CSE 599S Proof Complexity & Applications

Lecture 17 30 Nov 2020

Cutting Planes, Triangle DAGs, & Lifting

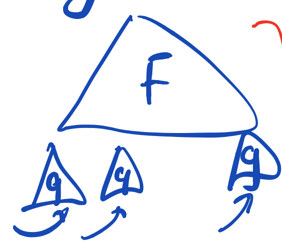
Lifting in general: formula F in n vars $z_1, \ldots, z_n$

Boolean function g

new formula $F \circ g^n$

new formula

separate vars



$TS^{(AND_k)}$

$g = AND_k$

$\oplus$

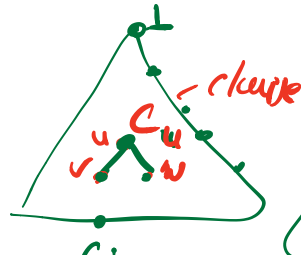
$PEB^{(\oplus 2)}$

$g = \oplus$

Recall: Cube-DAG for Resolution refutations

Search$_F$:

on input x find index of falsified clause



Associated subcube of inputs that falsify clause C

$C_u \subseteq C_v \cup C_w$ soundness

width = max length of clause in proof

New proof method: works for any ~~proof~~ sound system:
- fan-in 2
- each line integer linear inequality

semantic

Cutting Planes

Input to a line split in X vars

Y vars

Recall: R rectangle in $X \times Y$ iff

$R = A \times B$ for $A \subseteq X$, $B \subseteq Y$

$\exists\, a_R, b_R$ functions $\quad = \{(x,y) \mid a_R(x) = 1 \text{ and } b_R(y) = 1\}$

Def^n T triangle in $X \times Y$ iff

a_T, b_T functions $\quad T = \{(x,y) \mid a_T(x) < b_T(y)\}$

$a_T : X \to \mathbb{R}$

$b_T : Y \to \mathbb{R}$

proof line ℓ: $\quad a(x) + b(y) \geq D$

triangle $T = T_\ell$: $\quad a_T(x) = a(x)$

$\quad b_T(y) = D - b(y)$

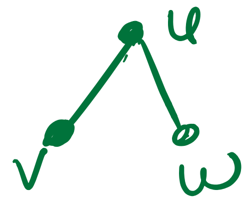
inputs falsified by ℓ

ℓ is false $\iff a(x) + b(y) < D$

$\iff a(x) < D - b(y)$

$\iff a_T(x) < b_T(y)$

Δ-dag   triangle DAG

- root labelled by $X \times Y$
- every node v labeled by Δ, T_v.
- 

$T_u \subseteq T_v \cup T_w$
- output is value at leaf.

Thm If $F(X;Y)$ has a semantic CP refutation of size $\leq S$ then Search_F has a Δ-dag of size $\leq S$

Leaf label contained in set of $X \times Y$ pairs that falsify a single clause of F

Note: given F get to choose X, Y permutation of any to prove lower bound on Δ-deg

---

Index funct.

$IND_m : [m] \times \{0,1\}^m$ $\quad$ $m = n^{\Theta(1)}$

$X \quad Y$

$$IND_m(X,Y) = Y_X$$

$$F \circ IND_m^n$$

Boolean version of IND_m:

instead of $x \in [m]$

$x \in \{0,1\}^m$ with exactly one 1

enforced with extra constraints $\boxed{\text{assume}}$ n copies of IND_m

$$z_i \longmapsto \underbrace{\bigwedge_{j=1}^{m} (x_{ij} \to y_{ij})}_{\text{selects } y_{ij} \text{ s.t. } x_{ij}=1}$$

$$\bar{z}_i \longmapsto \bigwedge_{j=1}^{m} (x_{ij} \to \bar{y}_{ij})$$

$$z_1 \vee \bar{z}_2 \vee z_3 \longmapsto \bigwedge_{j_1, j_2, j_3 \in [m]} (\bar{x}_{1j_1} \vee \bar{x}_{2j_2} \vee \bar{x}_{3j_3} \vee y_{1j_1} \vee \bar{y}_{2j_2} \vee y_{3j_3})$$

k $\quad$ m^k clauses $\quad$ $2k$

Enforcing one 1:

extra m vars per i:

$x'_{i1}, \ldots, x'_{im}$

$\bar{x}'_{ij} \vee x'_{i(j+1)} \equiv x'_{ij} \to x'_{i(j+1)}$ increasing

x'_{im} ending at 1

if $x'_{i1}=1$ then $x_{i1}=1$ $\to$ $x_{i1} = x'_{i1}$

$x_{ij}=1$ if $\to$ $x_{ij} \Leftrightarrow x'_{ij} \wedge \bar{x}'_{i(j-1)}$

x'_{ij} sequence jumps to 1 at j

enforces exactly one 1 in x_{ij}

"Boolean $FoIND^n_m$"

Thm If F requires resolution width w

then Boolean $FoIND^n_n$

for $m = n^c$ ($c \sim 100$)

requires semantic CP refutation size $n^{\Omega(w)}$

Cor $2^{n^{\Omega(1)}}$ lower bounds for many formulas

eg lifted random k-CNF

lifted Tseitin

etc

Proof idea:

Show: If $F \circ \mathrm{IND}^n_m$ has a Δ-deg of size $\leq n^d$ for $\mathrm{Search}_{F\circ \mathrm{IND}^n_m}$

then F has a resolution proof (cube-DAG) of with $O(d)$.

Proof: direct simulation complicated ....

simplified arg Meutz-Pitassi

Con   Lifted Directed Tseitin

DTS(G)

every vertex but 1
sum of indegrees
= sum of outdegrees
at one vertex
these differ by
2

bounded degree

has an easy refutation in
$NS_{\mathbb{R}}$
- preserved by lifting $n^{O(\log n)}$

but requires CP proofs
of size $2^{n^{\Omega(1)}}$

$\exists F$ s.t. $NS_{\mathbb{R}}$ much better than CP

Lower bounds for SA and SOS

Given $p_1 \geq 0, \ldots p_m \geq 0$ derive $p \geq 0$

SA: $q_0 + \sum_i q_i p_i \equiv_I p$

q_i positive sum of non-neg Juntas

$J_{P,N}(x) = \prod_{i \in P} x_i \prod_{j \in N} \bar{x}_j$

$\bar{x}_i = 1 - x_i$

SOS: $q_0 + \sum_i q_i p_i \equiv_I p$

q_i is a sum of squares

Lower bound method (related d-designs for NS proofs)

$p_1 = 0 \quad p_m = 0$

d-design $D: \mathbb{F}[x_1, \ldots x_n] \to \mathbb{F}$

D linear s.t. $D(1) = 1$

$D(r_i \cdot p_i) = 0 \quad \forall i \in [m]$

$\deg(r_i p_i) \leq d$.

SA Pseudoexpectation of deg d: linear $\tilde{\mathbb{E}}$ (mod I)

(1) $\tilde{\mathbb{E}}(1) = 1$

(2) $\tilde{\mathbb{E}}(J_{P,N}(x)) \geq 0$

(3) $\tilde{\mathbb{E}}(J_{P,N}(x) \cdot p_i(x)) \geq 0$

if $\deg \leq d$

A

Apply $\tilde{\mathbb{E}}$ to SA line of deg d

LHS: $\underbrace{\tilde{\mathbb{E}}(q_0)}_{\geq 0} + \underbrace{\tilde{\mathbb{E}}(\sum q_i p_i)}$

impossible

$\therefore$ SA refutation of deg d

RHS: $\tilde{\mathbb{E}}(-1) = -1$

Thm If $\exists$ deg d SA refutation

$\Rightarrow$ no deg d SA pseudo-expectation

Fact: This is an

$\Longleftrightarrow$

Farkas Lemma in linear programming

LP: $Y_{P,N}$ stands for the value of $J_{P,N}$

SOS degree 2d pseudo-expectation

- $\tilde{\mathbb{E}}(1) = 1$
- $\tilde{\mathbb{E}}(q^2(x)) \geq 0$ $\forall$ poly q of deg $\leq d$
- $\tilde{\mathbb{E}}(\underbrace{q^2(x)\, p_i(x)}_{\leq d}) \geq 0$ $\forall$ poly q of deg $\leq \frac{d - \deg(p_i)}{2}$

Thm $p_1 \geq 0, \ldots p_m \geq 0$ has no SOS deg 2d refutation iff it has a deg 2d-pseudoexpectation