Oct 1

Cutting Planes Proofs

Reasoning about boolean formulas using **integral linear inequalities** over the reals.

Linear inequality: $\sum a_i x_i \geq b$ $\quad$ x_i vars, $a_i \in \mathbb{R}$ $\quad b \in \mathbb{R}$

Integral if $a_i, b \in \mathbb{Z}$

How to encode CNF formula F as a system of linear inequalities? Use simplest method:

ex) If $C = x_1 \vee \overline{x}_2 \vee x_3 \longrightarrow x_1 + (1 - x_2) + x_3 \geq 1$

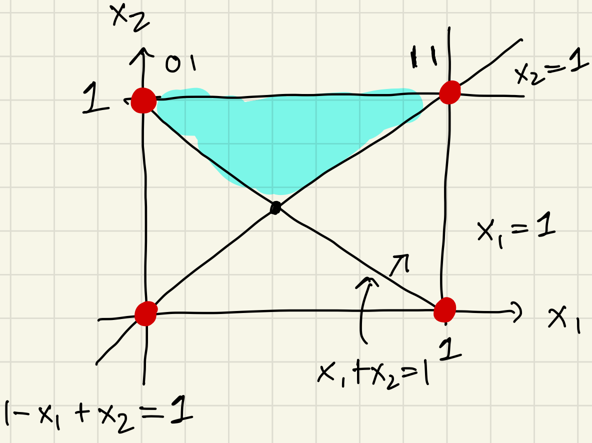
$x_i \in \{0,1\}$

$x \in \{0,1\}^3$ satisfies $C \iff$ this inequality is satisfied

ex) $F = (x_1 \vee x_2) \wedge (\overline{x}_1 \vee x_2) \longrightarrow$

$$x_1 + x_2 \geq 1$$
$$(1 - x_1) + x_2 \geq 1$$

$0 \leq x_1 \leq 1 \quad 0 \leq x_2 \leq 1$



Linear program / polyhedral set!

ex) $F = x_1 \vee x_2 \quad x_1 \vee \overline{x_2} \quad \overline{x_1} \vee x_2 \quad \overline{x_1} \vee \overline{x_2}$

$x_1 + x_2 \geq 1 \qquad x_1 + (1 - x_2) \geq 1 \qquad (1 - x_1) + x_2 \geq 1 \quad (1 - x_1) + (1 - x_2) \geq 1$

$$0 \leq x_1, x_2 \leq 1$$

Unsatisfiable over $\{0,1\}$, Satisfiable over $\mathbb{R}$!

$x_1 = \frac{1}{2} = x_2$

Fact Let $x \in \mathbb{R}^n$, $a \in \mathbb{Z}^n$, $b \in \mathbb{Z}$, and suppose there is a $d \in \mathbb{Z}^+$ s.t. d divides every entry of vector a.

→ as integer no remainder.

Then any integer solution of

$a \cdot x \geq b$ is also a solution of.

$$\frac{a}{d} x \geq \left\lceil \frac{b}{d} \right\rceil$$

$2x_1 \geq 3$

$x_1 \geq 3/2$ → $x_1 \geq 2$

Pf. If d divides b then obvious, if d doesn't divide b then

$$ax \geq b \iff \underbrace{\frac{a}{d} x}_{\text{integer}} \geq \frac{b}{d} \implies \frac{a}{d} x \geq \left\lceil \frac{b}{d} \right\rceil$$

ex) $F = x_1 \vee x_2 \quad x_1 \vee \bar{x}_2 \quad \bar{x}_1 \vee x_2 \quad \bar{x}_1 \vee \bar{x}_2$

$$x_1 + x_2 \geq 1 \qquad x_1 + (1 - x_2) \geq 1 \qquad (1 - x_1) + x_2 \geq 1 \qquad (1 - x_1) + (1 - x_2) \geq 1$$

$+$ $\qquad\qquad$ $+$

sound over $\mathbb{R}$

$$2x_1 \geq 1 \qquad\qquad 2(1 - x_1) \geq 1$$

$$1 \geq 2x_1$$

only sound over $\mathbb{Z}$

$$x_1 \geq 1 \qquad\qquad 0 \geq x_1$$

$+$

matrix!

$$0 \geq 1 \quad \bot\,!$$

Definition Let $Ax \geq b$ be a system of integer linear inequalities. A Cutting Planes derivation of the inequality $cx \geq d$ is a sequence of inequalities

$$a_1 x \geq b_1,\ a_2 x \geq b_2\ \cdots,\ a_s x \geq b_s$$

s.t. each inequality is either in $Ax \geq b$ or is deduced from earlier inequalities by one of the following two rules:

① Non-negative linear combos

$$\frac{a_j x \geq b_j \qquad a_k x \geq b_k}{(u a_j + v a_k) x \geq u b_j + v b_k} \qquad \begin{array}{l} \forall u, v \in \mathbb{Z} \\ u, v \geq 0 \end{array}$$

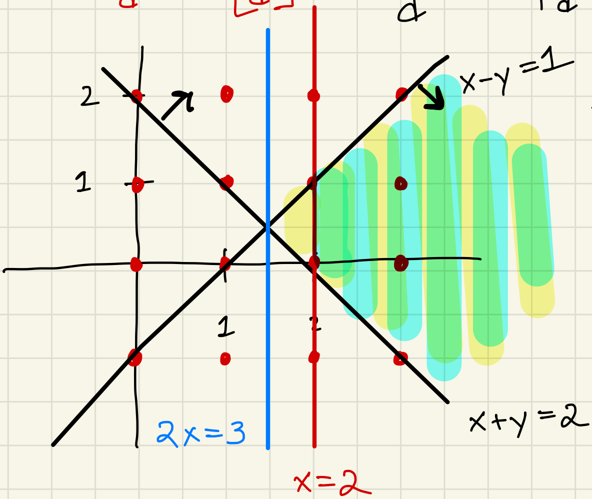
sound over real, integer solutions

② Division rule

$d \in \mathbb{Z}$

$$\frac{ax \leq b}{\frac{a}{d}x \leq \left\lfloor \frac{b}{d} \right\rfloor} \qquad \frac{ax \geq b}{\frac{a}{d}x \geq \left\lceil \frac{b}{d} \right\rceil}$$

for any $d \geq 0$ that divides all entries of a



$$\frac{x+y \geq 2 \qquad x-y \geq 1}{2x \geq 3}$$
$$\Big|$$
$$x \geq 2$$

A Cutting Planes (CP) refutation is a proof of $0 \geq 1$.

Complexity Measures

- The length of a Cutting Planes proof is s, the number of inequalities.
- The size of a CP proof is the number of bits in the binary encoding of each inequality in the proof. (Integers encoded in binary)
- The depth of a CP proof is the length of the longest source-sink path in the graph representation

"Cutting Planes" (division rule) was introduced by Gomory in 1963 to study the problem of finding integer solutions to systems of linear equations $Ax \geq b$.

Cutting Planes as a proof system was really defined Chvátal in 73. As a propositional proof system it was first studied by [CCT 87].

<u>Thm</u> [CCT 87]

If F is an unsat CNF formula and π is a CP refutation of F then there is another ref. π' s.t.

$$\text{size}(\pi') \leq \text{poly}(\text{length}(\pi), n)$$

i.e. coefficients can be assumed to be "small".

$L_{CP}(F) :=$ length of shortest CP ref. of F

$S_{CP}(F) :=$ size — smallest ————

$D_{CP}(F) :=$ depth of shallowest CP ref. of F.

<u>Thm</u> $L_{CP}(PHP_n^{n+1}) = O(n^3)$ (contrast to Res!)

<u>Pf.</u> PHP_n^{n+1} as inequalities:

Pigeon axiom: $\forall i \in [n+1]$: $\sum_{j=1}^{n} x_{ij} \geq 1$

Hole axiom: $\forall i_1 \neq i_2 \in [n+1], j \in [n]$: $x_{i_1 j} + x_{i_2 j} \leq 1$

$0 \leq x_{ij} \leq 1$

First deduce "~~every pigeon can go to at most one hole~~"

$$\forall j \in [n] \quad \sum_{i=1}^{n+1} x_{ij} \le 1 \qquad (*)$$

This really says every hole can have ≤ 1 pigeon

Sum pigeons over all i:

$$\sum_{i=1}^{n+1} \sum_{j=1}^{n} x_{ij} \geq n+1$$

Sum $(*)$ over all holes j:

$$\sum_{i=1}^{n+1} \sum_{j=1}^{n} x_{ij} \le n$$

Add together to get $n+1 \le n$, contradiction!

Remains to prove $(*)$.

$$\sum_{i=1}^{n+1} x_{ij} \le 1$$

We do it "inductively": deduce

$$\sum_{i=1}^{k} x_{ij} \le 1 \quad \text{for all } k = 1 \cdots n+1$$

$k=1 := \quad x_{1j} \le 1 \quad$ (in F)

$k=2 := \quad x_{1j} + x_{2j} \le 1 \quad$ (hole axiom!)

Assume we proved $\sum_{i=1}^{k} x_{ij} \le 1$, show $\sum_{i=1}^{k+1} x_{ij} \le 1$

- Sum up hole axioms
- $x_{ij} + x_{(k+1)j} \le 1$ for all $i \le k$

$$\sum_{i=1}^{k} x_{ij} + k\, x_{(k+1)j} \le k$$

Multiply $\sum_{i=1}^{k} x_{ij} \le 1$ by $(k-1)$ then add:

$$k \sum_{i=1}^{k+1} x_{ij} \le 2k-1$$

Division: $$\sum_{i=1}^{k+1} x_{ij} \le \left\lfloor 2 - \tfrac{1}{k} \right\rfloor = 1 \qquad \square$$

Can we get efficient proofs of other formulas that were hard for resolution?

Tseitin_G := conjectured to be hard since 80s

[Dadush–Tiwari 2020] $L_{CP}(\text{Tseitin}) \le n^{O(\log^c n)}$.
CCC Best Paper

Random k-CNFs := conjectured to be hard since 80s

Resolved independently for $k = O(\log n)$ by

[HP 17], [FPPR 17],

proved exponential lower bounds.

Open Problem Prove good lower bounds for random k-CNFs when $k = O(1)$.

Open Problem Understand "true" complexity of Tseitin in Cutting Planes