Sign Constraints for Real Polynomials: Representation Theorems

Let's recall some commutative algebra / algebraic geometry. We let $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$.

Let $h_1, \dots, h_m \in \mathbb{K}[X] = \mathbb{K}[x_1, \dots, x_n]$. We denote $V_{\mathbb{K}}(h_1, \dots, h_m) := \{ X \in \mathbb{K}^n \mid h_i(X) = 0 \ \forall i \}$ the (real or complex) common roots of the h_i, and $I_{\mathbb{K}}(h_1, \dots, h_m) := \left\{ \sum_{i=1}^{m} u_i h_i \in \mathbb{K}[X] \mid u_i \in \mathbb{K}[X] \ \forall i \right\}$ the ideal generated by $h_1, \dots, h_m$. If $I \trianglelefteq \mathbb{K}[X]$ is an ideal, we define $\sqrt{I} := \{ f \in \mathbb{K}[X] \mid \exists r : f^r \in I \}$ the radical of I.

Theorem (Hilbert's Nullstellensatz)

Given $p \in \mathbb{C}[X]$, $h_1, \dots, h_m \in \mathbb{C}[X]$, then

$$p = 0 \text{ on } V_{\mathbb{C}}(h_1, \dots, h_m) \iff p \in \sqrt{I_{\mathbb{C}}(h_1, \dots, h_m)}$$
$$\iff \exists r, u_i : p^r = \sum_{i=1}^{m} u_i h_i$$

What about $\mathbb{K} = \mathbb{R}$?

Example ($n=3$) $x^2+y^2+z^2 \in \mathbb{R}[x,y,z]$ is irreducible, (over $\mathbb{C}$ and over $\mathbb{R}$) so $I = \mathcal{I}_{\mathbb{R}}(x^2+y^2+z^2)$ is radical. $V_{\mathbb{R}}(x^2+y^2+z^2) = \{(0,0,0)\}$, $x=0$ on $V_{\mathbb{R}}(x^2+y^2+z^2)$ but $x \notin \sqrt{I} = I$.

($n=2$) the same example works with $x^2+y^2 \in \mathbb{R}[x,y]$, but in this case $x^2+y^2 = (x+iy)(x-iy)$ is reducible over $\mathbb{C}$.

Definition Let $I \trianglelefteq \mathbb{R}[x]$ be an ideal. the **Real Radical** $\sqrt[\mathbb{R}]{I}$ is defined as:

$$\sqrt[\mathbb{R}]{I} := \{ f \in \mathbb{R}[x] \mid \exists k \in \mathbb{N}, \sigma \in \Sigma^2 : f^{2k} + \sigma \in I \}.$$
$$= \sqrt{(I+\Sigma^2) \cap -(I+\Sigma^2)}$$

Remark: if $I = \mathcal{I}_{\mathbb{R}}(h_1,\dots,h_m)$ and $f \in \sqrt[\mathbb{R}]{I}$, then $f=0$ on $V_{\mathbb{R}}(h_1,\dots,h_m)$. Is the converse true?

Theorem (Real Nullstellensatz)

Given $p \in \mathbb{R}[x]$, $h_1,\dots,h_m \in \mathbb{R}[x]$, then

$$p = 0 \text{ on } V_{\mathbb{R}}(h_1,\dots,h_m) \Leftrightarrow p \in \sqrt[\mathbb{R}]{\mathcal{I}_{\mathbb{R}}(h_1,\dots,h_m)}$$
$$\Leftrightarrow \exists r, \sigma, u_i : p^r + \sigma = \sum_{i=1}^m u_i h_i$$

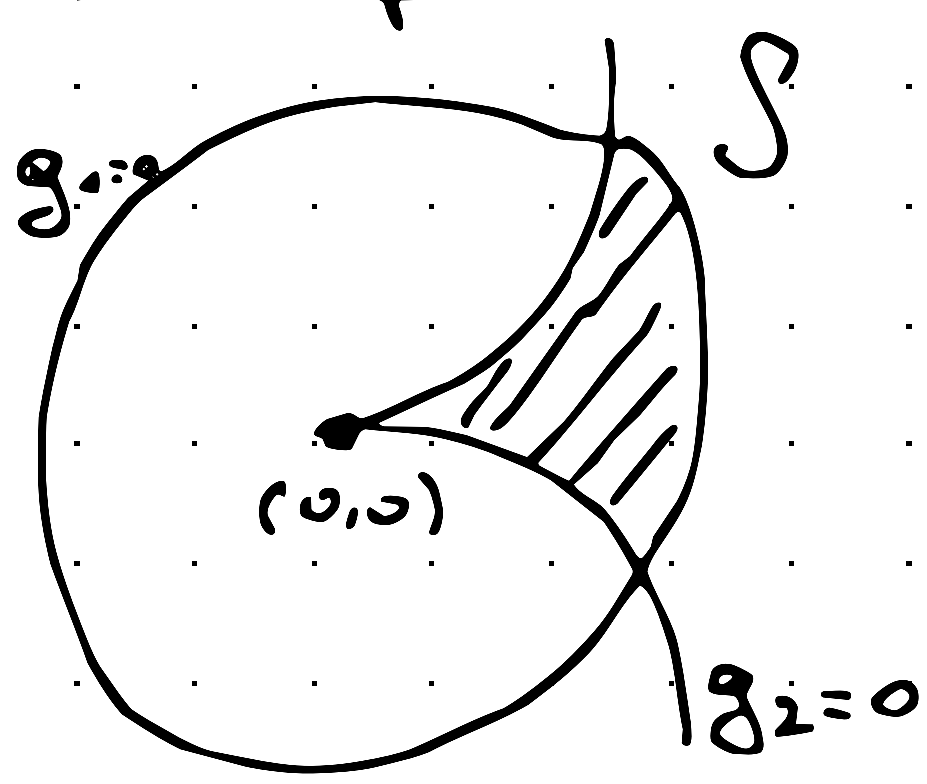
But $\mathbb{R}$ is an ordered field; we can consider also $\geq, >, \neq$ (and not only $=$).

Definition Let $g_1, \dots, g_m \in \mathbb{R}[X]$. We denote $\underline{g} = (g_1, \dots, g_m)$ the m-tuple of the g_i's, and we define the **basic, closed semialgebraic set** defined by $\underline{g}$:

$$S = S(\underline{g}) := \{ x \in \mathbb{R}^n \mid \forall i = 1, \dots, m \quad g_i(x) \geq 0 \}.$$

We also denote $P(S)$ the convex cone of non-negative polynomials on S.

Example $(n=2)$ $\quad g_1 = 1 - x^2 - y^2, \quad g_2 = x^3 - y^2.$



Clearly, $g_1 \geq 0$ on $S = S(\underline{g})$, $g_2 \geq 0$ on S, $g_1 \cdot g_2 \geq 0$ on S, and:

$$\Sigma^2 + \Sigma^2 \cdot g_1 + \Sigma^2 \cdot g_2 + \Sigma^2 \cdot g_1 g_2 \subset P(S)$$

But $x \in P(S)$ cannot be written as

$\sigma_0 + \sigma_1 g_1 + \sigma_2 g_2 + \sigma_3 g_1 g_2$, $\sigma_i \in \Sigma^2$

Definition Given $\underline{g} = (g_1, \dots, g_m)$, we define the (finitely generated) **preordering** $T = T(\underline{g})$ as:

$$T = T(\underline{g}) := \Sigma^2 + \Sigma^2 \cdot g_1 + \dots + \Sigma^2 \cdot g_m + \Sigma^2 \cdot g_1 g_2 + \dots + \Sigma^2 \cdot g_1 \cdots g_m$$
$$= \Big\{ \sum_{J \subset \{1, \dots, m\}} \sigma_J \prod_{j \in J} g_j \;\Big|\; \sigma_J \in \Sigma^2 \ \forall J \Big\}$$

(we use $\prod_{j \in \emptyset} g_j = 1$). Clearly, $T(\underline{g}) \subset P(S(\underline{g}))$, and if $p \in T(\underline{g}) \cap -T(\underline{g})$ then $p = 0$ on $S(\underline{g})$.

Theorem (Krivine - Stengle Positivstellensatz)

Let $S = S(\underline{g})$, $T = T(\underline{g})$ as before and $p \in \mathbb{R}[x]$. Then:

(i) $p > 0$ on $S \iff fp = 1 + h$ for some $f, h \in T$

(ii) $p \geq 0$ on $S \iff fp = p^{2k} + h$ for some $f, h \in T, k \in \mathbb{N}$

(iii) $p = 0$ on $S \iff -p^{2k} \in T$ for some $k \in \mathbb{N}$

$\iff p \in \sqrt{T \cap -T}$

(iv) $S = \emptyset \iff -1 \in T$.

Notice that: (ii) generalize Artin's theorem

(iii) generalize the Real Nullstellensatz.

Remark: the proof of the theorem is completely algebraic, and the same result holds true if we replace $\mathbb{R}$ with any real closed field R (we say that a field R is real closed if the ring $\frac{R[x]}{(x^2+1)}$ is an algebraically closed field: in this case R has a unique ordering)

Idea of the proof (enough to prove (iv)):

1) Assume $-1 \notin T$, and pick a minimal prime $\mathfrak{p} \supset T \cap -T$.

2) Consider the field extension $F := \mathrm{Quot}\left(\frac{R[x]}{\mathfrak{p}}\right)$ of R.

3) F has an ordering which extends the one of R.

4) Find a solution of $g_1 \geq 0, \dots, g_m \geq 0$ in F, and conclude that $S(\underline{g}) \neq \emptyset$ using the transfer principle.

Problem: denominators in the previous representations

can they be avoided?

Example: $(n=1)$ $1-x^2 \in P([-1,1])$, $1-x^2 \notin T((1-x^2)^3)$,

but $(1-x^2)^2(1-x^2) \in T((1-x^2)^3)$.

Theorem $(n=1)$

1) (Pólya - Szegö) $p \in P([0,+\infty)) \Rightarrow \exists \sigma_i \in \Sigma^2$:

$\Rightarrow p = \sigma_0 + \sigma_1 x$, $\deg(\sigma_0), \deg(\sigma_1 x) \leq \deg(p)$.

2) (Fekete, Markov-Lukácz)

- $p \in P([-1,1]) \Rightarrow \exists \sigma_i \in \Sigma^2$: $p = \sigma_0 + \sigma_1(1-x^2)$,

  $\deg(\sigma_0), \deg(\sigma_1(1-x^2)) \leq \deg(p)+1$.

- $p \in P([-1,1]) \Rightarrow \exists \sigma_i \in \Sigma^2$: $p = \sigma_1(1-x) + \sigma_2(1+x)$,

  $\deg(\sigma_1(1-x)), \deg(\sigma_2(1+x)) \leq \deg p$.

General case?

Theorem (Schmüdgen) If $S(\underline{g})$ is compact, $p \in \mathbb{R}[x]$ and $p > 0$ on $S(\underline{g})$, then $p \in T(\underline{g})$.

Remarks.

- General, denominator free Positivstellensatz
- No control on the degree of the representation $p \in T(\underline{g})$, and we have $2^m = 2^{\#\underline{g}}$ SoS multipliers

Definition. Let $\underline{g} = (g_1, \dots, g_m)$ be a tuple of polynomials. We define the (finitely generated) **quadratic module** $M(\underline{g}) = M$ generated by $\underline{g}$ as:

$$M = M(\underline{g}) := \Sigma^2 + \Sigma^2 \cdot g_1 + \dots + \Sigma^2 \cdot g_m$$
$$= \{\sigma_0 + \sigma_1 g_1 + \dots + \sigma_m g_m \mid \sigma_i \in \Sigma^2\}.$$

Lemma the following are equivalent:

(i) $\exists h \in M(\underline{g}) : S(h) = \{x \in \mathbb{R}^n : h(x) \geq 0\}$ is compact;

(ii) $\exists r \in \mathbb{N} : r - \sum_{i=1}^{n} x_i^2 = r - \|x\|_2^2 \in M(\underline{g})$

(iii) $\forall f \in \mathbb{R}[x], \exists r \in \mathbb{N} : r \pm f \in M(\underline{g})$.

Proof (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i) are trivial.

For (i) $\Rightarrow$ (iii), use Schmüdgen's theorem (Ex.)

Definition If $M(\underline{g})$ satisfies (i) (or (ii) or (iii)) we say that $M(\underline{g})$ is **Archimedean**

theorem (Putinar) If $M(\underline{g})$ is Archimedean and $p \in \mathbb{R}[x]$, then $p > 0$ on $S(\underline{g}) \Rightarrow p \in M(\underline{g})$

Proof See lecture 3.

Examples:

- If $g_i = 1 - x_i^2$, $i = 1, \dots, n$, $M(\underline{g})$ is Archimedean because $n - \|x\|_2^2 = \sum_{i=1}^n 1 - x_i^2 \in M(\underline{g})$. ($S(\underline{g}) = [-1,1]^n$)
- If $g_i = x_i$ for $i = 1, \dots, n$, $g_{n+1} = 1 - \sum_{i=1}^n x_i$; then $M(\underline{g})$ is Archimedean. Indeed: ($S(\underline{g})$ is a simplex)
  - $1 - x_i = (1 - \sum_{j=1}^n x_j) + \sum_{j \neq i} x_j \in M(\underline{g})$
  - $1 - x_i^2 = \frac{(1+x_i)^2}{2}(1 - x_i) + \frac{(1-x_i)^2}{2}(1 + x_i)$

  And conclude as in the previous point.
- (Jacobi, Prestel) ($n=2$)

  $g_1 = x_1 - \frac{1}{2}$, $g_2 = x_2 - \frac{1}{2}$, $g_3 = 1 - x_1 x_2$.

  $S(\underline{g})$ is compact, but $M(\underline{g})$ is not Archimedean (Ex.)

  Notice that $T(\underline{g})$ is Archimedean from Schmüdgen's theorem

Comments

- Schmüdgen and Putinar's theorems were first proven using functional analysis techniques, solving a dual Moment Problem. See lecture 4 for more.
- these theorems do not hold for arbitrary real closed fields R. they depend on analysis/approximation theory!
- We did not comment on degree bounds. this is an active area of research: see lecture 5.