On the complexity of Schmüdgen's Positivstellensatz

Markus Schweighofer

Universität Konstanz, Fachbereich Mathematik und Statistik, 78457 Konstanz, Allemagne [1]

Abstract

Schmüdgen's Positivstellensatz roughly states that a polynomial f positive on a compact basic closed semialgebraic subset S of $\mathbb{R}^n$ can be written as a sum of polynomials which are nonnegative on S for certain obvious reasons. However, in general, you have to allow the degree of the summands to exceed largely the degree of f. Phenomena of this type are one of the main problems in the recently popular approximation of nonconvex polynomial optimization problems by semidefinite programs. Prestel [PD] proved that there exists a bound on the degree of the summands computable from the following three parameters: The exact description of S, the degree of f and a measure of how close f is to having a zero on S. Roughly speaking, we make explicit the dependence on the second and third parameter. In doing so, the third parameter enters the bound only polynomially.

Key words: Positivstellensatz, complexity, positive polynomial, sum of squares, preordering, moment problem, optimization of polynomials

1 Introduction

Throughout the paper, we suppose $1 \leq n \in \mathbb{N}$ and abbreviate $(X_1, \dots, X_n)$ by $\bar{X}$. We let $\mathbb{R}[\bar{X}]$ denotes the polynomial ring over $\mathbb{R}$ in n indeterminates. By $\sum \mathbb{R}[\bar{X}]^2$ we mean the set of all sums of squares in this polynomial ring. For $\alpha \in \mathbb{N}^n$, we introduce the notation

$$|\alpha| := \alpha_1 + \cdots + \alpha_n \qquad \text{and} \qquad \bar{X}^\alpha := X_1^{\alpha_1} \cdots X_n^{\alpha_n}.$$

[1] The author was supported by the Deutsche Forschungsgemeinschaft (DFG) project "Darstellung positiver Polynome".

Definition 1 For a polynomial

$$f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha \frac{|\alpha|!}{\alpha_1! \cdots \alpha_n!} \bar{X}^\alpha \qquad (a_\alpha \in \mathbb{R}),$$

we define $\|f\| := \max\{|a_\alpha| \mid \alpha \in \mathbb{N}^n\}$.

This defines a norm on the real vector space $\mathbb{R}[\bar{X}]$. For homogeneous f, $\|f\|$ has already been introduced in [PR] with the different notation $L(f)$. It is a measure of the size of the coefficients of a polynomial with convenient properties illustrated by Lemma 8 below and the following example.

Example 2 For all $d \in \mathbb{N}$, $\left\|\sum_{k=0}^d (X_1 + \cdots + X_n)^k\right\| = 1$ since

$$(X_1 + \cdots + X_n)^k = \sum_{|\alpha|=k} \frac{k!}{\alpha_1! \cdots \alpha_n!} \bar{X}^\alpha.$$

The goal of this paper is to prove the following.

Theorem 3 *For all polynomials $g_1, \ldots, g_m \in \mathbb{R}[\bar{X}]$ defining a non–empty set*

$$S := \{x \in \mathbb{R}^n \mid g_1(x) \geq 0, \ldots, g_m(x) \geq 0\} \subseteq (-1,1)^n,$$

there is some $c \in \mathbb{N}$ with the following property:

Every $f \in \mathbb{R}[\bar{X}]$ of degree d with $f^* := \min\{f(x) \mid x \in S\} > 0$ can be written as

$$\sum_{\delta \in \{0,1\}^m} \sigma_\delta g_1^{\delta_1} \cdots g_m^{\delta_m} \qquad \textit{where} \qquad \sigma_\delta \in \sum \mathbb{R}[\bar{X}]^2 \tag{1}$$

such that $\sigma_\delta = 0$ or

$$\deg(\sigma_\delta g_1^{\delta_1} \cdots g_m^{\delta_m}) \leq c d^2 \left(1 + \left(d^2 n^d \frac{\|f\|}{f^*}\right)^c\right)$$

for all $\delta \in \{0,1\}^m$.

Here $(-1,1)$ denotes an open interval in $\mathbb{R}$. Note that the assumption on f to be contained in the open hypercube $(-1,1)^n$ has been made just for convenience. If we assume instead that S is contained in the open hypercube $(-r,r)^n$ for some $r > 0$, the statement remains true if we replace $\|f\|$ by $\|f(rX_1, \ldots, rX_n)\|$. This is clear from a simple scaling argument. Hence, we can actually apply the theorem to all bounded (or equivalently compact) S.

The second remark on the formulation of the theorem concerns the $\sigma_\delta \in \sum \mathbb{R}[\bar{X}]^2$. If $\sigma_\delta = \sum_{i=1}^t h_i^2$ for some $0 \neq h_1, \ldots, h_t \in \mathbb{R}[\bar{X}]$, then we have necessarily $2 \deg h_i \leq \deg \sigma_\delta \leq \deg \sigma_\delta g_1^{\delta_1} \cdots g_m^{\delta_m}$ which bounds also the degree of each h_i. Moreover, we may always choose t to be less or equal to $\binom{n+d'}{n}$ where $2d'$ denotes the degree of σ_δ since every sum of squares of degree $2d'$ is a sum of $\binom{n+d'}{n}$ squares in $\mathbb{R}[\bar{X}]$, see Theorem 8.1.3 in [PD].

Without the information on the degree of the summands, Theorem 3 is Schmüdgen's Positivstellensatz, see [Sn] or [PD]. The first algebraic proof of Schmüdgen's result is due to Wörmann [BW]. The author gave a third proof which is to a certain extent constructive [Sr1]. Giving up our goal in [Sr1] to symbolically compute representations (1), we manage here to give a tame version of this third proof which allows to keep track of complexity. To understand the proof of the above theorem which we will give in Section 3, it might certainly be helpful to read [Sr1] first.

Unfortunately, in Schmüdgen's theorem the condition $f > 0$ on S cannot be weakened to $f \geq 0$ on S. This is the main reason why there cannot exist a bound on the degree of the summands just depending on the description of S and the degree of f, see [Ste]. The third parameter $\|f\|/f^*$ in our bound is a natural measure of how close f is to having a zero on S.

Similar measures appear in the following theorems of other authors: Prestel proved by model and valuation theoretic methods the mere existence of a degree bound computable from the three parameters mentioned [PD, Theorem 8.3.4]. Stengle obtained a similar bound even more concrete than ours for the special case where $n = 1$ and S is a compact interval in $\mathbb{R}$ [Ste, Theorem 5] (see also [Mau]). Somehow related are also [Rez, Theorem 3.12] and [LS, Theorem 1.2]. An improved version of the latter due to Powers and Reznick [PR] will serve as one of the main ingredients in the proof given in Section 3.

The main drawback of Theorem 3 is that c depends on the description of S in an unspecified way. Note however that for any concrete situation, one can in principle hope to extract a suitable c from the proof in Section 3, see Remark 10.

We end this introduction with a short comparison between Schmüdgen's Positivstellensatz and classical related theorems with respect to complexity issues. We choose Artin's solution of Hilbert's 17th problem as a representative of the classical theorems. It says that every polynomial $f \in \mathbb{R}[\bar{X}]$ with $f \geq 0$ on $\mathbb{R}^n$ is a sum of squares in the quotient field $\mathbb{R}(\bar{X})$ of $\mathbb{R}[\bar{X}]$. In contrast to Schmüdgen's theorem (see, e.g., [PD, Lemma 8.2.3]), this statement remains valid when $\mathbb{R}$ is replaced by any other real closed field. Therefore, general model theoretic arguments imply the existence of a bound on the degree of the numerators and denominators in the expression of f as a sum of squares which depends solely on n and $\deg f$, confer [PD, Theorem 8.2.1]. One is tempted to think that it might then also be easier to get *explicit* degree bounds for

Hilbert's 17th problem than for Schmüdgen's theorem. But in fact, this is much harder and all the obtained bounds are multiply exponential [Sd].

This raises the question how this is compatible with the fact that all proofs of Schmüdgen's Positivstellensatz use classical results. In our proof of Theorem 3, the classical part comes in through the backdoor when we apply Schmüdgen's Theorem (without complexity information). Fortunately, at that point of the proof we can afford the lack of information about complexity on the expense of c. Altogether, we see that the classical situation has little to do with the situation we encountered here.

The author would like to thank two anonymous referees for their helpful comments and suggestions.

2 Approximation of polynomial optimization problems by semidefinite programs

In this section, we consider the problem of finding the minimum value f^* of a polynomial $f \in \mathbb{R}[\bar{X}]$ on a non–empty compact set

$$S := \{x \in \mathbb{R}^n \mid g_1(x) \geq 0, \ldots, g_m(x) \geq 0\}$$

defined by polynomials $g_1, \ldots, g_m \in \mathbb{R}[\bar{X}]$. We will partially investigate the efficiency of Lasserre's approach to this problem, see [Las], [Sr2] or [Mar] (compare also [Stu] and [PS]). In this approach, the given polynomial optimization problem gives rise to an infinite sequence of semidefinite optimization problems whose optimal values tend to the optimal value of the original problem.

For each $k \in \mathbb{N}$, denote by $C_k \subseteq \mathbb{R}[\bar{X}]$ the convex cone of all polynomials which can be expressed as a sum (1) where the degree of no summand exceeds k. Consider the following optimization problems:

(P_k) minimize $L(f)$ such that $L : \mathbb{R}[\bar{X}] \to \mathbb{R}$ is a vector–space homomorphism, $L(1) = 1$ and $L(C_k) \subseteq [0, \infty)$

(D_k) maximize a such that $f - a \in C_k$

For reasons which shall become clear in the sequel, we call (P_k) the k–th primal problem and (D_k) the k–th dual problem. For every $x \in S$, the evaluation at x

$$L_x : \mathbb{R}[\bar{X}] \to \mathbb{R} : h \mapsto h(x)$$

is a feasible solution of (P_k). Hence, if we denote by P_k^* the infimum of all $L(f)$ where L is a feasible solution of (P_k), we get $f^* \geq P_k^* \in \{-\infty\} \cup \mathbb{R}$. Moreover, if L is feasible in (P_k) and a in (D_k), then $L(f) \geq a$ since $f - a \in C_k$ implies $L(f) - a = L(f) - aL(1) = L(f - a) \geq 0$. Writing D_k^* for the supremum of all a feasible in (D_k), we get therefore

$$f^* \geq P_k^* \geq D_k^* \in \{-\infty\} \cup \mathbb{R}.$$

Lasserre observed that (P_k) and (D_k) can be easily formulated as so called semidefinite programs and are as such dual to each other, see [Sr2], [Las] or [Mar] (take notice of Remark 5). Semidefinite programs are generalizations of linear programs and can be solved efficiently whereas optimization of a polynomial is a hard problem.

This raises the question to what extent P_k^* and D_k^* approximate f^*. Since $C_0 \subseteq C_1 \subseteq C_2 \subseteq \dots$, the sequences $(P_k^*)_{k\in\mathbb{N}}$ and $(D_k^*)_{k\in\mathbb{N}}$ are of course increasing. Moreover, we have that $(D_k^*)_{k\in\mathbb{N}}$ and a fortiori $(P_k^*)_{k\in\mathbb{N}}$ converge to f^*. Indeed, for any $\varepsilon > 0$, we have $f - f^* + \varepsilon \in C_k$ for sufficiently large $k \in \mathbb{N}$ by Schmüdgen's Positivstellensatz, i.e., $f^* - \varepsilon$ is feasible in (D_k). But what about the rate of convergence? In the case $S \subseteq (-1,1)^n$, Theorem 4 shows that there exists some constant c (depending on the description of S) such that $f^* - cd^4n^{2d}\|f\|/\sqrt[c]{k}$ is feasible in (D_k) for sufficiently large k. This implies that the difference between the actual minimum f^* of f on S and D_k^* (hence also P_k^*) is not more than

$$cd^4n^{2d}\|f\|\frac{1}{\sqrt[c]{k}}.$$

Moreover, the "duality gap" $P_k^* - D_k^*$ is bounded by the same term. In this context, we should mention that in many cases $P_k^* = D_k^*$ holds anyway, see the original proof in [Las, Theorem 4.2(a)], Marshall's algebraic proof in [Mar, Note 3.3(1)] or its elementary exposition in [Sr2, Section 4].

Theorem 4 *For all polynomials $g_1, \dots, g_m \in \mathbb{R}[\bar{X}]$ defining a non–empty set*

$$S := \{x \in \mathbb{R}^n \mid g_1(x) \geq 0, \dots, g_m(x) \geq 0\} \subseteq (-1,1)^n,$$

there is some $1 \leq c \in \mathbb{N}$ with the following property:

For every $f \in \mathbb{R}[\bar{X}]$ of degree $d \geq 1$ and for all $k \in \mathbb{N}$ with $k \geq cd^cn^{cd}$, the polynomial

$$(f - f^*) + cd^4n^{2d}\|f\|\frac{1}{\sqrt[c]{k}}$$

equals an expression (1) with $\sigma_\delta = 0$ or $\deg(\sigma_\delta g_1^{\delta_1} \cdots g_m^{\delta_m}) \leq k$ for all $\delta \in \{0,1\}^m$.

Proof. Denote by c_0 the c guaranteed to exist by Theorem 3. We may assume $c_0 \geq 2$. Set $c := (4c_0)^{c_0} \geq 12c_0 \geq 3c_0 \geq c_0$. Suppose we have $f \in \mathbb{R}[\bar{X}]$ of degree $d \geq 1$ and $k \in \mathbb{N}$ with $k \geq cd^cn^{cd}$. We claim that

$$h := (f - f^*) + \mu$$

equals an expression (1) without summands of degree $> k$ even for

$$\mu := 12c_0 d^4 n^{2d} \|f\| \frac{1}{\sqrt[c_0]{k}} \leq c d^4 n^{2d} \|f\| \frac{1}{\sqrt[c]{k}}.$$

Noting that $k \geq (4c_0)^{c_0} d^{3c_0} n^{c_0 d}$, we get $\sqrt[c_0]{k} \geq 4c_0 d^3 n^d$ and then

$$3dn^d \|f\| \sqrt[c_0]{k} \geq 12c_0 d^4 n^{2d} \|f\| = \mu \sqrt[c_0]{k}.$$

This implies the second inequality in

$$\frac{6d^3 n^{2d} \|f\|}{\mu} \geq \frac{3dn^d \|f\|}{\mu} \geq 1. \tag{2}$$

Also note that (compare Example 2)

$$|f^*| \leq \max \left\{ \sum_{k=0}^{d} \|f\| \left(\sum_{i=1}^{n} |x_i| \right)^k \;\middle|\; x \in S \right\} \leq (d+1) n^d \|f\| \leq 2dn^d \|f\|. \tag{3}$$

Using these observations, we obtain

$$\begin{aligned}
& & k &= \left(\frac{12c_0 d^4 n^{2d} \|f\|}{\mu} \right)^{c_0} \\
&\text{(since } c_0 \geq 2\text{)} & &\geq 2c_0 d^2 \left(\frac{6d^3 n^{2d} \|f\|}{\mu} \right)^{c_0} \\
&\text{(by (2))} & &\geq c_0 d^2 \left(1 + \left(\frac{6d^3 n^{2d} \|f\|}{\mu} \right)^{c_0} \right) \\
& & &= c_0 d^2 \left(1 + \left(2d^2 n^d \frac{3dn^d \|f\|}{\mu} \right)^{c_0} \right) \\
&\text{(by (2))} & &\geq c_0 d^2 \left(1 + \left(d^2 n^d \left(\frac{3dn^d \|f\|}{\mu} + 1 \right) \right)^{c_0} \right) \\
& & &\geq c_0 d^2 \left(1 + \left(d^2 n^d \left(\frac{(1 + 2dn^d) \|f\|}{\mu} + 1 \right) \right)^{c_0} \right) \\
&\text{(by (3))} & &\geq c_0 d^2 \left(1 + \left(d^2 n^d \frac{\|f\| + f^* + \mu}{\mu} \right)^{c_0} \right) \\
& & &\geq c_0 d^2 \left(1 + \left(d^2 n^d \frac{\|h\|}{\mu} \right)^{c_0} \right).
\end{aligned}$$

Theorem 3 applied to h now shows our claim since

$$\mu = h^* := \min\{h(x) \mid x \in S\}. \qquad \square$$

Remark 5 Note that Lasserre works (under a certain extra condition) for efficiency reasons with representations

$$\sigma_0 + \sum_{i=1}^{m} \sigma_i g_i \qquad \text{where} \qquad \sigma_i \in \sum \mathbb{R}[\bar{X}]^2 \tag{4}$$

instead of representations (1), see [Las], [Sr2] and [Mar]. In other words, he does not necessarily allow the mixed products of the g_i to appear. Note however, that we could add redundant inequalities to the description of S corresponding to these mixed products in order to fit into Lasserre's framework. Unfortunately, we don't yet see how to avoid the mixed products in our work. On one hand, for the representations (4) there are powerful analogues to Schmüdgen's theorem due to Putinar, Jacobi and Prestel, see [Put], [JP] and [PD]. On the other hand, the proof of our theorems relies intrinsically on the mixed products as we shall see in the next section.

3 The proof

In this section, we will prove Theorem 3.

Definition 6 For $d \in \mathbb{N}$, we call a polynomial of the type

$$\sum_{|\alpha|=d} a_\alpha \bar{X}^\alpha \in \mathbb{R}[\bar{X}] \qquad (a_\alpha \in \mathbb{R})$$

a *d–form*. In other words, a d–form is either a homogeneous polynomial of degree d or the zero polynomial. If a polynomial is homogeneous, i.e., a d–form for some $d \in \mathbb{N}$, we call it a *form*. We call a form a *Pólya–form* if when written in the above way, $a_\alpha > 0$ for all $\alpha \in \mathbb{N}^n$ with $|\alpha| = d$ (in particular, all terms of degree d appear).

The reason why we introduced the term "Pólya–form" is that Pólya proved already a qualitative version of the next theorem in 1927 [Pól]. He proved that $F \cdot (X_1 + \cdots + X_n)^N$ is a Pólya–form for big enough N without specifying how big N has to be chosen. Loera and Santos gave a quantitative version [LS] which has been further improved to the following version by Powers and Reznick [PR].

Theorem 7 (Powers and Reznick) *Suppose that $F \in \mathbb{R}[\bar{X}]$ is a d–form positive on*

$$\Delta := \{x \in [0, \infty)^n \mid x_1 + \cdots + x_n = 1\}.$$

Then for $N \in \mathbb{N}$ with

$$N > \frac{d(d-1)\|F\|}{2 \min\{F(x) \mid x \in \Delta\}} - d,$$

$F \cdot (X_1 + \cdots + X_n)^N$ *is a Pólya–form.*

Lemma 8 *If* $F, G \in \mathbb{R}[\bar{X}]$ *are forms, then* $\|FG\| \leq \|F\|\|G\|$.

Proof. Let us write $F = \sum_{|\alpha|=d} a_\alpha \frac{d!}{\alpha_1! \cdots \alpha_n!} \bar{X}^\alpha$ and $G = \sum_{|\beta|=e} b_\beta \frac{e!}{\beta_1! \cdots \beta_n!} \bar{X}^\beta$ where $a_\alpha, b_\beta \in \mathbb{R}$. Computing the product, we get

$$\begin{aligned} FG &= \sum_{|\gamma|=d+e} \left(\sum_{\substack{\alpha+\beta=\gamma \\ |\alpha|=d}} a_\alpha b_\beta \frac{d!e!}{\alpha_1! \cdots \alpha_n! \beta_1! \cdots \beta_n!} \right) \bar{X}^\gamma \\ &= \sum_{|\gamma|=d+e} \underbrace{\left(\sum_{\substack{\alpha+\beta=\gamma \\ |\alpha|=d}} a_\alpha b_\beta \frac{d!e!\gamma_1! \cdots \gamma_n!}{(d+e)!\alpha_1!\beta_1! \cdots \alpha_n!\beta_n!} \right)}_{\leq \|F\|\|G\|s/\binom{d+e}{d} = \|F\|\|G\|} \frac{(d+e)!}{\gamma_1! \cdots \gamma_n!} \bar{X}^\gamma \end{aligned}$$

where $s := \sum_{|\alpha|=d} \binom{\gamma_1}{\alpha_1} \cdots \binom{\gamma_n}{\alpha_n}$ counts the number of possibilities to choose d elements from a union of n pairwise disjoint sets having the cardinalities $\gamma_1, \ldots, \gamma_n$. $\square$

Lemma 9 *Suppose* $g_1, \ldots, g_m \in \mathbb{R}[\bar{X}]$, $\varepsilon > 0$ *and*

$$S := \{x \in [-1+\varepsilon, 1-\varepsilon]^n \mid g_1(x) \geq 0, \ldots, g_m(x) \geq 0, \sum_{i=1}^m g_i(x) \leq 2n\varepsilon\} \subseteq \mathbb{R}^n$$

is not empty. Setting

$$\begin{aligned} p_1 := 1 - \varepsilon + X_1, \ldots, p_n := 1 - \varepsilon + X_n, \\ p_{n+1} := 1 - \varepsilon - X_1, \ldots, p_{2n} := 1 - \varepsilon - X_n, \\ p_{2n+1} := g_1, \ldots, p_{2n+m} := g_m, p_{2n+m+1} := 2n\varepsilon - (g_1 + \cdots + g_m), \end{aligned} \quad (5)$$

we can write alternatively $S = \{x \in \mathbb{R}^n \mid p_1(x) \geq 0, \ldots, p_{2n+m+1}(x) \geq 0\}$. *Then there is some* $c \in \mathbb{N}$ *such that every* $f \in \mathbb{R}[\bar{X}]$ *of degree* d *with* $f^* := \min\{f(x) \mid x \in S\} > 0$ *and* $\|f\| = 1$ *can be written as*

$$\sum_{\alpha_1 + \cdots + \alpha_{2n+m+1} = M} a_\alpha p_1^{\alpha_1} \cdots p_{2n+m+1}^{\alpha_{2n+m+1}} \quad (6)$$

where $0 < a_\alpha \in \mathbb{R}$ *for all* $\alpha \in \mathbb{N}^{2n+m+1}$ *with* $|\alpha| = M$ *and*

$$M \leq cd^2 \left(1 + \left(\frac{d^2 n^d}{f^*} \right)^c \right).$$

Before tackling the proof of the lemma, we shall show how the main theorem follows from it.

Proof of Theorem 3. Because S is a compact subset of $(-1,1)^n$, we can choose $\varepsilon > 0$ such that $S \subseteq [-1+2\varepsilon, 1-2\varepsilon]^n$. Define $p_1, \ldots, p_{2n+m+1}$ like in (5). After scaling all g_i with a small positive factor, we may assume $p_{2n+m+1} > 0$ on S. Then S could be equivalently defined as in Lemma 9. Moreover, each p_i has a representation (1). This is trivial for the g_i, and it follows from Schmüdgen's Positivstellensatz (without complexity information) for the other polynomials. Fix such a representation for each p_i. Choose $c_0 \in \mathbb{N}$ such that none of the $(2n+m+1)2^m$ summands in these $2n+m+1$ fixed representations (1) has a degree exceeding c_0. Denote by c_1 the constant c which exists according to Lemma 9. Choose $c \in \mathbb{N}$ such that

$$c_0 c_1 (1 + a^{c_1}) \leq c(1 + a^c) \qquad \text{for all } a \in [0, \infty).$$

Suppose $f \in \mathbb{R}[\bar{X}]$ is of degree $d \geq 1$ with $f > 0$ on S. Without loss of generality we can assume that $\|f\| = 1$. In the representation (6) of f, we can replace each p_i by its representation (1) which we have fixed before. Multiplying out and interpreting even powers as squares, we see in this way that f equals an expression (1) where no summand has degree more than

$$c_0 N \leq c_0 c_1 d^2 \left(1 + \left(\frac{d^2 n^d}{f^*}\right)^{c_1}\right) \leq c d^2 \left(1 + \left(\frac{d^2 n^d}{f^*}\right)^{c}\right). \qquad \square$$

We briefly outline the proof of Lemma 9 before giving it. Introduce new variables $(Y_1, \ldots, Y_{2n+m+1})$ abbreviated by $\bar{Y}$ and consider the surjective $\mathbb{R}$–algebra homomorphism $\varphi : \mathbb{R}[\bar{Y}] \to \mathbb{R}[\bar{X}] : Y_i \mapsto p_i$. Given $f \in \mathbb{R}[\bar{X}]$ with $f > 0$ on S, we have to find a Pólya–form of degree M not too high which is mapped to f by φ. To do this, we will apply Theorem 7. Complexity considerations aside, note that the following version of Pólya's theorem is true due to the homogeneity of F: Suppose that $F \in \mathbb{R}[\bar{Y}]$ is a form positive on

$$\Delta := \{x \in [0,\infty)^{2n+m+1} \mid y_1 + \cdots + y_{2n+m+1} = 2n\},$$

then $F \cdot ((Y_1 + \cdots + Y_{2n+m+1})/2n)^N$ is a Pólya–form for big N. Since $p_1 + \cdots + p_{2n+m+1} = 2n$, we have $\varphi(F \cdot ((Y_1 + \cdots + Y_{2n+m+1})/2n)^N) = \varphi(F)$. Therefore we have to find a form in $\mathbb{R}[\bar{Y}]$ which is mapped to f by φ and positive on Δ. (Of course, the exponent N should not get too high, so we have to control the norm and the degree of this form as well as its minimum on Δ.) To start with, it is easy to find a form $P \in \mathbb{R}[\bar{Y}]$ such that $\varphi(P) = f$. Just take any preimage of φ (which is suitable for keeping track of complexity) and multiply its homogeneous parts with suitable powers of $(Y_1 + \cdots + Y_{2n+m+1})/2n$ to make their degrees equal. For such a form P, the positivity of f on S translates into positivity of P on a certain subset Z of Δ which is defined by the points of Δ whose coordinates satisfy the algebraic relations among the p_i (i.e., Z is the variety belonging to the kernel of φ intersected with Δ), see Claim 1 in the proof and (14). On one hand, the algebraic relations among the p_i are responsible for the undesired fact that Z is a proper subset of S and therefore positivity of P cannot be guaranteed on the whole of Δ. On the other hand, the same algebraic relations allow to find a homogeneous form R in the kernel of φ of the same degree than P which is zero on Z and positive on $\Delta \setminus Z$. For high $\lambda \in \mathbb{R}$, the form $P + \lambda R$ will fulfill our needs, i.e., it is positive on Δ and it is mapped to f. Actually, λ should not be too high either since we don't want the norm of $P + \lambda R$ get too big, confer (23). Up to a power of $(Y_1 + \cdots + Y_{2n+m+1})/2n$ which ensures that P and R have the same degree, R will equal a form R_0 depending only on the description of S, see Claim 2. To give an estimate for the minimum of $P + \lambda R$ on Δ, we will have to use that P cannot decrease too fast (confer Claim 3) and R_0 cannot increase too slowly when moving away from Z inside Δ (Łojasiewicz inequality (8)).

Proof of Lemma 9. In this proof, we abbreviate $(Y_1, \dots, Y_{2n+m+1})$ by $\bar{Y}$. Consider the surjective $\mathbb{R}$–algebra homomorphism $\varphi : \mathbb{R}[\bar{Y}] \to \mathbb{R}[\bar{X}] : Y_i \mapsto p_i$. Its kernel $\ker \varphi$ contains $Y_1 + \cdots + Y_{2n+m+1} - 2n$. By Hilbert's basis theorem, we can choose polynomials $r_1, \dots, r_t$ such that

$$\ker \varphi = (Y_1 + \cdots + Y_{2n+m+1} - 2n, r_1, \dots, r_t). \tag{7}$$

Now set

$$\begin{aligned} \Delta &:= \{y \in [0, \infty)^{2n+m+1} \mid y_1 + \cdots + y_{2n+m+1} = 2n\} \qquad \text{and} \\ Z &:= \{y \in \Delta \mid r_1(y) = \cdots = r_t(y) = 0\} \subseteq \Delta. \end{aligned}$$

Claim 1. The linear map

$$l : \mathbb{R}^{2n+m+1} \to \mathbb{R}^n : (y_1, \dots, y_{2n+m+1}) \mapsto \left(\frac{1}{2}y_1 - \frac{1}{2}y_{n+1}, \dots, \frac{1}{2}y_n - \frac{1}{2}y_{2n}\right)$$

induces a bijection $l|_Z : Z \to S$.

We can view S as the set of $\mathbb{R}$–algebra homomorphisms $\mathbb{R}[\bar{X}] \to \mathbb{R}$ mapping each $p_i = \varphi(Y_i)$ into $[0, \infty)$. Similarly, Z can be seen as the set of $\mathbb{R}$–algebra homomorphisms $\mathbb{R}[\bar{Y}]/\ker \varphi \to \mathbb{R}$ mapping each $Y_i + \ker \varphi$ into $[0, \infty)$. Looked at both sets in this way, Z and S clearly correspond to each other under the $\mathbb{R}$–algebra isomorphism $\mathbb{R}[\bar{Y}]/\ker \varphi \to \mathbb{R}[\bar{X}]$ induced by φ. An element of Z corresponds to its composition with the inverse of this isomorphism. This inverse isomorphism maps X_i to $\left(\frac{1}{2}Y_i - \frac{1}{2}Y_{n+i}\right) + \ker \varphi$. Thinking of Z and S again as points, we therefore easily see that the map $l|_Z$ describes this correspondence.

Claim 2. We can find $1 \leq d_0 \in \mathbb{N}$ and a d_0–form $R_0 \in \ker \varphi$ such that $R_0 \geq 0$ on Δ and $Z = \{y \in \Delta \mid R_0(y) = 0\}$.

Indeed, if $\sum_{i=1}^{t} r_i^2$ is homogeneous, it does the job. (Note that it cannot have degree 0 since this would imply $Z = \emptyset$ contradicting $S \neq \emptyset$.) In general, multiply the homogeneous parts of lower degree in $\sum_{i=1}^{t} r_i^2$ by an appropriate power of $\frac{1}{2n}(Y_1 + \cdots + Y_{2n+m+1})$. This makes the polynomial homogeneous and does neither affect its membership in $\ker \varphi$ nor change its values on Δ. This proves Claim 2.

By a Łojasiewicz inequality (Corollary 2.6.7 in [BCR]), we can choose $1 \leq c_0, c_1 \in \mathbb{N}$ such that

$$\operatorname{dist}(y, Z)^{c_0} \leq c_1 R_0(y) \qquad \text{for all } y \in \Delta \tag{8}$$

where $\operatorname{dist}(y, Z)$ denotes the distance of y to Z (note that $Z \neq \emptyset$ since $S \neq \emptyset$). Set

$$c_2 := 2^{c_0+1} c_1 \sqrt{2n}, \tag{9}$$
$$c_3 := c_2 (2n)^{d_0} \|R_0\|, \tag{10}$$
$$c_4 := 2n^{d_0} \tag{11}$$

and choose c big enough to guarantee that

$$d_0^2(1 + c_4 a + c_3 a^{c_0+1}) \leq c(1 + a^c) \qquad \text{for all } a \in [0, \infty). \tag{12}$$

Now suppose we are given $f \in \mathbb{R}[\bar{X}]$ of degree $d \geq 1$ with $f > 0$ on S and $\|f\| = 1$, say $f = F_d + \cdots + F_0$ where $F_k \in \mathbb{R}[\bar{X}]$ is a k–form for each $k \in \{0, \ldots, d\}$. Then we set $d_1 := \max\{d, d_0\}$ and

$$P := \sum_{k=0}^{d} \underbrace{F_k \left(\frac{1}{2} Y_1 - \frac{1}{2} Y_{n+1}, \ldots, \frac{1}{2} Y_n - \frac{1}{2} Y_{2n} \right)}_{=: P_k} \left(\frac{Y_1 + \cdots + Y_{2n+m+1}}{2n} \right)^{d_1 - k}.$$

Observe that P is a d_1–form,

$$\varphi(P) = f \qquad \text{and} \tag{13}$$
$$P(y) = f(l(y)) \text{ for all } y \in \Delta. \tag{14}$$

Claim 1 implies together with (14)

$$\min\{P(y) \mid y \in Z\} = \min\{f(x) \mid x \in S\} = f^*. \tag{15}$$

It is easy to see that $\|P_k\| = \frac{1}{2^k}\|F_k\| \leq \frac{1}{2^k}\|f\| = \frac{1}{2^k}$. Using Lemma 8, this has

$$\|P\| \leq \sum_{k=0}^{d} \frac{1}{(2^k)(2n)^{d_1-k}} \leq \frac{d+1}{2^{d_1}} \tag{16}$$

as a consequence. Next define another d_1–form R by

$$R := R_0 \cdot \left(\frac{Y_1 + \cdots + Y_{2n+m+1}}{2n}\right)^{d_1-d_0}.$$

Again by Lemma 8, we get

$$\|R\| \leq \frac{1}{(2n)^{d_1-d_0}}\|R_0\|. \tag{17}$$

Also note that

$$R = R_0 \text{ on } \Delta. \tag{18}$$

Claim 3. $|P(y) - P(y')| \leq \|y - y'\|\sqrt{n}d^2n^{d-1}$ for all $y, y' \in \Delta$.

To show this, it suffices to prove

$$|f(x) - f(x')| \leq \|x - x'\|\sqrt{n}d^2n^{d-1} \qquad \text{for all } x, x' \in l(\Delta). \tag{19}$$

Indeed, (19) together with (14) and the estimate $\|l(y) - l(y')\| = \|l(y - y')\| \leq \|y - y'\|$ for all $y, y' \in \Delta$ (even in $\mathbb{R}^{2n+m+1}$) implies the claim. To prove (19), we determine the shape of $l(\Delta)$. Because Δ is the convex hull of the unit vectors in $\mathbb{R}^{2n+m+1}$ multiplied by a factor of $2n$ and l is linear, $l(\Delta)$ is the convex hull of the $2n$ vectors

$$\pm(n, 0, \dots, 0), \dots, \pm(0, \dots, 0, n) \in \mathbb{R}^n.$$

In particular, it follows that

$$|x_1| + \cdots + |x_n| \leq n \qquad \text{for all } x \in l(\Delta).$$

Since $l(\Delta)$ is convex, we can use the mean value theorem to show (19). If we denote by Df the derivative of f, it is enough to show

$$|Df(x)(e)| \leq \sqrt{n}d^2n^{d-1} \tag{20}$$

for all $x \in \Delta$ and $e \in \mathbb{R}^n$ with $\|e\| = 1$. Having in mind that $\|f\| = 1$, a small computation (compare Example 2) shows that

$$\begin{aligned}\left|\frac{\partial f}{\partial X_i}(x)\right| &\leq \frac{\partial \sum_{k=0}^{d}(X_1 + \cdots + X_n)^k}{\partial X_i}(|x_1|, \dots, |x_n|) \\ &= \sum_{k=1}^{d} k(|x_1| + \cdots + |x_n|)^{k-1} \leq \sum_{k=1}^{d} kn^{k-1} \leq d^2n^{d-1},\end{aligned}$$

from which we conclude for all $x \in \Delta$ and $e \in \mathbb{R}^n$ with $\|e\| = 1$,

$$|Df(x)(e)| = \left|\sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(x)e_i\right| \leq \sum_{i=1}^{n}\left|\frac{\partial f}{\partial X_i}(x)\right| \cdot |e_i| \leq d^2n^{d-1}\sum_{i=1}^{n}|e_i|.$$

This entails (20) and hence Claim 3 because for a vector e on the unit sphere in $\mathbb{R}^n$, $\sum_{i=1}^n |e_i|$ can reach at most $\sqrt{n}$.

For $y, y' \in \Delta$ with $P(y) \le f^*/2$ and $P(y') \ge f^*$, we know by Claim 3 that

$$\|y - y'\| \ge \frac{f^*}{2\sqrt{n}d^2n^{d-1}} \ge \frac{f^*}{2d^2n^d}.$$

In particular, by (15) we get

$$\operatorname{dist}(y, Z) \ge \frac{f^*}{2d^2n^d}$$

and then by (8) and (18)

$$\left(\frac{f^*}{2d^2n^d}\right)^{c_0} \le c_1 R(y) \tag{21}$$

for all $y \in \Delta$ with $P(y) \le f^*/2$. If we choose in Claim 3 for y' a minimizer of P on Z, we obtain

$$|P(y) - f^*| \le \operatorname{diam}(\Delta)\sqrt{n}d^2n^{d-1} = 2\sqrt{2n}d^2n^d$$

for all $y \in \Delta$, noting that the diameter $\operatorname{diam}(\Delta)$ of Δ is $2\sqrt{2}n$. In particular, we observe

$$P \ge f^* - 2\sqrt{2n}d^2n^d \qquad \text{on } \Delta. \tag{22}$$

By setting

$$\lambda := c_2 d^2 n^d \left(\frac{d^2n^d}{f^*}\right)^{c_0}, \tag{23}$$

we can ensure that

$$P + \lambda R \ge \frac{f^*}{2} \qquad \text{on } \Delta. \tag{24}$$

In fact, (24) is clear on the part of Δ where $P \ge f^*/2$ since $\lambda \ge 0$ and $R \ge 0$ on Δ, see (18) and Claim 2. To verify (24) on the rest of Δ, we use (21) and (22). If $y \in \Delta$ and $P(y) \le f^*/2$, then (23) and (21) imply that

$$\lambda R(y) \ge \frac{c_2}{c_1 2^{c_0}} d^2 n^d$$

which actually leads to

$$P(y) + \lambda R(y) \ge f^* - 2\sqrt{2n}d^2n^d + \frac{c_2}{c_1 2^{c_0}} d^2 n^d = f^* \ge \frac{f^*}{2}$$

by (22) and (9). Because we are going to apply Theorem 7 to the d_1–form $P + \lambda R$, we are shifting our attention from Δ to

$$\Delta_1 := \{y \in [0, \infty)^{2n+m+1} \mid y_1 + \cdots + y_{2n+m+1} = 1\}.$$

Then (24) translates into

$$P + \lambda R \geq \frac{f^*}{2(2n)^{d_1}} \qquad \text{on } \Delta_1.$$

Theorem 7 now guarantees that the $(d_1 + N)$–form

$$Q := (P + \lambda R) \cdot \left(\frac{Y_1 + \cdots + Y_{2n+m+1}}{2n} \right)^N$$

is a Pólya–form for all

$$N > \frac{d_1(d_1 - 1)\|P + \lambda R\|}{2\frac{f^*}{2(2n)^{d_1}}} - d_1 = d_1(d_1 - 1)(2n)^{d_1} \frac{\|P + \lambda R\|}{f^*} - d_1.$$

If we choose the lowest such N, we know that

$$\begin{aligned}
M := \deg Q &\leq d_1(d_1 - 1)(2n)^{d_1} \frac{\|P + \lambda R\|}{f^*} + 1 \\
&\leq d_1^2 (2n)^{d_1} \frac{\|P\| + \lambda \|R\|}{f^*} + 1 \\
\text{(by (16) and (17))} \quad &\leq d_1^2 \left(\frac{(2n)^{d_1}(d+1)}{2^{d_1} f^*} + \frac{\lambda}{f^*}(2n)^{d_0}\|R_0\| \right) + 1 \\
\text{(by (10) and (23))} \quad &\leq d_1^2 \left(\frac{n^{d_1}(d+1)}{f^*} + c_3 \left(\frac{d^2 n^d}{f^*} \right)^{c_0+1} \right) + 1 \\
\text{(since } d_1 \geq d \geq 1) \quad &\leq d_1^2 \left(1 + 2\frac{d^2 n^{d_1}}{f^*} + c_3 \left(\frac{d^2 n^d}{f^*} \right)^{c_0+1} \right) \\
\text{(since } d_1 \leq d d_0) \quad &\leq d^2 d_0^2 \left(1 + c_4 \frac{d^2 n^d}{f^*} + c_3 \left(\frac{d^2 n^d}{f^*} \right)^{c_0+1} \right) \\
\text{(by (12))} \quad &\leq c d^2 \left(1 + \left(\frac{d^2 n^d}{f^*} \right)^c \right).
\end{aligned}$$

This ends the proof of Lemma 9 since $\varphi(Q) = \varphi(P + \lambda R) = \varphi(P) + \lambda\varphi(R) = \varphi(P) = f$ by (13) and $R_0 \in \ker \varphi$. $\square$

Remark 10 The proof of the above lemma tells us how we could try to determine an appropriate c from given $g_1, \ldots, g_m \in \mathbb{R}[\bar{X}]$ and $\varepsilon > 0$. We have to compute $r_1, \ldots, r_t$ fulfilling (7). This can be done using Gröbner bases [Sr1, Section 4]. From these polynomials, we get a d_0–form R_0 like in Claim 2. Finally, we have to find c_0 and c_1 satisfying the Łojasiewicz inequality (8). Here Solernó's effective versions of this inequality [Sol] might help.

To determine a concrete c making Theorem 3 work for a given description of S, one essentially still needs to compute the c_0 from the proof of Theorem

3. Here we don't know of any other solution than trying to actually compute representations (1) for the polynomials p_i from (5). Of course, this is trivial for $g_1, \ldots, g_m$. To compute representations of the $1 - \varepsilon \pm X_i$, one could try to use the symbolical method from [Sr1] or the numerical method based on semidefinite programming, see [Las] and compare Section 2. Finally, we get the representation of $2n\varepsilon - (g_1 + \cdots + g_m)$ for free if we scale the g_i a bit more carefully than above. Indeed, from the representations of the $1 \pm X_i$ already computed, we can compute a representation (1) of $s - (g_1 + \cdots + g_m)$ for some $s > 0$, see Remark 5.3 in [Sr1]. We can assume $s = 2n\varepsilon$ by multiplying the g_i with a positive factor.

References

[BCR] J. Bochnak, M. Coste, M.-F. Roy: Real algebraic geometry, Ergebnisse der Mathematik und ihrer Grenzgebiete **36**, Berlin: Springer (1998)

[BW] R. Berr, T. Wörmann: Positive polynomials on compact sets, Manuscr. Math. **104**, 135–143 (2001)

[JP] T. Jacobi, A. Prestel: Distinguished representations of strictly positive polynomials, J. Reine Angew. Math. **532**, 223–235 (2001)

[Las] J. B. Lasserre: Global optimization with polynomials and the problem of moments, SIAM J. Optim. **11**, No. 3, 796–817 (2001)

[LS] J. A. de Loera, F. Santos: An effective version of Pólya's theorem on positive definite forms, J. Pure Appl. Algebra **108**, No. 3, 231–240 (1996); erratum ibid. **155**, 309–310 (2001)

[Mar] M. Marshall: Optimization of polynomial functions, Canad. Math. Bull. **46**, 575–587 (2003)

[Mau] E. Mauch: Complexity estimates for representations of Schmüdgen type, J. Complexity **18**, No. 1, 346–355 (2002)

[PD] A. Prestel, C. Delzell: Positive polynomials, Springer Monographs in Mathematics, Berlin: Springer (2001)

[Pól] G. Pólya: Über positive Darstellung von Polynomen, Vierteljahresschrift der Naturforschenden Gesellschaft in Zürich **73** (1928), 141–145; reprinted in: Collected Papers, Volume 2, 309–313, Cambridge: MIT Press (1974)

[PR] V. Powers, B. Reznick: A new bound for Pólya's Theorem with applications to polynomials positive on polyhedra, J. Pure Appl. Algebra **164**, No. 1–2, 221–229 (2001)

[PS] P. Parrilo, B. Sturmfels: Minimizing polynomial functions, DIMACS Series in Discrete Mathematics and Theoretical Computer Science **60**, 83–100 (2003)

[Put] M. Putinar: Positive polynomials on compact semi–algebraic sets, Indiana Univ. Math. J. **42**, No. 3, 969–984 (1993)

[Rez] B. Reznick: Uniform denominators in Hilbert's seventeenth problem, Math. Z. **220**, No. 1, 75–97 (1995)

[Sd] J. Schmid: On the degree complexity of Hilbert's 17th problem and the Real Nullstellensatz, Habilitationsschrift, Universität Dortmund (1998)

[Sn] K. Schmüdgen: The K–moment problem for compact semi–algebraic sets, Math. Ann. **289**, No. 2, 203–206 (1991)

[Sol] P. Solernó: Effective Łojasiewicz inequalities in semialgebraic geometry, Appl. Algebra Eng. Commun. Comput. **2**, No.1, 1–14 (1991)

[Sr1] M. Schweighofer: An algorithmic approach to Schmüdgen's Positivstellensatz, J. Pure Appl. Algebra **166**, No. 3, 307–319 (2002)

[Sr2] M. Schweighofer: Optimization of polynomials on compact semialgebraic sets, submitted
`http://www.mathe.uni-konstanz.de/homepages/schweigh/`

[Ste] G. Stengle: Complexity estimates for the Schmüdgen Positivstellensatz, J. Complexity **12**, No. 2, 167–174 (1996)

[Stu] B. Sturmfels: Solving systems of polynomial equations, CBMS regional conference series in mathematics **97**, American Mathematical Society (2002)