On special representations of strictly positive polynomials

Thomas Jacobi – Alexander Prestel

1 Introduction

Let $K = S(p_1, \dots, p_m)$ be a compact basic closed semi-algebraic subset of $\mathbb{R}^n$, i.e., $p_1, \dots, p_m$ are polynomials from $\mathbb{R}[X] := \mathbb{R}[X_1, \dots, X_n]$ and

$$S(p_1, \dots, p_m) := \{a \in \mathbb{R}^n \mid p_1(a) \geq 0, \dots, p_m(a) \geq 0\}.$$

In [Sch], Schmüdgen has shown that every $p \in \mathbb{R}[X]$, strictly positive on K, i.e., $p(a) > 0$ for all $a \in S$, has a representation

$$p = \sum_{\nu} p_1^{\nu_1} \cdots p_m^{\nu_m} \sigma_\nu \tag{1.1}$$

where $\nu = (\nu_1, \dots, \nu_m) \in \{0, 1\}^m$ and $\sigma_\nu \in \sum \mathbb{R}[X]^2$ = set of sums of squares in the ring $\mathbb{R}[X]$. In [Pu], Putinar investigated the problem, if every $p \in \mathbb{R}[X]$, strictly positive on K, would already allow a representation

$$p = \sigma_0 + p_1\sigma_1 + \cdots + p_m\sigma_m \tag{1.2}$$

with $\sigma_i \in \sum \mathbb{R}[X]^2$. He succeeded to prove that (1.2) holds for all p, strictly positive on K, if and only if (1.2) holds for at least one such p with $p^{-1}(\mathbb{R}_+)$ being bounded, e.g., for the polynomial $f := N^2 - \sum_1^n X_i^2$ where N is the radius of an open sphere with center 0 and containing $S(p_1, \dots, p_m)$. It remained as an open problem ([Pu], p. 973) whether for every bounded set $S(p_1, \dots, p_m)$, the polynomial f would admit a representation (1.2). In this paper we show that this need not always be so. We give a complete characterisation (3.2) of m-tuples $p_1, \dots, p_m$ for which every $p \in \mathbb{R}[X]$, strictly positive on $S(p_1, \dots, p_m)$ has a representation (1.2).

Schmüdgen and Putinar both prove their theorem by solving first an appropriate 'Moment-Problem' by functional analytic methods. In [W], Wörmann proved Schmüdgen's Theorem in an elementary algebraic way, using the representation theorem of Kadison-Dubois (which in [B-S] was also proved by algebraic methods). By generalising the Kadison-Dubois-Theorem suitably, the first author was able to give an elementary proof for Putinar's Theorem in [J1].

As already done in [J1], we continue to work with so-called semi-orderings (introduced in [Pr]). Moreover, we make extensive use of the so-called Bröcker-Prestel Local-Global-Principle for weak isotropy of quadratic forms (the proof of which is also based on semi-orderings).

As a consequence of our characterisation theorem 3.2, we are able to detect the 'gap' between Schmüdgen's representation (1.1) and Putinar's representation (1.2): We shall show that not all 2^m products $p_1^{\nu_1} \cdots p_m^{\nu_m}$ in (1.1) are really needed. There is always a subset of $2^{m-1}+1$ products, including $1, p_1, \ldots, p_m$, such that every $p \in \mathbb{R}[X]$, strictly positive on $S(p_1, \ldots, p_m)$, has a representation (1.1) w.r.t. this subset. If $m = 2$, we therefore see that a 'linear' representation is always possible, while for $m = 3$ this is no longer true. This strengthening of Schmüdgen's Theorem is in a sense best possible (see Example 4.5), and it also yields a corresponding strengthening of his solution of the Moment Problem for compact semi-algebraic sets $S(p_1, \ldots, p_m)$.

2 The semi-real spectrum of a ring

As we shall see, the difference between the representations (1.1) and (1.2) become clear by considering the semi-real spectrum of $\mathbb{R}[X]$, we are going to introduce now.

Let A be a commutative ring with 1. A subset P of A is called a *preordering* (of level 2) if

$$P + P \subset P, \quad P \cdot P \subset P, \quad A^2 \subset P, \quad -1 \notin P.$$

If P is maximal with those properties, we find in addition $P \cup -P = A$ and that $P \cap -P$ is a prime ideal in A (see e.g. [Pr], Lemma 1.4). A preordering with those additional properties is called an *ordering* of A. The collection of all orderings of A is called the *real spectrum* $\mathrm{Sper}(A)$ of A. The ring A is *formally real*, if $P = \sum A^2$ is a preordering of A, i.e., $-1 \notin \sum A^2$. A is formally real if and only if $\mathrm{Sper}(A) \neq \emptyset$. The ring A admits an ordering P satisfying $P \cap -P = \{0\}$ if and only if $\sum a_i^2 = 0$ implies $a_i = 0$ for all elements a_i of A. This is the case if and only if the field of fractions $\mathrm{ff}(A)$ of A is formally real. A prime ideal $\mathfrak{P}$ of A is called *real* if $\sum a_i^2 \in \mathfrak{P}$ implies $a_i \in \mathfrak{P}$ for all $a_i \in A$. Thus $\mathfrak{P}$ is real if and only if $\mathrm{ff}(A/\mathfrak{P})$ is formally real.

If P is a preordering, a set $M \subset A$ satisfying

$$1 \in M, \quad -1 \notin M, \quad M + M \subset M, \quad P \cdot M \subset M,$$

M is called a *P-module*. A P-module $M \subset A$ which is maximal with respect to inclusion, satisfies in addition

$$M \cup -M = A \quad \text{and} \quad M \cap -M \text{ is a prime ideal} \tag{2.1}$$

(see [J1], Remark 1). P-modules satisfying (2.1) will be called *P-semi-orderings*. For the rest of the paper, we always let $P = \sum A^2$, thus in particular A is formally real. A $\sum A^2$-semi-ordering is simply called a *semi-ordering*, always denoted by S, and a $\sum A^2$-module will be called a *quadratic module*. By Semi-Sper(A) we denote the collection of all semi-orderings S of A, and by Semi-Sper$_M(A)$ the collection of those containing M. Clearly

$$\operatorname{Sper}(A) \subset \operatorname{Semi-Sper}(A).$$

For every semi-ordering S we define $S^+ := S \setminus (-S)$. From [J1], Lemma 1, we recall the 'Positivstellensatz' for Semi-Sper$_M(A)$.

Lemma 2.1 *Let A be a formally real ring, $M \subset A$ a quadratic module, and $a \in A$. Then $a \in S^+$ for all $S \in$ Semi-Sper$_M(A)$ iff $\sigma a \in 1 + M$ for some $\sigma \in \sum A^2$ (or equivalently $(1+\sigma')a \in 1 + M$ for some $\sigma' \in \sum A^2$).*

Semi-orderings have a very natural connection to quadratic forms. We are going to explain this in the following.

Let F be any field and $p_1, \dots, p_m \in F$. We then denote by $\varrho = \langle p_1, \dots, p_m \rangle$ the quadratic form $\sum p_i Z^2$. By $\varrho^\star$ we denote the *regular part* of ϱ, i.e., the subform of ϱ consisting only of those entries p_i that are different from zero. A regular quadratic form ϱ is called *weakly isotropic* if $n \cdot \varrho := \varrho \perp \cdots \perp \varrho$ (n-times) is isotropic for some $n \geq 1$[1] In case F is formally real, $\varrho = \langle p_1, \dots, p_m \rangle$ is weakly isotropic if and only if $p_1\sigma_1 + \cdots + p_m\sigma_m = 0$ for some $\sigma_i \in \sum F^2$, not all zero. A regular quadratic form $\varrho = \langle p_1, \dots, p_m \rangle$ is called *indefinite* w.r.t. a semi-ordering S of F, if there are p_i and p_j of different sign w.r.t. S. Note that a semi-ordering S on a field F clearly satisfies $S \cap -S = \{0\}$. A regular quadratic form ϱ is weakly isotropic over F if and only if ϱ is indefinite w.r.t. all semi-orderings of F (see [Pr], Theorem 2.9). This fact helps to get rid of the semi-orderings in Lemma 2.1.

Lemma 2.2 *Let A be a commutative ring with 1, $M = \sum A^2 + p_1 \sum A^2 + \cdots + p_m \sum A^2$ a quadratic module of A, and $p \in A$. Then there exists $\sigma \in \sum A^2$ such that $\sigma p \in 1 + M$ if and only if for every real prime ideal $\mathfrak{P}$ of A the regular part of $\langle 1, -\overline{p}, \overline{p}_1, \dots, \overline{p}_m \rangle$ is weakly isotropic in the field of fractions $F = ff(\overline{A})$ of $\overline{A} = A/\mathfrak{P}$.*

Proof: Let S be a semi-ordering of A. Then $\mathfrak{P} = S \cap -S$ is a prime ideal of A. Thus S induces a semi-ordering $\overline{S}$ on $\overline{A} = A/\mathfrak{P}$ which canonically extends to a semi-ordering (again denoted by $\overline{S}$) on $F = \text{ff}(A)$. For every $q \in S^+$ we find $\overline{q} \in \overline{S} \setminus \{0\}$. Hence the form $\langle 1, -\overline{p}, \overline{p}_1, \dots, \overline{p}_m \rangle^\star$ is indefinite in F w.r.t. $\overline{S}$, if we assume that $p \in S^+$ for all $S \in$ Semi-Sper$_M(A)$. If conversly we have any semi-ordering on the field F and hence also on $\overline{A}$ (call it $\overline{S}$ on $\overline{A}$), then the preimage

[1] All notion from quadratic form theory used in this article can be found in [L].

on $\overline{S}$ in A, denoted by S, clearly is a semi-ordering on A with $S \cap -S = \mathfrak{P}$. Moreover, if $\overline{p}_1, \dots, \overline{p}_m \in \overline{S}$, we get $M \subset S$. Therefore, if $\langle 1, -\overline{p}, \overline{p}_1, \dots, \overline{p}_m \rangle^\star$ is indefinite w.r.t. $\overline{S}$, we find $p \in S^+$.

We have thus proved (by using Lemma 2.1), that there exists $\sigma \in \sum A^2$ with $\sigma p \in 1 + M$ if and only if for every real prime ideal $\mathfrak{P}$ of A, the regular part of the form $\langle 1, -\overline{p}, \overline{p}_1, \dots, \overline{p}_m \rangle$ is indefinite w.r.t. all semi-orderings of $F = \mathrm{ff}(A/\mathfrak{P})$, and hence is weakly isotropic in F. □

In the next chapter we shall apply Lemma 2.2 to the situation of Putinar's Theorem. It will be then important to have the following Local-Global-Principle for weak isotropy at hand.

Theorem 2.3 *Let F be a formally real field and $a_1, \dots, a_m \in F \setminus \{0\}$. Then the quadratic form $\varrho = \langle a_1, \dots, a_m \rangle$ is weakly isotropic in F if an only if*

(1) ϱ is indefinite w.r.t. all archimedean orderings on F, and

(2) ϱ is weakly isotropic in the henselisation $H = (F, v)^h$ of F w.r.t. every valuation v with formally real residue field.

Proofs of this theorem can be found in [Br] (Theorem 3.9), [Pr] (Theorem 8.12) or in [Scha] (Theorem 7.12).

3 The Characterisation Theorem

In this chapter A will always be an affine $\mathbb{R}$-algebra, i.e., $A = \mathbb{R}[x_1, \dots, x_n] = \mathbb{R}[X_1, \dots, X_n]/\mathcal{I}$ where $\mathcal{I}$ is any ideal of the polynomial ring $\mathbb{R}[X]$. If $\mathcal{I}$ is generated, say, by $h_1, \dots, h_l$, we shall consider the real variety $V(\mathcal{I}) = \{a \in \mathbb{R}^n \mid h_1(a) = 0, \dots, h_r(a) = 0\}$. In $V(\mathcal{I})$ we may define the basic closed semi-algebraic set $K = S(p_1, \dots, p_m) = \{a \in V(\mathcal{I}) \mid p_1(a) \geq 0, \dots, p_m(a) \geq 0\}$ and then study those $p \in \mathbb{R}[x]$ that are strictly positive on K.

Our main aim is to characterise those m-tuples $p_1, \dots, p_m \in \mathbb{R}[x]$ with compact set $K = S(p_1, \dots, p_m)$, such that every $p \in \mathbb{R}[x]$, strictly positive on K, has a representation (1.2). As a first step, we connect Putinar's condition with Lemma 2.1 and hence with Lemma 2.2.

Lemma 3.1 *Let M be a quadratic module of $\mathbb{R}[x] = \mathbb{R}[x_1, \dots, x_n]$. Then $f := N^2 - (x_1^2 + \dots + x_n^2) \in M$ for some $N \in \mathbb{N}$ if and only if $\sigma(C - (x_1^2 + \dots + x_n^2)) \in 1 + M$ for some $C \in \mathbb{N}$ and $\sigma \in \sum \mathbb{R}[x]^2$.*

Proof: The 'only if' part is obvious. For the 'if' part let $f := C - (x_1^2 + \dots + x_n^2)$ and assume $\sigma f \in 1 + M$ for some $\sigma \in \sum \mathbb{R}[x]^2$. We first note that the quadratic module $M(f) := \sum \mathbb{R}[x]^2 + f\mathbb{R}[x]^2$ is archimedean (i.e., for every $a \in A$, $k - a \in M$

for some $k \in \mathbb{N}$), since $(C+\frac{1}{2}) \pm x_i = \frac{1}{2}(1 \pm x_i)^2 + f + \sum_{j \neq i} x_j^2 \in M(f)$. By Lemma 2.1 we find $(1+\sigma')f \in M$ for some $\sigma' \in \sum \mathbb{R}[x]^2$. This yields $f+\sigma' C \in M$ and $(1+\sigma)M(f) \subset M$. We choose $C' \in \mathbb{N}$ such that $C' - \sigma' \in M(f)$ and hence $(1+\sigma')(C'-\sigma') \in M$. Thus $C'-\sigma' = (1+C')((1+\sigma')(C'-\sigma') + (C'-\sigma')^2) \in M$ and finally $C(1+C') - (x_1^2 + \cdots + x_n^2) = (f + C\sigma') + C(C'-\sigma') \in M$. □

In view of this lemma, Lemma 2.1 is saying that M is archimedean if and only if every semi-ordering $S \supset M$ is archimedean. Since the N such that $N^2 - (x_1^2 + \cdots + x_n^2) \in S$ need not be the same for all S, a little compactness argument is used to see the last statement.

Combining now Lemma 2.2 with Theorem 2.3 on the one hand side, and with Lemma 3.1 and Putinar's Theorem on the other side, we shall get the

Theorem 3.2 (Characterisation Theorem) *Let $p_1, \ldots, p_m \in \mathbb{R}[x_1, \ldots, x_n] = A$ such that $K = S(p_1, \ldots, p_m)$ is compact. Then every $p \in A$, strictly positive on K, has a representation (1.2) if and only if for every real prime ideal $\mathfrak{P}$ of A, the form $\langle 1, \overline{p}_1, \ldots, \overline{p}_m \rangle^\star$ is weakly isotropic in the henselisation $H = (F, v)^h$ of $F = ff(A/\mathfrak{P})$ w.r.t. every valuation v of F such that the residue field of H is formally real and $v(\overline{x}_i) < 0$ for at least one $i \leq n$.*

Before we come to the proof of Theorem 3.2, we recall a very useful method that allows us to check whether a regular quadratic form $\varrho = \langle a_1, \ldots, a_r \rangle$ with $a_1, \ldots, a_r \in H$, is isotropic (or weakly isotropic) over H. This is actually the case if and only if one of the so-called 'residue forms' of ϱ is isotropic (or weakly isotropic) over the residue field $\overline{H}$ of H. At that point we assume $\mathrm{char}(\overline{H}) \neq 2$, which in our case will always be true since $\overline{H}$ will be formally real.

The residue forms of ϱ are obtained in the following way: We first choose elements c_i $(i \leq s)$ such that the values $v(c_i)$ yield a set of representatives of the subset $\{v(a_\nu) + 2\Gamma \mid 1 \leq \nu \leq r\}$ of $\Gamma/2\Gamma$, where Γ denotes the value group of (H, v). As representative for $0 + 2\Gamma$ we always choose 1. We then group the elements a_ν $(1 \leq \nu \leq r)$ into blocks a_{ij} $(1 \leq i \leq s,\ 1 \leq j \leq r_i)$ such that

$$a_{ij} \equiv c_i \mod 2\Gamma.$$

Next we choose elements $b_{ij} \in H$ such that $a_{ij} c_i^{-1} b_{ij}^2$ is a unit in the valuation ring $\mathcal{O}$ of v. Finally we see that the quadratic form ϱ is isometric to

$$c_1 \varrho^{(1)} \perp \cdots \perp c_s \varrho^{(s)}$$

with $\varrho^{(i)} = \langle a_{i1} c_i^{-1} b_{i1}^2, \ldots, a_{ir_i} c_i^{-1} b_{ir_i}^2 \rangle$. The regular forms

$$\overline{\varrho}^{(i)} = \langle \overline{a_{i1} c_i^{-1} b_{i1}^2}, \ldots, \overline{a_{ir_i} c_i^{-1} b_{ir_i}^2} \rangle$$

of $\overline{H}$ are called the residue forms of ϱ. The form corresponding to $c = 1$ is called the first residue form. The proof of the following proposition is a standard application of Hensel's Lemma (see e.g. [Pr], Theorem 8.9).

Proposition 3.3 *ϱ is isotropic over H if and only if one of the residue forms $\overline{\varrho}^{(i)}$ is isotropic over $\overline{H}$.*

Proof of Theorem 3.2: By Lemma 2.2, Lemma 3.1 and Putinar's Theorem, we have to show that for every real prime ideal $\mathfrak{P}$ of A, the form $\langle 1, -\overline{f}, \overline{p}_1, \ldots, \overline{p}_m\rangle^\star$ with $f = N^2 - (x_1^2 + \cdots + x_n^2)$ is weakly isotropic in $F = \mathrm{ff}(\overline{A})$ with $\overline{A} = A/\mathfrak{P}$, if and only if the condition of the theorem holds for all such prime ideals $\mathfrak{P}$.

We first assume the assumption of the Theorem and prove weak isotropy of the form $\varrho := \langle 1, -\overline{f}, \overline{p}_1, \ldots, \overline{p}_m\rangle^\star$ by induction on the transcendence degree $\mathrm{trdeg}_{\mathbb{R}}(F)$ over $\mathbb{R}$.

If $\mathrm{trdeg}_{\mathbb{R}}(F) = 0$, then obviously $F = \mathbb{R}$. In this case ϱ is indefinite and hence isotropic over F. In fact, if none of the $\overline{p}_i = p_i(\overline{x})$ is negative, $\overline{x} \in K$ and hence $\overline{f} = f(\overline{x}) > 0$.

Now let $\mathrm{trdeg}_{\mathbb{R}}(F) > 0$. Then there are no archimedean orderings on F. Thus by the Local-Global-Principle (2.4), we have only to consider the henselisations $H = (F, v)^h$ with formally real residue field (and $v(H)$ not 2-divisible). If $v(\overline{x}_i) < 0$ for some i, the assumption of the theorem says that $\langle 1, \overline{p}_1, \ldots, \overline{p}_m\rangle^\star$ and hence in particular ϱ is weakly isotropic over H. It remains to look at those valuations v such that $\overline{H} \subset \mathcal{O}_v$. The maximal ideal $\mathfrak{M}_v$ of the valuation ring $\mathcal{O}_v$ then intersects $\overline{A}$ in a prime ideal $\mathfrak{P}'$. Since $\overline{A}' = \overline{A}/\mathfrak{P}'$ embeds into $\mathcal{O}_v/\mathfrak{M}_v$, the field of fractions F' of the ring $\overline{A}'$ is formally real and $\mathrm{trdeg}_{\mathbb{R}}(F') < \mathrm{trdeg}_{\mathbb{R}}(F)$. Thus by induction, the form $\langle 1, -\overline{f}', \overline{p}_1', \ldots, \overline{p}_m'\rangle^\star$ is weakly isotropic over F'. Since this form clearly is a subform of the first residue form of ϱ we find from Proposition 3.3, that ϱ is weakly isotropic over $H = (F, v)^h$.

For the converse, we assume that $\varrho = \langle 1, -\overline{f}, \overline{p}_1, \ldots, \overline{p}_m\rangle^\star$ is weakly isotropic in $F = \mathrm{ff}(\overline{A})$. We then show that the 'local' conditions of the theorem are satisfied for F. Let thus v be a valuation of F with formally real residue field L and $v(\overline{x}_1) \leq v(\overline{x}_j)$ for all $j \leq n$. Since the residue field L of (F, v) is formally real and $v(N) = 0$, we get $v(f) = v(\overline{x}_1^2) \in 2\Gamma$. Thus ϱ and the form $\tau = \langle 1, \overline{p}_1, \ldots, \overline{p}_m\rangle^\star$ have the same residue forms except for the first one. By assumption, ϱ is weakly isotropic over F, hence one of its residue forms is weakly isotropic over L. If such a form is not the first one, by Proposition 3.3, τ will be weakly isotropic over the henselisation $H = (F, v)^h$. Now assume the first residue form of ϱ is weakly isotropic over L. By choosing $b_{12} = \overline{x}_1^{-1}$ in the definition of the residue forms above we see that the residue of $-\overline{f} b_{12}^2$ will be a sum of squares in L. Thus the first residue form of ϱ being weakly isotropic in L, implies that the first residue form of τ is weakly isotropic in L as well. Now again by Proposition 3.3 we are done. $\square$

4 Optimal representations of positive polynomials

In this section we first study under what circumstances we could satisfy the local conditions of the Characterisation Theorem 3.2 in order to achieve a 'linear' representation (1.2) for every $p \in \mathbb{R}[x]$, strictly positive on $S(p_1, \dots, p_m)$. After that we shall improve Schmüdgen's Theorem in the general case.

For the first result of this section we let A be the ring of polynomials $\mathbb{R}[X] = \mathbb{R}[X_1, \dots, X_n]$. From the assumption that $K = S(p_1, \dots, p_m) \subset \mathbb{R}^n$ is compact, it follows that for every $a \in \mathbb{R}^n \setminus \{0\}$ and $t \in \mathbb{R}_+$ big enough, at least one of $p_1(ta), \dots, p_m(ta)$ has to be negative. If we write $p_i = p_i^* + p_i'$ where p_i^* is the homogeneous part of p_i of highest degree, and assume that $p_i^*(a) \neq 0$, then $p_i(ta)$ being eventually negative is just expressed by $p_i^*(a) < 0$. In general it need not be true that for every $a \in \mathbb{R}^n \setminus \{0\}$ always one of the $p_i^*(a)$ is negative. But, if it is so, we get a special representation for $p \in \mathbb{R}[X]$, being strictly positive on $S(p_1, \dots, p_m)$. In order to formulate this, let us rearrange the sequence $p_1, \dots, p_m$ into two sequences $p_1, \dots, p_r$ of even degree and $q_1, \dots, q_s$ of odd degree. Hence

$$(p_1, \dots, p_m) = (p_1, \dots, p_r, q_1, \dots, q_s).$$

We then have

Theorem 4.1 *Let $p_i \in \mathbb{R}[X] = \mathbb{R}[X_1, \dots, X_n]$ be as above and assume that $K = S(p_1, \dots, p_m)$ is compact. Moreover assume that for every $a \in \mathbb{R}^n \setminus \{0\}$ one of $p_1^*(a), \dots, p_m^*(a)$ is negative. Then every $p \in \mathbb{R}[X]$, strictly positive on K, has a representation*

$$p = \sigma_0 + p_1\sigma_1 + \cdots + p_m\sigma_m \tag{4.1}$$

with $\sigma_i \in \sum \mathbb{R}[x]^2$ if all p_i have even degree, or all p_i have odd degree. In particular, if $p_1, \dots, p_m$ are linear and K is compact and non-empty, a representation (4.1) always exists. Otherwise, p has a representation

$$p = \sigma_0 + \sum_{1 \le i \le r} p_i\sigma_i + \sum_{1 \le i < j \le s} q_i q_j \sigma_{ij} \tag{4.2}$$

with $\sigma_0, \sigma_i, \sigma_{ij} \in \sum \mathbb{R}[X]^2$.

Proof: Let us start by considering the case $r = m$, i.e., all p_i have even degree. In this case we first conclude that for every formally real field extension $L/\mathbb{R}$ of finite transcendence degree d and for every element $a \in L^n \setminus \{0\}$, the form

$$\tau = \langle 1, p_1^*(a), \dots, p_m^*(a) \rangle^\star$$

is weakly isotropic in L. In fact, this follows by induction on d:

If $d = 0$, then $L = \mathbb{R}$, and since at least one of the $p_i^*(a)$'s is negative, τ is (weakly) isotropic in L.

If $d > 0$, we apply the Local-Global-Principle 2.3. Thus let v be a valuation of L with formally real residue field. Assume that $v(a_1) \leq v(a_j)$ for all $j \leq n$. Replacing then a_j in p_i^* by a_j/a_1 amounts to multiply p_i^* by some even power of a_1. Concerning weak isotropy there is therefore no restriction in assuming that $v(a_j) \geq 0$ for all $j \leq n$. Now by the induction assumption, the form

$$\tau = \langle 1, p_1^*(\overline{a}), \ldots, p_m^*(\overline{a})\rangle^\star$$

is weakly isotropic in $\overline{L}$. (Note that here we use $\overline{\cdot}$ for the residue map w.r.t. the valuation v.) Hence by Hensel's Lemma, τ is weakly isotropic in the henselisation $(L, v)^h$. Since L has no archimedean ordering, we are therefore done with the Local-Global-Principle 2.3.

Returning now to the condition of Theorem 3.2, let $F = \mathrm{ff}(\overline{A})$ be formally real with $\overline{A} = A/\mathfrak{P}$ and let v be a valuation of F with, say, $v(\overline{X}_1) < 0$ and $v(\overline{X}_1) \leq v(\overline{X}_j)$ for all $j \leq n$. For every $i \leq n$ we let $d_i = \deg(p_i)$. Concerning isotropy, it does not matter, if we pass from the form $\langle 1, p_1(\overline{X}), \ldots, p_m(\overline{X})\rangle^\star$ to the form

$$\varrho = \langle 1, \overline{X}_1^{-d_1} p_1(\overline{X}), \ldots, \overline{X}_m^{-d_m} p_m(\overline{X})\rangle^\star.$$

This form, however, is weakly isotropic in $H = (F, v)^h$, since passing to the residue field L of (F, v), we obtain that the form

$$\langle 1, p_1^*(a), \ldots, p_m^*(a)\rangle^\star$$

is a subform of the first residue form of ϱ, where a_j is the residue image of $\overline{X}_j/\overline{X}_1$ in L. As we have seen above, this form is weakly isotropic in L. Now we can apply Theorem 3.2 to the sequence $p_1, \ldots, p_m$.

Next we consider the case $s = m$, i.e., all p_i have odd degree. The proof is essentially the same as in the even case. The only main change is that we don't deal with the form $\langle 1, p_1^*, \ldots, p_m^*\rangle^\star$, but instead with its subform $\langle p_1^*, \ldots, p_m^*\rangle^\star$. This has to be done since we are now scaling each $p_i^*(a)$ by some odd power of, say, a_1. From the assumption that, for each $a \in \mathbb{R}^n \setminus \{0\}$ one of the values $p_j^*(a)$ is negative, we also get that some value $p_j^*(a)$ is positive (simply take $-a$ for a). Thus the form $\langle p_1^*(a), \ldots, p_m^*(a)\rangle^\star$ is indefinite over $\mathbb{R}$, which starts the induction.

Finally, we consider the general situation. Again the proof is almost like that of the even case. In fact, we consider now the form

$$\tau = \langle 1, p_1^*, \ldots, p_m^*\rangle^\star \perp \langle q_i^* q_j^* \mid 1 \leq i < j \leq s\rangle^\star$$

of even degree homogeneous polynomials. For every $a \in \mathbb{R}^n \setminus \{0\}$, the assumption that at least one of $p_1^*(a), \ldots, p_m^*(a)$ is negative implies that $\tau(a)^\star$ is indefinite over $\mathbb{R}$. This starts the induction for showing that for every formally real field extension $L/\mathbb{R}$ and every $a \in L^n \setminus \{0\}$, the form $\tau(a)^\star$ is weakly isotropic over L. As in the even case we apply Theorem 3.2. This time, however, to the sequence $p_1, \ldots, p_m, q_i q_j$ $(1 \le i < j \le s)$ which as well defines the set $K = S(p_1, \ldots, p_m)$. $\square$

It's easy to check that Theorem 4.3 yields a representation (4.1) if K is compact, non-empty and all p_i's are linear: W.l.o.g. we can assume that $0 \in K$. If for some $a \in \mathbb{R}^n \setminus \{0\}$ all $p_i^\star(a)$'s are non-negative we find $p_i(\lambda a) = p_i(0) + \lambda p_i^\star(a) \ge 0$ for all $\lambda \ge 0$ and $1 \le i \le m$. Obviously, this would contradict the compactness of K and so the first condition of Theorem 4.3 is satisfied.

It should be noted that the conditions of Theorem 4.1 actually are conditions on the points 'at infinity'. In fact, let us recall the *homogenisation*

$$F(X_0, X_1, \ldots, X_n) := X_0^{\deg(f)} f\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right)$$

of a polynomial $f \in \mathbb{R}[X_1, \ldots, X_n]$. For $p_1, \ldots, p_m \in \mathbb{R}[X_1, \ldots, X_n]$ we define

$$S(P_1, \ldots, P_m) := \{a \in \mathbb{R}^{n+1} \setminus \{0\} \mid P_1(a) \ge 0, \ldots, P_m(a) \ge 0\}.$$

Then for $f := N^2 - (X_1^2 - \cdots - X_n^2)$, the condition

$$F > 0 \quad \text{on} \quad S(P_1, \ldots, P_m)$$

is equivalent to saying that $S(p_1, \ldots, p_m)$ is bounded (taking $X_0 = 1$) and that one of $p_1^*(b), \ldots, p_m^*(b)$ is negative for every $b \in \mathbb{R}^n \setminus \{0\}$ (taking $X_0 = 0$).

Before we come to the comparison of the representations (1.1) and (1.2), let us make a little excursion to the *Moment Problem* for the compact semi-algebraic set $K = S(p_1, \ldots, p_m)$.

Let $L : \mathbb{R}[X] \to \mathbb{R}$ be a linear functional. We want to know when there exists a non-negative Borel-measure μ on K such that for all $q \in \mathbb{R}[X]$,

$$L(q) = \int_K q \, d\mu.$$

By a theorem of Haviland (see [H]) this is true if and only if $L(q) \ge 0$ for all polynomials q such that $q \ge 0$ on K. The following corollary is a contribution to the solution of the K-Moment Problem.

Corollary 4.2 *Assume that $K = S(p_1, \ldots, p_m)$ is compact and that for every $a \in \mathbb{R}^n \setminus \{0\}$, at least on of $p_1^*(a), \ldots, p_m^*(a)$ is negative, e.g., if all p_i are linear. Then a linear functional $L : \mathbb{R}[X] \to \mathbb{R}$ comes from some non-negative Borel-measure on K if and only if for all $q \in \mathbb{R}[X]$,*

$$L(q^2) \ge 0, \quad L(q^2 p_i) \ge 0 \ (1 \le i \le m), \quad L(q^2 p_i p_j) \ge 0 \ (1 \le i < j \le m).$$

If all degrees of the $p_1, \ldots, p_m$ are even or if all are odd, the third condition is not needed.

Proof: Let $q \in \mathbb{R}[X]$ be non-negative on K. We then have to show that $L(q) \geq 0$. For every $\epsilon > 0$, $q+\epsilon$ is actually positive on K. Thus we get a representation (4.2), or even a representation (1.2) if all degrees of the p_i's are even or all are odd. Our assumption then yields $L(q+\epsilon) \geq 0$. By continuity of L we conclude $L(q) \geq 0$. □

In the final theorem of this paper we return to the situation of Section 3, i.e. A is an affine algebra $\mathbb{R}[x] = \mathbb{R}[x_1, \ldots, x_n] = \mathbb{R}[X_1, \ldots, X_n]/\mathcal{I}$ where $\mathcal{I}$ is any ideal of $\mathbb{R}[X_1, \ldots, X_n]$, and $S(p_1, \ldots, p_m) = \{a \in V(\mathcal{I}) \mid p_1(a) \geq 0, \ldots, p_m(a) \geq 0\}$. In Example 4.5 below we shall show that a 'linear' representation (1.2) is not always possible for $p \in \mathbb{R}[x]$, strictly positive on $S(p_1, \ldots, p_m)$. Not even a 'quadratic' representation (4.2) is possible in general. However, all products in (1.1) are *never* needed (except for $m = 1$).

Theorem 4.3 *Let $\mathbb{R}[x]$ be as above and assume that $K = S(p_1, \ldots, p_m)$ is compact and $m \geq 2$. Then there exists a subsequence $1, q_1, \ldots, q_l$ with $l = 2^{m-1}$, including $1, p_1, \ldots, p_m$, of the sequence of all products $p_1^{\nu_1} \cdots p_m^{\nu_m}$, $(\nu_1, \ldots, \nu_m) \in \{0,1\}^m$, such that every $p \in \mathbb{R}[x]$, strictly positive on K, has a representation*

$$p = \sigma_1 q_1 + \cdots + \sigma_l q_l \tag{4.3}$$

with $\sigma_i \in \sum \mathbb{R}[x]^2$. In particular, if $m = 2$, a representation (1.2) is always possible.

Proof: Let $A = \mathbb{R}[x]$ and choose $N \in \mathbb{N}$ such that $N^2 - (x_1^2 + \cdots + x_i^2) > 0$ on K. Next let us order the products $p_1^{\nu_1} \cdots p_m^{\nu_m}$ in a canonical way by taking first 1 then all linear factors $p_1, \ldots, p_m$, followed by all two-fold products $p_1p_2, \ldots, p_1p_m, p_2p_3, \ldots, p_2p_m, \ldots, p_{m-1}p_m$, and so on. Let $l = 2^{m-1}$ and denote the first $l+1$ terms of this sequence by $1, q_1, \ldots, q_l$. We then shall apply Theorem 3.2 to the sequence $q_1, \ldots, q_l$.

In order to do so let $\mathfrak{P}$ be a real prime ideal of A and let $F = \mathrm{ff}(\overline{A})$ with $\overline{A} = A/\mathfrak{P}$. For a fixed ordering P of F we know from the Tarski-Principle (see [Pr], Corollary 5.3) that the sentence

$$\forall\, v\ (p_1(v) \geq 0 \wedge \cdots \wedge p_m(v) \geq 0 \rightarrow N^2 - (v_1^2 + \cdots + v_n^2) > 0),$$

true over $\mathbb{R}$, also holds in the real closure of F w.r.t. P. Thus if $\overline{p}_1, \ldots, \overline{p}_m \in P$, we get that $-\overline{f} := -(N^2 - (\overline{x}_1^2 + \cdots + \overline{x}_i^2)) \notin P$. This, however, tells us that the form

$$\langle 1, -\overline{f}, \overline{p}_1, \ldots, \overline{p}_m \rangle^\star \quad \text{is indefinite} \tag{4.4}$$

w.r.t. all orderings of F.

According to Theorem 3.2 we have to check the heselisations $H = (F, v)^h$ w.r.t. every valuation v of F such that its residue class field is formally real and

$v(\overline{x}_i) < 0$ for some $i \leq m$. Since every ordering P of H is compatible with v (see [Pr], Theorem 8.3), we obtain from $v(\overline{x}_i) < 0$ that $-\overline{f}$ is positive w.r.t. P. Hence the form

$$\langle 1, \overline{p}_1, \ldots, \overline{p}_m \rangle^\star$$

is already indefinite w.r.t. every ordering of H. By Pfister's Local-Global-Principle for torsion forms (see [L], Theorem 8.3) we obtain that the so-called Pfisterform

$$\langle\langle\, \overline{p}_1, \ldots, \overline{p}_m \rangle\rangle^\star$$

is torsion in the Wittring of H, i.e., for some $r \in \mathbb{N}$, the form $r \cdot \langle\langle\, \overline{p}_1, \ldots, \overline{p}_m \rangle\rangle^\star$ is isometric to an orthogonal sum of hyperbolic forms $\langle \alpha, -\alpha \rangle$ where we can choose the $\alpha \in H \setminus \{0\}$ at our disposal. A little combinatorial argument shows that by the special choice of the sequence $1, q_1, \ldots, q_l$, it is possible to choose for every non-zero product $\alpha = \overline{p}_1^{\nu_1} \cdots \overline{p}_m^{\nu_m}$, not contained in the sequence $1, \overline{q}_1, \ldots, \overline{q}_l$ a hyperbolic plane $\langle \alpha, -\alpha \rangle$ in the decomposition of $r \cdot \langle\langle\, \overline{p}_1, \ldots, \overline{p}_m \rangle\rangle^\star$. By Witt's cancellation law we eventually find that the form

$$\langle 1, \overline{q}_1, \ldots, \overline{q}_l \rangle^\star$$

is weakly isotropic in H. Thus the conditions of Theorem 3.2 are satisfied and hence every $p \in \mathbb{R}[x]$, strictly positive on K, has a representation (4.3). □

By using the same arguments as in the proof of Corollary 4.2, Theorem 4.3 leads to a strengthening of Schmüdgen's solution to the Moment Problem:

Corollary 4.4 *Assume that $K = S(p_1, \ldots, p_m)$ is compact and let $1, q_1, \ldots, q_l$ be a subsequence as guaranteed by Theorem 4.3. Then a linear functional $L : \mathbb{R}[X] \to \mathbb{R}$ comes from some non-negative Borel-measure on K if and only if for all $p \in \mathbb{R}[X]$,*

$$L(p^2) \geq 0, \quad L(p^2 q_i) \geq 0 \ (1 \leq i \leq l).$$

The following example shows that for $n \geq 2$ and $m \geq 3$ a representation (1.2) need not exist in general for $N^2 - (x_1^2 + \cdots + x_n^2) > 0$ on K and K compact. It is easily checked that e.g. for $n = 2$ and $m = 3$, no sequence $1, q_1, q_2, q_3$ of $4 = 2^{m-1}$ products suffices to get a representation (4.3) for every $p \in \mathbb{R}[X_1, X_2]$, strictly positive on K. Thus the length $1 + 2^{m-1}$ in Theorem 4.3 is best possible.

Example 4.5 Let $n \geq 2$ and $m = n + 1$. We consider the polynomial ring $A = \mathbb{R}[X_1, \ldots, X_n]$ and choose $p_i := X_i - \frac{1}{2}$ $(1 \leq i \leq n)$ and $p_m := 1 - \prod_1^n X_i$. The region $K = S(p_1, \ldots, p_m)$ is compact. We then define a semi-ordering S on A as follows. First we order the n-tuples $(\nu_1, \ldots, \nu_n) \in \mathbb{N}^n$ lexicographically from left to right. This induces a linear order on the monomiales $X^\nu = X_1^{\nu_1} \cdots X_n^{\nu_n}$

and hence gives the possibility to write every $q \in \mathbb{R}[X]$ in a unique way starting with the highest monomial:

$$q = a(q)X^{\nu(q)} + \cdots, \quad a(q) \in \mathbb{R} \setminus \{0\}.$$

We then define $S \subset \mathbb{R}[X]$ to contain 0 and those $q \in \mathbb{R}[X] \setminus \{0\}$ such that

$$\begin{array}{lclll} \nu(q) & \not\equiv & (1,\ldots,1) \mod 2 & \text{and} & a(q) > 0, \text{ or} \\ \nu(q) & \equiv & (1,\ldots,1) \mod 2 & \text{and} & a(q) < 0. \end{array}$$

One easily checks that S is a semi-ordering. Moreover, all products $p_1^{\nu_1} \cdots p_n^{\nu_n}$ with $(\nu_1,\ldots,\nu_n) \not\equiv (1,\ldots,1) \mod 2$ belong to S as well as p_m. However, $N^2 - (X_1^2 + \cdots + X_n^2) \notin S$.

The 'first' counterexample to a representation (1.2) for $N^2 - (X_1^2 + \cdots + X_n^2) > 0$ on $S(p_1,\ldots,p_m)$, thus comes for $r = 2$ and $m = 3$. From Theorem 4.3 we know that for $m \leq 2$ there can be no such example. Thus it remains to look at the case $n = 1$. This case is treated by our last remark.

Remark 4.6 *Let $A = \mathbb{R}[x_1,\ldots,x_1]$ formally real with $\mathrm{trdeg}_{\mathbb{R}}(A) = 1$. Then every $p \in A$, strictly positive on a compact set $S(p_1,\ldots,p_m)$, has a representation (1.2).*

This follows from (4.4) in the proof of Theorem 4.3 simply by the fact that every formally real field $F = \mathrm{ff}(A/\mathfrak{P})$ is SAP (see [Pr], Theorem 9.4), i.e., every quadratic form which is indefinite w.r.t. all orderings of F is already weakly isotropic. Knowing that $\langle 1, -\overline{f}, \overline{p}_1, \ldots, \overline{p}_m\rangle^\star$ is weakly isotropic in F for $f = N^2 - (x_1^2 + \cdots + x_n^2)$, we may then apply Lemma 2.2, Lemma 3.1 and Putinar's Theorem.

The next example shows that in Theorem 3.2 (and in Lemma 2.2) the conditions for $\mathfrak{P} \neq \{0\}$ are actually needed and that the choice of the sequence $1, q_1, \ldots, q_l$ in Theorem 4.3 is essential.

Example 4.7 We consider the polynomial ring $A = \mathbb{R}[X_1, X_2, X_3]$ and let $p_1 = X_1 - \frac{1}{2}$, $p_2 = X_2 - \frac{1}{2}$, $p_3 = 1 - X_1X_2$, $p_4 = 1 - X_3^2$, and $f = N^2 - (X_1^2 + X_2^2 + X_3^2)$. Clearly, the region $S(p_1, p_2, p_3, p_4)$ is compact. As we saw in Example 4.5, the form $\langle 1, (X_1^2 + X_2^2) - N^2, p_1, p_2, p_3\rangle$ is not weakly isotropic in $\mathbb{R}(X_1, X_2)$ for $N \in \mathbb{N}$ big enough. Thus the form $(\overline{\varrho})^\star$ with

$$\varrho = \langle 1, -f, p_1, p_2, p_3, p_4, p_1p_4, p_2p_4, p_3p_4, p_1p_2p_4, p_1p_3p_4, p_2p_3p_4, p_1p_2p_3p_4\rangle$$

is not weakly isotropic in $F = \mathrm{ff}(A/\mathfrak{P})$ with $\mathfrak{P} = (X_3 - 1)A$. In $F = \mathrm{ff}(A)$, however, ϱ is weakly isotropic. This follows from the arguments in the proof of Theorem 4.3.

Let us mention at the end of this paper that our result can be improved in two ways. First we may replace the field of coefficients $\mathbb{R}$ by a subfield K of $\mathbb{R}$ with the induced archimedean positive cone K_+ of non-negative elements of K. We then consider $S(p_1, \ldots, p_m)$ with $p_i \in K[x] = K[X_1, \ldots, X_n]/\mathcal{I}$ where $\mathcal{I}$ is a any ideal of $K[X_1, \ldots, X_n]$. Now the σ_i in (1.1), (1.2), and so on have to be taken from the preordering $\sum K_+K[x]^2$. Next we may replace the exponent 2 by $2r$ where r is any natural number ≥ 1. If we do so, the σ_i in (1.1), (1.2), and so on have now to be taken from the preordering $\sum K_+K[x]^{2r}$ of level $2r$. For more details the reader is referred to the first author's thesis [J2].

References

[B-S] E. Becker and N. Schwartz: *Zum Darstellungssatz von Kadison-Dubois*, Archiv der Mathematik Vol 40 (1983), 421-428

[Be-W] R. Berr and T. Wörmann: *Positive polynomials and tame preorderings*, Preprint (1998)

[Br] L. Bröcker: *Zur Theorie der quadratischen Formen über formal reellen Körpern*, Mathematische Annalen 210 (1974), 233-256

[H] E. K. Haviland: *On the Momentum Problem for Distribution Functions in more than one Dimension II*, American Journal of Mathematics 58 (1936), 164-168

[J1] T. Jacobi: *A representation theorem for certain partially ordered commutative rings*, to appear in Mathematische Zeitschrift

[J2] T. Jacobi: *Über die Darstellung positiver Polynome auf semi-algebraischen Kompakta*, Dissertation an der Universität Konstanz (1999)

[L] T. Y. Lam: *The Algebraic Theory of Quadratic Forms* Mathematics lecture note series (1973), W. A. Benjamin

[Pr] A. Prestel: *Lectures on Formally Real Fields*, Lecture Notes in Mathematics 1093 (1984), Springer

[Pu] M. Putinar: *Positiv Polynomials on Compact Semi-Algebraic Sets*, Ind. Univ. Math. J. 42/3 (1993), 969-984

[Scha] W. Scharlau: *Quadratic and Hermitian Forms*, Grundlehren der mathematischen Wissenschaften 270 (1985), Springer

[Sch] K. Schmüdgen: *The K-Moment Problem for Compact Semi-Algebraic Sets*, Mathematische Annalen 289 (1991), 203-206

[W] T. Wörmann: *Strikt positive Polynome in der semialgebraischen Geometrie*, Dissertation an der Universität Dortmund (1998)

Thomas Jacobi – Prof. Dr. Alexander Prestel
Universität Konstanz
Fakultät für Mathematik und Informatik
D-78434 Konstanz

E-mail: jacobi@fmi.uni-konstanz.de – alex.prestel@uni-konstanz.de