CSE599S Proof Complexity & Applications

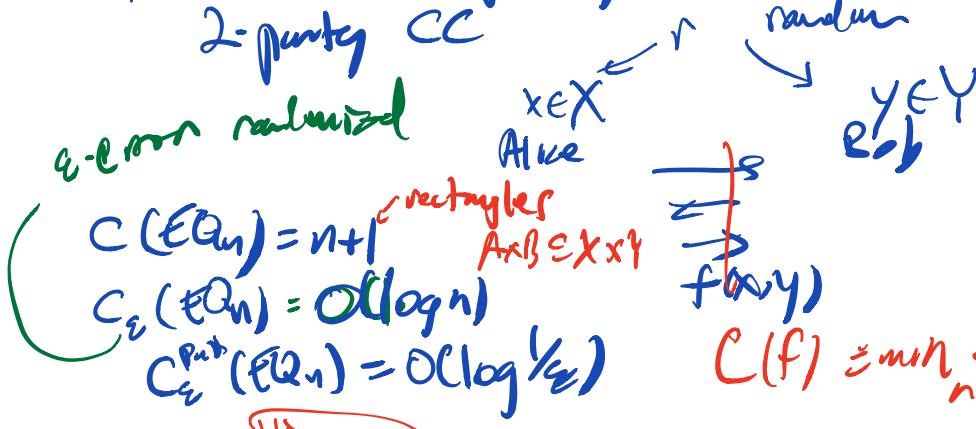
Lecture 15 23 Nov 2020

Goal: Lower bounds for strong tree-like proof systems
e.g. Cutting Planes (general lata)
Positivstellensatz Calculus of degree $\leq d$

Communication Complexity

2-party CC

ε-error randomized

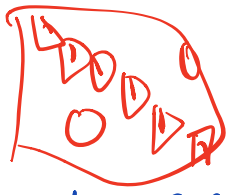


$C(EQ_n) = n+1$

$C_\varepsilon(EQ_n) = O(\log n)$

$C_\varepsilon^{Pub}(EQ_n) = O(\log 1/\varepsilon)$

$C(f)$ = min # of bits needed



k-party CC

$X_1 \quad \cdots \quad X_k$

$\Psi \qquad\qquad \Psi$

$x_1 \qquad\qquad x_k$

$f(x_1, \ldots, x_k)$

Number-In-Hand (NIH)
- i^{th} party has x_i

Number-On-Forehead (NOF)
- i^{th} party can see everything but x_i
- x_i is on the i^{th} party's forehead.

$C_\varepsilon^{k,NOF}$ $C^{k,NIH}$ $C_\varepsilon^{k,NOF}$ $C_\varepsilon^{k,NIH}$

eg. 2-party CC

Set Disjointness

$X = Y = \{0,1\}^n$

$x \in X$ x subset of $[n]$

$y \in Y$ $\approx$ subset of $[n]$

$DISJ_n(x,y) = \begin{cases} 1 & \text{if sets intersect} \\ 0 & \text{if sets are disjoint} \end{cases}$

i.e. $= \begin{cases} 1 & \text{if } \exists i \in [n] \ x_i = y_i = 1 \\ 0 & \text{o.w.} \end{cases}$

Yao #'s of applications

$C(DISJ_n) = n+1$

$C_\varepsilon(DISJ_n)$ is $\Omega(n)$

$UDISJ_n$: promise at most one i s.t. $x_i = y_i = 1$

$C_\varepsilon(UDISJ_n)$ is $\Omega(n)$

k-party

$UDISJ_n^k(x^1, x^2, \ldots, x^k)$

$DISJ_n^k(x^1, x^2, \ldots, x^k) = 1$ iff $\exists i$ s.t. $x_i^1 = x_i^2 = \ldots = x_i^k = 1$

Thm (Shevtsov)

$$C_{\varepsilon}^{k,NOF}(UDISJ_n^k)$$

if $\Omega\left(\frac{\sqrt{n}}{k2^k}\right)$

• (Rao, Yehudayoff)

$$C^{k,NOF}(UDISJ_n^k)$$

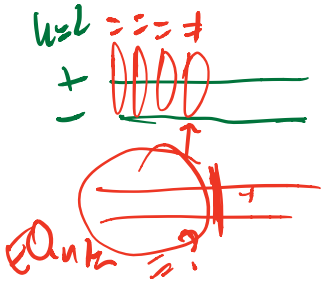
if $\Omega\left(\frac{n}{k4^k}\right)$

Example $GT_{n,k}$: Takes k signed integers $y_1, \ldots, y_k$ in $(-2^n, 2^n]$ and outputs 1 iff $y_1 + y_2 + \cdots + y_k \geq 0$

NIH

Trivial: $C^{k,NIH}(GT_{n,k}) \leq O(nk)$

Randomized: $C^{k,NIH}_{1/c}(GT_{n,k}) \leq O(k \log^2 n)$ †



find 1st place where bits differ - binary search

†

p polynomial of degree $(k-1)$

$p(x_1, \ldots, x_n) \geq 0$

Arbitrary partition of $[n]$ into $A_1 \cup \cdots \cup A_k = [n]$

NOF: i^{th} player has x_j for $j \in A_i$ on forehead.

Is $p(x_1, \ldots, x_n) \geq 0$?

Observe: every monomial in p can be seen by one of the players

$x_{i_1} \cdots x_{i_{k-1}}$ involves only $k-1$ players' foreheads

Can split p into k parts

$p(x_1 \cdots x_n) = p_1(x_{\overline{A_1}}) + p_2(x_{\overline{A_2}}) + \cdots + p_k(x_{\overline{A_k}})$

player 1 Y_1 ; player 2 Y_2 ; player k Y_k

eg 3 players

$x_1 x_2 x_3 + 2 x_3 x_4 x_5 - 3 x_1 x_2 x_5$

How big y_i? At most $n\binom{n}{k}$ terms

$|y_i| \le \binom{n}{k}$ max coeff

wlog. max coeff fits in $\binom{n}{k}\log\binom{n}{k}$ bits

$\Rightarrow O(k^4 \log^2 n)$ protocol

NOF.

$k \log^2\binom{n}{k}$

Communication Complexity for Search_F

Search_F for unsat $F = \bigwedge_i C_i$:
on input x find i s.t. $C_i(x) = 0$

Theorem Let P be a dynamic proof system s.t. (for all $n \geq 2$)
each line of P gives a Boolean function that has k-party CC at most $C(n)$
(and error at most $\varepsilon(n)$)

$\Rightarrow$ if CNF formula F tree-like proof size $\leq S$ in P
then k-party CC of Search_F is $O(C(n) \cdot \log S)$
at error is $O(\varepsilon(n) \cdot \log S)$

eg Clauses
linear inequality
poly :-

under any partition of input vars

eg. Resolution: $x_1 \vee x_2 \vee \bar{x}_3 \vee \cdots \vee x_m$ clauses have 2-party CC 2 bits

Cutting Planes: $a_1 x_1 + \cdots a_n x_n - b \geq 0$ 2-party

wlog a_i have $n \log n$ bit
a_i have $\log n$ bits CP*

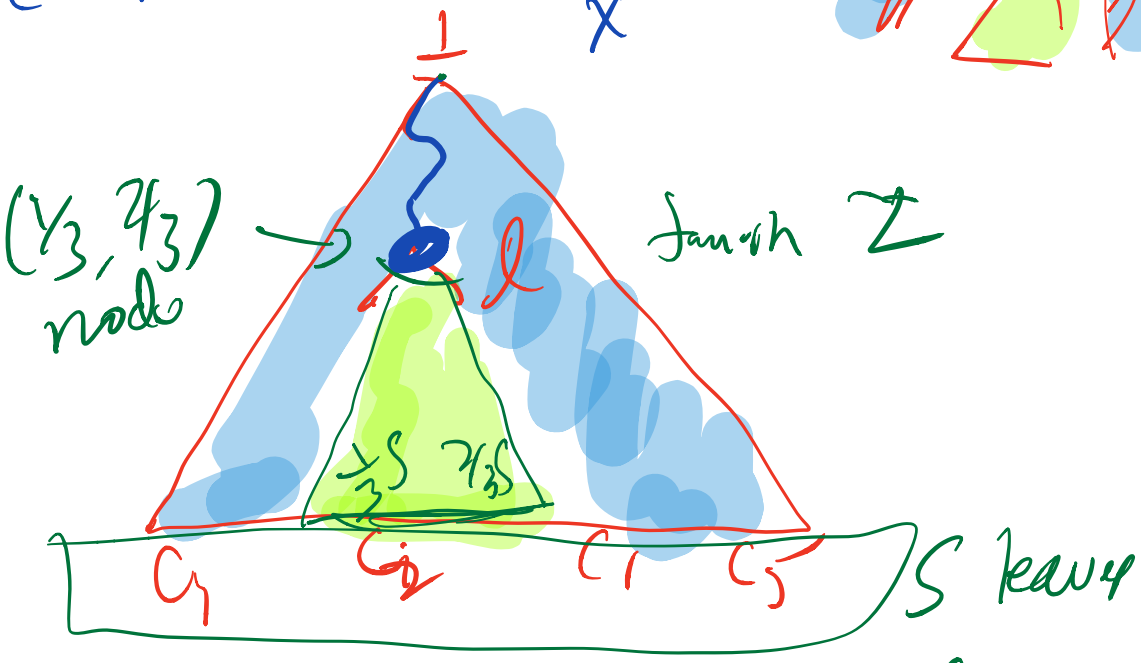
$O(\log^2 n)$ randomized for fixed $\varepsilon = 1/n$

$O(\log n)$

Positivstellensatz Calculus — deg d polys ≥ 0 — $O(d^4 \log^2 D)$ randomized.

Proof of Theorem

refutation in P_x



Find a node in proof with between $\frac{1}{3}S$ and $\frac{2}{3}S$ leaves below.

Take the child with more descendants until $\leq \frac{2}{3}S$ descendants

Alg: evaluate ℓ on input x.

if $\ell(x)=0$
recurse on subtree rooted at ℓ

if $\ell(x)=1$
recurse on r_{yt}

# of leaves $\leq (4/3)^S$

$O(\log S)$ steps

Example for which bipartite randomized NOF CC is larger

$TS(G,\ell)$

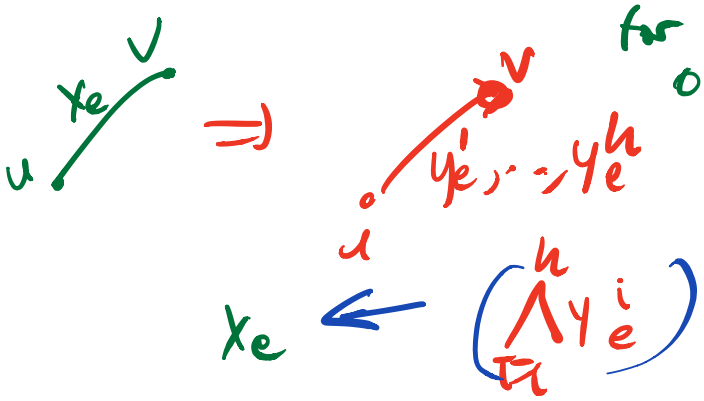
parity constraints at each vertex: match ℓ

Tseitin formula
G labelling ℓ: odd
low degree Δ
$2^{\Delta-1}$ clauses per vertex

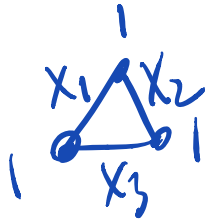
$TS(G, \ell)^{(\wedge h)}$:

G

substituted $\wedge$ of h new vars for each edge of G



expand into clauses



$x_1 \vee x_2$ $\quad \bar{x}_1 \vee \bar{x}_2$

$x_1 \vee x_3$ $\quad \bar{x}_1 \vee \bar{x}_1$

$x_2 \vee x_3$ $\quad \bar{x}_2 \vee \bar{x}_3$

$TS(\Delta, \vec{1})$

$(y_1^1 \wedge y_1^2) \vee (y_2^1 \wedge y_2^2)$ $\qquad TS^{(\wedge 2)}(\Delta, \vec{1})$

$\Downarrow$

$(y_1^1 \vee y_2^1) \wedge (y_1^1 \vee y_2^2) \wedge (y_1^2 \vee y_2^1) \wedge (y_1^2 \vee y_2^2)$

deg Δ

$2^{\Delta - 1}$ $\quad \Delta$ vars / clause

$k^{\Delta} \cdot 2^{\Delta - 1}$ $\quad \Delta$

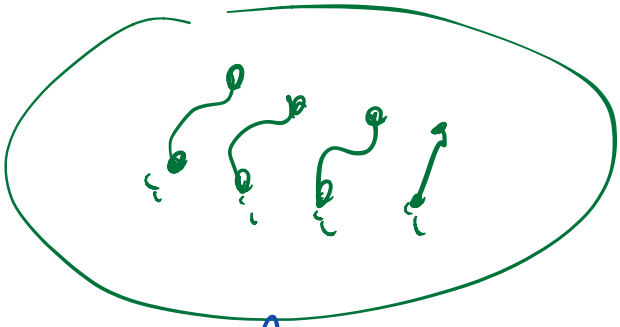
For Thm Solving & Search $TS(G_n, \ell)^{(AM)}$ implies an efficient protocol

$UDIST^{k}_{m}$

$m \sim n^{1/3}/\log n$

Cor $TS(G_n, \ell)^{(AM)}$ requires Positivstellensatz Calculus proofs of size $2^{n^{\Omega(1)}}$ for deg $\leq k-1$. R

G $\Delta = O(\log n)$ degree-expander



Open Any general lower bound for Pos. Calculus

Lovasz-Schrijver

deg 2 version of

LS

positivstellensatz

calculus

CB

Next time

Cutting planes

General proofs

Interpolation: