# Lecture 2: Algebraic Proof Systems

**PLAN:**
- Today + M: pf systems
- M/W: SDP
- Then: algorithm appl.

**LOGISTICS:**
- Survey!!

Last time, ended hoping

$$x^T L x \le c \quad \forall x \in \{\pm 1\}^n$$

$$\Downarrow ?$$

$$c - x^T L x = \sum_{i=1}^{n} (1 - x_i^2) q_i(x) + \sum_j s_j(x)^2$$

Q: Generally, when does ($\Downarrow$) hold? (for today)

① Systems of equations: $p_1, \dots, p_m \in \mathbb{C}[x_1, \dots, x_n]$

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

Ex: ($n = 1$, $m = 1$) FTOA.

Ex: $\exists ?$ cut of size exactly $c$? ($x^T L x - c = 0$, $1 - x_i^2 = 0 \ \forall i$)

Thm (Nullstellensatz) (Hilbert ~1890): Exactly one holds:

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

(2) $\exists q_1, \dots, q_m \in \mathbb{C}[x_1, \dots, x_n]$ s.t. $\sum_i p_i q_i = 1$ ("refutation", "Nullstellensatz proof"; poly. equality, coeff by coeff.)

I.e., Nullstellensatz proof system complete.

Q: Can we find Nullstellensatz proofs efficiently?

A1: $I := \{\sum_i p_i q_i : q_i \in \mathbb{C}[x]\}$ → find Gröbner basis $\tilde{p}_1, \dots, \tilde{p}_M$ s.t.

↳ $= \{\sum_i \tilde{p}_i q_i\}$, and some ordering cond. $\Rightarrow 1 \in I$ iff $\tilde{p}_1 = 1$.

Compute w/ Buchberger's alg., runtime worst-case $= (\max \deg p_i)^{2^{\Omega(n)}}$.

A2: Constrain $\deg p_i q_i \le D$

$\exists ? q_i$ s.t. $\sum_i p_i q_i = 1$ $\longleftrightarrow$ $\exists ? x$ s.t. $Ax = f$

$p_1 = x + y$

$p_2 = 3x + 4y + 1$

$(x+y)(ax+by+c) + (3x+4y+1)(dx+ey+f) = 1$

($p_2$, $q_2$, $p_1$, $q_2$)

$A$: monomial coeffs in ($\Box$); $x$: coeffs of $q_i$; $f = (1, 0, 0, \dots, 0)$; multiplication by $p_i$ and add.

Thm (Kollár '88): Enough to take $D = (\max \deg p_i)^n$

Research Q: (Nullstellensatz proof complexity) What $D$ needed for specific problems?

Systems over $\mathbb{R}$ (instead of $\mathbb{C}$): $p_1, \dots, p_m \in \mathbb{R}[x_1, \dots, x_n]$

Problem: $n=1, n=1$ $\quad p(x) = 1 + x^2$ $\quad \nexists\, x \in \mathbb{R}$ s.t. $p(x) = 0$

$\nexists\, q \in \mathbb{R}[x]$ s.t. $pq = 1$.

Generally, same w/ $p(x_1, \dots, x_n) = 1 + \sum_j s_j(x)^2$.

Df: $SOS := \left\{ \sum_j s_j(x)^2 \right\} \subset \mathbb{R}[x_1, \dots, x_n]$.

Thm: (Real Nstz) Exactly one holds:

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

(2) $\exists\, q_1, \dots, q_m \in \mathbb{R}[x_1, \dots, x_n]$ s.t. $\sum p_i q_i \in 1 + SOS$

$\left(= 1 + \sum_j s_j(x)^2\right)$

"Not most natural over $\mathbb{R}$. Better" $\rightsquigarrow$ $p_i(z) \geq 0$ (or $>$).

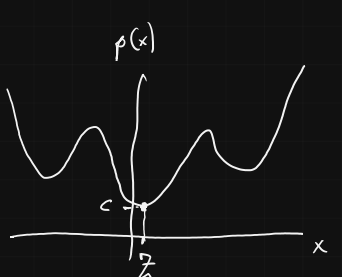
(e.g. $c - x^T C x \geq 0$)

SOS + Hilbert's 17th Problem:

Q: For $p_1, \dots, p_m \in \mathbb{R}[x_1, \dots, x_n]$, when $\exists\, z$ w/ $p_i(z) \geq 0\ \forall i$?

$n=1 \iff$ when is $p \geq 0$? $\rightarrow p(z) \geq 0\ \forall z$

Guess: $p \geq 0 \overset{(?)}{\iff} p \in SOS$




Prop: $p \in \mathbb{R}[x]$, $p \geq 0 \Rightarrow p \in SOS$

($n=1$)

Pf: $p(x) - c^{\geq 0} = (x - z)^{2k} r(x)$

Induction on degree.

Prop: $p \in \mathbb{R}[x_1, \dots, x_n]$, $p \geq 0$, $\deg p \leq 2 \Rightarrow p \in SOS$.

Pf: Homogeneous: $p(x) = \sum a_{ij} x_i x_j = x^T A x$

$p \geq 0 \leftrightarrow A \succeq 0 \leftrightarrow A = \sum_a v_a v_a^T \Rightarrow p(x) = \sum_a \langle v_a, x \rangle^2$.

Thm: (1) $p \in \mathbb{R}[x_1, x_2]$, $\deg p \leq 4$, $p \geq 0 \Rightarrow p \in SOS$

(Hilbert 1890) (2) Whenever we have $\begin{cases} n = 2, & d \geq 6 \\ n \geq 3, & d \geq 4 \end{cases}$ ($d$ even), $\exists\, p \in \mathbb{R}[x_1, \dots, x_n]$, $\deg p = d$, $p \geq 0$, $p \notin SOS$.

not constructive.

**Thm** (Motzkin): $p(x,y) = x^4y^2 + x^2y^4 + 1 - 3x^2y^2$ has $p \geq 0$, $p \notin SOS$.

**Pf**: $p \geq 0$: $\frac{x^4y^2 + x^2y^4 + 1}{3} \geq (x^6y^6)^{1/3} = x^2y^2$

$p \notin SOS$: Suppose $p(x) = \sum_j s_j(x)^2$ $\qquad s_j(x) = ax^2y + bxy^2 + cxy + d$

In each $s_j$ ...

- No monomial with $x^k$ or $y^k$ w/ $k \geq 3$
- No $x^2y^2$
- No $x^2$ or $y^2$
- No $x$ or $y$

$\rightsquigarrow$ coeff of $x^2y^2 \geq 0$ $\rightarrow\leftarrow$.

**Thm** (Artin 1927): $p \geq 0 \implies \exists\, r_j, s_j$ s.t. $p = \sum_j \left(\frac{r_j}{s_j}\right)^2 \iff \exists\, r, s \in SOS$ s.t. $p = \frac{r}{s}$.

($\exists\, s \in SOS$ s.t. $ps \in SOS$.)

GLOBAL

For optimization:

$\max_{x \in \mathbb{R}^n} p(x)$ $\xrightarrow{\text{Naive SOS}}$ $\min c$ s.t. $c - p(x) = s(x)$, $s(x) \in SOS$

$\xrightarrow{\text{Artin}}$ $\min c$ s.t. $t(x)(c - p(x)) = s(x)$, $s(x), t(x) \in SOS$ (non-linear $\rightarrow$ not SDP.)

**Q**: How many rational squares are needed in Artin? $A(n)$ s.t. $\forall p \in \mathbb{R}[x_1, \dots, x_n]$, $p \geq 0$ have $\exists\, r_1, \dots, r_{A(n)}, s_1, \dots, s_{A(n)}$ s.t. $\sum \left(\frac{r_j}{s_j}\right)^2 = p$.

**Thm** (Pfister): $A(n) \leq 2^n$

**Prop**: $A(n) \geq n+1$

} **Open Problem**: improve on either ?!

**Idea**: Sums of $2^n$ rational squares closed under multiplication.

$x^2y^2 = (xy)^2$,

$(w^2+x^2)(y^2+z^2) = (\text{bilinear}(w,x,y,z))^2 + (\text{bilinear}(w,x,y,z))^2$

$|w+ix|^2|y+iz|^2 = |(w+ix)(y+iz)|^2$

$\mathbb{R}, \mathbb{C}$, quaternions, octonions $\rightsquigarrow$ closure of 1, 2, 4, 8 squares.