An algorithmic approach to Schmüdgen's Positivstellensatz

Markus Schweighofer

Universität Konstanz, Fachbereich Mathematik und Statistik, 78457 Konstanz, Germany

Abstract

We present a new proof of Schmüdgen's Positivstellensatz concerning the representation of polynomials $f \in \mathbb{R}[X_1, ..., X_d]$ that are strictly positive on a *compact* basic closed semialgebraic subset S of $\mathbb{R}^d$. Like the two other existing proofs due to Schmüdgen and Wörmann, our proof also applies the classical Positivstellensatz to non–constructively produce an algebraic evidence for the compactness of S. But in sharp contrast to Schmüdgen and Wörmann we explicitly construct the desired representation of f from this evidence. Thereby we make essential use of a theorem of Pólya concerning the representation of homogeneous polynomials that are strictly positive on an orthant of $\mathbb{R}^d$ (minus the origin).

Key words: effective Positivstellensatz, strictly positive polynomials

1 Introduction

By refining the non–constructive methods which in 1923 enabled Artin to solve Hilbert's 17th problem, Krivine obtained in 1964 the following result (see [Kri]) [†]. (Throughout the paper $\bar{X}$ abbreviates $X_1, \ldots, X_d$.)

Theorem 1.1 (Classical Positivstellensatz) *Let $R \mid K$ be an extension of ordered fields such that R is real closed. Let $p_1, \ldots, p_n \in K[\bar{X}]$ define the set*

$$S := \{x \in R^d \mid p_1(x) \geq 0, \ldots, p_n(x) \geq 0\}.$$

[†] Just apply Tarski's transfer principle to Krivine's Théorème 7 in exactly the same manner as Krivine does to his Théorème 8. Then use a little trick (see e.g. [KS], III, §9, Satz 2) to get a denominator having the shape $1 + \cdots$. This theorem of Krivine was later rediscovered independently by Stengle [Ste] and Prestel [Pre].

Then for every $f \in K[\bar{X}]$ we have $f > 0$ on S if and only if f can be written in the form

$$\frac{1 + \sum_{e \in \{0,1\}^n} \left(\sum_i a_{ei} f_{ei}^2\right) p_1^{e_1} \cdots p_n^{e_n}}{1 + \sum_{e \in \{0,1\}^n} \left(\sum_i b_{ei} g_{ei}^2\right) p_1^{e_1} \cdots p_n^{e_n}} \tag{1.1}$$

where $0 \leq a_{ei}, b_{ei} \in K$ and $f_{ei}, g_{ei} \in K[\bar{X}]$.

In 1990 Schmüdgen (see [Sch]) showed by functional analytic methods that (1.1) can be replaced by a similar representation without denominator in the case that $K = R = \mathbb{R}$ and S is bounded (and thus compact). In 1998 Wörmann, in his thesis [Wör], gave an *algebraic* proof of a slight generalization of this result (where K may be a proper subfield of $\mathbb{R}$):

Theorem 1.2 (Schmüdgen's Positivstellensatz) *Let K be a subfield of $\mathbb{R}$. Let $p_1, \ldots, p_n \in K[\bar{X}]$ define the* compact *set*

$$S := \{x \in \mathbb{R}^d \mid p_1(x) \geq 0, \ldots, p_n(x) \geq 0\}.$$

Then for every $f \in K[\bar{X}]$ we have $f > 0$ on S if and only if f can be written in the form

$$a + \sum_{e \in \{0,1\}^n} \left(\sum_i a_{ei} f_{ei}^2\right) p_1^{e_1} \cdots p_n^{e_n} \tag{1.2}$$

where $0 < a \in K, 0 \leq a_{ei} \in K$ and $f_{ei} \in K[\bar{X}]$.

We introduce the notation $\Sigma := X_1^2 + \cdots + X_d^2$. The proofs of both Wörmann and Schmüdgen, apply the classical Positivstellensatz (in the case $R = \mathbb{R}$) to get a representation (1.1) of the polynomial $s - \Sigma$ for some $0 \leq s \in K$. Note that this polynomial is strictly positive on S if and only if S is contained in the open ball of radius $\sqrt{s}$ centered at the origin. As S is assumed to be compact the latter is the case for sufficiently large s.

Using this evidence for S being contained in a ball, Wörmann in the second step of his proof shows that for every $f \in K[\bar{X}]$ there exists $0 \leq t \in K$ such that the polynomials $t + f$ and $t - f$ have a representation

$$\sum_{e \in \{0,1\}^n} \left(\sum_i a_{ei} f_{ei}^2\right) p_1^{e_1} \cdots p_n^{e_n}, \tag{1.3}$$

where $0 \leq a_{ei} \in K$ and $f_{ei} \in K[\bar{X}]$. Note that this is a weakening of Schmüdgen's theorem because every polynomial is bounded on the compact set S. By slightly modifying this part of the proof we obtain an effective construction. We will explain this in Section 2.

The third and last step in Wörmann's proof is a simple application of a representation theorem of Krivine for rings with an archimedean subsemiring. This theorem goes under the name of Kadison–Dubois theorem (see Remark 5.2). It's a broad generalization of the well–known theorem that every archimedean ordered field can be embedded into $\mathbb{R}$. Instead, we apply a theorem of Pólya characterizing those homogeneous polynomials that are strictly positive on an orthant of $\mathbb{R}^d$ (minus the origin). Together with several preparatory steps, this is carried out in Section 3.

In Section 4 we show that our proof actually provides an algorithm doing the following. Given $p_1, \dots, p_n, f \in K[\bar{X}]$ such that $f > 0$ on S and a representation (1.1) of $s - \Sigma$ for some $0 \leq s \in K$, the algorithm computes a representation (1.2) of f. We also discuss some properties of this algorithm.

Finally, Section 5 is concerned with the situation where sufficiently many of the polynomials p_i are *linear*. In this case the algorithm does *not* require the input of a representation of $s - \Sigma$ and even produces a representation of f *not* involving sums of squares.

This article elaborates the author's Diplomarbeit at the Universität Passau/Germany under the supervision of Volker Weispfenning. The author acknowledges his valuable suggestions. The author wants to thank Matthias Aschenbrenner, Matthias Franz, Vicki Powers, Alexander Prestel, Bruce Reznick, Joachim Schmid and an anonymous referee for helping to improve earlier versions of this paper.

2 Revising Wörmann's second step

As in the first step of Wörmann's proof, i.e. the application of the classical Positivstellensatz 1.1, the assumption $K \subseteq \mathbb{R}$ is not needed either for the second step. In fact we can work over any ordered field K:

Lemma 2.1 *Let K be an ordered field and $0 \leq s \in K$. Then for every polynomial $g \in K[\bar{X}]$ there exists $0 \leq t \in K$ such that $t + g$ and $t - g$ can be written in the form*

$$\sum_i a_i f_i^2 + \left(\sum_i b_i g_i^2 \right) (s - \Sigma) \tag{2.1}$$

where $0 \leq a_i, b_i \in K$ and $f_i, g_i \in K[\bar{X}]$.

PROOF. The set of all g for which there exists such a t obviously contains K and is closed under addition. Because of the two equalities

$$tu \pm gh = \frac{1}{2}((t \pm g)(u+h) + (t \mp g)(u-h))$$

this set is also closed under multiplication. Finally the two equalities

$$\frac{s+1}{2} \pm X_i = \frac{1}{2}\left((X_i \pm 1)^2 + (s - \Sigma) + \sum_{j \neq i} X_j^2\right)$$

show that this set contains every X_i. Hence it is all of $K[\bar{X}]$. $\square$

It's quite obvious that Wörmann could have made his proof of Satz 4.10 in [Wör] constructive by avoiding to apply his Korollar 3.4:

Theorem 2.2 (Wörmann) *Let K be an ordered field and $p_1, \ldots, p_n \in K[\bar{X}]$. Given $0 \leq s \in K$ and a representation* (1.1) *of $s - \Sigma$, for every $f \in K[\bar{X}]$ one may find $0 \leq t \in K$ and representations* (1.3) *of the two polynomials $t \pm f$.*

PROOF. By Lemma 2.1 applied to f it is enough to show that there is $0 \leq s' \in K$ such that $s' - \Sigma$ has a representation (1.3).

By assumption there exist polynomials $g, h \in K[\bar{X}]$ such that

$$s - \Sigma = \frac{1+g}{1+h}, \tag{2.2}$$

and g and h can be written in the form (1.3). This implies that $(1+h)(s-\Sigma)$ has a representation (1.3) (provided by $1+g$). Since $h\Sigma$ has also a representation (1.3), we obtain such a representation of the sum

$$(1+h)(s-\Sigma) + h\Sigma = s - \Sigma + sh. \tag{2.3}$$

If $s = 0$ we are done by setting $s' = 0$. So now assume $s > 0$. Lemma 2.1 gives us a representation (2.1) of $t - sh$ for some $0 \leq t \in K$. We would be done if this were a representation (1.3) instead of (2.1). However we can make one out of it by multiplying with $1+h$: We have representations (1.3) of both $1+h$ and (by looking at equation (2.2)) $(1+h)(s-\Sigma)$. Thus we have a representation (1.3) of

$$(1+h)(t - sh) = t - sh + th - sh^2. \tag{2.4}$$

Finally adding the representations (1.3) of (2.3), (2.4) and

$$s\left(\frac{t}{2s} - h\right)^2 = s\left(\frac{t^2}{4s^2} - \frac{th}{s} + h^2\right) = \frac{t^2}{4s} - th + sh^2$$

yields a representation (1.3) of

$$\left(s + t + \frac{t^2}{4s}\right) - \Sigma,$$

and we are done by setting $s' = s + t + \frac{t^2}{4s}$. $\square$

3 Applying a theorem of Pólya

Let the conditions of Schmüdgen's Theorem 1.2 be satisfied. To prove the non–trivial direction let $f \in K[\bar{X}]$ be strictly positive on S.

First we observe that we may always enlarge the set $\{p_1, \ldots, p_n\}$ of polynomials defining S by finitely many polynomials $p_{n+1}, \ldots, p_m$ having a representation (1.3): This does not alter the set S and once we will have obtained a representation (1.2) of f with m instead of n we can therein replace $p_{n+1}, \ldots, p_m$ by their representations (1.3) to get a representation (1.2) of f.

Thus by Theorem 2.2 for every $p \in K[\bar{X}]$ and for sufficiently large $0 \leq s \in K$ we can adjoin $s + p$ to $p_1, \ldots, p_n$. By this means we can reduce to the case where

$$K[\bar{X}] = K[p_1, \ldots, p_n], \tag{3.1}$$

since otherwise we might adjoin $s_1 + X_1, \ldots, s_d + X_d$ to $p_1, \ldots, p_n$ for suitable $0 \leq s_1, \ldots, s_d \in K$. Moreover we may assume that $p_1 + \cdots + p_n = s$ for some $0 < s \in K$ (otherwise we adjoin the polynomial $s - (p_1 + \cdots + p_n)$ to $p_1, \ldots, p_n$ for suitable $0 < s \in K$). After scaling the p_i by a positive factor we may also assume $s = 1$ and thus attain

$$p_1 + \cdots + p_n = 1. \tag{3.2}$$

The only purpose of the preceding section was to establish (3.1) and (3.2). Now that these conditions hold not only do we produce a representation (1.2) of f, but we will even find a representation

$$a + \sum_{e \in \mathbb{N}^n} a_e p_1^{e_1} \cdots p_n^{e_n} \tag{3.3}$$

where $0 < a \in K, 0 \leq a_e \in K$ and almost all a_e are zero (see also Theorem 5.1).

More formally speaking we are looking for a polynomial $h \in K[\bar{Y}]$ ($\bar{Y}$ abbreviates $Y_1, \dots, Y_n$) having non–negative coefficients and a positive constant coefficient such that it is mapped to f by the K–algebra homomorphism

$$\varphi : K[\bar{Y}] \to K[\bar{X}] : Y_1 \mapsto p_1, \dots, Y_n \mapsto p_n.$$

By (3.1) φ is surjective and by (3.2) its kernel $I := \ker \varphi$ contains the polynomial $Y_1 + \cdots + Y_n - 1$. By Hilbert's Basis Theorem there are $r_1, \dots, r_t \in K[\bar{Y}]$ such that

$$I = (Y_1 + \cdots + Y_n - 1, r_1, \dots, r_t). \tag{3.4}$$

We now proceed as follows: We start with any $g \in K[\bar{Y}]$ such that $\varphi(g) = f$. Such g exists as φ is surjective. In Subsection 3.1 we will rewrite g by means of $r_1, \dots, r_t$ to make it satisfy a geometric positivity condition. Using the polynomial $Y_1 + \cdots + Y_n - 1$ we homogenize the obtained polynomial. Then we are in the position to apply a theorem of Pólya that transforms this *geometric* positivity condition into an *algebraic* positivity condition. In Subsection 3.4 we see that this is almost what we need.

3.1 Lifting

The fact that f is positive on S means that every K–algebra homomorphism $K[\bar{X}] \to \mathbb{R}$ mapping $p_1, \dots, p_n$ to non–negative real numbers maps f to a positive real number. Using the isomorphism

$$K[\bar{Y}]/I \to K[\bar{X}]$$

induced by φ this means that every K–algebra homomorphism $K[\bar{Y}]/I \to \mathbb{R}$ mapping $Y_1 + I, \dots, Y_n + I$ to non–negative real numbers maps $g + I$ to a positive real number. This shows that g is strictly positive on the set

$$U := \mathbb{R}^n_{\geq 0} \ \cap \ V_{\mathbb{R}}(I) \subseteq \mathbb{R}^n$$

where $V_{\mathbb{R}}(I)$ is the set of real zeroes of the ideal I. The closed set U is contained in the compact set

$$V := \{y \in \mathbb{R}^n \mid y_1 \geq 0, \dots, y_n \geq 0, y_1 + \cdots + y_n = 1\}. \tag{3.5}$$

Now the conditions of the following lemma are satisfied, setting $r = r_1^2 + \cdots + r_t^2$:

Lemma 3.1 *Let V be a compact topological space and $U \subseteq V$. Let g and r be continous functions $V \to \mathbb{R}$ having the following properties:*

$$g > 0 \text{ on } U, \quad r \geq 0 \text{ on } U \quad \text{and} \quad r > 0 \text{ on } V \setminus U.$$

Then $g + cr > 0$ on V for every sufficiently large $c \in \mathbb{R}$.

PROOF. We may assume that U is open in V because otherwise we can pass over from U to $g^{-1}(\mathbb{R}_{>0})$. Then $V \setminus U$ is closed in a compact space and thus also compact. Assume $U \neq V$ as otherwise we are done. Then r and g take on a minimum $\mu > 0$ respectively $\mu' \in \mathbb{R}$ on $V \setminus U$. For $0 \leq c \in \mathbb{R}$ we get $g + cr \geq g > 0$ on U and $g + cr \geq \mu' + c\mu$ on $V \setminus U$. Now $\mu > 0$ implies $\mu' + c\mu > 0$ for sufficiently large c. $\square$

Therefore we can choose $c \in K$ big enough such that the polynomial

$$g' := g + c(r_1^2 + \cdots + r_t^2) \tag{3.6}$$

is strictly positive on V. Thus we have found g' strictly positive on V such that $\varphi(g') = f$.

3.2 Homogenization

Now we multiply each monomial in g' whose degree is lower than the degree of g' by an appropriate power of $Y_1 + \cdots + Y_n$ to equal the degrees of all occuring monomials, i.e. to make the polynomial homogeneous. This neither varies the values of the polynomial on V nor alters the fact that φ maps the polynomial to f, since $Y_1 + \cdots + Y_n \equiv 1 \mod I$. We call G the resulting homogeneous polynomial. As homogeneous polynomials have constant sign on each ray emitted by the origin the positivity of G on V is equivalent to

$$G > 0 \quad \text{on} \quad \mathbb{R}^n_{\geq 0} \setminus \{0\}. \tag{3.7}$$

3.3 Pólya's theorem

Now G meets the conditions of the theorem below discovered by Pólya in 1927. The proof consists only of a pure calculation and elementary analysis (see [Pól], [HLP] or [PR]).

Theorem 3.2 (Pólya) *Let $G \in \mathbb{R}[\bar{Y}]$ be an homogeneous polynomial. Then $G > 0$ on $\mathbb{R}^n_{\geq 0} \setminus \{0\}$ if and only if $G \cdot (Y_1 + \cdots + Y_n)^N$ has for some $N \in \mathbb{N}$ the form*

$$\sum_{e_1+\cdots+e_n=k} a_e Y_1^{e_1} \ldots Y_n^{e_n} \tag{3.8}$$

where $0 < a_e \in K$ for all *$e \in \mathbb{N}^d$ with $e_1 + \cdots + e_n = k$.*

As $\varphi(Y_1 + \cdots + Y_n) = 1$ the above theorem gives us a homogeneous polynomial G' of the form (3.8) which is mapped to f by φ.

3.4 Conclusion of the proof

Now we simply choose some sufficiently small $0 < a \in K$ such that the polynomial $h := G' - a(Y_1 + \cdots + Y_n)^k + a \in K[\bar{Y}]$ has no negative coefficients. Then $\varphi(h) = f$ and h has the positive constant coefficient a. Thus h is a polynomial as desired.

4 The algorithm

4.1 Turning the construction into an algorithm

From our proof of Schmüdgen's theorem 1.2 we can extract an algorithm performing the following: Given $p_1, \dots, p_n, f \in K[\bar{X}]$ such that $f > 0$ on S and a representation (1.1) of $s - \Sigma$ for some $0 \leq s \in K$, the algorithm computes a representation (1.2) of f. The only points that have to be examined are the following:

- How to compute some $g \in K[\bar{Y}]$ that is mapped to f by φ?
- How to compute $r_1, \dots, r_t$ such that (3.4) holds?
- How to choose the $c \in K$ such that $g' > 0$ on V (see Subsection 3.1)?

The first two items are standard problems which can be solved using Gröbner bases: We compute a Gröbner basis G of the ideal in $K[X_1, \dots, X_d, Y_1, \dots, Y_n]$ generated by the polynomials $p_1 - Y_1, \dots, p_n - Y_n$ with respect to some term order that lets all terms containing some X_i be larger than all other terms (e.g. with respect to the lexicographical term order given by $X_1 > \cdots > X_d > Y_1 > \cdots > Y_n$). Then the first problem is solved by computing a standard form g of f modulo G. The fact that the intersection $G \cap K[\bar{Y}]$ is a Gröbner basis of I answers the second question. See for example [SS], [GTZ], Proposition 6.44 in [BW].

The third problem is solved by just delaying the choice of c: Instead of (3.6) we define $g' := g + C(r_1^2 + \cdots + r_t^2) \in K[C, Y_1, \dots, Y_n]$. Then we homogenize g' with respect to $Y_1, \dots, Y_n$ by multiplying each monomial by an appropiate power of $Y_1 + \cdots + Y_n$. We get a polynomial G of the form

$$\sum_{e_1 + \cdots + e_n = k} (\lambda_e + \mu_e C) Y_1^{e_1} \cdots Y_n^{e_n} \qquad (k \in \mathbb{N}, \lambda_e, \mu_e \in K). \tag{4.1}$$

For every polynomial $H \in K[C, Y_1, \dots, Y_n]$ of this form we can quickly decide if there is $c \in K$ such that $H(c, Y_1, \dots, Y_n) \in K[Y_1, \dots, Y_n]$ is of the form (3.8), i.e. all $\lambda_e + \mu_e c$ are positive. In this case we can also compute such a

c without effort. Now we check successively for $N = 0, 1, 2, \ldots$ the existence of such a $c \in K$ for the polynomial $G \cdot (Y_1 + \cdots + Y_n)^N$ which is again of the form (4.1). For N big enough such a c can be computed and $G' := G(c, Y_1, \ldots, Y_n) \cdot (Y_1 + \cdots + Y_n)^N$ is of the form (3.8).

4.2 The burden of the compactness evidence

Of course the main drawback of the described algorithm is that it requires an *evidence* of the fact that S is compact, namely a representation (1.1) of some $s - \Sigma$, guaranteed to exist by the Positivstellensatz 1.1. One observes that our algorithm *basically* draws the squares needed for the representation of f from this evidence. The theorem of Pólya 3.2 has once before been used by Habicht (see [Hab]) to constructivize a *seemingly* very general case of Hilbert's 17th problem. In a newer variant of this algorithm given by Loera and Santos in [LS] one sees that Habicht restricts to the case where only "very special" squares are needed. So both the author and Habicht fail to address the problem of "computing the required squares".

In spite of this drawback one should be aware of the trivial observation that one can always adjoin $t - \Sigma$ to $p_1, \ldots, p_n$ for some $0 \leq t \in K$ large enough to let the set S unchanged. Then for $s := t + 1$ we have an obvious representation (1.1) of $s - \Sigma$. Furthermore of course if one has found a representation (1.1) of some $s - \Sigma$ for certain $p_1, \ldots, p_n$ once, it can be used for all f.

4.3 Complexity issues

For any homogeneous polynomial $G \in \mathbb{R}[\bar{Y}]$ we define the *Pólya–exponent* of G to be the smallest $N \in \mathbb{N}$ such that $G \cdot (Y_1 + \cdots + Y_n)^N$ has the form (3.8), if such N exists, and ∞ otherwise. (Thus the theorem of Pólya states that G has finite Pólya–exponent if and only if $G > 0$ on $\mathbb{R}^n_{\geq 0} \setminus \{0\}$.)

Certainly the Pólya–exponent plays a crucial role for the complexity of our algorithm. In [PR] Powers and Reznick prove the upper bound

$$l(l-1)\frac{c}{\mu} + 1 - l$$

for a homogeneous polynomial $G \in \mathbb{R}[\bar{Y}]$ of degree l where

- c denotes the maximum absolute value of the coefficients of G and
- μ denotes the (positive) minimum of G on the set V defined by (3.5).

The dependence of this bound on $\frac{c}{\mu}$ is unsatisfactory. However it seems to be inherent to the problem as is shown by the following proposition (proved by model–theoretic reasoning in [Rob]):

Proposition 4.1 *Consider the set $\mathcal{H}$ of all homogeneous polynomials $H \in \mathbb{R}[\bar{Y}]$ of a certain fixed degree. We endow $\mathcal{H}$ with a topology by identifying its elements with the tuple of their coefficients (in some fixed order). Then as H tends in $\mathcal{H}$ to some $G \neq 0$ having a zero $\xi \in \mathbb{R}^n_{>0}$ the Pólya–exponent of H tends to ∞.*

PROOF. Assume to the contrary that the Pólya exponent of H does not converge to ∞. Then there exists some sequence $(H_i)_{i\in\mathbb{N}}$ converging to G and some $N \in \mathbb{N}$ such that the Pólya exponent of H_i does not exceed N for any $i \in \mathbb{N}$. Hence for suitable $k \in \mathbb{N}$ and for any $i \in \mathbb{N}$ we can write

$$H_i \cdot (Y_1 + \cdots + Y_n)^N = \sum_{e_1+\cdots+e_n=k} a_{ei} Y_1^{e_1} \ldots Y_n^{e_n} \tag{4.2}$$

where $0 < a_{ei} \in \mathbb{R}$. We specialize Y_j to ξ_j in this equation and get for all e and for all $i \in \mathbb{N}$

$$\frac{H_i(\xi)(\xi_1 + \cdots + \xi_n)^N}{\xi_1^{e_1} \cdots \xi_n^{e_n}} \geq a_{ei} > 0$$

because all ξ_j are positive. As $\lim_{i\to\infty} H_i(\xi) = G(\xi) = 0$ this shows

$$\lim_{i\to\infty} a_{ei} = 0$$

for all e. Hence we get $G \cdot (Y_1 + \cdots + Y_n)^N = \lim_{i\to\infty} H_i \cdot (Y_1 + \cdots + Y_n)^N = 0$ by taking the limit for $i \to \infty$ in the coefficients of (4.2). This contradicts $G \neq 0$. $\square$

As small (positive) values of f on S give rise to small values of the polynomial G (on which we apply the theorem of Pólya 3.2 in Subsection 3.3) on the set V the running time of our algorithm depends badly on the minimum of f on S. But any other algorithm solving the same problem must show the same bad behaviour: Stengle shows in [Ste'] that under certain circumstances any representation 1.2 of f on S must also become arbitrarily large (in some reasonable sense) if f has sufficiently small values on S (for the simple elaborations left to the reader in the proof of his Theorem 3 see e.g. the first part of the proof of Theorem 3.2 on page 191 of [BCR]).

5 Square–free representations and compact convex polyhedra

The following theorem is just proved by reviewing the beginning of Section 3 (by the way condition (3.1) is already implied by the hypotheses of the theorem).

Theorem 5.1 *Let K be a subfield of $\mathbb{R}$. Let $p_1, \dots, p_n \in K[\bar{X}]$. Suppose that for every $g \in K[\bar{X}]$ there is some $0 \leq s \in K$ such that the two polynomials $s \pm g$ have a representation*

$$\sum_{e \in \mathbb{N}^n} a_e p_1^{e_1} \cdots p_n^{e_n} \tag{5.1}$$

where $0 \leq a_e \in K$ and almost all a_e are zero. Then for every $f \in K[\bar{X}]$ we have $f > 0$ on the (compact) set

$$S := \{x \in \mathbb{R}^d \mid p_1(x) \geq 0, \dots, p_n(x) \geq 0\}$$

if and only if f can be written in the form (3.3).

Remark 5.2 The above theorem follows from Krivine's representation theorem (cf. introduction) applied to the ring $K[\bar{X}]$ together with its subsemiring generated by $p_1, \dots, p_n$ and the nonnegative elements from K. Krivine's work [Kri'] remained unnoticed until recently and therefore this theorem is usually attributed to Kadison and Dubois (see [Bec],[Dub],[Kad]) and its first algebraic proof to Becker and Schwartz (see [BS]). Another proof of Theorem 5.1 is due to Handelman (see [Han]). His methods are similar to those used by Kadison and Dubois. All these proofs are inherently non–constructive. By a somewhat more technical but essentially the same process as in Section 3 one can give a proof of Krivine's representation theorem (see [Scw]) which is constructive to some extent. Furthermore a strong connection between Pólya's theorem 3.2 and the theorem of Kadison–Dubois is now revealed: In [Wör] Wörmann has already shown that the former follows from the latter. We have now gone the other way round.

Remark 5.3 The identities in the proof of Lemma 2.1 show that the set of all g for which there exists s as postulated in the above theorem is a subalgebra of $K[\bar{X}]$. So the condition has only to be checked for a generating system $g_1, \dots, g_m$ of the algebra $K[\bar{X}]$.

Obviously we get an algorithm that computes a representation (3.3) of f from the following data:

- $p_1, \dots, p_n, f \in K[\bar{X}]$ such that $f > 0$ on S and
- a generating system $g_1, \dots, g_m$ of the algebra $K[\bar{X}]$

- together with representations (5.1) of the $2m$ polynomials $s_i \pm g_i$ for some $0 \le s_1, \ldots, s_m \in K$

In a special case we use the following result from the theory of linear inequalities to get a particularly nice result:

Theorem 5.4 *Let K be an ordered field. Let $p_1, \ldots, p_k \in K[\bar{X}]$ be* linear *polynomials (i.e. polynomials of degree ≤ 1) defining the* non–empty *convex polyhedron*

$$S' := \{x \in K^d \mid p_1(x) \ge 0, \ldots, p_k(x) \ge 0\}.$$

Then for every linear polynomial $f \in K[\bar{X}]$ we have $f \ge 0$ on S' if and only if f can be written in the form

$$a_0 + a_1 p_1 + \cdots + a_k p_k \tag{5.2}$$

where $0 \le a_0, \ldots, a_k \in K$.

By simple elaborations (see [Scw]) this theorem follows from the well–known fundamental theorem of linear inequalities as it is stated for example in [Scr]. Moreover the proof in [Scr] gives an algorithm to decide if the representation (5.2) exists and to compute it in that case. Now we get the following theorem which was (for a slightly more special case) non–constructively proved by Handelman in 1988 (see [Han]):

Theorem 5.5 *Let K be a subfield of $\mathbb{R}$. Let* the linear *polynomials $p_1, \ldots, p_k \in K[\bar{X}]$ define the* non–empty and compact *convex polyhedron*

$$S' := \{x \in \mathbb{R}^d \mid p_1(x) \ge 0, \ldots, p_k(x) \ge 0\}.$$

Let $p_{k+1}, \ldots, p_n \in K[\bar{X}]$ be arbitrary polynomials and

$$S := \{x \in \mathbb{R}^d \mid p_1(x) \ge 0, \ldots, p_n(x) \ge 0\}.$$

Then for every $f \in K[\bar{X}]$ we have $f > 0$ on S if and only if f can be written in the form (3.3).

PROOF. Suppose $f > 0$ on S. We choose a system $g_1, \ldots, g_m$ of *linear* generators of the algebra $K[\bar{X}]$, e.g. $m = n$, $g_i = X_i$. Because S' is compact we can choose $0 \le s_1, \ldots, s_m \in K$ such that the $2m$ conditions $s_i \pm g_i \ge 0$ hold on S', and so according to Theorem 5.4 have a representation (5.2) which is in particular a representation (5.1). Now by Remark 5.3 Theorem 5.1 applies. □

Because there is an algorithm for Theorem 5.4 we obviously get an algorithm which performs the following: Upon input of $p_1, \ldots, p_n$ satisying the conditions of the theorem and $f \in K[\bar{X}]$ which is strictly positive on S, it computes a representation (3.3) of f.

Remark 5.6 In 1924 Pólya and Szegö published their book [PS] in which they constructively prove the above theorem for the special case $d = 1, k = n = 2, p_1 = X, p_2 = 1 - X$ (Part VI, Solutions, 49, second solution). Having a close look at their algorithm one sees that it actually does carry out the same procedure than our algorithm does in this special case. However as the theorem of Pólya had not been established yet they use various other results for their proof.

In the same article [Pól] where Pólya proved his theorem he did also prove the above theorem for the special case $k = n, p_1 = X_1, \ldots, p_{n-1} = X_{n-1}, p_n = 1 - (X_1 + \cdots + X_{n-1})$. For this case our proof collapses into his.

Remark 5.7 With easy technical modifications all the results in this paper carry over to the more general setting where one considers an affine algebra $K[\bar{X}]/I$ instead of the polynomial algebra $K[\bar{X}]$.

References

[BCR] C. Berg, J.P.R. Christensen, P. Ressel: Harmonic analysis on semigroups, Graduate Texts in Mathematics **100**, New York: Springer–Verlag (1984)

[Bec] E. Becker: Partial orders on a field and valuation rings, Commun. Algebra **7**, 1933–1976 (1979)

[BS] E. Becker, N. Schwartz: Zum Darstellungssatz von Kadison–Dubois, Arch. Math. **40**, 421–428 (1983)

[BW] T. Becker, V. Weispfenning: Gröbner bases, Graduate Texts in Mathematics **141**, New York: Springer–Verlag (1993)

[Dub] D.W. Dubois: A note on David Harrison's theory of preprimes, Pacific J. Math. **21**, 15–19 (1967)

[GTZ] P. Gianni, B. Trager, G. Zacharias: Gröbner bases and primary decomposition of polynomial ideals, J. Symb. Comput. **6**, No. 2/3, 149–167 (1988)

[Hab] W. Habicht: Über die Zerlegung strikter definiter Formen in Quadrate, Comment. Math. Helv. **12**, 317–322 (1940)

[Han] D. Handelman: Representing polynomials by positive linear functions on compact convex polyhedra, Pac. J. Math. **132**, No.1, 35–62 (1988)

[HLP] G.H. Hardy, J.E. Littlewood, G. Pólya: Inequalities, second edition, Cambridge: Cambridge University Press (1967)

[Kad] R.V. Kadison: A representation theory for commutative topological algebra, Mem. Am. Math. Soc. **7** (1951)

[Kri] J.L. Krivine: Anneaux préordonnés, J. Anal. Math. **12**, 307–326 (1964)

[Kri'] J.L. Krivine: Quelques propriétés des préordres dans les anneaux commutatifs unitaires, C. R. Acad. Sci. Paris **258**, 3417–3418 (1964)

[KS] M. Knebusch, C. Scheiderer: Einführung in die reelle Algebra, Vieweg Studium **63**, Aufbaukurs Mathematik, Braunschweig: Vieweg (1989)

[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)

[LS'] J.A. de Loera, F. Santos: Corrections to An effective version of Pólya's theorem on positive definite forms, J. Pure Appl. Algebra, to appear

[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, submitted for the Méthodes Effectives en Géométrie Algébrique (MEGA) 2000 conference

[Pre] A. Prestel: Lectures on formally real fields, Rio de Janeiro: IMPA (1975), reprinted in: Lecture Notes in Mathematics **1093**, Berlin etc.: Springer–Verlag (1984)

[PS] G. Pólya, G. Szegö: Problems and theorems in analysis, Vol. II, Theory of functions – zeros – polynomials – determinants – number theory – geometry, Rev. and enl. translation of the 4th ed, Springer Study Edition, New York – Heidelberg – Berlin: Springer–Verlag (1976)

[Rob] A. Robinson: Algorithms in Algebra, D.H. Saracino, V. Weispfenning (ed.), Model Theory and Algebra, Lecture Notes in Mathematics **498**, Berlin etc.: Springer–Verlag, 28–33 (1975)

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

[Scr] A. Schrijver: Theory of linear and integer programming, Wiley–Interscience Series in Discrete Mathematics, Chichester: Wiley & Sons Ltd (1986)

[Scw] M. Schweighofer: Algorithmische Beweise für Nichtnegativ– und Positiv–stellensätze, Diplomarbeit, Universität Passau/Germany (1999)

[Ste] G. Stengle: A Nullstellensatz and a Positivstellensatz in semialgebraic geometry, Math. Ann. **207**, 87–97 (1974)

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

[SS] D. Shannon, M. Sweedler: Using Gröbner bases to determine algebra membership, split surjective algebra homomorphisms determine birational equivalence, J. Symb. Comput. **6**, No. 2/3, 267–273 (1988)

[Wör] T. Wörmann: Strikt positive Polynome in der semialgebraischen Geometrie, Dissertation, Universität Dortmund/Germany (1998)