MATH 8102 Fall 2026 Scribe: Tim Duff
10/28/26 Editor: Tim Duff

The Krivine-Stengle Positivstellensatz and Real Nullstellensatz (Theobald §6.5)

We retain the notation of the previous lecture. For finitely-many polynomials $h_1, \ldots, h_t \in R[\mathbf{x}]$, we define the multiplicative *monoid* that they generate as

$$\mathrm{Mon}(h_1, \ldots, h_t) = \left\{ \prod_{j=1}^{t} h_i^{\beta_i} \mid \boldsymbol{\beta} \in \mathbb{Z}_{\geq 0}^t \right\}.$$

By convention, $\mathrm{Mon}(\emptyset) = \{1\}$. We let $\langle f_1, \ldots, f_r \rangle$ denote the ideal of $R[\mathbf{x}]$ generated by $f_1, \ldots, f_r$, so that $\langle \emptyset \rangle = \{0\}$, and as before $\mathrm{PO}(g_1, \ldots, g_r)$ the preorder generated by $g_1, \ldots, g_r \in R[\mathbf{x}]$ with the convention that $\mathrm{PO}(\emptyset) = \Sigma R[\mathbf{x}]^2$.

Theorem 1 (Krivine-Stengle Positivstellensatz)**.** *For any multivariate polynomials*

$$f_1, \ldots, f_r, g_1, \ldots, g_s, h_1, \ldots, h_t \in R[\mathbf{x}]$$

over a real-closed field R, the semialgebraic set

$$S = \{\xi \in R^n \mid f_i(\xi) = 0,\, g_j(\xi) \geq 0,\, h_k(\xi) \neq 0, \quad \forall\, 1 \leq i \leq r, 1 \leq j \leq s, 1 \leq k \leq t\},$$

is empty if and only if there exist polynomials $F \in \langle f_1, \ldots, f_r \rangle$, $G \in \mathrm{PO}(g_1, \ldots, g_s)$, and $H \in \mathrm{Mon}(h_1, \ldots, h_t)$ such that $F + G + H^2 = 0$.

When $r = t = 0$, we have $\langle f_1, \ldots, f_r \rangle = 0$ and $\mathrm{Mon}(h_1, \ldots, h_t) = \{1\}$, and the conclusion reduces to our previous characterization of when a basic closed semialgebraic set is empty. In fact, our proof of the Krivine-Stengle Positivstellensatz will essentially reduce to this special case. Note that the case $r = 1$, $t = 0$ is general enough to furnish certificates of emptiness for any semialgebraic set, via the disjunctive normal form of previous lectures. On the other hand, using multiple equations $f_i = 0$ and inequations $h_k \neq 0$ may provide some additional flexibility in how such certificates are constructed.

Proof. First, observe that the existence of such F, G, H certifies the emptiness of S; at any point $\xi \in S$, we would necessarily have $G(\xi) = -H(\xi)^2 < 0$.

For the converse, consider first the case $t = 0$ where there are no inequations. In this case, S is the basic closed semialgebraic set defined by inequalities

$$f_i(\mathbf{x}) \geq 0, \quad -f_i(\mathbf{x}) \geq 0, \quad g_j(\mathbf{x}) \geq 0, \quad \forall\, 1 \leq i \leq r, 1 \leq j \leq s,$$

and hence $S = \emptyset$ implies

$$-1 \in \mathrm{PO}(f_1, \ldots, f_r, -f_1, \ldots, -f_r, g_1, \ldots g_m) \subset \langle f_1, \ldots, f_r \rangle + \mathrm{PO}(g_1, \ldots, g_s).$$

Now, for $t > 0$, introduce new variables $y_1, \ldots, y_t$ and note $S = \emptyset \Rightarrow S' = \emptyset$, where

$$S' = \{(\xi, \nu) \in R^{n+t} \mid \xi \in S, 1 - \nu_k h_k(\xi) = 0 \quad \forall\, 1 \leq k \leq t\}.$$

(This use of slack variables is sometimes called *Rabinowitsch's trick.*) If $S' = \emptyset$, then

$$-1 \in \mathrm{PO}(\pm f_1, \ldots, \pm f_r, g_1, \ldots, g_s, \pm(1 - y_1 h_1), \ldots, \pm(1 - y_t h_t)).$$

More explicitly, we have

$$-1 = F' + G', \tag{1}$$

where F' belongs to the ideal $\langle f_1, \ldots, f_r, 1 - y_1 h_1, \ldots, 1 - y_t h_t \rangle \subset R[\mathbf{x}, \mathbf{y}]$ and G' belongs to the preorder $\mathrm{PO}(g_1, \ldots, g_s) \subset R[\mathbf{x}, \mathbf{y}]$. Now, substitute $y_k \to \frac{1}{h_k}$ for all instances of y_k in (1) and multiply the result by H^2 for $H \in \mathrm{Mon}(h_1, \ldots, h_t)$ a monomial in $h_1, \ldots, h_t$ of sufficiently large degree so that

$$-H^2 = H^2 F' + H^2 G'$$

is an identity in $R[\mathbf{x}]$. Now set $F = H^2 F' \in \langle f_1, \ldots, f_r \rangle$ and $G = H^2 G' \in \mathrm{PO}(g_1, \ldots, g_s)$. □

The Positivstellensatz can also be used to furnish certificates of when a polynomial is positive, nonnegative, or nonzero on a semialgebraic set.

Corollary 1. *For $f, g_1, \ldots, g_s \in R[\mathbf{x}]$, $S = \mathcal{S}(g_1, \ldots, g_s)$, $P = \mathrm{PO}(g_1, \ldots, g_s)$,*

1. *$f > 0$ on S if and only if there exist $G, H \in P$ with $fG = 1 + H$.*
2. *$f \geq 0$ on S if and only if there exist $G, H \in P$ and $k \in \mathbb{Z}_{\geq 0}$ with $fG = f^{2k} + H$.*
3. *$f \neq 0$ on S if and only if there exists $H \in P$ and $k \in \mathbb{Z}_{\geq 0}$ with $0 = f^{2k} + H$.*

Proof. All statements follow by applying Theorem 1 to a suitable semialgebraic set. For example, the conditions of statement (1) hold if and only if $S \cap \{\xi \mid -f(\xi) \geq 0\} = \emptyset$, and hence if and only if $-1 \in \mathrm{PO}(g_1, \ldots, g_s, -f) = \mathrm{PO}(g_1, \ldots, g_s) - f\,\mathrm{PO}(g_1, \ldots, g_s)$. Thus, $\exists G, H \in \mathrm{PO}(g_1, \ldots, g_s)$ as in the statement. Proofs of (2) and (3) are similar. □

Finally, we will use the Krivine-Stengle Positivstellensatz to derive real analogues of the classical Nullstellensatz (which only holds over algebraically closed fields.) Just like the classical case, there are weak and strong forms of the real Nullstellensatz. The weak form is a simple application of the Krivine-Stengle theorem.

Corollary 2 (Weak Nullstellensatz)**.** *For $f_1, \ldots, f_r \in R[\mathbf{x}]$, the real algebraic set*

$$\mathcal{Z}(f_1, \ldots, f_r) = \{\xi \in R^n \mid f_i(\xi) = 0 \quad \forall\, 1 \leq i \leq r\}$$

is empty if and only if and only if there exists $F \in \langle f_1, \ldots, f_r \rangle$ and $G \in \Sigma R[\mathbf{x}]$ such that $F + G + 1 = 0$.

To state the strong Positivstellensatz, we define for any subset $V \subset R^n$ the *vanishing ideal* $\mathcal{I}(V) \subset R[\mathbf{x}]$ as

$$\mathcal{I}(V) = \{p \in R[\mathbf{x}] \mid p(\xi) = 0 \quad \forall \xi \in V\},$$

and the *real radical* of an ideal $I \subset R[\mathbf{x}]$ as

$$\sqrt[R]{I} = \{p \in R[\mathbf{x}] \mid \exists k \in \mathbb{Z}_{\geq 0},\ \exists q \in \Sigma R[\mathbf{x}]^2 \text{ w/ } p^{2k} + q \in I\}.$$

It is routine to verify that these operations both give ideals in $R[\mathbf{x}]$. Note that any ideal $I \subset R[\mathbf{x}]$ has a finite generating set $f_1, \ldots, f_r \in I$ by Hilbert's basis theorem. We may define $\mathcal{Z}(I) = \mathcal{Z}(f_1, \ldots, f_r)$: it is routine to verify that this definition is independent of the chosen generators.

Theorem 2 (Strong Real Nullstellensatz)**.** *For any ideal $I = \langle f_1, \ldots, f_r \rangle \subset R[\mathbf{x}]$, we have $\mathcal{I}(\mathcal{Z}(I)) = \sqrt[R]{I}$.*

Proof. If $p \in \sqrt[R]{I}$, then $p^{2k} + q = F$ for some integer k, sum-of-squares q and $F \in I$. For any $\xi \in \mathcal{Z}(I)$, we have

$$0 = f(\xi) = (p(\xi))^{2k} + q(\xi) \quad \Rightarrow \quad (p(\xi))^{2k} = -q(\xi).$$

Since $(p(\xi))^{2k}$ and $q(\xi)$ are both nonnegative, they must both be zero. This shows $p \in \mathcal{I}(\mathcal{Z}(I))$, and hence the inclusion $\sqrt[R]{I} \subset \mathcal{I}(\mathcal{Z}(I))$. For the reverse inclusion, we once again use Rabinowitsch's trick. For any nonzero $p \in \mathcal{I}(\mathcal{Z}(I))$, let t be a new variable, and construct an ideal $I' = \langle f_1, \ldots, f_r, tp - 1 \rangle \subset R[\mathbf{x}, y]$. Observe that $\mathcal{Z}(I') = \emptyset$. By the weak real Nullstellensatz, there exist $g_1, \ldots, g_s, h_1, \ldots, h_r, h \in R[\mathbf{x}, y]$ with

$$h_1 f_1 + \ldots + h_r f_r + h(pt - 1) = g_1^2 + \ldots + g_r^2 + 1.$$

Setting $t = 1/p$ and clearing denominators by p^{2k} for $k \gg 0$, we obtain a certificate of the real-radical membership $p \in \sqrt[R]{I}$. Hence $\sqrt[R]{I} \supset \mathcal{I}(\mathcal{Z}(I))$. $\square$