Lecture 10

SOS proof system

polynomials $p_1(X), \cdots, p_m(X), q(X)$

definition degree-ℓ SOS proof of statement

"$q(X) \geq 0$ over $\{p_1(X) \geq 0, \cdots, p_m(x) \geq 0\}$"

is any finite decomposition $q(X) = \sum_{r=1}^{R} S_r(X)^2 \cdot \bar{P}_r(X)$, where

- $\bar{P}_r$ is product of subset of $\{p_1(X), \cdots, p_m(X)\}$
- $\deg(S_r(X)^2 \cdot \bar{P}_r(X)) \leq \ell$

notation $\vec{p}(X) \geq 0 \vdash_{\ell}^{X} q(X) \geq 0$

examples of SOS proofs

(a) $\vdash_2^{a,b} a \cdot b \leq \frac{1}{2}a^2 + \frac{1}{2}b^2$

as $a \cdot b = \frac{1}{2}a^2 + \frac{1}{2}b^2 - \frac{1}{2}(a-b)^2$

(b) $\vdash_2^{a,b} \langle a, b \rangle \leq \frac{1}{2}\|a\|^2 + \frac{1}{2}\|b\|^2$ $\quad$ * $a = \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix}$ $b = \begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix}$ $\langle a, b \rangle = \sum_i a_i b_i$

(c) $\vdash_4^{a,b} \langle a, b \rangle^2 \leq \|a\|^2 \cdot \|b\|^2$

Justification: $\vdash_4^{a,b} \langle a, b \rangle^2 = \langle a \otimes b, b \otimes a \rangle \overset{(b)}{\leq} \frac{1}{2}\|a \otimes b\|^2 + \frac{1}{2}\|b \otimes a\|^2 = \|a\|^2 \cdot \|b\|^2$

(d) $\vdash_2^{X} \langle x, Mx \rangle \leq \underbrace{\|M\|}_{\text{spectral norm}} \cdot \|X\|^2$ $\quad$ (e) $\vdash_2^{X,M} \langle x, Mx \rangle \leq (1 + \|M\|_F^2) \cdot \|X\|^2$

$$
\begin{aligned}
\vdash \langle x, Mx \rangle &\overset{(b)}{\leq} \frac{1}{2}\|x\|^2 + \frac{1}{2}\|Mx\|^2 \\
&= \frac{1}{2}\|x\|^2 + \frac{1}{2}\sum_i \langle M_i, x \rangle^2 \\
&\overset{(c)}{\leq} \frac{1}{2}\|x\|^2 + \frac{1}{2}\sum_i \|M_i\|^2 \cdot \|x\|^2 \\
&= \frac{1}{2}\|x\|^2 + \frac{1}{2}\|x\|^2 \cdot \|M\|_F^2
\end{aligned}
$$

(f) $\vdash_t^{Z} z_1 \cdot \cdots \cdot z_t \leq \frac{1}{t}(z_1^t + \cdots + z_t^t)$, t even

for $t = 2^p$

$\vdash z_1 \cdots z_t = (z_1 \cdots z_{t/2})(z_{t/2+1} \cdots z_t) \overset{(a)}{\leq} \frac{1}{2} z_1^2 \cdots z_{t/2}^2 \cdot \frac{1}{2} z_{t/2+1}^2 \cdots z_t^2$

divide p times $\quad \vdots$

$\leq \frac{1}{2^p} z_1^{2^p} + \cdots + \frac{1}{2^p} z_t^{2^p}$

(g) $\vdash_t^{A,B} (A+B)^t \leq 2^{t-1} \cdot (A^t + B^t)$

$$
\begin{aligned}
\vdash (A+B)^t &= \sum_{s=0}^{t} \binom{t}{s} \underbrace{A^s B^{t-s}} \\
&\overset{(f)}{\leq} \frac{1}{t}(s \cdot A^t + (t-s) \cdot B^t) \\
&= 2^{t-1} A^t + 2^{t-1} \cdot B^t
\end{aligned}
$$

(h) $X^2 \leq C \cdot X \vdash^{X} X \leq C$, $C \geq 0$ $\quad$ * Divide by X?

$X = \left(\frac{1}{\sqrt{C}} X\right)(\sqrt{C}) \overset{(a)}{\leq} \frac{1}{2}\frac{X^2}{C} + \frac{1}{2}C$ $\quad$ − X is negative?!

$$x^2 \le cX \le \tfrac{1}{2}X + \tfrac{1}{2}C$$

– Not a polynomial operation!

"W looks Gaussian"

$$A(W) = \Big\{ \big\| \underbrace{\tfrac{1}{n}\textstyle\sum W_i^{\otimes t} - \mathbb{E}_{\underline{w}\sim N(0,I_d)}[\underline{w}^{\otimes t}]}_{d^{t/2} \text{ by } d^{t/2} \text{ matrix } E} \big\|_F^2 \le \tfrac{1}{100} \Big\}$$

$$B(\underset{d\times n}{X}, \underset{n\times k}{Z}) = \begin{cases} Z_{ia}^2 = Z_{ia}, \quad \sum_a Z_{ia} = 1 \\ \underbrace{Z_{ia}\cdot Z_{ja}}_{=1\cdot 1}\underbrace{(X_i - X_j)}_{=0} = 0 \end{cases}$$

"X is clustered"

if i,j are same cluster, then $X_i = X_j$

$$\boxed{\begin{array}{l}\underline{\text{Theorem}}\ \text{Suppose } (X^\circ, Y^\circ, Z^\circ) \text{ satisfies} \\ B(X^\circ, Z^\circ) \cup A(Y - X^\circ), \text{ then} \\ A(Y-X), B(X^\circ, Z^\circ) \vdash_{O(t)}^{X,Z} \|X - X^\circ\|_F^2 \le 4t \cdot k^{4/t}\end{array}}$$

$$U = X - X^\circ,\quad W = Y - X,\quad W^\circ = Y - X^\circ \to U = W^\circ - W$$

$\underline{\text{claim 1}}$ $A(W) \vdash_{n}^{X,V} \sum_{i=1}^n \langle U_i, V\rangle^t \le (4t)^{t/2} \cdot \|V\|^t$

$\underline{\text{Proof}}$

$$\frac{1}{n}\sum_{i=1}^n \langle W_i, V\rangle^t = \underbrace{(t-1)!! \cdot \|V\|^t}_{\mathbb{E}_{\underline{w}\sim N(0,I_d)}[\langle \underline{w}, t\rangle^t] = \langle V^{\otimes t/2}, \mathbb{E}[\underline{w}^{\otimes t}]V^{\otimes t/2}\rangle} + \langle V^{\otimes t/2}, E V^{\otimes t/2}\rangle$$

$$= \langle V^{\otimes t/2}, \big(\tfrac{1}{n}\textstyle\sum_{i=1}^n W_i^{\otimes t}\big) V^{\otimes t/2}\rangle$$

$* \ W^{\otimes t} \simeq \underbrace{(W^{\otimes t/2})(W^{\otimes t/2})^T}$

$\langle W, V\rangle^t = \langle V^{\otimes t/2}, \ \cdot \ V^{\otimes t/2}\rangle$

$$\vdash^{E,V} \langle \underbrace{V^{\otimes t/2}}_{X}, \underbrace{E}_{M} \underbrace{V^{\otimes t/2}}_{X}\rangle \overset{(e)}{\le} (1 + \|E\|_F^2)\|V\|^t$$

$$A(W) \vdash^{X,V} \frac{1}{n}\sum \langle W, V\rangle^t \le (t-1)!! \cdot \|V\|^t + (1 + \|E\|_F^2)\|V\|^t$$
$$\le (t-1)!!\|V\|^t + 1.01 \cdot \|V\|^t$$
$$\le t^{t/2} \cdot \|V\|^t$$

$$A(W) \vdash^{W,V} \frac{1}{n}\sum \langle U_i, V\rangle^t = \frac{1}{n}\sum_{i=1}^n \underbrace{(\langle W_i^\circ, V\rangle - \langle W_i, V\rangle)}^t$$
$$\overset{(g)}{\le} 2^{t-1}(\langle W_i^\circ, V\rangle^t + \langle W_i, V\rangle^t)$$
$$\le \underbrace{2^t \cdot t^{t/2}}_{(4t)^{t/2}} \cdot \|V\|^t$$

$\underline{\text{Claim 2:}}$ $B_k(X, Z) \vdash^{X,Z} B_{k^2}(U, Z')$, where $Z'_{iab} = Z_{ia} \cdot Z^\circ_{ib}$

$\underline{\text{Claim 2.2:}}$ $B(X,Z) \vdash Z'_{iab} Z'_{jab}(\langle U_i, U_j\rangle^t - \|U_i\|^t \cdot \|U_j\|^t) = 0$

$\underline{\text{together:}}$

$$A(W), B_k(X, Z) \vdash Z'_{jab} \cdot \|U_j\|^t \cdot \frac{1}{n}\sum_{i=1}^n Z'_{iab} \cdot \|U_i\|^t$$
$$\overset{\text{claim 2}}{=} Z'_{jab} \cdot \frac{1}{n}\sum Z'_{iab} Z'_{jab} \cdot \|U_i\|^t \cdot \|U_j\|^t$$
$$= Z'_{jab} \cdot \frac{1}{n}\sum_{i=1}^n Z'_{iab} Z'_{jab} \langle U_i, U_j\rangle^t$$
$$\overset{\text{claim 2}}{\le} Z'_{jab} \cdot \underbrace{\frac{1}{n}\sum_{i=1}^n \langle U_i, U_j\rangle^t}_{\overset{\text{claim 1}}{\le} (4t)^{t/2} \cdot \|U_j\|^t} \le Z'_{jab} (4t)^{t/2} \cdot \|U_j\|^t$$

$\underline{\text{Sum over all } j \in [n]}$

$$\cdots \vdash \Big(\sum_{i=1}^n Z'_{iab} \cdot \|U_i\|^t\Big)^2 \le (4t)^{t/2} \cdot \Big(\sum_{i=1}^n Z'_{iab} \|U_i\|^t\Big)$$

$$\underbrace{\qquad\qquad}_{X} \qquad\qquad \underbrace{\qquad\qquad}_{X}$$

$$\dots \vdash X^2 \leq C\cdot X$$

$$\dots \vdash X \leq C \longrightarrow \sum \mathcal{Z}'_{iab}\|u\|^t \leq (4t)^{t/2}$$

<u>sum over $a, b \in [k]$</u>

$$A, B \vdash \underbrace{\sum_{a,b}\frac{1}{n}\sum_i \mathcal{Z}'_{iab}\|u_i\|^t}_{=\frac{1}{n}\sum_i \|u_i\|^t} \leq k^2(4t)^{t/2}$$

$$\vdash^{v} \|v\|^2 \leq \frac{2}{t}\frac{\|v\|^t}{C^{t-2}} + \frac{t-2}{t}\cdot C^2 \quad \text{(Fact)}$$

$$A, B \vdash \frac{1}{n}\sum\|u_i\|^2 \overset{\text{fact}}{\leq} \frac{2}{t}\frac{1}{C^{t-2}}\underbrace{\left(\frac{1}{n}\sum_{i=1}^{n}\|u_i\|^t\right)}_{\leq k^2(4t)^{t/2}} + \frac{t-2}{t}C^2 = C^2 = 4t\cdot k^{4/t}.$$

Choose C such that $C^t = (4t)^{t/2}\cdot k^2$

<u>SOS meta algorithm</u>

N-dim. variables X, degree bound $\ell \in \mathbb{N}$, $X_1, \cdots, X_n$

<u>polynomials</u> $p \in \mathbb{R}[X]_{\leq \ell}$, monomial basis $X^\alpha = X_1^{\alpha_1}, \cdots, X_N^{\alpha_N}$

$p = \sum p_\alpha \cdot X^\alpha$ $\qquad\qquad \alpha_1 + \cdots + \alpha_N \leq \ell$

<u>linear functions</u> $L: \mathbb{R}[X]_{\leq \ell} \longrightarrow \mathbb{R}$ $\qquad$ <u>poly. system</u> $A = \{p_1(x) \geq 0, \cdots, p_m(x) \geq 0\}$

$L[p] = \sum L_\alpha \cdot p_\alpha$

<u>algorithm</u>: given A, find linear functions such that $L[1] = 1$

$L[q] \geq 0$ for all q such that $A \vdash_\ell q \geq 0$

and output $\hat{X}$ such that $\hat{X}_i = L[X_i]$

<u>claim</u>: If $A \vdash \|X - X^\circ\|_2^2 \leq C$, then $\hat{X}$ satisfies the same bound $\|\hat{X} - X^\circ\|_2^2 \leq C$.

<u>"pseudo expectation"</u> $L \overset{X}{\underset{\ell}{\models}} A$ (models, satisfies) iff $\forall q \in \mathbb{R}[X]_{\leq \ell}$, $(A \overset{X}{\underset{\ell}{\vdash}} q \geq 0 \Rightarrow L[q] \geq 0)$

and $L[1] = 1$.

<u>atomic functionals L</u>: $\exists X^\circ \in \mathbb{R}^N$, $\forall q \in \mathbb{R}[X]_{\leq \ell}$, $L[q] = q(X^\circ)$

$* \; L[q + q'] = (q + q')(X^\circ) = q(X^\circ) + q'(X^\circ) = L[q] + L[q']$ <u>not atomic</u>

<u>observation</u>: L atomic & $L \models A \Leftrightarrow X^\circ$ satisfies A

<u>Algorithm</u>

$$A \longrightarrow \boxed{\text{find } L \models A} \longrightarrow \hat{X} = L[X] \qquad * \; \|\mathbb{E}[X] - X^\circ\|^2 \leq \mathbb{E}[\|X - X^\circ\|^2] \leq C$$

<u>claim</u>: if $A \overset{X}{\underset{\ell}{\vdash}} \|X - X^\circ\|_2^2 \leq C$, $L \overset{X}{\underset{\ell}{\models}} A$, then $\|L[X] - X^\circ\|^2 \leq C$.

<u>Proof</u>: $u = X - X^\circ$, $\hat{u} = L[u] = L[X] - X^\circ$ constant, L does not change constant.

$$\|\hat{u}\|^2 = \langle \hat{u}, \hat{u} \rangle = \langle \hat{u}, L[u] \rangle = L[\langle \hat{u}, u \rangle]$$

$$\leq L\left[\tfrac{1}{2}\|\hat{u}\|^2 + \tfrac{1}{2}\|u\|^2\right] = \tfrac{1}{2}\|\hat{u}\|^2 + \tfrac{1}{2}L[\|u\|^2]$$

$\leq \frac{1}{2}\|\hat{u}\|^2 + \frac{1}{2}C$

claim: $\mathcal{X} = \{L \mid L \models \mathcal{A}\}$, $\mathcal{X}$ is convex

Proof: suppose $L, L' \in \mathcal{X}$, let $\bar{L} = \frac{1}{2}L + \frac{1}{2}L'$

suppose $\mathcal{A} \vdash q \geq 0$, $\bar{L}[q] = \frac{1}{2}\underbrace{L[q]}_{\geq 0} + \frac{1}{2}\underbrace{L'[q]}_{\geq 0} \geq 0$

$\rightarrow \bar{L} \in \mathcal{X}$

* $X^1, \cdots, X^k$ sols. to $\mathcal{A}$

atomic $L^1, \cdots, L^k$

convex comb $C^1, \cdots, C^k$

$X = \begin{cases} X^1 \text{ w.p } C_1 \\ X^2 \text{ w.p } C_2 \\ \vdots \\ X^k \text{ w.p } C^k \end{cases}$

$\bar{L} = \sum C_i \cdot L^i$

$\bar{L}[q] = \mathbb{E}[q(X)]$

claim: let $p \in \mathbb{R}[X]$, $d = \deg(p)$, $f = \frac{l-d}{2}$, then,

$$\inf_{S \in \mathbb{R}[X]_{\leq f}} L[p \cdot S^2] \geq 0 \text{ iff } M_{L,p} \succeq 0, \text{ where } (M_{L,p})_{\alpha,\alpha'} = L[p \cdot X^{\alpha} \cdot X^{\alpha'}]$$

Proof. $S = \sum_{|\alpha| \leq |f|} S_\alpha \cdot X^\alpha$, $\vec{S} = (S_\alpha)_{|\alpha| \leq f}$

$$L[p \cdot S^2] = L\left[p \cdot \sum_{\alpha,\alpha'} S_\alpha \cdot S_{\alpha'} \cdot X^{\alpha+\alpha'}\right]$$

$$= \sum_{\alpha,\alpha'} S_\alpha \cdot S_{\alpha'} \cdot \underbrace{L[p \cdot X^{\alpha+\alpha'}]}_{(M_{L,p})_{\alpha,\alpha'}}$$

$$= \langle \vec{S}, M_{L,p} \vec{S} \rangle$$

claim: $L \in \mathcal{X}$ iff $L[1] = 1$ and $M_{L,p} \geq 0$ for p that are products of poly. in $\mathcal{A}$

Theorem:

$\mathcal{X}$ has poly time separation oracle $(N+m)^{O(l)}$ - time