\le 1$ IH.

① $x_{1j}+x_{k+1,j}\le 1$ axiom

② $x_{2j}+x_{k+1,j}\le 1$ ⋮

⋮

ⓚ $x_{kj}+x_{k+1,j}\le 1$ ⋮

$(k-1)$⓪ + ① + ② + ⋯ + ⓚ

$k\cdot x_{1j}+k\cdot x_{2j}+\cdots k\cdot x_{kj}+k\cdot x_{k+1j}\le 2k-1$

div k $\quad \exists\ x_{1j}+x_{2j}+\cdots+x_{kj}+x_{k+1,j}\le\left\lfloor\frac{2k-1}{k}\right\rfloor = 1$ ∎

∴ For each hole in $O(m^2)$ lines $O(nm^2)$

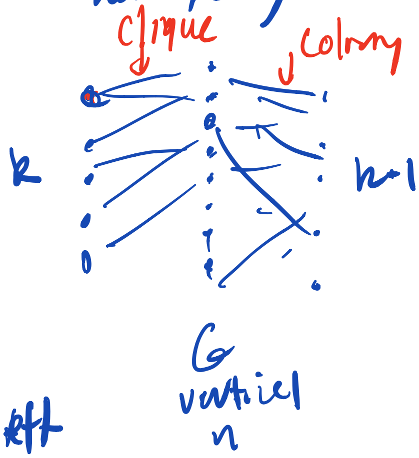
$$\sum_{i\in[m]} x_{ij}\le 1$$

For each pigeon $\sum_{j\in[n]} x_{ij}\ge 1$

$$n\ge\sum_{i\in[m]}\sum_{j\in[n]} x_{ij}\ge m$$

$$0\ge \underbrace{m-n}_{\ge 1}$$ ∎

What is hard/easy for CP?



Clique-Coloring formulas.

every vertex on left has an edge

two vertices with edges must be adjacent in G

cannot go to same vertex of G

every vertex in G maps to some point in RHS.

adjacent vertices in G cannot map to same RHS vertex

Conjectures: Random 3-CNF hard for CP?

Tseitin on expanders hard for CP?

Random $\Theta(\log n)$-CNF formulas are hard but $O(1)$-CNF open

Best paper at CCC2020

Tseitin has $n^{O(\log n)}$ size proofs in CP. $\triangle$

Pseudo-Boolean Solvers

generalization of CDCL Solvers