CSE 599 S Proof Complexity & Applications

Lecture 19 7 Dec 2020

Recall: Degree d SOS pseudoexpectation $\tilde{\mathbb{E}}$ for $\mathcal{P} = \{p_1, \ldots, p_m\}$. linear map mod ideal $I = \langle x_i^2 - x_i : i \rangle$

$\tilde{\mathbb{E}}[x_S] = y_S \quad \forall S \quad |S| \le T$

- $\tilde{\mathbb{E}}[1] = 1$ $\qquad \tilde{\mathbb{E}}, \tilde{y} \in \Sigma_d^{SOS}$ set of all such $\tilde{\mathbb{E}}$
- $\tilde{\mathbb{E}}[q^2(x)] \ge 0 \qquad \deg q \le d/2$
- $\tilde{\mathbb{E}}[q^2(x)\, p_i(x)] \ge 0 \qquad p_i \in \mathcal{P}.\ \deg q \le \frac{d - \deg(p_i)}{2}$

$\boxed{(M_{\tilde{\mathbb{E}}})_{ST} = \tilde{\mathbb{E}}(x_{S \cup T}) \text{ is PSD}}$

$\binom{n}{\le d} \times \binom{n}{\le d}$ matrix

± 1 version $\quad z_i^2 = 1 \qquad z_i = 1 - 2x_i \qquad z_i^2 = 1$

Deg d SOS pseudoexpectation $\tilde{\mathbb{E}}$ for $\mathcal{P}$
linear map mod ideal $I' = \langle z_i^2 - 1 : i \rangle$

$\tilde{\mathbb{E}}[z_S]$

- $\tilde{\mathbb{E}}(1) = 1$
- $\tilde{\mathbb{E}}[q^2(z)] \ge 0 \qquad \deg q \le d/2$
- $\tilde{\mathbb{E}}[q^2(z)\, p_i(z)] \ge 0 \qquad \deg q \le \frac{d - \deg(p_i)}{2}$, $\ p_i \in \mathcal{P}$

$\boxed{\forall q \quad q^T M q \ge 0}$

$(M_{\tilde{\mathbb{E}}})_{ST} = \tilde{\mathbb{E}}(z_{S \oplus T})$ ← symmetric difference

is PSD

---

recall Gaussian width of mod 2 equations

$x_1 \oplus x_2 \oplus x_3 = 1$

$x_2 \oplus x_3 \oplus x_4 = 0$

min ~~length~~ width of derived equation that yields a contradiction using linear combos of original equations

e.g. Tseitin formulas

Random 3-XOR width $\Omega(n)$

$\underbrace{x_1 \oplus x_3 \oplus x_4 \oplus x_5 = 1}_{\text{width } 4}$

Tseitin expander $\Omega(n)$

★ Before: PC degree of mod 2 equations $\doteq$ Gaussian width

Now Thm: SOS degree of mod 2 equations $\geq$ Gaussian width.

Proof use ± 1 version

(mod 2 equations in x_i $\xrightarrow{\text{same as PC}}$ product equations in z_i)

Suppose Gaussian width $> d$

we'll define deg d pseudo-expectation $\tilde{\mathbb{E}}$ for set of equations

ρ equations $x_i \oplus x_j \oplus x_k = b_e$

$\Downarrow$

$z_i z_j z_k = (-1)^{b_e}$

For each initial equation $\sum_{i \in S} x_i \equiv b_e \mod 2$

want $\tilde{\mathbb{E}}(z_S) = (-1)^{b_e}$

Direct construction more generally:

$\tilde{\mathbb{E}}$ will map every z_S to $\{0, 1, -1\}$ ($\in D$)

Start

Let $D \leftarrow \{\emptyset\}$, $\tilde{\mathbb{E}}[1] \leftarrow 1$

For all axioms e of form: $z_{S_e} = (-1)^{b_e}$

$D \leftarrow \{S_e\} \cup D$, $\tilde{\mathbb{E}}[z_{S_e}] = (-1)^{b_e}$

while $\exists\, S, T \in D$ s.t. $|S \oplus T| \le d$
and $S \oplus T \notin D$
$D \leftarrow D \cup \{S \oplus T\}$
$\tilde{\mathbb{E}}[z_{S \oplus T}] \leftarrow \tilde{\mathbb{E}}[z_S] \cdot \tilde{\mathbb{E}}[z_T]$

how does this relate to equations involving S, T

For all other $S \notin D$
$\tilde{\mathbb{E}}[z_S] \leftarrow 0$

exactly Gaussian operation

Claim: Since $d \leftarrow$ Gaussian width
we never get a

consistent if $S \oplus T = U \oplus V$
$|S \oplus T| \le d$, $|S|, |T|, |U|, |V| \le d$

$$\tilde{\mathbb{E}}[z_S] \cdot \tilde{\mathbb{E}}[z_T] = \tilde{\mathbb{E}}[z_{S \oplus T}] \overset{?}{=} \tilde{\mathbb{E}}[z_{U \oplus V}] = \tilde{\mathbb{E}}[z_U] \cdot \tilde{\mathbb{E}}[z_V]$$

✓

$(M_{\tilde{\mathbb{E}}})_{ST} = \tilde{\mathbb{E}}[z_{S \oplus T}]$ is PSD

Claim vectors v_S for all $S \subseteq \binom{[n]}{\le d}$
s.t. $\tilde{\mathbb{E}}[z_{S \oplus T}] = v_S^T \cdot v_T$

ie $\underbrace{\begin{array}{c|c|} & \\ S & v_S \\ & \end{array}}_{V} \; \underbrace{\begin{array}{|c|} v_T \end{array}}_{V^T} = M_{\tilde{\mathbb{E}}}$

$q^T M_E q = q^T V \cdot \underline{V^T q} = w^T \cdot w = \|w\|_2^2 \geq 0$

for $w = V^T q$

$\therefore M_E$ is PSD

V_S vector

Equivalence classes of sets S:

$S \sim T$ iff $S \oplus T \in D$

reflexive $S \oplus S = \phi$ ✓

symmetric defn ✓

$S \sim T$ and $T \sim U$

$\underline{S \oplus T \in D}$ $\underline{T \oplus U \in D}$

$(S \oplus T) \oplus (T \oplus U)$

$= S \oplus U \in D$ ✓

transitive

Vector V_S:

One index e for each equiv class in $\sim$

$V_S = [0,0,0,\ldots,\underset{\uparrow}{E[z]},0,0,0]$

equiv class of S

- S, T in same equiv class

$$V_S^T \cdot V_T = \tilde{\mathbb{E}}[z_S] \cdot \tilde{\mathbb{E}}[z_T]$$
$$= \tilde{\mathbb{E}}[z_{S \oplus T}]$$
since $S \oplus T \in D$

- If S, T in diff equiv classes $S \oplus T \notin D$

$$V_S^T \cdot V_T = 0$$
$$= \tilde{\mathbb{E}}[z_{S \oplus T}]$$

claim is proved $\boxtimes$

Cor SOS requires degree $\Omega(n)$ for

(· random k-XOR, random k-CNF
(· Tseitin on expander graphs

Also size $2^{\Omega(n)}$.

Knapsack: $x_1 + x_2 + \cdots + x_n = r$ e.g. $r = \frac{2k+1}{2}$

Claim refutation requires degree $\geq \min(r, n-r)$

Idea: pseudo-expectation

· symmetric wlog

$\boxed{\tilde{\mathbb{E}}_{new}(x_S) = \sum_{\pi} \tilde{\mathbb{E}}(x_{\pi(S)})}$ $\tilde{\mathbb{E}}[x_S] = f(|S|)$

$$n f(1) \underset{\text{symmetry}}{=} \sum_i \tilde{\mathbb{E}}(x_i) \underset{\text{linearity}}{=} \tilde{\mathbb{E}}(x_1 + x_2 + \cdots x_n) = r$$

$$\therefore f(1) = r/n$$

$$r f(1) = \tilde{\mathbb{E}}[x_1 \underbrace{(x_1 + x_2 + \cdots + x_n)}_{r}] = \tilde{\mathbb{E}}[x_1^2] + \sum_{j \neq 1} \tilde{\mathbb{E}}[x_1 x_j]$$

$$= f(1) + (n-1) \cdot f(2)$$

$$\therefore f(2) = \left(\frac{r-1}{n-1}\right) f(1)$$

$$\therefore f(k) = \frac{\binom{r}{k}}{\binom{n}{k}} \qquad \frac{r(r-1)\cdots(r-k+1)}{k!}$$

Claim this a proper pseudo expectation for deg as claimed

Also hard planted clique

largest clique size $O(\log n)$ → random graph G $G(n, 1/2)$

or ..... + planted clique of size $> \sqrt{n}$

pseudo-calibration

Application of SOS, SA to extension complexity

integer → $\boxed{\text{constraints given a polytope } P^*}$ + weights for a linear objective fn

maxcut, max CSP, ...

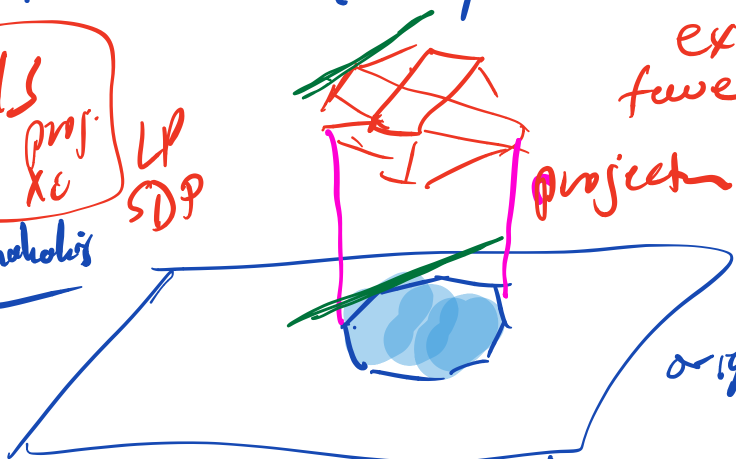
relax to rational P + some weight

extra vars.
fewer constraints

Y_S
Y_i proj. to X_i

LP
SDP

Yannakakis



MST

SA is a special case of extending LP

SOS . . . . SDP

Chan, Lee, Raghavendra Steurer: 2013 LP extension

For $d \le \frac{\log n}{\log\log n}$ size $n^{o(d)}$

$\Rightarrow$ degree d SA derivation

for any CSP

Kothari, Meka, Raghavendra 2016

Also holds for d up to $\Omega(n)$

[Lee, Raghavendra-Steurer 2015] SDP

For $d \le n^{\varepsilon}$ size $n^{o(d)}$ extension

$\exists$ degree d SOS derivation

Cor TSP, Clique $2^{\Omega(n^{\varepsilon})}$ size lower bound

Proof Idea: reduction to the SOS Knapsack lower bound $\boxed{}$

SA captures LP

SOS captures SDP

unconditional