Math 591 – Real Algebraic Geometry and Convex Optimization

Lecture 7: Certifying nonnegativity and the Positivstellensatz

Cynthia Vinzant, Spring 2019

Today we fix a basic closed semialgebraic set $S = \{x \in \mathbb{R}^n : g_1(x) \geq 0, \ldots, g_s(x) \geq 0\}$ and consider the set of polynomials that are nonnegative on S:

$$\mathcal{P}(S) \;=\; \{f \in \mathbb{R}[x_1, \ldots, x_n] \;:\; f(x) \geq 0 \text{ for all } x \in S\}.$$

Some important examples to keep in mind are $S = \mathbb{R}^n, (\mathbb{R}_{\geq 0})^n, [0,1]^n$, a real variety, or a finite collection of points.

The main question of the day is: what polynomials are *obviously* nonnegative on S? In other words, how would we *certify* that a polynomial belongs to $\mathcal{P}(S)$?

Some polynomials that are obviously nonnegative on S:

- h^2 for any $h \in \mathbb{R}[x_1, \ldots, x_n]$,
- $g_1, \ldots, g_s$,
- the sum of any of the above,
- the product of any of the above.

This list inspires the following definition:

Definition. A **preordering** of $\mathbb{R}[x_1, \ldots, x_n]$ is a subset $P \subset \mathbb{R}[x_1, \ldots, x_n]$ satisfying

- $h^2 \in P$ for all $h \in \mathbb{R}[x_1, \ldots, x_n]$ (contains all squares),
- $P + P \subseteq P$ (closure under addition), and
- $P \cdot P \subseteq P$ (closure under multiplication).

Clearly $\mathcal{P}(S)$ is a preordering of $\mathbb{R}[x_1, \ldots, x_n]$, but there others.

Example. An preordering contains squares and is closed under addition. Therefore the smallest preordering is the set of sums of squares:

$$\mathrm{SOS}_n \;=\; \left\{ \sum_{i=1}^{k} h_i^2 \;:\; k \in \mathbb{N},\; h_1, \ldots, h_k \in \mathbb{R}[x_1, \ldots, x_n] \right\}.$$

To see that this is closed under multiplication, note that $(\sum_i h_i^2)(\sum_j \tilde{h}_j^2) = \sum_{i,j} (h_i \tilde{h}_j)^2$.

One might also ask what the smallest preorder is that contains the given polynomials $g_1, \ldots, g_s$.

Definition/Proposition. The **preordering generated by** $g_1, \ldots, g_s \in \mathbb{R}[x_1, \ldots, x_n]$, denoted $\mathrm{PO}(g_1, \ldots, g_s)$, is the smallest preordering containing $g_1, \ldots, g_s$. It equals

$$\mathrm{PO}(g_1, \ldots, g_s) \;=\; \left\{ \sum_{\alpha \in \{0,1\}^s} \sigma_\alpha g_1^{\alpha_1} \cdots g_s^{\alpha_s} \;:\; \sigma_\alpha \in \mathrm{SOS}_n \text{ for all } \alpha \in \{0,1\}^s \right\}.$$

Proof. ($\supseteq$) By definition, a preordering containing $g_1, \ldots, g_s$ must contain polynomials of the form $\sigma_\alpha g_1^{\alpha_1} \cdots g_s^{\alpha_s}$ where σ_α is a sum of squares and sums of such polynomials.

($\subseteq$) To show that $\mathrm{PO}(g_1, \ldots, g_s)$ belongs to the RHS, it suffices to show that the RHS set is a preordering. It clearly contains squares and is closed under addition. It is also closed under multiplication! To see this, note that we can write the product of terms as

$$(\sigma_\alpha g_1^{\alpha_1}\cdots g_s^{\alpha_s})\cdot\left(\sigma_\beta g_1^{\beta_1}\cdots g_s^{\beta_s}\right) \;=\; \sigma_\alpha\cdot\sigma_\beta\cdot h^2\cdot g_1^{\gamma_1}\cdots g_s^{\gamma_s},$$

where $\gamma_i \equiv \alpha_i+\beta_i \mod 2$ and $h=\prod_i g_i^{(\alpha_i+\beta_i-\gamma_i)/2}$. Since the product of two sum of squares is again a sum of squares, we see that the coefficient $\sigma_\alpha\cdot\sigma_\beta\cdot h^2$ is a sum of squares and the product has the form of a sum of squares times a square-free product of $g_1,\ldots,g_s$. $\square$

Example. ($s=1$) The preorder generated by a single polynomial g has the form

$$\mathrm{PO}(g) \;=\; \{\sigma_0+\sigma_1 g \;:\; \sigma_0,\sigma_1\in \mathrm{SOS}_n\}.$$

For example, let's take $n=1$ and $g=1-x^2$. The semialgebraic set defined by g is the interval $[-1,1]$. Written in the monomial basis, it is unclear whether or not the polynomial $f=-4x^3-3x^2+4x+5$ is nonnegative on S, but we can write f as an element of $\mathrm{PO}(g)$:

$$f \;=\; -4x^3-3x^2+4x+5 \;=\; 1+x^4+(x+2)^2(1-x^2) \;=\; (1^2+(x^2)^2)+(x+2)^2 g,$$

which makes it clear that $f\geq 0$ on $[-1,1]$.

Example. ($s=2$) The preorder generated by two polynomials g_1,g_2 has the form

$$\mathrm{PO}(g_1,g_2) \;=\; \{\sigma_0+\sigma_1 g_1+\sigma_2 g_2+\sigma_{12}g_1g_2 \;:\; \sigma_0,\sigma_1,\sigma_2,\sigma_{12}\in\mathrm{SOS}_n\}.$$

For example, let's take $n=2$ and $g_1=x$ and $g_2=y$. The corresponding semialgebraic set is the nonnegative orthant $(\mathbb{R}_{\geq 0})^2$. Then polynomial $f=1+x+y-2x^2-2y^2+xy+x^3+y^3$ is nonnegative on $(\mathbb{R}_{\geq 0})^2$, as evidenced by its representation as an element in $\mathrm{PO}(x,y)$:

$$f=1+x+y-2x^2-2y^2+xy+x^3+y^3=1+(1-x)^2x+(1-y)^2y+xy.$$

This leads to the natural question: does $\mathrm{PO}(g_1,\ldots,g_s)$ contain every polynomial that is nonnegative on S? Let us consider this question in the case $S=\mathbb{R}^n$, where the preorder is the set of sums of squares.

It will be helpful to bound the degrees of the polynomials in question. Consider

$$\begin{aligned}\mathrm{SOS}_{n,\leq 2d} \;&=\; \left\{\sum_{i=1}^{k} h_i^2 \;:\; h_i\in\mathbb{R}[x_1,\ldots,x_n]_{\leq d}\right\}, \text{ and}\\ \mathcal{P}_{n,\leq 2d} \;&=\; \{f\in\mathbb{R}[x_1,\ldots,x_n]_{\leq 2d} \;:\; f(p)\geq 0 \text{ for all } p\in\mathbb{R}^n\}.\end{aligned}$$

The following is a classical theorem of Hilbert:

Theorem (Hilbert)**.** $\mathrm{SOS}_{n,\leq 2d}=\mathcal{P}_{n,\leq 2d}$ *if and only if* $n=1$, $2d=2$, *or* $(n,2d)=(2,4)$.

Sketch of proof. ($\Leftarrow$) ($n=1$) Suppose $f\in\mathbb{R}[x]$ is a nonnegative univariate polynomial. Then all real roots of f appear have even multiplicity and non-real roots come in complex conjugate pairs. Then we can write $f=\prod_j(x-r_j)^2\cdot\prod_k((x-a_k)^2+b_k^2)$ where r_j and $a_k\pm ib_k$ are the roots of f. Note that this is a product of sums of squares and therefore a sum of squares!

($2d=2$) Any quadratic polynomial $f\in\mathbb{R}[x_1,\ldots,x_n]_{\leq 2}$ can be (uniquely) written as $f(\underline{x})=\begin{pmatrix}1 & \underline{x}\end{pmatrix} Q \begin{pmatrix}1 & \underline{x}\end{pmatrix}^T$ for a $(n+1)\times(n+1)$ real symmetric matrix Q. Moreover if f is nonnegative on $\mathbb{R}^n$, then the matrix Q is positive semidefinite, in which case we can write $Q = \sum_{i=1}^{k} v_i v_i^T$ for some vectors $v_i \in \mathbb{R}^{n+1}$. Then

$$f(\underline{x}) \;=\; \left(1 \;\; \underline{x}\right) Q \left(1 \;\; \underline{x}\right)^T \;=\; \sum_{i=1}^{k} \left(1 \;\; \underline{x}\right) v_i v_i^T \left(1 \;\; \underline{x}\right)^T \;=\; \sum_{i=1}^{k} \left(\left(1 \;\; \underline{x}\right) \cdot v_i\right)^2,$$

which is a sum of squares.

The case $(n, 2d) = (2, 4)$ is more involved and we skip its proof.

($\Rightarrow$) The minimal $(n, 2d)$ pairs not covered above are $(n, 2d) = (2, 6)$ and $(3, 4)$. Hilbert's original proof was non-constructive, but here are explicit examples of nonnegative polynomials that are not sums of squares:

$$\begin{array}{ll} (n, 2d) = (2, 6) \qquad\qquad & 1 - 3x^2y^2 + x^4y^2 + x^2y^4 \\ (n, 2d) = (3, 4) \qquad\qquad & 1 - 4xyz + x^2y^2 + x^2z^2 + y^2z^2 \end{array}$$

These polynomials were found by Motzkin and Choi-Lam, respectively, almost a hundred years after Hilbert's original proof. (Neither the fact that these polynomials are nonnegative or nor that they are not sums of squares is obvious! As a challenge, try to show that they are nonnegative using the arithmetic-geometric mean inequality.)

From this, one can construct examples of nonnegative polynomials that are not sum of squares for all higher $n, 2d$. $\square$

Interestingly, if we multiply the Motzkin polynomial by $(1 + x^2 + y^2)$, the result *is* a sum of squares:

$$\begin{aligned}(1 + x^2 + y^2)(1 - 3x^2y^2 + x^4y^2 + x^2y^4) = {} & 2(\tfrac{1}{2}x^3y + \tfrac{1}{2}xy^3 - xy)^2 + (x^2y - y)^2 + (xy^2 - x)^2 \\ & + \tfrac{1}{2}(x^3y - xy)^2 + \tfrac{1}{2}(xy^3 - xy)^2 + (x^2y^2 - 1)^2.\end{aligned}$$

This expression as a *ratio* of sums of squares confirms that the Motzkin polynomial is nonnegative on $\mathbb{R}^2$. One of Hilbert's famous problems at the turn of the 20th century was to show that every nonnegative polynomial has such an expression.

Hilbert's 17th Problem. Is every nonnegative polynomial a ratio of sums of squares?

This was answered positively by Artin in 1927. A more general statement was proven by Krivine in 1964 and rediscovered by Stengle in 1974.

Theorem. *Let* $g_1, \ldots, g_s \in \mathbb{R}[x_1, \ldots, x_n]$ *and* $S = \{x \in \mathbb{R}^n : g_1(x) \geq 0, \ldots, g_s(x) \geq 0\}$. *Let* P *denote the preordering* $\mathrm{PO}(g_1, \ldots, g_s)$. *Then for any* $f \in \mathbb{R}[x_1, \ldots, x_n]$,

- $f > 0$ *on* S $\Leftrightarrow$ $q \cdot f = 1 + p$ *for some* $p, q \in P$,
- $f \geq 0$ *on* S $\Leftrightarrow$ $q \cdot f = f^{2m} + p$ *for some* $m \in \mathbb{N}$, $p, q \in P$,
- $f = 0$ *on* S $\Leftrightarrow$ $-f^{2m} \in P$ *for some* $m \in \mathbb{N}$, *and*
- $S = \emptyset$ $\Leftrightarrow$ $-1 \in P$

Idea of proof. The $\Leftarrow$ implications follow directly from the fact that all polynomials in P are nonnegative on the set S. These representations are *certificates* of the behavior of f.

The $\Rightarrow$ implications are much harder. The rough idea is to extend P to an *ordering* of $\mathbb{R}[x_1, \ldots, x_n]$ and from there to an ordering on a field over which the statement holds. One can then use *model theoretic* statements to show that it must hold over $\mathbb{R}$. In particular, this relies on

Theorem (Tarski Transfer Principle)**.** *If a system of polynomial inequalities with coefficients in $\mathbb{R}$ has a solution over some ordered field extension of $\mathbb{R}$, then it has a solution over $\mathbb{R}$.*

For more details, see, for example, the book *Positive Polynomials and Sums of Squares* by Murray Marshall. $\square$

The name "Positivstellensatz" literally means "positive place theorem" in German.

One corollary of this statement is that every nonnegative polynomial is a ratio of sums of squares (obtained by taking $P = \mathrm{SOS}_n$ and $S = \mathbb{R}^n$). Another characterized when a real variety is empty. (Literally, the real "zero place theorem".)

Corollary (Real Nullstellensatz)**.** *For $f_1, \ldots, f_r \in \mathbb{R}[x_1, \ldots, x_n]$, the real variety $V_{\mathbb{R}}(f_1, \ldots, f_r)$ is empty if and only if*

$$-1 \;=\; \sigma + \sum_{i=1}^{r} h_i f_i$$

for some sum of squares $\sigma \in \mathrm{SOS}_n$ and polynomial multipliers $h_i \in \mathbb{R}[x_1, \ldots, x_n]$.

Example. For example, take $f_1 = x^2 + y^2 - 1$ and $f_2 = y - 2$. While there are complex solutions to $f_1 = f_2 = 0$, there are no real solutions. As promised, by the real Nullstellensatz, we can find an expression

$$-1 \;=\; \left(\frac{x}{\sqrt{3}}\right)^2 - \frac{1}{3}(x^2 + y^2 - 1) + \frac{y+2}{3}(y-2) \;=\; \left(\frac{x}{\sqrt{3}}\right)^2 + \frac{-1}{3} \cdot f_1 + \frac{y+2}{3} \cdot f_2.$$

Plugging in a real point $(x, y) \in \mathbb{R}^2$ for which $f_1(x, y) = 0$ and $f_2(x, y) = 0$ would result in an expression $-1 \geq 0$, so no such point exists!

Next time we'll talk about how one might find such expressions.