Canad. Math. Bull. Vol. **46** (3), 2003 pp. 400–418

Approximating Positive Polynomials Using Sums of Squares

M. Marshall

Abstract. The paper considers the relationship between positive polynomials, sums of squares and the multi-dimensional moment problem in the general context of basic closed semi-algebraic sets in real n-space. The emphasis is on the non-compact case and on quadratic module representations as opposed to quadratic preordering presentations. The paper clarifies the relationship between known results on the algebraic side and on the functional-analytic side and extends these results in a variety of ways.

1 Introduction

Denote the polynomial ring $\mathbb{R}[X_1, \ldots, X_n]$ by $\mathbb{R}[X]$ for short. For any (not necessarily finite) subset S of $\mathbb{R}[X]$, let

$$\mathcal{X}_S = \{t \in \mathbb{R}^n \mid g(t) \geq 0 \text{ for all } g \in S\}, \quad \tilde{T}_S = \{f \in \mathbb{R}[X] \mid f \geq 0 \text{ on } \mathcal{X}_S\},$$

and let M_S denote the quadratic module in $\mathbb{R}[X]$ generated by S, *i.e.*, the set of finite sums of the form $t + \sum t_i g_i$, $g_i \in S$, t, t_i sums of squares in $\mathbb{R}[X]$.

According to a result of Haviland [4] [5], a linear functional $L\colon \mathbb{R}[X] \to \mathbb{R}$ which is non-negative on $\tilde{T}_S$ comes from a positive Borel measure μ on $\mathcal{X}_S$ in the sense that $\forall f \in \mathbb{R}[X]$, $L(f) = \int_{\mathcal{X}_S} f \, d\mu$. It is natural to ask if the same is true for any linear functional $L\colon \mathbb{R}[X] \to \mathbb{R}$ which is non-negative on M_S. This is the *Moment Problem* for the quadratic module M_S. The most interesting case seems to be when S is finite. A sufficient condition for it to be true is that each $f \in \tilde{T}_S$ can be approximated by elements of M_S in the sense that there exists an element $q \in \mathbb{R}[X]$ such that, for all rational $\epsilon > 0$, $f + \epsilon q \in M_S$ (since then $L(f) + \epsilon L(q) = L(f + \epsilon q) \geq 0$ for each rational $\epsilon > 0$ so $L(f) \geq 0$). In this paper we examine cases where such approximation is possible.

Additional motivation for studying this sort of approximation comes from the recent work of Parrilo and Sturmfels [13] which compares various methods for minimizing a given polynomial function. The results in [13] raise the possibility of applying approximation results of the type considered in the present paper to develop efficient algorithms to compute such minimum values.

The present paper is a continuation of joint work of S. Kuhlmann and the author in [9]. In [9] this same approximation question is considered (in the case where S is finite) but mainly in the easier case where the quadratic module M_S is replaced by

Received by the editors October 9, 2001.
This research was supported in part by NSERC of Canada.
AMS subject classification: 14P10, 44A60.

T_S, the quadratic preordering generated by S. In the present paper it is explained how various results proved in [9] and [10] extend to the quadratic module case. This involves using Jacobi's extension of the Kadison-Dubois theorem given in [6] to prove a variant of [10, Theorem 2.2], and also it involves generalizing the Jacobi-Prestel criterion given in [7, Theorem 3.2]. Another major feature of the present work is that it clarifies the relationship between the algebraic results in [9] and [10] and the analytic results of Putinar and Vasilescu in [17] and also that it extends many of the results in [17].

The author acknowledges the contribution of Salma Kuhlmann to the present work.

2 Approximation Theorems for Quadratic Modules

Let A be a commutative ring with 1. For simplicity assume $\mathbb{Q} \subseteq A$. By a *quadratic module* in A we mean a subset M of A satisfying $1 \in M$, $M + M \subseteq M$ and $a^2M \subseteq M$ for each $a \in A$. A *quadratic preordering* in A is a quadratic module in A which is also closed under multiplication. A quadratic module M in A is said to be *archimedean* if for each $a \in A$ there exists an integer k such that $k - a \in M$.

We denote by $\sum A^2$ the set of all finite sums $\sum a_i^2$, $a_i \in A$. $\sum A^2$ is the unique smallest quadratic module in A. $\sum A^2$ is closed under multiplication, so $\sum A^2$ is also the unique smallest quadratic preordering in A. The quadratic module in A generated by a subset S of A consists of all finite sums of the form $a = t + \sum t_i g_i$, $t, t_i \in \sum A^2$, $g_i \in S$. We denote this quadratic module by M_S. The quadratic preordering in A generated by S coincides with the quadratic module in A generated by the set of all finite products of elements of S. We denote this quadratic preordering by T_S.

For any subset S of A, $\mathcal{X}_S$ denotes the set of all ring homomorphisms $\alpha\colon A \to \mathbb{R}$ such that $\alpha(s) \geq 0$ for all $s \in S$. For $a \in A$, $\hat{a}\colon \mathcal{X}_S \to \mathbb{R}$ is defined by $\hat{a}(\alpha) = \alpha(a)$. $\mathcal{X}_S$ is given the weakest topology such that the functions $\hat{a}$, $a \in A$ are continuous. The mapping $a \mapsto \hat{a}$ defines a ring homomorphism from A into $C(\mathcal{X}_S)$, the ring of all continuous functions $f\colon \mathcal{X}_S \to \mathbb{R}$. We denote by $\tilde{T}_S$ the set of all $a \in A$ such that $\hat{a} \geq 0$ on $\mathcal{X}_S$ (*i.e.*, $\alpha(a) \geq 0$ for all $\alpha \in \mathcal{X}_S$). $\tilde{T}_S$ is a quadratic preordering in A containing S so $T_S \subseteq \tilde{T}_S$.

Note: (1) If $M = M_S$, $T = T_S$ and $\tilde{T} = \tilde{T}_S$ then $S \subseteq M \subseteq T \subseteq \tilde{T}$ and $\mathcal{X}_S = \mathcal{X}_M = \mathcal{X}_T = \mathcal{X}_{\tilde{T}}$.

(2) If A is the polynomial ring $\mathbb{R}[X] := \mathbb{R}[X_1, \ldots, X_n]$ then ring homomorphisms from A to $\mathbb{R}$ correspond to point evaluations $f \mapsto f(t)$, $t \in \mathbb{R}^n$, $\mathcal{X}_S$ is identified (as a topological space) with the set $\mathcal{X}_S = \{t \in \mathbb{R}^n \mid g(t) \geq 0 \text{ for all } g \in S\}$ defined earlier and $\tilde{T}_S$ is equal to the quadratic preordering $\tilde{T}_S = \{f \in \mathbb{R}[X] \mid f \geq 0 \text{ on } \mathcal{X}_S\}$ defined earlier.

(3) If M is a quadratic module in A which is archimedean then, for each $a \in A$, there exists an integer $k_a \geq 1$ such that $k_a - a, k_a + a \in M$ (so $|\hat{a}| \leq k_a$ on $\mathcal{X}_M$). Thus $\mathcal{X}_M$ is identified with a (closed) subspace of the product space $\prod_{a \in A}[-k_a, k_a]$, so $\mathcal{X}_M$ is compact. The converse is false in general.[1]

[1]The status of the converse in examined in detail in [7] in the important special case where A is a finitely generated $\mathbb{R}$-algebra and the quadratic module M is finitely generated.

https://doi.org/10.4153/CMB-2003-041-9 Published online by Cambridge University Press

We record the following special case of the representation theorem of Jacobi [6].

Theorem 2.1 *Suppose M is an archimedean quadratic module in A. Then, for $a \in A$, the following are equivalent:*

(1) $\hat{a} \geq 0$ *on* $\mathcal{X}_M$ *(i.e.,* $\alpha(a) \geq 0$ *for all* $\alpha \in \mathcal{X}_M$*).*
(2) $a + \epsilon \in M$ *holds for all rational* $\epsilon > 0$.

Note: For any element $a \in A$, (1) is a 'geometric' condition on a. (2) is an 'arithmetic' condition on a. The implication (2) $\Rightarrow$ (1) is trivial. The implication (1) $\Rightarrow$ (2) is non-trivial.

See [12] for an extension of Jacobi's result in [6]. For readers unfamiliar with the results in [6] and [12], an easy access to a proof of Theorem 2.1 can be found in [11, pages 41–43]. The result in [11], although not the most general, covers as special cases the case of archimedean quadratic modules and also the case of modules over archimedean preprimes, the result in the latter case being what is commonly referred to as the Kadison-Dubois Theorem.

We also use the following self-strengthening of Theorem 2.1:

Theorem 2.2 *Suppose M is a quadratic module in A and $p \in A$ is a unit such that $p - 1 \in M$ and, for all $a \in A$, there exist integers $k, \ell \geq 0$ such that $kp^\ell - a \in M$. Then, for any $a \in A$, the following are equivalent:*

(1) $\hat{a} \geq 0$ *on* $\mathcal{X}_M$.
(2) *There exists an integer* $k \geq 0$ *such that, for all rational* $\epsilon > 0$, $a + \epsilon p^k \in M$.

Note: Theorem 2.2 includes Theorem 2.1 as a special case, taking $p = 1$.

In practice, we will be applying Theorem 2.2 (and also Corollary 3.4 below) in the case where $p \in A$ is not a unit. This will be accomplished by going to the ring

$$A[1/p] := \{a/p^k \mid a \in A, k \geq 0\},$$

the localization of A at the multiplicative set $\{p^k \mid k \geq 0\}$, and

$$M[1/p^2] := \{a/p^{2k} \mid a \in M, k \geq 0\},$$

the quadratic module in $A[1/p]$ generated by M.

We examine the condition $p - 1 \in A$ a bit: If $p - 1 \in M$ then it follows that $p^2 - p = (p-1)^2 + (p-1) \in M$ and, multiplying each of $p - 1$, $p^2 - p$ by even powers of p, that $p^k - p^{k-1} \in M$ for all integers $k \geq 1$. It follows that the set $\{kp^\ell \mid k, \ell \text{ are integers} \geq 0\}$ is cofinal in the subring $\mathbb{Z}[p]$ of A with respect to the partial ordering associated to M. Thus, in the presence of the condition $p - 1 \in M$, the remainder of the hypothesis of Theorem 2.2 (that for each $a \in A$, there exist integers $k, \ell \geq 0$ such that $kp^\ell - a \in M$) is equivalent to the hypothesis that $\mathbb{Z}[p]$ is cofinal in A with respect to the partial ordering associated to M.

The proof of Theorem 2.2 follows exactly along the lines of the proof of a similar result for preprimes in [10, Theorem 2.2]. For the convenience of the reader we give a complete proof.

https://doi.org/10.4153/CMB-2003-041-9 Published online by Cambridge University Press

Proof The implication (2) $\Rightarrow$ (1) is trivial. Suppose there exists $\ell \geq 0$ such that for all rational $\epsilon > 0$, $a + \epsilon p^\ell \in M$. Then, for any $\alpha \in \mathcal{X}_M$, $\alpha(a) + \epsilon\alpha(p)^\ell \geq 0$, so $\alpha(a) \geq 0$.

(1) $\Rightarrow$ (2). Let

$$B = \{f \in A \mid \exists \text{ a positive integer } k \text{ such that } k + f, k - f \in M\}.$$

B is a subring of A [11, Proposition 3.3.3 (2)] and the quadratic module M' in B defined by $M' = M \cap B$ is obviously archimedean. Also, $1 - 1/p = (p^2 - p)/p^2$ and $1 + 1/p = (p^2 + p)/p^2$ both belong to M so $1/p \in B$. If $a \in A$ then $kp^j - a \in M$ and $kp^j + a \in M$ for some integers $j \geq 0, k \geq 1$. Replacing j by $j + 1$ if necessary, we can assume j is even, *i.e.*, $kp^{2\ell} - a, kp^{2\ell} + a \in M$ for some integer $\ell \geq 0$. It follows that, for each $a \in A$, $a/p^{2\ell} \in B$ for some integer $\ell \geq 0$. This implies that $A = B[p]$ (the localization of B at the multiplicative set in B consisting of all $1/p^i$, $i \geq 0$). Thus a ring homomorphism $\alpha\colon B \to \mathbb{R}$ lifts to a ring homomorphism $\alpha\colon A \to \mathbb{R}$ iff $\alpha(1/p) \neq 0$ and, in this case, the extension is unique. Moreover, if $\alpha \in \mathcal{X}_{M'}$. Suppose now that $\alpha(a) \geq 0$ holds for all $\alpha \in \mathcal{X}_M$. Then, for each $\alpha \in \mathcal{X}_{M'}$, either $\alpha(1/p) = 0$, so $\alpha(a/p^{2\ell+2}) = \alpha(a/p^{2\ell})\alpha(1/p)^2 = 0$, or $\alpha(1/p) > 0$ and, extending α, $\alpha(a/p^{2\ell+2})\alpha(p)^{2\ell+2} = \alpha(a) \geq 0$, so $\alpha(a/p^{2\ell+2}) \geq 0$. Thus $\alpha(a/p^{2\ell+2}) \geq 0$ holds in all cases so, by Theorem 2.1, $a/p^{2\ell+2} + \epsilon \in M'$ holds for all rational $\epsilon > 0$. Clearing fractions, this yields $a + \epsilon p^{2\ell+2} \in M$. ∎

Since Theorem 2.1 generalizes to the case where M is an archimedean module with respect to weakly torsion preprime [12], it is natural to wonder if Theorem 2.2 generalizes in some similar fashion.

3 Representation of Positive Linear Functionals

The results of the previous section have application to the Moment Problem described in the introduction. To see this application, we begin by giving a general criterion for the representability of a positive linear functional as an integral.

Theorem 3.1 *Suppose A is an $\mathbb{R}$-algebra, $\mathcal{X}$ a Hausdorff space and $\hat{}\colon A \to C(\mathcal{X})$ is an $\mathbb{R}$-algebra homomorphism. Suppose there exists $p \in A$ such that $\hat{p} \geq 0$ on $\mathcal{X}$ and, for each integer $n \geq 1$, the set $\mathcal{X}_n := \{\alpha \in \mathcal{X} \mid \hat{p}(\alpha) \leq n\}$ is compact. Then, for any linear function $L\colon A \to \mathbb{R}$ satisfying $\forall a \in A$, $\hat{a} \geq 0$ on $\mathcal{X} \Rightarrow L(a) \geq 0$, there exists a positive Borel measure[2] μ on $\mathcal{X}$ such that, $\forall a \in A$,*

$$L(a) = \int_{\mathcal{X}} \hat{a}\, d\mu.$$

Theorem 3.1 applies in a variety of cases. It applies, for example, in the case where $\mathcal{X}$ is a closed subset of $\mathbb{R}^n$ and A is a subalgebra of $C(\mathcal{X})$ containing the projections $t \mapsto t_i$, $i = 1, \ldots, n$, taking $p(t) = t_1^2 + \cdots + t_n^2$. In particular, Theorem 3.1 extends the result of Haviland in [4] [5].

[2] By Borel measure, we always mean regular Borel measure.

https://doi.org/10.4153/CMB-2003-041-9 Published online by Cambridge University Press

It is possible to deduce Theorem 3.1 from Choquet's theorem [3, Theorem 34.6]. Rather than attempt to explain how this is done, we prefer to give a direct proof.

Proof For $\alpha \in \mathcal{X}$, $\mathcal{X}_n$ is a neighborhood of α for n sufficiently large, so $\mathcal{X}$ is locally compact. Denote by $C'(\mathcal{X})$ the algebra of all continuous functions $f\colon \mathcal{X} \to \mathbb{R}$ which are bounded by some $\hat{a}$, $a \in A$ in the sense that there exists $a \in A$ such that $|f| \leq \hat{a}$ on $\mathcal{X}$. We begin by proving the existence of a positive linear functional $\bar{L}\colon C'(\mathcal{X}) \to \mathbb{R}$ such that $\bar{L}(\hat{a}) = L(a)$ for all $a \in A$. Let $A_0 = \{\hat{a} \mid a \in A\}$. If $\hat{a} = 0$ on $\mathcal{X}$ then, by our hypothesis, $L(a) = 0$. Thus we have a well-defined linear map $\bar{L}\colon A_0 \to \mathbb{R}$ given by $\bar{L}(\hat{a}) = L(a)$. Use Zorn's lemma to pick a pair $(V, \bar{L})$ where V is a subspace of $C'(\mathcal{X})$ containing A_0 and $\bar{L}$ is an extension of $\bar{L}$ to V maximal with the property that

$$\forall f \in V,\ f \geq 0 \quad \text{on } \mathcal{X} \Rightarrow \bar{L}(f) \geq 0.$$

We claim that $V = C'(\mathcal{X})$. Otherwise, we have some $g \in C'(\mathcal{X})$, $g \notin V$. If $f_1, f_2 \in V$ are such that $f_1 \leq g$, $g \leq f_2$ on $\mathcal{X}$ so $\bar{L}(f_1) \leq \bar{L}(f_2)$. Such f_1, f_2 exist, *e.g.*, pick $f_1 = -\hat{a}$, $f_2 = \hat{a}$ where $a \in A$ is such that $\hat{a} \geq |g|$. Thus there exists a real number e such that

$$\sup\{\bar{L}(f_1) \mid f_1 \in V, f_1 \leq g\} \leq e \leq \inf\{\bar{L}(f_2) \mid f_2 \in V, f_2 \geq g\}.$$

Then $\bar{L}$ extends to $V' = V + \mathbb{R}g$ via $\bar{L}(f + dg) = \bar{L}(f) + de$, a contradiction.

$C'(\mathcal{X})$ contains all continuous functions with compact support so, by the Riesz representation theorem [8, page 77], we have a unique positive Borel measure μ on $\mathcal{X}$ such that $\bar{L}(f) = \int_{\mathcal{X}} f\, d\mu$ holds for all continuous f with compact support. It remains to show that this is true for any f in $C'(\mathcal{X})$. Suppose $f \in C'(\mathcal{X})$ is given. Decomposing f as $f = f_+ - f_-$, $f_+ = (|f| + f)/2$, $f_- = (|f| - f)/2$, we can assume $f \geq 0$. Take $q = f + \hat{p}$ and, for each integer $n \geq 1$, set $\mathcal{X}'_n = \{\alpha \in \mathcal{X} \mid q(\alpha) \leq n\}$. $\mathcal{X}'_n$ is closed and $\mathcal{X}'_n \subseteq \mathcal{X}_n$ so $\mathcal{X}'_n$ is compact. Obviously $\mathcal{X}'_i \subseteq \mathcal{X}'_{i+1}$ and $\bigcup_{i\geq 1} \mathcal{X}'_i = \mathcal{X}$. Using Urysohn's lemma, we have continuous functions f_i with $0 \leq f_i \leq f$, $f_i = f$ on $\mathcal{X}'_i$, $f_i = 0$ off $\mathcal{X}'_{i+1}$. Since $q > i$ off $\mathcal{X}'_i$ we see that $q^2/i \geq f - f_i \geq 0$ on $\mathcal{X}$, so $\bar{L}(q^2)/i \geq \bar{L}(f) - \bar{L}(f_i) \geq 0$. This proves $\bar{L}(f) = \lim_{i\to\infty} \bar{L}(f_i)$ which in turn implies that

$$\int_{\mathcal{X}} f\, d\mu = \lim_{i\to\infty} \int_{\mathcal{X}} f_i\, d\mu = \lim_{i\to\infty} \bar{L}(f_i) = \bar{L}(f). \qquad \blacksquare$$

Corollary 3.2 *Assume the hypothesis of Theorem 3.1 holds and M is a quadratic module in A such that, for each $a \in A$, $\hat{a} \geq 0$ on $\mathcal{X} \Rightarrow$ there exists an element $q \in A$ such that $a + \epsilon q \in M$ for all rational $\epsilon > 0$. Then, for any linear function $L\colon A \to \mathbb{R}$ satisfying $L(M) \geq 0$, there exists a positive Borel measure μ on $\mathcal{X}$ such that $\forall a \in A$, $L(a) = \int_{\mathcal{X}} \hat{a}\, d\mu$.*

Proof Suppose $a \in A$ is such that $\hat{a} \geq 0$ on $\mathcal{X}$. By hypothesis, there exists $q \in A$ such that, for all real $\epsilon > 0$, $a + \epsilon q \in M$ (so $L(a) + \epsilon L(q) = L(a + \epsilon q) \geq 0$). It follows that $L(a) \geq 0$ for any such a, so the result follows from Theorem 3.1. $\blacksquare$

https://doi.org/10.4153/CMB-2003-041-9 Published online by Cambridge University Press

Combining Theorem 3.1 with the results in Section 2 yields additional corollaries:

Corollary 3.3 *Suppose A is an $\mathbb{R}$-algebra and M is a quadratic module in A which is archimedean. Then, for any linear function $L\colon A \to \mathbb{R}$ satisfying $L(M) \geq 0$, there exists a positive Borel measure μ on $\mathcal{X}_M$ such that $\forall a \in A$, $L(a) = \int_{\mathcal{X}_M} \hat{a}\, d\mu$.*

Corollary 3.4 *Suppose A is an $\mathbb{R}$-algebra, M is a quadratic module in A and $p \in A$ is a unit such that $p - 1 \in M$ and, for all $a \in A$, there exist integers $k, \ell \geq 0$ such that $kp^\ell - a \in M$. Then, for any linear function $L\colon A \to \mathbb{R}$ satisfying $L(M) \geq 0$, there exists a positive Borel measure μ on $\mathcal{X}_M$ such that $\forall a \in A$, $L(a) = \int_{\mathcal{X}_M} \hat{a}\, d\mu$.*

Proof Corollary 3.3 follows from Corollary 3.4, taking $p = 1$, so it suffices to prove Corollary 3.4. Let $\mathcal{X}_n = \{\alpha \in \mathcal{X}_M \mid \hat{p}(\alpha) \leq n\}$. If $a \in A$ there exist integers $k_a \geq 1$, $\ell_a \geq 0$ such that $k_a p^{\ell_a} \pm a \in M$. Then $|\hat{a}| \leq k_a \hat{p}^{\ell_a}$, so $|\hat{a}| \leq k_a n^{\ell_a}$ on $\mathcal{X}_n$. It follows that $\mathcal{X}_n$ is identified with a (closed) subspace of $\prod_{a\in A}[-k_a n^{\ell_a}, k_a n^{\ell_a}]$, so $\mathcal{X}_n$ is compact. Thus Theorem 3.1 applies. Suppose $a \in A$ is such that $\hat{a} \geq 0$ on $\mathcal{X}_M$. By Theorem 2.2, there exists an integer $k \geq 0$ such that, for all real $\epsilon > 0$, $a + \epsilon p^k \in M$ (so $L(a) + \epsilon L(p^k) = L(a + \epsilon p^k) \geq 0$). It follows that $L(a) \geq 0$ for all such a, so the result follows from Theorem 3.1. ∎

Remark 3.5 The positive Borel measures obtained in Corollary 3.3 and Corollary 3.4 are unique. It suffices to prove this in the case of Corollary 3.4. The corresponding result for Corollary 3.3 then follows, taking $p = 1$. Let $f \in C'(\mathcal{X}_M)$, say $|f| \leq k\hat{p}^\ell$ on $\mathcal{X}_M$. Define B and M' as in the proof of Theorem 2.2. Consider $g\colon \mathcal{X}_{M'} \to \mathbb{R}$ defined by

$$g(\alpha) = \begin{cases} f(\alpha)/\hat{p}(\alpha)^{\ell+1} & \text{if } \alpha(1/p) \neq 0 \\ 0 & \text{if } \alpha(1/p) = 0. \end{cases}$$

It is clear that g is continuous so, by the Stone-Weierstrass theorem, there exists a sequence $\{b_i\}$ in B with $\{\hat{b}_i\}$ converging to g. Thus, for each rational $\epsilon > 0$, $\epsilon \pm (g - \hat{b}_i) \geq 0$ on $\mathcal{X}_{M'}$ for i sufficiently large, so $\epsilon\hat{p}^{\ell+1} \pm (f - \hat{a}_i) \geq 0$ on $\mathcal{X}_M$ for i sufficiently large, where $a_i := p^{\ell+1} b_i$. It follows that

$$\bar{L}(f) = \lim_{i\to\infty} \bar{L}(\hat{a}_i) = \lim_{i\to\infty} L(a_i).$$

Uniqueness follows using the version of the Riesz representation theorem [8, page 77] quoted earlier.

We also note the following:

Corollary 3.6 *Suppose A is an $\mathbb{R}$-algebra, M is a quadratic module in A, $p \in A$ is a unit such that $p - 1 \in M$ and, for all $a \in A$, there exist integers $k, \ell \geq 0$ such that $kp^\ell - a \in M$. Define B and M' as in the proof of Theorem 2.2. Then, for any linear function $L\colon B \to \mathbb{R}$ satisfying $L(M') \geq 0$, there exists a positive Borel measure η on $\mathcal{X}_{M'}$, a positive Borel measure μ on $\mathcal{X}_M$ and a positive Borel measure ν on $H = \{\alpha \in \mathcal{X}_{M'} \mid \alpha(1/p) = 0\}$ such that $\forall b \in B$,*

$$L(b) = \int_{\mathcal{X}_{M'}} \hat{b}\, d\eta = \int_{\mathcal{X}_M} \hat{b} \circ \Phi\, d\mu + \int_H \hat{b}\, d\nu,$$

https://doi.org/10.4153/CMB-2003-041-9 Published online by Cambridge University Press

where $\Phi\colon \mathcal{X}_M \to \mathcal{X}_{M'}$ *is the natural map.*

Proof The quadratic module M' in B is archimedean. We get η by applying Corollary 3.3 to M'. η induces positive Borel measures μ' and ν on $\Phi(\mathcal{X}_M)$ and H respectively and the integral splits into two parts: $\int_{\mathcal{X}_{M'}} \hat{b}\, d\eta = \int_{\Phi(\mathcal{X}_M)} \hat{b}\, d\mu' + \int_H \hat{b}\, d\nu$. Taking μ to be the positive Borel measure on $\mathcal{X}_M$ corresponding to μ' via the embedding Φ, this yields $L(b) = \int_{\mathcal{X}_{M'}} \hat{b}\, d\eta = \int_{\mathcal{X}_M} \hat{b} \circ \Phi\, d\mu + \int_H \hat{b}\, d\nu$. ∎

Later, in Example 8.1, we compute B and M' explicitly in the case where $A = \mathbb{R}[X][1/p]$, $p := 1 + \sum X_i^2$. Once this is done it will be clear that Corollary 3.6 extends the result of Putinar and Vasilescu in [17, Theorem 3.2].

4 Application to Finitely Generated Algebras

We consider the application of the results in Sections 2 and 3 to finitely generated algebras over $\mathbb{R}$. We assume that A is such an algebra. Each presentation $A = \mathbb{R}[x_1, \ldots, x_n]$ of A determines a unique ideal $\mathfrak{a}$ of the polynomial ring $\mathbb{R}[X] := \mathbb{R}[X_1, \ldots, X_n]$ such that $\mathbb{R}[X]/\mathfrak{a} \cong A$ via $X_i + \mathfrak{a} \mapsto x_i$, $i = 1, \ldots, n$. Ring homomorphisms from A to $\mathbb{R}$ are identified with real zeros of the ideal $\mathfrak{a}$. For any set S in A, $\mathcal{X}_S$ is identified with the set of real zeros t of $\mathfrak{a}$ satisfying $g(t) \geq 0$ for all $g \in S$. For $f \in A$, we often abuse the notation, writing $f \geq 0$ on $\mathcal{X}_S$ instead of $\hat{f} \geq 0$ on $\mathcal{X}_S$ and writing $f(\alpha)$ in place of $\hat{f}(\alpha) = \alpha(f)$, for $\alpha \in \mathcal{X}_S$.

We recall the following result:

Proposition 4.1 *Suppose* $A = \mathbb{R}[x_1, \ldots, x_n]$ *and* M *is a quadratic module in* A. *Then the following are equivalent:*

(1) $\exists$ *a positive integer* k *such that* $k - \sum_{i=1}^n x_i^2 \in M$.
(2) M *is archimedean.*

Proof Assume (1) and consider the set

$$B = \{f \in A \mid \exists k \in \mathbb{Z} \text{ such that } k - f, k + f \in M\}.$$

By [11, Proposition 3.3.3], B is a subring of A containing $x_1, \ldots, x_n$. Since B obviously contains $\mathbb{R}$, this implies $B = A$. This proves (1) $\Rightarrow$ (2). The implication (2) $\Rightarrow$ (1) is trivial. ∎

In [6], Theorem 2.1 is used in conjunction with Proposition 4.1 to give an algebraic proof of certain results of Putinar and Vasilescu [17, Theorem 4.2, Corollary 4.3, Corollary 4.4, Theorem 4.5].[3]

[3] To be completely accurate, only the proof of [17, Theorem 4.2] is given in [6] but it is easy to see that exactly the same method yields [17, Corollary 4.4] and [17, Theorem 4.5]. Of course, [17, Corollary 4.3] is immediate from [17, Theorem 4.2]. The reader should also note that part of the required hypothesis of [17, Corollary 4.4] has been omitted in the statement in [17]. The polynomials $p_1, \ldots, p_m$ are required to have even degree.

https://doi.org/10.4153/CMB-2003-041-9 Published online by Cambridge University Press

Proposition 4.1 extends as follows:

Proposition 4.2 *Suppose $A = \mathbb{R}[x_1, \ldots, x_n]$, M is a quadratic module in A, and p is an element of A such that $p - 1 \in M[1/p^2]$. Then the following are equivalent:*

(1) *$\exists$ integers $k \geq 1$, $\ell \geq 0$ such that $kp^\ell - \sum_{i=1}^n x_i^2 \in M[1/p^2]$.*
(2) *$\forall f \in A[1/p]$, $\exists$ integers $k \geq 1$, $\ell \geq 0$ such that $kp^\ell - f \in M[1/p^2]$.*

Proof Assume (1) and consider

$$C = \{f \in A[1/p] \mid \exists q \in \mathbb{Z}[p] \text{ such that } q - f, q + f \in M[1/p^2]\}.$$

Exactly as in the proof of [11, Proposition 3.3.3] C is a subring of $A[1/p]$ and $x_1, \ldots, x_n \in C$. Since

$$1 \pm 1/p = (p \pm 1)/p = (p^2 \pm p)/p^2 \in M[1/p^2],$$

we also have $1/p \in C$. Since $x_1, \ldots, x_n, 1/p$ generate $A[1/p]$ as an algebra over $\mathbb{R}$ and $\mathbb{R} \subseteq C$, this implies $C = A[1/p]$. Combining this with the fact that the elements kp^ℓ, $k \geq 1$, $\ell \geq 0$ are cofinal in $\mathbb{Z}[p]$ with respect to the partial ordering associated to $M[1/p^2]$ proves (2). This proves (1) $\Rightarrow$ (2). The implication (2) $\Rightarrow$ (1) is trivial. ■

An important point to keep in mind is that the geometric condition

$$\exists \text{ integers } k \geq 1, \ell \geq 0 \text{ such that } kp^\ell - \sum_{i=1}^n x_i^2 \geq 0 \text{ on } \mathcal{X}_M$$

does not necessarily imply the arithmetic condition (1) of Proposition 4.2.[4] For example, if $\mathcal{X}_M$ is compact, one would like to be able to choose $p = 1$, but [7, Example 4.8] shows that this is not always possible. Similarly, if $x_i \geq 0$ on $\mathcal{X}_M$ for $i = 1, \ldots, n$, one would like to be able to choose $p = 1 + \sum_{i=1}^n x_i$ but, again, this may not be possible.

At the same time, it is equally important to realize that it is always possible to arrange things so that condition (1) of Proposition 4.2 holds. For example, take $p = 1 + \sum_{i=1}^n x_i^2$, $k = \ell = 1$ or $p = \prod_{i=1}^n (1 + x_i^2)$, $k = \ell = 1$. In special cases, better choices for p may be available.

Corollary 4.3 *Suppose $A = \mathbb{R}[x_1, \ldots, x_n]$, M is a quadratic module in A, and p is an element of A such that $p - 1 \in M[1/p^2]$. Suppose condition (1) of Proposition 4.2 holds (e.g., take $p = 1 + \sum_{i=1}^n x_i^2$). Then, for any $f \in A[1/p]$, the following are equivalent:*

(1) *$f \geq 0$ on $\mathcal{X}_{M[1/p^2]}$.*
(2) *There exists an integer $k \geq 0$ such that, for all rational $\epsilon > 0$, $f + \epsilon p^k \in M[1/p^2]$.*

[4] In the case where the quadratic module M is a finitely generated preordering, the geometric condition and the arithmetic condition are in fact equivalent [10, Corollary 1.4]. Later, in Section 7, we prove a stronger version of [10, Corollary 1.4] as an application of the general criterion we develop in Section 6.

https://doi.org/10.4153/CMB-2003-041-9 Published online by Cambridge University Press

Proof Combine Proposition 4.2 and Theorem 2.2. ∎

In [17, Theorem 2.5] Putinar and Vasilescu explain how the Moment Problem can be solved 'by dimension extension'. Our next result extends [17, Theorem 2.5] in a variety of ways.

Corollary 4.4 *Suppose $A = \mathbb{R}[x_1, \ldots, x_n]$, M is a quadratic module in A, and p is an element of A such that $p - 1 \in M[1/p^2]$. Suppose condition (1) of Proposition 4.2 holds, and $p \neq 0$ at each point of $\mathcal{X}_M$ (e.g., take $p = 1 + \sum_{i=1}^n x_i^2$). Then for each linear function $L\colon A[1/p] \to \mathbb{R}$ satisfying $L(M[1/p^2]) \geq 0$, there exists a unique positive Borel measure μ on $\mathcal{X}_M$ such that for all $f \in A$ and for all integers $k \geq 0$, $L(f/p^k) = \int_{\mathcal{X}_M} f/p^k \, d\mu$.*

Proof By Proposition 4.2 and Corollary 3.4 we have a positive Borel measure μ' on $\mathcal{X}_{M[1/p^2]}$ satisfying $L(f/p^k) = \int_{\mathcal{X}_{M[1/p^2]}} f/p^k \, d\mu'$. Take μ to be the positive Borel measure on $\mathcal{X}_M$ corresponding to μ' via the natural homeomorphism $\mathcal{X}_M \cong \mathcal{X}_{M[1/p^2]}$. Uniqueness is immediate from Remark 3.5. ∎

As pointed out already in [9, Corollary 4.4] and [11, Corollary 4.3.7] in the preordering case, it is possible to avoid 'dimension extension' altogether, provided one is willing to compensate by enlarging M a bit. Namely, we define

$$M_p = \{f \in A \mid \exists \text{ an integer } k \geq 0 \text{ such that } p^{2k} f \in M\}.$$

Corollary 4.5 *Suppose $A = \mathbb{R}[x_1, \ldots, x_n]$, M is a quadratic module in A, and p is an element of A such that $p - 1 \in M[1/p^2]$. Suppose condition (1) of Proposition 4.2 holds (e.g., take $p = 1 + \sum_{i=1}^n x_i^2$). Then for each linear function $L\colon A \to \mathbb{R}$ satisfying $L(M_p) \geq 0$, there exists a positive Borel measure μ on $\mathcal{X}_M$ such that $\forall f \in A$, $L(f) = \int_{\mathcal{X}_M} f \, d\mu$.*

Proof Suppose $f \geq 0$ on $\mathcal{X}_M$. By Corollary 4.3 there exists $\ell \geq 0$ such that, for all rational $\epsilon > 0$, $f + \epsilon p^\ell \in M[1/p^2]$ (so $f + \epsilon p^\ell \in M_p$). Now apply Corollary 3.2 to the quadratic module M_p. ∎

5 Cylinders

Although Theorem 2.2 is a nice general result, there are cases where it can be improved. Denote by $A[Y]$, polynomial ring in a single variable Y with coefficients in the ring A. The result in [9, Theorem 5.1] on cylinders with compact cross-section extends to the module case as follows:[5]

Theorem 5.1 *Suppose M is a quadratic module in A which is archimedean. Then, for any $f \in A[Y]$, the following are equivalent:*

(1) *$f \geq 0$ on $\mathcal{X}_M \times \mathbb{R}$.*

[5]The reader may check that the corollary [9, Corollary 5.4] in [9] extends in a similar way.

https://doi.org/10.4153/CMB-2003-041-9 Published online by Cambridge University Press

(2) *$\exists$ an integer $\ell \geq 0$ such that $\forall$ rational $\epsilon > 0$, $f+\epsilon(1+Y^2)^\ell$ belongs to the quadratic module in $A[Y]$ generated by M.*

Proof Denote by $\tilde{M}$ the quadratic module in $A[Y]$ generated by M. Suppose f satisfies (1). Take ℓ to be any integer such that $2\ell \geq \deg(f)$. Following exactly the proof in the preordering case given in [9], we see that $f + \epsilon q \in \tilde{M}$ holds for any rational $\epsilon > 0$ where $q = 3 + Y + 3Y^2 + Y^3 + \cdots + 3Y^{2\ell}$. Observing that

$$q + \frac{1}{2}\Big(\sum_{i=0}^{\ell-1}(1-Y)^2Y^{2i} + 1 + Y^{2\ell}\Big) = 4(1 + Y^2 + \cdots + Y^{2\ell}),$$

it is clear that $f + 4\epsilon(1 + Y^2)^\ell \in \tilde{M}$ also holds. ∎

Theorem 5.2 *Suppose M is a quadratic module in A and $p \in A$ is a unit such that $p - 1 \in M$ and, for all $a \in A$, there exist integers $k, \ell \geq 0$ such that $kp^\ell - a \in M$. Then, for any $f \in A[Y]$, the following are equivalent:*

(1) *$\hat{f} \geq 0$ on $\mathcal{X}_M \times \mathbb{R}$.*
(2) *$\exists$ integers $k, \ell \geq 0$ such that $\forall$ rational $\epsilon > 0$, $f + \epsilon p^k(1 + Y^2)^\ell$ belongs to the quadratic module in $A[Y]$ generated by M.*

Proof Define B, M' as in the proof of Theorem 2.2 and denote by $\tilde{M}'$ the quadratic module in $B[Y]$ generated by M'. Suppose $f \in A[Y]$, $f \geq 0$ on $\mathcal{X}_M \times \mathbb{R}$. Say $f = a_0 + \cdots + a_{2d}Y^{2d}$, $a_i \in A$. Choose ℓ so large that $a_i/p^{2\ell} \in B$ for each i. Then $f/p^{2\ell} \in B[Y]$ and one checks, as in the proof of Theorem 2.2, that $f/p^{2\ell+2} \geq 0$ on $\mathcal{X}_M \times \mathbb{R}$. By Theorem 5.1, $f/p^{2\ell+2} + \epsilon(1 + Y^2)^d \in \tilde{M}'$ holds for all rational $\epsilon > 0$. The result follows now, multiplying by $p^{2\ell+2}$. ∎

In both Theorem 5.1 and Theorem 5.2, the improvement over Theorem 2.2 comes from the fact that it is unnecessary to invert $1 + Y^2$. Thus, for example, working with the quadratic module $\sum \mathbb{R}[X, Y]^2$ in the polynomial ring in two variables X, Y over $\mathbb{R}$, one only needs to invert $1 + X^2$. This fact was overlooked in [9].

Corollary 5.3 *Suppose $A = \mathbb{R}[x_1, \ldots, x_n]$, M is a quadratic module in A, and p is an element of A such that $p - 1 \in M[1/p^2]$. Suppose condition (1) of Proposition 4.2 holds (e.g., take $p = 1 + \sum_{i=1}^n x_i^2$). Then, for any $f \in A[1/p][Y]$, the following are equivalent:*

(1) *$f \geq 0$ on $\mathcal{X}_{M[1/p^2]} \times \mathbb{R}$.*
(2) *$\exists$ integers $k, \ell \geq 0$ such that $\forall$ rational $\epsilon > 0$, $f + \epsilon p^k(1 + Y^2)^\ell$ belongs to the quadratic module in $A[1/p][Y]$ generated by M.*

Proof Combine Proposition 4.2 and Theorem 5.2. ∎

https://doi.org/10.4153/CMB-2003-041-9 Published online by Cambridge University Press

6 The Jacobi-Prestel Criterion Generalized

To be able to apply Corollary 4.3 and Corollary 5.3 properly we need to analyze the arithmetic condition

$$\exists \text{ integers } k \geq 1,\ \ell \geq 0 \text{ such that } kp^{\ell} - \sum_{i=1}^{n} x_i^2 \in M[1/p^2]$$

in more detail. In case the quadratic module M is finitely generated, it is possible to carry out such an analysis using tools from real algebra, generalizing what is done in [7]. ([7] deals with the case where $\mathcal{X}_M$ compact and $p = 1$.)

We use the following notation: We assume $A = \mathbb{R}[x_1, \ldots, x_n]$. We fix a finite set $S = \{g_1, \ldots, g_s\}$ in A and set $M = M_S$, the quadratic module in A generated by S. Thus $M = T + Tg_1 + \cdots + Tg_s$ where $T := \sum A^2$.

We fix $p \in A$ and work with the multiplicative set $\mathcal{P} = \{\ell p^m \mid \ell, m \text{ positive integers}\}$ in A. We set $x_0 = 1$, so $\sum_{i=0}^{n} x_i^2 = 1 + x_1^2 + \cdots + x_n^2$.

For each prime ideal $\mathfrak{p}$ in A, $F_{\mathfrak{p}}$ denotes the *residue field* of A at $\mathfrak{p}$, *i.e.*, the field of fractions of the integral domain $A/\mathfrak{p}$. Recall: $\mathfrak{p} \mapsto \mathfrak{p}[1/p]$ defines a one-to-one correspondence between prime ideals of A with $p \notin \mathfrak{p}$ and prime ideals of $A[1/p]$. The residue field of $A[1/p]$ at $\mathfrak{p}[1/p]$ is the same as the residue field of A at $\mathfrak{p}$.

We use notation and terminology from quadratic form theory: A *quadratic form* over a field F of characteristic $\neq 2$ is an n-tuple $\phi = \langle a_1, \ldots, a_n \rangle$ with $a_1, \ldots, a_n \in F$. ϕ is *regular* if each a_i is non-zero. For any quadratic form ϕ, ϕ^* denotes the regular quadratic form obtained from ϕ by deleting the entries of ϕ which are zero. A regular quadratic form $\phi = \langle a_1, \ldots, a_n \rangle$ over F is said to be *weakly isotropic* over F if there exists $k \geq 1$ and elements $x_{ij} \in F$, $i = 1, \ldots, n$, $j = 1, \ldots, k$, not all zero, such that $\sum_{i,j} a_i x_{ij}^2 = 0$.

We aim to prove the following generalization of the result in [7].

Theorem 6.1 *There exists $k \in \mathcal{P}$ such that $k - \sum_{i=0}^{n} x_i^2 \in M[1/p^2]$ iff*

(1) *There exists $k \in \mathcal{P}$ such that $k - \sum_{i=0}^{n} x_i^2 \geq 0$ on $\mathcal{X}_{M[1/p^2]}$ and*
(2) *There exists a positive integer ℓ such that, for all pairs $(\mathfrak{p}, v)$ where $\mathfrak{p}$ is a prime ideal of A with $p \notin \mathfrak{p}$ and $F_{\mathfrak{p}}$ formally real and v is a real valuation on $F_{\mathfrak{p}}$ with $\min\{v(x_i^2 + \mathfrak{p}) \mid i = 0, \ldots, n\} < v(p^{\ell} + \mathfrak{p})$, the quadratic form $\tau = \langle 1 + \mathfrak{p}, g_1 + \mathfrak{p}, \ldots, g_s + \mathfrak{p} \rangle^*$ is weakly isotropic over the henselization of $F_{\mathfrak{p}}$ at v.*

Thus, in order for our arithmetic condition to hold it is necessary and sufficient that conditions (1) and (2) both hold. Condition (1) is a purely geometric condition which is quite pleasant and natural. Condition (2) is purely valuation-theoretic and is in some sense much less pleasant. In the general both conditions are necessary. In the next section we will consider special cases where the geometric condition by itself suffices (in the sense that it implies the valuation-theoretic condition).

It is important to note that we do not assume $p - 1 \in M[1/p^2]$. On the other hand, if the arithmetic condition $k - \sum_{i=0}^{n} x_i^2 \in M[1/p^2]$ does hold then $k - 1 \in M[1/p^2]$ so we can apply Corollary 4.3, working with k instead of p.

Note: Since $k \in \mathcal{P}$, $A[1/k] = A[1/p]$ and $M[1/k^2] = M[1/p^2]$.

https://doi.org/10.4153/CMB-2003-041-9 Published online by Cambridge University Press

Proof To simplify notation we work in the ring $A[1/p]$, replacing A by $A[1/p]$ and M by $M[1/p^2]$ (so now A is generated by $x_1, \dots, x_n$ and $1/p$).

One implication is elementary. Assume $k \in \mathcal{P}$ is such that $k - \sum_{i=0}^n x_i^2 \in M$. Then (1) obviously holds. Let $k' = 2k^2$, $f = k' - \sum_{i=0}^n x_i^2$. Since $k - 1 = (k - \sum_{i=0}^n x_i^2) + \sum_{i=1}^n x_i^2$, we see that $k - 1 \in M$ and $2k^2 - (k+1) = 2(k-1)^2 + 3(k-1) + 1 \in M$. Thus $-1 = 2k^2 - (k+1) + (k - \sum_{i=0}^n x_i^2) - (2k^2 - \sum_{i=0}^n x_i^2) \in M - fT$. Thus $-1 = t_0 + \sum g_i t_i - ft$, *i.e.*, $(1^2 + t_0) + \sum g_i t_i - ft = 0$ for some $t, t_0, \dots, t_s \in T$ so, for each formally real residue field $F_\mathfrak{p}$ of A, the regular quadratic form $\phi = \langle 1 + \mathfrak{p}, g_1 + \mathfrak{p}, \dots, g_s + \mathfrak{p}, -f + \mathfrak{p} \rangle^*$ is weakly isotropic over $F_\mathfrak{p}$. Suppose v is a real valuation on $F_\mathfrak{p}$ satisfying $\min\{v(x_i^2 + \mathfrak{p}) \mid i = 0, \dots, n\} < v(k' + \mathfrak{p})$, and H is the henselization of $F_\mathfrak{p}$ at v. Since

$$v(k' + \mathfrak{p}) > \min\{v(x_i^2 + \mathfrak{p}) \mid i = 0, \dots, n\} = v\Big(\sum_{i=0}^n x_i^2 + \mathfrak{p} \Big),$$

$1 - (k' + \mathfrak{p}) / \big(\sum_{i=0}^n x_i^2 + \mathfrak{p} \big)$ is a square in H so

$$-f + \mathfrak{p} = \Big(\sum_{i=0}^n x_i^2 + \mathfrak{p} \Big) \Big(1 - (k' + \mathfrak{p}) \Big/ \Big(\sum_{i=0}^n x_i^2 + \mathfrak{p} \Big) \Big)$$

is a non-zero sum of squares in H. Since ϕ is weakly isotropic over H (since it is even weakly isotropic over $F_\mathfrak{p}$) this implies that τ is also weakly isotropic over H. Thus condition (2) holds, taking ℓ to be the exponent of p in k'.

The other implication is more subtle. Suppose $k \in \mathcal{P}$ satisfies the hypothesis of (1) and ℓ satisfies the hypothesis of (2). $k \geq 1$ on $\mathcal{X}_M$ so, replacing k by some multiple of some power of k, we may assume that $f := k^2 - \sum_{i=0}^n x_i^2$ is strictly positive on $\mathcal{X}_M$ and that the exponent of p in k is $\geq \ell$. The proof breaks into two parts. First we show that $-1 \in M - fT$. Next we show that this implies the arithmetic condition. For the first step, by Bröcker's local global principle for quadratic modules [11, Theorem 7.1.1], it suffices to show that for each formally real residue field $F_\mathfrak{p}$ of A, the quadratic form $\phi = \langle 1 + \mathfrak{p}, g_1 + \mathfrak{p}, \dots, g_s + \mathfrak{p}, -f + \mathfrak{p} \rangle^*$ is weakly isotropic over $F_\mathfrak{p}$. For this, by the local-global principle for weak isotropy [11, 6.2.2], it suffices to show that ϕ is indefinite with respect to every ordering of $F_\mathfrak{p}$ and that ϕ is weakly isotropic over the henselization of $F_\mathfrak{p}$ at v for each real valuation v of $F_\mathfrak{p}$ such that ϕ has at least two residue forms with respect to v. The fact that ϕ is indefinite at every ordering of $F_\mathfrak{p}$ comes from $f > 0$ on $\mathcal{X}_M$ in conjunction with Tarski's transfer principle: If $\leq$ is an ordering of $F_\mathfrak{p}$ satisfying $g_i + \mathfrak{p} \geq 0$ for each $i = 1, \dots, s$, then $f + \mathfrak{p} > 0$. Suppose v is a real valuation of $F_\mathfrak{p}$ such that ϕ has at least two residue forms with respect to v. There are three cases to consider:

Case 1. $\min\{v(x_i^2 + \mathfrak{p}) \mid i = 0, \dots, n\} < v(p^\ell + \mathfrak{p})$. Then τ is weakly isotropic over the henselization of $F_\mathfrak{p}$ with respect to v. Since τ is a subform of ϕ, ϕ is also weakly isotropic over the henselization.

Case 2. $0 > \min\{v(x_i^2 + \mathfrak{p}) \mid i = 0, \dots, n\} \geq v(p^\ell + \mathfrak{p})$. Then $\min\{v(x_i^2 + \mathfrak{p}) \mid i = 0, \dots, n\} = v(\sum_{i=0}^n x_i^2 + \mathfrak{p}) > v(k^2 + \mathfrak{p})$ so $f = (k^2 + \mathfrak{p}) \big(1 - (\sum_{i=0}^n X_i^2 + \mathfrak{p}) / (k^2 + \mathfrak{p}) \big)$

https://doi.org/10.4153/CMB-2003-041-9 Published online by Cambridge University Press

is a square in the henselization. ϕ is weakly isotropic over the henselization in this case.

Case 3. $0 = \min\{v(x_i^2 + \mathfrak{p}) \mid i = 0, \ldots, n\} = v(p^\ell + \mathfrak{p})$. Since A is generated over $\mathbb{R}$ by $x_1, \ldots, x_n, 1/p$ it follows that in this case the image of A under the $g \mapsto g + \mathfrak{p}$ is contained in the valuation ring B_v of v. Denote by $\mathfrak{p}'$ the kernel of the composite map $A \to B_v \to F'$, where F' is the residue field of the valuation v and consider the quadratic form $\phi' = \langle 1 + \mathfrak{p}', g_1 + \mathfrak{p}', \ldots, g_s + \mathfrak{p}', -f + \mathfrak{p}' \rangle^*$ defined over $F_{\mathfrak{p}'} \hookrightarrow F'$. Since ϕ has at least two residue forms with respect to v, one of the elements $c + \mathfrak{p}$ in the set $g_1 + \mathfrak{p}, \ldots, g_2 + \mathfrak{p}, -f + \mathfrak{p}$ is non-zero and also has positive value. Thus $c \in \mathfrak{p}' \setminus \mathfrak{p}$. Thus $\mathfrak{p} \subsetneqq \mathfrak{p}'$ so the transcendence degree of $F_{\mathfrak{p}'}$ over $\mathbb{R}$ is strictly less than the transcendence degree of $F_{\mathfrak{p}}$ over $\mathbb{R}$. By induction on transcendence degree, ϕ' is weakly isotropic over $F_{\mathfrak{p}'}$. Since ϕ' is identified with a subform of one of the residue forms of ϕ, ϕ is weakly isotropic over the henselization [11, Proposition 6.2.4].

This completes the first part of the proof. We know now that $-1 \in M - fT$ where $f := k^2 - \sum_{i=0}^n x_i^2$. Thus $tf = 1 + m$ for some $t \in T$, $m \in M$. Decompose f as $f = t_1 - t_2$, $t_1, t_2 \in T$ and let $t' \in T$ be defined by $t' = t + tt_2$. Then $(1 + t')f = (1+t+tt_2)f = f+1+m+t_2(1+m) = 1+m+t_1+t_2m \in M$. Thus, if $P := T + fT$, then $(1 + t')P \subseteq M$. By definition of P, $f = k^2 - \sum_{i=0}^n x_i^2 \in P$. In particular, $k^2 - 1 \in P$, so $k^2 - 1/k^2 \in P$. Thus $2k^2 - (\sum_{i=0}^n x_i^2 + 1/k^2) \in P$. Since $x_1, \ldots, x_n, 1/k$ generate A, Proposition 4.2 applies to P: There exists $k_1 \in \mathcal{P}$ (some multiple of some power of $2k^2$) such that $k_1 - (t' + 2)/2 \in P$. Thus $k_1^2 - (1 + t') = 2(1 + t')(k_1 - (t' + 2)/2) + (k_1 - (1+t'))^2 \in M$ so $k^2k_1^2 - \sum_{i=0}^n x_i^2 = (1+t')f + t' \sum_{i=0}^n x_i^2 + k^2(k_1^2 - (1+t')) \in M$. Since $k^2k_1^2 \in \mathcal{P}$, this completes the proof. ∎

7 Applications

We continue to assume that A is a finitely generated algebra over $\mathbb{R}$, say $A = \mathbb{R}[x_1, \ldots, x_n]$ and that $S = \{g_1, \ldots, g_s\}$, a finite subset of A. Denote by S' the complete set of $(2^s - 1)$ products

$$g_1, \ldots, g_s, g_1g_2, \ldots, g_{s-1}g_s, \ldots, g_1 \cdots g_2.$$

Also, denote by $\tilde{S}$ the set consisting of the first 2^{s-1} products in this list. (Convention: if $S = \varnothing$, then $\tilde{S} = S$.) Thus $M_S \subseteq M_{\tilde{S}} \subseteq M_{S'}$ and $\mathcal{X}_S = \mathcal{X}_{\tilde{S}} = \mathcal{X}_{S'}$. $M_{S'}$ is equal to T_S, the quadratic preordering in A generated by S.

Note: If $s \leq 2$ then $\tilde{S} = S$.

For $\mathfrak{p}$ a prime ideal of A with $p \notin \mathfrak{p}$ and $F_{\mathfrak{p}}$ formally real, denote by τ' and $\tilde{\tau}$ the quadratic forms over $F_{\mathfrak{p}}$ determined by S' and $\tilde{S}$ respectively. τ' is a Pfister form of dimension 2^t for some $t \leq s$ (t is the number of indices i with $g_i \notin \mathfrak{p}$) and, as pointed out in [7] [11], $\tilde{\tau}$ is a subform of τ' of dimension $\geq 2^{t-1} + 1$ if $t \geq 1$. If $t = 0$, then $\tilde{\tau} = \tau' = \tau = \langle 1 + \mathfrak{p} \rangle$.

Fix integers $k, \ell \geq 1$ such that the geometric condition holds, *i.e.*, $f := kp^\ell - \sum_{i=0}^n x_i^2 \geq 0$ on $\{\alpha \in \mathcal{X}_S \mid p(\alpha) \neq 0\}$. By the Tarski's transfer principle, for any ordering $\leq$ on $F_{\mathfrak{p}}$, $(g_1 + \mathfrak{p} \geq 0$ and $\cdots$ and $g_s + \mathfrak{p} \geq 0) \Rightarrow f + \mathfrak{p} \geq 0$. Let v be a real valuation of $F_{\mathfrak{p}}$ such that $v(\sum_{i=0}^n x_i^2 + \mathfrak{p}) < v(p^\ell + \mathfrak{p})$ and let H be the henselization

https://doi.org/10.4153/CMB-2003-041-9 Published online by Cambridge University Press

of $F_{\mathfrak{p}}$ at v. Then, for every ordering $\leq$ of H, $f + \mathfrak{p} < 0$, so $g_i + \mathfrak{p} < 0$ for some i. Consequently, the Pfister form τ' is indefinite at every ordering of H, so τ' is weakly isotropic over H. (This follows from the signature criterion for weak isotropy [11, 6.3.2] since $\tau' \sim 0$ over H.) By [11, Corollary 6.4.3], the quadratic form $\tilde{\tau}$ is also weakly isotropic over H.

This proves that, for the derived set $\tilde{S}$, the valuation-theoretic condition (2) of Theorem 6.1 is implied automatically by the geometric condition (1). In particular, we obtain the following:

Corollary 7.1 *Suppose there exist positive integers k, ℓ such that $kp^{\ell} - \sum_{i=0}^{n} x_i^2 \geq 0$ holds on the set $\{\alpha \in \mathcal{X}_S \mid p(\alpha) \neq 0\}$. Then, for $f \in A[1/p]$, the following are equivalent:*

(1) *$f \geq 0$ on $\{\alpha \in \mathcal{X}_S \mid p(\alpha) \neq 0\}$.*
(2) *$\exists$ an integer $\ell \geq 0$ such that $\forall$ rational $\epsilon > 0$, $f + \epsilon p^{\ell} \in M_{\tilde{S}}[1/p^2]$.*

Proof Immediate from the above analysis, using Corollary 4.3 and Theorem 6.1. ■

Note: This extends the result in [10, Corollary 3.1]. It also extends the corresponding result of Jacobi and Prestel for $p = 1$ in [7, Theorem 4.4]. Both of these latter results, in turn, extend the basic result of Schmüdgen [19] [21].

Using Corollary 5.3 instead of Corollary 4.3, we also have a corresponding result for cylinders:

Corollary 7.2 *Suppose there exist positive integers k, ℓ such that $kp^{\ell} - \sum_{i=0}^{n} x_i^2 \geq 0$ holds on the set $\{\alpha \in \mathcal{X}_S \mid p(\alpha) \neq 0\}$. Then, for $f \in A[1/p][Y]$, the following are equivalent:*

(1) *$f \geq 0$ on $\{\alpha \in \mathcal{X}_S \mid p(\alpha) \neq 0\} \times \mathbb{R}$.*
(2) *$\exists$ integers $k, \ell \geq 0$ such that $\forall$ rational $\epsilon > 0$, $f + \epsilon p^k (1 + Y^2)^{\ell}$ belongs to the quadratic module in $A[1/p][Y]$ generated by $M_{\tilde{S}}$.*

Of course, it is important to keep in mind that $\tilde{S} = S$ if $s \leq 2$.

Remark 7.3 (Compare to [7, Remark 4.7]) If $A[1/p]$ has real dimension ≤ 1 (*i.e.*, $F_{\mathfrak{p}}$ has transcendence degree ≤ 1 over $\mathbb{R}$ for each prime $\mathfrak{p}$ of A with $p \notin \mathfrak{p}$, $F_{\mathfrak{p}}$ formally real) then the valuation-theoretic condition (2) of Theorem 6.1 is automatically implied by the geometric condition (1). The geometric condition (1) and the hypothesis of the valuation-theoretic condition (2) force the quadratic form $\tau = \langle 1 + \mathfrak{p}, g_1 + \mathfrak{p}, \ldots, g_s + \mathfrak{p} \rangle^*$ to be indefinite over H. Since H has transcendence degree 1 over $\mathbb{R}$, H is SAP by [15, Theorem 9.4], so τ is weakly isotropic over H. Thus in the case where $A[1/p]$ had real dimension ≤ 1, one can improve on Corollary 7.1 and Corollary 7.2, replacing $\tilde{S}$ by S in the statements of these results.

It is not clear how to generalize [7, Theorem 4.1] to the non-compact case.

8 Two Examples

In the case where the ring A is a finitely generated $\mathbb{R}$-algebra, one would like to understand the geometric meaning of the ring B and the quadratic module M' in B defined

https://doi.org/10.4153/CMB-2003-041-9 Published online by Cambridge University Press

in the proof of Theorem 2.2. We work out two examples in detail. In both of these examples the quadratic module M we consider is in fact a preordering.

We introduce some convenient notation: We define $\mathbb{R}$-subalgebras B_i of $A[1/p]$ inductively by $B_0 = A[1/p]$ and B_{i+1} = the ring of elements of B_i which are geometrically bounded on $\mathcal{X}_{M_i}$ where $M_i := M[1/p^2] \cap B_i$. The B_i are a certain 'poor man's version' of the iterated holomorphy rings defined in [1] and [20].[6] Also, as in the proof of Theorem 2.2,

$$B := \{f \in A[1/p] \mid \exists \text{ an integer } k \text{ such that } k - f, k + f \in M[1/p^2]\},$$

the ring of arithmetically bounded elements, and $M' := M[1/p^2] \cap B$. Thus

$$A[1/p] = B_0 \supseteq B_1 \supseteq \cdots \supseteq B$$

and there are canonical restriction maps

$$\mathcal{X}_M = \mathcal{X}_{M[1/p^2]} = \mathcal{X}_{M_0} \to \mathcal{X}_{M_1} \to \cdots \to \mathcal{X}_{M'}.$$

Since $B[p] = A[1/p]$, these various $\mathbb{R}$-algebras all have the same transcendence degree over $\mathbb{R}$.

Example 8.1 (Compare to [17, Theorem 3.2]) Take $A = \mathbb{R}[X] := \mathbb{R}[X_1, \ldots, X_n]$, the polynomial ring in n variables, $M = \sum A^2$, and $p = 1 + \sum_{i=1}^n X_i^2$. Thus $M[1/p^2] = \sum A[1/p]^2$ and $\mathcal{X}_M$ and $\mathcal{X}_{M[1/p^2]}$ are naturally identified with $\mathbb{R}^n$ (associating to each $t \in \mathbb{R}^n$ the ring homomorphism $f \mapsto f(t)$). Clearly

$$p \pm 1 \in M,\ p \pm X_i^2 \in M, \text{ and } p \pm 2X_iX_j \in M \quad \text{for } i \neq j$$

(since $X_i^2 \pm 2X_iX_j + X_j^2 = (X_i \pm X_j)^2 \in M$). Multiplying by $1/p = (1/p)^2 p \in \sum A[1/p]^2$, this yields $1 \pm 1/p$, $1 \pm X_i^2/p$, $1/2 \pm X_iX_j/p \in \sum A[1/p]^2$, $i \neq j$. As well, $1 - (X_i/p)^2 = (1 - 1/p) + (1 - X_i^2/p)/p \in \sum A[1/p]^2$, so $1 \pm X_i/p = \left((1 \pm X_i/p)^2 + (1 - X_i^2/p^2)\right)/2 \in \sum A[1/p]^2$. In particular, the elements $1/p$, X_i^2/p, X_i/p and X_iX_j/p, $i \neq j$ belong to the subring B of $A[1/p]$ defined in the proof of Theorem 2.2.

We introduce some notation: Let $Y_{ij} = X_iX_j/p$, $i, j = 0, \ldots, n$ where $X_0 := 1$. Thus $\mathbb{R}[Y_{ij} \mid i, j = 0, \ldots, n] \subseteq B$, $Y_{ij} = Y_{ji}$, $Y_{ij}Y_{i'j'} = Y_{ii'}Y_{jj'}$, and $\sum_{i=0}^n Y_{ii} = 1$.

Claim: *For $f \in A$ of degree $d \in \{2k, 2k-1\}$, $f/p^i \in \mathbb{R}[Y_{ij} \mid i, j = 0, \ldots, n]$ if $i \geq k$. If $i < k$ then $f/p^i \notin B_1$.* For let $i_1, \ldots, i_d$ be in the set $\{0, \ldots, n\}$ with $d = 2k$ or $d = 2k - 1$, $k \geq 1$. Then it is clear that $X_{i_1} \cdots X_{i_d}/p^k$ is expressible as a product of elements Y_{ij}. It follows that if $f \in A$ has degree $d \in \{2k, 2k-1\}$ then f/p^k lies in the $\mathbb{R}[Y_{ij} \mid i, j = 0, \ldots, n]$. Since $1/p = Y_{00}$, the same is true for f/p^i, $i > k$. It remains to show $f/p^i \notin B_1$ if $i < k$. Decompose f as $f = f_0 + \cdots + f_d$ where

[6] As long as the $\mathbb{R}$-algebras B_i and the quadratic modules M_i remain finitely generated, the two definitions will coincide, by the Tarski transfer principle.

https://doi.org/10.4153/CMB-2003-041-9 Published online by Cambridge University Press

f_i is homogeneous of degree i. Since $f_d \neq 0$, there exists $x \in \mathbb{R}^n$ such that $f_d(x) \neq 0$. Then, for any integer ℓ and any real $\lambda > 0$, one of

$$\ell \pm \frac{f(\lambda x)}{p(\lambda x)^i} = \ell \pm \frac{f_0 + \lambda f_1(x) + \cdots + \lambda^d f_d(x)}{\left(1 + \lambda^2(x_1^2 + \cdots + x_n^2)\right)^i}$$

approaches $-\infty$ as $\lambda \to \infty$ if $i < k$. Since this holds for any integer ℓ, this proves that f/p^i is not bounded on $\mathbb{R}^n$, *i.e.*, $f/p^i \notin B_1$ if $i < k$.

It follows from the claim that $B_1 = B = \mathbb{R}[Y_{ij} \mid i, j = 0, \ldots, n]$. It also follows from the claim that $M' = B \cap M[1/p^2] = B \cap \sum A[1/p]^2$ is equal to $\sum B^2$. For suppose $f/p^{2k} = \sum (f_i/p^k)^2 \in M'$. Since $f/p^{2k} \in B$ our claim implies that $4k \geq \deg(f)$. Since $f = \sum f_i^2$, this implies $2k \geq \deg(f_i)$ for each i so, again by the claim, $f_i/p^k \in B$. This proves $M' = \sum B^2$.

Since $B[p] = A[1/p]$, B has Krull dimension n. On the other hand it is known from the theory of Veronese varieties that the polynomial ring $\mathbb{R}[Z_{ij} \mid i, j = 0, \ldots, n]$ factored by the ideal generated by $Z_{ij} - Z_{ji}$, $Z_{ij}Z_{i'j'} - Z_{ii'}Z_{jj'}$, and $\sum_{i=0}^n Z_{ii} - 1$ is an integral domain of Krull dimension n. It follows that the only relations relating the Y_{ij} are the Veronese relations $Y_{ij} = Y_{ji}$, $Y_{ij}Y_{i'j'} = Y_{ii'}Y_{jj'}$ and $\sum_{i=0}^n Y_{ii} = 1$. Thus $\mathcal{X}_{M'}$ is identified with the Veronese variety

$$V := \left\{ y = (y_{ij}) \in \mathbb{R}^{(n+1)^2} \;\middle|\; y_{ij} = y_{ji}, y_{ij}y_{i'j'} = y_{ii'}y_{jj'}, \sum_{i=0}^n y_{ii} = 1 \right\}.$$

The map from $\mathcal{X}_M$ to $\mathcal{X}_{M'}$ is identified with the map $x \mapsto y = (y_{ij})$ from $\mathbb{R}^n$ to V where

$$y_{00} = 1 \Big/ \left(1 + \sum x_i^2\right), \; y_{0i} = y_{i0} = x_i \Big/ \left(1 + \sum x_i^2\right),$$
$$y_{ij} = x_i x_j \Big/ \left(1 + \sum x_i^2\right) \quad i, j \geq 1.$$

The image of $\mathcal{X}_M$ in $\mathcal{X}_{M'}$ is identified with the set of $y \in V$ with $y_{00} \neq 0$.

The reader will note that the Veronese variety V is just an affine version of real projective n-space. V and $\mathrm{P}(\mathbb{R}^n)$ are identified via $(u_0, \ldots, u_n) \mapsto y = (y_{ij})$ where $y_{ij} = u_i u_j / (\sum u_i^2)$. The composite map from $\mathbb{R}^n$ to $\mathrm{P}(\mathbb{R}^n)$ is just the standard embedding $x \mapsto (1, x_1, \ldots, x_n)$. ∎

The fact that the presentation of B given in Example 8.1 coincides (essentially) with the presentation of the algebra $\mathcal{Q}_\theta$ considered in [17, Theorem 3.2] shows the promised connection between Corollary 3.6 and [17, Theorem 3.2].

Unfortunately, the assumption that the $\mathbb{R}$-algebra A is a finitely generated does not necessarily imply that the $\mathbb{R}$-algebra B is finitely generated. Also, even if the quadratic module M in A is finitely generated, the quadratic module M' in B may not be finitely generated. Our next example illustrates this.

https://doi.org/10.4153/CMB-2003-041-9 Published online by Cambridge University Press

Example 8.2 Consider the polynomial

$$q(X,Y,Z) = X^2(1-Z^2) - (X^4+Y^4);$$

see [2, page 54]. Let $A = \mathbb{R}[X,Y,Z][1/q]$, let M be the quadratic module (equivalently, the quadratic preordering) in A generated by $1/q - 1$. Since $1 - q = 3/4 + (1/2 - X^2)^2 + X^2Z^2 + Y^4 \in \sum \mathbb{R}[X,Y,Z]^2$, $\mathcal{X}_M$ is identified with the set

$$W := \{(x,y,z) \in \mathbb{R}^3 \mid q(x,y,z) > 0\}.$$

Take $p = 1/q$ (so $A[1/p] = A$). We compute the subring B of A and the quadratic module $M' = M \cap B$ defined in the proof of Theorem 2.2.

Claim 1. $B_1 = \mathbb{R}[X,Y,Z]$. Since the set $\mathcal{X}_M = W$ is bounded, one inclusion is clear. For the other, suppose $g \in B_1$. Write $g = f/q^k$ with $f \in \mathbb{R}[X,Y,Z]$, $k \geq 0$ minimal. If $k \geq 1$ then, choosing a sequence of points $(x_n, y_n, z_n) \in W$ approaching a boundary point of W, and using the fact that g is bounded on W, we see that f vanishes on the boundary of W. Since the boundary of W is Zariski dense in the set $V = \{(x,y,z) \in \mathbb{R}^3 \mid q(x,y,z) = 0\}$ and the prime ideal (q) is real [2, Theorem 4.5.1], this implies that $q|f$. This proves $k = 0$ so $g = f \in \mathbb{R}[X,Y,Z]$.

Claim 2. *M_1 is the quadratic module in B_1 generated by q.* Since $q = 1/p \in M \cap \mathbb{R}[X,Y,Z]$, one inclusion is clear. For the other, suppose $g = s + t(1/p - 1) = s + tq(1-q)$ with $g \in \mathbb{R}[X,Y,Z]$, $s,t \in \sum A^2$. Write $s = s'/q^{2k}$, $t = t'/q^{2k}$ with $s', t' \in \sum \mathbb{R}[X,Y,Z]^2$, $k \geq 0$ minimal. Then $q^{2k}g = s' + t'q(1-q)$ so, if $k \geq 1$, then q divides s'. Since q is irreducible in $\mathbb{R}[X,Y,Z]$ and the prime ideal (q) in $\mathbb{R}[X,Y,Z]$ is real, we see that $s' = q^2 s''$, $s'' \in \sum \mathbb{R}[X,Y,Z]^2$. Substituting and dividing by q, we see that q also divides t' and that $t' = q^2 t''$, $t'' \in \sum \mathbb{R}[X,Y,Z]^2$. This contradicts the minimal choice of k. Thus $k = 0$. Since $1 - q \in \sum \mathbb{R}[X,Y,Z]^2$, the proof is complete.

It follows from Claims 1 and 2 that

$$\mathcal{X}_{M_1} = W \cup V = \{(x,y,z) \in \mathbb{R}^3 \mid q(x,y,z) \geq 0\}.$$

Since V contains the Z-axis, this set is unbounded.

Claim 3. *The elements XZ^i, YZ^i, $i \geq 0$ belong to B.* We know that $q \in M$. Adding $(1-X^2)^2 + X^2Z^2 + Y^4$ to q, we see that $1 - X^2 \in M$. We claim that $1 - X^2Z^{2i} \in M$ for all $i \geq 0$. Adding $X^4 + Y^4$ to q, we see that $X^2 - X^2Z^2 \in M$. Multiplying by Z^{2i} this yields $X^2Z^{2i} - X^2Z^{2(i+1)} \in M$. Thus, if we assume inductively that $1 - X^2Z^{2i} \in M$, then, adding, we see that $1 - X^2Z^{2(i+1)} \in M$. This proves the claim. Adding $X^2Z^2 + X^4$ to q, we see that $X^2 - Y^4 \in M$. Multiplying by Z^{4i} and adding $1 - X^2Z^{4i}$, this implies that $1 - Y^4Z^{4i} \in M$. Adding $(1 - Y^2Z^{2i})^2$, this implies $1 - Y^2Z^{2i} \in M$. Adding $(1 \pm XZ^i)^2$ to $1 - X^2Z^{2i}$ and $(1 \pm YZ^i)^2$ to $1 - Y^2Z^{2i}$, we see, finally, that $1 \pm XZ^i \in M$ and $1 \pm YZ^i \in M$, so $XZ^i, YZ^i \in B$ for all integers $i \geq 0$.

https://doi.org/10.4153/CMB-2003-041-9 Published online by Cambridge University Press

Claim 4. $B_2 = B = \mathbb{R}[XZ^i, YZ^i \mid i \geq 0]$. For suppose $g \in B_2$. Using the fact that V contains the Z-axis, we see that g is bounded on the Z-axis, *i.e.*, the polynomial $g(0,0,Z)$ is constant. This proves $g \in \mathbb{R}[XZ^i, YZ^i \mid i \geq 0]$. This completes the proof.

$\mathcal{X}_{M'}$ is obtained from $\mathcal{X}_M = W$ in two steps: First adjoin the points in V to W to obtain $\mathcal{X}_{M_1} = W \cup V$. Then collapse the points in V lying on the Z-axis to a single point to obtain $\mathcal{X}_{M_2} = \mathcal{X}_{M'}$. If $\alpha \in \mathcal{X}_{M'}$ is not in $\mathcal{X}_M = W$ then $\alpha(q) = 0$. If $\alpha(X) = 0$, this forces $\alpha(XZ^i) = 0$ (using $X^2Z^{2i} - X^2Z^{2(i+1)} \in M$ and induction) and $\alpha(YZ^i) = 0$ (using $X^2Z^{4i} - Y^4Z^{4i} \in M$) for each $i \geq 0$. There is a unique such α. If $\alpha(X) \neq 0$, then α extends to $\mathbb{R}[X,Y,Z]$ via $\alpha(Z) = \alpha(XZ)/\alpha(X)$ and α corresponds to a point of V which is not on the Z-axis.

It is clear from Claim 4 that B is not finitely generated. If B is finitely generated then finitely many of the XZ^i, YZ^i would generate B, say XZ^i, YZ^i, $0 \leq i \leq k$. In particular, XZ^{k+1} would be expressible as a polynomial in $X, XZ, \ldots, XZ^k$, $Y, YZ, \ldots, YZ^k$. But this is impossible.

Claim 5. $M_2 = M' = \sum B^2 + \sum B_1^2 q$. If $g \in M'$ then, by Claim 2, $g = s + tq$ with $s, t \in \sum B_1^2$. From the definition of q and Claim 4, we see that $tq \in B$ so $s \in B$, *i.e.*, $s(0,0,Z)$ is constant. Say $s = \sum f_i^2$. Thus $\sum f_i(0,0,Z)^2$ is constant. This implies each $f_i(0,0,Z)$ is constant, *i.e.*, $f_i \in B$.

It follows that the quadratic module M' in B is not finitely generated. Otherwise, M' would be generated by finitely many elements $f_i^2 q$, $f_i \in B_1$, $1 \leq i \leq t$. Choose $f \in B_1$ so that $f(0,0,Z)$ has degree greater than the maximum of the degrees of the $f_i(0,0,Z)$. Then $f^2 q = \sum g_j^2 + \sum g_{ij}^2 f_i^2 q$ with $g_j, g_{ij} \in B$. Thus $g_j = h_j q$, $h_j \in B_1$, and $f^2 = \sum h_i^2 q + \sum g_{ij}^2 f_i^2$. Evaluating at $X = 0$, $Y = 0$ yields $f(0,0,Z)^2 = \sum g_{ij}(0,0,Z)^2 f_i(0,0,Z)^2$. Since the $g_{ij}(0,0,Z)$ are constant, this contradicts our assumption. ∎

Example 8.2 also settles a question of E. Becker. Becker asked if $B_1 = B$. Example 8.2 shows that this is not always the case.

References

[1] E. Becker and V. Powers, *Sums of powers in rings and the real holomorphy ring*. J. Reine Angew. Math **480**(1996), 71–103.

[2] J. Bochnak, M. Coste and M.-F. Roy, *Géométrie algébrique réelle*. Springer-Verlag, 1987.

[3] G. Choquet, *Lectures on analysis, Volume II*. Benjamin Math. Lecture Note Series, 1969.

[4] E. K. Haviland, *On the momentum problem for distribution functions in more than one dimension*. Amer. J. Math. **57**(1935), 562–572.

[5] ———, *On the momentum problem for distribution functions in more than one dimension II*. Amer. J. Math. **58**(1936), 164–168.

[6] T. Jacobi, *A representation theorem for certain partially ordered commutative rings*. Math. Z. **237**(2001).

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

[8] J. L. Kelley and T. P. Srinivasan, *Measure and Integral, Volume 1*. Graduate Texts in Math. **116**, Springer-Verlag, 1988.

https://doi.org/10.4153/CMB-2003-041-9 Published online by Cambridge University Press

[9] S. Kuhlmann and M. Marshall, *Positivity, sums of squares and the multi-dimensional moment problem*. Trans. Amer. Math. Soc. **354**(2002), 4285–4301.
[10] M. Marshall, *Extending the archimedean Positivstellensatz to the non-compact case*. Canad. Math. Bull. **44**(2001), 223–230.
[11] ———, *Positive polynomials and sums of squares*. Dottorato de Ricerca in Matematica, Dept. di Mat., Univ. Pisa, 2000.
[12] ———, *A general representation theorem for partially ordered commutative rings*. Math. Z. **242**(2002), 217–225.
[13] P. Parrilo and B. Sturmfels, *Minimizing polynomial functions*. DIMACS Series in Discrete Mathematics and Theoretical Computer Science, to appear.
[14] V. Powers and C. Scheiderer, *The moment problem for non-compact semialgebraic sets*. Adv. Geom. **1**(2001), 71–88.
[15] A. Prestel, *Lectures on formally real fields*. Springer Lecture Notes in Math. **1093**, 1984.
[16] M. Putinar, *Positive polynomials on compact semi-algebraic sets*. Indiana Univ. Math. J. (3) **42**(1993), 969–984.
[17] M. Putinar and F.-H. Vasilescu, *Solving the moment problem by dimension extension*. Ann. of Math. **149**(1999), 1087–1107.
[18] C. Scheiderer, *Sums of squares of regular functions on real algebraic varieties*. Trans. Amer. Math. Soc. **352**(1999), 1030–1069.
[19] K. Schmüdgen, *The K-moment problem for compact semi-algebraic sets*. Math. Ann. **289**(1991), 203–206.
[20] M. Schweighofer, *Iterated rings of bounded elements and generalizations of Schmüdgen's Positivstellensatz.* J. Reine Angew. Math. **554**(2003), 19–45.
[21] T. Wörmann, *Short algebraic proofs of theorems of Schmüdgen and Pólya*. preprint.

Department of Computer Science
University of Saskatchewan
Saskatoon, Saskatchewan
S7N 5E6
e-mail: marshall@math.usask.ca