Polynomial Optimization Methods

Piet van Eeghen

March 8, 2013

Master Thesis Mathematics

Supervisor: Prof. dr. A. Schrijver

Faculty of Science
University of Amsterdam

Abstract

This thesis is an exposition of ideas and methods that help understanding the problem of minimizing a polynomial over a basic closed semi-algebraic set. After the introduction of some theory on mathematical tools such as sums of squares, nonnegative polynomials and moment matrices, several Positivstellensätze are considered. Positivstellensätze provide sums of squares representations of polynomials, positive on basic closed semi-algebraic sets. Subsequently, semi-definite programming methods, in particular based on Putinar's Postivstellensatz, are considered. In order to use semi-definite programming, certain degree bounds are set. These bounds give rise to a hierarchy of approximations of the minimum of a polynomial, which will also be discussed. Finally, some new results are given that are obtained by looking at sums of squares representations of a positive polynomial when minimizing over the unit hypercube .

Master Thesis

Title: Polynomial Optimization Methods

Author: Piet van Eeghen, cpvaneeghen@gmail.com, 6390137
Thesis advisor: Prof. M. Laurent
Supervisor: Prof. dr. A. Schrijver
Co-supervisor: Prof. dr. A.J. Homburg
Member of examination board: dr. J. H. Brandts

Date: March 8, 2013

Korteweg de Vries Institute for Mathematics
University of Amsterdam
Science Park 904, 1098 XH Amsterdam
The Netherlands

Contents

Introduction

In this thesis we are focusing on the following optimization problem: given a polynomial p and a subset K of $\mathbb{R}^n$, find

$$p_{min} := \inf\{p(x) : x \in K\}. \tag{1}$$

Note that this problem becomes a linear program when p is a linear function and K is a polytope. However, this problem is NP-hard in general. This can be understood by the following examples where $K = \mathbb{R}^n$.

Example 0.1. The partition problem asks whether, for a set of positive integers $a_1, ..., a_n$, there exists a subset $J \subset \{1, ..., n\}$ such that

$$\sum_{i \in J} a_i = \sum_{i \in \{1,...,n\} \setminus J} a_i.$$

This problem can also be formulated as a polynomial minimization problem. For this purpose we consider the following polynomial:

$$p := \left(\sum_{i=1}^{n} a_i X_i \right)^2 + \sum_{i=1}^{n} (X_i^2 - 1)^2.$$

Let p_{min} denote the minimum of p over $\mathbb{R}^n$. Now we have that $p_{min} = 0$ if and only if there exist a partition of the set $\{a_1, ..., a_n\}$. Note indeed that if $p_{min} = 0$, then $\sum_{i=1}^{n} a_i X_i = 0$ and $X_i = \pm 1$ for $i \in \{1, ..., n\}$. As is explained in [6], the partition problem is an NP-complete problem.

Remark 0.2. Note that it does not matter whether we consider p over $\mathbb{R}^n$, $[-1, 1]^n$ or $\{-1, 1\}^n$ when checking whether the minimum of p equals 0. In all cases the minimum of p equals 0 if and only if there is a partition of the set $\{a_1, ..., a_n\}$.

Example 0.3. A matrix $M \in \mathbb{R}^{n\times n}$ is said to be copositive if $x^T M x \geq 0$ for all $x \in \mathbb{R}^n_{\geq 0}$. Clearly, this is the same as checking whether $p_{min} \geq 0$ for the polynomial $p := \sum_{i,j=1}^n X_i^2 X_j^2 M_{ij}$, where $p \in \mathbb{R}[X_1, ..., X_n]$. As is explained in [23], testing whether a matrix is not copositive is an NP-complete problem.

Throughout this thesis, instead of looking at the infimum as in (1) we consider the supremum

$$p_{min} = \sup\{\lambda \in \mathbb{R} : p - \lambda \geq 0 \text{ on } K\}, \tag{2}$$

which obviously gives the same value for p_{min}. We will study relaxations of this problem, which are obtained by considering sums of squares representations of positive polynomials. The representations are obtained when K in (2) is a basic closed semi-algebraic set. We are going to use semi-definite programming to find these representations and to create a hierarchy of approximations for p_{min} as described in (2), where K is a basic closed semi-algebraic set.

Outline of this thesis

The first chapter introduces some necessary preliminaries for the rest of the thesis.
The second chapter mostly serves as an introduction to the set of sums of squares polynomials and the set of nonnegative polynomials. We give an exposition of the study of relationships between the two sets, initiated by Hilbert. Then, in Theorem 2.8, it is stated that every nonnegative polynomial can be approximated with an a priori fixed precision by a sum of squares of polynomials. For this result Lasserre [12] received the Lagrange Prize 2009.
The third chapter starts with an introduction to the concepts moment matrices and moments sequences and explains the duality relation between sums of squares and sequences whose moment matrix is positive semi-definite. Then some more properties of moment matrices are given. Subsequently, in Theorem 3.8 characterizations of moment sequences with a representing measure on the hypercube are given. This chapter ends with the proof of Theorem 2.8 by Lasserre. This proof combines most of the theory of the third chapter.
In the fourth chapter we make the reader familiar with Positivstellensätze, in particular with Putinar's Positivstellensatz. Positivstellensätze give sum of squares representations for polynomials that are positive on a basic closed

semi-algebraic set.
Then in the fifth chapter we discuss sequences of semi-definite programming relaxations, in particular relaxations of Putinar's Positivstellensatz. From these approximations, approximation hierarchies are deduced. We will discuss under what conditions these hierarchies have finite convergence.
In the sixth chapter we consider minimization of the polynomial $X_1 \cdots X_n$ over the n-dimensional unit cube and give some new obtained results regarding sums of squares representations for the polynomial $X_1 \cdots X_n$ in the quadratic module of the unit hypercube.

Notations

$\underline{X}$ is shorthand for the n-tuple of variables $(X_1, ..., X_n)$.
We write $\mathbb{R}[\underline{X}]$ for $\mathbb{R}[X_1, ..., X_n]$.
Further by $x = (x_1, ..., x_n) \in \mathbb{R}^n$ we indicate the vector x.
Moreover, for a polynomial $f \in \mathbb{R}[\underline{X}]$, $f(x)$ denotes the result of evaluating f at x.

Chapter 1

Preliminaries

In this chapter we introduce positive semi-definite matrices. We give several characterizations of a matrix for being positive semi-definite. Subsequently we introduce semi-definite programming and some of its duality theory relevant for this thesis. The chapter is based on [16] and [17].

1.1 Positive semi-definite matrices

Let S^n denote the set of symmetric matrices in $\mathbb{R}^{n\times n}$. The following theorem is mostly based on the spectral decomposition theorem. This spectral theorem states that any $X \in S^n$ has eigenvalues $\lambda_1, ..., \lambda_n$ and corresponding eigenvectors $v_1, ..., v_n$ that form an orthonormal system in $\mathbb{R}^n$. As a consequence X can be written as $X = \sum_{i=1}^{n} \lambda_i v_i v_i^T$.

Theorem 1.1. Let $X \in S^n$. The following assertions are equivalent.

(1) X is positive semi-definite (abbreviated as *PSD*). This is denoted by $X \succeq 0$. We use the following definition: $X \succeq 0$ if $x^T X x \geq 0$ for all $x \in \mathbb{R}^n$.

(2) The eigenvalues of X are nonnegative.

(3) $X = LL^T$ for some matrix $L \in \mathbb{R}^{n\times k}$ (for some $k \geq 1$). We call this decomposition a Choleski decomposition of X.

(4) There exist vectors $v_1, ..., v_n \in \mathbb{R}^k$ (for some $k \geq 1$), such that $X_{ij} = v_i^T v_j$ for all $i, j \in \{1, ..., n\}$. The matrix X is called the Gram matrix of the vectors $v_1, ..., v_n$.

(5) All principal minors of X are nonnegative.

By $S^n_{\succeq 0}$ we denote the cone of positive semi-definite matrices. To define its dual cone we introduce the trace inner product of two matrices $X, Y \in \mathbb{R}^{n\times n}$ as follows:

$$\langle X, Y\rangle = \sum_{i=1}^{n}\sum_{j=1}^{n} X_{ij}Y_{ij}. \tag{1.1}$$

The dual cone of $S^n_{\succeq 0}$ is given by

$$(S^n_{\succeq 0})^* = \{X \in S^n : \langle X, Y\rangle \geq 0 \quad \text{for all} \quad Y \in S^n_{\succeq 0}\}. \tag{1.2}$$

Note that $(S^n_{\succeq 0})^* = S^n_{\succeq 0}$ since we have that

$$\begin{aligned}
\langle X, Y\rangle \geq 0 \ \text{ for all } \ Y \in S^n_{\succeq 0} &\Leftrightarrow \left\langle X, \sum_i \lambda_i v_i v_i^T \right\rangle \geq 0 \ \text{ for all } \ v_i \in \mathbb{R}^n, \lambda_i \geq 0 \\
&\Leftrightarrow \lambda \left\langle X, vv^T \right\rangle \geq 0 \ \text{ for all } \ v \in \mathbb{R}^n, \lambda \geq 0 \\
&\Leftrightarrow v^T X v \geq 0 \ \text{ for all } \ v \in \mathbb{R}^n \\
&\Leftrightarrow X \succeq 0.
\end{aligned}$$

In other words the cone $S^n_{\succeq 0}$ is self-dual.

1.2 Semi-definite programming

Semi-definite programming is a generalization of linear programming. Whereas one optimizes over $\mathbb{R}^n_{\geq 0}$ in linear programming, one optimizes over $S^n_{\succeq 0}$ in semi-definite programming. Semi-definite programming is interesting because there exist polynomial time algorithms to solve a semi-definite program (abbreviated as *sdp*). A method that can be used to solve a semi-definite program in polynomial time up to a fixed precision is the ellipsoid method [19]. However in practice it turns out that this method is too time consuming. Therefore, as an alternative method, the interior point method [34] is often used.

Since semi-definite programming is a generalization of linear programming, every linear program can be written as an sdp. To understand this, recall that the standard primal form of a linear program is given by

$$\min\{c^T x : a_j x = b_j, j \in \{1, ..., m\}, x \in \mathbb{R}^n_{\geq 0}\}, \tag{1.3}$$

where $c, a_j \in \mathbb{R}^n$ and $b_j \in \mathbb{R}$. The standard primal form of an sdp is given by

$$\sup_{X \in S_n} \{\langle C, X\rangle : \langle A_1, X\rangle = b_1, ..., \langle A_m, X\rangle = b_m,\ X \succeq 0\}. \tag{1.4}$$

Here $A_1, ..., A_m, C \in S^n$ and $b_j \in \mathbb{R}$. So if we set $C = \text{diag}(c_1, ..., c_n)$ and $A_j = \text{diag}((a_j)_1, ..., (a_j)_n)$ in (1.4), we obtain (1.3).
We say that the sdp in (1.4) is *feasible* if the set

$$\{X \in S^n : \langle A_1, X\rangle = b_1, ..., \langle A_m, X\rangle = b_m,\ X \succeq 0\} \tag{1.5}$$

is non-empty. We say the sdp is *strictly feasible* if there exists an element in the set described in (1.5, which is an element of the interior of the semi-definite cone. The dual of (1.4) is given by

$$\inf \left\{ \sum_{j=1}^{m} y_j b_j : y_1, ..., y_m \in \mathbb{R}, \sum_{j=1}^{m} y_j A_j - C \succeq 0 \right\}. \tag{1.6}$$

Feasibility and strict feasibility for the dual program are defined analogously. We now state the following fundamental result on primal and dual sdp's.

Theorem 1.2. Given a pair of primal and dual semi-definite programs as above. Let p^* be the supremum of the primal program and let d^* be the infimum of the dual program.

(i) (*Weak duality*). Suppose X is a feasible solution of the primal program and y is a feasible solution of the dual program. Then

$$\langle C, X\rangle \leq b^T y. \tag{1.7}$$

So $p^* \leq d^*$.

(ii) (*Strong duality*). If the primal sdp is bounded from above and strictly feasible, then the dual sdp attains its infimum and there is no duality gap.
If the dual sdp is bounded from below and strictly feasible, then the primal sdp attains its supremum and there is no duality gap: $p^* = d^*$.

Proof. The proof of strong duality is omitted. See for example Chapter 3 of [17]. The proof of weak duality is as follows:

$$\sum_{j=1}^{m} y_j b_j = \sum_{j=1}^{m} y_j \langle A_j, X\rangle \geq \langle C, X\rangle\,, \tag{1.8}$$

where, in the last inequality, we have used the fact that $S^n_{\succeq 0}$ is self-dual and that $\sum_{j=1}^n y_j A_j - C \succeq 0$ and $X \succeq 0$ to see that $\left\langle \sum_{j=1}^m y_j A_j - C, X \right\rangle \geq 0$. $\square$

Chapter 2

Sums of squares and nonnegative polynomials

In this chapter we introduce the set of sums of squares and the set of nonnegative polynomials. We state that every nonnegative polynomial can be written as a sum of squares of polynomials by adding an arbitrarily small high degree perturbation to it. Further we show how the problem of checking whether a polynomial is a sum of squares can be transformed to solving an sdp. Moreover we give sufficient conditions, in terms of their coefficients, for polynomials to be sums of squares of polynomials.

2.1 Preliminaries on polynomials

This section is based on [31] and Chapter 1 of [20].

Let $\mathbb{R}[\underline{X}]$ denote the polynomial ring $\mathbb{R}[X_1, ..., X_n]$ for short. A polynomial $p \in \mathbb{R}[\underline{X}]$ can be written as $p = \sum_\alpha p_\alpha \underline{X}^\alpha$ for finitely many $p_\alpha \neq 0$, where $p_\alpha \in \mathbb{R}$, $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n$ and $\underline{X}^\alpha = X_1^{\alpha_1} \dots X_n^{\alpha_n}$. So p is a sum of finitely many non-zero terms $p_\alpha \underline{X}^\alpha$ for $\alpha \in \mathbb{N}^n$. The maximum value $|\alpha| = \sum \alpha_i$ for which $p_\alpha \neq 0$ is the degree of p. A homogeneous polynomial or *form* is a polynomial whose monomials all have the same degree.
For a nonnegative integer d, we denote by $[\underline{X}]_d$ the vector consisting of all monomials $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ of degree at most d. Moreover $\mathbb{R}[\underline{X}]_d$ denotes the set of polynomials in $\mathbb{R}[\underline{X}]$ with degree d or smaller.

Remark 2.1. The dimension of $\mathbb{R}[\underline{X}]_d$ is $\binom{n+d}{d}$. This can be understood as follows. There are n variables and every monomial can have degree at most d. The number of different possible monomials $X_1^{\alpha_1}\cdots X_n^{\alpha_n}$ with $\sum_i \alpha_i \leq d$ (the dimension) is the same as the number of ways to colour d out of $n+d$ white squares red, which is $\binom{n+d}{d}$. To see that every monomial corresponds uniquely to such a colouring we let the uncoloured squares represent $X_1, ..., X_n$ from left to right. Then the power of an X_i equals the number of successive red coloured squares at its right. For example for $n = 3$ and $d = 2$ (and w and r representing a white and red squares, respectively) we have that $wwrrw$ represents X_2^2 and $rwwwr$ represents X_3.

For a polynomial $p = \sum_\alpha p_\alpha \underline{X}^\alpha$, the vector $\mathbf{p} = (p_\alpha)$ denotes the vector of coefficients of p in the monomial basis. Let $\deg(p) = d$. We denote by $\mathbb{N}_d^n$ the set of sequences $\alpha \in \mathbb{N}^n$ with $|\alpha| \leq d$. We define $s(n,d) := |\mathbb{N}_d^n| = \binom{n+d}{d}$. Now p can be rewritten as follows:

$$p = \sum_{\alpha\in\mathbb{N}_d^n} p_\alpha \underline{X}^\alpha = \mathbf{p}^T[\underline{X}]_d. \tag{2.1}$$

We say a polynomial $p \in \mathbb{R}[\underline{X}]$ is positive semi-definite (abbreviated as *psd*) if $p(x) \geq 0$ for all $x \in \mathbb{R}^n$ and p is positive if $p(x) > 0$ for all $x \in \mathbb{R}^n$. As an exception, a form $\bar{p}$ is said to be positive if $\bar{p} > 0$ for all $x \in \mathbb{R}^n$ not equal to the zero vector. Further, let $P_{n,d}$ and denote the set of psd polynomials in n variables of degree smaller than or equal to d and let $\bar{P}_{n,d}$ denote the set of psd forms in n variables of degree d. Note that $P_{n,d}$ and $\bar{P}_{n,d}$ are closed under addition and multiplication with positive scalars, so $P_{n,d}$ and $\bar{P}_{n,d}$ are convex cones. Further, if n and d are not specified, we use P and $\bar{P}$ to denote the set of all psd polynomials and psd forms, respectively. We denote the set of all psd forms and psd polynomials on some set K by $P(K)$ and $\bar{P}(K)$, respectively.
A polynomial $p \in \mathbb{R}[\underline{X}]$ is a sum of squares (abbreviated as *sos*) if p can be written as a sum of squares of polynomials, i.e. $p = \sum_{i=1}^k p_i^2$ for some $p_i \in \mathbb{R}[\underline{X}]$ and $k \in \mathbb{N}$. Let $\bar{\Sigma}_{n,d}$ denote the subset of $\bar{P}_{n,d}$ of sos forms in n variables of degree d. Let $\Sigma_{n,d}$ denote the subset of $P_{n,d}$ of sos polynomials in n variables of degree smaller than or equal to d. Further, if n and d are not specified, we let $\bar{\Sigma}$ and Σ denote the set of all sos forms and sos polynomials, respectively. The property of being psd and sos, turns out to be preserved upon homogenization and dehomogenization. Before making that explicit we state the following lemma.

Lemma 2.2. Suppose $p = p_1^2 + ... + p_k^2$ for some non-zero $p_i \in \mathbb{R}[\underline{X}]$ for some integer $k \geq 1$. Then

$$\deg(p) = 2 \max_i \{\deg(p_i)\}. \tag{2.2}$$

Proof. We write $p_i = p_{i0} + ... + p_{id_i}$, where each p_{ij} is a nonzero form of degree j. We set $d = \max_i\{\deg(p_i)\}$. Since p_{id} is non-zero for at least one index i we obtain the result. □

Lemma 2.3. For a polynomial $p(X_1, ..., X_n)$ with even degree d and its homogenization $\bar{p}(X_0, X_1, ..., X_n) = X_0^d p(X_0, \frac{X_1}{X_0}, ..., \frac{X_n}{X_0})$, the following holds.

(i) p is an sos if and only if $\bar{p}$ is an sos.

(ii) $p \geq 0$ on $\mathbb{R}^n$ if and only if $\bar{p} \geq 0$ on $\mathbb{R}^n$.

Proof. (i) ($\Rightarrow$). If $p = \sum_{i=1}^k p_i^2$, then $\bar{p} = \sum_{i=1}^k \left(X_0^{\frac{d}{2}} p_i \left(\frac{X_1}{X_0}, ..., \frac{X_n}{X_0} \right) \right)^2$ for p_i with $\deg(p_i) \leq \frac{d}{2}$ by Lemma 2.2, which clearly again is an sos, but now an sos of forms of degree $\frac{d}{2}$.
($\Leftarrow$). If $\bar{p} = \sum_{i=1}^k \bar{p}_i^2$, then $p = \bar{p}(1, X_1, ..., X_n) = \sum_{i=1}^k \bar{p}_i(1, X_1, ..., X_n)^2$.

(ii) ($\Rightarrow$). If $x_0 \neq 0$, we use that $\bar{p}(x_0, ..., x_n) = x_0^d p(\frac{x_1}{x_0}, ..., \frac{x_n}{x_0})$. If $x_0 = 0$, we use that $\bar{p}(0, x_1, ..., x_n) = \lim_{\epsilon \to 0} \epsilon^d p\left(\frac{x_1}{\epsilon}, ..., \frac{x_n}{\epsilon}\right)$,
($\Leftarrow$). If $\bar{p} \geq 0$ then we use that $p(x_1, ..., x_n) = \bar{p}(1, x_1, ..., x_n)$.

□

In the sequel we sometimes homogenize or dehomogenize a polynomial when proving a psd or sos property.

Remark 2.4. The property of being positive is not preserved upon homogenization. For example $f(x_1, x_2) = x_1^2 + (1 - x_1x_2)^2 > 0$ for $x_1, x_2 \in \mathbb{R}$, but $\bar{f}(x_0, x_1, x_2) = x_1^2x_0^2 + (x_0^2 - x_1x_2)^2$ equals 0 at $(1, 0, 0)$ and $(0, 1, 0)$.

2.2 Hilbert's theorem

Clearly we have that the cone of homogeneous sums of squares polynomials is contained in the cone of homogeneous psd polynomials, i.e. $\bar{\Sigma} \subseteq \bar{P}$. So an obvious question regarding the sets $\bar{\Sigma}_{n,d}$ and $\bar{P}_{n,d}$ one might ask is whether $\bar{\Sigma}_{n,d} = \bar{P}_{n,d}$. In general it does not hold. However, for certain pairs (n, d) equality holds. Hilbert has characterized all these pairs already in 1888 in [8].

Theorem 2.5. $\bar{\Sigma}_{n,d} = \bar{P}_{n,d}$ if and only if $n \leq 2$, or $d = 2$, or $(n, d) = (3, 4)$.

Proof. Below we will prove the cases $n \leq 2$ and $d = 2$. The proof for the case $(n, d) = (3, 4)$ is harder. An elementary proof for this case is given by Scheiderer and Pfister in [32].
(Case: $n \leq 2$). Let $\bar{p} \in \bar{P}_{2,d}$. We show that $\bar{p}$ is a sum of squares. For this purpose we dehomogenize $\bar{p}$ to obtain a univariate polynomial $p \in \mathbb{R}[X]$. Since we know that the complex zeros come in conjugate pairs, we can factorize p as follows:

$$p = \underbrace{p_0 \prod_i (X - q_i)^{k_i}}_{\text{real factorization}} \underbrace{\prod_j [(X - a_j)^2 + b_j^2]^{l_j}}_{\text{complex factorization}} . \tag{2.3}$$

Here $p_0, q_i, a_j, b_j \in \mathbb{R}, k_i, l_j \in \mathbb{N}$. For the complex part of the factorization we have used that

$$(X - (a_j + b_j\mathbf{i}))(X - (a_j - b_j\mathbf{i})) = X^2 + a_j^2 - 2a_jX + b_j^2 = (X - a_j)^2 + b_j^2. \tag{2.4}$$

For the real part, we can deduce that k_i is even for all i, i.e. all real roots have even multiplicity. For if we suppose that a real root a has odd multiplicity, we see that p changes sign around a, which contradicts the positivity assumption. Returning to (2.3), we see that p is a product of a square, the real part, and a product of sums of two squares, the complex part. From the following equation we derive that a sum of two squares times a sum of two squares again is a sum of two squares:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2, \tag{2.5}$$

so the complex part as a whole can be written as one sum of two squares. Concluding, the factorization of p can be written as a square times a sum of two squares, so p can be written as a sum of two squares. By applying Lemma 2.3, we conclude $\bar{p}$ is an sos.
(Case: $(d = 2)$). Since $\bar{p}$ a form, $\bar{p}$ can be written as

$$\bar{p} = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} X_i X_j = \underline{X}^T A \underline{X}, \tag{2.6}$$

where $\underline{X}$ can be seen here as an $(n \times 1)-$column vector. Further we may assume that the matrix $A := (a_{ij})$ is symmetric, since if $a_{ij} \neq a_{ji}$, we can obtain $\bar{p}$ by redefining A as $A := (a'_{ij})$, where $a'_{ij} := \frac{a_{ij}+a_{ji}}{2}$. Since by assumption $\bar{p} \geq 0$, we know by definition (Theorem 1.1(1)) that A is PSD. Moreover by Theorem 1.1 we know A has a Choleski-decomposition and we can write $A = LL^T$, where L is an $(n \times k)-$matrix with real coefficients. Now we see that $\bar{p}$ is sos, because of the following manipulation:

$$\bar{p} = \underline{X}^T A \underline{X} = \underline{X}^T LL^T \underline{X} = (L^T \underline{X})^T (L^T \underline{X}) = ||L^T \underline{X}||^2. \tag{2.7}$$

□

For all the other cases (n, d) with $n \geq 3$ and $d \geq 6$ and for the cases (n, d) with $n \geq 4$ and $d \geq 4$, there are examples of forms that are nonnegative, but not an sos. In 1967, Motzkin [22] discovered the first explicit example of such a form for the case $(n, d) = (3, 6)$.

Example 2.6. [Motzkin's example].
The form $f(X, Y, Z) = Z^6 - 3X^2Y^2Z^2 + X^2Y^4 + X^4Y^2$ is an element of $\bar{P}_{3,6} \backslash \bar{\Sigma}_{3,6}$. In fact, Motzkin proved that the nonhomogeneous polynomial

$$f(X, Y, 1) = 1 - 3X^2Y^2 + X^2Y^4 + X^4Y^2 \in P_{2,6} \backslash \Sigma_{2,6}. \tag{2.8}$$

The proof is given below.

Proof. To prove the nonnegativity of $f(X, Y, 1)$, the geometric mean inequality for $n = 3$ (given in Corollary 2.15),

$$\frac{x_1 + x_2 + x_3}{3} \geq \sqrt[3]{x_1 x_2 x_3}, \qquad \text{for } x_1, x_2, x_3 \geq 0, \tag{2.9}$$

can be used. We substitute $x_1 = 1, x_2 = x^2y^4$ and $x_3 = x^4y^2$ and we immediately get the result.
To prove that $f(X, Y, 1)$ can not be written as an sos, assume for contradiction that $f(X, Y, 1)$ is an sos, i.e. $f(X, Y, 1) = \sum_i f_i^2$ for some polynomials $f_i \in \mathbb{R}[X, Y]$ with $\deg(f_i) \leq 3$. Since $f(X, Y, 1)$ contains no monomial of the form

$$X^6, Y^6, X^4, Y^4, X^2, Y^2 \tag{2.10}$$

we know that the f_i do not contain monomials of the form

$$X^3, Y^3, X^2, Y^2, X, Y. \tag{2.11}$$

Therefore all f_i should be of the form $a_i + b_iXY + c_iX^2Y + d_iXY^2$, for $a_i, b_i, c_i, d_i \in \mathbb{R}$. However, since we can only obtain the monomial $-3X^2Y^2$

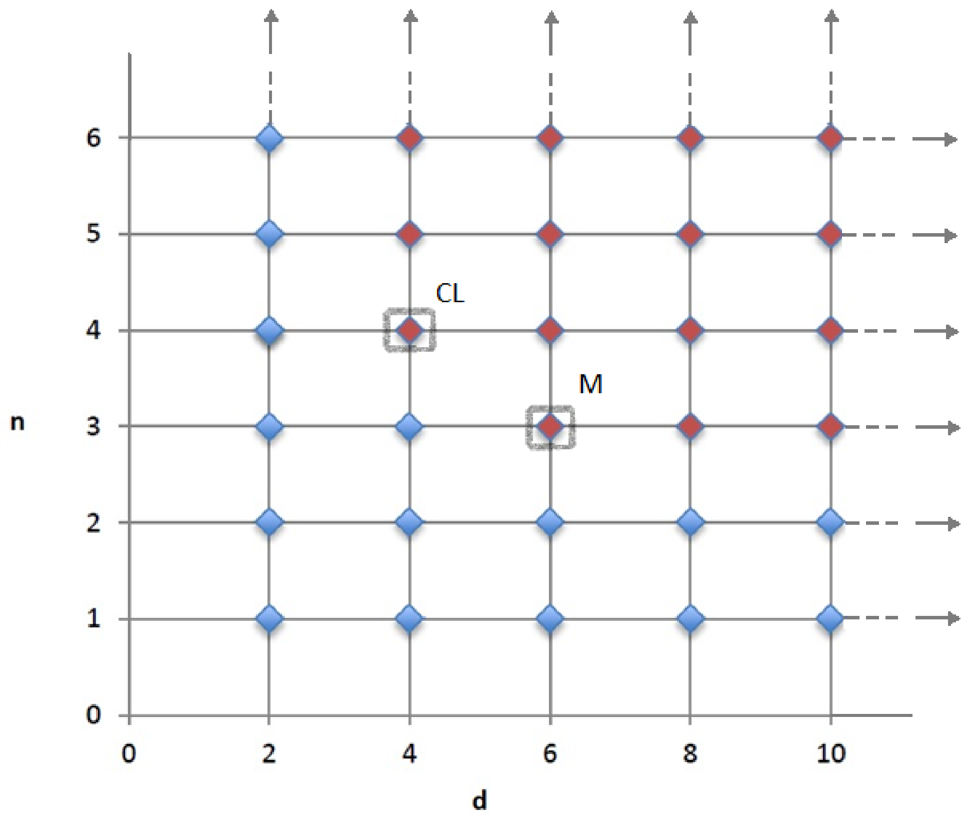

Figure 2.1: Here CL and M indicate the Choi-Lam and Motzkin examples, respectively. Further a blue coordinate means that $\bar{P}_{n,d} = \bar{\Sigma}_{n,d}$ and a red coordinate means that there exists a form $p \in \bar{P}_{n,d} \backslash \bar{\Sigma}_{n,d}$. All coordinates in the area $n \geq 4, d \geq 4$ and the area $n \geq 3, d \geq 6$ are red. Further, the coordinates on the line $d = 2$ remain blue as n grows, and the coordinates on the lines $n = 1, n = 2$ remain blue as d grows.

in $f(X, Y, 1)$ by squaring and then summing the $b_i XY$, we see that we must have $-3 = \sum_i b_i^2$, which gives a contradiction. Again using Lemma 2.3, we see that $f(X, Y, Z) \in \bar{P}_{3,6} \backslash \bar{\Sigma}_{3,6}$. $\square$

The following example for $(n, d) = (3, 4)$ was considered and proved by Choi-Lam [4] in 1977.

Example 2.7. [The Choi-Lam example].
The polynomial $g(W, X, Y, Z) = W^4 + X^2Y^2 + Y^2Z^2 + Z^2X^2 - 4WXYZ$ is an element of $\bar{P}_{4,4} \backslash \bar{\Sigma}_{4,4}$. In fact, the Choi-Lam example was originally nonhomogeneous and stated that

$$g(1, X, Y, Z) = 1 + X^2Y^2 + Y^2Z^2 + Z^2X^2 - 4XYZ \in P_{3,4} \backslash \Sigma_{n,d}. \quad (2.12)$$

The proof can be found in [4].

Now we show how the Choi-Lam and Motzkin examples are used to give a counterexample for $d \geq 6$ and $n \geq 3$, or $d \geq 4$ and $n \geq 4$, where d is even in both cases. For $d \geq 6$ and $n \geq 3$, note that for the non-homogeneous polynomial $f(X, Y, 1)$ from the Motzkin example we have that

$$Z^d f(\frac{X}{Z}, \frac{Y}{Z}, 1) \in \bar{P}_{n,d} \backslash \bar{\Sigma}_{n,d}$$

(just substitute $Z = 1$ and apply Lemma 2.3). For $d \geq 4$ and $n \geq 4$, note that for the non-homogeneous polynomial $g(1, X, Y, Z)$ from the Choi-Lam example we have that $W^d g(\frac{X}{W}, \frac{Y}{W}, \frac{Z}{W}) \in \bar{P}_{n,d} \backslash \bar{\Sigma}_{n,d}$ (again just substitute $W = 1$ and apply Lemma 2.3). Figure 2.2 summarizes the above results.

2.3 How big is the gap between P and Σ?

It turns out that Σ is dense in P with respect to the l_1-norm if we fix the number of variables, but there are few polynomials in Σ compared to P if we let the number of variables grow. These two assertions are made more precise by Theorem 2.8 and Theorem 2.9, respectively.

Theorem 2.8. [14] Let f be a polynomial in $\mathbb{R}[\underline{X}]$ which is nonnegative on $[-1, 1]^n$. For all $\epsilon > 0$ there exists an integer $t_0 \geq 0$ such that

$$f + \epsilon \left(1 + \sum_{i=1}^{n} X_i^{2t} \right) \in \Sigma,$$

for all $t \geq t_0$.

Proof. Although this is a result about sums of squares, the proof makes use of moment matrices, moments sequences and linear forms, which are all concepts introduced in chapter 3. Therefore this proof is given at the end of chapter 3. □

So for a fixed n, every polynomial nonnegative on $[-1,1]^n$ can be approximated by an sos by adding a small high degree perturbation. The following theorem shows that when n is unfixed, we get a different result.

Theorem 2.9. [2] There exist universal constants $c, C \in \mathbb{R}$ such that

$$cn^{(d-1)/2} \leq \left(\frac{\mathrm{vol}(\widehat{P}_{n,2d})}{vol(\widehat{\Sigma}_{n,2d})}\right)^{1/D} \leq Cn^{(d-1)/2} \tag{2.13}$$

Proof. See [2] for a proof. $\square$

Here $D = \binom{n+2d-1}{2d} - 1$ is the dimension of the space in which $\widehat{P}_{n,2d}$ lives. Further $\widehat{P}_{n,2d}$ is the cone $\bar{P}_{n,d}$ intersected with a hyperplane given by $\{p : \int_{\mathbf{S}^{n-1}} p(x)\sigma(dx) = 1\}$, where σ is the rotation invariant probability measure on S^{n-1} and $\widehat{\Sigma}_{n,2d}$ is the cone $\bar{\Sigma}_{n,d}$ intersected by the same hyperplane. In fact, we are dealing with the cones $\Sigma_{n,2d}$ and $P_{n,2d}$ and check the quantitative ratio between them, measured on a hyperplane intersecting the cones.

2.4 Checking whether a polynomial is an sos by using semi-definite programming

Although Σ is not dense in P for an unfixed number of variables, we are still interested in finding out whether a given polynomial is an sos.

The claim is that checking whether a polynomial is an sos, can be reformulated as an sdp. The following manipulation with $p_i \in \mathbb{R}[\underline{X}]_d$ is helpful in understanding this:

$$\sum_{i=1}^{n} p_i^2 = [\underline{X}]_d^T (\sum_{i=1}^{n} \mathbf{p}_i \mathbf{p}_i^T)[\underline{X}]_d = [\underline{X}]_d^T Q [\underline{X}]_d, \tag{2.14}$$

where $Q := \sum_{i=1}^{n} \mathbf{p}_i \mathbf{p}_i^T$. Therefore Q is PSD (see Theorem 1.1), so there is a one-to-one correspondence between PSD matrices and sos's. Powers and Wörmann [36] worked out this idea of checking whether a polynomial is an sos by using semi-definite programming. The following lemma is a result of this.

Lemma 2.10. Let $p \in \mathbb{R}[\underline{X}]_{2d}$. Then p is sos if and only if the set

$$\{Q \in S^{s(n,d)} \mid Q \succeq 0, \sum_{\substack{\beta,\gamma \in \mathbb{N}^n_d \\ \beta+\gamma=\alpha}} Q_{\beta,\gamma} = p_\alpha, \quad \forall \alpha \in \mathbb{N}^n_{2d}\} \tag{2.15}$$

is non-empty.

Unfortunately, the size of matrix Q grows rapidly as the number of variables and the degree grow. As explained in Remark 2.1, the number of rows of Q equals $\binom{n+d}{d}$. However, for specific examples one can often decrease the size of Q, by eliminating unnecessary elements of $[\underline{X}]_d$. Consider the following examples from [36].

Example 2.11. Let $f = X^4 + 2X^2Y^2 + 4X^3Z + Z^4$. In this example we want to check whether f is an sos. For this purpose we try to find a PSD matrix Q such that $f = [\underline{X}]_2^T Q [\underline{X}]_2$, where

$$[\underline{X}]_2 = (1, X, Y, Z, XY, XZ, YZ, X^2, Y^2, Z^2)^T.$$

Firstly note that f is a form of degree 4. This means that f is an sos if and only if f is an sos of forms of degree 2. We therefore can immediately remove the monomials $1, X, Y, Z$ from $[\underline{X}]_2$. Further since Y^4 is not a monomial in f, Y^2 can be removed as well. Similarly we can remove YZ. Notice that X^2Z^2 can be written as a product of XZ and XZ, but also as a product of X^2 and Z^2. So the only elements of $[\underline{X}]_2$ that correspond to a nonzero row and column are XY, XZ, X^2, Z^2. So have obtained the following:

$$f = \begin{pmatrix} X^2 \\ XY \\ XZ \\ Z^2 \end{pmatrix}^T \begin{pmatrix} 1 & 0 & 2 & \lambda \\ 0 & 2 & 0 & 0 \\ 2 & 0 & -2\lambda & 0 \\ \lambda & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} X^2 \\ XY \\ XZ \\ Z^2 \end{pmatrix} \tag{2.16}$$

for some $\lambda \in \mathbb{R}$. Now we want to find λ. From (5) of definition 1.1, we know that all principal minors of Q have to be nonnegative. So taking the determinant of the submatrix indexed by $\{X^2, Z^2\}$, we get that $|\lambda| \leq 1$ and taking the determinant of the submatrix indexed by $\{X^2, XZ\}$ we get that $\lambda \leq -2$, so we have a contradiction. So f is not an sos by Lemma 2.10.

Example 2.12. Consider the polynomial $h = X^2Y^2 + X^2 + Y^2 + 1$. Clearly h is an sos. We now will try to find all possible sos decompositions of h.

Note that as deduced in the latter example, we can assume that the only monomials that might occur in $[\underline{X}]_2$ are $XY, X, Y, 1$. So we can decompose h as follows.

$$h = \begin{pmatrix} XY \\ X \\ Y \\ 1 \end{pmatrix}^T \begin{pmatrix} 1 & 0 & 0 & \lambda \\ 0 & 1 & -\lambda & 0 \\ 0 & -\lambda & 1 & 0 \\ \lambda & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} XY \\ X \\ Y \\ 1 \end{pmatrix} \tag{2.17}$$

for some $\lambda \in \mathbb{R}$. We call the above matrix Q. Note that the coefficients of Q indexed by $(1, XY), (XY, 1), (X, Y)$ and (Y, X) are variables but sum up to zero, since XY is not a monomial appearing in h.
Further it is easy to verify that the eigenvalues of Q are 1 and $1 - \lambda^2$, both with multiplicity two. Therefore Q is psd if and only if $|\lambda| \leq 1$. To obtain the possible sos decompositions of Q, we diagonalize Q and write $Q = VDV^T$, where $D = \text{diag}(1, 1, 1 - \lambda^2, 1 - \lambda^2)$ and

$$V = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -\lambda & 1 & 0 \\ \lambda & 0 & 0 & 1 \end{pmatrix} \tag{2.18}$$

So we obtain that $h = (XY + \lambda)^2 + (X - \lambda Y)^2 + (\sqrt{1 - \lambda^2}y)^2 + (\sqrt{1 - \lambda^2})^2$. As explained, for all λ satisfying $|\lambda| \leq 1$, this is an sos.

In the next chapters, we will return to this idea of using semi-definite programming to find an sos decomposition of a polynomial. Using semi-definite programming in practice, means setting bounds on the degree of the monomials in the sums of squares. In Chapters 5 and 6 we work out this principle.

2.5 Sufficient conditions for being a sum of squares

Instead of solving an sdp to check whether a polynomial has an sos decomposition, a method has been developed that uses the coefficients of a polynomial to check a condition that, when satisfied, implies that the polynomial is an sos. This condition is a sufficient condition, not a necessary.

The following notation is used. For a polynomial $f(\underline{X}) = \sum_{\alpha \in \mathbb{N}^n} f_\alpha \underline{X}^\alpha$ of degree $2d$ we define

$$\Omega(f) := \{\alpha \in \mathbb{N}^n : f_\alpha \neq 0\} \backslash \{\underline{0}, 2de_1, ..., 2de_n\}, \tag{2.19}$$

where $e_i = (\delta_{i1}, ..., \delta_{in})$, where δ is the Kronecker symbol. Further we define

$$\Delta(f) := \{\alpha \in \Omega(f) : f_\alpha \underline{X}^\alpha \text{ is not a square in } \mathbb{R}[\underline{X}]\}. \tag{2.20}$$

The following theorem shows that if the coefficients of a polynomial satisfy certain conditions, then it is an sos. For the coefficient $f_{2d\epsilon_i}$ of X_i^{2d} we also write $f_{2d,i}$ for short.

Theorem 2.13. [21] Let f be a form of degree $2d$. Then f is an sos if there exist nonnegative numbers $a_{\alpha,i} \in \mathbb{R}$, for $\alpha \in \Delta(f)$ and $i \in \{1, ..., n\}$, such that the following two assertions hold:

(i) $\forall \alpha \in \Delta(f) : \quad (2d)^{2d} a_\alpha^\alpha = f_\alpha^{2d} \alpha^\alpha$

(ii) $f_{2d,i} \geq \sum_{\alpha \in \Delta(f)} a_{\alpha,i}$, for $i \in \{1, ..., n\}$

Here $a_\alpha := (a_{\alpha,1}, ..., a_{\alpha,n}), a_\alpha^\alpha := a_{\alpha,1}^{\alpha_1} \cdots a_{\alpha,n}^{\alpha_n}$ and $\alpha^\alpha := \alpha_1^{\alpha_1} \cdots \alpha_n^{\alpha_n}$.

The proof of this theorem uses the following result of Hurwitz ([9]) and Reznick ([29] and [30]).

Theorem 2.14 (Hurwitz and Reznick)**.** Let

$$p(\underline{X}) = \sum_{i=1}^n \alpha_i X_i^{2d} - 2d X_1^{\alpha_1} \cdots X_n^{\alpha_n},$$

where $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n$, $|\alpha| = 2d$. Then p is an sos.

Proof. The proof will be done by induction on n. Recall that n is the number of variables. For $n = 1$ we see that, since $\alpha_1 = 2d$, $p = 0$, which of course is an sos. First we exclude $n = 2$ and assume $n \geq 3$. So we assume the theorem holds for $n - 1$. We assume that all α_i are non-zero since otherwise the number of variables immediately reduces to $n - 1$. Further, we may assume that $\alpha_j, \alpha_k \leq d$, for two coefficients of α indexed by j and k. We now write $\alpha = (\alpha_1, ..., \alpha_n)$ as a sum of two elements $\beta, \gamma \in \mathbb{N}^n$, such that $\alpha = \gamma + \beta$, where $\beta_j = 0$ and $\gamma_k = 0$ (so $\gamma_j = \alpha_j$ and $\beta_k = \alpha_k$) and $|\beta| = |\gamma| = d$. The following identity is a logical result of this decomposition of α.

$$(\underline{X}^\beta - \underline{X}^\gamma)^2 = \underline{X}^{2\beta} - 2\underline{X}^\beta\underline{X}^\gamma + \underline{X}^{2\gamma} = \underline{X}^{2\beta} - 2\underline{X}^\alpha + \underline{X}^{2\gamma}. \tag{2.21}$$

With this identity we can deduce the following:

$$\begin{aligned}
p(\underline{X}) &= \sum_{i=1}^n \alpha_i X_i^{2d} - 2d\underline{X}^\alpha \\
&= \sum_{i=1}^n \alpha_i X_i^{2d} + 2d\frac{(\underline{X}^\beta - \underline{X}^\gamma)^2 - \underline{X}^{2\beta} - \underline{X}^{2\gamma}}{2} \\
&= \sum_{i=1}^n \alpha_i X^{2d} - d(\underline{X}^{2\beta} + \underline{X}^{2\gamma} - (\underline{X}^\beta - \underline{X}^\gamma)^2) \\
&= \sum_{i=1}^n \beta_i X_i^{2d} - d\underline{X}^{2\beta} + \sum_{i=1}^n \gamma_i X_i^{2d} - d\underline{X}^{2\gamma}) + d(\underline{X}^\beta - \underline{X}^\gamma)^2
\end{aligned}$$

Since both γ and β are $(n-1)$-dimensional, we can use the induction hypothesis to conclude that each of the last terms are sums of squares.
The theorem remains to be proven for the case $n = 2$. Therefore we need to show that $p(X_1, X_2) = \alpha_1 X_1^{2d} + \alpha_2 X_2^{2d} - 2dX_1^{\alpha_1}X_2^{\alpha_2}$ is an sos for $\alpha_1 + \alpha_2 = 2d$. To show this, we consider $p(1, X_2) = \alpha_1 + \alpha_2 X_2^{2d} - 2dX_2^{\alpha_2}$. We want to show that $p(1, X_2) \geq 0$. For this purpose we calculate its derivative and set it equal to 0.

$$p'(1, X_1) = 2d\alpha_2 X_2^{2d-1} - 2d\alpha_2 X_2^{\alpha_2 - 1} = 0 \tag{2.22}$$

So we have critical points at $X_2 = 0, X_2 = 1$ and, if α_2 is even, $X_2 = -1$. We see that we have a minimum at $X_2 = 1$ and $X_2 = -1$ (if α_2 is even), since $p(1, X_2) \geq 0$ for $|X| \geq 1$. Further we have a maximum at $X_2 = 0$. So we can conclude that $p(1, X_2) \geq 0$. Now after applying Lemma 2.3 and Theorem 2.5, we can conclude that $p(X_1, X_2)$ can be written as an sos. □

Corollary 2.15. The following inequality, called the arithmetic-geometric inequality, is a direct corollary of Theorem 2.14:

$$\sqrt[n]{x_1 \cdots x_n} \leq \frac{x_1 + \ldots + x_n}{n} \tag{2.23}$$

for $x_1, \ldots, x_n \in \mathbb{R}_{\geq 0}$ and any integer $n \geq 1$.

Proof. If we set $\alpha = (1, ..., 1)$ and we substitute $X_i = \sqrt[n]{x_i}$, then $p(\underline{X})$ from Theorem 2.14 becomes $\sum_{i=1}^n x_i - n\sqrt[n]{x_1} \cdots \sqrt[n]{x_n}$ for $x_i \in \mathbb{R}_{\geq 0}$ and since $p(\underline{X}) \geq 0$, we obtain (2.23) for even n. To see that it holds for all positive integers note that for n odd we can make the following manipulations:

$$\sqrt[n]{x_1 \cdots x_n} = \sqrt[2n]{x_1^2 \cdots x_n^2} \leq \frac{2x_1 + \ldots + 2x_n}{2n} = \frac{x_1 + \ldots + x_n}{n}.$$

□

Here follows a corollary by Fidalgo and Kovacec [5] of Theorem 2.14, which will an important step in the proof of Theorem 2.13.

Corollary 2.16. For a form $p(\underline{X}) = \sum_{i=1}^n \beta_i X_i^{2d} - \mu \underline{X}^\alpha$, such that $\alpha \in \mathbb{N}^n$, $|\alpha| = 2d$, $\beta_i \geq 0$ for $i = 1, ..., n$ and $\mu \geq 0$ if all α_i even, the following three assertions are equivalent:

(i) p is psd

(ii) $\mu^{2d} \prod_{i=1}^n \alpha_i^{\alpha_i} \leq (2d)^{2d} \prod_{i=1}^n \beta_i^{\alpha_i}$

(iii) p is sos.

Proof. Suppose that an α_i is odd and $\mu < 0$, we can then make a change of variables $Y_i = X_i$ and $Y_j = X_j$ for all $j \neq i$. Then μ will be replaced by $-\mu$. Therefore we can assume that $\mu \geq 0$. Now suppose $\mu = 0$. Clearly $(i), (ii), (iii)$ are true. So we only need to consider $\mu > 0$. Further, suppose $\beta_i = 0$. Then since we assume that $\mu > 0$, (ii) is not satisfied and (i) will not be satisfied if we set $X_j = 1$ for all $j \neq i$ and we let $X_i \to \infty$. Further, suppose that $\alpha_i = 0$ for some i, and $\alpha_j \neq 0$ for $j \neq i$. If we set $X_i = 0$, we obtain a polynomial p' in $n-1$ variables of the form $p(\underline{X})$ with all coefficients of α positive. Since we will proof this below we assume the equivalence of the assertions $(i), (ii)$ and (iii) hold for p'. Now we obtain $p(\underline{X})$ (with $\alpha_i = 0$) from p' by adding $\beta_i X_i^{2d}$. Clearly for this $p(\underline{X})$ (with $\alpha_i = 0$), the assertions $(i), (ii)$ and (iii) still are equivalent. Now in the rest of the proof, we assume that $\alpha_i > 0$, $\mu \geq 0$ and $\beta_i > 0$ for all $i \in \{1, ..., n\}$.
$(iii) \Rightarrow (i)$ is trivial. For $(i) \Rightarrow (ii)$, we assume that p is *psd*. We set x as follows:

$$x := \left(\left(\frac{\alpha_1}{\beta_1}\right)^{1/2d}, ..., \left(\frac{\alpha_n}{\beta_n}\right)^{1/2d}\right). \tag{2.24}$$

Now, after substitution, we get:

$$p\left(\left(\frac{\alpha_1}{\beta_1}\right)^{1/2d},...,\left(\frac{\alpha_n}{\beta_n}\right)^{1/2d}\right) = \sum_{i=1}^{n}\alpha_i - \mu\prod_{i=1}^{n}\left(\frac{\alpha_i}{\beta_i}\right)^{\alpha_i/2d}$$
$$= 2d - \mu\prod_{i=1}^{n}\left(\frac{\alpha_i}{\beta_i}\right)^{\alpha_i/2d} \geq 0,$$

where the last inequality proves (ii).
Now we assume (ii). To prove (iii), we will apply a variable change to get $p(\underline{X})$ in a form on which we can apply Theorem 2.14. So we define $X_i = (\frac{\alpha_i}{\beta_i})^{1/2d}Y_i$ for $i = 1,...,n$. Further let $\mu_1 := \mu\prod_{i=1}^{n}(\frac{\alpha_i}{\beta_i})^{\alpha_i/2d}$. Now, after raising both sides to the power $2d$ and multiplying by $\prod_{i=1}^{n}\frac{1}{\beta_i}$ we apply our assumption (ii) on μ_1 and see that $\mu_1 \leq 2d$, i.e. $1 \leq \frac{2d}{\mu_1}$. Now substituting our new variables and using that $1 \leq \frac{2d}{\mu_1}$, we can write the following:

$$\begin{aligned} p(\underline{X}) &= \sum_{i=1}^{n}\alpha_i Y_i^{2d} - \mu_1\underline{Y}\alpha \\ &= \frac{\mu_1}{2d}[\sum_{i=1}^{n}\alpha_i Y_i^{2d}(\frac{2d}{\mu_1}-1) + \sum_{i=1}^{n}\alpha_i Y_i^{2d} - 2d\underline{Y}^{\alpha}] \\ &= \sum_{i=1}^{n}(\alpha_i(1-\frac{\mu_1}{2d}) + \alpha_i\frac{\mu_1}{2d})Y_i^{2d} - 2d\underline{Y}^{\alpha} \end{aligned}$$

Since $(\alpha_i(1-\frac{\mu_1}{2d}) + \alpha_i\frac{\mu_1}{2d}) = \alpha_i$ we can apply Hurwitz-Reznick and conclude that (iii) is implied by (ii). $\square$

Now we give the proof of Theorem 2.13 as an application of this last corollary.

Proof. Here we proof Theorem 2.13. Assume that that the $a_{\alpha,i} \in \mathbb{R}$ exist satisfying the conditions (i) and (ii) of Theorem 2.13. We now combine the implication $(ii) \Rightarrow (iii)$ of Corollary 2.16 and assertion (i) of Theorem 2.13 to obtain that $\sum_{i=1}^{n}a_{\alpha,i}X_i^{2d} + f_\alpha\underline{X}^{\alpha}$ is an sos for each $\alpha \in \Delta$. Taking the sum over all α in Δ, we see that

$$\sum_{i=1}^{n}\left(\sum_{\alpha\in\Delta}a_{\alpha,i}\right)X_i^{2d} + \sum_{\alpha\in\Delta}f_\alpha\underline{X}^{\alpha} \tag{2.25}$$

is an sos. Now we use assertion (ii) of Theorem 2.13 to see that

$$\sum_{i=1}^{n} f_{2d,i} X_i^{2d} + \sum_{\alpha\in\Delta} f_\alpha \underline{X}^\alpha.$$

Here we use that a nonnegative constant times X^{2d} added to an sos again gives an sos. Now by the definition of Δ we know that for each $\alpha \in \Omega\backslash\Delta$ we have that $f_\alpha \underline{X}^\alpha$ is a square. Therefore $f(\underline{X})$ is an sos. $\square$

A corollary of Theorem 2.13 is the following.

Corollary 2.17. [13] A polynomial $f \in \mathbb{R}[\underline{X}]$ of degree $2d$ is an sos if the following two conditions hold.

(1) $f_0 \geq \sum_{\alpha\in\Delta(f)} |f_\alpha| \frac{2d-|\alpha|}{2d}$

(2) $f_{2d,i} \geq \sum_{\alpha\in\Delta(f)} |f_\alpha| \frac{\alpha_i}{2d}$ for all $i \in \{1, ..., n\}$.

Proof. Let $f \in \mathbb{R}[\underline{X}]$ satisfy the conditions (1) and (2) of Corollary 2.17. The idea of the proof is to apply Theorem 2.13 to its homogenization $\bar{f}(\underline{X}, X_0)$. For this purpose we choose $a_{\alpha,i}$ in such a way that the conditions (i) and (ii) of Theorem 2.13 are satisfied.

So we apply Theorem 2.13 to the polynomial $\bar{f}(\underline{X}, X_0)$. For this purpose we set $a_{\alpha,i} = |f_\alpha| \frac{\alpha_i}{2d}$ for $i = 1, ..., n$ and we set $a_{\alpha,0} = |f_\alpha| \frac{2d-|\alpha|}{2d}$ for $i = 0$. Now we can show condition (ii) of Theorem 2.13. For this purpose we need to show that $\bar{f}_{2d,i} \geq \sum_{\alpha\in\Delta} |f_\alpha| \frac{\alpha_i}{2d}$ for $i \in \{1, ..., n\}$ and $\bar{f}_{2d,0} = f_0 \geq \sum_{\alpha\in\Delta} |f_\alpha| \frac{2d-|\alpha|}{2d}$ for $i = 0$. These conditions are exactly the conditions of Corollary 2.17. So only (i) of Theorem 2.13 needs to be shown. For this purpose we use that $a_\alpha^\alpha := a_{\alpha,0}^{2d-|\alpha|} a_{\alpha,1}^{\alpha_1} \dots a_{\alpha,n}^{\alpha_n}$, where $i = 0, 1, ..., n$. For the first power of a in the latter identity, we used that $\alpha_0 = 2d - |\alpha|$. Now note the following manipulation.

$$\begin{aligned}
(2d)^{2d} a_\alpha^\alpha &= (2d)^{2d} \left(\frac{|f_\alpha|(2d - |\alpha|)}{2d} \right)^{2d-|\alpha|} \prod_{i=1}^{n} \left(\frac{|f_\alpha|\alpha_i}{2d} \right)^{\alpha_i} \\
&= (2d)^{2d} |f_\alpha|^{2d-|\alpha|} (2d - |\alpha|)^{2d-|\alpha|} |f_\alpha|^{|\alpha|} \alpha^\alpha (2d)^{-2d} \\
&= |f_\alpha|^{2d} \alpha^\alpha (2d - |\alpha|)^{2d-|\alpha|}.
\end{aligned}$$

So (i) holds for each pair $(2d - |\alpha|, \alpha) \in \Delta(\bar{f})$, where $\alpha \in \Delta(f)$. So (i) and (ii) hold. Now we again apply Lemma 2.3 and we are done. $\square$

Example 2.18. Let $f(x) = \prod_{i=1}^{n} x_i + 1 + \sum_{i=1}^{n} (x_i^2 - x_i) x_i^{n-2}$ with even degree $n = 2d$. The monomials corresponding to the indices of $\Delta(f)$ that are not a square or have a negative coefficient are $\prod_{i=1}^{n} x_i, -x_1^{n-1}, ..., -x_n^{n-1}$. So the first condition of Corollary 2.17 is verified since

$$f_0 = 1 = 0 + \underbrace{\frac{1}{2d} + ... + \frac{1}{2d}}_{\text{n times}}. \tag{2.26}$$

The second condition clearly also is satisfied, since

$$f_{2d,i} = 1 = \frac{1}{2d} + \frac{n-1}{2d} \tag{2.27}$$

for all $i \in \{1, ..., n\}$. So by Corollary 2.17, f is an sos.

Chapter 3

Moment matrices and moment sequences

In this chapter we introduce moment sequences and moment matrices. Moreover we discuss the duality relation between sums of squares and moment matrices and illustrate it with an example. Further we give a characterization of bounded moment sequences that have a representing measure on the hypercube. We finish this chapter with the proof of Theorem 2.8 (on the approximation of nonnegative polynomials by sums of squares) from chapter 2, that combines most of the theory from this chapter.

3.1 Basic facts and definitions

In this thesis we consider Borel measures on $\mathbb{R}^n$. Borel measures are implicitly assumed to be positive. The support of a measure μ, denoted by $\text{supp}(\mu)$, is the smallest closed set $S \subseteq \mathbb{R}^n$ for which $\mu(\mathbb{R}^n \backslash S) = 0$. We also might say that μ is a measure supported by $K \subseteq \mathbb{R}^n$ if $\text{supp}(\mu) \subseteq K$.
Let μ be a measure on $\mathbb{R}^n$. For $\alpha \in \mathbb{N}^n$, the quantity $y_\alpha := \int x^\alpha \mu(dx)$ is called the moment of order α of the measure μ. By $(y_\alpha)_{\alpha \in \mathbb{N}^n}$ we denote the sequence of moments of measure μ. Moreover the truncated sequence $(y_\alpha)_{\alpha \in \mathbb{N}^n_t}$ is the sequence of moments up to order t. We say μ is a representing measure for y if y is the sequence of moments of the measure μ. Here follows the definition of a moment matrix:

Definition 3.1. Given a sequence $(y_\alpha)_{\alpha \in \mathbb{N}^n} \in \mathbb{R}^{\mathbb{N}^n}$, its moment matrix is the (infinite) matrix $M(y)$ given by

$$M(y) := (y_{\alpha+\beta})_{\alpha,\beta} \text{ for } \alpha, \beta \in \mathbb{N}^n. \tag{3.1}$$

For a truncated sequence $(y_\alpha)_{\alpha \in \mathbb{N}^n_t} \in \mathbb{R}^{\mathbb{N}^n_t}$ we consider the same definition for its moment matrix $M_t(y)$, but now only indexed by $\mathbb{N}^n_t$. Further we define the following sequence for $g \in \mathbb{R}[\underline{X}]$ and $y \in \mathbb{R}^{\mathbb{N}^n}$

$$gy := M(y)g \in \mathbb{R}^{\mathbb{N}^n}, \tag{3.2}$$

which is called *shifted vector*, with entry $(gy)_\alpha := \sum_\beta g_\beta y_{\alpha+\beta}$ for $\alpha \in \mathbb{N}^n$. In the following lemma we see that the moment matrix of a sequence that has a representing measure is PSD.

Lemma 3.2. If $y \in \mathbb{R}^{\mathbb{N}^n_{2t}}$ is the sequence of moments of a measure μ, then $M_t(y) \succeq 0$.

Proof. For a polynomial $p \in \mathbb{R}[\underline{X}]_t$ the following holds:

$$\begin{aligned} \mathbf{p}^T M_t(y)\mathbf{p} &= \sum_{\alpha,\beta \in \mathbb{N}^n_t} p_\alpha p_\beta y_{\alpha+\beta} \\ &= \sum_{\alpha,\beta \in \mathbb{N}^n_t} p_\alpha p_\beta \int x^{\alpha+\beta} \mu(dx) \\ &= \int p(x)^2 \mu(dx) \geq 0. \end{aligned}$$

The above three equalities are due to the definition of moment matrices, the definition of moment sequences and the definition of a polynomial, respectively. □

To a sequence $y = (y_\alpha)_{\alpha \in \mathbb{N}^n}$ corresponds a linear form L on the polynomial ring $\mathbb{R}[\underline{X}]$. This linear form is defined as $L : \mathbb{R}[\underline{X}] \to \mathbb{R}$ such that $\underline{X}^\alpha \mapsto y_\alpha$ and $L(1) = 1$. So we see that $L(\sum_\alpha f_\alpha X^\alpha) = \sum_\alpha f_\alpha y_\alpha$.

Lemma 3.3. Let $y = (y_\alpha)_{\alpha \in \mathbb{N}^n}$ and L be its associated linear form. Then for $f \in \mathbb{R}[\underline{X}]$ we have

$$L(f^2) = \mathbf{f}^T M(y)\mathbf{f}. \tag{3.3}$$

So $L \geq 0$ on Σ if and only if $M(y) \succeq 0$.

Proof.

$$L(f^2) = L\left(\sum_{\alpha,\beta} f_\alpha f_\beta x^{\alpha+\beta}\right) = \sum_{\alpha,\beta} f_\alpha f_\beta y_{\alpha+\beta} = \mathbf{f}^T M(y)\mathbf{f}. \tag{3.4}$$

□

3.2 Duality relations

In this section we treat duality between the set of sequences whose moment matrices are PSD and sums of squares. Moreover we explain that the set of nonnegative polymials has the of moment sequences as dual set.

We introduce the following definitions: For an $\mathbb{R}$-vector space A, its dual vector space A^* consists of all linear maps $L : A \to \mathbb{R}$. Further, for a cone $B \subseteq A$, its dual cone is defined as

$$B^* := \{L \in A^* : L(b) \geq 0 \text{ for all } b \in B\}. \tag{3.5}$$

Note that when we consider the semi-definite cone, its dual described in (1.2) can be obtained from equation (3.5). From the definition in (3.5) we can obtain the duals of the cones P and Σ by setting $A = \mathbb{R}[\underline{X}]$. We obtain the following:

$$P^* = \{L \in (\mathbb{R}[\underline{X}])^* : L(p) \geq 0 \text{ for all } p \in P\} \tag{3.6}$$

and

$$\Sigma^* = \{L \in (\mathbb{R}[\underline{X}])^* : L(p^2) \geq 0 \text{ for all } p \in \mathbb{R}[\underline{X}]\}. \tag{3.7}$$

Now let us consider the definitions of the cone of moment sequences and the cone of sequences whose moment matrix is PSD, respectively:

$$M := \{y \in \mathbb{R}^{\mathbb{N}^n} : y \text{ has a representing measure}\} \tag{3.8}$$

and

$$M_{\succeq 0} := \{y \in \mathbb{R}^{\mathbb{N}^n} : M(y) \succeq 0\}. \tag{3.9}$$

Recall that every linear form corresponds to a sequence $(y_\alpha)_{\alpha\in\mathbb{N}^n}$. So we see as a direct consequence of Lemma 3.3 that $\Sigma^* = M$.
The following theorem shows the equivalence between a sequence having a representing measure on a set K and the corresponding linear form being positive for all polynomials nonnegative on K.

Theorem 3.4. [7][Haviland's theorem] Let K be a closed subset in $\mathbb{R}^n$. The following two assertions are equivalent for a linear form $L \in \mathbb{R}[X]^*$:

(i) $L(p) \geq 0$ for any polynomial $p \in \mathbb{R}[\underline{X}]$ such that $p \geq 0$ on K.

(ii) There exists a measure μ on K such that $L(p) = \int_K p(x)\mu(dx)$ for all $p \in \mathbb{R}$.

Proof. For a proof see section 4.6 of [16]. $\square$

Clearly, from Theorem 3.4 we can deduce that $P^* = M$. In Proposition 4.9 of [16], the full proof that P and M are duals and that Σ and $M_{\succeq 0}$ are duals is given. Recall that $\Sigma \subseteq P$ and note that by Lemma 3.2, we have that $M \subseteq M_{\succeq 0}$. Now we are able to give an overview of the above duality and inclusion relations:

$$\begin{tikzcd}
P \arrow[r, dash, "\supseteq"] \arrow[d, dash, "duals"'] & \Sigma \arrow[d, dash, "duals"] \\
M \arrow[r, dash, "\subseteq"] & M_{\succeq 0}
\end{tikzcd}$$

3.2.1 Duality example

In this subsection we give an example of a duality pair, in which the cones Σ and $M_{\succeq 0}$ are involved. Let $\deg(f) = 2t$. We will consider the following sdp's and show that they are duals:

$$\sup\{\lambda \in \mathbb{R} : f - \lambda \in \Sigma\} \tag{3.10}$$

and

$$\inf\{\sum f_\alpha y_\alpha : y_0 = 1, M_t(y) \succeq 0\}. \tag{3.11}$$

The main step in showing the duality is to rewrite the program in (3.10) in standard form as described in (1.4). We do this as follows. By Lemma 2.10 we know $f - \lambda \in \Sigma$ if and only is there exists a PSD matrix $X \in S^{s(n,t)}$ such that

$$\sum_{\substack{\beta,\gamma \in \mathbb{N}^n_t \\ \beta+\gamma=\alpha}} X_{\beta,\gamma} = (f - \lambda)_\alpha, \quad \forall \alpha \in \mathbb{N}^n_{2t}. \tag{3.12}$$

Here $(f-\lambda)_\alpha$ indicates the coefficient of the monomial X^α of the polynomial $f-\lambda$. So we can already rewrite (3.10) as

$$\sup\{\lambda \in \mathbb{R} : X \succeq 0, \sum_{\substack{\beta,\gamma \in \mathbb{N}_t^n \\ \beta+\gamma=\alpha}} X_{\beta,\gamma} = (f-\lambda)_\alpha \text{ for all } \alpha \in \mathbb{N}_{2t}^n\}. \tag{3.13}$$

However, we want to rewrite these equations described in (3.12) by using matrix inner products (as in the standard form is done). For this purpose we define the matrix A_α as follows:

$$(A_\alpha)_{\beta,\gamma} = \left\{ \begin{array}{ll} 1 & \text{if} \quad \beta+\gamma=\alpha \\ 0 & \text{else} \end{array} \right\}, \text{ for all } \alpha \in \mathbb{N}_{2t}^n \text{ and } \beta,\gamma \in \mathbb{N}_t^n. \tag{3.14}$$

So we can rewrite the equations in (3.12) as:

$$\langle A_\alpha, X\rangle = f_0 - \lambda \text{ if } \alpha = 0 \text{ and } \langle A_\alpha, X\rangle = f_\alpha \text{ else.} \tag{3.15}$$

In order to write λ as an inner product of matrices, we let C be the matrix in $S^{s(n,t)+1}$ given by

$$C_{\alpha,\beta} = \begin{cases} 0 & \text{if} \quad (\alpha,\beta) \neq (s(n,t)+1, s(n,t)+1), \\ 1 & \text{if} \quad (\alpha,\beta) = (s(n,t)+1, s(n,t)+1) \end{cases} \tag{3.16}$$

Moreover, let $\widetilde{X} \in S^{s(n,t)+1}$. Now by setting

$$\widetilde{X}_{s(n,t)+1,s(n,t)+1} = \lambda$$

we obtain that $\langle C, \widetilde{X}\rangle = \lambda$. Finally, in order to formulate (3.10) in standard form we define the following matrix of order $s(n,t)+1$:

$$\widetilde{A}_\alpha = \left(\begin{array}{c|c} A_\alpha & 0 \\ \hline 0 & 1 \end{array}\right) \quad \text{if} \quad \alpha = 0 \tag{3.17}$$

and

$$\widetilde{A}_\alpha = \left(\begin{array}{c|c} A_\alpha & 0 \\ \hline 0 & 0 \end{array}\right) \quad \text{else.} \tag{3.18}$$

Now, the standard form of our program described in (3.10) is given as follows:

$$\sup\{\langle C, \widetilde{X}\rangle : \widetilde{X} \succeq 0, \langle \widetilde{A}_\alpha, \widetilde{X}\rangle = f_\alpha \quad \text{for all } \alpha \in \mathbb{N}_{2t}^n, \ \}. \tag{3.19}$$

As explained in section 1.2 of Chapter 1, its dual is given by:

$$\inf\{\sum_{\alpha\in\mathbb{N}^n_{2t}} f_\alpha y_\alpha : \sum_{\alpha\in\mathbb{N}^n_{2t}} y_\alpha \widetilde{A}_\alpha - C \succeq 0\} \tag{3.20}$$

Since $L(1) = 1$ by definition, we have that $y_0 = L(X^0) = L(1) = 1$. Further, it is very important to note that we have defined A_α such that

$$M_t(y) = \sum_{\alpha\in\mathbb{N}^n_{2t}} y_\alpha A_\alpha.$$

By combining these last two remarks we see that the program described in program (3.20) is exactly equal to the dual described in (3.11).

3.3 Basic properties of moment matrices

In this section we give some basic properties of moment matrices. First we show two technical lemmas in which upper bounds of certain coefficients of moment matrices are obtained. From these lemmas we obtain a corollary, which shows that if $M_t(y) \succeq 0$, all entries y_α can be bounded in terms of the y_α that correspond to the monomials 1 and X_i^{2t}.

We use the following notation:

$$\tau_k := \max\{y_{(2k,0,\dots,0)}, \dots, y_{(0,\dots,0,2k)}\} = \max_i y_{2ke_i} \text{ for } 0 \le k \le t. \tag{3.21}$$

So $\tau_0 = y_0$.

Lemma 3.5. Assume $M_t(y) \succeq 0$ in the univariate case ($n = 1$). Then $y_{2k} \le \max\{\tau_0, \tau_t\}$ for $0 \le k \le t$.

Proof. The proof will be by induction on t. For $t = 0$ we use that $\tau_0 = y_0$. Further for $t = 1$ we use that $\tau_1 \ge y_2$. Now assuming the lemma holds for $t-1$ where $t > 1$, this means that $y_0, \dots, y_{2t-2} \le \max\{y_0, y_{2t-2}\}$. Firstly we assume $y_0 \ge y_{2t-2}$. The result $y_0, \dots, y_{2t} \le \max\{y_0, y_{2t}\}$ easily follows. Secondly we assume that $y_0 < y_{2t-2}$. Since the $M_t(y) \succeq 0$, we deduce from the submatrix of $M_t(y)$ indexed by $\{\alpha, \beta\}$ that

$$y^2_{\alpha+\beta} \le y_{2\alpha} y_{2\beta}. \tag{3.22}$$

We can use this, the assumption $y_0 < y_{2t-2}$ and the induction hypothesis to obtain the following (in)equalities: $y_{2t-2}^2 = y_{t+t-2}^2 \leq y_{2t-4}y_{2t} \leq y_{2t-2}y_{2t}$. From this we can deduce that $y_{2t-2} \leq y_{2t}$, which leads to the same conclusion that $y_0, ..., y_{2t} \leq \max\{y_0, y_{2t}\}$. $\square$

Lemma 3.6. Let $M_t(y) \succeq 0$. Then $y_{2\alpha} \leq \tau_k$ for all $|\alpha| = k \leq t$.

Proof. In the univariate case it is obvious, since $y_{2k} = \tau_k$. Before we state the induction hypothesis, we check it for $n = 2$. Therefore we define

$$s := \max_{|\alpha|=k} y_{2\alpha}.$$

Assume this maximum is attained at $y_{2\alpha^*}$. Since $\alpha_1^* + \alpha_2^* = k$, clearly we have that $2\alpha_1^* \geq k \Leftrightarrow 2\alpha_2^* \leq k$. Now, without loss of generality we can assume that $2\alpha_1^* \geq k$. So, in order to apply the inequality described in (3.22) we make the following rewriting:

$$\begin{aligned} 2\alpha^* &= (k, 0) + (2\alpha_1^* - k, 2\alpha_2^*) \\ &= (k, 0) + (2\alpha_1^* - k + 2k - 2(\alpha_1^* + \alpha_2^*), 2\alpha_2^*) \\ &= (k, 0) + (k - 2\alpha_2^*, 2\alpha_2^*). \end{aligned}$$

Applying inequality (3.22), we get: $y_{2\alpha^*}^2 \leq y_{(2k,0)}y_{(2k-4\alpha_2^*,4\alpha_2^*)}$. Since $s^2 = y_{2\alpha^*}^2$ and $s \geq y_{(2k-4\alpha_2^*,4\alpha_2^*)}$ (definition s) and $y_{(2k,0)} \leq \tau_k$ (definition τ), this means that $s^2 \leq s\tau_k$. We thus can conclude that $s \leq \tau_k$, since $y_{2\alpha}$ is a diagonal element of $M_t(y)$ and therefore nonnegative. So we have finished the proof for $n = 2$.
Now we assume $n \geq 3$ and we assume that Lemma 3.6 holds for $n - 1$. In other words we assume that $y_{2\alpha} \leq \tau_k$ if $|\alpha| = k$ and $\alpha_i = 0$ for some i. Now, without loss of generality we assume that $1 \leq \alpha_1 \leq \alpha_2 \leq ... \leq \alpha_n$ and we consider the following sequences:

$$\gamma := (2\alpha_1, 0, \alpha_3 + \alpha_2 - \alpha_1, \alpha_4, ..., \alpha_n) \text{ and } \gamma' := (0, 2\alpha_1, \alpha_3 + \alpha_1 - \alpha_2, \alpha_4, ..., \alpha_n).$$

Note that the assumed ordering is needed here, since γ and γ' can not have negative entries. However a different ordering could be handled with likewise. We clearly have $|\gamma| = |\gamma'| = |\alpha| = k$ and $\gamma + \gamma' = 2\alpha$. Since $\gamma_2 = \gamma_1' = 0$, we can apply the induction hypothesis and see that $y_{2\gamma}, y_{2\gamma'} \leq \tau_k$. Hence, we see that $y_{2\alpha}^2 = y_{\gamma+\gamma'}^2 \leq y_{2\gamma}y_{2\gamma'} \leq \tau_k^2$, which implies that $y_{2\alpha} \leq \tau_k$. $\square$

We now combine the two above lemmas to get to the following corollary.

Corollary 3.7. Assume $M_t(y) \succeq 0$. Then $|y_\alpha| \leq \max_{0\leq k\leq t} \tau_k = \max\{\tau_0, \tau_t\}$ for all $|\alpha| \leq 2t$.

Proof. From Lemma 3.5 we can deduce that $y_{(2k,0,\ldots,0)} \leq \max\{\tau_0, \tau_t\}$, since

$$y_{2k} = L(X^{2k}) = L(X^{2k}X^0 \cdots X^0) = y_{(2k,0,\ldots,0)}.$$

This means that $\tau_k \leq \max\{\tau_0, \tau_t\}$ and so we obtain that

$$\max_{0\leq k\leq t} \tau_k = \max\{\tau_0, \tau_t\} =: \tau. \tag{3.23}$$

Moreover, by Lemma 3.6 we get that $y_{2\alpha} \leq \tau$ for $|\alpha| \leq t$. Now consider a sequence γ such that $|\gamma| \leq 2t$. We can obviously write $\gamma = \alpha + \beta$, where $|\alpha|, |\beta| \leq t$ for some $\alpha, \beta \in \mathbb{N}^n$. This enables us to write: $y_\gamma^2 \leq y_{2\alpha}y_{2\beta} \leq \tau^2$. So we see that $|y_\gamma| \leq \tau$. □

3.4 Characterizing bounded moment sequences with a representing measure on the hypercube

Recall the duality and inclusion relations of the sets $M, M_{\succeq 0}, \Sigma$ and P as explained in Section 3.2 . Whereas in chapter two Theorem 2.8 deals with the sets Σ and P, the theorem treated in this section deals with the discrepancy between the sets M and $M_{\succeq 0}$. It states that if a certain bound on the coefficients y_α of a PSD moment matrix $M(y)$ in terms of α can be set, then the sequence y, supported by the hypercube, has a representing measure.

Theorem 3.8. [1] Let $y \in \mathbb{R}^{\mathbb{N}^n}, C \in \mathbb{R}_{\geq 0}$ and $K := [-C, C]^n$. We now have equivalence for the following two assertions:

(i) y has a representing measure supported by the set K.

(ii) $M(y) \succeq 0$ and there exists a constant $C_0 \geq 0$ such that $|y_\alpha| \leq C_0 C^{|\alpha|}$ for all $\alpha \in \mathbb{N}^n$.

First we prove $(ii) \Rightarrow (i)$. For this direction, we need the following two lemmas:

Lemma 3.9. Assume $M(y) \succeq 0$ and $|y_\alpha| \leq C_0 C^{|\alpha|}$ for all $\alpha \in \mathbb{N}^n$ for some constants $C_0, C > 0$. Then $|y_\alpha| \leq y_0 C^{|\alpha|}$ for all $\alpha \in \mathbb{N}^n$.

Proof. First assume that $y_0 = 0$. Since $M(y) \succeq 0$ we know that the row (and column) of $M(y)$ starting from y_0 only contains zero's. Since this row contains all entries of y, we deduce that all elements in the sequence y are equal to zero. Further $y_0 \geq 0$ because $M(y) \succeq 0$. So we may assume that $y_0 > 0$. Now we rescale the sequence and assume that $y_0 = 1$. What remains to be shown is that $|y_\alpha| \leq C^{|\alpha|}$ for all $\alpha \in \mathbb{N}^n$.
First, note that $y_\alpha^2 \leq y_{2\alpha}$, since $\begin{pmatrix} 1 & y_\alpha \\ y_\alpha & y_{2\alpha} \end{pmatrix}$ is the submatrix of M indexed by $\{1, \alpha\}$. Next, we use this to show by induction on k that $|y_\alpha| \leq (y_{2^k\alpha})^{1/2^k}$ for any $k \geq 1$.
Namely for $k = 1$, we get $|y_\alpha| \leq (y_{2\alpha})^{1/2}$. Then after taking squares on both sides, which is possible because both sides are positive, we obtain the inequality $y_\alpha^2 \leq y_{2\alpha}$. Assuming that our hypothesis is right for k, we see that $(y_{2^{k+1}\alpha})^{1/2^{k+1}} \geq (((y_{2^k\alpha})^{1/2^k})^{1/2})^2 = (y_{2^k\alpha})^{1/2^k} \geq |y_\alpha|$, and this small induction proof is done.

As assumed in Lemma 3.9 we have that $|y_\alpha| \leq C_0 C^{|\alpha|}$. When we substitute $2^k\alpha$ for α in this inequality, we obtain $|y_{2^k\alpha}| \leq C_0 C^{|2^k\alpha|}$. By combining this with $|y_\alpha| \leq (y_{2^k\alpha})^{1/2^k}$, we obtain $|y_\alpha| \leq (C_0 C^{2^k|\alpha|})^{1/2^k} = C_0^{1/2^k} C^{|\alpha|}$. Now, after letting k go to infinity, we obtain $|y_\alpha| \leq C^{|\alpha|}$ as desired. $\square$

Lemma 3.10. If $C > 0$ and $K = [-C, C]^n$, then

$$S = \{y \in \mathbb{R}^{\mathbb{N}^n} \mid y_0 = 1, M(y) \succeq 0, \quad |y_\alpha| \leq C^{|\alpha|} \ \forall \alpha \in \mathbb{N}^n\} \tag{3.24}$$

is a convex set whose extreme points are the vectors $\zeta_x = (x^\alpha)_{\alpha \in \mathbb{N}^n}$ for $x \in K$.

Proof. For the proof of the convexity of S, only the positive semi-definite condition is non-trivial, but after noting that

$$M(\lambda x + (1-\lambda)y) = \lambda M(x) + (1-\lambda)M(y) \tag{3.25}$$

for $\lambda \in (0,1)$ and $x, y \in S$, this is also easy.
Now we will prove that the extreme points of S are indeed the vectors ζ_x. So assume y is an extreme point of S. Fix $\alpha_0 \in \mathbb{N}^n$. In order to prove that y is indeed equal to a vector ζ_x we will show the following property of y:

$$y_{\alpha+\alpha_0} = y_\alpha y_{\alpha_0} \quad \forall \alpha \in \mathbb{N}^n. \tag{3.26}$$

First we continue with the rest of the proof. Later we prove (3.26). We can set $x = (y_{(1,0,\ldots,0)}, \ldots, y_{(0,\ldots,0,1)})$. Since $y \in S$, we have $|x_i| \leq C$, hence

$x \in K$. Further, since we know (3.26) is true for all $\alpha_0 \in \mathbb{N}^n$, we see that $y_\alpha = y_{(\alpha_1,\ldots,\alpha_n)} = y_{\alpha_1 e_1} \cdots y_{\alpha_n e_n} = y_{(1,0,\ldots,0)}^{\alpha_1} \cdots y_{(0,\ldots,0,1)}^{\alpha_n} = x^\alpha$ for all α. So we see that $y = \zeta_x$ and that every y corresponds to a unique vector ζ_x.

It remains to show that equation (3.26) holds. The idea is that we create two elements in S, for which (3.26) holds, such that y is a convex combination of these elements. This would imply that y is one of them since y is assumed to be an extreme point. First we define the sequence $y_\alpha^{(\epsilon)} := C^{|\alpha_0|} y_\alpha + \epsilon y_{\alpha+\alpha_0}$ for $\alpha \in \mathbb{N}^n$ and $\epsilon \in \{\pm 1\}$. Subsequently, we apply Lemma 3.9 to this sequence. So we see that $|y_\alpha^{(\epsilon)}| \leq C^{|\alpha_0|}(1+\epsilon)C^{|\alpha|}, \quad$ for all $\alpha \in \mathbb{N}^n$, where we use the definition of $y^{(\epsilon)}$ and the fact that y is an element of S. Secondly we will show that $M(y^{(\epsilon)}) \succeq 0$, i.e. for all $p \in \mathbb{R}[\underline{X}]$ we have that

$$p^T M(y^{(\epsilon)}) p = \sum_{\gamma,\gamma} p_\gamma p_{\gamma'} y_{\gamma+\gamma'}^{(\epsilon)} \geq 0. \tag{3.27}$$

To show this, we fix $p \in \mathbb{R}[\underline{X}]$ and we define a new sequence

$$z := M(y^{(\epsilon)}) \mathrm{vec}(p^2) \in \mathbb{R}^{\mathbb{N}^n}$$

with $z_\alpha = \sum_{\gamma,\gamma'} p_\gamma p_{\gamma'} y_{\alpha+\gamma+\gamma'}^{(\epsilon)}$ for $\alpha \in \mathbb{N}^n$ and where $\mathrm{vec}(p^2)$ denotes the coefficient vector of p^2 . Clearly we are done if $z_0 \geq 0$. Now combining the fact that y is an element of S (so $|y_\alpha| \leq C^{|\alpha|}$) and some standard absolute value properties, we see that $|z_\alpha| \leq (\sum_{\gamma,\gamma'} |p_\gamma p_{\gamma'}| C^{|\gamma|+|\gamma'|}) C^{|\alpha|} \quad \forall \alpha \in \mathbb{N}^n$. Furthermore we see that by definition (see equation (3.2) in Section 3.3) $z := M(y)vec(p^2) := gy$ for $g = p^2$. Now using elementary arithmetic on moment matrices (see Section 4.1.4 of [16]), we come to the following:

$$\mathbf{q}^T M(z) \mathbf{q} = \mathbf{q}^T M(p^2 y) \mathbf{q} = vec(pq)^T M(y) vec(pq) \geq 0 \quad \forall q \in \mathbb{R}[\underline{X}], \tag{3.28}$$

where the last inequality holds because $M(y) \succeq 0$. So $M(z) \succeq 0$, which implies that $z_0 \geq 0$. Hence $M(y^{(\epsilon)}) \succeq 0$. Now we again can apply Lemma 3.9 and conclude that $|y_\alpha^{(\epsilon)}| \leq y_0^{(\epsilon)} C^{|\alpha|}$ for all α.
We are now able to prove equation (3.26). Firstly, if we assume that $y_0^{(\epsilon)} = 0$ for some $\epsilon \in \{\pm 1\}$, then $y^{(\epsilon)} = 0 \quad$ (since $M(y^{(\epsilon)}) \succeq 0$). Then, if we set $\alpha = (0, ..., 0)$ in the definition of $y_\alpha^{(\epsilon)}$, we get that $0 = C^{|\alpha_0|} y_0 \pm y_{\alpha_0}$ and hence $y_0 = y_{\alpha_0} = 0$ and we are done.
Now we assume that $y_0^{(\epsilon)} > 0$ for $\epsilon \in \{\pm\}$. Then we have that $\frac{y^{(\epsilon)}}{y_0^{(\epsilon)}}$ belongs to S

for both $\epsilon = 1$ and $\epsilon = -1$, since all properties of the set S are easily verified because $|y_\alpha^{(\epsilon)}| \leq y_0^{(\epsilon)} C^{|\alpha|}$. Furthermore the sequences $y^{(\epsilon)}$ are constructed such that

$$y = \frac{y_0^{(1)}}{2C^{|\alpha_0|}} \frac{y^{(1)}}{y_0^{(1)}} + \frac{y_0^{(-1)}}{2C^{|\alpha_0|}} \frac{y^{(-1)}}{y_0^{(-1)}}. \tag{3.29}$$

So y is a convex combination of the points $\frac{y^{(1)}}{y_0^{(1)}}$ and $\frac{y^{(-1)}}{y_0^{(-1)}} \in S$ (note that $\frac{y_0^{(1)}}{2C^{|\alpha_0|}} + \frac{y_0^{(-1)}}{2C^{|\alpha_0|}} = 1$). Since we assumed that y is an extreme point of S, y is equal to one of them, i.e. $y = \frac{y^{(1)}}{y_0^{(1)}}$ or $y = \frac{y^{(-1)}}{y_0^{(-1)}}$. Now we are done because $y_\alpha = \frac{C^{|\alpha_0|} y_\alpha + \epsilon y_{\alpha+\alpha_0}}{C^{|\alpha_0|} + \epsilon y_{\alpha_0}}$ and after multiplication by $C^{|\alpha_0|} + \epsilon y_{\alpha_0}$ on both sides and some basic algebra we obtain (3.26). $\square$

Here follows the rest of the proof of Theorem 3.8 for the part $(ii) \Rightarrow (i)$. First assume that $M(y) \succeq 0$ and $|y_\alpha| \leq C_0 C^{|\alpha|}$ for all $\alpha \in \mathbb{N}^n$ for some C_0. We will prove that y has a representing measure supported by K. The idea is to show that $y \in S$. Then we make use of the fact that the extreme points of S have a representing measure and the Krein-Milman Theorem to conclude that y has a representing measure.
Suppose $y_0 = 0$. Then we have that $y = 0$ for which the zero measure can be the representing measure, so we are done. So we may assume that $y_0 = 1$ (else we rescale y). By Lemma 3.9 we know that $|y_\alpha| \leq y_0 C^{|\alpha|}$ for all $\alpha \in \mathbb{N}^n$. So y belongs to S (as described in (3.24)). Recall that the extreme points of S are $\{\zeta_x : x \in [-C, C]^n\}$. Knowing these extreme points, we can use the Krein-Milman theorem, which implies that S is equal to the closure of the convex hull of the extreme points of S. So we deduce that y is an element of closure of the convex hull of the extreme points of S. So $y = \lim_{i \to \infty} y^{(i)}$, where $y^{(i)}$ is an element of the convex hull of the extreme points of S . All these elements $y^{(i)}$, which are sequences itself, are linear combinations of sequences that have a representing measure and therefore also have a representing measure. Now we want to show that the limit y of this sequence $(y^{(i)})_{i \geq 0}$ of sequences has a representing measure. By Theorem 3.4, showing that y has representing measure is the same as showing that $\sum_\alpha p_\alpha y_\alpha \geq 0$ for all polynomials $p \in \mathbb{R}[X]$ such that $p \geq 0$ on K. Since all $y^{(i)}$ have a representing measure, we know by the above theorem that $\sum_\alpha p_\alpha y_\alpha^{(i)} \geq 0$ for any polynomial $p \in \mathbb{R}[X]$ such that $p \geq 0$ on K for all $i = 1, 2, \ldots.$ Now we can take the limit and get the following: $\lim\limits_{i \to \infty} \sum_\alpha p_\alpha y_\alpha^{(i)} = \sum_\alpha p_\alpha \lim_{i \to \infty} y_\alpha^{(i)} = \sum_\alpha p_\alpha y_\alpha \geq 0$, where the last

inequality holds since the limit can not be negative if all the elements in the sequence converging to it are nonnegative.

Now we show $(i) \Rightarrow (ii)$ for Theorem 3.8. So we assume that y has a representing measure supported by K. In order to show that the infinite matrix $M(y)$ is positive semi-definite, we need to show that $M_t(y) \succeq 0$ for all integers $t \geq 1$ (by definition). This follows immediately from Lemma 3.2. Further, since $K = [-C, C]$, $|x_i| \leq C$ for all i. Therefore $|y_\alpha| \leq \int_K |x^\alpha| \mu(dx) \leq \mu(K) C^{|\alpha|}$ and the proof of Theorem 3.8 is finished.

3.5 Density result for sos polynomials - Proof of Theorem 2.8

Recall that Theorem 2.8 is given as follows:

Theorem 2.8. Let f be a polynomial in $\mathbb{R}[\underline{X}]$ which is nonnegative on $[-1,1]^n$. For all $\epsilon > 0$ there exists an integer $t_0 \geq 0$ such that

$$f + \epsilon \left(1 + \sum_{i=1}^{n} X_i^{2t} \right) \in \Sigma,$$

for all $t \geq t_0$.

Firstly we would like to note that Lasserre has won the Lagrange prize 2009 (http://www.mathopt.org/?nav=lagrange_2009), because of this result. The fact that the proof makes use of a large scala of different tools such as semi-definite programming, duality theory, convexity theory, moment theory and more, makes it a beautiful proof. Here follows a rough sketch of the proof: The goal is to prove that $f + \epsilon(1 + \sum_{i=1}^{n} X_i^{2t})$ is an sos. For this purpose we have formulated the sdp in (3.32) below, which computes the largest value $-d_t^*$ for $-d_t^* \in \langle -\infty, 0]$ depending on t for which $f + d_t^*(1+\sum_{i=1}^{n} X_i^{2t})$ is an sos. By obtaining the dual formulation ϵ_t^*, as described in (3.31) below, of d_t^* and showing that there is no duality gap, it can be shown that $f+\epsilon(1+\sum_{i=1}^{n} X_i^{2t})$ is an sos as long as $\epsilon \geq \epsilon_t^*$. Finally, since it can be shown that $\lim_{t\to\infty} \epsilon_t^* = 0$ it we obtain an sos for every $\epsilon > 0$.
The following proposition is the main body of the proof of Theorem 2.8. In this proposition we use the following notation:

$$\Theta_t = 1 + \sum_{i=1}^{n} X_i^{2t}. \tag{3.30}$$

Proposition 3.11. Given a polynomial $f \in \mathbb{R}[\underline{X}]$, consider the following program:

$$\epsilon_t^* := \inf\{\mathbf{f}^T y \mid M_t(y) \succeq 0, \; y^T \mathbf{\Theta}_t \leq 1\} \tag{3.31}$$

for an integer $t \geq \lceil \deg(f)/2 \rceil$. Now the following three assertions hold:

(i) $-\infty < \epsilon_t^* \leq 0$ and the infimum of (3.31) is attained.

(ii) For $\epsilon \geq 0$ we have the following equivalence: $f + \epsilon\Theta_t$ is an sos $\Leftrightarrow \epsilon \geq -\epsilon_t^*$. In particular: f is an sos $\Leftrightarrow \epsilon_t^* = 0$.

(iii) If f is nonnegative on $[-1,1]^n$, then $\lim_{t\to\infty} \epsilon_t^* = 0$.

Proof. Here we prove (i). Since $y = 0$ is a solution to (3.31), we see the feasible region of (3.31) is non-empty. Furthermore, assume y is a feasible solution of (3.31). Then, because $y_0, y_{(2t,0,\dots,0)}, \dots, y_{(0,\dots,0,2t)}$ are diagonal elements of $M_t(y)$ and because their sum is less or equal then 1 (from the constraint of (3.31)), we know that $0 \le y_0, y_{(2t,0,\dots,0)}, \dots, y_{(0,\dots,0,2t)} \le 1$. Now by using Corollary 3.7, we deduce that $|y_\alpha| \le 1$ for all α. Therefore we know that the feasible region of (3.31) is bounded. So the infimum is attained and $-\infty < \epsilon_t^* \le 0$.

Here we prove (ii). First we will show that the dual of ϵ_t^* is given by:

$$d_t^* = \sup_{\lambda \ge 0}\{-\lambda : \ f + \lambda\Theta_t \ \text{ is an sos}\}. \tag{3.32}$$

The main step in showing this, is to write ϵ_t^* in standard form as described in (1.6). For this purpose we write $1 - y^T\boldsymbol{\Theta}_t = 1 - y_0 - \sum_i y_{2te_i}$. Moreover note again that $M_t(y) = \sum_{|\alpha|\le 2t} A_\alpha y_\alpha$, where A_α is defined as in (3.14), so A_α has order $s(n,t)$. In order to obtain the right standard form constraints, we define the following matrix of order $s(n,t)+1$:

$$\widetilde{A}_\alpha = \left(\begin{array}{c|c} A_\alpha & 0 \\ \hline 0 & -1 \end{array}\right) \quad \text{if} \quad \alpha \in \{0, 2te_1, \dots, 2te_n\} \tag{3.33}$$

and

$$\widetilde{A}_\alpha = \left(\begin{array}{c|c} A_\alpha & 0 \\ \hline 0 & 0 \end{array}\right) \quad \text{else.} \tag{3.34}$$

Further we set $C' = -C$, where C is described in (3.16). Now ϵ_t^* can be written as the following standard form:

$$\inf\{\sum_{|\alpha|\le 2t} f_\alpha y_\alpha : \sum_{|\alpha|\le 2t} y_\alpha \widetilde{A}_\alpha - C' \succeq 0\}. \tag{3.35}$$

Its dual is

$$\sup\{\langle C', \widetilde{X}\rangle : \widetilde{X} \succeq 0, \langle \widetilde{A}_\alpha, \widetilde{X}\rangle = f_\alpha \ \text{ for all } \ \alpha\}, \tag{3.36}$$

where $\widetilde{X} \in S^{s(n,t)+1}$. Let us set $\widetilde{X}_{s(n,t)+1,s(n,t)+1} = \lambda$. Note that the constraint $\langle \widetilde{A}_\alpha, \widetilde{X}\rangle = f_\alpha$ of the program described in (3.36) can be rewritten as follows:

$$\left\langle \left(\begin{array}{c|c} A_\alpha & 0 \\ \hline 0 & 0 \end{array}\right), \widetilde{X} \right\rangle = f_\alpha + \lambda \quad \text{if} \quad \alpha \in \{0, 2te_1, \dots, 2te_n\} \tag{3.37}$$

and

$$\left\langle \left(\begin{array}{c|c} A_\alpha & 0 \\ \hline 0 & 0 \end{array} \right), \widetilde{X} \right\rangle = f_\alpha \quad \text{else.} \tag{3.38}$$

Let $X \in S^{s(n,t)}$. We can rewrite (3.36) now as follows:

$$\sup_{\lambda \geq 0}\{-\lambda : X \succeq 0, (f - \lambda\Theta_t)_\alpha = \sum_{\beta,\gamma:\beta+\gamma=\alpha} X_{\beta,\gamma} \text{ for all } \alpha\}. \tag{3.39}$$

From Lemma 2.10 we know that $f - \lambda\Theta_t$ is an sos if and only if there exists an $X \in S^{s(n,t)}$ such that $X \succeq 0$ and that $(f - \lambda\Theta_t)_\alpha = \sum_{\beta+\gamma=\alpha} X_{\beta,\gamma}$ for all α. So now it should be clear that the dual of ϵ_t^* can be given by

$$d_t^* := \sup_{\lambda \geq 0}\{-\lambda \;\; : \;\; f + \lambda\Theta_t \text{ is an sos}\}. \tag{3.40}$$

Further we see that (3.31) is strictly feasible, because we can pick a sequence of moments of a measure that has positive density all over $\mathbb{R}^n$, where the moments up to order $2t$ are finite. Then after rescaling (if necessary) we obtain a moment sequence such that $y^T\Theta_t \leq 1$. So we obtain a strictly feasible solution.
Since (3.32) is also bounded from above, we use strong duality (see Theorem 1.2) and conclude that (3.32) attains its supremum and there is no duality gap ($\epsilon_t^* = d_t^*$). Now note the following equivalence: $f + \epsilon\Theta_t$ is an sos $\Leftrightarrow -\epsilon \leq d_t^* = \epsilon_t^*$, (i.e. $\epsilon \geq -\epsilon_t^*$). Here the direction '$\Leftarrow$' is trivial. For the direction '$\Rightarrow$' we note that $-\epsilon_t^* + c = \epsilon$ for some $c \in \mathbb{R}_{\geq 0}$. Hence $f + \epsilon\Theta_t = f + (-\epsilon_t^* + c)\Theta_t$ which clearly is an sos since Θ_t and $f - \epsilon_t^*\Theta_t$ are sums of squares.

Here we prove (*iii*). First note that, from (i), we know that $\epsilon_t^* \leq 0$ for all integers $t > 0$. So we only need to show that $\lim_{t\to\infty} \epsilon_t^* \geq 0$. The idea is to take a subsequence of $(\epsilon_t^*)_{t\geq 0}$ and then to show that this sequence only has one accumulation point which is larger than or equal to 0. We start by assuming $y^{(t)}$ is the optimal solution for (3.31). From the proof of (i) we know that $y^{(t)} \in [-1,1]^{\mathbb{N}^n_{2t}}$. Now we complete $y^{(t)}$ to the element $\tilde{y}^{(t)} = (y^{(t)}, 0, ..., 0) \in [-1,1]^{\mathbb{N}^n}$ and we consider the sequence $(\tilde{y}^{(t)})_{t\geq 0}$. Since $[-1,1]^{\mathbb{N}^n}$ is compact, we know this sequence has a converging subsequence $(\tilde{y}^{(t_l)})_{l\geq 0}$ which converges to some limit $y^* \in [-1,1]^{\mathbb{N}^n}$. To this limit we want to apply Theorem 3.8. Therefore first note that the there is coordinate-wise convergence to y^*, i.e. $\tilde{y}_\alpha^{(t_l)} \to y_\alpha^*$ as $l \to \infty$. Since $M_{t_l}(y) \succeq 0$ (sine we assumed that $y^{(t)}$ is the optimal solution for (3.31)) for all $l \geq 0$, we know that $M(y^*) \succeq 0$. Moreover, recall that $y \in [-1,1]^{\mathbb{N}^n}$. So we can deduce from Theorem 3.8 that y^* has a representing measure μ on $[-1,1]^{\mathbb{N}^n}$. In particular, we see that $f^T y^* = \int_{[-1,1]^n} f(x)\mu(dx)$. By assumption, we know that $f \geq 0$ on $[-1,1]^n$, so $f^T y^* \geq 0$. Now we see that $\lim_{l\to\infty} \epsilon^*_{t_l} \geq 0$. Therefore we can conclude that ϵ^*_t also converges to 0 as $t \to \infty$.

Now we can prove Theorem 2.8. Let $\epsilon > 0$. From (iii) from Proposition 3.11 we know that $\lim_{t\to\infty} \epsilon^*_t = 0$. So there exists a $t_0 \in \mathbb{N}$ such that $\epsilon^*_t \geq -\epsilon$ for all $t \geq t_0$. Then from (ii) from proposition 3.11 , we now know that $f + \epsilon\Theta_t$ is an sos. $\square$

Chapter 4

Positivstellensätze

In this chapter we start by showing the relation between classical algebraic geometry and real algebraic geometry. Further, we introduce quadratic modules and preorderings. Then, after these preliminaries, we are able to state several Positivstellensätze.

Where classical algebraic geometry deals with zeros of polynomial equations as subsets of $\mathbb{C}^n$, real algebraic geometry deals with subsets of $\mathbb{R}^n$ defined by polynomial equations and inequalities. These subsets are called semi-algebraic sets. A basic closed semi-algebraic set K is given by

$$K = \{x \in \mathbb{R}^n : g_1 \geq 0, ..., g_m \geq 0\}, \tag{4.1}$$

where $g_1(x), ..., g_m(x) \in \mathbb{R}[\underline{X}]$. Throughout we set $g_0 = 1$.
Classical and real algebraic geometry both deal with Stellensätze. In classical algebraic geometry, Nullstellensätze are considered. The first Nullstellensatz was discovered by Hilbert and was given as follows:

Theorem 4.1. [Hilbert's Nullstellensatz] For $p, g_1, ..., g_m \in \mathbb{R}[\underline{X}]$ we have that

$$p = 0 \text{ on } \{x \in \mathbb{C}^n : g_1(x) = 0, ..., g_m(x) = 0\} \Leftrightarrow p^k = \sum_{j=1}^{n} u_j g_j, \tag{4.2}$$

for some $u_j \in \mathbb{R}[\underline{X}]$ and $k \in \mathbb{N}$.

A corrolary of Theorem 4.3, also referred to as the *strong Nullstellensatz*, is the *weak Nullstellensatz*. The weak Nullstellensatz characterizes when a system of polynomials has no roots in common.

Corollary 4.2 (The weak Nullstellensatz)**.** For $g_1, ..., g_m \in \mathbb{R}[\underline{X}]$ and the ideal $I \subseteq \mathbb{R}[\underline{X}]$ generated by $(g_1, ..., g_m)$, we have the following:

$$\{x \in \mathbb{C}^n : g_1(x) = 0, ..., g_m(x) = 0\} = \emptyset \Leftrightarrow 1 = \sum_{j=1}^{n} u_j g_j \text{ for some } u_j \in \mathbb{R}[\underline{X}].$$

Proof. ($\Leftarrow$). Suppose $\{x \in \mathbb{C}^n : g_1(x) = 0, ..., g_m(x) = 0\}$ is not empty, then there exists an $x \in \mathbb{C}^n$ such that $0 = \sum_{j=1}^{n} u_j g_j \neq 1$ for all $u_j \in \mathbb{R}[\underline{X}]$.
($\Rightarrow$). We apply Theorem 4.3 for the constant polynomial $p = 1$. The result immediately follows. $\square$

The Real Nullstellensatz, the real variant of Hilbert's Nullstellensatz, is given as follows:

Theorem 4.3. [The Real Nullstellensatz] For $g_1, ..., g_m \in \mathbb{R}[\underline{X}]$ we have that

$$p = 0 \text{ on } \{x \in \mathbb{R}^n : g_1(x) = 0, ..., g_m(x) = 0\} \Leftrightarrow p^{2k} + s = \sum_{j=1}^{n} u_j g_j, \quad (4.3)$$

for some $u_j \in \mathbb{R}[\underline{X}]$, $s \in \Sigma$ and $k \in \mathbb{N}$.

Analogously as for Hilbert's Nullstellensatz, a certificate for the nonexistence of a real solution to a system of polynomial equations can be derived.

Corollary 4.4. For $g_1, ..., g_m \in \mathbb{R}[\underline{X}]$ we have that

$$\{x \in \mathbb{R}^n : g_1(x) = 0, ..., g_m(x) = 0\} = \emptyset$$

if and only if

$$-1 = s + \sum_{j=1}^{n} u_j g_j$$

for some $u_j \in \mathbb{R}[\underline{X}], s \in \Sigma$.

Proof. The proof is analogous to the proof of Corollary 4.2. $\square$

Remark 4.5. Considering Hilbert's Nullstellensatz, we see that checking whether p^k equals sum $\sum_{j=1}^{n} u_j g_j$, amounts to solving a linear program after setting bounds on the degree of the u_j. The constraints from this linear program are obtained by equating the coefficients of p^k with the coefficients of $\sum_{j=1}^{n} u_j g_j$. However, in The Real Nullstellensatz there is an sos polynomial s involved. Finding s and the u_j now amounts to solving an SDP. For this purpose, we again set a degree bound on the u_j. Since $\deg(s) = \deg(\sum_{j=1}^n u_j g_j - p^{2k})$, we can find an integer d such that $s \in \mathbb{R}[\underline{X}]_d$. So we have to try to find a PSD matrix Q such that $s = [\underline{X}]_d Q [\underline{X}]_d$, such that $p^{2k} + s = \sum_{j=1}^n u_j g_j$.

The analogue of a Nullstellensätz in real algebraic geometry is a Positivstellensatz. This is a result of the following form:

$$p > 0 \text{ on } K \Rightarrow p = \sum_j s_j g_j \tag{4.4}$$

for $s_j \in \Sigma$ and g_j as in (4.1) and (possibly) a condition on K.

Before formulating Krivine's Positivstellensatz, we introduce the following terminology following [20].

Let R be a commutative ring in which 2 is a unit.

Definition 4.6. A preordering of R is a subset T of R that satisfies the following properties: $T + T \subseteq T, T \cdot T \subseteq T$ and $f^2 \in T$ for all $f \in R$.

For example, the preordering of $\mathbb{R}[\underline{X}]$ generated by $\mathbf{g} = (g_1, ..., g_m)$ (with the $g_1, ..., g_m \in \mathbb{R}[\underline{X}]$) is given by

$$\mathbf{T}(\mathbf{g}) = \left\{ s_0 + \sum_{J \subseteq \{1,...,m\}} s_J g_J : s_0, s_J \in \Sigma \right\}, \tag{4.5}$$

where $g_J = \prod_{j \in J} g_j$.

Remark 4.7. Note that there are 2^n different subsets of $\{1, ..., n\}$. So there can be involved up to 2^n sos polynomials in an element of $\mathbf{T}(\mathbf{g})$.

Theorem 4.8. [11][Krivine's Positivstellensatz,1964]. For K as in (4.1) and $p \in \mathbb{R}[\underline{X}]$, the following assertions hold.

(i) $p > 0$ on $K \Leftrightarrow pf = 1 + h$ for some $f, h \in \mathbf{T}(\mathbf{g})$.

(ii) $p \geq 0$ on $K \Leftrightarrow pf = p^{2k} + h$ for some $f, h \in \mathbf{T}(\mathbf{g})$ and $k \in \mathbb{N}$.

(iii) $p = 0$ on $K \Leftrightarrow -p^{2k} \in \mathbf{T}(\mathbf{g})$ for some $k \in \mathbb{N}$.

(iv) $K = \emptyset \Leftrightarrow -1 \in \mathbf{T}(\mathbf{g})$.

Proof. For a proof see Chapter 2 of [20]. □

Note that $\mathbf{T}(\mathbf{g}) \subseteq P(K)$. These sets are not equal in general. Consider the following example.

Example 4.9. Let $B = \{x \in \mathbb{R} : g = (1-x^2)^3 \geq 0\}$ and $p = 1-X^2$. Clearly $p = (1-x^2) \geq 0$ on B. Now, assume for contradiction that $p \in \mathbf{T}(\mathbf{g})$. Then

$$1 - X^2 = s_0 + s_1(1 - X^2)^3$$

for some $s_0, s_1 \in \Sigma$. Then, since both $1-X^2$ and $(1-X^2)^3$ can be divided by $1-X^2$, also s_0 can be divided by $1-X^2$. Since $s_0 \in \Sigma$, this would mean that $(1-X^2)^2$ also divides s_0. However, now $(1-X^2)^2$ divides $s_0+s_1(1-X^2)^3$, but clearly it does not divide $1-X^2$, so we have a contradiction. Hence $p \in P(B)$ and $p \notin \mathbf{T}((1-X^2)^3)$. However, note that $pg = p^4$, which supports (ii) of Theorem 4.8.

Schmüdgen discovered the following Positivstellensatz, which gives a representation result for positive polynomials on compact sets. This has been a very important improvement on (i) of Theorem 4.8, since it gives a denominator free representation of a polynomial.

Theorem 4.10. [33][Schmüdgen's Positivstellensatz,1991] Assume that K from (4.1) is compact. Then the following implication holds:

$$p(x) > 0 \text{ for all } x \in K \Rightarrow p \in \mathbf{T}(\mathbf{g}). \tag{4.6}$$

We will not prove this theorem here. However, we would like to mention that Schmüdgen's Positivstellensatz can be given as a direct application of a representation theorem (Theorem 5.4.4 of [20]), by using the following result of Wörmann.

Theorem 4.11. [35] For $\mathbf{T}(\mathbf{g})$ as in (4.5) and K as in (4.1), the following holds.

$$\mathbf{T}(\mathbf{g}) \text{ is Archimedean if and only if } K \text{ is compact.} \tag{4.7}$$

Proof. We postpone the proof to the end of this chapter. □

Although Schmüdgen's Positivstellensatz clearly is an improvement on (i) of Theorem 4.8, there still are 2^n unknown sos polynomials in the representation of p. So for semi-definite programming purposes an improvement is needed. Putinar has found such an improvement on Schmudgen's Positivstellensatz by setting a stronger condition on K. He proved that, under this stronger condition, there is a representation of p with only $n+1$ unknown sos polynomials. We introduce the following terminology.

Definition 4.12. A quadratic module of a ring R is a subset M of R with the following properties:

$$M + M \subseteq M, \Sigma M \subseteq M \text{ and } 1 \in M. \tag{4.8}$$

For example, a quadratic module can be given by

$$\mathbf{M}(\mathbf{g}) = \left\{ s_0 + \sum_{j=1}^{m} s_j g_j : s_j \in \Sigma \text{ for } j \in \{0, 1, ..., m\} \right\}, \tag{4.9}$$

where $\mathbf{g} = (g_1, ..., g_m)$.

Remark 4.13. [20] For a quadratic module $M \subseteq R$, $M \cap -M$ is an ideal. To see this let $I = M \cap -M$. Then $I + I \subseteq I$. Further $-(M \cap -M) = M \cap -M$, so $I = -I$. Further $0 \in I$, since $0 \in R$. Moreover $a^2 I \subseteq I$ for all $a \in R$, since $a^2 M \subseteq M$ and $a^2(-M) \subseteq -M$. Now assuming that 2 is a unit in A, we see that $aI \subseteq I$ for any $a \in A$, since

$$aI = \left(\left(\frac{a+1}{2} \right)^2 - \left(\frac{a-1}{2} \right)^2 \right) I = \left(\frac{a+1}{2} \right)^2 I - \left(\frac{a-1}{2} \right)^2 I \subseteq I, \tag{4.10}$$

where we use that $-(\frac{a-1}{2})^2 I \subseteq -I = I$ for the last inclusion.

Proposition 4.14. The following conditions on a quadratic module $\mathbf{M}(\mathbf{g})$ are equivalent.

(1) There exists an $h \in \mathbf{M}(\mathbf{g})$ such that $\{x \in \mathbb{R}^n : h(x) \geq 0\}$ is compact.

(2) There exists an $N \in \mathbb{N}$ such that $N - \sum_{i=1}^{n} X_i^2 \in \mathbf{M}(\mathbf{g})$.

(3) For all $f \in \mathbb{R}[\underline{X}]$, there exist an $N \in \mathbb{N}$ such that $N + f \in \mathbf{M}(\mathbf{g})$ and $N - f \in \mathbf{M}(\mathbf{g})$.

Proof. (3) $\Rightarrow$ (2) is clear. For (2) $\Rightarrow$ (1), recall that in $\mathbb{R}^n$ a set is compact if and only if it is closed and bounded. Clearly, the set

$$\{x \in \mathbb{R}^n : N - \sum_{i=1}^{n} x_i^2 \geq 0\}$$

satisfies both of these conditions. For (1) $\Rightarrow$ (3), consider a polynomial $f \in \mathbb{R}[\underline{X}]$ and note that the set $K = \{x \in \mathbb{R}^n : h(x) \geq 0\}$ is bounded. Now, since f is a polynomial and thus a continuous function, there exists a natural number $N \in \mathbb{N}$ such that $-N < f(x) < N$ on the compact set K. So $N + f, N - f > 0$ on K. Now by Theorem 4.10 we see that $N + f, N - f \in \mathbf{T}(h)$. To conclude, note that $\mathbf{T}(h) \subseteq \mathbf{M}(\mathbf{g})$, since $h \in \mathbf{M}(\mathbf{g})$. Therefore $N + f, N - f \in \mathbf{M}(\mathbf{g})$. □

Definition 4.15. We say that $\mathbf{M}(\mathbf{g})$ is Archimedean if $(1), (2)$ or (3) of Proposition 4.14 is satisfied.

Example 4.16. Consider the set $K = \{x \in \mathbb{R}^n : x_i \geq 0, \sum_{i=1}^{n} x_i \leq 1\}$. We will show that the quadratic module $QM = \mathbf{M}(X_1, ..., X_n, 1 - \sum_{i=1}^{n} X_i)$ that corresponds to K is Archimedean. For this end we show that condition (2) of definition 4.15 holds, i.e. that there exists an $N \in \mathbb{N}$ such that

$$N - \sum_{i=1}^{n} X_i^2 \in QM.$$

We pick $N = n$ and show that $n - \sum_{i=1}^{n} X_i^2 \in QM$. Note the following manipulations.

$$\begin{aligned} n - \sum_i X_i^2 &= \sum_i (1 - X_i^2) = \sum_i (1 - X_i)(1 + X_i) \\ &= \sum_i \underbrace{\left(\frac{1 + X_i}{2} + \frac{1 - X_i}{2}\right)}_{=1} (1 - X_i)(1 + X_i) \\ &= \sum_i \frac{(1 + X_i)^2}{2}(1 - X_i) + \frac{(1 - X_i)^2}{2}(1 + X_i). \end{aligned}$$

Now note that $1 - X_i = (1 - \sum_j X_j) + \sum_{j \neq i} X_j \in QM$. So, since also $1 + X_i \in QM$, we are done.

Putinar discovered the following Positivstellensatz, using this Archimedean property.

Theorem 4.17. [28][Putinar's Positivstellensatz, 1993]. Assume that the quadratic module $\mathbf{M}(\mathbf{g})$ as in (4.9) is Archimedean, then the following implication holds:

$$p(x) > 0 \text{ for all } x \in K \Rightarrow p \in \mathbf{M}(\mathbf{g}). \tag{4.11}$$

Proof. For a proof see Chapter 13 of [16]. □

One could wonder whether every compact set K corresponds to an Archimedean quadratic module $M(\mathbf{g})$. The answer is no. However, constructing such an example is not trivial. The first explicit counterexample with this property was given by Jacobi and Prestel [10].

Example 4.18 (Jacobi-Prestel example)**.** Consider the semi-algebraic set

$$S = \{x \in \mathbb{R}^n : g_1(x) \geq 0, ..., g_n(x) \geq 0, g_{n+1}(x) \geq 0\}, \tag{4.12}$$

with $g_1 = X_1 - \frac{1}{2}, ..., g_n = X_n - \frac{1}{2}, g_{n+1} = 1 - \prod_{i=1}^{n} X_i$.
Clearly S is closed and bounded and thus compact. Now we construct a quadratic module $H \in \mathbb{R}[\underline{X}]$ with the following properties:

(i) H contains $g_1, ..., g_{n+1}$.

(ii) $k - \sum_{i=1}^{n} X_i^2 \notin H$ for all k.

If we can construct such a quadratic module, which clearly is non-Archimedean because of property *(ii)*, we see that the quadratic module $M(\mathbf{g})$ corresponding to S also is non-Archimedean. This can be understood by considering (1) of Proposition 4.14 as definition for the Archimedean property for a quadratic module.
We are going to construct a quadratic module satisfying the above properties. For this purpose we consider the group $\Gamma := \mathbb{Z}^n$ ordered lexicographically. Now for $f \in \mathbb{R}[\underline{X}], f \neq 0$, we define the 'degree' $\delta(f)$ of f as the largest $k = (k_1, ..., k_n)$ with respect to the lexicographic order, of which the corresponding monomial $\underline{X}^k = X_1^{k_1} \cdots X_n^{k_n}$ has a non-zero coefficient in f. Furthermore, we define the 'leading coefficient' $a(f)$ of f as the coefficient of the monomial $\underline{X}^{\delta(f)}$ in f. Now we pick for H the set that contains $\{0\}$ and all $f \in \mathbb{R}[\underline{X}]$ such that it satisfies one of the following two properties:

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

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

Clearly $g_1, ..., g_n$ satisfy 1) since their 'leading coefficient' is 1 and g_{n+1} satisfies 2), since its leading coefficient is -1. Furthermore, note that (ii) is satisfied since it can be seen that there does not exist an integer k such that $k - \sum_{i=1}^n X_i^2 \in H$, since $a(k - \sum_{i=1}^n X_i^2) < 0$ and $\delta(k - \sum_{i=1}^n X_i^2) \not\equiv (1, ..., 1) \mod 2\Gamma$.

Remark 4.19. Here follow two more notes on Archimedean quadratic modules and their corresponding compact sets.

(1) The set K to which an Archimedean quadratic module $\mathbf{M}(\mathbf{g})$ corresponds is compact. As $\mathbf{M}(\mathbf{g})$ is Archimedean, there exists namely a positive integer N such that $N - \sum_{i=1}^n X_i^2 \in \mathbf{M}(\mathbf{g})$. So this means that $||x||^2 \leq N$ for all $x \in K$, hence K is compact.

(2) If K is compact, it is contained in a ball of radius N for some number $N \in \mathbb{N}$. Hence, we may add the (redundant) inequality $N - \sum_i X_i \geq 0$ to the description of K. Now the corresponding quadratic module is Archimedean. So we see that the Archimedean property does not only depend on K, but also on the inequality description of K.

Here we prove Wörmann's result as stated in Theorem 4.11.

Proof. First note that every preordering is a quadratic module. Therefore Definition 4.15 also applies for preorderings.
($\Rightarrow$). This direction has already been proved in (1) of remark 4.19. For the other direction ($\Leftarrow$), we show that condition (2) of definition 4.15 holds. So we assume that K is compact. Then there exists an integer $k \geq 1$, such that $k - \sum_{i=1}^n X_i^2 > 0$ on K. Now we can apply (1) of Theorem 4.8 to deduce that there exist $p, q \in \mathbf{T}(\mathbf{g})$ such that

$$(k - \sum_{i=1}^{n} X_i^2)p = 1 + q. \tag{4.13}$$

Multiplication by $k - \sum_{i=1}^n X_i^2$ yields that

$$(1 + q)(k - \sum_{i=1}^{n} X_i^2) = p(k - \sum_{i=1}^{n} X_i^2)^2 \in \mathbf{T}(\mathbf{g}).$$

We define a new preordering T' in $\mathbb{R}[\underline{X}]$ corresponding to

$$K' := \{x \in \mathbb{R}^n : g_1(x) \geq 0, ..., g_m(x) \geq 0, k - \sum_{i=1}^{n} x_i^2 \geq 0\}.$$

Now since $k - \sum_{i=1}^{n} X_i^2 \in T'$, we know by (2) of definition 4.15 that T' is Archimedean. So by (3) of Definition 4.15, we know that for each $a \in \mathbb{R}[\underline{X}]$ there exists an integer $m \geq 1$ such that $m + a \in T'$. So we know that for some $t_1, t_2 \in \mathbf{T}(\mathbf{g})$ we can write $m + a = t_1 + (k - \sum_{i=1}^{n} X_i^2)t_2$. Now by using this, we can obtain that

$$(m + a)(1 + q) = t_1(1 + q) + p(k - \sum_{i=1}^{n} X_i^2)^2 t_2 \in \mathbf{T}(\mathbf{g}). \tag{4.14}$$

If we substitute $-q$ for a in the last equation, we can deduce that

$$(m - q)(1 + q) \in \mathbf{T}(\mathbf{g}).$$

So moreover $(\frac{m}{2} - q)^2 + (m - q)(1 + q) \in \mathbf{T}(\mathbf{g})$. We multiply the latter element of $\mathbf{T}(\mathbf{g})$ by k and add $(1 + q)(k - \sum_{i=1}^{n} X_i^2)$ and $q \sum_{i=1}^{n} X_i^2$, both elements of $\mathbf{T}(\mathbf{g})$, to obtain:

$$k \left(\frac{m}{2} + 1\right)^2 - \sum_{i=1}^{n} X_i^2 \in \mathbf{T}(\mathbf{g}). \tag{4.15}$$

After again using (2) of Definition 4.15, we are done. □

Chapter 5

Semi-definite approximation hierarchies

In this chapter we consider semi-definite programming relaxations of Putinar's Positivstellensatz, constructed for the optimization problem described in (5.3) below. By setting different bounds on the sos polynomials in a quadratic module, a hierarchy of semi-definite relaxations is obtained. We discuss under which conditions this hierarchy converges in finitely many steps. Moreover, we consider an alternative semi-definite approximation hierarchy when considering unconstrained optimization.

In this chapter we turn to the following optimization problem:

$$f_{min} = \inf\{f(x) : x \in K\}, \tag{5.1}$$

where

$$K = \{x \in \mathbb{R}^n : g_1(x) \geq 0, ..., g_m(x) \geq 0\} \tag{5.2}$$

and $f, g_1(x), ..., g_m(x) \in \mathbb{R}[\underline{X}]$. Throughout we have set $g_0 = 1$. Recall that by $P(K)$ we denote the set of nonnegative polynomials on K. Often, the problem of (5.1) is reformulated as

$$f_{min} = \sup_{\lambda \in \mathbb{R}}\{\lambda : f - \lambda \in P(K)\}. \tag{5.3}$$

Recall that Putinar's Positivstellensatz claimed that if a polynomial f is positive on the set K and $M(\mathbf{g})$ is Archimedean, then $f \in M(\mathbf{g})$. To use this we define the following parameter:

$$f_{put} = \sup_{\lambda \in \mathbb{R}}\{\lambda : f - \lambda \in M(\mathbf{g})\}. \tag{5.4}$$

Note that $f_{put} \leq f_{min}$ and that equality holds if $M(\mathbf{g})$ is Archimedean. If we want to use semi-definite programming to check whether a polynomial is an element of $M(\mathbf{g})$, we need to set bounds on the degree of the sums of squares in $M(\mathbf{g})$. For this purpose we define the truncated quadratic module:

$$M_{2t}(\mathbf{g}) = \left\{ \sum_{j=0}^{m} g_j s_j : s_j \in \Sigma,\ \deg(s_j g_j) \leq 2t \ \ (j = 0, ..., m) \right\}. \tag{5.5}$$

The corresponding obtained parameter is given by

$$f_{put}^{(t)} = \sup\{\lambda : f - \lambda \in M_{2t}(\mathbf{g})\}. \tag{5.6}$$

Clearly $f_{put}^{(t)} \leq f_{put} \leq f_{min}$ for all $t \in \mathbb{N}$. By increasing the bounds on the sos polynomials in $M(\mathbf{g})$, a hierarchy $f_{put}^{(t)} \leq f_{put}^{(t+1)} \leq f_{put}^{(t+2)} \leq \cdots \leq f_{min}$ is constructed. In general, the hierarchy of semi-definite relaxations of f_{min}, introduced by Lasserre [15], is referred to as *Lasserre's hierarchy*. It should be mentioned that these semi-definite relaxations can also be constructed for the dual formulation of (5.4), in which moment sequences are involved. However, in this thesis we will only consider sos relaxations. Note the following result showing asymptotic convergence of the sos bounds to the infimum of f over K.

Lemma 5.1. Assume that $M(\mathbf{g})$ is Archimedean. Then $f_{put}^{(t)} \to f_{min}$ as $t \to \infty$.

Proof. Let $\epsilon > 0$. Then $f - f_{min} + \epsilon > 0$ on K. Since $M(\mathbf{g})$ is Archimedean, we know by Putinar's Positivstellensatz that $f - f_{min} + \epsilon \in M(\mathbf{g})$. Moreover there exists a $t \in \mathbb{N}$, such that $f - f_{min} + \epsilon \in M_{2t}(\mathbf{g})$. Combining this and the definition of $f_{put}^{(t)}$, we know that $f_{min} - \epsilon \leq f_{put}^{(t)}$. So if $t \to \infty$, this holds for all $\epsilon > 0$. Therefore $f_{put}^{(t)} \to p_{min}$ as $t \to \infty$. $\square$

5.1 Finite convergence

As we have seen in the latter lemma, we have asymptotic convergence for the hierarchy of sos relaxations constructed for f_{min}. It turns out there is finite convergence under certain conditions.

5.1.1 Finite real variety

In this subsection we consider the following optimization problem:

$$f_{min} = \sup_{\lambda \in \mathbb{R}} \{\lambda : f - \lambda \in P(K)\}, \tag{5.7}$$

where $K = \{x \in \mathbb{R}^n : g_1(x) \geq 0, ..., g_{m_1} \geq 0, h_1(x) = ... = h_{m_2}(x) = 0\}$. Here $g_j, h_i, f \in \mathbb{R}[\underline{X}]$ for $j \in \{1, ..., m_1\}$ and $i \in \{1, ..., m_2\}$. Before we formulate Lasserre's hierarchy for this optimization problem, we introduce some notation.

Let $h = (h_1, ..., h_{m_2})$. Then h generates the ideal $h_1\mathbb{R}[\underline{X}] + ... + h_{m_2}\mathbb{R}[\underline{X}]$. Furthermore, for optimization purposes, we define the *truncated ideal* of h as

$$\langle h \rangle_{2k} := \{\sum_{i=1}^{m_2} \phi_i h_i : \phi_i \in \mathbb{R}[\underline{X}], \deg(\phi_i h_i) \leq 2k\}. \tag{5.8}$$

This is called the $2k$-th truncated ideal generated by h. Further we define the real variety of h as

$$V_{\mathbb{R}}(h) = \{x \in \mathbb{R}^n : h_1(x) = 0, ..., h_{m_2}(x) = 0\}. \tag{5.9}$$

Lasserre's hierarchy constructed for the problem in (5.7) is the sequence $(f_k)_{k \geq 1}$ of the following sos relaxations

$$f_k = \max\{\gamma : f - \gamma = \phi + \sigma, \phi \in \langle h \rangle_{2k}, \;\; \sigma \in M_{2k}(g)\}. \tag{5.10}$$

Here k is called the relaxation order. Note that indeed $\phi + \sigma \geq 0$ on K for $\phi \in \langle h \rangle_{2k}$ and $\sigma \in M_{2k}(g)$. Next, we will show that if $V_{\mathbb{R}}(h)$ is finite, then f_k converges to f_{min} in finitely many steps.

Theorem 5.2. [24] Let $f, g_1, ..., g_{m_1}, h_1, ..., h_{m_2} \in \mathbb{R}[\underline{X}]$. Let f_k be the optimal value of the sdp given in (5.10) and f_{min} be the optimal value of (5.7). Then if the real variety $V_{\mathbb{R}}(h)$ is finite, then $f_k = f_{min}$ for a large enough k.

For the proof we use the following lemma.

Lemma 5.3. Let $p, q \in \mathbb{R}[\underline{X}]$. Further let $I \subseteq \mathbb{R}[\underline{X}]$ be an ideal such that $p^{2l} + q \in I$ for an integer $l > 0$. Then

$$s_c(t) := 1 + t + ct^{2l} \tag{5.11}$$

is an sos for all $c \geq c_0 := \frac{1}{2l}(1 - \frac{1}{2l})^{2l-1}$. Furthermore for all $\epsilon > 0$ we have that

$$p + \epsilon - (\epsilon s_c\left(\frac{p}{\epsilon}\right) + c\epsilon^{1-2l} q) = -c\epsilon^{1-2l}(p^{2l} + q) \in I. \tag{5.12}$$

Proof. We will prove that s_c described in Lemma 5.3 is nonnegative over $\mathbb{R}$ when c satisfies the condition described in Lemma 5.3. Then, since s_c is a univariate polynomial, we can use Theorem 2.5 in combination with Lemma 2.3 to see that $s_c(t)$ is an sos. The last statement of the lemma follows by an easy manipulation.
In order to show that s_c is nonnegative, we use the fact that the second derivative of s_c is positive to see that s_c is convex. So since $s_c(t)$ contains a positive point (for $t = 0$ for example), we only need to show that the minimum is nonnegative. Note that $s_c'(t) = 1 + 2lct^{2l-1}$ and that the unique real critical point is $\kappa := (\frac{-1}{2lc})^{\frac{1}{2l-1}}$. So to find the minimum of s_c, we substitute κ in s_c and obtain $s_c(\kappa) = 1 + (\frac{-1}{2lc}^{\frac{1}{2l-1}}(1 - \frac{1}{2l}))$. From this we can deduce that $s_c(\kappa) \geq 0$ if and only if $c \geq c_0$. As explained this implies that s_c is an sos. Further note that:

$$
\begin{aligned}
&p + \epsilon - (\epsilon s_c(p/\epsilon) + c\epsilon^{1-2l}q) \\
&= p + \epsilon - (\epsilon(1 + \frac{p}{\epsilon} + c\left(\frac{p}{\epsilon}\right)^{2l}) + c\epsilon^{1-2l}q) \\
&= p + \epsilon - \epsilon - p - c\epsilon^{1-2l}p^{2l} - c\epsilon^{1-2l}q = -c\epsilon^{1-2l}(p^{2l} + q).
\end{aligned}
$$

Since $p^{2l} + q \in I$ and $-c\epsilon^{1-2l} \in \mathbb{R}[\underline{X}]$, we are done. $\square$

Proof. Here we prove Theorem 5.2. We will make use of the Real Nullstellensatz (Theorem 4.3) and Lemma 5.3.
Since we have assumed that $V_{\mathbb{R}}(h)$ is finite, we can write $V_{\mathbb{R}}(h) = \{u_1, ..., u_N\}$, for $u_1, ..., u_N \in \mathbb{R}^n$. Next, we will consider some interpolation polynomials $\phi_i \in \mathbb{R}[\underline{X}]$ for $i = 1, ..., N$, which attain the following values on the real variety of h:

$$
\phi_i(u_j) = \begin{cases} 0 & \text{if} \quad i \neq j, \\ 1 & \text{if} \quad i = j. \end{cases} \tag{5.13}
$$

Further we define $a_i \in \mathbb{R}[\underline{X}]$ as

$$
a_i = \begin{cases} (f(u_i) - f_{min})\phi_i^2 & \text{if} \quad f(u_i) - f_{min} \geq 0, \\ \frac{(f(u_i) - f_{min})}{g_{j_i}(u_i)} g_{j_i}\phi_i^2 & \text{if} \quad f(u_i) - f_{min} < 0. \end{cases} \tag{5.14}
$$

Note that if $f(u_i) - f_{min} < 0$, then there exists an index $j_i \in \{1, ..., m_1\}$ such that $g_{j_i}(u_i)$ is negative, since f_{min} is the smallest value that f attains on K. So a_i is nonnegative on K.
Now, for N_1 large enough we see that $a_i \in M_{N_1}(\mathbf{g})$, since a_i is either an

element of Σ (for the case $f(u_i) - f_{min} \geq 0$) or a_i is of the form Σg_{j_i} (for the case $f(u_i) - f_{min} < 0$).
Hence we have that $\sigma_1 := a_1 + ... + a_N \in M_{N_1}(\mathbf{g})$. Next, we define

$$\widehat{f} := f - f_{min} - \sigma_1. \tag{5.15}$$

Now note that the Real Nullsellensatz (Theorem 4.3) is applicable to $\hat{f}$ since $\hat{f} = 0$ on $V_{\mathbb{R}}(h)$ (NB. $\sigma_1(u_i) = f(u_i) - f_{min}$), i.e. $\hat{f}$ vanishes on $V_{\mathbb{R}}(h)$. The Real Nullstellensatz implies that there exists an integer $l > 0$ and an sos polynomial $\sigma_2 \in \mathbb{R}[\underline{X}]$ such that $\hat{f}^{2l} + \sigma_2 \in \langle h \rangle$.
Let $c > 0$ be a constant that satisfies the condition in Lemma 5.3, when applied to $p = \hat{f}$, $q = \sigma_2$ and $I = \langle h \rangle$. Further for a constant $\epsilon > 0$ we define

$$\sigma_\epsilon := \epsilon s_c(\hat{f}/\epsilon) + c\epsilon^{1-2l}\sigma_2 + \sigma_1 \tag{5.16}$$

Note that, by Lemma 5.3, we know that $s_c(\hat{f}/\epsilon)$ is an sos. Therefore we see that $\sigma_\epsilon \in M_{N_1}(\mathbf{g})$ for all $\epsilon > 0$. Subsequently we define the following polynomial using Lemma 5.3:

$$\phi_\epsilon := \hat{f} + \epsilon + \sigma_1 - \sigma_\epsilon = -c\epsilon^{1-2l}(\hat{f}^{2l} + \sigma_2) \tag{5.17}$$

Note that $\phi_\epsilon \in \langle h \rangle$ because of Lemma 5.3. This means that there exists an $N_2 > 0$ such that $\phi_\epsilon \in \langle h \rangle_{2N_2}$ for all $\epsilon > 0$. Now note that the following holds:

$$f - (f_{min} - \epsilon) = \phi_\epsilon + \sigma_\epsilon. \tag{5.18}$$

Finally, we define $N_3 := \max\{N_1, N_2\}$. So we see that $\sigma_\epsilon \in M_{2k}(g)$ and $\phi_\epsilon \in \langle h \rangle_{2k}$ for all $k \geq N_3$ and for all $\epsilon > 0$. To conclude, note that

$$f_k = \max_{\phi,\sigma}\{f - \phi - \sigma\} \geq \max\{f - \phi_\epsilon - \sigma_\epsilon\} \geq f_{min} - \epsilon$$

for all $\epsilon > 0$. So $f_k \geq f_{min}$ for $k \geq N_3$, but $f_k \leq f_{min}$ for all k and hence $f_k = f_{min}$ for all $k \geq N_3$. $\square$

5.1.2 Generic finite convergence

In [25], Nie states that the hierarchy of relaxations as described in (5.10) has finite convergence on an Archimedean set K if three optimality conditions on $g = (g_1, ..., g_{m_1})$ and $h = (h_1, ..., h_{m_2})$ from nonlinear programming theory are satisfied for every global minimizer. These conditions are called the

constrained qualification, *strict complementarity* and *second order sufficiency condition*. Nie moreover proves that these optimality conditions hold on a Zariski-open set. This means that Lasserre's hierarchy has finite convergence generically. Below we introduce the above mentioned conditions.
We are still considering the minimization problem from (5.7). Let u be a local minimizer of (5.7). We call the set of active inequality constraints $J(u) = \{1 \leq j \leq m_2 : g_j(u) = 0\}$ and write $J(u) = \{j_1, ..., j_r\}$. We say that the *constraint qualification condition* holds at u if the following condition is satisfied:
if the gradients $\nabla h_1(u), ..., \nabla h_{m_1}(u), \nabla g_{j_1}(u), ..., \nabla g_{j_r}(u)$ are linearly independent, then there exist Lagrange multipliers $\lambda_1, .., \lambda_{m_1}, \mu_1, ..., \mu_{m_2}$ such that the following equalities and inequalities are satisfied:

$$\nabla f(u) = \sum_{i=1}^{m_1} \lambda_i \nabla h_i(u) + \sum_{j=1}^{m_2} \mu_j \nabla g_j(u)$$
$$\mu_1 g_1(u) = \cdots = \mu_{m_2} g_{m_2}(u) = 0$$
$$\mu_1 \geq 0, ..., \mu_{m_2} \geq 0.$$

If we furthermore have that

$$\mu_1 + g_1(u) > 0, ..., \mu_{m_2} + g_2 > 0, \tag{5.19}$$

then the *strict complementarity condition* holds at u.
Corresponding to the Lagrange multipliers we define the Lagrange function:

$$L(x) = f(x) - \sum_{i=1}^{m_1} \lambda_i h_i(x) - \sum_{j \in J(u)} \mu_j g_j(x). \tag{5.20}$$

Further by $G(x)$, we denote the Jacobian of the active constraining polynomials:

$$G(x) = \begin{bmatrix} \nabla h_1(x) & \cdots & \nabla h_{m_1}(x) & \nabla g_{m_1}(x) & \cdots & \nabla g_{j_r}(x) \end{bmatrix}. \tag{5.21}$$

By $G(u)^{\perp}$ we denote the null space of $G(u)$. Now we say that the *second order sufficiency condition* holds at u if

$$v^T \nabla_x^2 L(u) v > 0 \quad \text{for all } 0 \neq v \in G(u)^{\perp}. \tag{5.22}$$

5.2 Unconstrained minimization

Another development focuses on unconstrained minimization. Recall that this problem is formulated as follows: find

$$p_{min} := \min_{x \ \in\mathbb{R}^n} p(x). \tag{5.23}$$

Firstly, we assume that $\deg(p) = 2d$, since $p_{min} = -\infty$ if $\deg(f)$ is odd. Further recall that $p_{put}^{(t)}$ is given as in equation (5.6) by

$$p_{put}^{(t)} = \sup\{\lambda : p - \lambda \in M_{2t}(\mathbf{g})\}. \tag{5.24}$$

Since there are no constraints, we get that

$$p_{put}^{(t)} = p_{put}^{(d)} \leq p_{min} \text{ for all } t \geq d.$$

Moreover $p_{min} = p_{put}^{(t)}$ if and only if $p - p_{min}$ is an sos. So it seems a natural idea to transform the unconstrained problem into a constrained problem. Nie, Demmel and Sturmfels proposed in [26] to make use of the gradient ideal defined as follows:

$$I_p^{grad} = \begin{pmatrix} \frac{\delta p}{\delta x_1} & \cdots & \frac{\delta p}{\delta x_n} \end{pmatrix}. \tag{5.25}$$

Recall that if x is global minimizer of p over $\mathbb{R}^n$, then all derivatives of p vanish at x. Using this, the latter authors proposed to turn the problem of (5.23) into the following problem: find

$$p_{min} = \min_{x\in V_{\mathbb{R}}(I_p^{grad})} p(x). \tag{5.26}$$

Note that we need to assume that p has a minimum. Consider for example $p = X_1^2 + (1 - X_1X_2)^2$. Then $p_{min} = 0$, but $\min_{x\in V_{\mathbb{R}}(I_p^{grad})} p(x) = 1$ since $V_{\mathbb{R}}(I_p^{grad}) = \{0\}$.
So in the obtained constrained case we would like to look at a hierarchy of approximations. However, $V_{\mathbb{R}}(I_p^{grad})$ does not satisfy the Archimedean property so we can not apply Lemma 5.1. Yet, asymptotic convergence holds and sometimes even finite convergence holds. This is proven in [26] and based on the following theorem.

Theorem 5.4. [26] If $p(x) > 0$ for all $x \in V_{\mathbb{R}}(I_p^{grad})$, then p is an sos modulo its gradient ideal I_p^{grad}.

So in an analogous manner as Lasserre's hierarchy was formulated for a minimization problem using Putinar's Positivstellensatz, a hierarchy can be formulated for approximation of p_{min} using Theorem 5.4 by setting bounds on the sos. In [3] it is shown that, if the minimum of a polynomial is attained, there is a hierarchy of relaxation problems which involve the gradient ideal for which there always is finite convergence.

Chapter 6

Sums of squares representations for optimization over the unit hypercube

A basic idea in order to find the errors that are made when considering Putinar type semi-definite relaxations, is to relate the truncated quadratic module $M_n(g)$ and the truncated preordering $T_n(g)$ (defined in (6.2) below), where $g = (g_1, ..., g_n)$ is the set of polynomials describing the unit hypercube. Therefore, in this chapter we will consider the polynomial $X_1 \cdots X_n \in T_n(g)$ and we try to find the smallest constant C_n such that $X_1 \cdots X_n + C_n \in M_n(g)$. This chapter is based on the final remarks of [18].

Let $\mathbf{g} = (g_1, ..., g_m)$ for $g_i \in \mathbb{R}[\underline{X}]$. Further $g_0 = 1$. Recall that the truncated quadratic module is given by:

$$M_{2t}(\mathbf{g}) = \left\{ \sum_{j=0}^{m} g_j s_j : s_j \in \Sigma,\ \deg(s_j g_j) \leq 2t \right\}. \tag{6.1}$$

Similarly, the truncated preordering is given by

$$\mathbf{T}_{2t}(\mathbf{g}) = \left\{ \sum_{J \subseteq \{1,\ldots,m\}} s_J g_J : \deg(s_J g_J) \leq 2t, s_0, s_J \in \Sigma \right\}, \tag{6.2}$$

where $g_J = \prod_{j \in J} g_j$.
In this chapter we consider optimization over the n-dimensional unit cube,

given by

$$UQ = \{x \in \mathbb{R}^n : x_1 - x_1^2 \geq 0, ..., x_n - x_n^2 \geq 0\}. \tag{6.3}$$

Note that as explained in Remark 0.2, optimization over the unit hypercube in general is a hard problem.
Let $M_{2t}(g)$ and $\mathbf{T}_{2t}(g)$ be the truncated quadratic module and truncated preordering corresponding to the unit cube, respectively, where we have set $g = (X_1 - X_1^2, ..., X_n - X_n^2)$. Clearly we have that $M_{2t}(g) \subseteq \mathbf{T}_{2t}(g)$. However the reverse inclusion does not hold, since the monomial $\prod_{i=1}^k X_i$ does not belong to $M(g)$ for $1 < k \leq n$. We prove this in the following lemma:

Lemma 6.1. $\prod_{i=1}^k X_i \notin M(g)$ for $1 < k \leq n$.

Proof. Suppose there exist $\sigma_0, \sigma_1, ..., \sigma_n \in \Sigma$ such that

$$X_1 \cdots X_n = \sigma_0 + \sum_{i=1}^n \sigma_i (X_i - X_i^2). \tag{6.4}$$

Let $low(f)$ denote the smallest degree of all non-zero monomials of a polynomial f. Clearly σ_0 contains no constant term. Therefore $low(\sigma_0) \geq 2$. This implies that $low(\sigma_i) \geq 1$ and thus that $low(\sigma_i) \geq 2$ for all $i \in \{1, ..., n\}$. Subsequently, this implies that $low(\sigma_0) \geq 3$. Since σ_0 is an sos, this means that $low(\sigma_0) \geq 4$, which implies that $low(\sigma_i) \geq 3$, which implies $low(\sigma_i) \geq 4$ and so on until we have that $low(\sigma_0) = n$ or $low(\sigma_i) = n - 2$. Suppose $low(\sigma_0) = n$. This would imply that $\sigma_i = 0$ for $i \in \{1, ..., n\}$, which would mean that $\sigma_0 = X_1 \cdots X_n$ which gives a contradiction. Suppose $low(\sigma_i) = n - 2$. As above explained this means that $low(\sigma_0) = n$, so we are done. $\square$

In this chapter we are interested in finding the smallest real constant C_n for n even such that the following holds:

$$X_1 \cdots X_n + C_n \in M_n(g). \tag{6.5}$$

Already in [18] it is proved that (6.5) holds for $C_n \leq 1$. The argument is that $\prod_{i=1}^n x_i + 1 + \sum_{i=1}^n (x_i^2 - x_i) x_i^{n-2}$ is an sos, as we have explained in example 2.18. So for this case $s_i = x_i^{n-2}$ for $i \in \{1, ..., n\}$ and $\sigma_0 = 0$. In [18] it is moreover conjectured that $C_n = \frac{1}{n(n+2)}$. In Lemma 6.3 below, we give an analytic proof of this conjecture for the case $n = 2$. First note that looking for the smallest real constant C_n such that equation (6.5) is satisfied, is the same as looking for $-f_{put}^{(\frac{n}{2})}$ from equation (5.6) when setting $f = X_1 \cdots X_n$ and setting $M_n(\mathbf{g}) = M_n(g)$:

$f_{put}^{(\frac{n}{2})} = \sup\{\lambda : f - \lambda \in M_n(g)\} = -\inf\{-\lambda : X_1 \cdots X_n + \lambda \in M_n(g)\} = -C_n.$

Since the degrees in $M_n(g)$ are bounded we can compute C_n with a semi-definite program in which $n+1$ PSD matrices corresponding to $\sigma_0, ..., \sigma_n$ are involved. The following result shows that if there is a solution for (6.5) then there also is a symmetric solution. This means that instead of $n+1$, we only have to find two PSD matrices.

Lemma 6.2. Let S_n denote the symmetrical group that acts on the polynomial ring in n variables by permuting the variables. Let $\tau_{1j} \in S_n$ such that $\tau_{1j}(f(X_1, ..., X_n)) = f(X_j, X_2, ..., X_{j-1}, X_1, X_{j+1}, ..., X_n)$ for a polynomial $f \in \mathbb{R}[\underline{X}]$. The claim is the following: if there exist $\sigma_0, ..., \sigma_n$ such that

$$X_1 \cdots X_n + C_n = \sigma_0 + \sum_{i=1}^{n} \sigma_i (X_i - X_i^2) \tag{6.6}$$

holds for some real constant $C_n > 0$, then there exist another solution given by $\sigma'_0, ..., \sigma'_n$ such that $\tau_{1j}(\sigma'_1) = \sigma'_j$ and σ'_0 is invariant under S_n

Proof. Note that

$$p = X_1 \cdots X_n + C_n = \sigma_0 + \sum_{i=1}^{n} \sigma_i (X_i - X_i^2) \tag{6.7}$$

is invariant under S_n. For $\pi \in S_n$ and $f \in \mathbb{R}[\underline{X}]$ we now have:

$$p = \pi p = \pi\sigma_0 + \sum_{i=1}^{n} \pi\sigma_i (X_{\pi(i)} - X_{\pi(i)}^2). \tag{6.8}$$

If we sum over all $\pi \in S_n$ we obtain:

$$n!p = \sum_{\pi} \pi\sigma_0 + \sum_{\pi} \sum_{i=1}^{n} \pi\sigma_i (X_{\pi(i)} - X_{\pi(i)}^2). \tag{6.9}$$

So let us set $\sigma'_0 = \sum_\pi \pi\sigma_0$. Clearly σ'_0 is invariant under S_n. Further we write

$$\begin{aligned} \sum_{\pi} \sum_{i=1}^{n} \pi\sigma_i (X_{\pi(i)} - X_{\pi(i)}^2) &= \sum_{i=1}^{n} \sum_{\pi} (X_{\pi(i)} - X_{\pi(i)}^2)\pi\sigma_i \\ &= \sum_{i} \phi_i (X_i - X_i^2), \end{aligned}$$

where we have set

$$\phi_j = \sum_{i,\pi:\pi(i)=j} \pi\sigma_i \text{ for } j = 1, ..., n. \tag{6.10}$$

Now the claim is that $\phi_j = \tau_{1j}\phi_1$ for $j \in \{1, ..., n\}$. To see this note the following:

$$\begin{aligned}\tau_{1j}\phi_1 &= \sum_{i,\pi:\pi(i)=1} \tau_{1j}\pi\sigma_i \\ &= \sum_{i,\pi':\pi'(i)=j} \pi'\sigma_i \\ &= \phi_j,\end{aligned}$$

where we have set $\pi' = \tau_{1j}\pi$. Here we have used that when $\pi(i) = 1$ we have that $\pi'(i) = \tau_{1j}(1) = j$. □

By this result we are able to prove analytically that $C_2 = \frac{1}{8}$.

Lemma 6.3. $C_2 = \frac{1}{8}$.

Proof. We want to solve C_2 out of the following equation:

$$X_1X_2 + C_2 = \sigma_0 + \sigma_1(X_1 - X_1^2) + \sigma_2(X_2 - X_2^2),$$

where $\sigma_0, \sigma_1, \sigma_2 \in \Sigma$. We use Lemma 2.10 to rewrite the equation as follows:

$$X_1X_2 + C_2 = \begin{pmatrix} 1 \\ X_1 \\ X_2 \end{pmatrix}^T \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix} \begin{pmatrix} 1 \\ X_1 \\ X_2 \end{pmatrix} + \sigma_1(X_1 - X_1^2) + \sigma_2(X_2 - X_2^2),$$

where $\begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix} \succeq 0$ and $a, b, c, d, e, f \in \mathbb{R}$. Further $\deg(\sigma_1), \deg(\sigma_2) = 0$, so σ_1, σ_2 are constants. Since we know from Lemma 6.2 that there is a solution such that σ_1, σ_2 are equal under symmetry, we we can pick $\sigma_1 = \sigma_2$. We equate the coefficients of the monomials in the equation above to get that $a = C_2, 2b = -\sigma_1, 2c = -\sigma_1, d = \sigma_1, 2e = 1$ and $f = \sigma_1$. Now we can obtain:

$$X_1X_2 + C_n = \begin{pmatrix} 1 \\ X_1 \\ X_2 \end{pmatrix}^T \begin{pmatrix} C_2 & -\frac{1}{2}\sigma_1 & -\frac{1}{2}\sigma_1 \\ -\frac{1}{2}\sigma_1 & \sigma_1 & \frac{1}{2} \\ -\frac{1}{2}\sigma_1 & \frac{1}{2} & \sigma_1 \end{pmatrix} \begin{pmatrix} 1 \\ X_1 \\ X_2 \end{pmatrix} + \sigma_1(X_1 - X_1^2) + \sigma_1(X_2 - X_2^2).$$

Since the principal minors of

$$\begin{pmatrix} C_2 & -\frac{1}{2}\sigma_1 & -\frac{1}{2}\sigma_1 \\ -\frac{1}{2}\sigma_1 & \sigma_1 & \frac{1}{2} \\ -\frac{1}{2}\sigma_1 & \frac{1}{2} & \sigma_1 \end{pmatrix}$$

are nonnegative, we get that $\sigma_1 \geq \frac{1}{2}$ and that $C_2 \geq \frac{1}{4}\sigma_1$. So we see that $C_2 \geq \frac{1}{8}$. Now the following identity concludes the proof:

$$X_1X_2 + \frac{1}{8} = \frac{1}{2}\left(X_1 + X_2 - \frac{1}{2}\right)^2 + \frac{1}{2}(X_1 - X_1^2) + \frac{1}{2}(X_2 - X_2^2).$$

□

As already stated in [18], we can compute that $C_4 \leq \frac{1}{24}$ and that $C_6 \leq \frac{1}{48}$ using the programs MATLAB, in which the modelling language of YALMIP is integrated. In the Appendix we give two programs that compute C_4. In one of them we use Lemma 6.2. The program that uses this result is slightly faster than the program that did not do this, as expected.
Further, we also have tried to compute C_8. However, the sizes of the matrices corresponding to the sos polynomials then become 165×165, which is equal to precisely $\binom{8+3}{3}$, as is explained in Remark 2.1. These sizes were to big for a standard computer to deal with. Clearly, also the significance of Lemma 6.2 rapidly reduces as the number of variables grows.
Concluding, we can say that the conjecture that $C_n = \frac{1}{n(n+2)}$ is not proven yet. However, the result we presented in Lemma 6.2 on the symmetry of the solutions of (6.5) is a small step in the right direction for an analytical proof of the conjecture.

Appendix

Computation of an upper bound for C_4

With the following MATLAB programs in which the YALMIP modelling language is integrated, we compute an upper bound for C_4. Recall that this is the smallest value C_4 such that

$$X_1 \cdots X_4 + C_4 \in M_4(g) \tag{6.11}$$

holds, where $g = (g_1, ..., g_4)$ and $g_i = X_i - X_i^2$. The programs below look for the smallest value (in the program called 'lower') C_4, such that it can find sos decompositions for $\sigma_0, \sigma_1, ..., \sigma_4$. For the search of these sos decompositions YALMIP is used. Both programs below obtained $C_4 \leq 0.0417 \approx \frac{1}{24}$. In the following program we have not used the idea of Lemma 6.2.

```
% Here we define the decision variables. By 'lower' we denote C_4.
sdpvar x1 x2 x3 x4 lower;

p4=x1*x2*x3*x4;

g=[x1-x1^2;x2-x2^2; x3-x3^2; x4-x4^2];


% Here we define 4 polynomials in the variables
% x1,...,x4 with degree at most 2.

[s1, c1]=polynomial([x1 x2 x3 x4],2);
```

```
[s2, c2]=polynomial([x1 x2 x3 x4],2);


[s3, c3]=polynomial([x1 x2 x3 x4],2);


[s4, c4]=polynomial([x1 x2 x3 x4],2);


%Here we define the constraints for the function below.

F=[sos(p4+ lower - [s1 s2 s3 s4]*g), sos(s1), sos(s2), sos(s3), sos(s4)];

%We use the function solvesos that has the following form:
%[sol,m,B] = solvesos(Constraints,Objective,options,decisionvariables)

solvesos(F, lower,[],[c1;c2;c3;c4;lower]);
```

Below we show the program that uses Lemma 6.2 to compute an upper bound for C_4.

```
%First we define decision variables.
sdpvar x1 x2 x3 x4 lower;
p4=x1*x2*x3*x4;
g=[x1-x1^2;x2-x2^2; x3-x3^2; x4-x4^2];

% The commands below generate a vector of
% monomials in variables x1,...,x4 up to degree 1.
% The number 1, indicates the maximum degree these monomials.
v1=monolist([x1 x2 x3 x4],1);
v2=monolist([x2 x1 x3 x4],1);
v3=monolist([x3 x2 x1 x4],1);
v4=monolist([x4 x2 x3 x1],1);

% Here we generate a matrix of variables.
H=sdpvar(length(v1));
```

```
% Here use the symmetrical properties of
% the sums of squares s1,...,s4.
s1=v1'*H*v1;
s2=v2'*H*v2;
s3=v3'*H*v3;
s4=v4'*H*v4;

% We have the following constraints:
F=[sos(p4+ lower - [s1 s2 s3 s4]*g), sos(s1)];

% The function below computes 'lower' and computes
% the PSD matrix Q such that s_i=v_i*Q*v_i.
[sol,v,Q]=solvesos(F, lower,[],H);

% In the remaining lines of the program we
% check whether we have found the correct matrix Q.
SS1=v1'*Q{2}*v1;
SS2=v2'*Q{2}*v2;
SS3=v3'*Q{2}*v3;
SS4=v4'*Q{2}*v4;

% The command clean(x,1e-6) checks whether x is in a neighbourhood
% of 1e-6 of 0. So in fact we just substitute our results in the
% equation and check whether it holds.
clean(p4+0.0417-[SS1 SS2 SS3 SS4]*g-v{1}'*Q{1}*v{1},1e-6)
```

Bibliography

[1] C. Berg, P.H. Maserick, *Exponentially bounded positive definite functions*, Illinois Journal of Mathematics 28: 162-179, 1984.

[2] G. Blekherman, *There are Significantly More Nonnegative Polynomials than Sums of Squares*, Israel Journal of Mathematics, Vol. 153, 2006.

[3] M. A. Bucero, B. Mourrain, P. Trebuchet, *Unconstraint global polynomial Optimization via gradient ideal*, preprint, 2013.

[4] M.D. Choi, T.-Y. Lam, *Extremal positive semi-definite forms*, Math. Ann. 231,1-18, 1977.

[5] C. Fidalgo, A. Kovacec, *Positive semidefinite diagonal minus tail forms are sums of squares*, Math. Z.,269 (629-645), 2011.

[6] M.R. Garey, D.S Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, San Francisco, W.H. Freeman & Company, Publishers, 1979.

[7] E.K.Haviland, *On the momentum problem for distributions in more than one dimension*, American Journal of Mathematics, 57: 562-568, 1935.

[8] D. Hilbert, *Über die Darstellung definiter Formen als Summe von Formenquadraten*, Math. Ann. 32, 342-350, 1888.

[9] A. Hurwitz, *Über den Vergleich des arithmetischen und des geometrischen Mittels*, J. Reine Angew. Math.,108 (266-268),1891.

[10] T. Jacobi, A. Prestel, *Distinguished representations of strictly positive polynomials*, J. Reine Angew. Math. 532, 223-235, 2001.

[11] J.-L. Krivine, *Anneaux préordonnés*, J. Analyse Math. 12, 307-326, 1964.

[12] J.B. Lasserre, *A sum of squares approximation of nonnegative polynomials*, SIAM J. Optim. 16, pp 751-765, 2006.

[13] J.B. Lasserre, *Sufficient conditions for a polynomial to be a sum of squares*, Arch. Math. 89, pp. 390–398, 2007.

[14] J.B. Lasserre,T. Netzer, *SOS approximations of nonnegative polynomials via simple high degree perturbations*. Math. Zeitschrift 256, pp. 99–112, 2006.

[15] J.B.Lasserre, *Global optimization with polynomials and the problem of moments*, SIAM J. Optim., 11(3):796-817, 2001.

[16] M. Laurent, *Sums of squares, moment matrices and optimization over polynomials*, In Emerging Applications of Algebraic Geometry, Vol. 149 of IMA Volumes in Mathematics and its Applications, M. Putinar and S. Sullivant (eds.), Springer, pages 157-270, 2010.

[17] M. Laurent, F. Vallentin, lecture notes on semi-definite optimization, Chapters 1,2,3,4,13,14 and 15, 2012.

[18] M. Laurent, E. de Klerk, *Error bounds for some semidefinite programming approaches to polynomial minimization on the hypercube*, SIAM Journal on Optimization, 20(6):3104-3120, 2010.

[19] M. Grötschel, L. Lovász and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*, Springer-Verlag, Berlin, 1988.

[20] M. Marshall, *Positive Polynomials and Sums of Squares*, Mathematical surveys and Monographs, vol. 146, AMS, 2008.

[21] M. Marshall, M. Ghasemi, *Lower bounds for polynomials using geometric programming*, SIAM Journal on Optimization, 22(2):460-473, 2012.

[22] T. Motzkin, *The arithmetic geometric inequalities*, In: Inequalities (O. Shisha, ed.), Proc. Symp. Wright-Patterson AFB,August 19-27, 1965, Academic press, 205-224, 1967.

[23] K.G. Murty and S.N Kabadi, *Some NP-Complete problems in quadratic and non-linear programming*, Mathematical Programming, 39: 117-129, 1987.

[24] J. Nie, *Polynomial optimization with real varieties*, preprint, 2012.

[25] J. Nie, *Optimality conditions and finite convergence of Lasserre's Hierarchy*, preprint, 2012.

[26] J. Nie, J. Demmel and B. Sturmfels, *Minimizing polynomials via sums of squares over the gradient ideal*, Mathematical Programming Series A 106: 587-606, 2006.

[27] P. Parrilo, R. Thomas and G. Blekherman, *Semidefinite Optimization and Convex Algebraic Geometry*, SIAM Optimization Series, vol. 13, 2013.

[28] M. Putinar, *Positive polynomials on compact semi-algebraic sets*, Indiana Univ. Math. J. (3) 43, 969-984, 1993.

[29] B. Reznick, *A quantitative version of Hurwitz's theorem on the arithmetic-geometric inequality*, J. Reine Angew. Math. 377(108-112), 1987.

[30] B. Reznick, *Forms derived from the arithmetic geometric inequality*, Math. An.283 (431-464), 1989.

[31] B. Reznick, *Some concrete aspects of Hilbert's 17th problem*, Seminaire de Structures Algébriques Ordonnées, (F. Delon, M.A. Dickmann, D. Gondard eds), Publ. Équipe de Logique, Univ. Paris VII, 1996.

[32] C. Scheiderer and Albrecht Pfister, *An elementary proof of Hilbert's theorem on ternary quartics*. J. Algebra 371, 1-25, 2012.

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

[34] Y.E. Nesterov and A. Nemirovski, *Interior Point Polynomial Methods in Convex Programming*, Studies in Applied Mathematics, vol. 13, SIAM, Philadelphia, PA, 1994.

[35] T. Wörmann, *Strikt positive Polynome in der semialgebraischen Geometrie*, Dissertation, Univ. Dortmund, 1998.

[36] T. Woŕmann, V. Powers, *An algorithm for sums of squares of real polynomials*, J. Pure and Appl. Alg. 127, 99-104, 1998.