3. Putinar's Theorem

We derive some fundamental theorems which (under certain conditions) provide beautiful and useful representations of polynomials p strictly positive on a semialgebraic set. In particular, we are concerned with Putinar's Theorem, which will be the basis for the semidefinite hierarchies for polynomial optimization discussed later, as well as with the related statement of Jacobi and Prestel.

In the following let $g_1, \ldots, g_m \in \mathbb{R}[x] = \mathbb{R}[x_1, \ldots, x_n]$ and $S = S(g_1, \ldots, g_m)$. Recall from Example 1.7 that $\mathrm{QM}(g_1, \ldots, g_m)$ is the quadratic module defined by $g_1, \ldots, g_m$. Before we state Putinar's Theorem, we provide several equivalent formulations of the precondition which we need.

A quadratic module $M \subset \mathbb{R}[x]$ is *Archimedean* if for every $h \in \mathbb{R}[x]$ there is some $N \in \mathbb{N}$ such that $N \pm h \in M$.

THEOREM 1.15. *For a quadratic module $M \subset \mathbb{R}[x]$, the following conditions are equivalent:*

(1) M is Archimedean.
(2) There exists $N \in \mathbb{N}$ such that $N - \sum_{i=1}^n x_i^2 \in M$.

PROOF. The implication $1 \Longrightarrow 2$ is obvious.

For the implication $2 \Longrightarrow 1$, let $N \in \mathbb{N}$ such that $N - \sum_{i=1}^n x_i^2 \in M$. It suffices to prove that the set

$$Z := \{p \in \mathbb{R}[x] \ : \ \exists N' > 0 \text{ with } N' \pm p \in M\}$$

coincides with $\mathbb{R}[x]$.

Clearly, the set $\mathbb{R}$ is contained in Z and Z is closed under addition. Z is also closed under multiplication, which follows from setting $g := p \pm q$, $h := p \mp q$ and considering the identity

$$\begin{aligned} \frac{N_1^2}{2} \mp pq &= \frac{1}{4}\Big(N_1^2 + h^2 + \frac{1}{2N_1}\left((N_1+g)(N_1^2-g^2) + (N_1-g)(N_1^2-g^2)\right)\Big) \\ &= \frac{1}{4}\left(N_1^2 + h^2 + \frac{1}{2N_1}\left((N_1+g)^2(N_1-g) + (N_1-g)^2(N_1+g)\right)\right). \end{aligned}$$

Moreover, Z contains each variable x_i because of the identity

$$\frac{N+1}{2} \pm x_i = \frac{1}{2}\left((x_i \pm 1)^2 + (N - \sum_{j=1}^n x_j^2) + \sum_{j \neq i} x_j^2\right).$$

As a consequence of these properties, we have $Z = \mathbb{R}[x]$. □

We give further equivalent characterizations of the property that M is Archimedean.

Remark 1.16. For a quadratic module $\mathrm{QM}(g_1, \ldots, g_m)$ mit $g_1, \ldots, g_m \in \mathbb{R}[x]$, the following conditions are equivalent as well:

(1) The quadratic module $\mathrm{QM}(g_1, \ldots, g_m)$ is Archimedean.
(2) There exists an $N \in \mathbb{N}$ such that $N - \sum_{i=1}^{n} x_i^2 \in \mathrm{QM}(g_1, \ldots, g_m)$.
(3) There exists an $h \in \mathrm{QM}(g_1, \ldots, g_m)$ such that $S(h)$ is compact.
(4) There exist finitely many polynomials $h_1, \ldots, h_r \in \mathrm{QM}(g_1, \ldots, g_m)$ such that $S(h_1, \ldots, h_r)$ is compact and $\prod_{i \in I} h_i \in \mathrm{QM}(g_1, \ldots, g_m)$ for all $I \subset \{1, \ldots, r\}$.

The implications $1 \Longrightarrow 2 \Longrightarrow 3 \Longrightarrow 4$ are obvious. We will give a proof of $4 \Longrightarrow 1$ in Lemma 1.28 in the next section.

The conditions in Theorem 1.15 and Remark 1.16 are actually not conditions on the compact set S, but on its representation in terms of the polynomials $g_1, \ldots, g_m$. See Exercise 12 for an example which shows that the conditions are stronger than just requiring that S is compact. In many practical applications, the precondition in Theorem 1.15 can be imposed by adding a witness of compactness, $N - \sum_{i=1}^{n} x_i^2 \geq 0$ for some $N > 0$.

Theorem 1.17 (Putinar). *Let $S = S(g_1, \ldots, g_m)$ and suppose that $\mathrm{QM}(g_1, \ldots, g_m)$ is Archimedean. If a polynomial $f \in \mathbb{R}[x]$ is positive on S then $f \in \mathrm{QM}(g_1, \ldots, g_m)$. That is, there exist sums of squares $\sigma_0, \ldots, \sigma_m \in \Sigma[x]$ with*

$$f \;=\; \sigma_0 + \sum_{i=1}^{m} \sigma_i g_i \,. \tag{3.1}$$

It is evident that each polynomial of the form (3.1) is nonnegative on the set S.

Example 1.18. The strict positivity in Putinar's Theorem is essential, even for univariate polynomials. This can be seen in the example $p = 1 - x^2$, $g = g_1 = (1 - x^2)^3$, see Figure 3.

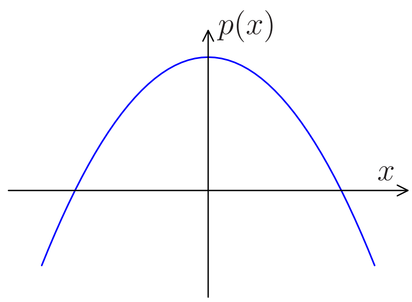

Figure 3. Graph of $p(x) = 1 - x^2$.

The feasible set S is the interval $S = [-1, 1]$, and hence the minima of the function $p(x)$ are at $x = -1$ and $x = 1$, both with function value 0. The precondition of Putinar's theorem is satisfied since

$$\frac{2}{3} + \frac{4}{3}\left(x^3 - \frac{3}{2}x\right)^2 + \frac{4}{3}\left(1 - x^2\right)^3 \;=\; 2 - x^2 \,.$$

If a representation of the form (3.1) existed, i.e.,

$$1 - x^2 \;=\; \sigma_0(x) + \sigma_1(x)(1-x^2)^3 \quad \text{with } \sigma_0, \sigma_1 \in \Sigma[x]\,, \tag{3.2}$$

then the right hand side of (3.2) must vanish at $x = 1$ as well. The second term has at 1 a zero of at least third order, so that σ_0 vanishes at 1 as well; by the SOS-condition this zero of σ_0 is of order at least 2. Altogether, on the right hand side we have at 1 a zero of at least second order, in contradiction to the order 1 of the left side. Thus there exists no representation of the form (3.2).

When p is nonnegative on a compact set $S(g_1, \ldots, g_m)$ and the module $\mathrm{QM}(g_1, \ldots, g_m)$ is Archimedean, then $p + \varepsilon \in \mathrm{QM}(g_1, \ldots, g_m)$. However, for $\varepsilon \to 0$, the smallest degrees of those representations may be unbounded.

In the remaining part of the chapter, we present a proof of Putinar's Theorem. Let $g_1, \ldots, g_m \in \mathbb{R}[x]$ and $K := \{x \in \mathbb{R}^n \,:\, g_j(x) \geq 0,\, 1 \leq j \leq m\}$. We say that $g_1, \ldots, g_m$ have the *Putinar property*, if each strictly positive polynomial on K is contained in $\mathrm{QM}(g_1, \ldots, g_m)$.

LEMMA 1.19. *Let $g_1, \ldots, g_m \in \mathbb{R}[x]$ such that K is compact and $g_1, \ldots, g_m$ has the Putinar property. For every $g_{m+1} \in \mathbb{R}[x]$, the sequence $g_1, \ldots, g_{m+1}$ has the Putinar property as well.*

For the proof, we us the following special case of the Stone-Weierstraß Theorem from classical analysis.

THEOREM 1.20. *For each continuous function f on a compact set $C \subset \mathbb{R}^n$, there exists a sequence (f_k) of polynomials which converges uniformly to f on C.*

PROOF OF LEMMA 1.19. Let $g_1, \ldots, g_m$ have the Putinar property. Further let f be a polynomial which is strictly positive on

$$K' := \{x \in \mathbb{R}^n \,:\, g_j(x) \geq 0,\, 1 \leq j \leq m+1\}.$$

It suffices to show that there exists some $\sigma_{m+1} \in \Sigma[x]$ with $f - \sigma_{m+1} g_{m+1} > 0$ on K. We can assume that f is not strictly positive on K, since otherwise we can simply set $\sigma_{m+1} \equiv 0$. Set

$$D \;:=\; K \setminus K' \;=\; \{x \in \mathbb{R}^n \;:\; g_j(x) \geq 0,\, 1 \leq j \leq m,\, g_{m+1} < 0\}$$

and

$$M \;:=\; \max \left\{ \frac{f(x)}{g_{m+1}(x)} \;:\; x \in D \right\} + 1. \tag{3.3}$$

This maximum exists, since the closure of D is compact and $\frac{f}{g_{m+1}}$ converges to $-\infty$ when $x \in D$ tends to $(\mathrm{cl}\, D) \setminus D$. Since $g_{m+1}(x) < 0$ on D and there exists $y \in D$ with $f(y) \leq 0$, we see that M is positive. Define the function $\bar{\sigma}_{m+1} : \mathbb{R}^n \to \mathbb{R}$ as

$$\bar{\sigma}_{m+1}(x) \ := \ \begin{cases} \min\left\{M, \frac{f(x)}{2g_{m+1}(x)}\right\} & \text{if } g_{m+1}(x) > 0, \\ M & \text{if } g_{m+1}(x) \le 0. \end{cases}$$

$\bar{\sigma}_{m+1}$ is positive on K and continuous, and the continuous function $f - \bar{\sigma}_{m+1} g_{m+1}$ is positive on K as well. By the Stone-Weierstraß Theorem 1.20, the polynomial $\sqrt{\bar{\sigma}_{m+1}}$ can be approximated by some polynomial $r \in \mathbb{R}[x]$ such that

$$f - r^2 g_{m+1} > 0 \text{ on } K,$$

because g_{m+1} is bounded on K. Setting $\sigma_{m+1} := r^2$ gives the desired statement. □

Example 1.21. Let $m = 1$. We show that for every $N > 0$, the polynomial

$$g_1 = N - \sum_{i=1}^{n} x_i^2$$

has the Putinar property. By a scaling argument, we can assume $N = 1$. The identity

$$\frac{1}{2}\left((x_1 - 1)^2 + \sum_{i=2}^{n} x_i^2 + (1 - \sum_{i=1}^{n} x_i^2)\right) \ = \ 1 - x_1 \tag{3.4}$$

shows that the affine polynomial $1 - x_1$ is contained in $\mathrm{QM}(g_1)$. The variety $V := \{x \in \mathbb{R}^n : 1 - x_1 = 0\}$ of this polynomial is a tangent hyperplane to the unit sphere $\mathbb{S}^{n-1}$, and by spherical symmetry, the polynomials underlying all tangent hyperplanes of $\mathbb{S}^{n-1}$ are contained in $\mathrm{QM}(g_1)$.

Let $h_1, \ldots, h_{n+1}$ be polynomials describing tangent hyperplanes to $\mathbb{S}^{n-1}$, such that

$$\Delta := \{x \in \mathbb{R}^n : h_i(x) \ge 0, \, 1 \le i \le n+1\}$$

forms a simplex containing $\mathbb{S}^{n-1}$. If p is strict positive polynomial on Δ, then there exists a Handelman representation

$$p = \sum_{\beta} c_\beta h_1^{\beta_1} \cdots h_{n+1}^{\beta_{n+1}}$$

with non-negative coefficients c_β. Each polynomial h_i in this representation defines a hyperplane to $\mathbb{S}^{n-1}$ and thus be can expressed through (3.4) in terms of the polynomial $1 - \sum_{i=1}^{n} x_i^2$ and sums of squares. Even powers of $1 - \sum_{i=1}^{n} x_i^2$ can be viewed as sums of squares, so that p can be written as

$$p \ = \ \sigma_0 \left(1 - \sum_{i=1}^{n} x_i^2\right) + \sigma_1$$

with sums of squares σ_0 and σ_1. By Theorem 1.15, the sequence of affine polynomials $h_1, \ldots, h_{n+1}$ has the Putinar property. To see this, consider without loss of generality the polynomials $1 - x_1, \dots, 1 - x_n, \sum_{i=1}^n x_i$. Further, Lemma 1.19 implies that the sequence $h_1, \dots, h_{n+1}, 1 - \sum_{i=1}^n x_i^2$ has the Putinar property. Since

$$\mathrm{QM}\left(h_1, \dots, h_n, 1 - \sum_{i=1}^n x_i^2\right) = \mathrm{QM}\left(1 - \sum_{i=1}^n x_i^2\right),$$

the single polynomial $1 - \sum_{i=1}^n x_i^2$ has the Putinar property.

Proof of Putinar's Theorem 1.17. Since $\mathrm{QM}(g_1, \dots, g_m)$ is Archimedean, there exists $N > 0$ such that $N - \sum_{i=1}^n x_i^2 \in \mathrm{QM}(g_1, \dots, g_m)$. Since $\mathrm{QM}(g_1, \dots, g_m) = \mathrm{QM}(g_1, \dots, g_m, N - \sum_{i=1}^n x_i^2)$, it suffices to show that $g_1, \dots, g_m, N - \sum_{i=1}^n x_i^2$ has the Putinar property.

By Example 1.21, the single polynomial $N - \sum_{i=1}^n x_i^2$ has the Putinar property. Inductively, Lemma 1.19 then implies that $g_1, \dots, g_m, N - \sum_{i=1}^n x_i^2$ has the Putinar property. □

In Example 1.21, we have already encountered sequences of affine polynomials. The subsequent statement says that quadratic modules generated by a sequence of affine polynomials with compact feasible sets are always Archimedean.

Lemma 1.22. *Let $g_1, \dots, g_m \in \mathbb{R}[x]$ affine and $K := \{x \in \mathbb{R}^n : g_j(x) \geq 0,\ 1 \leq j \leq m\}$ compact, then $\mathrm{QM}(g_1, \dots, g_m)$ is Archimedean.*

Proof. It suffices to show that there exists $N > 0$ such that $N - \sum_{i=1}^n x_i^2 \in \mathrm{QM}(g_1, \dots, g_m)$. In the special case $K = \emptyset$, Farkas' Lemma from linear programming yields that the constant -1 is a nonnegative linear combination of the affine polynomials $g_1, \dots, g_m$. Hence, $\mathrm{QM}(g_1, \dots, g_m) = \mathbb{R}[x]$, which implies the proof of the special case.

Now let $K \neq \emptyset$. Then the example follows from from Example 1.21, where first a simplex was considered, and then the addition of further inequalities preserves the Putinar property. □

As a corollary, we obtain the following Positivstellensatz of Jacobi and Prestel, which does not need any additional technical precondition concerning the Archimedean property of the quadratic module.

In the following, let $g_1, \dots, g_m \in \mathbb{R}[x] = \mathbb{R}[x_1, \dots, x_n]$ and $S = S(g_1, \dots, g_m)$. Recall from Example 1.7 that $\mathrm{QM}(g_1, \dots, g_m)$ is the quadratic module defined by $g_1, \dots, g_m$.

Theorem 1.23 (Jacobi-Prestel). *Suppose that S is nonempty and bounded, and that $\mathrm{QM}(g_1, \dots, g_m)$ contains linear polynomials $\ell_1, \dots, \ell_k$ with $k \geq 1$ such that the polyhedron $S(\ell_1, \dots, \ell_k)$ is bounded. If p is strictly positive on S, then $p \in \mathrm{QM}(g_1, \dots, g_m)$.*

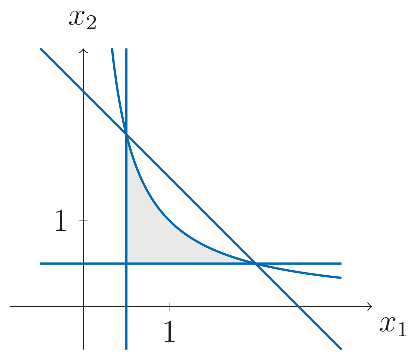

FIGURE 4. The feasible region $S(g_1, \ldots, g_4)$ for $g_1 = x_1 - 1/2$, $g_2 = x_2 - 1/2$, $g_3 = 1 - x_1 x_2$, $g_4 = 5/2 - x_1 - x_2$.

PROOF. By Lemma 1.22, the quadratic module $\mathrm{QM}(\ell_1, \ldots, \ell_k)$ is Archimedean. Hence, it has the Putinar property. By Lemma 1.19, $\mathrm{QM}(\ell_1, \ldots, \ell_k, g_1, \ldots, g_m)$ has the Putinar property as well, and so does $\mathrm{QM}(g_1, \ldots, g_m) = \mathrm{QM}(\ell_1, \ldots, \ell_k, g_1, \ldots, g_m)$. □

EXAMPLE 1.24. Let $g_1 = x_1 - 1/2$, $g_2 = x_2 - 1/2$, $g_3 = 1 - x_1 x_2$, $g_4 = 5/2 - x_1 - x_2$, see Figure 4 for an illustration of $S = S(g_1, \ldots, g_4)$. The polynomial $p = 8 - x_1^2 - x_2^2$ is strictly positive on the set $S = S(g_1, g_2, g_3, g_4)$, and since $S(g_1, g_2, g_4)$ is a bounded polygon, Theorem 1.23 guarantees that $p \in \mathrm{QM}(g_1, \ldots, g_4)$. To write down one such a representation, first observe that the identities

$$\begin{aligned} 2 - x_i &= \left(\frac{5}{2} - x_1 - x_2\right) + \left(x_{3-i} - \frac{1}{2}\right), \\ 2 + x_i &= \left(x_i - \frac{1}{2}\right) + \frac{5}{2} \end{aligned}$$

($i \in \{1, 2\}$) allow that we may additionally use the box contraints $2 - x_i \geq 0$ and $2 + x_i \geq 0$ for our representation. Then, clearly, one possible Jacobi-Prestel representation for p is provided by

$$p = \frac{1}{4} \sum_{i=1}^{2} \left((2 + x_i)^2 (2 - x_i) + (2 - x_i)^2 (2 + x_i)\right).$$

Note that the feasible S does not change if we omit the linear constraint $g_4 \geq 0$. Interestingly, then the precondition of Theorem 1.23 is no longer satisfied, and, as we will see in Exercise 12, although p is strictly positive on $S(g_1, g_2, g_3)$, it is not contained $\mathrm{QM}(g_1, g_2, g_3)$.

Schmüdgen's Theorem. The following fundamental Theorem of Schmüdgen is closely related to Putinar's Theorem. Under the condition of compactness of the feasible set, it characterizes (in contrast to Theorem 1.12) a representation of the polynomial p itself in terms of the preorder of the polynomials defining the feasible set.