Lecture 3: Algebraic Proof Systems, ctd. (Positivstellensätze)

Last time:

- Nsatz + proof system $\longrightarrow$ refute poly sys. over $\mathbb{C}$ by linear systems.
- Over $\mathbb{R}$ $\longrightarrow$ "SOS obstruction" $p \in SOS \implies p \geq 0$
  $1 + p$ never zero.
- Global certification: $p \geq 0 \not\Rightarrow p \in SOS$ (Hilbert)
  $\implies p \in \frac{SOS}{SOS}$ (Artin)

This time: constrained systems over $\mathbb{R}$.

Thm: (Krivine-Stengle '60s-'70s Positivstellensatz) $p_1, \ldots, p_m \in \mathbb{R}[x_1, \ldots, x_n]$ Exactly one holds:

(1) $\exists z \in \mathbb{R}^n$ s.t. $p_1(z) \geq 0, \ldots, p_m(z) \geq 0$

(2) $\exists q_S \in SOS$ for $S \subseteq [m]$ s.t.

$$\sum_{S \subseteq [m]} q_S \prod_{i \in S} p_i \overset{(p)}{=} -1$$

polynomial equality

Cor: (Real Nsatz) Exactly one holds:

(1) $\exists z \in \mathbb{R}^n$ s.t. $p_1(z) = \cdots = p_m(z) = 0$

(2) $\exists s \in SOS$, $q_1, \ldots, q_m \in \mathbb{R}[x_1, \ldots, x_n]$ s.t.

$$s + \sum p_i q_i \overset{(p)}{=} -1$$

Rk: Every poly $\in SOS - SOS$

$$\frac{1}{4}(1+p)^2 - \frac{1}{4}(1-p)^2 = p.$$

Pf: Use Psatz with $\pm p_m$ $\longrightarrow S = \emptyset \rightsquigarrow s = q_\emptyset$

$$-1 = s + \sum_{\substack{S \subseteq [m] \\ S \neq \emptyset}} (q_S^+ - q_S^-) \prod_{i \in S} p_i = s + \sum_{i=1}^m \tilde{q}_i p_i \quad \tilde{q}_i \in \mathbb{R}[x].$$

Cor: (Psatz certification)

$K := \{z \in \mathbb{R}^n : p_1(z) \geq 0, \ldots, p_m(z) \geq 0\}$ (semi-alg. set)

$\mathcal{S} := \left\{ \sum_{S \subseteq [m]} q_S(x) \prod_{i \in S} p_i(x) : q_S \in SOS \text{ for each } S \right\}$ ("SOS over K")

Let $r(x) \in \mathbb{R}[x_1, \ldots, x_n]$.

→ (1) $r(z) > 0 \ \forall z \in K \longleftrightarrow \exists s, t \in \mathcal{S} : r = \frac{1+s}{t}$

(2) $r(z) \geq 0 \ \forall z \in K \longleftrightarrow \exists s, t \in \mathcal{S}, a \in \mathbb{N} : r = \frac{r^{2a} + s}{t}$ ←

↪ follows from more general K-S Psatz.

Pf: (of (1)) $r(z) > 0 \ \forall z \in K \longleftrightarrow \left[\begin{cases} p_1(z) \geq 0 \\ \vdots \\ p_m(z) \geq 0 \\ -r(z) \geq 0 \end{cases}\right]$ has no solution

$r(z) \leq 0$

Psatz $\longrightarrow \exists\, s, t$ s.t. $\underbrace{-rs} + \underbrace{t} = -1 \longrightarrow r = \dfrac{1+t}{s}$.

Cor: (Artin) $p \geq 0$ on $\mathbb{R}^n \longrightarrow \exists\, s, t \in SOS$ s.t. $r = \dfrac{p^{2n} + s}{t}$ $\begin{matrix} \in SOS \\ \in SOS \end{matrix}$

<u>Psatz without denominators:</u>

Thm (Schmüdgen Psatz) $r(z) > 0 \ \forall z \in K$, $\boxed{\text{AND } K \text{ COMPACT}} \implies r \in \mathcal{S}$

I.e. $r = \sum_{S \subseteq [n]} SOS \cdot \prod_{i \in S} p_i$

$2^{\Omega(n)}$ terms.

Ex: Max Cut: n variables $x_1, \dots, x_n$, $m = n$ constraints $x_i^2 = 1$. $\rightarrow 2^n$ SOS indeterminates.

Def: $\mathcal{S}^{(0)} = \left\{ q_0(x) + \sum_{i=1}^m q_i(x) p_i(x) : q_0, q_1, \dots, q_m \in SOS \right\}$

$\sum x_i^2 \leq R \ \forall x \in K$.

(Archimedean) System $\{p_i(x) \geq 0\}_{i=1}^m$ Archimedean if $\exists\, R$ s.t. $R - \sum_{i=1}^n x_i^2 \in \mathcal{S}^{(0)}$.

"Effective/symbolic compactness"

Thm: (Putinar Psatz) $r(z) > 0 \ \forall z \in K$, $\boxed{\text{AND CONSTRAINTS ARCHIMEDEAN}}$ then $r \in \mathcal{S}^{(0)}$

I.e. $r(x) = q_0(x) + \sum_{i=1}^m q_i(x) p_i(x)$ for $q_i \in SOS$. $\boxed{\text{MOST USEFUL}}$

$O(m)$ terms

<u>Example:</u> Putinar over $\{\pm 1\}^n$ (e.g. MaxCut)

What does it say? $r \in \mathbb{R}[x_1, \dots, x_n]$, $r(z) > 0 \ \forall z \in \{\pm 1\}^n$ $(m = 2n)$

$\{\pm 1\}^n = \{ z : z_i^2 - 1 = 0 \} = \{ z : p_i^{\pm} \geq 0 \}$ $\quad p_i^{\pm}(x) = \pm (x_i^2 - 1)$

System Archimedean b/c ... $\sum_{i=1}^n (1 - x_i^2) = \overset{R}{\overset{\shortparallel}{n}} - \sum_{i=1}^n x_i^2$

Putinar $\implies \exists\, q_0, q_1^{\pm}, \dots, q_m^{\pm} \in SOS$ s.t.

$r(x) \overset{(p)}{=} q_0(x) + \sum_{i=1}^m (x_i^2 - 1)(q_i^+ - q_i^-)$

$\iff \exists\, s \in SOS$, $q_1, \dots, q_m \in \mathbb{R}[x_1, \dots, x_n]$ s.t.

$r(x) \overset{(p)}{=} s(x) + \sum_{i=1}^m (x_i^2 - 1) q_i(x)$ AS PROMISED!

Concrete construction:

$\boxed{1}$ $r \geq 0$ on $\{\pm 1\}^n \implies \exists s \in SOS$ s.t. $\underbrace{r = s \text{ on } \{\pm 1\}^n}_{\text{not an } \overset{\text{cpl}}{=} \text{ !}}$

Claim: (Boolean FA) $\forall f : \{\pm 1\}^n \to \mathbb{R}$, $\exists p \in \mathbb{R}[x_1, \dots, x_n]$ s.t. $p = f$ on $\{\pm 1\}^n$

Pf: (of $\boxed{1}$) $r \geq 0 \rightsquigarrow \sqrt{r} : \{\pm 1\}^n \to \mathbb{R}$

Claim $\implies \sqrt{r} = p$ on $\{\pm 1\}^n$ for $p \in \mathbb{R}[\underline{x}] \rightsquigarrow r = p^2$ on $\{\pm 1\}^n$

Pf: (of Claim) $V = \{ f : \{\pm 1\}^n \to \mathbb{R} \}$ vector space, $\dim V = 2^n$

Usual basis $\delta_y(x) = \mathbb{1}\{x = y\}$.

"Fourier basis" = "Monomial basis" = $f_S(x) = \prod_{i \in S} x_i \overset{\text{multilinear}}{=: x^S}$ over $S \subseteq [n]$.

$f_S \in V$, there are $2^n \rightsquigarrow$ enough to show f_S linearly independent.

Enough to show $p(x) = \sum_S c_S \underbrace{x^S}_{f_S(x)}$, $p = 0$ on $\{\pm 1\}^n \implies c_S = 0 \ \forall S$.

$\mathbb{E}_{x \sim \mathrm{Unif}(\{\pm 1\}^n)} p(x)^2 = \sum c_S^2 = 0 \implies c_S = 0 \ \forall S$. ∎ ←

$\langle f, g \rangle := \mathbb{E}_x f(x) g(x)$ $\langle f_S, f_T \rangle = \delta_{S,T} \rightsquigarrow f_S$ o.n. basis for V.

$\implies F = \sum_S \langle F, f_S \rangle \underbrace{f_S}_{x^S}$ ← "Fourier expansion".

$\boxed{2}$ $\overset{p}{\overline{r, s}} \in \mathbb{R}[\underline{x}]$ s.t. $\overset{p = 0}{\overline{r = s}}$ on $\{\pm 1\}^n$, then $\exists q_1, \dots, q_n \in \mathbb{R}[\underline{x}]$

$\overset{p}{\overline{\underbrace{r}_{\text{our poly. in } \boxed{1}} - \underbrace{s}_{SOS}}} = \sum \underbrace{q_i (x_i^2 - 1)}$.

$p(x) = x_1^2 + x_2^3 x_3 = \underline{1} + \underbrace{(x_1^2 - 1)} + \underbrace{x_2 x_3}_{\text{multilinear.}} + \underbrace{x_2 x_3 (x_2^2 - 1)}$.