Today: Cutting Planes, Interpolation + Automatizability

CUTTING PLANES - Chvatal

Refutation System

Lines are linear inequalities $\sum_i a_i x_i \geq k$

a_i, k are integers

Axioms $x_i \geq 0$

$1 - x_i \geq 1$

Rules (1) addition $\sum a_i x_i \geq k$, $\sum b_i x_i \geq k'$

$$\sum (a_i + b_i) x_i \geq k + k'$$

(2) multiplication $\sum a_i x_i \geq k \Rightarrow c \cdot \sum a_i x_i \geq c \cdot k$

$c > 0$

(3) $\sum 2 \cdot a_i x_i \geq k \Rightarrow \sum a_i x_i \geq \lceil \frac{k}{2} \rceil$

Ex. $2x_1 + 2x_2 \geq 1$

$x_1 + x_2 \geq 1$

A CP refutation of a set of linear inequalities $L = \{l_1, l_2 \ldots l_q\}$ is a sequence of inequalities $\{s_1, s_2, \ldots s_m\}$ s.t. each s_i is either in L or is an axiom, or follows from previous lines by a rule, & final line s_m is $\underbrace{0 \geq 1}$

Length of a ~~proof~~ is the sum of the sizes of all of the coeffs written in binary
$\approx$ the # of lines in the Pf

[Muroga's Thm
wlog coeff's are all poly bded]

Lemma CP p-simulates Resolution

Let $f = C_1 \wedge \dots \wedge C_m$ be an unsat formula with a Res refutation R.

Then the corresponding family of linear ineq's has a CP refutation of size $|R|$

$$C_i = (x_1 \vee \bar{x}_2 \vee x_3) \longrightarrow x_1 + (1 - x_2) + x_3 \geq 1$$

$(x_1 \vee \bar{x}_2)\ (x_2 \vee x_3 \vee x_1)\ (\bar{x}_1 \vee x_3)\ (\bar{x}_3)$

$x_1 + 1 - x_2 \geq 1$ $\quad x_2 + x_3 + x_1 \geq 1$ $\quad 1 - x_1 + x_3 \geq 1$ $\quad 1 - x_3 \geq 1$

$(x_1 \vee x_3)$

$2x_1 + x_3 \geq 1$ $\quad x_3 \geq 0$

$2x_1 + 2x_3 \geq 1$

$x_1 + x_3 \geq 1$

x_3

$2x_3 \geq 1$

$x_3 \geq 1$

$\emptyset$ $\quad 0 \geq 1$

On the other hand CP is more powerful

CPs has really short ref's of PHP.

$$P_{1,1}+P_{12}+\dots+P_{1n} \geq 1$$

$$P_{21}+P_{22}+\dots+P_{2n} \geq 1$$

$$P_{n+1,1}+\dots+P_{n+1,n}$$

$$\sum P_{ij} \geq n+1$$

$$1-P_{i,j} + 1-P_{i_2 j} \geq 1$$

$\forall j \in [n]$

$$P_{1j}+\dots+P_{n+1,j} \leq 1$$

$$\sum P_{ij} \leq n$$

Automatizability + Feasible Interpolation

Interpolation

Let $A(\bar{p},\bar{q}) \wedge B(\bar{p},\bar{r})$ be an UNSAT CNF

A craig interpolant for this formula is a function $C(\vec{p})$ s.t.

$$\forall \alpha \quad C(\alpha) = 0 \Rightarrow A(\alpha, \bar{q}) \text{ is UNSAT}$$
$$\forall \alpha \quad C(\alpha) = 1 \Rightarrow B(\alpha, \bar{r}) \text{ is UNSAT}$$

If $\bar{p}$ occurs only positively in A, then $C(\vec{p})$ is monotone

Defn A proof system P has feasible interpolation property if $\forall$ UNSAT $f = A(\bar{p}, \bar{q}) \wedge B(\bar{p}, \bar{r})$ with a P-proof of size s, $\exists$ a craig interpolant circuit for f of size $\mathrm{poly}(s)$

P has <u>monotone</u> <u>feas</u> <u>interp.</u> if
$\forall$ monotone $f = A(\bar{p}\ \bar{q}) \wedge B(\bar{p}, \bar{r})$ with.. s
$\exists$ a monotone craig interp circuit for f
of size $\mathrm{poly}(s)$

Thm Let $\mathcal{P}$ be a prop. pf system

(1) If $\mathcal{P}$ has feas interp and $NP \not\subseteq P/poly$

then $\mathcal{P}$ is not poly bdd

(2) If $\mathcal{P}$ has monotone feas interpolation

the $\mathcal{P}$ is not poly bdd

Pf sketch.

(1) spose $\mathcal{P}$ has feas interp. & is poly bdd

Let $A(\bar{p}\,\bar{q})$: $\bar{p}$ encodes a 3CNF formula and $\bar{q}$ is a sat. ass. for $\bar{p}$

Let $B(\bar{p},\bar{r})$: $\bar{p}$ encodes a CNF formula and $\bar{r}$ encodes a $\mathcal{P}$-ref of $\bar{p}$

since $\mathcal{P}$ is poly bdd, $A \wedge B$ has length poly in n (# vars underly $\bar{p}$).

Since $\mathcal{P}$ is poly bded $A \wedge B$ has a
$\mathcal{P}$-ref of size poly(n)

Since $\mathcal{P}$ has feas int, $\exists$ C of size poly(n)
that tells us if $A(\alpha, \bar{q})$ UNSAT
OR $B(\alpha, \bar{r})$ is UNSAT

$\therefore$ C is deciding SAT in poly size

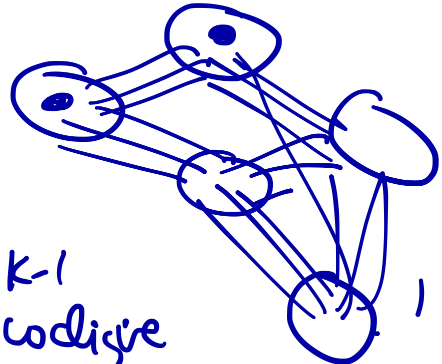
---

2 Spose $\mathcal{P}$ has monotone feas interp &
$\mathcal{P}$ is poly bded.

Let $A(\bar{p}, \bar{q})$: $\bar{p}$ encode a graph on n vertices
$\bar{q}$ encode a K-clique
A says if $i, j \in K$-clique
then (i,j) ~~one~~ is in $\bar{p}$

$B(\bar{p}, \bar{r})$: $\bar{p}$, $\bar{q}$ encode $(K-1)$ co clique
~~B says (i,j)~~

B says
if i, j are in the same class,
then (i,j) is not in $\bar{P}$



$k-1$ coclique

partition of V into $k-1$ pieces

If P is poly bdd,
$A \wedge B$ has a P-ref of size poly(n). Since P also has monotone feas. interp, this means there is a monotone polysized circuit $C(\vec{\alpha})$:

1 if α is a k-clique

0 if α is a $(k-1)$ coclique

<u>Razborov</u> $\exists \varepsilon$, $k = \frac{n}{10}$ there is no size $2^{n^{\varepsilon}}$ monotone circuit C

We will show:

1. Resolution has monotone feas interp
   also has " "

2. CP also has monotone feas interp
   & feas interp

$\Uparrow$

as a corollary of the prev thm
this implies expl LBs for Res & CPs refutations of Clique/coclique split formula

You can't have your cake & eat it too:

<u>Lemma</u> Let P be a proof system closed under restrictions.
Then if P is automatizable then P has feas. interpolation

If P ~~[illegible]~~ has feas interp $\Rightarrow$ it is weak + we can prove lower bds for it

If P doesn't have feas interp $\Rightarrow$ it is complex, + we can't find the pfs

Pf of Lemma Assume $\mathcal{P}$ is aut.

Let s be a $\mathcal{P}$-ref of $A(\bar{p}\,\bar{q}) \wedge B(\bar{p}, \bar{r})$

1. Run aut. alg for $\mathcal{P}$ on $A(\bar{p}\,\bar{q}) \wedge B(\bar{p}\,\bar{r})$
to get a $\mathcal{P}$-proof s', $|s'| = \text{poly}(s)$ ← size of shortest $\mathcal{P}$ ref of $A \wedge B$

2. Suppose $B(\bar{\alpha}, \bar{r})$ is satisfiable
& let $B(\bar{\alpha}, \bar{\gamma})$ be 1
Since $\mathcal{P}$ is closed under restrictions
$A(\bar{\alpha}, \bar{q}) \wedge B(\bar{\alpha}, \bar{\gamma})$ also has a $\mathcal{P}$-ref
of size $\text{poly}(s') = \text{poly}(s)$

$C(\underline{\bar{\alpha}})$:
So we will run aut. alg on $A(\bar{\alpha}, \bar{q})$
for $\text{poly}(s')$ steps
If it outputs a valid ref $\rightarrow$ say $A(\bar{\alpha}, \bar{q})$ UNSAT
If it doesnt $\Longrightarrow$ $B(\bar{\alpha}, \bar{r})$ is UNSAT

On Negative Results

Thm BPR, KP

If factoring Blum integers is hard then Frege proofs do not have feas. interpolation

If factoring Blum integers is really hard then AC_0-Frege pfs ...

PAC Learning Valiant

Concept class $\mathcal{C}^n$

Ex $\mathcal{C}$ = all poly size in n DNF formulas

$\mathcal{C}$ = all poly size formulas

$\mathcal{C}$ = all linear threshold functions

$\{\mathcal{C}^n\}$ is (ε, δ)-PAC learnable

if there is an alg A (unknown distribution $\mathcal{D}$ on $\{0,1\}^n$) underlying $f_n \in \mathcal{C}$

gets access to pairs

$(\alpha, f(\alpha))$ $\alpha \sim \mathcal{D}$

after poly(n) steps, A output some hypothesis $h_n : \{0,1\}^n \to \{0,1\}$

With prob. $(1-\delta)$ $\Pr_{\alpha \sim \mathcal{D}}[h_n(\alpha) = f_n(\alpha)] \geq 1 - \varepsilon$

Known: Dec trees are

DNFs ?

AC_0-circuits
poly size formulas

are not PAC learnable under crypto assumptions