Non-negative Polynomials on Compact Semi-algebraic Sets in One Variable Case

A Thesis Submitted to the
College of Graduate Studies and Research
in Partial Fulfillment of the Requirements
for the degree of Master of Science
in the Department of Mathematics and Statistics
University of Saskatchewan
Saskatoon

By

Wei Fan

Permission to Use

Head of the Department of Mathematics and Statistics
University of Saskatchewan
Saskatoon, Saskatchewan, Canada
S7N 5E6

Abstract

Positivity of polynomials, as a key notion in real algebra, is one of the oldest topics. In a given context, some polynomials can be represented in a form that reveals their positivity immediately, like sums of squares. A large body of literature deals with the question which positive polynomials can be represented in such a way.

The milestone in this development was Schmüdgen's solution of the moment problem for compact semi-algebraic sets. In 1991, Schmüdgen proved that if the associated basic closed semi-algebraic set K_S is compact, then any polynomial which is strictly positive on K_S is contained in the preordering T_S.

Putinar considered a further question: when are 'linear representations' possible? He provided the first step in answering this question himself in 1993. Putinar proved if the quadratic module M_S is archimedean, any polynomial which is strictly positive on K_S is contained in M_S, i.e., has a linear representation.

In the present thesis, we concentrate on the linear representations in the one variable polynomial ring. We first investigate the relationship of the two conditions in Schmüdgen's Theorem and Putinar's Criterion: K_S compact and M_S archimedean. They are actually equivalent. We find another proof for this result and hereby we can improve Schmüdgen's Theorem in the one variable case.

Secondly, we investigate the relationship of M_S and T_S. We use elementary arguments to prove in the one variable case when K_S is compact, they are equal.

Thirdly, we present Scheiderer's Main Theorem with a detailed proof. Scheiderer established a local-global principle for the polynomials non-negative on K_S to be contained in M_S in 2003. This principle which we call Scheiderer's Main Theorem here extends Putinar's Criterion.

Finally, we consider Scheiderer's Main Theorem in the one variable case, and give a simplified version of this theorem. We also apply this Simple Version of the Main Theorem to give some elementary proofs for existing results.

Acknowledgements

I would like to express my sincere thanks to my supervisors, Professor M. Marshall and S. Kuhlmann, for their invaluable advice and patient guidance during my studies and the preparation of the thesis.

At the same time, I would also like to express my thanks to all members of my advisory committee for taking the time and effort to read this thesis.

My appreciation is also expressed to those professors with whom there was an opportunity to take at least a course.

Thanks to the Department of Mathematics and Statistics and the University of Saskatchewan for their financial support during my studies.

Last but not least, I want to thank my family and friends, for their moral support and encouragement.

Dedicated to

My Parents

Contents

Chapter 1

Positive Polynomials

Positivity is one of the most basic mathematical concepts. In many areas of mathematics (like analysis, real algebraic geometry, functional analysis, etc.) it shows up as positivity of a polynomial on a certain subset of $\mathbb{R}^n$ which itself is often given by polynomial inequalities. Positivity of polynomial functions is among the most classic topics in real algebraic geometry, but it is still a very active area of research.

1.1 Hilbert's 17th Problem

Hilbert's occupation with sums of squares representations of positive polynomials has, in many ways, triggered what today we consider as modern real algebra.

As standard, let $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ denote the set of natural numbers, the ring of integers, the field of rationals and the field of real numbers, respectively. Let $\mathbb{N}^+$, $\mathbb{Z}^+$, $\mathbb{Q}^+$ and $\mathbb{R}^+$ denote the non-negative elements of $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$, respectively. $\mathbb{R}[x_1, ..., x_n]$ denotes the ring of polynomials of n variables, $x_1, ..., x_n$ with real coefficients. It can be defined inductively: $\mathbb{R}[x_1, ..., x_n] = \mathbb{R}[x_1, ..., x_{n-1}][x_n]$. We also denote it by $\mathbb{R}[X]$ for short. Thus X is shorthand for the n-tuple of variables

$(x_1, ..., x_n)$. For $f \in \mathbb{R}[X]$ and $x = (x_1, ..., x_n) \in \mathbb{R}^n$, $f(x) \in \mathbb{R}$ denotes the result of evaluating f at x.

A polynomial $f \in \mathbb{R}[X]$ is said to be positive semidefinite (psd for short) if it has non-negative values on all of $\mathbb{R}^n$. i.e.,

$$f(x) \geq 0 \qquad \text{for any } x \in \mathbb{R}^n.$$

It is easy to see there is a 'simple' sufficient condition for f to be psd: f can be decomposed as a finite sum of squares. i.e.,

$$f = \textstyle\sum_{i=1}^m f_i^2, \qquad f_i \in \mathbb{R}[X].$$

If $n = 1$, then conversely every psd is a sum of squares, actually, a sum of two squares. To see this, we use the factorization in the one variable polynomial ring $\mathbb{R}[x]$: If $f(x) \geq 0$ for all $x \in \mathbb{R}$, then

$$f = d^2 \textstyle\prod_i (x - a_i)^{k_i} \prod_j ((x - b_j)^2 + c_j^2)^{l_j},$$

where $d \in \mathbb{R}$, $k_i, l_j \in \mathbb{N}$ with k_i even.

The two squares identity: $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$ tells us the product of sums of two squares is equal to a sum of two squares. Applying it to $\prod_j ((x - b_j)^2 + c_j^2)^{l_j}$ yields

$$\textstyle\prod_j ((x - b_j)^2 + c_j^2)^{l_j} = p(x)^2 + q(x)^2 \text{ for some } p(x),\ q(x) \in \mathbb{R}[x].$$

Therefore, $f(x) = g(x)^2 + h(x)^2$, where $g(x) = d \prod_i (x - a_i)^{k_i/2} p(x)$, $h(x) = d \prod_i (x - a_i)^{k_i/2} q(x)$.

For every $n \geq 2$, Hilbert (1888) showed that there exist psd polynomials in n variables which cannot be written as a sum of squares of polynomials. Hilbert proved this result in a non-constructive way. The following is a summary of Hilbert's original argument: (It is only a rough idea of the proof; Hilbert's original proof is very involved.)

Proof. ([Re, p.253]) Let $\phi(x, y)$ and $\varphi(x, y)$ be two real cubic polynomials with no non-constant factor, and with common zeros at $\{P_1, ..., P_9\} \subset \mathbb{R}^2$. (By Bezout's Theorem, nine is the maximum number of common zeros of two cubics.) It is well-known that any cubic $h(x, y)$ that vanishes at eight of the P_j's must vanish at the ninth. Choose a quadratic polynomial $f(x, y) \neq 0$ that vanishes at P_1, P_2, P_3, P_4, and P_5 and a quadric polynomial $g(x, y) \neq 0$ that vanishes at P_1, P_2, P_3, P_4, and P_5 and is singular at P_6, P_7 and P_8. (Such curve exists by constant-counting arguments: there are 5 conditions on f and $\binom{4}{2} = 6$ coefficients in a quadratic, and $5+3\times 3 = 14$ conditions on g and $\binom{6}{2} = 15$ coefficients in a quadratic.) It can be shown that there exists λ so that

$$F(x, y) := \phi^2(x, y) + \varphi^2(x, y) + \lambda f(x, y)g(x, y) \geq 0.$$

for all real (x, y), and that $F(P_j) = 0$ for $1 \leq j \leq 8$, but $F(P_9) > 0$. If $F = \sum_k h_k^2$, then each h_k is a cubic and $h_k(P_j) = 0$ for $1 \leq j \leq 8$, hence $h_k(P_9) = 0$ for all k, contradicting $\sum_k h_k^2(P_9) = F(P_9) > 0$. □

For a long time it was a challenge to name a specific polynomial that is positive semi-definite on the plane, but is not a sum of squares. The first explicit example was found by Motzkin in 1967 [Mo]:

$$f(x, y) = 1 - 3x^2y^2 + x^2y^4 + x^4y^2. \tag{1.1}$$

In his 1900 address to the International Congress of Mathematics in Paris [Hi2], Hilbert posed his famous 17th question, now known as Hilbert's 17th problem:

Must every psd polynomial f be a sum of squares of rational functions?

He was able to prove the case for $n = 2$ (1893) [Hi1]. For more than two variables, however, he found himself unable to prove this. The question was later decided in the positive by Emil Artin (1927) [Ar], using the Artin-Schreier theory of real closed fields:

Theorem 1.1.1. Let R be a real closed field, and let f be a psd polynomial in $R[X]$. Then there exists an identity

$$fh^2 = f_1^2 + ... + f_r^2$$

where $h \neq 0$ and $f_1, ..., f_r$ are polynomials in $R[X]$.

1.2 Main Problem

Even though Hilbert gave a negative answer to the statement that every psd polynomial in n variables can be decomposed as a sum of squares of polynomials, it was the beginning of a very fruitful development.

The concepts defined following will be defined formally in Chapter II. Let S be a finite subset of the polynomial ring $\mathbb{R}[X]$, $S = \{g_1, g_2, ..., g_s\}$. We define $K = K_S := \{p \in \mathbb{R}^n \mid \forall g \in S, g(p) \geq 0\}$. It is called the *basic closed semialgebraic set in* $\mathbb{R}^n$ *generated by* S. Let us denote by T_S^{alg} the set

$$\{f \in \mathbb{R}[X] |\ f \geq 0 \text{ on } K_S\}.$$

Let T_S denote the *preordering in* $\mathbb{R}[X]$ *generated by* S, i.e.,

$$T_S = \{\sum_{e\in\{0,1\}^s} \sigma_e g^e : \ \sigma_e \in \sum \mathbb{R}[X]^2\},$$

where $g^e := g_1^{e_1}...g_s^{e_s}$, and $\sum\mathbb{R}[X]^2$ denotes the set of all sums of squares in $\mathbb{R}[X]$. i.e., $\sum\mathbb{R}[X]^2 := \{f \in\mathbb{R}[X] \mid f = \sum_{i=1}^m f_i^2$, where $f_i \in\mathbb{R}[X]\}$.

Let M_S denote the *quadratic module in* $\mathbb{R}[X]$ *generated by* S, i.e.,

$$M_S = \{\sigma_0 + \sigma_1 g_1 + ... + \sigma_s g_s |\ \sigma_i \in \sum\mathbb{R}[X]^2,\ i = 0, 1, ..., s\}.$$

The quadratic module M_S is said to be *archimedean* if for all $f \in \mathbb{R}[x]$, there exists an integer $n \geq 1$ such that $n \pm f \in M_S$.

Now we consider the following important question:

What are the characterizations of the polynomials which are non-negative on K_S *(i.e.,* $f \in T_S^{alg}$*)?*

Our first guess might be that

$$f \in T_S^{alg} \Leftrightarrow f \in T_S$$

or

$$f \in T_S^{alg} \Leftrightarrow f \in M_S$$

Unfortunately, this is not true: When S is empty, $K_S = \mathbb{R}^n$, it becomes our original question discussed in last section, to which Hilbert already gave a negative answer. However another question arises:

(*) Is it possible to impose conditions on K_S that ensure $T_S^{alg} = T_S$ or $T_S^{alg} = M_S$?

Two celebrated results answered this question partially:

Theorem 1.2.1. (Schmüdgen's Theorem (1991) [Sc, Cor 3]) If $S = \{g_1, ..., g_s\}$ is a finite subset of $\mathbb{R}[X]$ such that the closed semi-algebraic set $K_S = \{x \in \mathbb{R}^n \mid \forall g \in S, g(x) \geq 0\}$ is compact then,

$$\forall f \in \mathbb{R}[X],\ f > 0 \text{ on } K_S \Rightarrow f \in T_S.$$

Theorem 1.2.2. (Putinar's Theorem (1993) [P, Th 1.4]) Suppose $S = \{g_1, ..., g_s\}$ is a finite subset of $\mathbb{R}[X]$ such that the quadratic module M_S generated by S is archimedean, then,

$$\forall f \in \mathbb{R}[X],\ f > 0 \text{ on } K \Rightarrow f \in M_S.$$

Remark 1.2.1. Schmüdgen was motivated by a problem in functional analysis, which is called *Moment Problem*. Part of the importance of Schmüdgen's Theorem is that it solves the moment problem for all compact basic closed semi-algebraic sets K. We will talk about these two theorems in more detail in the next chapter.

However, we can see that both of the two theorems only work for the f which are strictly positive on K_S. What can we say when f is non-negative on K_S, i.e., $f \in T_S^{alg}$? It will be more complicated to determine: Many examples are known such that $f \geq 0$ on K_S with K_S compact (M_S archimedean), but $f \notin T_S$ (M_S).

Example 1.2.3. Take $n = 1$, $S = \{x^3, 1 - x\}$. Then $K_S = [0, 1]$ is compact, $x \geq 0$ on K_S, but $x \notin T_S$. For suppose

$$x = t_0 + t_1 x^3 + t_2(1 - x) + t_3 x^3(1 - x),\ t_0, t_1, t_2, t_3 \in \mathbb{R}[x]^2.$$

Say $t_0 = \sum f_i^2$. Evaluating at 0 yields $t_0(0) + t_2(0) = 0$, so $t_0(0) = \sum f_i(0)^2 = 0$, so $f_i(0) = 0$. Thus $f_i = x g_i$ so $t_0 = x^2 t_0'$ where $t_0' = \sum g_i^2$. Similarly, $t_2 = x^2 t_2'$ where $t_2' = \sum h_i^2$. Substituting and cancelling x, this yields

$$1 = xt_0' + x^2t_1 + x(1-x)t_2' + x^2(1-x)t_3$$

Evaluating at $x = 0$ yields $1 = 0$, a contradiction.

In 2003, Scheiderer gave a sufficient condition for $f \in \mathbb{R}[X]$, $f \geq 0$ on K_S to imply that $f \in M_S$ (which is called the Scheiderer's Main Theorem in this thesis) in [S4, Th 2.8].

Theorem 1.2.4. (Scheiderer's Main Theorem): Suppose S is a finite subset in $\mathbb{R}[X]$. K is the basic closed semi-algebraic set generated by S and M is the quadratic module generated by S. If M is archimedean, $f \geq 0$ on K and $\mathbb{R}[X]/J$ has (Krull) dimension ≤ 0, where $J := (M+(f)) \cap -(M+(f))$. Then the following are equivalent:

(1) $f \in M$.

(2) For each $a = (a_1, ..., a_n) \in K$ with $f(a) = 0$, f lies in the closed quadratic module in $\widehat{\mathbb{R}[X]}_a$ generated by M. Here, $\widehat{\mathbb{R}[X]}_a$ denotes the power series ring $\mathbb{R}[[t_1, ..., t_n]]$, where $t_i = x_i - a_i$, $i = 1, ..., n$. (The *closed quadratic module in* $\widehat{\mathbb{R}[X]}_a$ *generated by* M is $\hat{M} := \underleftarrow{lim}(M + I^k)/I^k$, where $I = (x_1 - a_1, ..., x_n - a_n)$. See chapter IV for details.)

Scheiderer established a similar criterion in the preordering case first in [S3, Cor 3.17]. Theorem 1.2.4 extends this criterion to the quadratic module case. The original version of this theorem obtained by Scheiderer is actually much more general, applying to any Noetherian ring A, instead of the polynomial ring $\mathbb{R}[X]$ (see Th 4.1.4). By this Main Theorem, Scheiderer gives an answer to (*) in the low dimension case (since the assumption of the theorem requires $\mathbb{R}[X]/J$ has dimension ≤ 0).

In my thesis, I will concentrate on the one variable case, (i.e., $\mathbb{R}[X] = \mathbb{R}[x]$, the polynomial ring in one variable) and give some elementary proofs for the existing results.

In chapter III, I will use elementary arguments to prove in the one variable case, K_S compact implies M_S archimedean and $M_S = T_S$. Whether K_S compact implies $M_S = T_S$ was an open question posed by S. Kuhlmann, M. Marshall and N. Schwartz in [K-M-S]. Scheiderer first settled this question as an application of his Main Theorem. In chapter IV, I will give a detailed proof (quoted from [M4]) of the Main Theorem based on the knowledge of abstract algebra and some commutative algebra. In chapter V, I will give a simplified Scheiderer's Main Theorem in the one variable case which is easier to understand and apply this simple version of Main Theorem to prove $M_S = T_S$ in a different way from chapter III. I will also give a criterion (Th 5.2.5) to answer (*) in the one variable case. This criterion is already known in [K-M-S, Th 3.2], and it is just a special case of a general criterion for curves proved by Scheiderer in [S3, Th 5.17]. Here I will apply the simple version of Main Theorem to give another proof.

In the next chapter, I will introduce some terminology and give a brief overview of some classical results which are related to my thesis.

Chapter 2

Some Classical Results

Starting with Hilbert's question whether every nonnegative real polynomial in several variables is a sum of squares of real rational functions, many questions arose in this field and many interesting results are known. In this chapter, I will give a quick review of some of the most famous results.

2.1 Basic Terminology

As stated in last chapter, Schmüdgen's 1991 paper settles the Moment Problem (see section 4) in the compact case. In [Sc], Schmüdgen uses Stengle's Positivstellensatz (see section 2) to give a representation of polynomials strictly positive on a bounded basic closed semi-algebraic set in $\mathbb{R}^n$. In [P], Putinar gives a criterion for linear 'representations' to exist. Jacobi and Prestel show how Schmüdgen's representation can be improved and determine when the linear representations considered by Putinar are possible. Schmüdgen and Putinar use methods from functional analysis. In [W1], Wörmann uses the Kadison-Dubois theorem (see section 3) to give a purely algebraic proof of Schmüdgen's result. In [J], Jacobi proves a new variant of Kadison-Dubois theorem (see section 5) and uses this to give an algebraic proof of Putinar's criterion for linear representations. Before reaching these classical results, we need to be familiar with some basic terminology.

We first look at the abstract definitions of preorderings and quadratic modules, which are very important concepts in Real Algebra and Real Algebraic Geometry.

Let A be a commutative ring with 1. For simplicity assume $\mathbb{Q}\subseteq A$. $\sum A^2$ denotes the set of all finite sums of squares, i.e. $\{\sum_{i=1}^m a_i^2 | \ a_i \in A \text{ and } m \in\mathbb{N}\}$.

A *preordering* in A is a subset T of A such that $T+T \subseteq T, TT \subseteq T$, and $a^2 \in T$ for all $a \in A$. Clearly, $\sum A^2$ is a preordering of A and $\sum A^2 \subseteq T$ for any preordering T of A. The set T enjoys the baisc properties of “positive” elements. The most prominent examples are:

(i)Any subring A of the field $\mathbb{R}$ of real numbers, where T consists of those elements of A that are nonnegative in $\mathbb{R}$.

(ii)The ring $C(\chi, \mathbb{R})$ of all continuous functions from a nonempty topological space χ to $\mathbb{R}$, where T consists of those functions f such that $f(x) \geq 0$ for all $x \in \chi$.

The *preordering generated by some finite subset* $S = \{g_1, ..., g_s\}$ of A, i.e., the smallest preordering of A containing the elements $g_1, ..., g_s$, consists of all finite sums of terms of the form

$$\sigma g_1^{e_1} ... g_s^{e_s}, \qquad \sigma \in \sum A^2, e_i \in \{0,1\}, i = 1, ..., s.$$

We denote this preordering by T_S. Thus, if we use the standard shorthand g^e for $g_1^{e_1} ... g_s^{e_s}$, where $e = (e_1, ..., e_s)$, then

$$T_S = \{\textstyle\sum_{e\in\{0,1\}^s} \sigma_e g^e | \ \sigma_e \in \sum A^2 \text{ for all } e \in \{0,1\}^s\}.$$

For example, if $S = \{g\}$, $T_{\{g\}} = \sum A^2 + \sum A^2 g$;

if $S = \{g, h\}$, $T_{\{g,h\}} = \sum A^2 + \sum A^2 g + \sum A^2 h + \sum A^2 gh$.

A *preprime* of A is a subset T of A such that $T+T \subseteq T$, $TT \subseteq T$, and $\mathbb{Q}^+ \subseteq T$, where $\mathbb{Q}^+$ denotes the set of non-negative rationals.

A preprime T of A is said to be *archimedean* if for all $a \in A$, there exists an integer $n \geq 1$ such that $n \pm a \in T$.

A preprime T of A is said to be *generating* if $T - T = A$.

Remark 2.1.1. (1) For any preprime T of A, $T-T$ is a subring of A. $\Big(1 = 1-0 \in T-T$; $0 = 0-0 \in T-T$; $(t_1-t_2)+(t_3-t_4) = (t_1+t_3)-(t_2+t_4) \in T-T$; $(t_1-t_2)(t_3-t_4) = (t_1t_3+t_2t_4)-(t_1t_4+t_2t_3) \in T-T$; $-(t_1-t_2) = t_2-t_1 \in T-T.\Big)$

(2) $\mathbb{Q}^+$ is the unique smallest preprime of A, $\mathbb{Q}^+ - \mathbb{Q}^+ = \mathbb{Q}$, so $\mathbb{Q}^+$ is not generating unless $A = \mathbb{Q}$.

(3) If T is archimedean, then T is generating. (For $\forall a \in A$, $a = (a+n)-n \in T-T$)

(4) Any preordering T of A is also a preprime of A and it is generating. $\Big(\forall \frac{m}{n} \in \mathbb{Q}^+$, $\frac{m}{n} = (\frac{1}{n})^2(nm) = (\frac{1}{n})^2 + ... + (\frac{1}{n})^2 \in T$; $\forall a \in A$, $a = (\frac{a+1}{a})^2 - (\frac{a-1}{a})^2 \in T-T.\Big)$

Let T be a preprime of A, a subset M of A is said to be a T*-module* if $M+M \subseteq M$, $TM \subseteq M$, and $1 \in M$ (i.e. $T \subseteq M$).

A T-module M of A is said to be *archimedean* if for all $a \in A$, there exists an integer $n \geq 1$ such that $n \pm a \in M$.

Remark 2.1.2. (1) T itself is a T-module.

(2) If T is archimedean then any T-module M is also archimedean (since $T \subseteq M$).

Especially, we call a $\sum A^2$-module a *quadratic module*, i.e., a subset M of A such that $M+M \subseteq M, 1 \in M$ and $a^2M \subseteq M$ for all $a \in A$.

Remark 2.1.3. (1) A preordering T is a quadratic module which is also closed under multiplication. This is clear.

(2) The identity $a = (\frac{a+1}{2})^2 - (\frac{a-1}{2})^2$ implies that if $-1 \in M$, then $M = A$. We say the quadratic module M is *proper* if $-1 \notin M$.

The *quadratic module of A generated by some finite subset* $S = \{g_1, ..., g_s\}$ of A, i.e., the smallest quadratic module of A containing the elements $g_1, ..., g_s$ consists of all finite sums of terms of the form

$$\sigma_i g_i, \qquad \text{where } g_0 = 1,\ \sigma_i \in \sum A^2,\ i = 0, 1, ..., s.$$

We denote this quadratic module by M_S. Then

$$M_S = \{\sigma_0 + \sigma_1 g_1 + ... + \sigma_s g_s \mid \sigma_i \in \sum A^2,\ i = 0, 1, ..., s\}.$$

Note: In the special case $A = \mathbb{R}[X]$, these abstract definitions coincide with those we introduced in last chapter.

2.2 Stengle's Positivstellensatz

As the name indicates, the Positivstellensatz (resp. Nichtnegativstellensatz) describe the polynomials which are strictly (resp. non-strictly) positive on the set K_S. Different kinds of Positivstellensatz and Nichtnegativstellensatz give representations of polynomials with certain properties on semi-algebraic sets.

In 1991, Schmüdgen proved a surprisingly strong version of Positivstellensatz about the representation of positive definite polynomials on a compact basic closed semi-algebraic set using methods from functional analysis in conjunction with Stengle's Positivstellensatz. Later Wörmann gave a purely algebraic proof based on the Kadison-Dubois Theorem. In this section, I will introduce Stengle's Positivstellensatz, which is a standard tool in Real Algebraic Geometry.

We continue to denote the polynomial ring $\mathbb{R}[x_1, ..., x_n]$ by $\mathbb{R}[X]$. Fix a finite subset $S = \{g_1, ...g_s\}$ of $\mathbb{R}[X]$. Let $K = K_S = \{x \in \mathbb{R}^n \mid g_i(x) \geq 0, i = 1, ..., s\}$. Let $T = T_S$, the preordering on $\mathbb{R}[X]$ generated by S. Recall T_S^{alg} denotes the set $\{f \in \mathbb{R}[X] \mid f \geq 0 \text{ on } K_S\}$. The study of the relationship between T_S^{alg} and T_S goes back at least to Hilbert and is a corner stone of modern semi-algebraic geometry. The following is a version of the Positivstellensatz proved by G. Stengle in 1974 [St, Ths 1,3,4].

Theorem 2.2.1. (Stengle's Positivstellensatz): Suppose S is a finite subset of $\mathbb{R}[X]$, $K = K_S$, $T = T_S$ defined as in the last chapter. Then, for any $f \in \mathbb{R}[X]$,

(1) $f > 0$ on $K_S \Leftrightarrow$ there exist p, $q \in T_S$ such that $pf = 1 + q$.

(2) $f \geq 0$ on K_S ($i.e.$, $f \in T_S^{alg}$) $\Leftrightarrow$ there exists an integer $m \geq 0$ and $p, q \in T_S$ such that $pf = f^{2m} + q$.

(3) $f \equiv 0$ on $K_S \Leftrightarrow$ there exists an integer $m \geq 0$ such that $-f^{2m} \in T_S$.

(4) $K_S = \emptyset \Leftrightarrow -1 \in T_S$.

Note: The proof makes the essential use of Tarski's Transfer Principle (see [T]). Also see [M1, chapter 2, 2.2.1] for a proof.

2.3 Kadison-Dubois Theorem

The Kadison-Dubois representation theorem has a remarkable history, starting from functional analytic proofs by Kadison [Ka] and Dubois [Du]. Later, Becker and Schwartz give a short algebraic proof in the commutative case in [B-S].

The representation theorem has found fruitful applications in real algebraic geometry: for instance in studying sums of squares of polynomials and the moment problem. Wörmann [W1] used the representation theorem to reprove and generalize Schmüdgen's Theorem. Jacobi [J] generalized the Kadison-Dubois representation in the case of commutative rings. Using the improved representation he gave an algebraic proof of Putinar's Criterion. Before reaching this theorem, we first introduce some notations which will be needed.

Let A be any commutative ring with 1, $\mathbb{Q} \subseteq A$. Let $\chi = Hom(A,\mathbb{R})$ denote the set of all (unitary) ring homomorphisms: $\alpha : A \to \mathbb{R}$, $\alpha(1) = 1$.

We have the embedding $Hom(A,\mathbb{R}) \hookrightarrow \mathbb{R}^A$, the set of all functions from A to $\mathbb{R}$. $\mathbb{R}^A$ has the product topology. This topology is Hausdorff. If $a \in A$, $\alpha \in \mathbb{R}^A$ define

$$\hat{a} : \mathbb{R}^A \to \mathbb{R}$$

by $\hat{a}(\alpha) = \alpha(a) \in \mathbb{R}$. The set $\hat{a}^{-1}(U)$, $a \in A$, $U \subseteq \mathbb{R}$ open, form a subbasis for the topology on $\mathbb{R}^A$ i.e. the topology on $\mathbb{R}^A$ is just the weakest topology such that all the $\hat{a}$: $\mathbb{R}^A \to \mathbb{R}$, $a \in A$ are continuous. Therefore, $Hom(A,\mathbb{R})$ has the induced topology as a subspace of $\mathbb{R}^A$ i.e., the weakest topology on $\chi = Hom(A,\mathbb{R})$ such that each $\hat{a} : Hom(A,\mathbb{R}) \to \mathbb{R}$, $a \in A$ is continuous.

Proposition 2.3.1. ([M1, Prop 3.1.2]) (1) The identity map is the only homomorphism from $\mathbb{R}$ to $\mathbb{R}$. ($Hom(\mathbb{R},\mathbb{R})$ has only one point)

(2) Ring homomorphism from $\mathbb{R}[X]$ to $\mathbb{R}$ are in one to one correspondence with points in $\mathbb{R}^n$.

Proof. (1) Suppose α: $\mathbb{R} \to \mathbb{R}$ is a ring homomorphism, $\alpha(1) = 1$, $\alpha(0) = 0$, $\alpha(n) = n$ for any integer n. $\alpha(n)\alpha(\frac{m}{n}) = \alpha(m) = m \Rightarrow \alpha(\frac{m}{n}) = \frac{m}{n}$ for $\forall \frac{m}{n} \in \mathbb{Q}$. If $r, s \in \mathbb{R}$, $r \geq s$, then $\alpha(r) \geq \alpha(s)$ because $r - s \geq 0$, $r - s = t^2$ for some $t \in \mathbb{R}$. $\alpha(r) - \alpha(s) = \alpha(t^2) \geq 0 \Rightarrow \alpha(r) \geq \alpha(s)$. Now, suppose $r \in \mathbb{R}$, $\alpha(r) \neq r$. WLOG, assume $\alpha(r) > r$, there $\exists s \in\mathbb{Q}$, s.t. $\alpha(r) > s > r$; but $s = \alpha(s) \geq \alpha(r)$, contradiction. Therefore, $\alpha(r) = r$ for $\forall r \in\mathbb{R}$.

(2) Suppose $f \in\mathbb{R}[X]$, $f = \sum_{e_1,\dots,e_n\geq 0} a_{e_1\dots e_n} x_1^{e_1}\dots x_n^{e_n}$; $\alpha \in Hom(\mathbb{R}[X],\mathbb{R})$, $\alpha(f) = \sum_{e_1,\dots,e_n\geq 0} a_{e_1\dots e_n}\alpha(x_1)^{e_1}\dots\alpha(x_n)^{e_n} = f(\alpha(x_1), \dots\alpha(x_n))$. So, we get $(\alpha(x_1), \dots, \alpha(x_n)) \in\mathbb{R}^n$ and this point determines α. Conversely, if $x \in\mathbb{R}^n$ is any point, get α: $\mathbb{R}[X] \to\mathbb{R}$, $\alpha(f) = f(x)$. It is easy to check that $\alpha \in Hom(\mathbb{R}[X],\mathbb{R})$. So χ is identified with $\mathbb{R}^n$ via the mapping $\alpha \mapsto x$ described above. □

Remark 2.3.1. When $A =\mathbb{R}[X]$, what is the induced topology on $\mathbb{R}^n$? We know from the last proposition that: $\hat{f}(\alpha) = \alpha(f) = f(x)$, so the induced topology on $\mathbb{R}^n$ is the weakest topology such that all polynomial functions $x \mapsto f(x)$ are continuous. Since $x_1, \dots, x_n$ generate $\mathbb{R}[X]$ over $\mathbb{R}$ and the sum and product of continuous functions is continuous, it is the weakest such that each of the projections $x \mapsto x_i$, $i = 1, \dots, n$ is continuous, i.e., it is the usual (product) topology on $\mathbb{R}^n$.

For any topological space X, we denote by $Cont(X,\mathbb{R})$ the ring of all the continuous functions $f : X \to\mathbb{R}$ with operations defined pointwise. Thus, if $f, g \in Cont(X,\mathbb{R})$, $f + g$ and fg are defined by

$$(f + g)(x) = f(x) + g(x),\ (fg)(x) = f(x)g(x) \text{ for all } x \in X.$$

When, $X = \chi = Hom(A,\mathbb{R})$, we have the natural map

$$\phi : A \to Cont(\chi,\ \mathbb{R}),\ a \mapsto \hat{a}$$

It is easy to check ϕ is a ring homomorphism.

Note: If $A =\mathbb{R}[X]$ then, after identifying χ with $\mathbb{R}^n$, the map ϕ is just the obvious one, i.e., $\phi(f)$ is just the polynomial function $x \to f(x)$.

If S is any subset of A, we denote by χ_S the set of all ring homomorphisms $\alpha \in Hom(A,\mathbb{R})$ such that $\alpha(S) \subseteq \mathbb{R}^+$.

The Representation Theorem has a long history, and there are many other theorems of a similar flavor. In 1940, Stone first formulated the Representation Theorem in case of complete normed $\mathbb{R}$-algebras. In 1951, Kadison showed that in Stone's Theorem the requirement $A^2 \subseteq T$ was not necessary, and thus extended to the case of complete $\mathbb{R}$-algebras. In 1967, Dubois extended Kadison's result to a more general class of rings called Stone rings. Dubois, however, did not identify the compact Hausdorff space χ in the ring $Cont(\chi, \mathbb{R})$ used in his representation theorem. This was done by Becker and Schwartz in 1983. The following version of so-called Kadison-Dubois Theorem is that given by Becker and Schwartz in [B-S]. Also See [M1, chapter3, 3.4] for a proof.

Theorem 2.3.2. (Kadison-Dubois Theorem): Let A be any commutative ring with 1, $\mathbb{Q} \subseteq A$. Suppose M is a T-module, where T is an archimedean preprime, and $-1 \notin M$. Then,

(1) $\chi_M \neq \emptyset$.

(2) χ_M is compact.

(3) The ring homomorphism $\phi_M : A \to Cont(\chi_M,\mathbb{R})$ $a \to \hat{a}|_{\chi_M}$ has dense image.

(4) $\hat{a} > 0$ on χ_M if and only if $\exists$ rational $\varepsilon > 0$ such that $a - \varepsilon \in M$. (This implies: if $\hat{a} > 0$ on χ_M, then $a \in M$.)

(5) $\hat{a} \geq 0$ on χ_M if and only if $\forall$ rational $\varepsilon > 0$, $a + \varepsilon \in M$.

(6) $\hat{a} = 0$ on χ_M if and only if $\forall$ rational $\varepsilon > 0$, $\varepsilon + a \in M$, $\varepsilon - a \in M$.

Remark 2.3.2. To get the conclusion (1), (2) and (3) of the above theorem, we actually only need the weaker assumption that M is an archimedean T-module, T a generating preprime (see [M1, Cor 3.4.4]). This result will be used for several times in my later proofs. So it is worth being listed as a theorem as follows:

Theorem 2.3.3. Let A be any commutative ring with 1, $\mathbb{Q}\subseteq A$. Suppose M is an archimedean T-module, T a generating preprime (especially, M could be an archimedean quadratic module). If $-1 \notin M$, then

(1) $\chi_M \neq \emptyset$.

(2) χ_M is compact.

(3) The ring homomorphism $\phi_M : A \to Cont(\chi_M,\mathbb{R})$ $a \to \hat{a}|_{\chi_M}$ has dense image.

In particular, If $A = \mathbb{R}[X]$, then, for $\alpha \in \chi$, $g \in \mathbb{R}[X]$, $\alpha(g) \geq 0$ if and only if $g(x) \geq 0$, where $x \in \mathbb{R}^n$ is the point corresponding to α. Thus, for any finite subset $S = \{g_1, ..., g_s\}$ of $\mathbb{R}[X]$, $T = T_S$, the preordering generated by S, $M = M_S$ the quadratic module generated by S, $\chi_T = \chi_M = \chi_S$ is identified with the set:

$$K_S = \{x \in \mathbb{R}^n \mid g_i(x) \geq 0, i = 1, ..., s\}.$$

Now, assume T_S is an archimedean preordering. Applying the Kadison-Dubois Theorem to the T_S-module T_S, we get the following important result:

Corollary 2.3.4. Suppose S is a finite subset in $\mathbb{R}[X]$, T_S denotes the preordering generated by S in $\mathbb{R}[X]$, T_S is archimedean, and $-1 \notin T_S$, then:

(1) $K_S \neq \emptyset$.

(2) K_S is compact.

(3) for any $f \in \mathbb{R}[X]$, $f > 0$ on $K_S \Rightarrow f \in T_S$.

2.4 The Moment Problem and Schmüdgen's Theorem

One reason for the interest in nonnegative polynomials, was (and continues to be) the link to the classical moment problem.

In 1894, Thomas Jan Stieltjes (1856-1894) published an extremely influential paper: *Recherches sur les fractions continues*, Ann. Fac. Sci. Toulouse, 8, 1-122: 9, 5-47. He introduced what is now known as the Stieltjes integral with respect to an increasing function ϕ, the latter describing a distributions of mass (a measure μ) via the convention that the mass in an interval $[a, b]$ is $\mu[a, b]{=}\phi(b) - \phi(a)$. This integral was used to solve the following problem which is called *the Moment Problem*:

Given a sequence $s_0, s_1, ...$ of real numbers. Find the necessary and sufficient conditions for the existence of a measure μ on $[0, \infty)$ so that

$$s_n = \int_0^\infty x^n d\mu(x) \qquad \text{for} \qquad n = 0, 1, ...$$

The number s_n is called the *n·th moment* of μ, and the sequence of (s_n) is called the *moment sequence* of μ.

Stieltjes was led to the Stieltjes moment problem above via a study of continued fractions. Later, in 1920, Hamburger extended the Stieltjes moment problem to the real line, and established the moment problem as a theory of its own. In the same time, Hausdorff defined the *the Hausdorff Moment Problem* on a finite interval.

A given moment sequence can be thought to specify a linear operator on the linear space spanned by the monomials corresponding to the given moments.

Thus we consider the following general Moment Problem:

Given a closed set K in $\mathbb{R}^n$ and a linear mapping $L : \mathbb{R}[X] \to \mathbb{R}$ when does there exist a Borel measure μ on K such that $\forall f \in \mathbb{R}[X]$, $L(f) = \int_K f d\mu$?

Note: *A Borel measure on X* is a (positive) measure on X such that every set in $\text{ß}^\sigma(X)$ is measurable, where $\text{ß}^\sigma(X) :=$ the σ-ring generated by the compact set in X. (means that the smallest family of subsets of X containing all compact sets of X, closed under finite union, complimentation and countable intersection.)

It is clear that: If there exist a Borel measure μ on K such that $\forall f \in \mathbb{R}[X]$, $L(f) = \int_K f d\mu$, then $f \geq 0$ on $K \Rightarrow L(f) \geq 0$. Is the converse also true?

In 1935 Haviland proved (See [H1], [H2]):

Theorem 2.4.1. For any closed set $K \subseteq \mathbb{R}^n$ and any linear $L : \mathbb{R}[X] \to \mathbb{R}$, the following are equivalent:

(1) $\exists$ a Borel measure μ on K, s.t.$\forall f \in \mathbb{R}[X]$, $L(f) = \int_K f d\mu$. (We say L comes from a Borel measure on K)

(2) $\forall f \in \mathbb{R}[X]$, $f \geq 0$ on $K \Rightarrow L(f) \geq 0$.

For a proof based on the Reisz representation theorem, see [M3, Th 3.1], for example.

Recall $T_S^{alg} = \{f \in \mathbb{R}[X] : f \geq 0 \text{ on } K_S\}$. We also set:

$$T_S^\vee = \{L : \mathbb{R}[X] \to \mathbb{R} \text{: } L \text{ is linear } (\neq 0) \text{ and } L(T_S) \geq 0\},$$

and

$$T_S^{lin} = T_S^{\vee\vee} = \{f \in \mathbb{R}[X] : L(f) \geq 0 \text{ for all } L \in T_S^\vee\}$$

T_S, T_S^{lin} generally depend on S. T_S^{alg} depends only on the basic closed set K_S. Since T_S^{alg} is not finitely generated in general, one is interested in approximating it by T_S. Therefore, one study the following concrete Moment Problem: When is it true that every $L \in T_S^\vee$ comes from a positive Borel measure on K_S. By the Haviland's Theorem, this is equivalent to ask when the following condition (called *strong moment property* (SMP)) holds:

$$(*) \qquad T_S^{alg} = T_S^{lin}$$

Therefore, the moment problem is in some sense dual to the problem of determining positivity of polynomials.

Remark 2.4.1. (1). It is easy to see that the set T_S^{alg} is a preordering, called the *saturation* of T_S. We say T_S is *saturated* if $T_S^{alg} = T_S$. The set T_S^{lin} is the *closure* of T_S in $\mathbb{R}[X]$, giving $\mathbb{R}[X]$ *the unique finest locally convex topology* [P-S, p. 76],

$$T_S^{lin} = \overline{T_S} = \bigcap_{L \in T_S^\vee} L^{-1}(\mathbb{R}^+).$$

The set T_S^{lin} is a preordering [P-S, Lem. 1.2]. We say T_S is *closed* if $T_S^{lin} = T_S$.

(2). $T_S^{alg} = \{f \in \mathbb{R}[X] : f \geq 0 \text{ on } K_S\} = \bigcap_{x \in K_S} L_x^{-1}(\mathbb{R}^+)$, where $L_x : \mathbb{R}[X] \to \mathbb{R}$ is the algebra homomorphism defined by $L_x(f) = f(x)$. Points x in $\mathbb{R}^n$ are in one-to-one correspondence with algebra homomorphism $L : \mathbb{R}[X] \to \mathbb{R}$ via $x = (L(x_1), ..., L(x_n))$, $L(f) = f(x)$. Under this correspondence, points x in K_S correspond to algebra homomorphisms L satisfying $L(g_i) \geq 0$, $i = 1, ..., s$ or, equivalently, $L(T_S) \geq 0$. Since every algebra homomorphism is, in particular, a linear map, we have that $T_S^{alg} \supseteq T_S^{lin}$.

In the landmark paper [Sc], Schmüdgen proved (SMP) when the basic closed semi-algebraic set K_S is compact:

Theorem 2.4.2. (Schmüdgen's Theorem [Sc, Cor 3]) If K_S is compact then, for any $f \in \mathbb{R}[X]$, $f > 0$ on $K_S \Rightarrow f \in T_S$.

As an immediate corollary, he gets the following substantial improvement of Positivstellensatz: for compact K_S,

$$(\dagger) \qquad \forall f \in \mathbb{R}[X], f \geq 0 \text{ on } K_S \Rightarrow \forall \text{ real } \varepsilon > 0, f + \varepsilon \in T_S.$$

Now assuming (†) holds, and $f \in T_S^{alg}$, i.e.,$f \geq 0$ on K_S, then for any real $\varepsilon > 0$, $f + \varepsilon \in T_S$. Then for any $L \in T_S^{\vee}$, $L(f + \varepsilon) = L(f) + \varepsilon L(1) \geq 0$. Since ε could be arbitrary small, we must have $L(f) \geq 0$, i.e., $f \in T_S^{lin}$. Therefore, (†) implies (*). Thus (SMP) holds if K_S is compact.

Schmüdgen proves his theorem by functional analytic methods. Wörmann obtained Schmüdgen's result in an elementary algebraic way [W1]: He proved

K_S is compact if and only if T_S is archimedean.

Then he arrived at Schmüdgen's Theorem as a corollary of the Kadison-Dubois Theorem.

Since Schmüdgen's Theorem's appearance, this result has triggered much activity and stimulated new directions of research.

2.5 Putinar's Criterion

In the last 10 years, Schmüdgen's original result has been strengthened and extended in various ways. One of the most important questions is due to Putinar: When 'linear' representations are possible? i.e., If f is non-negative on the subset $K := \{g_1 \geq 0, ..., g_s \geq 0\}$ of $\mathbb{R}^n$, is it possible to represent f in the form:

$$f = \sigma_0 + \sigma_1 g_1 + ... + \sigma_s g_s,$$

where the σ_i are sums of squares of polynomials.

Schmüdgen's Theorem asserts: K_S compact is a sufficient condition for $f > 0$ on $K_S \Rightarrow f \in T_S$. Can we just replace T_S by M_S in the theorem? If $n = 1$, it is true. In fact, we can prove $M_S = T_S$ in the one variable case (see chapter III, section 2). But in the general case, the answer turned out to be no (see Example 3.1.7). This is because we make use of the Positivstellensatz in the proof of Schmüdgen's Theorem, which does not work for the quadratic module. Actually, what we really need to make this work through is a stronger condition than K_S compactness, which is M_S archimedean.

The first step in answering this question was provided by Putinar himself. By refining the functional analytic approach of Schmüdgen, Putinar gave in [P] a criterion for linear representations to exist: Suppose there exists a polynomial $g = \tau_0 + \sum_1^s \tau_i g_i$, τ_i sums of squares of polynomials, such that $K_{\{g\}} = \{a \in \mathbb{R}^n | g(a) \geq 0\}$ is bounded. Then every f which is strictly positive on $K_{\{g_1,\dots,g_s\}}$ can be written as $f = \sigma_0 + \sigma_1 g_1 + \dots \sigma_s g_s$ for σ_i sums of squares of polynomials.

The following theorem includes Putinar's result and other results as well.

Theorem 2.5.1. (Putinar's Criterion): Suppose S is a finite subset of $\mathbb{R}[X]$. The following are equivalent:

(1) M_S is archimedean.

(2) K_S is compact and, for all $f \in \mathbb{R}[X]$, $f > 0$ on $K_S \Rightarrow f \in M_S$.

(3) There exists a positive integer k such that $k \pm x_i \in M_S$, $i = 1, 2.., n$.

(4) There exists a positive integer k such that $k - \Sigma_{i=1}^n x_i^2 \in M_S$.

(5) There exists some $g \in M_S$ such that $K_{\{g\}} = \{x \in \mathbb{R}^n | g(x) \geq 0\}$ is compact.

Putinar's original proof use methods from functional analysis. In [J], Jacobi extends the classical Kadison-Dubois Theorem and uses this to give a straightforward algebraic proof of Putinar's Criterion.

Theorem 2.5.2. (Generalization of Kadison-Dubois Theorem): Suppose M is an archimedean $\sum A^2$-module (i.e., quadratic module) in A. Then, for any $a \in A$,

$$\hat{a} > 0 \text{ on } \chi_M \Rightarrow a \in M.$$

Remark 2.5.1. Jacobi's original version of this theorem assumes: M is an archimedean T-module, where T a preordering of higher order (i.e., a preprime $T \subseteq A$ that contains A^{2n} for some natural number n). In [M2], Marshall proves a more general representation theorem for archimedean T-modules, where T is a weakly torsion preprime. Both of these two versions of theorems are more general than the one given above. But in this thesis, we are only interested in quadratic modules, and assuming M an archimedean quadratic module, we have a very concise proof as follows:

Proof. Set $T = \sum A^2$. For any $a \in A$ such that $\hat{a} > 0$ on χ_M, set $M_1 = M - aT$. M_1 is a T-module. Clearly, $-a \in M_1$, $M \subseteq M_1$, so $\chi_{M_1} \subseteq \chi_M$.

Claim $\chi_{M_1} = \emptyset$. If $\alpha \in \chi_{M_1}$, then $\alpha \in \chi_M$ and $\alpha(-a) \geq 0$, $-\alpha(a) \geq 0$, $\alpha(a) \leq 0$, so $\hat{a}(\alpha) \leq 0$. This contradicts $\hat{a}(\alpha) > 0$ on χ_M.

By Theorem 2.3.3, $-1 \in M_1$, so there $\exists s \in M, t \in T$ such that $-1 = s - at$. Therefore, $at - 1 = s \in M$.

Let $\Sigma = \{r \in \mathbb{Q} \mid r + a \in M\}$. Since M is archimedean, there exists a positive integer n such that $n + a \in M$. So $\Sigma \neq \emptyset$.

Since M is archimedean, there exists a positive integer k such that $2k-1-t^2a \in M$. It follows that

$$2k - t = (2k - 1 - t^2a) + t(ta - 1) + 1 \in M.$$

Consider the identity

$$k^2a + k^2r - 1 = (k - t)^2(a + r) + 2k(ta - 1) + rt(2k - t) + (2k - 1 - t^2a),$$

where $(k - t)^2 \in T, a + r \in M, ta - 1 \in M, rt \in T$ if r is non-negative, $2k - t \in M, 2k - 1 - t^2a \in M$. This identity shows that if r is a non-negative rational such that $a + r \in M$, then $k^2(a + r) - 1 \in M$, so $\frac{1}{k^2}[k^2(a + r) - 1] = a + r - \frac{1}{k^2} \in M$. Since k dependents only on a and t, by repeating the process, r decreases by $\frac{1}{k^2}$ at each step. Thus, we can finally get a $r \in \Sigma$ such that $r < 0$. Therefore $r + a \in M, -r > 0$, so $a = (r + a) + (-r) \in M$. □

Applying this Generalization of Kadison-Dubois Theorem to the polynomial ring, we have Putinar's Criterion as an immediate corollary.

In the following chapters, we will mainly consider the one variable case, i.e., $\mathbb{R}[X] = \mathbb{R}[x]$, the polynomial ring in one variable. I will focus the discussion on the quadratic module and linear representations.

Chapter 3

Some Results in One Variable Case

In this chapter, we will focus our discussion on the relationship between the quadratic module M_S and the preordering T_S generated by a finite subset S of $\mathbb{R}[x]$. It is easy to see that $M_S \subseteq T_S$, but $M_S \neq T_S$ in general, as M_S may not be closed under multiplication. See Example 3.2.7.

Now assuming the associated basic closed semi-algebraic set K_S is compact in $\mathbb{R}$, we are asking does this imply that $M_S = T_S$? Actually, this is an open problem from S. Kuhlmann, M. Marshall and N. Schwartz's 2004 article "*Positivity, sums of squares and the multi-dimensional moment problem II*" [K-M-S, Open Problem 6].

The answer turned out to be yes. Scheiderer first settled this problem in [S4, Cor 4.4] based on his "local-global principle for quadratic modules" which is called "the Scheiderer's Main Theorem" in this thesis. Scheiderer proved it in a more general situation, but his proof is not easy to be understood. In this chapter, I will concentrate on this question, and give a more elementary proof in section 2.

3.1 K_S compact $\Rightarrow$ M_S archimedean

Suppose S is a finite subset of $\mathbb{R}[x]$, we now consider the following two conditions: K_S compact and M_S archimedean. We have already known from Wörmann's proof

[W1] of Schmüdgen's Theorem that T_S archimedean is equivalent to K_S compact. By the definition, we also know $M_S \subseteq T_S$, so M_S archimedean implies T_S archimedean. Therefore we have,

$$M_S \text{ archimedean} \Rightarrow T_S \text{ archimedean} \Leftrightarrow K_S \text{ compact}.$$

It is natural to ask is it true that K_S compact implies M_S archimedean? The counter examples at the end of this section show that this is not true in general. Roughly, this is because the proof of K_S compact $\Rightarrow T_S$ archimedean uses the Positivstellensatz which does not work any more in the quadratic modules case. However, when $n = 1$ i.e., the one variable case, it is true. The goal of this section is to establish this result.

We first look at the general commutative ring A and give a useful criterion for judging whether a quadratic module M of A is archimedean.

Lemma 3.1.1. ([M1, Prop 3.3.3]) Suppose A is a commutative ring with 1, $\mathbb{Q} \subseteq A$, M a quadratic module of A. We define H_M as follows,

$$H_M := \{a \in A |\ \exists \text{ an integer } n \geq 1 \text{ such that } n \pm a \in M\}.$$

We call H_M *the ring of bounded elements of A with respect to M*. Then

(1) H_M is a subring of A.

(2) M is archimedean if and only if $H_M = A$.

(3) $a^2 \in H_M \Rightarrow a \in H_M$.

(4) $\sum_{i=1}^{k} a_i^2 \in H_M \Rightarrow a_i \in H_M$, $i = 1, ..., k$.

Proof. (1) Since M is a ΣA^2-module, $\mathbb{Q}^+ \in M$ and $\mathbb{Q} \in H_M$. Suppose $n_1 \pm a \in H_M$,

$n_2 \pm b \in H_M$, then $(n_1+n_2) \pm (a-b) \in H_M$. So H_M is a additive subgroup of A. In view of the identity

$$ab = \tfrac{1}{4}((a+b)^2 - (a-b)^2),$$

to show H_M is closed under multiplication, it suffices to show

$$a \in H_M \Rightarrow a^2 \in H_M.$$

Suppose $n \pm a \in M$. Then $n^2 + a^2 \in M$ and also

$$n^2 - a^2 = \tfrac{1}{2n}((n+a)(n^2-a^2) + (n-a)(n^2-a^2)) =$$

$$\tfrac{1}{2n}((n+a)^2(n-a) + (n-a)^2(n+a)) \in M,$$

so $a^2 \in H_M$.

(2) This is clear.

(3) If $n - a^2 \in M$, then

$$n \pm a = \tfrac{1}{2}((n-1) + (n-a^2) + (a \pm 1)^2) \in M.$$

(4) If $n - \Sigma a_i^2 \in M$ then

$$n - a_i^2 = (n - \sum a_i^2) + \sum_{j \neq i} a_j^2 \in M$$

so, by (3), $a_i \in H_M$.

□

Applying this Lemma to the polynomial ring $\mathbb{R}[x]$,we have:

Corollary 3.1.2. If M is quadratic module of $\mathbb{R}[X]$, then M is archimedean if and only if $k - \sum_{i=1}^{n} x_i^2 \in M$ for some integer $k \geq 1$.

Proof. (⇐) Since every element of $\mathbb{R}^+$ is a square, $\mathbb{R}^+ \subseteq M$, so $\mathbb{R} \subseteq H_M$. By the assumption and Lemma 3.1.1 (4), $x_1, ..., x_n \in H_M$. By Lemma 3.1.1 (1), H_M is a subring of $\mathbb{R}[X]$, thus $H_M = \mathbb{R}[X]$, so the result follows from 3.1.1 (2).

The implication (⇒) is trivial. □

As usual, in the one variable polynomial ring, we define the *degree* of a polynomial to be the highest power of the variable appearing in it; the term in a polynomial which contains the highest power of the variable is called the *leading term*; the coefficient of a polynomial's leading term is called the *leading coefficient*.

Lemma 3.1.3. Suppose $S = \{g_1(x), ..., g_s(x)\}$ is a finite subset of $\mathbb{R}[x]$, the polynomial ring in one variable. M_S denotes the quadratic module generated by S. $K_S := \{x \in \mathbb{R} : g_1(x) \geq 0, ..., g_s(x) \geq 0\}$ is the associated basic closed semi-algebraic set. Then, K_S compact in $\mathbb{R} \Rightarrow M_S$ contains a polynomial f which has even degree and negative leading coefficient.

Proof. We assume there is no such f contained in M_S.

Since K_S is compact, K_S is bounded above. If every polynomial g_i contained in S has positive leading coefficient, then there exists a $N \in \mathbb{N}$ such that $g_i \geq 0$ on $[N, \infty)$ for every $g_i \in S$, i.e., $[N, \infty) \subseteq K_S$. Therefore, S must contain a polynomial f_1 which has negative leading coefficient. So M_S contains f_1. By our hypothesis, f_1 must have odd degree.

Similarly, K_S is bounded below implies there must exists $f_2 \in M_S$, f_2 has positive leading coefficient and odd degree.

We assume that

$$f_1 = -a_m x^m + ... + a_1 x + a_0, \text{ where } a_m > 0 \text{ and } m \text{ is odd.}$$

$$f_2 = b_l x^l + ... + b_1 x + b_0, \text{ where } b_l > 0 \text{ and } l \text{ is odd.}$$

If $m \neq l$, without lost of generality, let $m > l$. $m - l$ is even and positive, so we can assume $m - l = 2d$, where $d \geq 1$. Now, take

$$g = \tfrac{a_m}{b_l} x^{2(d-1)}(x-t)^2, \text{ where } 2t > \tfrac{a_{m-1}}{a_m} + \tfrac{b_{l-1}}{b_l}.$$

$$\text{Then} \qquad f_1 + f_2 g = (-a_m 2t + a_m \tfrac{b_{l-1}}{b_l} + a_{m-1})x^{m-1} + ...$$

Since $-a_m 2t + a_m \frac{b_{l-1}}{b_l} + a_{m-1} < 0$, $m-1$ is even, $f_1 + f_2 g$ has even degree and negative leading coefficient. It is also easy to see that g is a square in $\mathbb{R}[x]$, so $f_1 + f_2 g \in M_S$. If $m = l$, take $f_3 = f_1 x^2 = -a_m x^{m+2} + ... + a_1 x^3 + a_0 x^2$. Now f_3 is a polynomial contained in M_S having odd degree $m+2$ ($> l$) and negative leading coefficient. The same argument as above shows that there exists a polynomial in M_S which has even degree and negative leading coefficient. A contradiction. □

Now we reach the main result of this section:

Theorem 3.1.4. Suppose $S = \{g_1(x), ..., g_s(x)\}$ is a finite subset of $\mathbb{R}[x]$, the polynomial ring in one variable. M_S denotes the quadratic module generated by S. $K_S := \{x \in \mathbb{R} : g_1(x) \geq 0, ..., g_s(x) \geq 0\}$ is the associated basic closed semi-algebraic set. Then, K_S compact $\Rightarrow$ M_S archimedean.

Proof. By Corollary 3.1.2., it is enough to show there exists an integer k such that $k - x^2 \in M_S$.

By Lemma 3.1.3 and assumption, M_S contains a f with even degree and negative leading coefficient. Say

$$f = -a_n x^n + a_{n-1}x^{n-1} ... + a_0, \text{ where } n \text{ is even and } a_n > 0.$$

There exists m $\in \mathbb{N}$, such that $2^m \geq n$; denote $2^m - n$ by d, d is a positive even number. Then,

$$\frac{x^d}{a_n} f = -x^{2^m} + d_{2^m-1} x^{2^m-1} + ... + d_0 x^d \in M_S. \tag{3.1}$$

where $d_{2^m-1} = \frac{a_{n-1}}{a_n}$, ..., $d_0 = 0$. Try to write $\frac{x^d}{a_n} f$ in the following form:

$$\frac{x^d}{a_n} f = -(x^{2^{m-1}} + b_{2^{m-1}-1} x^{2^{m-1}-1} + ... + b_0)^2 + c_{2^{m-1}} x^{2^{m-1}} + ... + c_0. \tag{3.2}$$

Expanding (3.2) and comparing it with (3.1) for the first $2^{m-1} - 1$ terms, gives us the following identities:

$$\begin{cases} 2b_{2^{m-1}-1} = -d_{2^m-1} \\ 2b_{2^{m-1}-2} + b^2_{2^{m-1}-1} = -d_{2^m-2} \\ 2b_{2^{m-1}-3} + 2b_{2^{m-1}-1} b_{2^{m-1}-2} = -d_{2^m-3} \\ ... \\ 2b_1 + 2b_2 2b_{2^{m-1}-1} + ... = -d_{2^{m-1}+1} \end{cases} \tag{3.3}$$

We can solve $b_{2^{m-1}-1}$, $b_{2^{m-1}-2}$, ..., b_1 in turn from the above system of equations. Now compare the coefficient of the term $x^{2^{m-1}}$

$$-(2b_0 + 2b_1 2b_{2^{m-1}-1} + ...) + c_{2^{m-1}} = d_{2^{m-1}}$$

We choose b_0 small enough such that $c_{2^{m-1}} < 0$. Then,

$$\tfrac{x^d}{a_n} f + (x^{2^{m-1}} + b_{2^{m-1}-1} x^{2^{m-1}-1} + ... + b_0)^2 = c_{2^{m-1}} x^{2^{m-1}} + ... + c_0 \in M_S.$$

Dividing by $-c_{2^{m-1}}$ yields, $f_1 = -x^{2^{m-1}} - \frac{c_{2^{m-1}-1}}{c_{2^{m-1}}} x^{2^{m-1}-1} - ... - \frac{c_0}{c_{2^{m-1}}} \in M_S$.

By induction, we will finally get

$$f_{m-1} = -x^2 + t_1 x + t_0 \in M_S.$$

The identity $-x^2+t_1x+t_0 = -\frac{3}{4}x^2-(\frac{1}{2}x-t_1)^2+t_1^2+t_0$ shows that $-\frac{3}{4}x^2+t_1^2+t_0 \in M_S$. Therefore, there exists a $k \in \mathbb{N}$, such that $k > \frac{4}{3}(t_1^2+t_0)$, $k - x^2 \in M_S$. □

However, if we look at the multi-variable case, this result does not hold any more. The following are some examples where K_S is compact, but M_S is not archimedean.

Example 3.1.5. (i). Take $n \geq 2$. Take $S = \{g_1, .., g_{n+1}\}$ where

$$g_i = x_i - \tfrac{1}{2},\ i = 1, ..., n,\ g_{n+1} = 1 - \textstyle\prod_{i=1}^n x_i$$

(so $s = n+1 \geq 3$). The region K_S is compact and could have any dimension ≥ 2 (depending on n). We will construct a quadratic module Q such that $g_1, ..., g_{n+1} \in Q$, but for each positive integer k, $k - \sum_{i=1}^n x_i^2 \notin Q$. This shows that M is not archimedean. To construct such a quadratic module Q, we consider the abelian group $\Gamma := \mathbb{Z}^n$ ordered lexicographically. For $f \in \mathbb{R}[X]$, $f \neq 0$, define the 'degree' $\delta(f)$ of f to be the largest $k = (k_1, ..., k_n)$ such that the monomial $x^k = x_1^{k_1}...x_n^{k_n}$ appears in f. Define the 'leading coefficient' $a(f)$ of f to be the coefficient of the monomial $x^{\delta(f)}$ in f. Take Q to consist of 0 and all $f \neq 0$ such that either

(1) $\delta(f) \not\equiv (1, ..., 1) \bmod 2\Gamma$ and $a(f) > 0$ or

(2) $\delta(f) \equiv (1, ..., 1) \bmod 2\Gamma$ and $a(f) < 0$.

It is easy to check Q is a quadratic module, $Q \cup -Q = \mathbb{R}[X]$, $Q \cap -Q = 0$. $\delta(k - \sum_{i=1}^n x_i^2) \not\equiv (1, ..., 1) \bmod 2\Gamma$, and $a(k - \sum_{i=1}^n x_i^2) < 0$ for all k, so $k - \sum_{i=1}^n x_i^2 \notin Q$. By the definition, Q is not archimedean.

$\delta(g_1) \equiv (1, ..., 0) \bmod 2\Gamma$ and $a(g_1) = 1 > 0$;

$\delta(g_2) \equiv (0, 1, ..., 0) \bmod 2\Gamma$ and $a(g_2) = 1 > 0$;

......

$\delta(g_n) \equiv (0, ..., 1) \bmod 2\Gamma$ and $a(g_n) = 1 > 0$;

$\delta(g_{n+1}) \equiv (1, 1, ..., 1)$ mod 2Γ and $a(g_{n+1}) = -1 < 0$;

So $g_i \in Q$ $(i = 1, ..., n+1)$, which means $M \subseteq Q$. Therefore, M is not archimedean.

Remark 3.1.1. The above example is due to Jacobi and Prestel [J-P, Ex 4.6]. It shows that with K compact and K has dimension ≥ 2, the quadratic module M could be non-archimedean. One may wonder is there any examples that K has dimension < 2, K compact and M is not archimedean? Actually, we can produce such examples in a similar way.

(ii). Let M be the quadratic module in $\mathbb{R}[x, y]$ generated by g_1, g_2, g_3 where $g_1 = x$, $g_2 = y$, $g_3 = -xy - 1$. The associated basic closed semi-algebraic set K in $\mathbb{R}^2$ is the empty set which has dimension -1. (Convention: The empty set has dimension -1.) We construct the quadratic module Q in the exactly same way as example (i), such that $g_1, g_2, g_3 \in Q$, but for each positive integer k, $k - (x^2 + y^2) \notin Q$.
(iii). Let M be the quadratic module in $\mathbb{R}[x, y]$ generated by $h^2 g_1, h^2 g_2, h^2 g_3$ where g_1, g_2, g_3 are the same as example (ii), and $h = x^2 + y^2$. The associated basic closed semi-algebraic set K consists of a single point (the origin) which has dimension 0. We construct the same quadratic module Q. Q is not archimedean, and it is easy to check $h^2 g_1, h^2 g_2, h^2 g_3 \in Q$.
(iv). Take the same non-archimedean quadratic module Q, and the same g_1, g_2, g_3 as above. Take $h = x^2 + y^2 - 1$. The associated basic closed semi-algebraic set K now is the unit circle $x^2 + y^2 = 1$ which has dimension 1. It is easy to check that $h^2 g_1, h^2 g_2, h^2 g_3 \in Q$.

Thus, we have all the examples that for any dimensional (≥ -1) basic closed semi-algebraic set K, K compact, the quadratic module M is non-archimedean.

Combining Theorem 3.1.4 with the Kadison-Dubois Theorem, we can improve the Schmüdgen's Theorem in the one variable case.

Theorem 3.1.6. Suppose $S = \{g_1(x), ..., g_s(x)\}$ is a finite subset of $\mathbb{R}[x]$, the polynomial ring of one variable. If K_S is compact then, for any $f \in \mathbb{R}[x]$, $f > 0$ on $K_S \Rightarrow f \in M_S$.

Note: this proof does not use the classical Positivstellensatz.

It is natural for one to ask does this enhanced Schmüdgen's Theorem still hold true in the multi-variable case?

It is obviously true when $s = 1$ i.e., S contains only one element. In [J-P], Jacobi and Prestel prove it is also true when $s = 2$ (for any n) [J-P, Them 4.4], but it is false when $s \geq 3$, $n \geq 2$. Example 3.1.5 is a counter example, because K_S compact implies there must exist a N such that $N - \sum_{i=1}^{n} x_i^2 > 0$ on K_S. The following example is a more explicit one:

Example 3.1.7. Let M_S be a quadratic module in $\mathbb{R}[x, y]$ generated by S, where $S = \{x - \frac{1}{2}, y - \frac{1}{2}, 1 - xy\}$.

K_S is obviously compact and $xy \geq \frac{1}{4} > 0$ on K_S, but $xy \notin M_S$.

For if we assume $xy \in M_S$, that is, $xy = \sigma_0 + \sigma_1(x - \frac{1}{2}) + \sigma_2(y - \frac{1}{2}) + \sigma_3(1 - xy)$, where σ_i (i=0,1,2,3) are sums of squares. The leading term of each σ_i must have even power of x and even power of y and have positive leading coefficient. (Here we are using the same definition as Example 3.1.5: For $f \in \mathbb{R}[x, y]$, $f \neq 0$ define the 'degree' $\delta(f)$ of f to be the largest $k = (k_1, k_2)$ such that the monomial $x^{k_1}y^{k_2}$ appears in f; define the leading term to be the monomial with the largest degree; define the 'leading coefficient' $a(f)$ of f to be the coefficient of its leading term.) If we look at the four terms on the right side of the identity, we have the following: $\delta(\sigma_0) \equiv (0,0) \bmod 2\Gamma$ and $a(\sigma_0) > 0$; $\delta(\sigma_1(x-\frac{1}{2})) \equiv (1,0) \bmod 2\Gamma$ and $a(\sigma_1(x-\frac{1}{2})) > 0$; $\delta(\sigma_2(y-\frac{1}{2})) \equiv (0,1) \bmod 2\Gamma$ and $a(\sigma_2(y-\frac{1}{2})) > 0$; $\delta(\sigma_3(1-xy)) \equiv (1,1) \bmod 2\Gamma$ and $a(\sigma_3(1-xy)) < 0$. Since they all have different degrees, their leading terms cannot be canceled. Therefore, their sum which is xy must have the same leading term as one of them. Thus, there are four possibilities for xy: $\delta(xy) \equiv (0,0) \bmod 2\Gamma$ and $a(xy) > 0$ or $\delta(xy) \equiv (1,0) \bmod 2\Gamma$ and $a(xy) > 0$ or $\delta(xy) \equiv (0,1) \bmod 2\Gamma$ and $a(xy) > 0$ or $\delta(xy) \equiv (1,1) \bmod 2\Gamma$ and $a(xy) < 0$. None of them is true. We get the contradiction.

At the end of this section, we need to point out that the finiteness of S is another essential assumption. If S is infinite subset of $\mathbb{R}[x]$, even T_S could be non-archimedean with K_S compact. The following are counter examples:

Example 3.1.8. Assume that $S = \{f_1, f_2, ..., f_i, ...\}$.

(i). We take $\quad f_1 = x-1;\ \ f_2 = x-2;\ \ ...;\ \ f_i = x-i;\ \ ....$

Now $K_S = \emptyset$. If T_S is archimedean, there exists an integer number N, such that $N - x^2 \in M_S$. Then

$$N - x^2 = h_1 g_1 + h_2 g_2 + ... + h_n g_n + h_0, \tag{3.4}$$

where each h_k $(k = 0, 1, ..., n)$ is a sum of squares and each g_k $(k = 1, 2, ..., n)$ is a finite product of the elements of S. So the leading coefficient of each h_k and each g_k is positive. Therefore, when $x \to \infty$, $h_k \to \infty$, $g_k \to \infty$, the right side of (3.4) $\to \infty$; but the left side $\to -\infty$. A contradiction.

(ii). Set $f_1 = x(x-1)(x-2)$; $f_2 = x(x-1)(x-3)$; ...; $f_i = x(x-1)(x-i-1)$; ......

Now $K_S = [0, 1]$, which is compact. Applying the similar argument as the example (i), we get T_S is not archimedean.

3.2 $M_S = T_S$

In [K-M-S], the authors listed the following question as an open problem:

Whether $\mathbb{R}[x]$ contains a finitely generated quadratic module M_S which is not a pre-ordering (i.e., $M_S \neq T_S$), but whose associated basic closed semi-algebraic set K_S is compact?

Scheiderer applies his "Main Theorem" to give this question a negative answer [S4, Cor 4.4]. In the chapter V, I will give this fact a similar but more elementary proof depending on the "Simple Version of the Main Theorem". Now, in this section, I give another elementary proof without using the "Scheiderer's Main Theorem".

We first introduce an important criterion for determining when T_S is saturated in the one variable case. I will make essential use of this theorem in my proof.

Theorem 3.2.1. Let $K_S = \bigcup_{j=0}^{k}[a_j, b_j],\ b_{j-1} < a_j,\ j = 1, 2, ..., k,\ S = \{g_1, ..., g_s\}$, Then T_S is saturated (T_S is said to be saturated if for any $f \in \mathbb{R}[X]$ and $f \geq 0$ on K_S implies $f \in T_S$) if and only if the following two conditions hold:

(a) for each endpoint a_j $\exists i \in \{1, ..., s\}$ such that $g_i(a_j) = 0$ and $g_i'(a_j) > 0$,

(b) for each endpoint b_j $\exists i \in \{1, ..., s\}$ such that $g_i(b_j) = 0$ and $g_i'(b_j) < 0$.

Note: This theorem is just a special case of a general criterion for curves proved in [S3, Th 5.17]. For a proof independent from "Scheiderer's Main Theorem", see [K-M-S, Th 3.2]. I will give another proof based on the Simple Version of Scheiderer's Main Theorem in Chapter V.

Lemma 3.2.2. Suppose g is a polynomial such that g can be factored as the product of different linears in $\mathbb{R}$, (i.e., $g = d(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)$ with $\alpha_1 > \alpha_2 > ... > \alpha_n$, $d \in \mathbb{R}$.) and $K_{\{g\}}$ is compact, then

(1) $M_{\{g\}} = T_{\{g\}}$ is saturated.

(2) If f is another polynomial being factored as the product of different linears in $\mathbb{R}$, $T_{\{f,g\}}$ is saturated.

Proof. (1) Since $K_{\{g\}}$ is compact, g must have even degree, and have the negative leading coefficient. So we can assume that

$$g = -d(x - a_1)(x - a_2)...(x - a_{2n-1})(x - a_{2n}),$$

where $a_1 > a_2 > ... > a_{2n-1} > a_{2n}, \ \ d > 0$.

Therefore, $K_{\{g\}} = \bigcup_{i=1}^{n} [a_{2i}, a_{2i-1}]$.

For each endpoint a_{2i-1}, $g(a_{2i-1}) = 0$, and

$$g'(a_{2i-1}) = -d(a_{2i-1} - a_{2i})(\prod_{j \neq i}(a_{2i-1} - a_{2j-1})(a_{2i-1} - a_{2j})) < 0;$$

For each endpoint a_{2i}, $g(a_{2i}) = 0$, and

$$g'(a_{2i}) = -d(a_{2i} - a_{2i-1})(\prod_{j \neq i}(a_{2i-1} - a_{2j-1})(a_{2i-1} - a_{2j})) > 0.$$

Theorem 3.2.1 applies, we obtain $T_{\{g\}}$ is saturated. Since $T_{\{g\}}$ is generated by only one polynomial, $M_{\{g\}} = T_{\{g\}}$.

Actually, with a similar argument as above, it is not hard to see that given any polynomial f being factored as the product of different linears in $\mathbb{R}$, no matter whether $K_{\{f\}}$ compact or not, for each right endpoint a_{2i-1} of some closed interval $[a_{2i}, a_{2i-1}]$ of $K_{\{f\}}$, $f(a_{2i-1}) = 0$, and $f'(a_{2i-1}) < 0$; for each left endpoint a_{2i} of some closed interval $[a_{2i}, a_{2i-1}]$ of $K_{\{f\}}$, $f(a_{2i}) = 0$, and $f'(a_{2i}) > 0$.

(2) $K_{\{f,g\}} = K_{\{f\}} \cap K_{\{g\}}$. Since $K_{\{g\}}$ is compact, i.e., a finite union of bounded closed intervals, $K_{\{f\}}$ is a finite union of closed intervals, $K_{\{f,g\}}$ is also compact, say $K_{\{f,g\}} = \bigcup_{i=1}^{m}[b_{2i}, b_{2i-1}]$, where $b_1 \geq b_2 > b_3 \geq b_4 ... > b_{2m-1} \geq b_{2m}$.

If $b_{2i-1} = b_{2i}$, then $b_{2i-1} = b_{2i}$ must be a left (right) endpoint of some closed interval of $K_{\{f\}}$ on the one hand, and a right (left) endpoint of some closed interval of $K_{\{g\}}$ on the other hand. Therefore, in this case, $f(b_{2i-1}) = g(b_{2i-1}) = 0$, and $f'(b_{2i-1}) > (<)0$, $g'(b_{2i-1}) < (>)0$. Theorem 3.2.1 applies.

If $b_{2i-1} > b_{2i}$, then b_{2i-1} must be a right endpoint of some interval of $K_{\{f\}}$ (or $K_{\{g\}}$). Therefore, $f(b_{2i-1}) = 0$ ($g(b_{2i-1}) = 0$) and $f'(b_{2i-1}) < 0$ ($g'(b_{2i-1}) < 0$). b_{2i} must be a left endpoint of some interval of $K_{\{f\}}$ (or $K_{\{g\}}$). Therefore, $f(b_{2i}) = 0$ ($g(b_{2i}) = 0$) and $f'(b_{2i}) > 0$ ($g'(b_{2i}) > 0$). Theorem 3.2.1 applies. □

Remark 3.2.1. $K_{\{g\}}$ is compact is really an essential assumption in this Lemma. See the following counterexample.

Example 3.2.3. Let $g = x(x-1)(x-2)$, $f = x$, then $K_{\{g\}} = [0,1] \cup [2, \infty)$, $f \geq 0$ on $K_{\{g\}}$.

Assume that $f = \sigma_0 + \sigma_1 g$, i.e., $x = \sigma_0 + \sigma_1 x(x-1)(x-2)$, where σ_0 and σ_1 are sums of squares in $\mathbb{R}[x]$.

σ_0 and σ_1 must have even degrees and positive leading coefficients. $\sigma_1 \neq 0$, otherwise, $\sigma_0 = x$ has an odd degree. Therefore, $\sigma_1 x(x-1)(x-2)$ has degree at least 3. Since both σ_0 and $\sigma_1 x(x-1)(x-2)$ have positive leading coefficients, their leading terms cannot be canceled when they added together, so $\sigma_0 + \sigma_1 x(x-1)(x-2)$ has degree at least 3. But x has degree one. A contradiction.

Proposition 3.2.4. Suppose f and g are two polynomials in $\mathbb{R}[x]$ such that $K_{\{g\}}$ is compact. Then $fg = \sigma_0 + \sigma_1 f + \sigma_2 g$, where σ_i $(i = 0, 1, 2)$ are sums of squares in $\mathbb{R}[x]$.

Proof. Claim: We only need to consider the case where f, g are polynomials which can be factored as the products of different linears in $\mathbb{R}$ with leading coefficients 1 or -1.

f can be written as $f = \sigma_f f_0$, where σ_f is a sum of squares in $\mathbb{R}[x]$, and f_0 is a polynomial being factored as the product of different linears in $\mathbb{R}$, with leading coefficient 1 or -1. Similarly, $g = \sigma_g g_0$, where σ_g is a sum of squares. So, if $K_{\{g\}}$ is compact, $K_{\{g_0\}}$ is also compact. If it is true that $f_0 g_0 = \sigma_0 + \sigma_1 f_0 + \sigma_2 g_0$, then we just multiply by $\sigma_f \sigma_g$ to both sides. It gives

$$\sigma_f f_0 \sigma_g g_0 = \sigma_0 \sigma_f \sigma_g + \sigma_1 \sigma_g \sigma_f f_0 + \sigma_2 \sigma_f \sigma_g g_0$$

Therefore,

$$fg = \tau_0 + \tau_1 f + \tau_2 g$$

where $\tau_0 = \sigma_0 \sigma_f \sigma_g$, $\tau_1 = \sigma_1 \sigma_g$, $\tau_2 = \sigma_2 \sigma_f$, which are all sums of squares in $\mathbb{R}[x]$.

Since $K_{\{g\}}$ is compact and g is a product of different linears, we can assume that $g = -(x - a_1)(x - a_2)...(x - a_{2n-1})(x - a_{2n})$, where $a_1 > a_2 > ... > a_{2n-1} > a_{2n}$. Therefore, $K_{\{g\}} = [a_2, a_1] \cup ... \cup [a_{2n}, a_{2n-1}]$.

Now, we want to construct a polynomial h which is also a product of different linears such that $K_{\{h\}}$ is compact and $g \geq 0$ on $K_{\{h\}}$, $fh \geq 0$ on $K_{\{g\}}$. If this is done, applying Lemma 3.2.2, we have

$$g = \sigma_0 + \sigma_1 h, \text{ and } fh = \tau_0 + \tau_1 g.$$

From the first identity, we have

$$g - \sigma_0 = \sigma_1 h.$$

Multiplying by σ_1 to the both sides of the second identity yields

$$f\sigma_1 h = \sigma_1\tau_0 + \sigma_1\tau_1 g,$$

therefore,

$$f(g - \sigma_0) = \sigma_1\tau_0 + \sigma_1\tau_1 g,$$

$$fg = \sigma_1\tau_0 + \sigma_0 f + \sigma_1\tau_1 g.$$

We construct such a h by considering the roots of f on the interval $(a_1, a_2) \cup ... \cup (a_{2n-1}, a_{2n})$.

If there is no such root of f exists, then either $f \geq 0$ on $K_{\{g\}}$ or $-f \geq 0$ on $K_{\{g\}}$. In the first case, $f = \sigma_0 + \sigma_1 g$ where σ_0 and σ_1 are sum of squares. Thus $fg = \tau_0 + \tau_1 g$, where $\tau_0 = \sigma_1 g^2$, $\tau_1 = \sigma_0$, which are both sum of squares. In the second case, $h = -1$ satisfies all of our requirements.

If there exist such roots of f, say $b_1, b_2..., b_m$ are the roots of f on the interval (a_2, a_1), $b_1 > b_2 > .... > b_m$.

Since f is a product of different linears in $\mathbb{R}$, $f^{'}(b_1) \neq 0$.

If $f^{'}(b_1) > 0$, let $c_1 = a_1$, $c_2 = b_1$, $c_3 = b_2$, ..., $c_{m+1} = b_m$. If $m + 1$ is even, let $h_1 = (x-c_1)(x-c_2)...(x-c_{m+1})$. Otherwise, let $h_1 = (x-c_1)(x-c_2)...(x-c_{m+1})(x-c_{m+2})$, where $c_{m+2} = a_2$.

If $f^{'}(b_1) < 0$, let $c_1 = b_1$, $c_2 = b_2$, ..., $c_m = b_m$. If m is even, let $h_1 = (x - c_1)(x - c_2)...(x - c_m)$. Otherwise, let $h_1 = (x - c_1)(x - c_2)...(x - c_m)(x - c_{m+1})$, where $c_{m+1} = a_2$.

We consider the roots of f on other intervals $(a_4, a_3)...(a_{2n}, a_{2n-1})$. By the same algorithm, we will get a series of polynomials h_2,...,h_n. The following is the algorithm for a general interval (a_{2i}, a_{2i-1}):

Suppose $d_1, d_2..., d_l$ are the roots of f on (a_{2i}, a_{2i-1}), $d_1 > d_2 > .... > d_l$.

If $f^{'}(d_1) > 0$, let $e_1 = a_{2i-1}$, $e_2 = d_1$, $e_3 = d_2$,..., $e_{l+1} = d_l$. If $l + 1$ is even, let $h_i = (x - e_1)(x - e_2)...(x - e_{l+1})$. Otherwise, let $h_i = (x - e_1)(x - e_2)...(x - e_{l+1})(x - e_{l+2})$, where $c_{l+2} = a_{2i}$.

If $f^{'}(d_1) < 0$, let $e_1 = d_1$, $e_2 = d_2$,..., $e_l = d_l$. If l is even, let $h_i = (x - e_1)(x - e_2)...(x - e_l)$. Otherwise, let $h_i = (x - e_1)(x - e_2)...(x - e_l)(x - e_{l+1})$, where $e_{l+1} = a_{2i}$.

If there is no root of f exists on the interval (a_{2i}, a_{2i-1}), we just set $h_i = 1$.

We notice the following obvious properties for h_i (i=1,2,...,n).

(1). $K_{\{-h_i\}}$ is a finite union of bounded closed intervals, therefore is compact.

(2). $(-h_i)f \geq 0$ on $[a_{2i}, a_{2i-1}]$.

(3). $g \geq 0$ on $K_{\{-h_i\}}$.

(4). $h_i \geq 0$ on $K_{\{g\}} \setminus [a_{2i}, a_{2i-1}]$.

Now, let $h = -h_1 h_2 ... h_n$, we will show this h satisfies all requirements.

Since $K_{\{h\}} = \bigcup_{i=1}^{n} K_{\{-h_i\}}$, $K_{\{h\}}$ is a compact subset of $\mathbb{R}$. By (2) $(-h_i)f \geq 0$ on $[a_{2i}, a_{2i-1}]$, and by (4), $h_j \geq 0$ on $[a_{2i}, a_{2i-1}]$ for all $j \neq i$, therefore, $fh = f(-h_i) \prod_{j \neq i} h_j \geq 0$ on $[a_{2i}, a_{2i-1}]$ for any $i = 1, ..., n$. Thus, $fh \geq 0$ on $K_{\{g\}}$. By (3) $g \geq 0$ on $K_{\{-h_i\}}$ for any i, $g \geq 0$ on $K_{\{h\}} = \bigcup_{i=1}^{n} K_{\{-h_i\}}$.

Therefore, we can always find such a h. □

Proposition 3.2.5. Suppose f, g, h are polynomials in $\mathbb{R}[x]$ such that $K_{\{g\}}$ is compact. Then $fh = \sigma_0 + \sigma_1 f + \sigma_2 h + \sigma_3 g$, where σ_i $(i = 0, 1, 2, 3)$ are sums of squares in $\mathbb{R}[x]$.

Proof. For the same reason as last proposition, we can always assume f, g, h are polynomials which can be factored as products of different linears in $\mathbb{R}$ with leading coefficients 1 or -1.

Since $K_{\{g\}}$ is compact, i.e., a finite union of bounded closed intervals, we assume $K_{\{g\}} = \bigcup_{i=1}^{n}[a_{2i}, a_{2i-1}]$, $a_1 > a_2 > ... > a_{2n}$ (because g is the product of different linears), $a_i \in \mathbb{R}$ for all $i = 1, ..., 2n$. Then $K_{\{g\}} \cap K_{\{h\}}$ must be also compact. Therefore, we can assume that $K_{\{g\}} \cap K_{\{h\}} = \bigcup_{i=1}^{m}[b_{2i}, b_{2i-1}]$, $b_1 \geq b_2 > b_3 \geq b_4 ... > b_{2m-1} \geq b_{2m}$, $b_i \in \mathbb{R}$ for all $i = 1, ..., 2m$.

It suffices to show that there exists a polynomial h_0 which is the product of different linears, i.e., $h_0 = -(x-d_1)(x-d_2)...(x-d_{2l-1})(x-d_{2l})$, $\Big(d_i \in \mathbb{R}$ for all $i = 1, ..., 2l$ and $d_1 > d_2 > ... > d_{2l-1} > d_{2l}\Big)$ such that $h \geq 0$ on $K_{\{h_0\}}$, and $h_0 \geq 0$ on $K_{\{g,h\}}$.

If this is done, since $K_{\{h_0\}}$ is compact, $h \geq 0$ on $K_{\{h_0\}}$, applying Lemma 3.2.2, we have:

$$h = \sigma_0 + \sigma_1 h_0, \text{ where } \sigma_0, \sigma_1 \text{ are both sums of squares in } \mathbb{R}[x].$$

Therefore, $fh = \sigma_0 f + \sigma_1 f h_0$. By Proposition 3.2.4, $fh_0 = \tau_0 + \tau_1 f + \tau_2 h_0$, where τ_i (i=0,1,2) are sums of squares in $\mathbb{R}[x]$. Thus, $fh = \tau_0\sigma_1 + (\tau_1\sigma_1 + \sigma_0)f + \tau_2\sigma_1 h_0$.

Since $h_0 \geq 0$ on $K_{\{g,h\}}$, applying Lemma 3.2.2 again

$$h_0 = \alpha_0 + \alpha_1 h + \alpha_2 g + \alpha_3 hg,$$

where $\alpha_i (i = 0, 1, 2, 3)$ are sums of squares in $\mathbb{R}[x]$.

Using Proposition 3.2.4 again, yields:

$$hg = \beta_0 + \beta_1 h + \beta_2 g,$$

where $\beta_i (i = 0, 1, 2)$ are sums of squares in $\mathbb{R}[x]$.

So, we obtain: $h_0 = (\alpha_0 + \alpha_3\beta_0) + (\alpha_1 + \alpha_3\beta_1)f + (\alpha_2 + \alpha_3\beta_2)g$. Therefore,

$$fh = \tau_0\sigma_1 + (\tau_1\sigma_1 + \sigma_0)f + \tau_2\sigma_1 h_0$$

$= \tau_0\sigma_1+\tau_2\sigma_1\alpha_0+\tau_2\sigma_1\alpha_3\beta_0+(\tau_1\sigma_1+\sigma_0)f+(\tau_2\sigma_1\alpha_1+\tau_2\sigma_1\alpha_3\beta_1)h+(\tau_2\sigma_1\alpha_2+\tau_2\sigma_1\alpha_3\beta_2)g.$

where $\tau_0\sigma_1 + \tau_2\sigma_1\alpha_0 + \tau_2\sigma_1\alpha_3\beta_0$, $\tau_1\sigma_1 + \sigma_0$, $\tau_2\sigma_1\alpha_1 + \tau_2\sigma_1\alpha_3\beta_1$, $\tau_2\sigma_1\alpha_2 + \tau_2\sigma_1\alpha_3\beta_2$ are all sums of squares.

In the following, we are going to construct such a h_0:

Assume $K_{\{h\}} = \bigcup_{i=1}^{l}[c_{2i}, c_{2i-1}]$, where $c_1 > c_2 > ... > c_{2l-1} > c_{2l}$ (since h is the product of different linears), c_1 could be ∞ and c_{2l} could be $-\infty$.

We set $d_i = c_i$ for $i = 2, 3, ..., 2l - 1$.

When $c_1 \neq \infty$, set $d_1 = c_1$.

When $c_1 = \infty$, we set $d_1 = a_1$ if $a_1 > c_2$; otherwise, we set $d_1 = c_2 + 1$.

Similarly, When $c_{2l} \neq -\infty$, set $d_{2l} = c_{2l}$.

When $c_{2l} = -\infty$, we set $d_{2l} = a_{2n}$ if $a_{2n} < c_{2l-1}$; otherwise, we set $d_{2l} = c_{2l-1} - 1$.

Let $h_0 = -(x - d_1)(x - d_2)...(x - d_{2l-1})(x - d_{2l})$.

Clearly, $[d_{2i}, d_{2i-1}] \subseteq [c_{2i}, c_{2i-1}]$ for all $i = 1, 2, ..., l$, therefore, $K_{\{h_0\}} = \bigcup_{i=1}^{l}[d_{2i}, d_{2i-1}] \subseteq \bigcup_{i=1}^{l}[c_{2i}, c_{2i-1}] = K_{\{h\}}$. Since $h \geq 0$ on $K_{\{h\}}$, $h \geq 0$ on $K_{\{h_0\}}$.

It is also easy to see that $K_{\{h,g\}} \subseteq K_{\{h_0\}}$, therefore, $h_0 \geq 0$ on $K_{\{h,g\}}$. Thus, this h_0 satisfies all of our requirements.

□

By Theorem 3.1.4, K_S compact implies M_S archimedean, so by Corollary 3.1.2, there exists an integer N such that: $N - x^2 \in M_S$. Therefore, K_S compact guarantees that there exists a $g = N - x^2 \in M_S$ with $K\{g\}$ compact. Thus we obtain the following result.

Theorem 3.2.6. Suppose S is a finite subset of $\mathbb{R}[x]$ such that K_S is compact, then $M_S = T_S$.

Proof. With the preceding paragraph and Proposition 3.2.5, we know that for any $f, h \in M_S$, $fh \in M_S$. Therefore, M_S is closed under multiplication. Thus, $M_S = T_S$. □

Remark 3.2.2. K_S compact is an essential assumption in Theorem 3.2.6. The following is an example where K_S is not compact and $M_S \neq T_S$.

Example 3.2.7. Take $S = \{x+1, x(x-1)\}$. Then $K_S = [-1, 0] \cup [1, \infty)$, $(x+1)x(x-1) \in T_S$ but $(x+1)x(x-1) \notin M_S$.

For suppose $(x+1)x(x-1) \in M_S$, i.e., $(x+1)x(x-1) = \sigma_0 + \sigma_1(x+1) + \sigma_2 x(x-1)$, $\sigma_i (i = 0, 1, 2)$ are sums of squares in $\mathbb{R}[x]$. Evaluating at -1 yields $\sigma_0(-1) + 2\sigma_2(-1) = 0$, so $\sigma_0(-1) = \sigma_2(-1) = 0$. Thus, $(x+1)^2 \mid \sigma_0$, $(x+1)^2 \mid \sigma_2$. Similarly, $x^2 \mid \sigma_0$, $x^2 \mid \sigma_1$, $(x-1)^2 \mid \sigma_0$, $(x-1)^2 \mid \sigma_1$. Therefore, $\sigma_0 = (x+1)^2 x^2 (x-1)^2 \tau_0$, $\sigma_1 = x^2(x-1)^2\tau_1$, $\sigma_2 = (x+1)^2\tau_2$, where $\tau_i (i = 0, 1, 2)$ are sums of squares.
Substituting and canceling $(x+1)x(x-1)$, this yields

$$1 = (x+1)x(x-1)\tau_0 + x(x-1)\tau_1 + (x+1)\tau_2.$$

τ_0, τ_1, τ_2 cannot be all equal to 0, otherwise, it yields $1 = 0$.
Since τ_0, τ_1 and τ_2 have positive leading coefficients, their leading terms cannot be canceled out when they added together. So if not all of them are equal to 0, $(x+1)x(x-1)\tau_0 + x(x-1)\tau_1 + (x+1)\tau_2$ has degree at least 1. But 1 has the degree zero. A contradiction.

By Schmüdgen's Theorem, when K_S is compact, for any f, $f > 0$ on K_S implies that $f \in T_S$, therefore, Example 3.1.5 and 3.1.7 also show that when $n \geq 2$, Theorem 3.2.6 does not hold any more.

Chapter 4

Scheiderer's Main Theorem

In chapter II, we introduced Schmüdgen's Theorem and Jacobi's Representation Theorem (Cor 2.4.3) which assert that K_S compact or M_S archimedean are sufficient conditions for T_S or M_S containing all polynomials strictly positive on K_S respectively. In this chapter, we want to extend these results to where f is only required to be non-negative, i.e., f is allowed to have zeros in K_S.

Scheiderer made great contributions toward this question. In [S3, Cor 3.17], he established a local-global criterion for the polynomials non-negative on K_S to be contained in T_S, which extends Schmüdgen's Theorem:

If K_S is compact, and f is non-negative and has finitely many zeros on K_S, then f lies in T_S if and only if f lies in the preordering generated by T_S in the completed local ring at each of its zeros.

For the quadratic module case, Scheiderer gave a similar statement which extends Jacobi's Representation Theorem. This is found in his paper *Distinguished representations of non-negative polynomials* [S4, Th 2.8]. Roughly, if we assume that M_S is archimedean and the zero set of f in K_S is finite, it says again that f contained in the quadratic module generated by M_S in the completed local ring at each of its zeros is equivalent to f contained in M_S. However, we still need another condition to guarantee the equivalence, namely: dimension of $\mathbb{R}[X]/[(M+(f))\cap-(M+(f))] \leq 0$, which is stronger than the finiteness of the zeros of f in K_S. We refer to this theorem as the "Scheiderer's Main Theorem" here.

Scheiderer's Main Theorem is a powerful tool in dealing with the low dimensional case. We will get some nice results in the next chapter by applying it to the one variable case. In this chapter, I will give this Main Theorem a proof based on the Basic Lemma provided in [K-M-S, Lem 2.1]. (The proof given here is quoted from [M4], not the original one by Scheiderer.)

4.1 The Main Theorem

In the last section of chapter II, we considered the problem of "linearly representing" a polynomial f which is strictly positive on K_S. According to Jacobi's Representation Theorem (Cor 2.4.3), we have:

$$\text{If } M_S \text{ is archimedean, then } f > 0 \text{ on } K_S \Rightarrow f \in M_S.$$

However, if we replace $f > 0$ on K_S by $f \geq 0$ on K_S, this result does not hold anymore.

In his main theorem in [S4, Th 2.8], Scheiderer gives sufficient conditions (on f) for M_S to be saturated. Recall"saturated" means $T_S^{alg} = M_S$, which is equivalent to saying: $f \geq 0$ on $K_S \Rightarrow f \in M_S$.

In order to prove the Scheiderer's Main Theorem, we begin with the Basic Lemma [K-M-S, Lem 2.1].

Lemma 4.1.1. Let X be a compact hausdorff space, A a commutative ring with 1 with $\frac{1}{n} \in A$ for some integer $n \geq 2$ and ϕ: $A \to Cont(X, \mathbb{R})$ a ring homomorphism.

Suppose f, $g \in A$ are such that $\phi(f) \geq 0$, $\phi(g) \geq 0$ and $(f, g) = (1)$. Then there exist $s, t \in A$ such that $sf + tg = 1$ and $\phi(s), \phi(t)$ are strictly positive.

Proof. We suppress ϕ from the notation. Let s, $t \in A$ be such that $1 = sf + tg$. On the compact set

$$L_1 := \{p \in C |\ s(p) \leq 0\},$$

$tg = 1 - sf \geq 1$. Thus $g > 0$ on L_1 so, for N sufficiently large, $s + Ng > 0$ on L_1. On $C - L_1$ this is obviously also true. Define $s_1 = s + Ng$, $t_1 = t - Nf$. Thus, $1 = s_1 f + t_1 g$ in A and $s_1 > 0$ on C. Choose a positive rational $\delta \in A$ so small that $\delta fg < 1$ on C. Choose a positive rational $\epsilon \in A$ so small that, on the compact set

$$L_2 = \{p \in C : g(p) \leq \epsilon\},$$

$f > 0$, $1 > \epsilon\delta f$ and $\epsilon t_1 + s_1 f > 0$. Choose k so large that, on the set L_2, $\epsilon t_1 + s_1 f > s_1 f(1 - \epsilon\delta f)^k$ and, on the set

$$L_3 = \{p \in C : g(p) \geq \epsilon\},$$

$s_1 f(1-\epsilon\delta f)^k < 1$. Choose $r = s_1 \delta f \sum_{i=0}^{k-1} (1-\delta fg)^i$. Choose $\sigma = s_1 - rg$, $\tau = t_1 + rf$. Thus $1 = \sigma f + \tau g$ in A. It remains to verify that σ, $\tau > 0$ on C. Using the identity $(1 - z) \sum_{i=1}^{k-1} z^i = 1 - z^k$, we see that, on C,

$$\sigma = s_1 - rg = s_1 - s_1 \delta fg \sum_{i=0}^{k-1} (1-\delta fg)^i = s_1 - s_1(1-(1-\delta fg)^k) = s_1(1-\delta fg)^k > 0$$

On L_2,

$$\tau = t_1 + rf = t_1 + s_1 \delta f^2 \sum_{i=0}^{k-1} (1 - \delta fg)^i \geq t_1 + s_1 \delta f^2 \sum_{i=0}^{k-1} (1 - \epsilon\delta f)^i =$$

$$t_1 + (s_1 f/\epsilon)(1 - (1 - \epsilon\delta f)^k) > 0.$$

On L_3,

$$\tau = t_1 + rf = t_1 + (f/g)rg = t_1 + (f/g)s_1(1 - (1 - \delta fg)^k) =$$

$$t_1 + s_1 f/g - (s_1 f/g)(1 - \delta fg)^k = 1/g - (s_1 f/g)(1 - \delta fg)^k) > 0.$$

This completes the proof. □

Combining the Basic Lemma with Jacobi's representation theorem, yields the following key result, which is due to Scheiderer.

Lemma 4.1.2. If M is archimedean and $f \in A$ is ≥ 0 on χ_M, then $f \in M$ if and only if $f \in M + (f^2)$.

Remark 4.1.1. For any ideal $I \in A$, $M + I$ is a quadratic module. Suppose $x, y \in M + I$, $x = m_1 + i_1; y = m_2 + i_2$, where $m_1, m_2 \in M$; $i_1, i_2 \in I$. Then $x + y = (m_1 + m_2) + (i_1 + i_2) \in M + I$; $a^2x = a^2m_1 + a^2i_2 \in M + I$ for any $a \in A$.

Proof. $f \in M \Rightarrow f \in M + (f^2)$ is obvious. Now we look at the other direction. Suppose $f \in M + (f^2)$, i.e., $f = t + af^2$, $t \in M$, $a \in A$. Using $a = (\frac{a+1}{2})^2 - (\frac{a-1}{2})^2$, we see that $f = u - b^2f^2$ where $u = t + (\frac{a+1}{2})^2 f^2 \in M$, and $b = \frac{a-1}{2}$. Thus $f(1 + b^2f) = u$. Clearly $(f, 1 + b^2f) = (1)$, f and $1 + b^2f$ are ≥ 0 on χ_M. M is archimedean implies χ_M is compact. So, by Lemma 4.1.1, there exist $c, d \in A$, $c, d > 0$ on χ_M such that

$$1 = cf + d(1 + b^2f) \tag{4.1}$$

By Jacobi's Theorem, $c, d, cd \in M$. Multiplying equation (4.1) by df yields

$$df = cdf^2 + d^2f(1 + b^2f) = cdf^2 + d^2u \in M.$$

Multiplying the same equation by f yields

$$f = cf^2 + df(1 + b^2f) = cf^2 + df + db^2f^2 \in M$$

□

To exploit Lemma 4.1.2, we use another lemma, which we will be applying to the quadratic module $M + (f^2)$.

Lemma 4.1.3. Let M be a quadratic module, $J := M \cap -M$. Then

(1) J is an ideal.

(2) For each minimal prime I over J, $(M + I) \cap -(M + I) = I$. Equivalently, for all $s_1, s_2 \in M$, $s_1 + s_2 \in I \Rightarrow s_1, s_2 \in I$.

(3) $(M + \sqrt{J}) \cap -(M + \sqrt{J}) = \sqrt{J}$.

Note: for any ideal J of A, $\sqrt{J}$ denotes the *radical* of J: $\sqrt{J} := \{x \in A : x^n \in J$ for some $n > 0\}$. It is not hard to see that $\sqrt{J}$ is also an ideal.

Proof. (1) For any $x \in A$, $\pm x \in M \Leftrightarrow x \in J$. If $x, y \in J$, $\pm x \in M$, $\pm y \in M \Rightarrow \pm(x - y) \in M$ and $\pm a^2 x \in M$ for any $a \in A$. So, $J - J \subseteq J$ and $a^2 J \subseteq J$ for any $a \in A$. Using $a = b^2 - c^2$, $b = \frac{a+1}{2}$, $c = \frac{a-1}{2}$, this yields $aJ = (b^2 - c^2)J \subseteq b^2 J - c^2 J \subseteq J - J \subseteq J$. Thus J is an ideal.

(2) First we prove the equivalence. Since $I = \pm(0 + I) \subseteq \pm(M + I)$, $I \subseteq (M + I) \cap -(M + I)$ is always true. Now suppose $(M + I) \cap -(M + I) \subseteq I$, and $s_1, s_2 \in M$, $s_1 + s_2 \in I$. Clearly, $s_1 \in M \subseteq M + I$. We also have $-s_1 = s_2 - (s_1 + s_2) \in M + I$, so $s_1 \in (M + I) \cap -(M + I) \subseteq I$. The proof that $s_2 \in I$ is the same.

Conversely, suppose $x \in (M + I) \cap -(M + I)$, then $x = m_1 + i_1$; $-x = m_2 + i_2$, where $m_1, m_2 \in M$, $i_1, i_2 \in I$. $(m_1 + i_1) + (m_2 + i_2) = x + (-x) = 0 \Rightarrow m_1 + m_2 = -(i_1 + i_2) \in I$ and $m_1, m_2 \in M$. By the assumption, $m_1, m_2 \in I$. Therefore, $x = m_1 + i_1 \in I$. This proves $(M + I) \cap -(M + I) \subseteq I$.

Let I be a minimal prime ideal over J. I/J is a prime ideal of the quotient ring

A/J. Now, we consider the prime ideals of the localization of A/J at I/J. They are one-to-one correspondent with the prime ideals of A/J which are contained in I/J. But every ideal of A/J has the form P/J, where P is an ideal of A containing J. Since I is a minimal prime ideal over J, $S^{-1}I/J$ is the unique prime ideal and therefore is the nilradical of the localization of A/J at I/J, where S denote the multiplicative subset: $A/J \backslash I/J$ (The *Nilradical* is the radical of zero ideal i.e., $\sqrt{0} = \{x \in A : x^n = 0 \text{ for some } n > 0\}$, as well as the intersection of all prime ideals of the ring). So, for any $a \in I$, $a + J \in I/J$, $\frac{a+J}{1+J} \in S^{-1}I/J \Rightarrow (\frac{a+J}{1+J})^n = 0$ in the localization of A/J at I/J for some integer $n \geq 1$, which means $(a+J)^n(b+J) = 0$ for some $b \notin I$ in the quotient ring A/J,

$$\text{i.e. } (a+J)^n(b+J) = J \Rightarrow a^n b + J = J \Rightarrow a^n b \in J,\ b \notin I.$$

Suppose $s_1, s_2 \in M$ and $s_1 + s_2 \in I$. From the above, $u(s_1+s_2)^n \in J$ for some integer $n \geq 1$ and some $u \notin I$. Thus $u^2(s_1+s_2)^n \in J$. We can choose n to be odd. Note that $s_1^i s_2^{n-i} \in M$, e.g., if i is even, then $n - i$ is odd and $s_1^i \in A^2, s_2^{n-i} \in A^2 s_2$, so $s_1^i s_2^{n-i} \in A^2 s_2 \subseteq M$. Thus expanding $u^2(s_1+s_2)^n$ as

$$u^2(s_1+s_2)^n = \sum_{i=0}^{n} \binom{n}{i} u^2 s_1^i s_2^{n-i}$$

and transposing terms yields $-u^2 s_1^n \in M$. Since we also have $u^2 s_1^n \in M$, this yields $u^2 s_1^n \in J$. Since $J \subseteq I$, and I is prime and $u \notin I$, this implies $s_1 \in I$. The proof that $s_2 \in I$ is the same.

(3) As we proved in (2), it is always true that: $\sqrt{J} \subseteq (M + \sqrt{J}) \cap -(M + \sqrt{J})$. We only need to prove for the other inclusion. Since $\sqrt{J}$ is also the intersection of the minimal prime ideals lying over J, $\pm(M + \sqrt{J}) \subseteq \pm(M + I)$ for any minimal prime ideals I lying over J. We already know from (2): $(M+I) \cap -(M+I) = I$, so

$(M+\sqrt{J})\cap -(M+\sqrt{J}) \subseteq (M+I)\cap -(M+I) = I$ for each minimal prime ideals I lying over J. So, $(M+\sqrt{J})\cap -(M+\sqrt{J}) \subseteq \cap_i I = \sqrt{J}$. □

Before reaching the Main Theorem, let us introduce some terminologies and results from commutative algebra which will appear in the theorem and its proof:

We define a *ascending chain* of ideals of a ring A to be an increasing sequence $I_1 \subseteq I_2 \subseteq I_3 ...$, where I_k $(k = 1, 2, ...)$ are ideals of A. If for every such chain of A, there is an integer n such that $I_i = I_n$ for all $i \geq n$, the ring A is said to be *Noetherian*.

(1) If A is Noetherian, the polynomial ring $A[X]$ is also Noetherian. In particular, $\mathbb{R}[X]$ is Noetherian. (See [At-M, Th 7.5])

(2) If A is Noetherian, I is an ideal of A, then, the quotient ring A/I is also Noetherian. (See [At-M, Th 6.6])

Similarly, we define a *descending chain* of ideals of a ring A to be a decreasing sequence $I_1 \supseteq I_2 \supseteq I_3 ....$ If for every such chain of A, there is an integer m such that $I_i = I_m$ for all $i \geq m$, the ring A is said to be *Artinian*.

(1) If A is Artinian, then every prime ideal I_i of A is maximal.

(2) If A is Artinian, A has only finite number of prime ideals I_i, $i = 1, ..., p$.

(3) If A is Artinian, the nilradical $\Re$ of A is nilponent, i.e. $(\Re)^k = (\bigcap_{i=1}^p I_i)^k = 0$ for some sufficiently large integer k.

We define a chain of prime ideals of a ring A to be a finite strictly increasing sequence $p_0 \subset p_1 \subset ... \subset p_n$, where p_i are prime ideals of A; the length of the chain is n. We define the (Krull) *dimension* of A to be the supremum of the lengths of all chains of prime ideals in A: it is an integer ≥ 0, or $+\infty$ (assuming $A \neq 0$). A field has dimension 0; The ring $\mathbb{Z}$ has dimension 1. A is Artinian is equivalent to A is Noetherian and A has dimension 0. (See [At-M, chapter 8])

Theorem 4.1.4. (Main Theorem) Suppose A is Noetherian, M is an archimedean quadratic module in A, $f \in A$ $f \geq 0$ on χ_M and A/J has (Krull) dimension ≤ 0, where $J := (M + (f^2)) \cap -(M + (f^2))$. Then the following are equivalent:

(1) $f \in M$

(2) For each prime ideal I lying over J and each $k \geq 0$, $f \in M + I^k$.

Proof. (1) $\Rightarrow$ (2) is clear. Now we prove the other direction.

Assume (2). Since $M + (f^2)$ is a quadratic module, by (1) of Lemma 4.1.3 J is an ideal. $(f^2) \in J$, so $M + (f^2) \subseteq M + J$. Note that: $M \subseteq M + (f^2)$ and $J = (M + (f^2)) \cap -(M + (f^2)) \subseteq M + (f^2)$, therefore, $M + J = M + (f^2)$. By Lemma 4.1.2, it suffices to show $f \in M + J$.

Since A/J is Noetherian and zero dimensional, A/J is artinean. Therefore, $(\Re)^k = (\bigcap_{i=1}^p I_i/J)^k = 0$ for some sufficiently large integer k, where $I_1, ..., I_p$ are the minimal prime ideals of A lying over J. Since each I_i/J is also maximal in A/J, I_i/J and I_j/J are *coprime* for $i \neq j$ (two ideals a, b are said to be *coprime* if $a + b = (1)$). Using the identity $\sqrt{a+b} = \sqrt{\sqrt{a} + \sqrt{b}}$ and $\sqrt{a} = (1) \Leftrightarrow a = (1)$, where a, b are ideals, we can conclude: a, b are coprime if and only if $\sqrt{a}$ and $\sqrt{b}$ are coprime. Since $\sqrt{a} = \sqrt{a^k}$ for any integer $k \geq 1$, a, b are coprime is equivalent to a^k and b^k are coprime. Therefore, we get $(\frac{I_i}{J})^k$ and $(\frac{I_j}{J})^k$ are coprime for any integer $k \geq 1$ and $i \neq j$. Since when a, b are coprime, $ab = a \cap b$, we have

$$\bigcap_{i=1}^p (\tfrac{I_i}{J})^k = \prod_{i=1}^p (\tfrac{I_i}{J})^k = (\prod_{i=1}^p \tfrac{I_i}{J})^k = (\bigcap_{i=1}^p \tfrac{I_i}{J})^k = \Re^k = 0.$$

Let $J_i = I_i^k + J$, then $(\frac{I_i}{J})^k = \frac{I_i^k + J}{J} = \frac{J_i}{J}$. The above identity tells us $\cap_{i=1}^p J_i = J$ for sufficiently large k. Since I_i is maximal in A, I_i and I_j are coprime in A for $i \neq j$. By the last paragraph, we know I_i^k and I_j^k are also coprime. Thus, J_i, J_j are coprime if $i \neq j$. Therefore, according to the Chinese Remainder Theorem (see [At-M, Prop 1.10]), $A/J \cong \prod_{i=1}^{p} A/J_i$. By hypothesis, $f \in M + I_i^k$, so $f \in M + J_i$. Thus $f \equiv f_i \mod J_i$, $f_i \in M$, $i = 1, ..., p$. Choose $e_1, ..., e_p \in A$ such that $e_i \equiv 1 \mod J_i$, $e_i \equiv 0 \mod J_j$ for $j \neq i$. Note that $e_i^2 \equiv e_i \mod J$. Thus $f \equiv \sum_{i=1}^{p} e_i f_i \equiv \sum_{i=1}^{p} e_i^2 f_i \mod J$, $e_i^2 f_i \in M$, $\sum_{i=1}^{p} e_i^2 f_i \in M$, so $f \in M + J$. □

Remark 4.1.2. (1) The preordering version of this Theorem is found already in [S3, Cor 3.17].

(2) The assumption that A/J is zero dimensional can also be rephrased as follows: Define $J' := (M+(f)) \cap -(M+(f))$. Note that J and J' have the same nilradical. It is easy to see that $J \subseteq J'$, so $\sqrt{J} \subseteq \sqrt{J'}$. By Lemma 4.1.3 (3), $(M+\sqrt{J}) \cap -(M+\sqrt{J}) = \sqrt{J}$. Using the fact that $f^2 \in J$, we have $f \in \sqrt{J}$, $M+(f) \subseteq M+\sqrt{J}$, $-(M+(f)) \subseteq -(M+\sqrt{J})$. Then, $J' = (M+(f)) \cap -(M+(f)) \subseteq (M+\sqrt{J}) \cap -(M+\sqrt{J}) = \sqrt{J}$. It is easy to check that: for any ideal I, $\sqrt{\sqrt{I}} = \sqrt{I}$, so we get $\sqrt{J'} \subseteq \sqrt{\sqrt{J}} = \sqrt{J}$. Therefore, $\sqrt{J} = \sqrt{J'}$. Since every prime ideal containing ideal J must contain $\sqrt{J}$, $I \supseteq J$ is equivalent to $I \supseteq J'$. Thus the assumption that A/J is zero dimensional is equivalent to the assumption that A/J' is zero dimensional.

(3) The set of prime ideals lying over J is equal to $\{ker(\alpha) | \alpha \in \chi_M, f(\alpha) = 0\}$.

Proof. Let I be a minimal (=maximal) prime ideal of A lying over J. Since M is archimedean, $M + I$ is also archimedean and $-1 \notin M + I$ by Lemma 4.1.3 (2) (otherwise, $1 \in I$) so, by Theorem 2.3.3, χ_{M+I} is non-empty, i.e., there exists a ring homomorphism $\alpha : A \to R$ with $\alpha(M + I) \geq 0$.

Claim: $\alpha(I) = 0$. Suppose $a \in I$, then $a = 0 + a \in M + I$, so $\alpha(a) \geq 0$. Similarly, $-a = 0 + (-a) \in M + I$, so $\alpha(-a) \geq 0$, i.e., $\alpha(a) \leq 0$. Thus, $\alpha(a) = 0$.

Therefore, $I \subseteq ker(\alpha)$. Since I is maximal, $I = ker(\alpha)$. Clearly $\alpha \in \chi_{M+I} \subseteq \chi_M$. $f^2 \in (M + (f^2)) \cap -(M + (f^2)) = J \subseteq I \Rightarrow f \in I$ (I is prime), so $f(\alpha) = 0$.

Conversely, given any $\alpha \in \chi_M$ such that $f(\alpha) = 0$, $\frac{A}{ker(\alpha)}$ is isomorphic to a subring of $\mathbb{R}$, which is an integral domain, so $ker(\alpha)$ is a prime ideal. $\alpha \in \chi_M \Rightarrow \alpha \geq 0$ on M, and $\alpha(f) = 0$, thus, $\alpha \geq 0$ on $M + (f^2)$, $\alpha \leq 0$ on $-(M + (f^2))$. Therefore, $\alpha = 0$ on J, $J \subseteq ker(\alpha)$. Since A/J has dimension zero, $ker(\alpha)$ is a minimal prime ideal of A lying over J. □

4.2 Completions

Theorem 4.1.4 gives us a criterion for judging whether a polynomial f which is non-negative on K is contained in the quadratic module M. But it has only theoretical value, since we cannot test if f is contained in $M + I^k$ for all $k \geq 0$. In this section, we will introduce the concept of "completions" which will make the theorem practical.

4.2.1 Graded Ring and Filtration

A *graded ring* is a ring R that is expressible as $\bigoplus_{n \geq 0} R_n$ where R_n are additive subgroups such that $R_m R_n \subseteq R_{m+n}$. Sometimes, R_n is referred to as the n^{th} *graded piece* and elements of R_n are said to be *homogenous of degree* n. The prototype is a polynomial ring in several variables, with R_d consisting of all homogenous polynomials of degree d (along with the zero polynomial). A *graded module over a graded ring* R is a module M expressible as $\bigoplus_{n \geq 0} M_n$, where $R_m M_n \subseteq M_{m+n}$.

Note that the identity element of a graded ring R must belong to R_0. For if 1 has a component a of maximum degree $n > 0$, then $1a = a$ forces the degree of a to exceed n, a contradiction.

Now suppose that $\{R_n\}$ is a *filtration* of the ring R, in other words, the R_n are additive subgroups such that

$$R = R_0 \supseteq R_1 \supseteq ... \supseteq R_n \supseteq ...$$

with $R_n R_m \subseteq R_{m+n}$. We call R a *filtered ring.* A *filtered module*

$$M = M_0 \supseteq M_1 \supseteq ... \supseteq M_n \supseteq ...$$

over the filtered ring R may be defined similarly. In this case, each M_n is a submodule and we require that $R_m M_n \subseteq M_{m+n}$.

If I is an ideal of the ring R and M is an R module, we will be interested in the *I-adic filtrations* of R and of M, given respectively by $R_n = I^n$ and $M_n = I^n M$. (Take $I^0 = R$, so that$M_0 = M$.)

We can make M into a topological abelian group in which the module operations are continuous. The sets $I^m M$ are a base for the neighborhoods of 0, and the translations $x + I^m M$ form a basis for the neighborhoods of an arbitrary point $x \in M$. The resulting topology is called the *I-adic topology* on M.

4.2.2 Inverse Limits

Suppose we have countably many R-modules M_0, M_1,..., with R-module homomorphism $\theta_n : M_n \to M_{n-1}$, $n \geq 1$. The collection of modules and maps is called an *inverse system.*

A sequence (x_i) in the direct product $\prod M_i$ is said to be *coherent* if respects the maps θ_n in the sense that for every i we have $\theta_{i+1}(x_{i+1}) = x_i$. The collection M of all coherent sequences is called the *inverse limit* of the inverse system. The inverse limit is denote by

$$\underleftarrow{lim} M_n$$

Note that M becomes an R-module with componentwise addition and scalar multiplication of coherent sequences. In other words, $(x_i)+(y_i) = (x_i+y_i)$ and $r(x_i) = (rx_i)$. An inverse limit of an inverse system of rings can be constructed in a similar fashion, as coherent sequences can be multiplied componentwise, that is, $(x_i)(y_i) = (x_iy_i)$.

Example 4.2.1. (1). Take $R = \mathbb{Z}$, and let I be the ideal (p) where p is a fixed prime. Take $M_n = \mathbb{Z}/I^n$ and $\theta_{n+1}(a + I^{n+1}) = a + I^n$. The inverse limit of the M_n is the ring $\mathbb{Z}_p$ of p-adic integers.

(2). Suppose A is a commutative ring, let $R = A[x_1, ..., x_n]$ be a polynomial ring in n variables, and I the maximal ideal $(x_1, ..., x_n)$. Let $M_n = R/I^n$ and $\theta_n(f + I^n) = f+I^{n-1}$, $n = 1, 2, ...$ An element of M_n is represented by a polynomial f of degree at most $n-1$. (We take the degree of f to be the maximal degree of a monomial in f.) The image of f in I^{n-1} is represented by the same polynomial with the term of degree $n-1$ deleted. Thus the inverse limit can be identified with the ring $A[[x_1, ..., x_n]]$ of formal power series.

Remark 4.2.1. For any commutative ring A, the formal power series $f = \sum_{i=0}^{\infty} a_i x^i$ with coefficients in A form a ring, which is called *the power series ring over* A *in the variable of* x, denoted by $A[[x]]$. It is relatively straightforward to extend this idea to define a *formal power series ring over* A *in* n *variables*, denoted by $A[[x_1, ..., x_n]]$.

Elements of this ring may be expressed uniquely in the form $\sum_{i\in\mathbb{N}^n} a_i X^i$, where $a_i \in A$, $i = (i_1, ..., i_n) \in \mathbb{N}^n$ and X^i denotes monomial $x_1^{i_1}...x_n^{i_n}$.

4.2.3 Completion

Let $\{M_n\}$ be a filtration of R-module M. Recalling the construction of the reals from the rationals, or the process of completing an arbitrary metric space, let us try to come up with something similar in this case. If we go far out in a Cauchy sequence, the difference between terms becomes small. Thus we define a *Cauchy sequence* (x_n) *in* M by the requirement that for every positive integer r there is a positive integer N such that $x_n - x_m \in M_r$ for $n, m \geq N$. We identify the Cauchy sequences (x_n) and (y_n) if they get close to each other for large n. More precisely, given a positive integer r there exists a positive integer N such that $x_n - y_n \in M_r$ for all $n \geq N$. Notice that the condition $x_n - x_m \in M_r$ is equivalent to $x_n + M_r = x_m + M_r$. This suggests the essential feature of Cauchy condition is that the sequence is coherent with respect to the maps $\theta_n : M/M_n \to M/M_{n-1}$. Motivated by this observation, we define the *completion* of M as

$$\hat{M} = \varprojlim(M/M_n)$$

In particular, the completion of M with respect to the I-adic filtration $M_n = I^n M$ is called the *I-adic completion.* There is a natural map from a filtered module M to its completion $\hat{M}$ given by $x \to (x + M_n)$.

For an arbitrary commutative ring A, denote by $\hat{A}$ the completion of A at the ideal I, i.e., $\hat{A} = \varprojlim A/I^k$, $k \geq 1$. Let M be a quadratic module of A. The *closed* *quadratic module* in $\hat{A}$ generated by (the image of) M is $\hat{M} := \varprojlim (M + I^k)/I^k$. Clearly, $\hat{M}$ contains the image of M under the natural map $i\colon\ A \to \hat{A}$ defined by $i(a) = (a + I, a + I^2, ...)$.

Proposition 4.2.2. Suppose A is a commutative ring containing 1, I is a proper ideal of A, M is a quadratic module of A. Then $\hat{M} = \varprojlim (M + I^k)/I^k$ is a quadratic module of $\hat{A} = \varprojlim A/I^k$.

Proof. We look at the truncation map $\pi_k : \hat{A} \to \frac{A}{I^k}$ defined by $\pi_k((x_i)) = x_k + I^k$ for $(x_i) \in \hat{A}$. The operations in $\hat{A}$ is just what we defined for the inverse limit in 4.2.2, i.e., $(x_i) + (y_i) = (x_i + y_i)$, $(x_i)(y_i) = (x_i y_i)$. It is easy to check that π_k is a homomorphism.

Therefore, for any $(x_i), (y_i) \in \hat{M}$, $\pi_k((x_i)+(y_i)) = \pi_k((x_i))+\pi_k((y_i))$. Since $\pi_k((x_i))$, $\pi_k((y_i)) \in M+I^k$, $\pi_k((x_i)+(y_i)) \in M+I^k$ for any $k \geq 1$. This implies $(x_i)+(y_i) \in \hat{M}$. Similarly, for any $(z_i) \in \hat{A}$, $\pi_k((z_i)^2(x_i)) = [\pi_k((z_i))]^2\pi_k((x_i))$. $[\pi_k((z_i))]^2 \in \sum A^2+I^k$ and $\pi_k((x_i)) \in M + I^k$, so $\pi_k((z_i)^2(x_i)) \in M + I^k$ for any $k \geq 1$. This implies $(z_i)^2(x_i) \in \hat{M}$. Clearly, $1 \in \hat{M}$, where $1 = (1, 0, 0, ...)$. Thus, $\hat{M}$ is a is a quadratic module of $\hat{A}$. ☐

In particular, when $M = \sum A^2$, we have the following corollary:

Corollary 4.2.3. Suppose A is a commutative ring containing 1, I is a proper ideal of A. Then $\sum \hat{A}^2 \subseteq \widehat{\sum A^2} = \varprojlim (\sum A^2 + I^k)/I^k$.

Let $A = \mathbb{R}$ in the Example 4.2.1 (2). For any point $p = (p_1, ..., p_n) \in \mathbb{R}^n$, the completion of $\mathbb{R}[X] = \mathbb{R}[x_1, ..., x_n]$ at the maximal ideal $I = (x_1 - p_1, ..., x_n - p_n)$ (also called the *completion of* $\mathbb{R}[X]$ *at* p) is the formal power series ring $\mathbb{R}[[t_1, ..., t_n]]$ with coefficients in $\mathbb{R}$, where $t_i := x_i - p_i$. Then based on the remarks (2), (3) beneath the Theorem 4.1.4, we have the following result.

Corollary 4.2.4. (Scheiderer, [S4, Them 2.8]) Suppose S is a finite subset in $\mathbb{R}[X]$. K is the basic closed semi-algebraic set generated by S and M is the quadratic module generated by S. If M is archimedean, $f \geq 0$ on K and $\mathbb{R}[X]/J$ has (Krull) dimension ≤ 0, where $J := (M + (f)) \cap -(M + (f))$. Then the following are equivalent:

(1) $f \in M$.

(2) For each $a \in K$ with $f(a) = 0$, f lies in the closed quadratic module in $\widehat{\mathbb{R}[X]}_a$ generated by M. Here, $\widehat{\mathbb{R}[X]_a}$ denotes the power series ring $\mathbb{R}[[t_1, ..., t_n]]$, where $t_i = x_i - a_i$, $i = 1, ..., n$.

This Main Theorem allow us to work in the power series ring which has better properties than the polynomial ring. In the next chapter, I will prove some results in the power series ring and extend them to the polynomial ring by applying the Scheiderer's Main Theorem.

Chapter 5

Simple Version of the Main Theorem and its Application

In the last chapter, we have introduced Scheiderer's Main Theorem, which requires some advanced knowledge from commutative algebra to understand. However, if we consider the Main Theorem at the case of the polynomial ring in one variable, i.e., $\mathbb{R}[x]$, it is much easier to understand and apply, because we are not restricted by the dimensions of $\mathbb{R}[x]/J$ any more: this condition is always satisfied in the one variable case. Hence it is worth giving this 'simplified' Main Theorem (which is called the "simple version of the Main Theorem" in this thesis) here. In section 1, I will give the simple version of Main Theorem an independent proof. In the section 2, I will apply the Main Theorem and this simple version of Main Theorem to give some elementary proofs.

5.1 Simple Version of the Main Theorem

Recall Scheiderer's Main Theorem (Th 4.1.4) says:

Suppose A is Noetherian, M is archimedean, $f \geq 0$ on K and A/J has (Krull) dimension ≤ 0, where $J := (M + (f^2)) \cap -(M + (f^2))$. Then the following are equivalent:

(1) $f \in M$

(2) For each prime ideal I *lying over* J *and each* $k \geq 0$, $f \in M + I^k$.

Now let $A = \mathbb{R}[x]$, the polynomial ring in one variable, then $A = \mathbb{R}[x]$ is Noetherian. $\mathbb{R}[x]/J$ has dimension zero for any proper ideal J of $\mathbb{R}[x]$, since $\mathbb{R}[x]$ has dimension one. (Note that this is not true for the multi-variable polynomial ring.) Each prime ideal I lying over J is equal to $ker(a)$, where a is a root of f in K. $ker(a)$ is prime, hence $ker(a) = ((x-a))$, the ideal generated by $(x-a)$. By Theorem 3.1.4, K_S compact is equivalent to M_S archimedean. Therefore, we have the following simplified version of Main Theorem:

Theorem 5.1.1. Suppose S is a finite subset of $\mathbb{R}[x]$, the polynomial ring of one variable, $M = M_S$, $K = K_S$ as usual. Assume K is compact, $f \in \mathbb{R}[x]$, $f \neq 0$, and $f \geq 0$ on K, Then the following are equivalent:

1) $f \in M$

2) $f \in M + (f^2)$

3) For each root a of f in K, if $(x-a)^e \mid f$ and $(x-a)^{e+1} \nmid f$, then $f \in M + ((x-a)^{2e})$

3′) For each root a of f in K and each $n \geq 1$, $f \in M + ((x-a)^n)$

Proof. We show 1) $\Rightarrow$ 3′) $\Rightarrow$ 3) $\Rightarrow$ 2) $\Rightarrow$ 1)

1) $\Rightarrow$ 3′) Trivial.

3′) $\Rightarrow$ 3) Trivial.

Now, we are going to prove: 3) $\Rightarrow$ 2).

Observe that $f = \prod_{i=1}^{k} p_i^{e_i}$, where p_i is the irreducible polynomial of $\mathbb{R}[x]$. So for any $i \neq j$, the ideals $(p_i^{2e_i})$ and $(p_j^{2e_j})$ are coprime.

Then, by Chinese Remainder Theorem, we have the following isomorphism:

$$\frac{R[x]}{(f^2)} \cong \prod_{i=1}^{k} \frac{R[x]}{(p_1^{2e_i})}.$$

Using this, it suffices to show: $f \in M + (p_i^{2e_i})$ for each $i = 1, 2, ..., k$.

Because if $f \equiv f_i \pmod{p_i^{2e_i}}$ for $i = 1, 2, ..., k$, where $f_i \in M$, we can pick $e_i \in R[x]$, $e_i \equiv \delta_{ij} \pmod{p_j^{2e_i}}$, (where $\delta_{ij} = 0$ when $i \neq j$; $\delta_{ij} = 1$ when $i = j$), then by Chinese Remainder Theorem,

$$f \equiv \sum_{i=1}^{k} e_i f_i \pmod{(f^2)} \equiv \sum_{i=1}^{k} e_i^2 f_i \pmod{(f^2)}$$

which means $f \in M + (f^2)$

There are two possibilities for the irreducible polynomial p_i in $\mathbb{R}[x]$:

1. $p_i = (x-a)^2 + b^2$.

$p_i^{2e_i} = ((x-a)^2 + b^2)^{2e_i} = (x-a)^{4e_i} + 2e_i(x-a)^{4e_i-2}b^2 + ... + 2e_i(x-a)^2 b^{4e_i-2} + b^{4e_i}$.

Moving b^{4e_i} to the other side, yields

$$p_i^{2e_i} - b^{4e_i} = (x-a)^{4e_i} + 2e_i(x-a)^{4e_i-2}b^2 + ... + 2e_i(x-a)^2 b^{4e_i-2},$$

So, $p_i^{2e_i} - b^{4e_i}$ is a sum of squares. Therefore $p_i^{2e_i} - b^{4e_i} \in M$.

Then, $-b^{4e_i} = p_i^{2e_i} - b^{4e_i} - p_i^{2e_i} \in M + (p_i^{2e_i}) \implies -1 \in M + (p_i^{2e_i})$, which means $M + (p_i^{2e_i}) = \mathbb{R}[x]$. So, $f \in M + (p_i^{2e_i})$

2. $p_i = (x-a)$.

When $a \in K$, it is trivial.

When a is not in K, then there must exist $h \in S \subseteq M$ such that $h(a) < 0$.

$h(x) = g(x)(x-a) + h(a) \implies h(x) - h(a) = g(x)(x-a)$.

We denote $-h(a)$ by b, $b > 0$, then $(h(x)+b)^{2e_i} = [g(x)(x-a)]^{2e_i}$.

By the Binomial Theorem:

$$h(x)^{2e_i} + 2e_i b h(x)^{2e_i-1} + ... + b^{2e_i} = g(x)^{2e_i}(x-a)^{2e_i}.$$

Since $h(x)^{2k}$ a square, and $h(x) \in M$, $h(x)^{2k+1} = h(x)h(x)^{2k} \in M$ for any $k > 0$, which implies except for the last term, every term on the left side is contained in M. Therefore,

$-b^{2e_i} = h(x)^{2e_i} + 2e_i b h(x)^{2e_i-1} + ... + 2e_i h(x) b^{2e_i-1} - g(x)^{2e_i}(x-a)^{2e_i} \in M + (p_i^{2e_i})$.

Thus, $-1 \in M + (p_i^{2e_i})$, which means $M + (p_i^{2e_i}) = \mathbb{R}[x]$.

So, $f \in M + (p_i^{2e_i})$. That finishes the proof of 3) $\Rightarrow$ 2).

2) $\Rightarrow$ 1) We have already known from the Lemma 4.1.2. □

5.2 Applications

In chapter III, we proved that when $n = 1$, the associated semi-algebraic set K is compact, then any quadratic module M is a preordering. In this section, I will give another proof based on Scheiderer's Main Theorem. We first prove the result holds in the one variable power series ring:

Lemma 5.2.1. In the power series ring $\mathbb{R}[[t]]$, every positive unit is a square.

Note: for any $u \in \mathbb{R}[[t]]$, if $u = a_0 + a_1 t + ...$, where $a_0 \neq 0$, then we say u is a *unit* in $\mathbb{R}[[t]]$. If $a_0 > 0$, we say u is a *positive unit*; if $a_0 < 0$, we say u is a *negative unit*. If u is a positive (negative) unit, $1/u$ is also a positive (negative) unit. Furthermore, the product of two units are still unit. The product of two positive (negative) units is a positive unit; the product of a positive unit and a negative unit is a negative unit.

Proof. By hypothesis, $u = a_0 + a_1 t + ...$, where $a_0 > 0$. We try to write u as a square, i.e., $u = (b_0 + b_1 t + ...)^2$.

Compare the coefficients of each monomial, we get the following equations:

$$\begin{cases} b_0 = a_0 \\ 2b_0 b_1 = a_1 \\ 2b_0 b_2 + 2b_1^2 = a_2 \\ \dots \end{cases} \tag{5.1}$$

Easy to see that we can always solve b_0,b_1,... in turn from the above system of equations. Therefore any positive unit u is a square in $\mathbb{R}[[t]]$. □

Proposition 5.2.2. Let $\mathbb{R}[[t]]$ denote the power series ring in one variable; $M^c_{\{f,g\}}$ denote the quadratic module generated by f, g in $\mathbb{R}[[t]]$. Then, $fg \in M^c_{\{f,g\}}$.

Proof. For any $f \in R[[t]]$, $f = ut^k$, where u is a unit and $k \in \mathbb{Z}$, $k \geq 0$.

Assuming $f = u_1 t^{k_1}$; $g = u_2 t^{k_2}$, our objective is finding three sums of squares in $\mathbb{R}[[t]]$: $\sigma_0, \sigma_1, \sigma_2$ such that: $fg = \sigma_0 + \sigma_1 f + \sigma_2 g$.

There are 16 cases about f and g depending on u_i and k_i $(i = 1, 2)$ totally. But most of them are very similar. By symmetry, we only need to consider the following 6 cases:

1. If u_1 is positive, k_1 is even; no matter what are u_2 and k_2. We can set $\sigma_0 = 0, \sigma_1 = 0, \sigma_2 = u_1 t^{k_1}$.

2. If u_1 is negative, k_1 is even; no matter what are u_2 and k_2. We can set $\sigma_0 = -(\frac{g-1}{2})^2 f, \sigma_1 = (\frac{g+1}{2})^2, \sigma_2 = 0$.

3. If u_1 is negative, k_1 is odd; and u_2 is negative, k_2 is odd. Then we can set $\sigma_0 = u_1 u_2 t^{k_1} t^{k_2}, \sigma_1 = 0, \sigma_2 = 0$.

4. If u_1 is positive, k_1 is odd; and u_2 is positive, k_2 is odd. Then we can set $\sigma_0 = u_1 u_2 t^{k_1} t^{k_2}, \sigma_1 = 0, \sigma_2 = 0$.

5. u_1 is negative, k_1 is odd; u_2 is positive, k_2 is odd and $k_2 \geq k_1$. Then we can set

$\sigma_0 = -fg, \sigma_1 = g^2 - fg - \frac{u_2}{u_1}t^{k_2-k_1}, \sigma_2 = (f+1)^2 - fg.$

It is easy to verify that $fg = \sigma_0 + \sigma_1 f + \sigma_2 g$.

6. u_1 is negative, k_1 is odd; u_2 is positive, k_2 is odd and $k_1 > k_2$. Then we can set

$\sigma_0 = -fg, \sigma_1 = (g+1)^2 - fg, \sigma_2 = f^2 - fg - \frac{u_1}{u_2}t^{k_1-k_2}.$

It is easy to verify that $fg = \sigma_0 + \sigma_1 f + \sigma_2 g$.

Now, all the cases have been considered, so we can conclude that $fg \in M^c_{\{f,g\}}$. □

Remark 5.2.1. The result does not hold for multi-variable power series rings. See the following example:

Example 5.2.3. $xy \notin M^c_{\{x,y\}}$, the quadratic module generated by x and y in the power series ring $\mathbb{R}[[x, y]]$.

Proof. Suppose $xy \in M^c_{\{x,y\}}$, then

$$xy = \alpha + \beta x + \gamma y, \tag{5.2}$$

where α, β, γ are sum of squares in the power series ring $\mathbb{R}[[x, y]]$. Assume

$$\alpha = \textstyle\sum_{k=1}^{n}(\alpha_{k0} + \alpha_{k1}x + \alpha_{k2}y + ...)^2;$$

$$\beta = \textstyle\sum_{k=1}^{m}(\beta_{k0} + \beta_{k1}x + \beta_{k2}y + ...)^2;$$

$$\gamma = \textstyle\sum_{k=1}^{l}(\gamma_{k0} + \gamma_{k1}x + \gamma_{k2}y + ...)^2$$

Compare the constant terms from both sides of identity (5.2): The left side does not have the constant term, so $\sum_{k=1}^{n}(\alpha_{k0})^2 = 0$ and $\alpha_{k0} = 0$, $k = 1, 2, ..., n$. Therefore, $\alpha = \sum_{k=1}^{n}(\alpha_{k1}x + \alpha_{k2}y + ...)^2$. Similarly, by comparing the coefficients of the terms x and y of both sides, we have: $\sum_{k=1}^{m}(\beta_{k0})^2 = 0$ and $\sum_{k=1}^{l}(\gamma_{k0})^2 = 0$, so $\beta_{k0} = 0$, $k = 1, 2, ..., m$; and $\gamma_{k0} = 0$, $k = 1, 2, ..., l$. The lowest powers of βx and γy are 3, therefore xy comes from α. But by comparing the coefficients of the term x^2 and y^2 of both sides, we have $\alpha_{k1} = \alpha_{k2} = 0$, $k = 1, 2, ..., n$. Therefore, the lowest powers of α is 4, which is impossible. A contradiction. $\square$

Suppose S is a finite subset of $\mathbb{R}[x]$, we use M_S^c denotes the quadratic module generated by (the image of) S in the power series ring, i.e., the smallest quadratic module containing (the image of) S in $\mathbb{R}[[x]]$. By Proposition 4.2.2, $\hat{M}_S$ is also a quadratic module in $\mathbb{R}[[x]]$ containing (the image of) M_S and hereby containing (the image of) S. Therefore, $M_S^c \subseteq \hat{M}_S$. Combining with Theorem 3.1.4 and Proposition 5.2.2, yields the following result which has been proved in a totally different way in chapter III:

Theorem 5.2.4. $\mathbb{R}[x]$ is the polynomial ring in one variable, S is a finite subset, K_S compact. Then $M_S = T_S$.

Proof. For any f, $g \in M_S$, $f \geq 0$ on K_S, $g \geq 0$ on K_S, therefore, $fg \geq 0$ on K_S. By Proposition 5.2.2, for any $a \in \mathbb{R}$, $fg \in M_{\{f,g\}}^c \subseteq M_S^c \subseteq \hat{M}_S$, the closed quadratic module in $\mathbb{R}[[x - a]]$ generated by S. By Theorem 3.1.4, M_S is archimedean, hence Scheiderer's Main Theorem applies, $fg \in M_S$. M_S is closed under multiplication. $\square$

In chapter III, we mentioned an important criterion (Them 3.1.2) in one variable case giving the necessary and sufficient conditions for T_S saturated when K_S is compact. Since we already know that $T_S = M_S$ in the one variable case, we can restate this theorem as following:

Theorem 5.2.5. Let $K_S = \bigcup_{j=0}^{k} [a_j, b_j]$, $b_{j-1} < a_j$, $j = 1, 2, ..., k$, $S = \{g_1, ..., g_s\}$, Then M_S is saturated if and only if the following two conditions hold:

(a) for each endpoint a_j $\exists i \in \{1, ..., s\}$ such that $g_i(a_j) = 0$ and $g_i'(a_j) > 0$,

(b) for each endpoint b_j $\exists i \in \{1, ..., s\}$ such that $g_i(b_j) = 0$ and $g_i'(b_j) < 0$.

Proof. (Necessity)

We prove the necessity of condition (a). The necessity of condition (b) is proved similarly.

Let $a = a_j$. There exists $f \in R[X]$ (of degree two), $f \geq 0$ on K_S, $f(a) = 0$, $f^{'}(a) > 0$. Since T_S is saturated, f has a representation

$$f = \sum_{i=0}^{s} \sigma_i g_i, \text{ where } g_0 = 1,\ \sigma_i \in \sum \mathbb{R}[X]^2\ i = 0, 1, ..., s.$$

Since $f(a) = 0$, and each term $\sigma_i g_i \geq 0$ at a, $\sigma_i g_i = 0$ for all $i = 0, 1, ..., s$. Then each term $\sigma_i g_i$ is divisible by $x - a$. Since $f^{'}(a) > 0$, there exists i with $(\sigma_i g_i)^{'}(a) > 0$. If $(x-a)^2 \mid \sigma_i g_i$, then $(\sigma_i g_i)^{'}(a) = 0$, a contradiction. Thus $\sigma_i(a) \neq 0$, $g_i(a) = 0$, and $\sigma_i(a)$ is strictly positive at a. So $g_i^{'}(a) > 0$.

(Sufficiency)

By Theorem 5.1.1, we only need to show: for each root a of f in K_S, if $(x-a)^e \mid f$ and $(x-a)^{e+1} \nmid f$, then $f \in M + ((x-a)^{2e})$

Assume $f(x) = h(x)(x-a)^e$, $h(a) \neq 0$ and $e \in \mathbb{N}$. If a is an interior point of K_S, then $h(a) > 0$ and e is an even number, say $e = 2d$, where $d \geq 0$. Otherwise, we can find a point b which is contained in K_S and close enough to a such that $f(b) < 0$.

We assume $h(x) = a_n(x-a)^n + a_{n-1}(x-a)^{n-1} + ... + h(a), n \geq 2d-1$ (otherwise, we let $a_i = 0$ when $i = n+1, ..., 2d-1$). Since $h(a) > 0$, $a_{2d-1}(x-a)^{2d-1} + ... + a_1(x-a) + h(a)$ is a positive unit in $\mathbb{R}[[x-a]]$ and hereby a square in $\mathbb{R}[[x-a]]$. By Corollary 4.2.3, there exists a $r_1(x) \in ((x-a)^{2d})$ such that

$$g(x) = r_1(x) + a_{2d-1}(x-a)^{2d-1} + ... + a_1(x-a) + h(a) \in \sum \mathbb{R}[x]^2.$$

Since $h(x) - g(x) \in ((x-a)^{2d})$,

$$f(x) - (x-a)^{2d} g(x) = (x-a)^{2d}(h(x) - g(x)) \in ((x-a)^{4d}),$$

where $(x-a)^{2d} g(x) \in \sum \mathbb{R}[x]^2 \subseteq M$. Therefore, $f(x) \in M + ((x-a)^{4d})$.

If a is a non-isolated boundary point of K_S. We assume a is a left endpoint. Then, $f(x) = (x-a)^e h(x)$ and $h(a) > 0$. If e is even, we can prove it in the same way as interior point case. If e is odd, assume $e = 2d+1$. By condition (a), there exists a $g(x) \in S \subseteq M$ such that $g(a) = 0$ and $g'(a) > 0$. So $g(x) = p(x)(x-a)$, where $p(x) = c_m(x-a)^m + ... + c_1(x-a) + p(a)$ and $p(a) > 0$.

Assume $h(x) = a_n(x-a)^n + ... + a_1(x-a) + h(a)$, $n \geq 2d+1$. We choose

$$q(x) = b_{2d+1}(x-a)^{2d+1} + ... + b_1(x-a) + q(a)$$

such that

$$q(x)p(x) = u(x)(x-a)^{2d+2} + a_{2d+1}(x-a)^{2d+1} + ... + a_1(x-a) + h(a)$$

for some $u(x)$. This is possible by solving $q(a)$, b_1, ..., b_{2d+1} in turn from the following system of equations:

$$\begin{cases} q(a)p(a) = h(a) \\ b_1 p(a) + q(a)c_1 = a_1 \\ b_2 p(a) + c_1 b_1 + q(a)c_2 = a_2 \\ \text{......} \\ b_{2d+1}p(a) + b_{2d}c_1 + ... + q(a)c_{2d+1} = a_{2d+1} \end{cases} \tag{5.3}$$

Since $q(a) = h(a)/p(a) > 0$, By Corollary 4.2.3, there always exists a $r_2(x) \in ((x-a)^{2d+2})$ such that $q(x) + r_2(x) \in \sum \mathbb{R}[x]^2$.

$$h(x) - p(x)q(x) \in ((x-a)^{2d+2}), \text{ so}$$

$$h(x) - p(x)(q(x) + r_2(x)) = h(x) - p(x)q(x) - r_2(x)p(x) \in ((x-a)^{2d+2}).$$

Thus,

$f(x) - (x-a)^{2d}(q(x) + r_2(x))g(x) = (x-a)^{2d+1}[h(x) - p(x)(q(x) + r_2(x))] \in ((x-a)^{4d+3}) \subseteq ((x-a)^{4d+2})$, where $g(x) \in M$ and $(x-a)^{2d}(q(x)+r_2(x)) \in \sum \mathbb{R}[x]^2$

Therefore, $f(x) \in M + ((x-a)^{4d+2})$.

The proof is similar when a is a right endpoint.

If a is an isolated boundary point of K_S, i.e., a is both a left endpoint and a right endpoint. So both condition (a) and (b) hold for a. $f(x) = (x-a)^e h(x)$, $h(x) = a_n x^n + a_{n-1}x^n - 1 + ... + h(a)$, $n \geq e$. When e is even, $h(a) > 0$, apply the same argument as the interior point case; when e is even, $h(a) < 0$, apply the same argument as the right endpoint case; when e is odd, $h(a) > 0$, apply the same argument as the left endpoint case. So there is only one case left: e is even, $e = 2d$ and $h(a) < 0$.

We have $g_1, g_2 \in S \subseteq M_S$ such that, $g_1(a) = 0, g_1'(a) > 0; g_2(a) = 0, g_2'(a) < 0$. So, $g_1(x) = p_1(x)(x-a), g_2(x) = p_2(x)(x-a)$ where

$$p_1(x) = b_m(x-a)^m + ... + b_1(x-a) + p_1(a),\ p_1(a) > 0;$$

$$p_2(x) = c_l(x-a)^l + ... + c_1(x-a) + p_2(a),\ p_2(a) < 0.$$

We construct

$$q_1(x) = r(x-a)^2 + t(x-a) - \tfrac{p_2(a)}{p_1(a)}$$

where $t < \frac{b_1\frac{p_2(a)}{p_1(a)} - c_1}{p_1(a)}$, $r = t^2/[-4\frac{p_2(a)}{p_1(a)}]$. Therefore, $q_1(x)$ is a square and hence $\in \sum \mathbb{R}[x]^2$. Then

$$q_1(x)p_1(x) + p_2(x) = (x-a)[(x-a)v(x) + s]$$

for some $v(x) \in \mathbb{R}[x]$ and $s = tp_1(a) - b_1\frac{p_2(a)}{p_1(a)} + c_1 < 0$.

By comparing the coefficients and solving the system of equations, we can choose $q_2(x) = d_{2d-1}(x-a)^{2d-1} + ... + d_1(x-a) + q_2(a)$ such that

$$q_2(x)[(x-a)v(x) + s] = w(x)(x-a)^{2d} + a_{2d-1}(x-a)^{2d-1} + ... + a_1(x-a) + h(a)$$

for some $w(x) \in \mathbb{R}[x]$, where $q_2(a) = \frac{h(a)}{s} > 0$.

Then, $h(x) - q_2(x)[(x-a)v(x) + s] \in ((x-a)^{2d})$.

By Corollary 4.2.3, there exists a $r_3(x) \in ((x-a)^{2d})$ such that $r_3(x)+q_2(x) \in \sum \mathbb{R}[x]^2$.

Therefore,

$$f(x) - (x-a)^{2d-2}(r_3(x) + q_2(x))[q_1(x)g_1(x) + g_2(x)] =$$
$$(x-a)^{2d}\{h(x) - q_2(x)[(x-a)v(x) + s] - r_3(x)[(x-a)v(x) + s]\} \in ((x-a)^{4d}),$$

where $(x-a)^{2d-2}(r_3(x) + q_2(x)) \in \sum \mathbb{R}[x]^2$ and $q_1(x)g_1(x) + g_2(x) \in M$. Thus $f \in M + ((x-a)^{4d})$.

□

In fact, this theorem is just a special case of a general criterion for curves proved in [S3, Th. 5.17]. It can be also found in [K-S-M]. Here we apply the simple version of the Main Theorem to give another proof.

Bibliography

[A-C] P. Alexander,N.D. Charles, *Positive Polynomials: from Hilbert's 17th problem to real algebra*, Springer-Verlag, New York, 2001.

[Ar] E. Artin, *Uber die Zerlegung definiter Funktionen in Quadrate.*, Hamb. Abh. 5 (1927), 100-115; see Collected Papers (S. Lang, J.Tate, eds.), Addison-Wesley 1965, reprinted by Springer-Verlag, New York, et. al. , pp. 273-288.

[At-M] M.F. Atiyah, I.G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Pub. Co., 1969.

[B] C. Berg, *Moment problems and orthogonal polynomials*, preprint.

[B-C-R] J. Bochnak, M. Coste, M-F. Roy, *Real algebraic geometry*, Springer-Verlag, 1998.

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

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

[H1] E. K. Haviland, *On the momentum problem for distribution functions in more than one dimension*, Amer. J. Math. 57 (1935), 562-572.

[H2] E. K. Haviland, *On the momentum problem for distribution functions in more than one dimension II*, Amer. J. Math. 58 (1936), 164-168.

[Hi1] D. Hilbert, *Uber turnare definite Formen*, Acta Math. 17 (1893), 169-197; see Ges. Abh. 2, 345-366, Springer, Berlin, 1933, reprinted by Chelea, New York, 1981.

[Hi2] D. Hilbert, *Mathematische Probleme*, Arch. f. Math. u. Phys. 3 (1901), 44-63, 213-237; see Ges. Abh. 3, 290-329, Springer, Berlin, 1935, reprinted by Chelsea, New York, 1981; English translation by Mary Winston in Bull. Amer. Math. Soc. 8 (1902), 437-479.

[F] Keqin Feng, *Basic commutative algebra*, Higher Education Press, 1985.

[J] T. Jacobi, *A representation theorem for certain partially ordered commutative rings*, Math. Zeit. 237 (2001), 223-235.

[J-P] T. Jacobi, A. Prestel, *Distinguished representation of strictly positive polynomials*, J. reine angew. Math. 532 (2001), 223-235.

[K] I. Klep, *A Kadison-Dubois representation for associative rings*, preprint.

[Ka] R.V. Kadison, *A representation theory for commutative topological algebra*, Memoirs of the Amer. Math. Soc. 7 (1951).

[K-M] S. Kuhlmann, M. Marshall, *Positivity, sums of squares and the multi-dimensional moment problem*, Trans. Amer. Mat. Soc. 354 (2002), 4285-4301.

[K-M-S] S. Kuhlmann, M. Marshall, N. Schwartz, *Positivity, sums of squares and the multi-dimensional moment problem II*, Adv. Geom. 5 (2005), no. 4, 583–606.

[M1] M. Marshall, *Positive polynomials and sums of squares, Dottorato de Ricerca in Mathematica*, Univ. Pisa, 2000.

[M2] M. Marshall, *A General Representation Theorem For Partially Ordered Commutative Rings*, Math. Zeit. 242 (2002), no. 2, 217–225.

[M3] M. Marshall, *Approximation positive polynomials using sums of squares*, Canada. Math. Bull. 46 (2003), 400-418.

[M4] M. Marshall, *Representations of non-negative polynomials having finitely many zeros*, (2004).

[M5] M. Marshall, *Quadratic modules and quadratic preorderings*, preprint (2004).

[M6] M. Marshall, *Representations of non-negative polynomials, degree bounds and applications to optimization*, (2006).

[Mo] T.S. Motzkin, *The arithmetic-geometric inequality*, In: Inequalities (Ed. O. Shisha), Academic Press, New York, (1967), 205-244.

[N] T. Netzer, *An elementary proof of Schmüdgen's Theorem on the moment problem of closed semi-algebraic sets*, preprint.

[P-S] V. Powers, C. Scheiderer, *The Moment Problem for non-compact semialgebraic sets*, Adv. Geom. 1 (2001), 71-88.

[P] M. Putinar, *Positive polynomials on compact semi-algebraic sets*, Indiana Univ. Math. J. 42 (1993), 969-984.

[Re] B. Reznick, *Some concrete aspects of Hilbert's 17th problem*, in: Real Algebraic Geometry and Ordered Structures (Eds. C.N. Delzell, J.J. Madden), Contemporary Mathematics, vol. 253, Amer. Math. Soc., Providence, RI 2000, pp. 251-272.

[S1] C. Scheiderer, *Sums of squares of regular functions on real algebraic varieties*, Trans. Amer. Math. Sco. 352 (1999), 1039-1069.

[S2] C. Scheiderer, *Positivity and sums of squares: a guide to some recent results*, Preprint 2003, available at www.Ihp-raag.org/publications.

[S3] C. Scheiderer, *Sum of squares on real algebraic curves*, Math. Zeit. 245 (2003), 725-760.

[S4] C. Scheiderer, *Distinguished representations of non-negative polynomials*, J. Algebra 289 (2005), 558-573.

[S5] C. Scheiderer, *Sum of squares on real algebraic surfaces*, Manuscripta Math. 119 (2006), no. 4, 395–410.

[Sc] K. Schmüdgen, *The K-moment problem for compact semi-algebraic sets*, Math. Ann. 289 (1991), 203-206.

[Schw] N. Schwartz, *About Schmüdgen's Theorem*, presented in the seminar "Reelle algebraische Geometrie" in Regensburg (2003).

[St] G. Stengle, *A nullstellensatz and a positivstellensatz in semialgebraic geometry*, Math. Ann. 207 (1974), 87-97.

[T] A. Tarski, *A decision method for elementary algebra and geometry*, University of California Press Press, 1948

[W1] T. Wörmann, *Short algebraic proofs of theorems of Schmüdgen and Polya*, preprint.

[W2] T. Wörmann, *Strikt positive Polynome in der semialgebraischen Geometrie*, PhD Thesis, Dortmund, 1998.