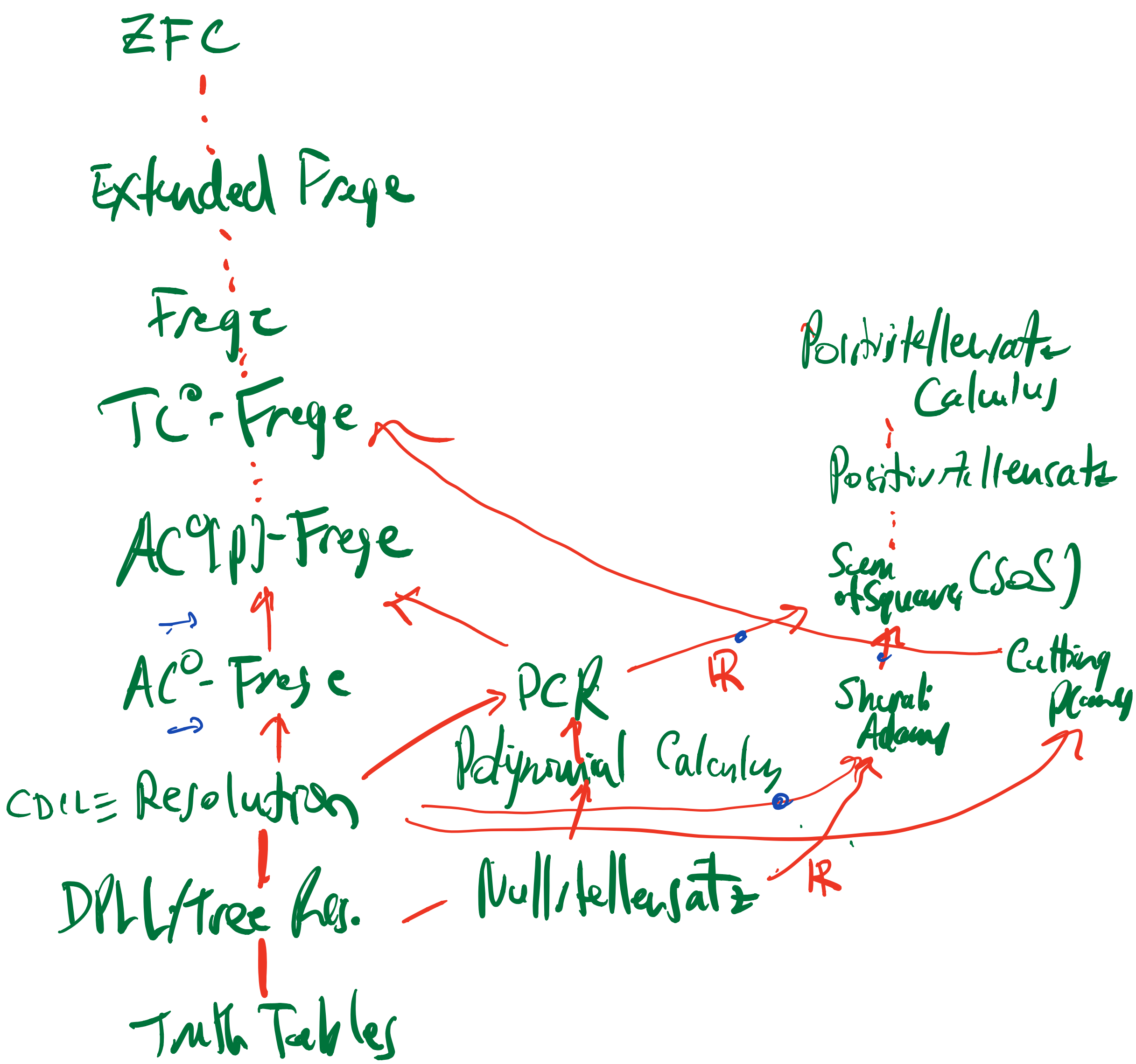
Lecture 13 CSE 599S Proof Complexity & Applications

Logical	Algebraic	SemiAlgebraic
clause C	polynomial $p_C, \bar{p}_C = 0$	$\ell_C \geq 0$, $\bar{\ell}_C \geq 0$ (or $p_C, \bar{p}_C = 0$)



Sherali-Adams Proofs (recap)

non-negative junta : monomial of bounded degree

$\prod_{i \in P} x_i \prod_{j \in N} (1-x_j) \geq 0$ in $x_i, \bar{x}_i$

$\boxed{J_{P,N}} \longrightarrow \prod_{i \in P} x_i \prod_{j \in N} \bar{x}_j$

Given $\{h_1 \geq 0, \dots h_m \geq 0; f_1 = 0, \dots f_n = 0\}$

always include $x_i^2 - x_i = 0$, $x_i + \bar{x}_i - 1 = 0$

derive $h \geq 0$ a

$$\boxed{g_0 + \sum_{i \in [m]} g_i h_i + \sum_{i \in [n]} e_i f_i = h}$$

arbitrary polys

where g_i are of the form

$$\sum_{(P,N)} a_{P,N} J_{P,N} \quad \text{where } a_{P,N} \geq 0$$

$g_i \geq 0$

degree, size = # monomials, bitsize total # of bits

Nsatz : derive -1

Can derive $-\bar{p}_c$ in degree $|c|$ for $l_c \geq 0$ $\Rightarrow$ SA simulates Nsatz

Theorem If CNF F has a resolution refutation of width ω and size S then it has an SA refutation of degree $\leq \omega+1$ and size poly(S, ω). (with dual vars)

Proof Prove by induction that for every clause C in the resolution proof can derive poly $-\bar{P}_C$ in degree $\leq \omega+1$

Start: $l_C \geq 0 \Rightarrow -\bar{P}_C$

Proof step: argue by induction for each resolution step

$$-\bar{P}_{A \cup x}, \; -\bar{P}_{B \cup \bar{x}}$$
$$\Downarrow$$
$$-\bar{P}_{A \cup B}$$

details HW.

At end can get $-\bar{p}_{\perp} = -1$

i.e. $-1 \geq 0$ which

a SA contradiction ☒

Sum of Squares (SoS) Proofs

idea: the square of any polynomial is always ≥ 0.

Given $\{h_1 \geq 0, \ldots, h_m \geq 0 \,;\, f_1 = 0, \ldots f_m = 0\}$ ⊛

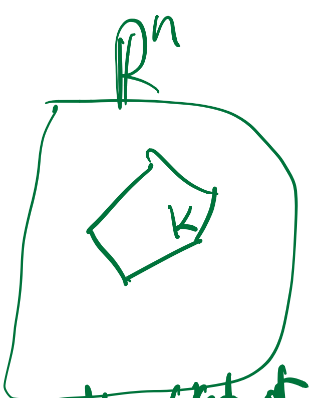
Goal: infer $h \geq 0$.

SoS proof of this

$$q_0 + \sum_{i \in [m]} q_i h_i + \sum e_i f_i = h$$

q_i is a sum of squares of polynomials

$q_i \geq 0$



K subset of $\mathbb{R}^n$ defined by ⊛

$h \geq 0$ on K.

Assume start with $l_C \geq 0$

and f_i are just the Boolean $x_i^2 - x_i$

For a CNF $F = \bigwedge_i C_i$ SOS derivation of $h \geq 0$

$$q_0 + \sum_i q_i \, l_{C_i} \equiv_{\mathcal{I}} h$$

multilinearize apply dual if needed

q_i: sum of squares of polys.

refutation $h = -1$.

$$\boxed{q_0 = \sum_j p_j^2}$$

Prop Every non-neg Junta g of degree d

$$g = q + \sum_{j \in [n]} e_i (x_j^2 - x_j)$$

when q is square

$\deg(g), \max_j(\deg(e_i) + 2) \leq 2d$

Proof

$$\underset{g}{x} = \underset{q}{x^2} - \underset{e = -1}{1} \cdot (x^2 - x)$$

$$\underset{\deg 1}{(1-x)} = \big(\underset{1 - 2x + x^2}{1-x}\big)^2 - 1 \cdot (x^2 - x)$$

RHS deg 2.

multiply to get larger degree ∎

Thm There is a deg 3 polysize SoS refutation of PHP^m_n

Proof For $j \in [n]$ x_{ij}

$$\underbrace{\Big(1-\overbrace{\sum_i x_{ij}}^{a}\Big)^2}_{q_0} + \sum_{\substack{i,i'\in[m]\\ i\neq i'}} \underbrace{x_{ij}^2}_{q_{ii'j}}\underbrace{(1-x_{ij}-x_{i'j})}_{\text{axiom}}$$

cancel

$$1+2\sum_{i\neq i'} x_{ij}x_{i'j} + \sum_i x_{ij}^2 - 2\sum_i x_{ij} = -\sum_i x_{ij}$$

$$x_{ij}^2(1-x_{ij}) \equiv 0$$

$$(1-a)^2 = 1-2a+a^2$$

$$\therefore\ x_{ij}^2(1-x_{ij}-x_{i'j}) \equiv -x_{ij}x_{i'j}$$

Hole $\boxed{1-\sum_i x_{ij} \geq 0}$ for each j

n

PHP^m_n $\sum_j x_{ij} - 1 \geq 0$ pigeon clauses

m

Pigeon $\sum_i \sum_j x_{ij} - m \geq 0$

Hole $n - \sum_i \sum_j x_{ij} \geq 0$

LHS < 0

$\therefore n - m \geq 0$

but $m > n$

contradiction

Thm (Buchholz)

$PC_{\mathbb{R}}$ proof	$\Rightarrow$	SoS proof
deg d		deg $2d$
size S		size $S^{O(1)}$
bitsize B		bitsize $B^{O(1)}$
derivation of f		derivation of $-f^2$

Proof Let $f_1 \cdots f_m ; f_{m+1} \cdots f_{\#}$ be a be a $PC_{\mathbb{R}}$ derivation and assume every coefficient c in proof $1/K \leq 4c^2 \leq K$.

Claim $\exists$ sequence of $q_{m+1} - q_T$ of

$\deg(q_i) \le d$ and

for every $t \le T$ we get

an expression $\mathcal{E}_t$

$$\boxed{\mathcal{E}_t = \sum_{i=1}^{m} -(c_i f_i)\cdot f_i + \sum_{i=m+1}^{t} c_i q_i^2 \equiv -f_t^2}$$

$\mathcal{P} = 0$

$1/K^t \le c_i \le K^t$ and

every coefficient of q_i is $\le 2c^2$

Proof $\quad$ PCR $f_i = 0$

$i = 1 \ldots m$

$\mathcal{E}_i = (f_i) f_i \equiv -f_i^2$

$c_i = 1$ not 0.

PC$_{\mathbb{R}}$ rules: multiply by x_j

$f_t = x_j \cdot f_{t'}$ $\quad t' < t$

by IH. $\mathcal{E}_{t'} = \sum_{i=1}^{m} -(c_i f_i) f_i + \sum_{i=m+1}^{t'} c_i q_i^2 = -f_{t'}^2$

$\boxed{\deg(f_{t'}) \le d-1}$

Set $q_t = (1 - x_j) f_{t'}$ $\quad \deg(q_t) \le d$

$$q_t^2 = (1-x_j)^2 f_{t'}^2$$
$$= (1-2x_j+x_j^2) f_{t'}^2$$
$$= (1-x_j^2) f_{t'}^2 = f_{t'}^2 - \underbrace{x_j^2 f_{t'}^2}$$
$$= f_{t'}^2 - f_t^2$$

$$\Sigma_t = \Sigma_{t'} + q_t^2$$
$$= -f_{t'}^2 + (f_{t'}^2 - f_t^2) = -f_t^2$$

additive $f_t = a f_{t'} + b f_{t''}$

by IH $\underline{\Sigma_{t'} = -f_{t'}^2}$ $\quad \Sigma_{t''} = -f_{t''}^2$

Set $q_t = a f_{t'} - b f_{t''}$ dagged

$$q_t^2 = a^2 f_{t'}^2 - 2ab f_{t'} f_{t''} + b^2 f_{t''}^2$$
$$f_t^2 = a^2 f_{t'}^2 + 2ab f_{t'} f_{t''} + b^2 f_{t''}^2$$
$$f_t^2 + q_t^2 = 2a^2 f_{t'}^2 + 2b^2 f_{t''}^2$$
$$= -2a^2 \Sigma_{t'} - 2b^2 \Sigma_{t''}$$

$$\varepsilon_t = 2a^2 \varepsilon_{t'} + 2b^2 \varepsilon_{t''} + q_t^2$$

$$\boxed{\varepsilon_t \equiv -f_t^2}$$

coefficient

$\leq 4 \max(a^2, b^2)$

$\blacksquare$