CSE 599S Proof Complexity and Applications

Lecture 8 26 October 2020

Algebraic Proof Systems

Advantage: Non-clausal representation of constraints

e.g. PHP^m_n $\bigvee_{j=1}^n x_{ij}$ $\prod_{j=1}^n \overline{x_{ij}}=0$

deg n Clausal translation

deg 2 P_i Pigeon deg 1 $\sum_{j=1}^n x_{ij}-1=0$ for $i\in[m]$

Hole $x_{ij}\cdot x_{i'j}=0$ $\forall\, i\neq i'\in[m]$, $j\in[n]$

"almost" functional

$f_1 \cdots f_m$

NS proof

$\sum_{i=1}^n f_i g_i \equiv_I 1$

multilinearize

$\mathbb{F}$ = integers mod p

Functional $x_{ij}\cdot x_{ij'}=0$ $\forall\, i\in[m]$, $j\neq j'\in[n]$

Q_j Onto $\sum_{i=1}^{n+1} x_{ij}-1=0$

Bijective-PHP^{n+1}_n

Prop This version of Bijective-PHP^{n+1}_n has a degree 1 refutation NS over any field.

n # pigeon

n # holes

$$\sum_{i,j} X_{i,j} = \#\text{ free vars}$$

$$\sum_{i=1}^{n+1} \underbrace{\sum_{j=1}^{n} X_{ij}}_{} = \sum_{i=1}^{n+1} (P_i+1) = n+1$$

$$= \sum_{j=1}^{n} (Q_j+1) = n$$

$$\boxed{-\sum_{i=1}^{n+1} P_i + \sum_{j=1}^{n} Q_j = 1}$$

Count^{pn+1}_{p}

"can't partition $pn+1$ elements into sets of size p."

Thm NS in fields of char p can prove Count^{n}_{p} in degree 1 but it requires large deg in fields of char $q \neq p$

$\to$ field matters

Lower Bounds for NSATZ - Proofs

Def^n Vector $\vec{F} = (f_1, \dots, f_m)$ of polys

a d-design for $\vec{f}$ is a linear mapping: $D: \mathbb{F}^{\leq d}[x_1, \dots, x_n] \to \mathbb{F}$ s.t.

$\leftarrow$ wlog. multilinear

- $D(1) = 1$ ✓
- $\forall$ poly $g \in \mathbb{F}[x_1, \dots, x_n]$ s.t. $\deg(f_i \cdot g) \leq d$ $\quad f_i \in \vec{f}$

$D(f_i \cdot g) = 0$

$\uparrow$ wlog g is monomial

linear eqn

Prop If $\vec{f}$ has a d-design over $\mathbb{F}$ then $\vec{f}$ requires $NS_{\mathbb{F}}$ degree $\geq d+1$

Proof $NS_{\mathbb{F}}$ proof of deg $\leq d$

$$\sum_i f_i g_i = 1 \quad (*)$$

$\forall i \quad \deg(f_i g_i) \leq d$

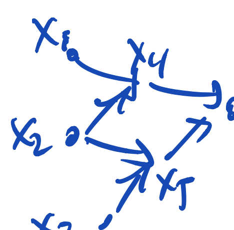
Apply D on both sides

LHS $= 0$ $\qquad$ RHS $= 1$ $(*)$ fails $\mathbb{F}$

Notation $X_S = \prod_{i \in S} x_i$ $\qquad$ $D(X_S)$ for all subsets S with $|S| \leq d$

$\binom{n}{\leq d}$ $\qquad$ shorthand $D(S)$

Pebbling Formulas $\quad PEB(G)$



d.a.g $\quad G$

single sink

$x_v \quad \forall v \in V(G)$

- v source $\quad x_v$
- t sink $\quad \overline{x}_t$
- v $\quad \bigvee_{u \in pred(v)} \overline{x}_u \vee x_v$

Special case $\quad$  $\quad P_n$

IND_n " induction principle" $\quad x_1, \overline{x}_1 \vee x_2, \overline{x}_2 \vee x_3, \ldots \overline{x}_{n-1} \vee x_n$

Thm $NS_{\mathbb{F}}$ degree of IND_n is $\lceil \log_2(n+1) \rceil$

$NS_{\mathbb{F}}$ degree of $PEB(G)$ is the "reversible pebbling number" of G.

— ordinary pebble #

for P_n $= 2$

n nodes

n

$\sim \sqrt{n}$ pebbles

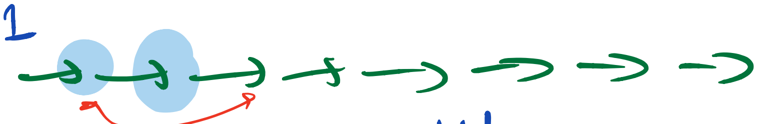
$\Theta(n/\log n)$ bounded degree

reversible pebbling

- If pebble on all pred of v can pebble v.
- If pebble on all pred of v can remove a pebble from v.

G:

1



1

3

p pebbles

$2^p - 1$ steps

Design for PEB(G) given a lower bound on # of pebbles to reversibly pebble sink of G.

$D(S)$

S configuration of $\leq d$ pebbles where $d <$ reversible pebble #

$D(S)=1$ [Some S are reachable from empty configuration

$D(S)=0$ [These are not (including any S that contains t)

$D(\phi)=1$

Polynomial Calculus

Size-Degree relationship

monomials

x $\quad PC_{\mathbb{F}}(\vec{F})$ min size of a $PC_{\mathbb{F}}$ refutation of $\vec{F}$

$x, \bar{x}$ $\quad PCR_{\mathbb{F}}(\vec{f})$ min size of a $PCR_{\mathbb{F}}$ ... of $\vec{F}$

$PCdeg_{\mathbb{F}}(\vec{f})$ degree

Thm F CNF. If $PC(F) \leq S$ or $PCR(F) \leq S$

n vars

then $PCdeg(F) \leq 2\sqrt{2n \ln(S)} + w(F)$

Cor

$$PCR(F) \geq e^{\frac{[PCdeg(F) - w(F)]^2}{8n}}$$

n vars

Gaussian Width

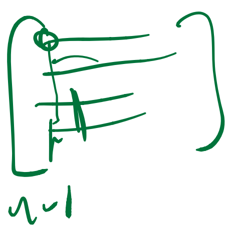
System of linear equations

unsat

$$x_1 + x_2 + x_3 = 1$$
$$x_1 - x_2 + x_3 = 2 \quad 2x_1 + 2x_3 = 3$$
$$x_1 + x_3 = 2 \rightarrow 2x_1 + 2x_3 = 4$$

$\mathcal{L}$ Gaussian elimination to prove unsat

each new line is a linear combination of two previous lines $0=1$



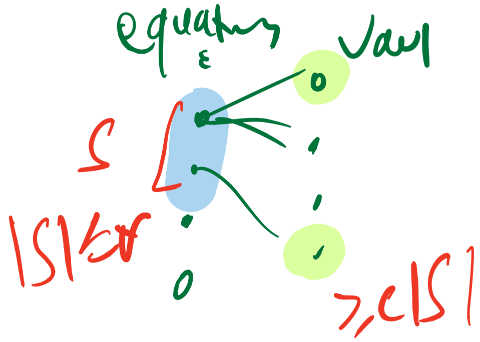
Contradiction $\boxed{0=1}$

lines in Gaussian refutation of system

$O(n^2)$

Gaussian Width: max # of vars in a line of the proof.

$w_G(\mathcal{L})$



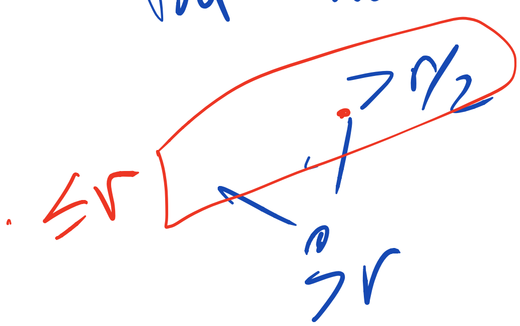
$G_{\mathcal{L}}$

(r, c)-boundary expander

Thm If $G_{\mathcal{L}}$ is an (r,c)-boundary expander then

$$w_G(\mathcal{L}) \geq rc/2$$

Pf min unsat collection of equations has size > r



QED

If G is an (r,c)-edge expander

view TS(G, ℓ) as system of linear equations mod 2

$$w_G(TS(G,\ell)) \geq rc/2$$