Canad. Math. Bull. Vol. **44** (2), 2001 pp. 223–230

Extending the Archimedean Positivstellensatz to the Non-Compact Case

M. Marshall

Abstract. A generalization of Schmüdgen's Positivstellensatz is given which holds for any basic closed semialgebraic set in $\mathbb{R}^n$ (compact or not). The proof is an extension of Wörmann's proof.

The Positivstellensatz, proved by G. Stengle in [12], is a standard tool in real algebraic geometry; see [2] [5] [7]. In his solution of the K-moment problem in [11], Schmüdgen proves a surprisingly strong version of the Positivstellensatz in the compact case. Schmüdgen's result has since been extended and improved in various ways; see [1] [4] [6] [9] [10]. In the present paper we describe an extension in another direction, to the non-compact case.

Let V be an algebraic set in $\mathbb{R}^n$. The coordinate ring $\mathbb{R}[V]$ of V is the ring of all polynomial functions $f\colon V \to \mathbb{R}$. $\mathbb{R}[V]$ is generated as an $\mathbb{R}$-algebra by $x_1, \ldots, x_n$ where $x_i\colon V \to \mathbb{R}$ denotes the i-th coordinate function. For any finite subset $S = \{f_1, \ldots, f_r\}$ of $\mathbb{R}[V]$, let $K = K_S$ be the basic closed semialgebraic set in V defined by the r inequalities $f_i \geq 0$, $i = 1, \ldots, r$, *i.e.*,

$$K = \{a \in V \mid f_i(a) \geq 0, i = 1, \ldots, r\}$$

and let $T = T_S$ denote the preordering of $\mathbb{R}[V]$ generated by $f_1, \ldots, f_r$, *i.e.*, the set of all functions of the form $f = \sum_e s_e f_1^{e_1} \cdots f_r^{e_r}$, $e = (e_1, \ldots, e_r)$ running through the set $\{0,1\}^r$, where each s_e is a sum of squares in $\mathbb{R}[V]$. A basic version of the Positivstellensatz [7, Lemma 7.5] asserts that, for any $f \in \mathbb{R}[V]$,

$$f > 0 \text{ on } K \text{ iff } (1+s)f = 1+t \quad \text{for some } s, t \in T.$$

For more comprehensive formulations of the Positivstellensatz, see [2] [5] [7].

In [11], Schmüdgen proves, for K compact and $f \in \mathbb{R}[V]$, $f > 0$ on $K \Rightarrow f \in T$ or, equivalently,

$$f \geq 0 \text{ on } K \text{ iff } f + \epsilon \in T \quad \text{for any rational } \epsilon > 0.$$

We refer to this latter result as the archimedean Positivstellensatz. Schmüdgen's proof uses methods from functional analysis. In [13] [14] Wörmann gives an algebraic proof. As one might expect, both proofs rely heavily on the Positivstellensatz.

Received by the editors June 17, 1999.

This research was funded in part by NSERC of Canada. Part of the work was done while the author was on sabbatical leave at Universidad Complutense in Madrid. This part was funded by Universidad Complutense.

AMS subject classification: Primary: 12D15, 14P10; secondary: 44A60.

As is well-known, the Positivstellensatz remains true with $\mathbb{R}$ replaced by an arbitrary real closed field. This is not true for the archimedean Positivstellensatz. On the other hand, it is possible to extend the archimedean Positivstellensatz so as to include the case where K is not compact. This is the content of the present paper.

The idea is to replace the constant function 1 by any function $p \in 1 + T$ which grows sufficiently rapidly on K in the sense that there exists integers $M, k \geq 0$ such that $Mp^k \geq x_i \geq -Mp^k$ holds on K, $i = 1, \dots, n$. Such a function p always exists (see Note 1.5 below) and, for any such p, we prove (see Corollary 3.1 below) that

$$\begin{cases} f \geq 0 \text{ on } K \iff \exists \text{ an integer } m \geq 0 \text{ such that } \forall \text{ rational } \epsilon > 0, \\ \exists \text{ an integer } \ell \geq 0 \text{ such that } p^\ell(f + \epsilon p^m) \in T. \end{cases}$$

Of course, if K is compact then we can take $p = 1$ and what we have then is exactly the archimedean Positivstellensatz. For another (more complicated) variation of this same result, but with with '$f > 0$' replacing '$f \geq 0$', see Corollary 3.2 below. Our proof follows closely the form of Wörmann's proof given in [13] [14].

The author wishes to thank C. Andradas and E. Becker, for looking at early versions of the paper, and for providing useful comments.

1 Extension of a Result of Wörmann

Throughout, A denotes a commutative ring with 1 and Sper(A) denotes the real spectrum of A, *i.e.*, the set of all orderings of A [2] [5] [7]. A preordering of A is a subset T of A satisfying

$$T + T \subseteq T,\ TT \subseteq T \text{ and } a^2 \in T \quad \text{for all } a \in A.$$

If T is a preordering in A, $\mathrm{Sper}_T(A)$ denotes the set of orderings of A lying over T. For simplicity, we always assume $\mathbb{Q} \subseteq A$.

In his proof of the archimedean Positivstellensatz in [13] [14], Wörmann proves the following result in the case $B = \mathbb{R}$. Our proof is an easy generalization of Wörmann's proof.

Theorem 1.1 *Suppose B is a subring of A such that A is finitely generated over B, say $A = B[x_1, \dots, x_n]$, and T is a preordering of A such that, on $\mathrm{Sper}_T(A)$, each x_i is bounded by an element of $B \cap T$. Then, for each $a \in A$ there exists $b \in B \cap T$ such that $b \pm a \in T$.*

Recall that a preprime of A is a subset T of A such that

$$T + T \subseteq T, \quad TT \subseteq T, \quad \mathbb{Q}^+ \subseteq T, \quad \text{and} \quad -1 \notin T.$$

Note 1.2 For any preprime T of A, the set

$$C = \{a \in A \mid \exists b \in B \cap T \text{ such that } b \pm a \in T\}$$

https://doi.org/10.4153/CMB-2001-022-2 Published online by Cambridge University Press

is a subring of A. This follows from the identity

$$b_1 b_2 \pm a_1 a_2 = \frac{1}{2}(b_1 \mp a_1)(b_2 - a_2) + \frac{1}{2}(b_1 \pm a_1)(b_2 + a_2).$$

Any preordering is a preprime. If T is a preordering and $b - a^2 \in T$, $b \in B \cap T$, then $b + \frac{1}{4} \in T$ and $b + \frac{1}{4} \pm a = (b - a^2) + (a \pm \frac{1}{2})^2 \in T$. Thus, if $a^2 \in C$ then $a \in C$. More generally, if $b - (a_1^2 + \cdots + a_k^2) \in T$ for some $b \in B \cap T$, then $b - a_i^2 \in T$ so $a_i \in C$ for $i = 1, \ldots, k$. Also, since $b^2 - b^2 = 0 \in T$, b^2, and consequently b, lies in C for any $b \in B$, so $B \subseteq C$.

Proof of Theorem 1.1 Let $z = x_1^2 + \cdots + x_n^2$. By our assumption, there exists $c \in B \cap T$ such that $c - z > 0$ on $\mathrm{Sper}_T(A)$. By the (abstract) Positivstellensatz, there exists $p, q \in T$ such that $(1 + p)(c - z) = 1 + q$. Let $T' = T + (c - z)T$. Then $c - z \in T'$ so, by Note 1.2 (applied to T'), for every element $a \in A$, there exists $d \in B$ such that $d - a \in T'$, so $(d - a)(1 + p) \in T$. In particular, there exists $d \in B$ such that $(d - p)(1 + p) \in T$. Adding $(\frac{d}{2} - p)^2$, this yields $(d + \frac{d^2}{4}) - p \in T$. Multiplying this by $c \in T$ and adding $(1 + p)(c - z) \in T$, and $pz \in T$, this yields $c(1 + \frac{d}{2})^2 - z \in T$. Since $c(1 + \frac{d}{2})^2 \in B \cap T$, we are done, using Note 1.2 again (this time applied to T). ■

Corollary 1.3 *Suppose A is a finitely generated $\mathbb{R}$-algebra, say $A = \mathbb{R}[x_1, \ldots, x_n]$, T is a preordering of A, and p is an element of $1 + T$ such that $Mp^k \geq \pm x_i$ on $\mathrm{Sper}_T(A)$, $i = 1, \ldots, n$, for some integers $k, M \geq 0$. Then, for each $f \in A$, there exist integers $k, M \geq 0$ such that*

$$Mp^k \pm f \in T.$$

Proof Take $B = \mathbb{R}[p]$. The hypothesis implies that each x_i is bounded by an element of B on $\mathrm{Sper}_T(A)$, so, by Theorem 1.1, there exists $g \in B$ such that $g \pm f \in T$, say $g = \sum_{j=0}^{k} r_j p^j$. Take M to be any integer satisfying $M \geq \sum_{j=0}^{k} |r_j|$. Then, since $p - 1 \in T$, $Mp^k - g \in T$ so, adding, $Mp^k \pm f \in T$. ■

Corollary 1.4 *Suppose A is the coordinate ring of an algebraic set $V \subseteq \mathbb{R}^n$, $T = T_S$ for some finite subset S of A, and p is an element of $1 + T$ such that $Mp^k \geq |x_i|$ holds on K_S, $i = 1, \ldots, n$, for some integers $k, M \geq 0$. Then, for each $f \in A$, there exist integers $k, M \geq 0$ such that*

$$Mp^k \pm f \in T.$$

Proof By Tarski's Transfer Principle (*e.g.*, see [5]), since the inequality $Mp^k \geq \pm x_i$ holds on the set K_S, it holds on the bigger set $\mathrm{Sper}_T(A)$. ■

Note 1.5

(1) Such an element p always exists, *e.g.*, take

$$p = 1 + \sum_{i=1}^{n} x_i^2.$$

https://doi.org/10.4153/CMB-2001-022-2 Published online by Cambridge University Press

(2) Depending on the nature of $\mathrm{Sper}_T(A)$, there may be a "better" choice for p. For example:

- If each x_i is ≥ 0 on $\mathrm{Sper}_T(A)$ and $\sum x_i - 1 \in T$, we can take $p = \sum x_i$.
- If each x_i is bounded on $\mathrm{Sper}_T(A)$, we can take $p = 1$.

(3) The integers k, M such that $Mp^k \pm f \in T$ are difficult to estimate. If we know $Mp^k \pm x_i \in T$, $i = 1, \dots, n$, the identity in Note 1.2 yields $NM^d p^{kd} \pm f \in T$ where d is the degree of f (viewed as a polynomial in $x_1, \dots, x_n$) and N is any integer $\geq$ the sum of the absolute values of the coefficients. This estimate also applies to preprimes.

(4) If the $\mathbb{R}$-algebra A is not finitely generated, Corollary 1.3 may break down in various ways. In the ring of global real analytic functions on a real analytic manifold, for example, one does not normally expect $\exp(p)$ to be bounded by a polynomial in p. The preordering considered in [8] provides another example:

Example 1.6 Take A to be the polynomial algebra over $\mathbb{R}$ in countably many variables $X_1, X_2, \dots$ and let T be the preordering in A generated by the elements X_i and $(1 - X_i)(1 + X_{i+1})$, $i \geq 1$. Then

$$1 \geq X_i \geq 0$$

holds on $\mathrm{Sper}_T(A)$, so any $p \in 1 + T$ satisfies the hypothesis of Corollary 1.3. On the other hand, p does not satisfy the conclusion. There is some least integer $\ell \geq 0$ such that $p \in \mathbb{R}[X_1, \dots, X_\ell]$. Then, for any $f \in A$, if $Mp^k - f^2 \in T$ for some integers $k, M \geq 0$ then $f \in \mathbb{R}[X_1, \dots, X_\ell]$. The proof is the same as the proof of [8, Proposition 1]. $T = \cup_{n \geq 1} T_n$ where T_n denotes the preordering in $\mathbb{R}[X_1, \dots, X_n]$ generated by $X_1, \dots, X_n$ and $(1-X_i)(1+X_{i+1})$, $i = 1, \dots, n-1$. If $f \notin \mathbb{R}[X_1, \dots, X_\ell]$, then $Mp^k - f^2 \in T_n \setminus T_{n-1}$, $n > \ell$. By [8, Lemma 2], the leading coefficient of $Mp^k - f^2$, viewing $Mp^k - f^2$ as a polynomial in X_n, is $-g^2$, where g is the leading coefficient of f, and $-g^2 \in S_{n-1}$, the preordering in $\mathbb{R}[X_1, \dots, X_{n-1}]$ generated by X_i, $1 - X_i$, $i = 1, \dots, n - 1$. Since $S_{n-1} \cap -S_{n-1} = \{0\}$ [8, Lemma 1], this is impossible.

2 The Kadison-Dubois Theorem

The other ingredient in Wörmann's proof is the Kadison-Dubois Theorem. For T a preprime of A, let $X(T)$ denote the set of ring homomorphisms $\alpha\colon A \to \mathbb{R}$ such that $\alpha(T) \geq 0$. If A is the coordinate ring of a real algebraic set V, $X(T)$ is naturally identified with the set

$$\{a \in V \mid f(a) \geq 0 \text{ for all } f \in T\}.$$

If $T = T_S$, the preordering generated by some finite set S in A, this is just the set K_S considered at the beginning. The part of the Kadison-Dubois Theorem that we work with is the following:

Theorem 2.1 *Suppose T is a preprime of A which is Archimedean, i.e., for each $f \in A$, there exists an integer $M \geq 0$ such that $M \pm f \in T$. Then, for any $f \in A$, the following are equivalent:*

1. *$\alpha(f) \geq 0$ for each $\alpha \in X(T)$.*
2. *$f + \epsilon \in T$ for each rational $\epsilon > 0$.*

Proof See [3]. ∎

We use a certain self-strengthening of Theorem 2.1:

Theorem 2.2 *Suppose T is a preprime of A, and p is an element of $1 + T$ such that, for each $f \in A$, there exists integers $k, M \geq 0$ such that $Mp^k \pm f \in T$. Then, for any $f \in A$, the following are equivalent:*

1. *$\alpha(f) \geq 0$ for each $\alpha \in X(T)$.*
2. *For any sufficiently large integer m and for each rational $\epsilon > 0$, there exists an integer $\ell \geq 0$ such that $p^\ell(f + \epsilon p^m) \in T$.*

Note: If $p = 1$ this is just Theorem 2.1.

Proof Consider the localization $A[\frac{1}{p}]$ of A at p and the extension $T[\frac{1}{p}]$ of T to $A[\frac{1}{p}]$, and let

$$C = \left\{ f \in A\left[\frac{1}{p}\right] \;\middle|\; \text{there exists an integer } N \geq 0 \text{ such that } N \pm f \in T\left[\frac{1}{p}\right] \right\}.$$

Thus the preprime $T' := T[\frac{1}{p}] \cap C$ in C is Archimedean. Note: $1 \pm \frac{1}{p} \in T[\frac{1}{p}]$ (since $p \in 1+T$), so $\frac{1}{p} \in T'$. Also, for each $f \in A$, $\frac{f}{p^k} \in C$ for some $k \geq 0$, so $C[p] = A[\frac{1}{p}]$. Also, we have

$$X(T) \simeq X\Big(T\Big[\frac{1}{p}\Big]\Big) \hookrightarrow X(T'),$$

the latter map being restriction. The image of $X(T[\frac{1}{p}])$ in $X(T')$ consists of those α in $X(T')$ satisfying $\alpha(\frac{1}{p}) \neq 0$ (so $\alpha(\frac{1}{p}) > 0$.) Now fix $f \in A$ and pick m so large that $\frac{f}{p^{m-1}} \in C$. If (1) holds, then $\alpha(\frac{f}{p^m}) \geq 0$ for all $\alpha \in X(T')$ so, by Theorem 2.1, $\frac{f}{p^m} + \epsilon \in T'$ for all rational $\epsilon > 0$ and, clearing fractions, $p^\ell(f + \epsilon p^m) \in T$ for sufficiently large $\ell \geq 0$. Conversely, if (2) holds, then dividing by $p^{m+\ell}$, $\frac{f}{p^m} + \epsilon \in T'$ for all rational $\epsilon > 0$ so, by Theorem 2.1, $\alpha(\frac{f}{p^m}) \geq 0$ for all $\alpha \in X(T')$. Clearly this implies $\alpha(f) \geq 0$ for all $\alpha \in X(T)$. ∎

Remark 2.3

(1) It is possible to generalize Theorem 2.2, replacing the set $\{p^k \mid k \geq 0\}$ by any multiplicative set in $1 + T$.

(2) If the image of $X(T)$ is dense in $X(T')$, we can replace m by $m - 1$ in the above argument.

https://doi.org/10.4153/CMB-2001-022-2 Published online by Cambridge University Press

(3) If $A = \mathbb{R}[x_1, \dots, x_n]$, the ring C in the proof can be replaced by a ring which is finitely generated over $\mathbb{R}$. For example, we can fix $k, M \geq 0$ so that $Mp^k \pm x_i \in T$, $i = 1, \dots, n$ and take

$$C = \mathbb{R}\Big[\frac{x_1}{p^k}, \dots, \frac{x_n}{p^k}, \frac{1}{p}\Big].$$

Also, if we decompose f as $f = \sum_{j=0}^{d} f_j(x_1, \dots, x_n)$ where f_j is homogeneous of degree j, then

$$\frac{f}{p^{kd}} = \sum_{j=0}^{n} \frac{1}{p^{k(d-j)}} f_j\Big(\frac{x_1}{p^k}, \dots, \frac{x_n}{p^k}\Big) \in C,$$

so we can take $m = kd + 1$.

The following example, pointed out to the author by E. Becker, is closely related to the proof of the theorem of Pólya given in [13] [14].

Example 2.4 Let A to be the polynomial ring $\mathbb{R}[X_1, \dots, X_n]$, T the preprime in A generated by $\mathbb{R}^+, X_1, \dots, X_n, \sum X_i - 1$ and take $p = \sum X_i$. Then $p \in 1 + T$ and $p \pm X_i \in T$, $i = 1, \dots, n$, so the hypothesis of Theorem 2.2 is satisfied. By the above remark, we can take

$$C = \mathbb{R}\Big[\frac{X_1}{p}, \dots, \frac{X_n}{p}, \frac{1}{p}\Big].$$

$X(T)$ is identified with

$$\Big\{a \in \mathbb{R}^n \mid a_i \geq 0, \sum a_i \geq 1\Big\},$$

$X(T')$ is identified with

$$\Big\{(b, c) \in \mathbb{R}^{n+1} \mid b_i \geq 0, \sum b_i = 1, 1 \geq c \geq 0\Big\},$$

and the image of $X(T)$ in $X(T')$ is identified with

$$\Big\{(b, c) \in \mathbb{R}^{n+1} \mid b_i \geq 0, \sum b_i = 1, 1 \geq c > 0\Big\}.$$

The image of $X(T)$ is dense in $X(T')$. By the above remark, if $d = \deg(f)$, then $\frac{f}{p^d} \in C$, and we can take $m = d$. Thus we have the following:

Corollary 2.5 *Let T be the preprime in the polynomial ring $\mathbb{R}[X_1, \dots, X_n]$ generated by $\mathbb{R}^+$, $X_1, \dots, X_n$ and $\sum X_i - 1$, and let $p = \sum X_i$. Then a polynomial $f \in \mathbb{R}[X_1, \dots, X_n]$ of degree d is non-negative on the set $\{a \in \mathbb{R}^n \mid a_i \geq 0, \sum a_i \geq 1\}$ iff for all rational $\epsilon > 0$ there exists an integer $\ell \geq 0$ such that $p^\ell(f + \epsilon p^d) \in T$.*

3 Extension of the Archimedean Positivstellensatz

We return now to the geometric set-up considered at the beginning. *i.e.*, V is an algebraic set in $\mathbb{R}^n$ with coordinate ring $\mathbb{R}[V] = \mathbb{R}[x_1, \dots, x_n]$, $S = \{f_1, \dots, f_r\}$ is a finite subset of $\mathbb{R}[V]$, $T = T_S$, the preordering of $\mathbb{R}[V]$ generated by $f_1, \dots, f_r$, and

$$K = K_S = \{a \in V \mid f_i(a) \geq 0, i = 1, \dots, r\}.$$

Corollary 3.1 *Suppose $p \in 1 + T$ is chosen so that there exist integers $k, M \geq 0$ such that $Mp^k \geq |x_i|$ holds on K, $i = 1, \dots, n$. Then, for any $f \in \mathbb{R}[V]$, the following are equivalent:*

(1) f is non-negative on K.
(2) For any sufficiently large integer m and for all rational $\epsilon > 0$, there exists an integer $\ell \geq 0$ such that $p^\ell(f + \epsilon p^m) \in T$.

Proof By Corollary 1.4, we are in a position to apply Theorem 2.2. Since $X(T)$ is identified with K, this gives us what we want. ■

Corollary 3.2 *Suppose $p \in 1 + T$ is chosen so that there exist integers $k, M \geq 0$ such that $Mp^k \geq |x_i|$ holds on K, $i = 1, \dots, n$. Then, for any $f \in \mathbb{R}[V]$, the following are equivalent:*

(1) f is strictly positive on K.
(2) There exists $k \geq 0$ and a rational $\epsilon > 0$ such that $p^k f \geq \epsilon$ on K.
(3) There exists $k \geq 0$ and a rational $\epsilon_1 > 0$ such that for any sufficiently large integer m and for all rational $\epsilon_2 > 0$, there exists an integer $\ell \geq 0$ such that $p^\ell(p^k f - \epsilon_1 + \epsilon_2 p^m) \in T$.

Proof (2) $\Rightarrow$ (1) is clear, and (2) $\Leftrightarrow$ (3) is immediate from Corollary 3.1, so it only remains to check (1) $\Rightarrow$ (2). By the Positivstellensatz, $rf = 1 + s$ for some $r, s \in T$. Choose kk L so large that $Lp^k \geq r$ on K. Then $Lp^k f \geq rf = 1 + s \geq 1$, so $p^k f \geq \frac{1}{L}$ on K. ■

Of course, there are always plenty of choices for p; see Note 1.5. Also, if K is compact, one can take $p = 1$, and what we have then is just the archimedean Positivstellensatz.

Remark 3.3 Corollary 1.4 carries over, suitably generalized, to an arbitrary real closed field R. The results in Section 3 cannot be so extended (unless R is archimedean) because they depend, in an essential way, on the Kadison-Dubois Theorem. The Kadison-Dubois Theorem tells only about the meaning of the statement '$f \geq 0$' on $X(T)$. In the non-archimedean situation, $X(T) = \varnothing$, so this has nothing much to do with the basic closed set K.

References

[1] F. Acquistapace, C. Andradas and F. Broglia, *The strict Positivstellensatz for global analytic functions and the moment problem for semianalytic sets*. preprint.
[2] C. Andradas, L. Bröcker and J. M. Ruiz, *Constructible sets in real geometry*. Ergeb Math., Springer, Berlin, Heidelberg, New York, 1996.
[3] E. Becker and N. Schwartz, *Zum Darstellungssatz von Kadison-Dubois*. Arch. Math. **39**(1983), 421–428.
[4] R. Berr and T. Wörman, *Positive polynomials and tame preorderings*. Math. Z., (to appear).
[5] J. Bochnak, M. Coste and M. F. Roy, *Géométrie Algébrique Réelle*. Ergeb Math., Springer, Berlin, Heidelberg, New York, 1987.
[6] T. Jacobi, *A representation theorem for certain partially ordered commutative rings*. Math. Z., (to appear).
[7] T. Y. Lam, *An introduction to real algebra*. Rocky Mountain J. Math. **14**(1984), 767–814.
[8] M. Marshall, *A real holomorphy ring without the Schmüdgen property*. Canad. Math. Bull. **42**(1999), 354–358.
[9] J. P. Monnier, *Anneaux d'holomorphie et Positivstellensatz archimédien*. Manuscripta Math. **97**(1998), 269–302.
[10] M. Putinar, *Positive polynomials on compact semi-algebraic sets*. Indiana Univ. Math. J. **42**(1993), 969–984.
[11] K. Schmüdgen, *The K-moment problem for compact semialgebraic sets*. Math. Ann. **289**(1991), 203–206.
[12] G. Stengle, *A Nullstellensatz and a Positivstellensatz in semialgebraic geometry*. Math. Ann. **207**(1974), 67–97.
[13] T. Wörmann, *Short algebraic proofs of theorems of Schmüdgen and Pólya*. preprint.
[14] ———, *Strikt positive Polynome in der semialgebraischen Geometrie*. PhD Thesis, Dortmund, 1998.

Department of Mathematics and Statistics
University of Saskatchewan
Saskatoon, Saskatchewan
S7N 0W0
e-mail: marshall@math.usask.ca