5

Stellensätze and non-negativity

The solution to Hilbert's 17th problem characterizes non-negative polynomials on $\mathbb{R}^n$ as the sums of squares of rational functions. In this chapter we extend this result in two directions: (1) to other sign constraints such as strict positivity or vanishing of a polynomial function, and (2) to constrained semialgebraic sets in place of $\mathbb{R}^n$. These questions are highly relevant in polynomial optimization and we complement the theoretical treatment based on [Mar08] with a computational approach from semidefinite programming [BPT13].

5.1 The Positivstellensatz and its variants

A fundamental task in algebraic geometry is to study the behavior of polynomial functions on varieties. In the ordered setting, we study more concretely signs of polynomials on semialgebraic sets. From Theorem 4.5 we know when exactly polynomials are globally non-negative. We also observed that Theorem A.5 fails for non-algebraically closed fields. After more preliminary real algebra, we are ready to formulate and prove the appropriate analogue of this theorem which works over real-closed fields: the celebrated Positivstellensatz.

To this end it is advantageous to work with ordered rings, in particular polynomial rings. The definition of ordering and cone from Chapter 1 apply verbatim — although not all of the results from that chapter do. Also recall from Exercise 1.4 that if the ordered ring $\mathcal{R}$ is reduced, then it is an integral domain and its orderings are in bijection with the orderings of its fraction field $\mathsf{ff}(\mathcal{R})$. Any family of elements $f_i \in \mathcal{R}$ generates the following subsets of $\mathcal{R}$:

- Their *ideal* $\mathcal{I} = \mathcal{I}(f_i)$ contains all f_i and satisfies $\mathcal{I} + \mathcal{I} \subseteq \mathcal{I}$ and $\mathcal{R} \cdot \mathcal{I} \subseteq \mathcal{I}$.
- Their *cone* $\mathcal{P} = \mathcal{P}(f_i)$ contains all f_i as well as all squares f^2 for $f \in \mathcal{R}$ and satisfies $\mathcal{P} + \mathcal{P} \subseteq \mathcal{P}$ and $\mathcal{P} \cdot \mathcal{P} \subseteq \mathcal{P}$.
- Their *(multiplicative) monoid* $\mathcal{U} = \mathcal{U}(f_i)$ contains all f_i as well as $1 \in \mathcal{R}$ and satisfies $\mathcal{U} \cdot \mathcal{U} \subseteq \mathcal{U}$.

It is helpful to imagine these objects in a polynomial ring $\mathcal{R} = \mathbb{F}[x_1, \dots, x_n]$ over an ordered field $\mathbb{F}$. Elements of the ideal $\mathcal{I}(f_i)$ vanish whenever all of the f_i vanish; elements of the cone are non-negative whenever the f_i are non-negative; and elements of the monoid do not vanish whenever all of the f_i do not vanish. The following extensional characterizations are easy to prove:

Lemma 5.1. Let $f_i \in \mathcal{R}$, $i \in I$, be an arbitrary family.

— $\mathcal{I}(f_i)$ consists of $\sum_{i \in F} g_i f_i$ for $F \subseteq I$ finite and $g_i \in \mathcal{R}$.

— $\mathcal{P}(f_i)$ consists of $\sum_{i \in F} \sigma_i P_i$ for $F \subseteq I$ finite, $\sigma_i \in \sum \mathcal{R}^2$ and $P_i \in \mathcal{U}(f_i)$.

— $\mathcal{U}(f_i)$ consists of $\prod_{i \in F} f_i^{m_i}$ for $F \subseteq I$ finite and $m_i \in \mathbb{N}$.

We prove at first a weak version of the Positivstellensatz and then derive the strong version from it. For this we require the following extension principle which we supply without proof.

Lemma 5.2. Let $\mathcal{P}$ be a proper cone in a ring $\mathcal{R}$. Then there exists a homomorphism $\varphi : \mathcal{R} \to \mathbb{F}$ into a real-closed field $\mathbb{F}$ whose order cone extends $\varphi(\mathcal{P})$.

Lemma 5.3: Weak Positivstellensatz. Let $\mathbb{F}$ be real-closed, $f_1, \ldots, f_r \in \mathbb{F}[x_1, \ldots, x_n]$ and let $K = \{ f_i \geq 0 \}$ denote their basic closed semialgebraic set and $\mathcal{P} = \mathcal{P}(f_i)$ the cone generated by them in $\mathbb{F}[x_1, \ldots, x_n]$. Then $K = \emptyset$ if and only if $-1 \in \mathcal{P}$.

Proof. If $-1 \in \mathcal{P}$, then for every $x \in K$ we have $-1 = \sum_j \sigma_j \prod_i f_i(x)^{m_{ij}} \geq 0$ according to Lemma 5.1 since all summands are non-negative but this is absurd.

Now suppose $-1 \notin \mathcal{P}$. Then $\mathcal{P}$ is proper and Lemma 5.2 furnishes a homomorphism $\varphi : \mathbb{F}[x] \to \mathbb{F}'$ into a real-closed field $\mathbb{F}'$ whose ordering extends $\varphi(\mathcal{P})$. As a ring homomorphism between fields, the composition $\mathbb{F} \hookrightarrow \mathbb{F}[x] \to \mathbb{F}'$ is injective and so $\mathbb{F}'$ is a real-closed extension of $\mathbb{F}$. Since $f_i \in \mathcal{P}$ we have $\mathbb{F}' \models \exists x : f_i(x) \geq 0$ analogously to the proof of Theorem 4.5. Hence Tarski's transfer principle shows $\mathbb{F} \models \exists x : f_i(x) \geq 0$, i.e., K is non-empty. □

The prototypical example is the empty circle in $\mathbb{R}^2$: if $r < 0$, then $\{ x^2 + y^2 = r \}$ is empty and indeed $-1 = ({}^1/\!\sqrt{-r} \cdot x)^2 + ({}^1/\!\sqrt{-r} \cdot y)^2 \in \sum \mathbb{R}[x,y]^2$. Here, we do not even need the two inequalities $x^2 + y^2 - r \geq 0$ and $-x^2 - y^2 + r \geq 0$ which generate $\mathcal{P}$. Another description of the empty set is $\{ x \geq 1, -x \geq 1 \}$ and we obtain $-1 = {}^1/_2(x-1) + {}^1/_2(-x-1) \in \mathcal{P}$ using only that ${}^1/_2$ is a sum of squares in $\mathbb{R}$.

Positivstellensatz. Let $\mathbb{F}$ be real-closed, $f_1, \ldots, f_r \in \mathbb{F}[x_1, \ldots, x_n]$ and let $K = \{ f_i \geq 0 \}$ denote their basic closed semialgebraic set and $\mathcal{P} = \mathcal{P}(f_i)$ the cone generated by them in $\mathbb{F}[x_1, \ldots, x_n]$. For any $f \in \mathbb{F}[x_1, \ldots, x_n]$ we have:

(1) $f > 0$ on K if and only if $\exists p, q \in \mathcal{P} : pf = 1 + q$.

(2) $f \geq 0$ on K if and only if $\exists m \in \mathbb{N}\, \exists p, q \in \mathcal{P} : pf = f^{2m} + q$.

(3) $f = 0$ on K if and only if $\exists m \in \mathbb{N} : -f^{2m} \in \mathcal{P}$.

(4) $K = \emptyset$ if and only if $-1 \in \mathcal{P}$.

Proof. Since we know by Lemma 5.3 that (4) is true, it suffices to show that all statements are equivalent. Note that all "if" assertions are obvious, for instance in (1): if $pf = 1 + q$, then on every point $x \in K$ we have $p(x) \cdot f(x) = 1 + q(x) > 0$, so $p(x) > 0$ and thus $f(x) = \frac{1+q(x)}{p(x)} > 0$. Thus in the equivalence proofs we only need to prove the "only if" parts.

(1) $\Rightarrow$ (2): Suppose that (1) is true for all $f, f_1, \dots, f_r$. For the "if" part of (2) suppose that $f \geq 0$ on K. Introduce a new variable y and consider $K' = \{\, f_i \geq 0, yf = 1 \,\}$. Let $F(x,y) = f(x)$. Since $f \geq 0$ on K, we have that $F > 0$ on K', so by (1) we get $P, Q \in \mathcal{P}(f_i) \subseteq \mathbb{F}[x,y]$ with $PF = 1 + Q$. P is a finite sum

$$P = \sum_j \sigma_j P_j, \quad \text{where } \sigma_j \in \sum \mathbb{F}[x,y]^2 \text{ and } P_j \in \mathcal{U}(f_j, yf-1, -yf+1).$$

Substituting $y = {}^1\!/\!{}_{f(x)}$ in this expression kills all summands in which P_j involves a factor $yf - 1$ or $-yf + 1$. In all other instances, y appears only in the σ_j terms. Write

$$\sigma_j(x,y) = \sum_k g_{jk}(x,y)^2 = \sum_k \left(\sum_\ell g_{jk\ell}(x) y^\ell \right)^2,$$

then multiply through with a sufficiently large even power of f:

$$f^{2m}(x)\sigma_j\left(x, \frac{1}{f(x)}\right) = \sum_k \left(\sum_\ell g_{jk\ell}(x) f^{m-\ell}(x) \right)^2 \in \sum \mathbb{F}[x]^2.$$

Thus we obtain $p = f^{2m}(x) P\left(x, \frac{1}{f(x)}\right) \in \mathcal{P}$ if only m is sufficiently large. The same argument applies to q and thus we have an equation $pf = f^{2m} + q$ as desired.

(2) $\Rightarrow$ (3): Suppose $f = 0$ on K. This just means that $f \geq 0$ and $-f \geq 0$, so we obtain two sets of numbers m_1, m_2 and polynomials $p_1, p_2, q_1, q_2 \in \mathcal{P}$ such that $p_1 f = f^{2m_1} + q_1$ and $-p_1 f = f^{2m_2} + q_2$. But then

$$-p_1 p_2 f^2 = f^{2(m_1+m_2)} + f^{2m_1} q_2 + f^{2m_2} q_1 + q_1 q_2.$$

Rearranging the terms gives $-f^{2(m_1+m_2)} \in \mathcal{P}$.

(3) $\Rightarrow$ (4): If $K = \emptyset$ then the constant 1 vanishes on K and we obtain $-1 \in \mathcal{P}$.

(4) $\Rightarrow$ (1): If $f > 0$ on K, then $K' = \{\, f_i \geq 0, -f \geq 0 \,\} = \emptyset$ and we have $-1 \in \mathcal{P}(-f)$. Since $\mathcal{P}(-f) = \mathcal{P} - f\mathcal{P}$ we obtain $-1 = q - fp$ for $p, q \in \mathcal{P}$ as desired. □

The Positivstellensatz as stated above applies only to basic closed semialgebraic sets. With just a few more algebraic tools one can prove the following technical refinement which has consequences of theoretical and practical interest. We merely state it here and refer to [BCR98, Chapter 4] for the proof.

Formal Positivstellensatz. Let $\mathcal{R}$ be a commutative ring and $f_i, g_j, h_k \in \mathcal{R}$. Let $\mathcal{I}$ be the ideal generated by the f_i, $\mathcal{P}$ the cone generated by the g_j and $\mathcal{U}$ the multiplicative monoid generated by the h_k in $\mathcal{R}$. Then the following two statements are equivalent:

(a) There is no ring homomorphism $\varphi : \mathcal{R} \to \mathbb{F}$ into a real-closed field $\mathbb{F}$ such that $\varphi(f_i) = 0$, $\varphi(g_j) \geq 0$ and $\varphi(h_k) \neq 0$ for all i, j, k.

(b) There exist $f \in \mathcal{I}$, $g \in \mathcal{P}$ and $h \in \mathcal{U}$ such that $f + g + h^2 = 0$.

Remark 5.4. The Positivstellensatz is recovered by taking $\mathcal{R} = \mathbb{F}[x_1, \dots, x_n]$ with $\mathbb{F}$ real-closed. By Tarski's transfer principle, the existence of the homomorphism φ in this case really only postulates the existence of a solution to the polynomial system $\{ f_i = 0, g_j \geq 0, h_k \neq 0 \}$ in $\mathbb{F}$. Notice that every primary semialgebraic set is of the form considered in the theorem. Existence of a solution on a general semialgebraic set can be treated on each primary semialgebraic set in the decomposition afforded by Lemma 2.5 separately, and so Formal Positivstellensatz can be put to use with every semialgebraic set.

When $\mathcal{R} = \mathbb{F}[x_1, \dots, x_n]$ for an ordered field $\mathbb{F}$, there always exists a homomorphism $\mathbb{F} \to \mathsf{rcl}(\mathbb{F})$ and the Formal Positivstellensatz may be read as a *theorem of the alternative* analogous to Theorem A.6. In this form, it is also an algebraic version of the completeness of RCF: for every definable (semialgebraic) set, either there exists a point inside it over the real closure of the coefficient field and plugging it into the defining polynomials provides an algebraic proof that the point belongs to the set; or there is no point and an algebraic proof of the emptiness of the set exists in the form of three polynomials f, g, h.

Since this theorem is valid for arbitrary commutative rings, it applies even to $\mathcal{R} = \mathbb{Z}[x_1, \dots, x_n]$. This case is of special significance and we call it

Alternatives in real algebraic geometry. Let $K = \{ f_i = 0, g_j > 0 \} \subseteq \mathbb{R}^n$ be a $\mathbb{Z}$-defined primary semialgebraic set. Then either K is non-empty and has a $\mathsf{rcl}(\mathbb{Q})$-rational point or it is empty and there exist $f \in \mathcal{I}(f_i)$, $g \in \mathcal{P}(g_j)$ and $h \in \mathcal{U}(g_j)$ with *integer coefficients* such that $f + g + h^2 = 0$.

Proof. If $f + g + h^2 = 0$, then K must be empty because on every point $x \in K$ the expression evaluates to the contradiction $0 = f(x) + g(x) + h(x)^2 > 0$ by the choice of f, g, h relative to K.

Conversely, if K has no $\mathsf{rcl}(\mathbb{Q})$-rational point, then Tarski's transfer principle forbids the existence of a homomorphism of $\mathbb{Z}[x]$ into a real-closed field over which the system has a solution. Hence existence of f, g, h follows from the Formal Positivstellensatz. □

In either case, solvability or unsolvability, the result can be *certified* by a finite amount of data which can be exactly represented on a computer, stored and later used for fast and independent verification in off-the-shelf computer algebra systems.

Real Nullstellensatz. Let $\mathcal{I}$ be an ideal in $\mathbb{F}[x_1, \dots, x_n]$, $\mathbb{F}$ real-closed, and $V = \{ x \in \mathbb{F}^n : f(x) \; \forall f \in \mathcal{I} \}$ its variety. The vanishing ideal of V is

$$\left\{ f \in \mathbb{F}[x_1, \dots, x_n] : \exists m \in \mathbb{N} : -f^{2m} \in \mathcal{I} + \sum \mathbb{F}[x_1, \dots, x_n]^2 \right\}.$$

Proof. By Theorem A.4, the ideal $\mathcal{I}$ is finitely generated, by polynomials $f_1, \dots, f_r \in \mathbb{F}[x_1, \dots, x_n]$. Then Positivstellensatz shows that f vanishes on V if and only if there exists $m \in \mathbb{N}$ such that $-f^{2m} \in \mathcal{P}(f_i, -f_i)$. Clearly $\mathcal{P}' = \mathcal{P}(f_i, -f_i)$ sits inside the cone $\mathcal{I} + \sum \mathbb{F}[x_1, \dots, x_n]^2$. Conversely, $\mathcal{P}'$ contains the smallest cone $\sum \mathbb{F}[x_1, \dots, x_n]^2$ and it also contains $\mathcal{I}$ as $\sum_i g_i f_i = \sum_i \left(\frac{g_i+1}{2}\right)^2 f_i + \sum_i \left(\frac{g_i-1}{2}\right)^2 (-f_i) \in \mathcal{P}'$. □

5.2 Semidefinite programming

5.3 Exercises

Choose exercises to solve from the list below for up to 5 bonus points. Solutions must be submitted on MyCourses by **Thursday, June 1, 12:00**.

5.1 Derive the Positivstellensatz from the Formal Positivstellensatz. $\boxed{\text{2 points}}$

5.2 Derive Theorem 4.5 from the Positivstellensatz. $\boxed{\text{2 points}}$

5.3 Derive the Positivstellensatz from the Real Nullstellensatz. $\boxed{\text{4 points}}$

5.4 Use the `TSSOS` package in Julia to compute an approximate sums of squares decomposition of the Motzkin polynomial. $\boxed{\text{3 points}}$

5.5 Consider the set PD_3 consisting of positive definite symmetric 3×3-matrices. This is a full-dimensional set in the 6-dimensional spaces of symmetric matrices $\mathrm{Sym}_3(\mathbb{R})$. Show that the polynomial

$$\sigma_{13}^2\sigma_{23}^2 - 2\sigma_{12}\sigma_{13}\sigma_{23}\sigma_{33} + \sigma_{12}^2\sigma_{33}^2$$

is non-negative on this space. $\boxed{\text{5 points}}$