Moment Matrices and Optimization over Polynomials
A Survey on Selected Topics - Work in Progress

Monique Laurent[*][†]

September 5, 2005

Abstract

We consider the problem of minimizing a polynomial over a semialgebraic set defined by polynomial equations and inequalities, which is NP-hard in general. Hierarchies of semidefinite relaxations have been proposed, in particular, by Lasserre and by Parrilo, based on positive semidefinite moment matrices and the dual theory of sums of squares of polynomials. We present these hierachies of approximations and their main properties: asymptotic/finite convergence, optimality certificate, and extraction of global optimum solutions. We review the mathematical tools underlying these properties, in particular, some results about moment matrices of Curto and Fialkow, and the algebraic eigenvalue method for solving zero-dimensional systems of polynomial equations. We try whenever possible to provide detailed proofs and background.

1 Introduction

We consider the problem:

$$p_{\min} := \inf \ p(x) \ \text{ subject to } h_1(x) \geq 0, \ldots, h_m(x) \geq 0 \tag{1}$$

of minimizing a polynomial $p(x)$ over a semialgebraic set

$$K := \{x \in \mathbb{R}^n \mid h_1(x) \geq 0, \ldots, h_m(x) \geq 0\},$$

where $p, h_1, \ldots, h_m \in \mathbb{R}[x_1, \ldots, x_n]$. This is a hard, in general, nonconvex optimization problem. A first instance is the *unconstrained minimization problem*:

$$p_{\min} = \inf_{x \in \mathbb{R}^n} \ p(x), \tag{2}$$

when $K = \mathbb{R}^n$. This contains the problem of testing whether a matrix is copositive. Indeed, an $n \times n$ symmetric matrix M is said to be *copositive* if $x^T M x \geq 0$ for all

[*]CWI, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands
[†]Supported by the Netherlands Organisation for Scientific Research grant NWO 639.032.203.

$x \in \mathbb{R}^n_+$; equivalently, M is copositive if and only if $p_{\min} = 0$ in (2) for the polynomial $p(x) := \sum_{i,j=1}^n x_i^2 x_j^2 M_{ij}$. The *partition problem* can also be cast as an unconstrained polynomial minimization problem. A sequence $a_1, \ldots, a_n$ of positive integers can be partitioned if $x^T a = 0$ for some $x \in \{\pm 1\}^n$. Equivalently, the sequence can be partitioned if $p_{\min} = 0$ in (2) for the polynomial $p(x) := (a^T x)^2 + \sum_{i=1}^n (x_i^2 - 1)^2$. Recall that checking matrix copositivity is a co-NP-complete problem [29] and that the partition problem is NP-complete [14]. Thus unconstrained polynomial minimization is NP-hard, already when the polynomial p has degree 4 (while it is polynomial time solvable when p has degree 2).

The problem (1) also contains 0/1 linear programming, which can be formulated as

$$\min\ c^T x \ \text{ s.t. } Ax \leq b,\ x_i^2 = x_i\ \forall i = 1, \ldots, n$$

where $c \in \mathbb{R}^n$, $b \in \mathbb{R}^m$, A is an $m \times n$ matrix. For instance, the problem of computing the stability number $\alpha(G)$ (i.e., the largest cardinality of a stable set) of a graph $G = (V, E)$ can be formulated as

$$\alpha(G) = \max \sum_{i \in V} x_i \ \text{ s.t. } x_i + x_i \leq 1\ (ij \in E),\ x_i^2 = x_i\ (i \in V).$$

Alternatively, using the theorem of Motzkin-Straus [28], the stability number can be formulated as

$$\frac{1}{\alpha(G)} = \min\ x^T (I + A_G) x \ \text{ s.t. } \sum_{i \in V} x_i = 1,\ x_i \geq 0\ (i \in V).$$

(Here, A_G is the adjacency matrix of G, i.e., the 0/1 symmetric matrix indexed by V whose ij-th entry is 1 precisely for $ij \in E$.) As computing $\alpha(G)$ is an NP-hard problem (see e.g., [14]), we see that (1) is NP-hard already in the following two instances: linear constraints and quadratic objective function, linear objective function and quadratic constraints (while it is polynomial time solvable in the linear case, when the objective function and the constraints are all linear).

Several authors, in particular, Lasserre [21], Nesterov [30], Parrilo [31, 32], Shor [45], have proposed to approximate the problem (1) by a hierarchy of convex (in fact, semidefinite) relaxations. Such relaxations can be constructed using representations of nonnegative polynomials as sums of squares of polynomials and the dual theory of moments. The paradigm underlying this approach is that, while testing whether a polynomial is nonnegative is a hard problem, testing whether a polynomial is a sum of squares of polynomials can be formulated as a semidefinite problem. Now, efficient algorithms exist for solving semidefinite programs (to any arbitrary precision) (see, e.g., the handbook [47]).

Before indicating how sums of squares can be recognized via semidefinite programs, we recall some basic notation about polynomials. $\mathbb{R}[x_1, \ldots, x_n]$ denotes the set of polynomials in n variables. For $\alpha \in \mathbb{Z}^n_+$, x^α denotes the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$; its degree is $|\alpha| := \sum_{i=1}^n \alpha_i$. Write a polynomial $f(x) \in \mathbb{R}[x_1, \ldots, x_n]$ as $f(x) = \sum_{\alpha \in \mathbb{Z}^n_+} f_\alpha x^\alpha$, where there are only finitely many nonzero f_α's. The degree of f is the largest integer k for which there exists α with $|\alpha| = k$ and $f_\alpha \neq 0$. Set $S_k := \{\alpha \in \mathbb{Z}_+^n \mid |\alpha| = \sum_{i=1}^n \alpha_i \leq k\}$. Throughout the paper, we often identify a polynomial $f(x)$ with its sequence of coefficients $f = (f_\alpha)_\alpha$. Thus, f can be seen as a vector of $\mathbb{R}^{S_k}$ if $\deg f \leq k$, as $f_\alpha = 0$ whenever $|\alpha| \geq k+1$.

Lemma 1 *[36]* **(Recognizing sums of squares of polynomials)**
Consider a polynomial $p(x) = \sum_{\alpha||\alpha|\leq 2d} p_\alpha x^\alpha$ of degree $\leq 2d$. The following assertions are equivalent.

(i) *$p(x)$ can be written as a sum of squares of polynomials, i.e., $p(x) = \sum_j (u_j(x))^2$ for some polynomials $u_j \in \mathbb{R}[x_1, \ldots, x_n]$.*

(ii) *The following semidefinite program is feasible:*

$$\begin{cases} X \succeq 0 \\ \displaystyle\sum_{\substack{\beta,\gamma||\beta|,|\gamma|\leq d \\ \beta+\gamma=\alpha}} X_{\beta,\gamma} = p_\alpha \quad (|\alpha| \leq 2d). \end{cases} \tag{3}$$

Proof. Let $z := (x^\alpha \mid |\alpha| \leq d)$ denote the vector containing all monomials of degree at most d. Then, $\sum_j (u_j(x))^2 = z^T(\sum_j u_j u_j^T)z$. Therefore, $p(x)$ is a sum of squares of polynomials if and only if $p(x) = z^T X z$ for some positive semidefinite matrix X. Equating the coefficients of the two polynomials $p(x)$ and $z^T X z$, we find the system (3). ∎

The system (3) is a system in the matrix variable X, which is indexed by S_d and thus has size $\binom{n+d}{d}$, and with $\binom{n+2d}{2d}$ equations. Therefore, this system has polynomial size if either n is fixed, or d is fixed. We will come back to positive polynomials and sums of squares in the next section.

Our objective in this paper is to survey the method proposed for approximating (1) by constructing hierarchies of semidefinite relaxations based on sums of squares of polynomials and the dual theory of moments, following mainly the exposition of Lasserre [21]. The hierarchies of bounds which are obtained for problem (1) enjoy several properties. In particular, under some assumptions, there is convergence to the optimum of (1), one can formulate conditions ensuring that the relaxed problem solves the original problem (1) at optimality, and one can then extract global optimum solutions. These properties rely on some algebraic results about positive polynomials, and about moment matrices, that we will present in detail. Whenever possible we try to give full proofs.

Contents of the paper. We introduce in Sections 2.1 and 2.2 the necessary background on moment matrices and the moment problem, and we introduce in Section 2.3 the hierarchies of relaxations for the optimization problem (1). Section 3 contains algebraic preliminaries about polynomial ideals, varieties, and the eigenvalue method for solving systems of polynomial equations. In Section 4, we group several results about moment matrices, essentially due to Curto and Fialkow, that have important application to polynomial optimization. In Section 5, we return to the optimization problem (1) and explain how the previous results about moment matrices apply. Finally the Appendix contains the proof of a result of Curto and Fialkow about flat extensions of truncated moment matrices, which is a bit technical.

2 Moment Sequences, Moment Matrices and Optimization

2.1 Moment sequences and moment matrices

We group here some basic definitions and notation about moment sequences and moment matrices.

For a real symmetric matrix M, the notation $M \succeq 0$ means that M is positive semidefinite, i.e., $M = VV^T$ for some $n \times r$ matrix V. When M is an infinite matrix, the notation $M \succeq 0$ means that every finite principal submatrix of M is positive semidefinite.

Definition 2 *Given a nonnegative (Borel) measure μ on $\mathbb{R}^n$, the quantity $y_\alpha := \int x^\alpha \mu(dx)$ is called its* moment of order α. *Then, the sequence $(y_\alpha)_{\alpha\in\mathbb{Z}_+^n}$ is called the sequence of moments of the measure μ and, given an integer $t \geq 1$, the (truncated) sequence $(y_\alpha)_{\alpha\in S_t}$ is called the sequence of moments of μ up to order t. We also say that μ is a* representing measure *for y.*

A basic problem in the theory of moments concerns the characterization of (infinite or truncated) moment sequences, i.e., the characterization of those sequences $y = (y_\alpha)_\alpha$ that are the sequences of moments of some nonnegative measure. Given a subset $K \subseteq \mathbb{R}^n$, the *K-moment problem* asks for the characterization of those sequences that are sequences of moments of some nonnegative measure supported by the set K. This problem has received considerable attention in the litterature, especially in the case when $K = \mathbb{R}^n$ (the basic moment problem) or when K is a compact semialgebraic set.

The following notions of moment matrix and shift operator play a central role in the moment problem.

Definition 3 **(i)** *Given a sequence $y = (y_\alpha)_{\alpha\in\mathbb{Z}_+^n}$, its* moment matrix *is the (infinite) matrix $M(y)$ indexed by $\mathbb{Z}_+^n$, with (α,β)-th entry $y_{\alpha+\beta}$, for $\alpha,\beta \in \mathbb{Z}_+^n$.*

(ii) *Given an integer $t \geq 1$ and a (truncated) sequence $y = (y_\alpha)_{\alpha\in S_{2t}}$, its* moment matrix of order t *is the matrix $M_t(y)$ indexed by S_t, with (α,β)-th entry $y_{\alpha+\beta}$, for $\alpha,\beta \in S_t$.*

(iii) *Given $h, y \in \mathbb{R}^{\mathbb{Z}_+^n}$ with h having a finite support (i.e., h is the vector of coefficients of a polynomial), define $h * y := M(y)h$, called* shifted vector, *whose α-th entry is $(h * y)_\alpha := \sum_\beta h_\beta y_{\alpha+\beta}$ for $\alpha \in \mathbb{Z}_+^n$. The notation $h * y$ will also be used for denoting the truncated vector $((h*y)_\alpha)_{\alpha\in S_t}$ of $\mathbb{R}^{S_t}$ for an integer $t \geq 1$. The moment matrices of $h * y$ are also known as the* localizing matrices.

As moment matrices are indexed by $\mathbb{Z}_+^n$, as well as polynomials in $\mathbb{R}[x_1, \ldots, x_n]$, the quantity $f^T M(y) g$ is well defined for polynomials $f, g \in \mathbb{R}[x_1, \ldots, x_n]$; namely, $f^T M(y) g = \sum_{\alpha,\beta \in \mathbb{Z}_+^n} f_\alpha g_\beta y_{\alpha+\beta}$ if $f(x) = \sum_\alpha f_\alpha x^\alpha$, $g(x) = \sum_\beta g_\beta x^\beta$. The following simple calculus about moment matrices will be repeatedly used in the paper.

Lemma 4 *Given polynomials $f, g, h \in \mathbb{R}[x_1, \ldots, x_n]$, we have:*

$$f^T M(y)(gh) = y^T(fgh) = f^T M(h * y) g.$$

Here, gh stands for the vector of coefficients of the polynomial $g(x)h(x)$; similarly, fgh stands for the vector of coefficients of the polynomial $f(x)g(x)h(x)$. In particular,

$$f^T M(y)(gh) = (fg)^T M(y) h, \;\; f^T M(y) f = y^T(f^2), \;\; 1^T M(y) f = y^T f,$$

where 1 *stands for the constant polynomial equal to 1.*

Proof. As $g(x)h(x) = \sum_\beta x^\beta (\sum_{\gamma,\delta | \beta = \gamma+\delta} g_\gamma h_\delta)$, the β-th coefficient of gh is $(gh)_\beta = \sum_{\gamma,\delta|\gamma+\delta=\beta} g_\gamma h_\delta$. Hence,

$$f^T M(y)(gh) = \sum_{\alpha,\beta} f_\alpha (gh)_\beta y_{\alpha+\beta} = \sum_{\alpha,\gamma,\delta|\gamma+\delta=\beta} f_\alpha g_\gamma h_\delta y_{\alpha+\beta} = \sum_{\alpha,\gamma,\delta} f_\alpha g_\beta h_\delta y_{\alpha+\gamma+\delta} = y^T(fgh)$$

since the β-th coefficient of $f(x)g(x)h(x)$ is equal to $\sum_{\alpha,\gamma,\delta|\alpha+\gamma+\delta=\beta} f_\alpha g_\gamma h_\delta$. The identity $f^T M(h * y) g = (fh)^T M(y) g$ follows analogously. ∎

Given $x \in \mathbb{R}^n$, δ_x denotes the *Dirac measure* at x, having mass 1 at x and mass 0 elsewhere. Hence, the sequence of moments of the Dirac measure δ_x is the vector $\zeta_x := (x^\alpha)_{\alpha \in \mathbb{Z}_+^n}$, called the *Zeta vector* of x. Given an integer $t \geq 1$, $\zeta_{t,x} := (x^\alpha)_{\alpha \in S_t}$ denotes the *truncated Zeta vector*.

The results of Curto and Fialkow which we will discuss in the paper deal essentially with moment sequences of finite atomic measures, i.e., measures having a finite support. We now give a precise definition.

Definition 5 *Given a measure μ on $\mathbb{R}^n$, its* support *$supp(\mu)$ is the smallest closed set $S \subseteq \mathbb{R}^n$ for which $\mu(\mathbb{R}^n \setminus S) = 0$. When the support of μ is finite, say, $supp(\mu) = \{x_1, \ldots, x_r\}$, then μ is of the form $\mu = \sum_{i=1}^r \lambda_i \delta_{x_i}$ for some $\lambda_1, \ldots, \lambda_r \neq 0$; the x_i's are called the* atoms *of μ and one also says that μ is r-*atomic.

The next lemma gives some easy well known necessary conditions for moment sequences.

Lemma 6 **(i)** *If $y \in \mathbb{R}^{S_{2t}}$ is the sequence of moments (up to order $2t$) of a nonnegative measure μ, then $M_t(y) \succeq 0$. Moreover, if $p(x)$ is a polynomial of degree $\leq t$ such that $M_t(y)p = 0$, then the support of μ is contained in the set of zeros of $p(x)$. If μ is r-atomic, then* rank $M_t(y) \leq r$.

(ii) *Let $h(x)$ be a polynomial of degree $2d$ or $2d-1$ ($d \geq 1$) and $K := \{x \mid h(x) \geq 0\}$. If $y \in \mathbb{R}^{S_{2t}}$ is the sequence of moments of a nonnegative measure μ supported by K, then $M_{t-d}(h * y) \succeq 0$.*

(iii) *If $y \in \mathbb{R}^{\mathbb{Z}_+^n}$ is the sequence of moments of a nonnegative measure μ, then $M(y) \succeq 0$. Moreover, if μ is r-atomic, then* rank *$M(y) \leq r$.*

PROOF. (i) Let $p(x)$ be a polynomial of degree $\leq t$ and $p \in \mathbb{R}^{S_t}$ its vector of coefficients. Then,

$$p^T M_t(y) p = \sum_{\alpha,\beta \in S_t} p_\alpha p_\beta y_{\alpha+\beta} = \sum_{\alpha,\beta \in S_t} p_\alpha p_\beta \int x^{\alpha+\beta} \mu(dx) = \int p(x)^2 \mu(dx) \geq 0,$$

showing that $M_t(y) \succeq 0$. If $M_t(y)p = 0$, then $0 = p^T M_t(y) p = \int p(x)^2 \mu(dx)$. As μ is nonnegative, this implies that the support of μ is contained in the set Z of zeros of $p(x)$. [As Z is a closed set, $supp(\mu) \subseteq Z$ holds if we can show that $\mu(\mathbb{R}^n \setminus Z) = 0$. Indeed, $\mathbb{R}^n \setminus Z = \cup_{k \geq 0} U_k$, setting $U_k := \{x \in \mathbb{R}^n \mid p(x)^2 \geq \frac{1}{k}\}$ for positive $k \in \mathbb{Z}$. As $0 = \int p(x)^2 \mu(dx) = \int_{\mathbb{R}^n \setminus Z} p(x)^2 \mu(dx) \geq \int_{U_k} p(x)^2 \mu(dx) \geq \frac{1}{k} \mu(U_k)$, this implies $\mu(U_k) = 0$ for all k and thus $\mu(\mathbb{R}^n \setminus Z) = 0$.]

Assume that μ is r-atomic, say, $\mu = \sum_{i=1}^r \lambda_i \delta_{x_i}$ where $\lambda_1, \ldots, \lambda_r > 0$ and $x_1, \ldots, x_r \in \mathbb{R}^n$. Then, $M_t(y) = \sum_{i=1}^r \lambda_i \zeta_{t,x_i} (\zeta_{t,x_i})^T$, which shows that rank $M_t(y) \leq r$.
(ii) Let $p(x)$ be a polynomial of degree $\leq t-d$ and $p \in \mathbb{R}^{S_{t-d}}$ its vector of coefficients. Then,

$$\begin{aligned} p^T M_{t-d}(h * y) p &= \sum_{\alpha,\beta \in S_{t-d}} p_\alpha p_\beta (h * y)_{\alpha+\beta} = \sum_{\alpha,\beta \in S_{t-d}} p_\alpha p_\beta \sum_{\gamma \in S_{2d}} h_\gamma y_{\alpha+\beta+\gamma} \\ &= \sum_{\alpha,\beta \in S_{t-d},\ \gamma \in S_{2t-2d}} p_\alpha p_\beta h_\gamma \int x^{\alpha+\beta+\gamma} \mu(dx) = \int_K h(x) p(x)^2 \mu(dx) \geq 0, \end{aligned}$$

which shows that $M_{t-d}(h * y) \succeq 0$. (iii) follows directly from (i). ∎

Corollary 7 *Let $y \in \mathbb{R}^{S_{2t}}$ be the sequence of moments (up to order $2t$) of a nonnegative measure supported by the set*

$$K := \{x \in \mathbb{R}^n \mid h_1(m) \geq 0, \ldots, h_m(x) \geq 0\}, \tag{4}$$

where each $h_j(x)$ is a polynomial with degree $2d_j$ or $2d_j - 1$. Then,

$$M_t(y) \succeq 0, \quad M_{t-d_j}(h_j * y) \succeq 0 \ (j = 1, \ldots, m). \tag{5}$$

Curto and Fialkow have proven a sequence of results which show that, under certain restrictions on the rank of the matrix $M_t(y)$, the implication from Corollary 7 holds as an equivalence; that is, the condition (5) is sufficient for ensuring that y is the sequence of moments of a nonnegative measure supported by K. We summarize these results in Section 4 below. Before that we recall some other classic theorems about the moment problem.

2.2 The Moment Problem

2.2.1 The basic moment problem

The moment problem is concerned with the characterization of the sequences $y \in \mathbb{R}^{\mathbb{Z}_+^n}$ that are the sequences of moments of a probability measure μ. The analogous problem can be posed for truncated sequences $y \in \mathbb{R}^{S_t}$ ($t \geq 1$ integer). As we saw above, necessary conditions can be formulated in terms of the positive semidefiniteness of certain associated moment matrices. It may give more insight to reformulate the results in terms of conic duality of certain associated cones.

Let $\mathcal{M}$ denote the set of sequences $y \in \mathbb{R}^{\mathbb{Z}_+^n}$ that admit a representing measure and set

$$\mathcal{M}_+ := \{y \in \mathbb{R}^{\mathbb{Z}_+^n} \mid M(y) \succeq 0\}.$$

Then, $\mathcal{M}$ and $\mathcal{M}_+$ are convex cones lying in the vector space $\mathbb{R}^{\mathbb{Z}_+^n}$ (equipped with the topology of pointwise convergence). A linear functional $L : \mathbb{R}^{\mathbb{Z}_+^n} \to \mathbb{R}$ is of the form $L(y) = \sum_\alpha p_\alpha y_\alpha$ (for $y \in \mathbb{R}^{\mathbb{Z}_+^n}$) for some sequence $p = (p_\alpha)_{\alpha \in \mathbb{Z}_+^n}$ having a finite support. Therefore, the dual space of $\mathbb{R}^{\mathbb{Z}_+^n}$ can be identified with the vector space $\mathbb{R}[x_1, \ldots, x_n]$ of polynomials. We now indicate the dual cones of the cones $\mathcal{M}$ and $\mathcal{M}_+$. Recall that, for a cone $C \subseteq \mathbb{R}^{\mathbb{Z}_+^n}$, its *dual cone* is the set C^* consisting af all $p \in \mathbb{R}^{\mathbb{Z}_+^n}$ having a finite support and satisfying $p^T y \geq 0$ for all $y \in C$. Define the cone

$$\mathcal{P} := \{p \in \mathbb{R}[x_1, \ldots, x_n] \mid p(x) \geq 0 \ \forall x \in \mathbb{R}^n\}$$

consisting of the polynomials that are nonnegative over $\mathbb{R}^n$, and the cone

$$\Sigma := \{p \in \mathbb{R}[x_1, \ldots, x_n] \mid p = \sum_{\ell=1}^{L} p_\ell^2 \ \text{ for some } p_1, \ldots, p_L \in \mathbb{R}[x_1, \ldots, x_n]\}$$

consisting of the polynomials that can be written as a sum of squares of polynomials.

Proposition 8 *The cones $\mathcal{M}$ and $\mathcal{P}$ (resp., $\mathcal{M}_+$ and Σ) are dual of each other. That is, $\mathcal{P} = \mathcal{M}^*$, $\mathcal{M}_+ = \Sigma^*$, $\mathcal{M} = \mathcal{P}^*$, $\Sigma = (\mathcal{M}_+)^*$.*

PROOF. The first two equalities are easy. Indeed, if $p \in \mathcal{P}$ and $y \in \mathcal{M}$, then $p^T y = \sum_\alpha p_\alpha y_\alpha = \int p(x)\mu(dx) \geq 0$, which shows the inclusions $\mathcal{P} \subseteq \mathcal{M}^*$ and $\mathcal{M} \subseteq \mathcal{P}^*$. The inclusion $\mathcal{M}^* \subseteq \mathcal{P}$ follows from the fact that, if $p \in \mathcal{M}^*$ then, for any $x \in \mathbb{R}^n$, $p(x) = p^T \zeta_x \geq 0$ (since $\zeta_x \in \mathcal{M}$) and thus $p \in \mathcal{P}$. If $y \in \mathcal{M}_+$ and $p \in \mathbb{R}[x_1, \ldots, x_n]$, then $y^T(p^2) = p^T M(y) p$ (by Lemma 4) is nonnegative, which shows the inclusions $\mathcal{M}_+ \subseteq \Sigma^*$ and $\Sigma \subseteq (\mathcal{M}_+)^*$. The inclusion $\Sigma^* \subseteq \mathcal{M}_+$ follows reversing the argument. The remaining two inclusions $\mathcal{P}^* \subseteq \mathcal{M}$ and $(\mathcal{M}_+)^* \subseteq \Sigma$ are proved, respectively, by Haviland [15] and by Berg, Christensen and Jensen [3]. ∎

Obviously,

$$\mathcal{M} \subseteq \mathcal{M}_+ \ \text{ and } \ \Sigma \subseteq \mathcal{P}.$$

As is well known, the inclusion $\Sigma \subseteq \mathcal{P}$ holds at equality when $n = 1$ and it is strict for $n \geq 2$. For instance, the Motzkin polynomial $p(x_1, x_2) := x_1^2 x_2^2(x_1^2 + x_2^2 - 3) + 1$ belongs to $\mathcal{P} \setminus \Sigma$ (see [3]). [Indeed, $p(x_1, x_2) \geq 0$ if $x_1^2 + x_2^2 \geq 3$. Otherwise, set $x_3^2 = 3 - x_1^2 - x_2^2$. By the arithmetic geometric mean inequality, we have $\frac{x_1^2+x_2^2+x_3^2}{3} \geq \sqrt[3]{x_1^2 x_2^2 x_3^2}$, giving again $p(x_1, x_2) \geq 0$. One can verify directly that p cannot be written as a sum of squares of polynomials.]

The celebrated theorem of Hilbert [1888] characterizes the pairs (n, d) for which every degree d polynomial in n variables which is nonnegative on $\mathbb{R}^n$ can be written as a sum of squares of polynomials. Namely, this happens precisely when $n = 1$, or $d = 2$, or $(n, d) = (3, 4)$. See, e.g., Reznick [40] for a detailed exposition. As a consequence, equality $\mathcal{M} = \mathcal{M}_+$ holds when $n = 1$ (this is Hamburger's theorem) and the inclusion $\mathcal{M} \subseteq \mathcal{M}_+$ is strict when $n \geq 2$.

There are however some classes of sequences y for which the implication:

$$y \in \mathcal{M}_+ \Longrightarrow y \in \mathcal{M} \tag{6}$$

holds. Curto and Fialkow [10] show that this is the case when the matrix $M(y)$ has finite rank.

Theorem 9 *[10] If $M(y) \succeq 0$ and $M(y)$ has finite rank r, then y has a (unique) r-atomic representing measure.*

We will come back to this result in Theorem 22 below. This result plays in fact a crucial role in the application to polynomial optimization, since it permits to give an optimality certificate for the semidefinite hierarchy based on moment matrices; see Section 5 for details.

Berg, Christensen, and Ressel [4] show that the implication (6) also holds when the sequence y is bounded, i.e., when there is a constant C for which $|y_\alpha| \leq C$ for all $\alpha \in \mathbb{Z}_+^n$. More generally, Berg and Maserick [5] show that (6) holds when y is exponentially bounded. We need a definition. An *absolute value* on $\mathbb{Z}_+^n$ is a function $\sigma : \mathbb{Z}_+^n \to \mathbb{R}_+$ satisfying $\sigma(0) = 1$ and $\sigma(\alpha + \beta) \leq \sigma(\alpha)\sigma(\beta)$ for all $\alpha, \beta \in \mathbb{Z}_+^n$. A sequence $y \in \mathbb{R}^{S_{2t}}$ is said to be *bounded w.r.t.* σ if $|y_\alpha| \leq C\sigma(\alpha)$ for all $\alpha \in \mathbb{Z}_+^n$, for some constant C, and y is *exponentially bounded* if it is bounded w.r.t. some absolute value. Observe that if y has a representing measure μ supported by a compact set K then y is exponentially bounded. Indeed, the function σ_K defined by $\sigma_K(\alpha) := \sup_{x \in K} |x^\alpha|$ is an absolute value and y is bounded w.r.t. σ_K, since $|y_\alpha| \leq \int_K |x^\alpha| \mu(dx) \leq \sigma_K(\alpha)\mu(K)$. Berg and Maserick [5] show that the sequences having a representing measure with a compact support are precisely those that are exponentially bounded with a positive semidefinite moment matrix.

Theorem 10 *[5] Given $y \in \mathbb{R}^{\mathbb{Z}_+^n}$, y has a representing measure with a compact support if and only if y is exponentially bounded and $M(y) \succeq 0$.*

The proof uses the following fact.

Lemma 11 *Assume $M(y) \succeq 0$. If y is bounded w.r.t. an absolute value σ, then $|y_\alpha| \le y_0\sigma(\alpha)$ $\forall \alpha \in \mathbb{Z}_+^n$.*

Proof. Assume $|y_\alpha| \le C\sigma(\alpha)$ $\forall \alpha$ for some constant C. If $y_0 = 0$ then y is identically zero. Assume $y_0 > 0$; w.l.o.g., $y_0 = 1$ (else rescale y). As $M(y) \succeq 0$, we have $y_\alpha^2 \le y_{2\alpha}$ for all α. Then, $|y_\alpha| \le (y_{2^k\alpha})^{1/2^k}$ for any integer $k \ge 1$ (easy induction) and thus $|y_\alpha| \le (C\sigma(2^k\alpha))^{1/2^k} \le C^{1/2^k}\sigma(\alpha)$. Letting k go to ∞, we find that $|y_\alpha| \le \sigma(\alpha)$. ∎

Lemma 12 *Given an absolute value σ on $\mathbb{Z}_+^n$, set $K_\sigma := \prod_{i=1}^n [-\sigma(e_i), \sigma(e_i)]$, where $e_1, \ldots, e_n$ are the standard unit vectors in $\mathbb{R}^n$, and $S_\sigma := \{y \in \mathbb{R}^{\mathbb{Z}_+^n} \mid y_0 = 1,\ M(y) \succeq 0,\ |y_\alpha| \le \sigma(\alpha)\ \forall \alpha \in \mathbb{Z}_+^n\}$. Then, S_σ is a convex set whose extreme points are of the form ζ_x for $x \in K_\sigma$.*

Proof. Let y be an extreme point of S_σ. Fix $\alpha_0 \in \mathbb{Z}_+^n$. For $\epsilon = \pm 1$, define $z^{(\epsilon)} \in \mathbb{R}^{\mathbb{Z}_+^n}$ by $z_\alpha^{(\epsilon)} := \sigma(\alpha_0)y_\alpha + \epsilon y_{\alpha+\alpha_0}$ for $\alpha \in \mathbb{Z}_+^n$. We first show that $M(z^{(\epsilon)}) \succeq 0$. For this, given $p \in \mathbb{R}[x_1, \ldots, x_n]$, we have to show that

$$p^T M(z^{(\epsilon)})p = \sum_{\gamma,\gamma'} p_\gamma p_{\gamma'} z_{\gamma+\gamma'}^{(\epsilon)} \ge 0. \tag{7}$$

We proceed as follows. Define the sequence $x := (p^2){*}y \in \mathbb{R}^{\mathbb{Z}_+^n}$ with $x_\alpha = \sum_{\gamma,\gamma'} p_\gamma p_{\gamma'} y_{\alpha+\gamma+\gamma'}$ for $\alpha \in \mathbb{Z}_+^n$. Then, $|x_\alpha| \le (\sum_{\gamma,\gamma'} |p_\gamma p_{\gamma'}|\sigma(\gamma)\sigma(\gamma'))\sigma(\alpha)$, which shows that x is bounded w.r.t. σ. Moreover, $M(x) \succeq 0$. Indeed, for $q \in \mathbb{R}[x_1, \ldots, x_n]$, by Lemma 4, $q^T M(x)q = (pq)^T M(y)(pq) \ge 0$. Hence, by Lemma 11, $-x_0\sigma(\alpha) \le x_\alpha \le x_0\sigma(\alpha)$ which, for $\alpha = \alpha_0$, gives relation (7). As $M(z^{(\epsilon)}) \succeq 0$ and $z^{(\epsilon)}$ is bounded w.r.t. σ, we deduce from Lemma 11 that $|z_\alpha^{(\epsilon)}| \le \sigma(\alpha)z_0^{(\epsilon)}$ for all α. If $z_0^{(\epsilon)} = 0$ for some $\epsilon = \pm 1$, then $z^{(\epsilon)} = 0$, implying $y_{\alpha+\alpha_0} = y_\alpha y_{\alpha_0}$ for all α. Assume now $z_0^{(\epsilon)} > 0$ for $\epsilon = \pm 1$. Then, $\frac{z^{(\epsilon)}}{z_0^{(\epsilon)}}$ belongs to S_σ and $y = \frac{z_0^{(1)}}{2\sigma(\alpha_0)} \frac{z^{(1)}}{z_0^{(1)}} + \frac{z_0^{(-1)}}{2\sigma(\alpha_0)} \frac{z^{(-1)}}{z_0^{(-1)}}$ is a convex combination of two points of S_σ. As y is an extreme point, $y = \frac{z^{(\epsilon)}}{z_0^{(\epsilon)}}$ for $\epsilon = \pm 1$ which implies again $y_{\alpha+\alpha_0} = y_\alpha y_{\alpha_0}$ for all α. Setting $x_i := y_{e_i}$ $(i = 1, \ldots, n)$, we find that $y = \zeta_x$ with $x \in K_\sigma$. ∎

Proof of theorem 10. Assume $M(y) \succeq 0$ and y is bounded w.r.t. an absolute value σ. If $y_0 = 0$ then $y = 0$. Assume $y_0 = 1$ (else rescale y). Then y belongs to the convex set S_σ introduced in Lemma 12. By the Krein-Milman theorem, y is a convex combination of extreme points of S_σ. Hence, y has a representing measure μ whose support is contained in K_σ and thus is compact. ∎

2.2.2 The K-moment problem

Let us now turn to the K-moment problem, where

$$K = \{x \in \mathbb{R}^n \mid h_1(x) \geq 0, \ldots, h_m(x) \geq 0\}$$

is a semialgebraic set, with $h_1, \ldots, h_m \in \mathbb{R}[x_1, \ldots, x_n]$. Let $\mathcal{M}(K)$ denote the set of sequences $y \in \mathbb{R}^{\mathbb{Z}_+^n}$ having a representing measure supported by the set K. Define

$$\mathcal{M}_+^{sch}(h_1, \ldots, h_m) := \{y \in \mathbb{R}^{\mathbb{Z}_+^n} \mid M(h_I * y) \succeq 0 \ \forall I \subseteq \{1, \ldots, m\}\}, \tag{8}$$

setting $h_I := \prod_{i \in I} h_i$ for $I \subseteq \{1, \ldots, m\}$, $h_\emptyset = 1$, and

$$\mathcal{M}_+^{put}(h_1, \ldots, h_m) := \{y \in \mathbb{R}^{\mathbb{Z}_+^n} \mid M(y) \succeq 0,\ M(h_i * y) \succeq 0 \ \forall i = 1, \ldots, m\}. \tag{9}$$

(The indices ‘sch’ and ‘put’ refer respectively to Schmüdgen and to Putinar; see Theorems 13 and 14 below.) Define also the cone

$$\mathcal{P}(K) := \{p \in \mathbb{R}[x_1, \ldots, x_n] \mid p(x) \geq 0 \ \forall x \in K\}$$

of polynomials nonnegative on the set K, the cone

$$T(h_1, \ldots, h_m) := \{\sum_{I \subseteq \{1, \ldots, m\}} u_I h_I \mid u_I \in \Sigma\},$$

known as the *preordering* generated by $h_1, \ldots, h_m$, and the cone

$$M(h_1, \ldots, h_m) := \{u_0 + \sum_{j=1}^{m} u_j h_j \mid u_0, u_j \in \Sigma\}$$

known as the *quadratic module* generated by $h_1, \ldots, h_m$. (See, e.g., [37].) Obviously,

$$\mathcal{M}(K) \subseteq \mathcal{M}_+^{sch}(h_1, \ldots, h_m) \subseteq \mathcal{M}_+^{put}(h_1, \ldots, h_m),$$

$$M(h_1, \ldots, h_m) \subseteq T(h_1, \ldots, h_m) \subseteq \mathcal{P}(K).$$

It is easy to verify that

$$\mathcal{P}(K) = (\mathcal{M}(K))^*,\ \mathcal{M}_+^{sch}(h_1, \ldots, h_m) = (T(h_1, \ldots, h_m))^*,$$

$$\mathcal{M}_+^{put}(h_1, \ldots, h_m) = (M(h_1, \ldots, h_m))^*.$$

Moreover, $\mathcal{M}(K) = (\mathcal{P}(K))^*$ (Haviland [15]) and Schmüdgen [41] shows:

Theorem 13 *[41] If K is compact, then $\mathcal{M}(K) = \mathcal{M}_+^{sch}(h_1, \ldots, h_m)$. Moreover, every polynomial p which is positive on K [i.e., $p(x) > 0$ for all $x \in K$] belongs to $T(h_1, \ldots, h_m)$.*

Putinar [38] proves a refinement of Schmüdgen's result, which holds when the polynomials $h_1, \ldots, h_m$ defining K satisfy the following additional condition:

$$\exists p \in M(h_1, \ldots, h_m) \text{ for which the set } \{x \in \mathbb{R}^n \mid p(x) \geq 0\} \text{ is compact.} \tag{10}$$

This condition admits several equivalent reformulations; for instance, it is equivalent to the condition:

$$\exists N \in \mathbb{Z}_+ \text{ for which } N - \sum_{i=1}^{n} x_i^2 \in M(h_1, \ldots, h_m)$$

or to the condition:

$$\forall p \in \mathbb{R}[x_1, \ldots, x_n] \ \exists N \in \mathbb{Z}_+ \ \text{ for which } N \pm p \in M(h_1, \ldots, h_m).$$

See Schweighofer [43] for a detailed discussion. Note that (10) implies that K is compact (since $K \subseteq \{x \mid p(x) \geq 0\}$ for $p \in M(h_1, \ldots, h_m)$). Note also that (10) makes an assumption on the description of K, rather than on the set K itself. (10) holds, e.g., if the set $\{x \in \mathbb{R}^n \mid h_j(x) \geq 0\}$ is compact for one of the constraints defining K. It also holds, e.g., in the 0/1 case, when the constraints $x_i^2 - x_i = 0$ $(i = 1, \ldots, n)$ are present in the description of K. If an explicit ball of radius R is known containing K, one may add the (redundant) constraint $R^2 - \sum_{i=1}^n x_i^2 \geq 0$ to obtain a presentation of K satisfying (10).

Theorem 14 *[38] If (10) holds, then $\mathcal{M}(K) = \mathcal{M}_+^{put}(h_1, \ldots, h_m)$. Moreover, every positive polynomial on K belongs to $M(h_1, \ldots, h_m)$.*

Let us conclude this section with a few words about the proof technique used for proving the above mentioned results from Theorems 9, 13, 14. Consider $y \in \mathbb{R}^{\mathbb{Z}_+^n}$ satisfying $M(y) \succeq 0$. Let $L_y : \mathbb{R}[x_1, \ldots, x_n] \longrightarrow \mathbb{R}$ denote the corresponding linear operator defined by $L(p) = p^T y = \sum_{\alpha \in \mathbb{Z}_+^n} p_\alpha y_\alpha$ for $p \in \mathbb{R}[x_1, \ldots, x_n]$. The assumption: $M(y) \succeq 0$ means that L_y is nonnegative on the cone Σ.

The kernel $I := \{p \in \mathbb{R}[x_1, \ldots, x_n] \mid M(y)p = 0\}$ of $M(y)$ can be seen as an ideal in $\mathbb{R}[x_1, \ldots, x_n]$ (see Lemma 23) and the quotient space $A := \mathbb{R}[x_1, \ldots, x_n]/I$ has the structure of an algebra. One can define an inner product on A by setting $\langle p, q \rangle := p^T M(y) q = 1^T M(y)(pq) = L_y(pq)$ (see Lemma 4). In this way, A is a Hilbert space. For $i = 1, \ldots, n$, consider the multiplication operator $m_{x_i} : A \longrightarrow A$ defined by $m_{x_i}(p) = x_i p \mod I$. Obviously, the operators $m_{x_1}, \ldots, m_{x_n}$ pairwise commute. (See also Section 3.2.)

Under the assumption of Theorem 9, $M(y)$ has a finite rank and thus the Hilbert space A has finite dimension. Curto and Fialkow [10] use the spectral theorem and the Riesz representation theorem for proving the existence of a representing measure for y.

Consider now the case when the assumptions of Schmüdgen's theorem hold; that is, the operator L_y is nonnegative on the cone $T(h_1, \ldots, h_m)$. As K is compact, there exists $\rho > 0$ for which the polynomial $\rho^2 - \sum_{i=1}^n x_i^2$ is positive on K. Using the Positivstellensatz, this implies that $(\rho^2 - \sum_{i=1}^n x_i^2)g = 1 + h$ for some $g, h \in T(h_1, \ldots, h_m)$. Then, the main step in Schmüdgen's proof consist of showing that the operators m_{x_i} are bounded; namely,

$\langle x_i p, x_i p\rangle \leq \rho^2 \langle p, p\rangle$ for all $p \in \mathbb{R}[x_1, \ldots, x_n]$. Then the existence of a representing measure μ for y follows using the spectral theorem and Schmüdgen uses Weierstrass theorem for proving that the support of μ is contained in K.

Thus these proofs use in an essential way functional analytic methods. Schweighofer [42] gives an alternative more elementary proof for (the second part of) Schmüdgen's theorem, which uses only the Positivstellensatz and a theorem of Polya concerning the representation of positive homogeneous polynomials on the nonnegative orthant. (An elementary proof of this result of Polya can be found in Powers and Reznick [35]). Moreover, starting from a certificate: $(\rho^2 - \sum_{i=1}^n x_i^2)g = 1 + h$ with $g, h \in T(h_1, \ldots, h_m)$ given by the Positivstellensatz, Schweighofer constructs explicitely a representation of a positive polynomial on K proving its membership in $T(h_1, \ldots, h_m)$. Schweighofer [43] also gives an alternative elementary proof for Putinar's theorem relying on Polya's theorem.

We will give in Section 4.1 an alternative elementary proof (taken from Laurent [26]) for the result by Curto and Fialkow from Theorem 9. Our proof is based on the observation that the kernel of $M(y)$ is a radical ideal and it uses an algebraic fact (the Nullstellensatz) instead of functional analytic tools.

2.3 Optimization over polynomials

We consider again the problem (1). We sketch here the method proposed by Lasserre [21] for approximating problem (1). A basic observation underlying Lasserre's construction is the fact that

$$p_{\min} := \inf_{x \in K} p(x) = \inf_{\mu} \int p(x)\mu(dx)$$

where the second infimum is taken over all probability measures μ on $\mathbb{R}^n$ supported by the set K (i.e., μ is a nonnegative measure with $supp(\mu) \subseteq K$ and total mass $\mu(K) = 1$). Note that $\int p(x)\mu(dx) = \sum_\alpha p_\alpha \int x^\alpha \mu(dx) = p^T y$, where y is the sequence of moments of μ. Therefore, $p_{\min}$ can be reformulated as

$$p_{\min} = \inf\ p^T y \ \text{ s.t. } y \in \mathcal{M}(K),\ y_0 = 1, \tag{11}$$

where $\mathcal{M}(K)$ is the set of sequences $y \in \mathbb{R}^{\mathbb{Z}_+^n}$ having a representing measure which is a probability measure supported by K, introduced in Section 2.2.2. Relaxing the condition $y \in \mathcal{M}(K)$ by the weaker condition $y \in \mathcal{M}_+(K)$ (recall (9)), we obtain the following lower bound for $p_{\min}$:

$$p^* := \inf\ p^T y \ \text{ s.t. } y_0 = 1,\ M(y) \succeq 0,\ M(h_j * y) \succeq 0\ (j = 1, \ldots, m). \tag{12}$$

One can alternatively formulate $p_{\min}$ as

$$p_{\min} := \inf_{x \in K} p(x) = \sup\ \rho \ \text{ s.t. } p(x) - \rho \geq 0\ \forall x \in K.$$

That is,

$$p_{\min} = \sup\ \rho \ \text{ s.t. } p(x) - \rho \in \mathcal{P}(K). \tag{13}$$

Using the conic duality between the cones $\mathcal{M}(K)$ and $\mathcal{P}(K)$, one finds that the programs (11) and (13) are conic dual programs. Replacing the condition $p - \rho \in \mathcal{P}(K)$ by the stronger condition $p - \rho \in M(h_1, \ldots, h_m)$, we find the following lower bound for $p_{\min}$:

$$\rho^* := \sup \ \rho \ \text{ s.t. } p(x) - \rho \in M(h_1, \ldots, h_m). \tag{14}$$

We have

$$\rho^* \le p^* \le p_{\min}. \tag{15}$$

Indeed, $(p-\rho)^T y = p^T y - \rho \ge 0$ for $p \in M(h_1, \ldots, h_m)$ and $y \in \mathcal{M}_+(K)$ with $y_0 = 1$, since $\mathcal{M}_+(K) = (M(h_1, \ldots, h_m))^*$.

Although the programs (12) and (14) involve semidefinite conditions, they cannot be directly computed. Indeed, (12) involves infinite matrices, while (14) involves sums of squares of polynomials with no a priori bound on their degrees. In order to obtain computable lower bounds for $p_{\min}$, we truncate the programs (12) and (14). Namely, we consider truncated moment matrices in (12), which leads to the following hierarchy of lower bounds for $p_{\min}$:

$$p_t^* := \inf \ p^T y \ \text{ subject to } y_0 = 1, \ M_t(y) \succeq 0, \ M_{t-d_j}(y) \succeq 0 \ (h = 1, \ldots, m), \tag{16}$$

and we impose degree bounds in (14), which leads to the following hierarchy of lower bounds for $p_{\min}$:

$$\begin{array}{rll} \rho_t^* := & \max & \rho \\ & \text{s.t.} & p(x) - \rho = u_0(x) + \sum_{j=1}^m u_j(x) h_j(x) \\ & & \text{where } u_0, u_1, \ldots, u_m \text{ are sums of squares of polynomials} \\ & & \text{with } \deg(u_0), deg(u_1 h_1), \ldots, \deg(u_m h_m) \le 2t, \end{array} \tag{17}$$

for any $t \ge \max(d_0, d_1, \ldots, d_m)$. Here, we set

$$d_0 := \lceil \deg(p)/2 \rceil, \ d_j := \lceil \deg(h_j)/2 \rceil (j = 1, \ldots, m), \ d := \max(d_1, \ldots, d_m). \tag{18}$$

Obviously, $p^* = \sup_t p_t^*$ and $\rho^* = \sup_t \rho_t^*$. Now the programs (16) and (17) are well defined semidefinite programs involving matrices of size $\binom{n+2t}{2t} = O(n^{2t})$ and $O(n^{2t})$ variables. Hence, for any *fixed* t, p_t^* and ρ_t^* can be computed in polynomial time (to any precision). Moreover, one can verify that (16) and (17) are dual semidefinite programs, which implies

$$\rho_t^* \le p_t^*.$$

This inequality can also be seen directly using the 'calculus' from Lemma 4. Let y be feasible for (16) and ρ be feasible for (17); that is, $p - \rho = u_0 + \sum_j u_j h_j$ where u_0, u_j are sums of squares and $\deg(u_0), \deg(u_j h_j) \le 2t$. Then, $p^T y - \rho = (p-\rho)^T y = y^T u_0 + \sum_j y^T(u_j h_j) \ge 0$. Indeed, letting $u_0 = \sum_\ell a_\ell^2$, $u_j = \sum_\ell a_{j,\ell}^2$, from Lemma 4 we have $y^T u_0 = \sum_\ell y^T(a_\ell^2) = \sum_\ell a_\ell^T M_t(y) a_\ell \ge 0$, and $y^T(u_j h_j) = \sum_\ell a_{j,\ell}^T M_{t-d_j}(h_j * y) a_{j,\ell} \ge 0$.

(Lemma 4 is formulated for infinite moment matrices but it also applies to truncated matrices as long as there is compatibility between the degrees of the polynomials and the sizes of the moment matrices involved, which is the case here.)

For t large enough, there is no duality gap between (16) and (17), i.e., $\rho_t^* = p_t^*$, if K has a nonempty interior (Lasserre [21], see also Schweighofer [43]).

The semidefinite programs (16) and (17) can therefore be used for approximating the minimum value of a polynomial over a semialgebraic set. They produce hierarchies of bounds p_t^* and ρ_t^* which enjoy the following properties:

(i) For any *fixed* t, ρ_t^* and p_t^* can be efficiently computed (to an arbitrary precision).

(ii) Under certain conditions on the set K, there is **asymptotic** (sometimes even **finite**) **convergence** of the bounds p_t^*, ρ_t^* to $p_{\min}$.

(iii) **Optimality certificate:** If the optimum solution $M_t(y)$ to program (16) satisfies a certain rank condition, then $p_t^* = p_{\min}$.

(iv) Moreover, under this rank condition, one can **extract global minimizers** for the problem (1), i.e., one can construct points $x \in K$ for which $p_{\min} = p(x)$.

The complexity result (i) was just noted above. The asymptotic convergence to $p_{\min}$ in (ii) can be derived from representation theorems for positive polynomials, like Putinar's theorem.

Theorem 15 *[21] If the semialgebraic set K satisfies Putinar's assumption (10), then the programs (1), (11) and (13) have the same optimum values; that is, $\rho^* = p^* = p_{\min}$. In other words, $\lim_{t\to\infty} \rho_t^* = \lim_{t\to\infty} p_t^* = p_{\min}$.*

PROOF. Given $\epsilon > 0$, the polynomial $p(x) - p_{\min} + \epsilon$ is positive on K. By Theorem 14, it belongs to $\Sigma_{put}(K)$ and thus the scalar $p_{\min} - \epsilon$ is feasible for the program (17) for some t. Therefore, there exists t for which $\rho_t^* \geq p_{\min} - \epsilon$. Letting ϵ go to 0, we find that $\rho^* = \lim_{t\to\infty} \rho_t^* \geq p_{\min}$, implying $\rho^* = p^* = p_{\min}$. ∎

Note that if we would have a representation result valid for *nonnegative* (instead of *positive*) polynomials, this would immediately imply the *finite convergence* of the bounds ρ_t^*, p_t^* to $p_{\min}$. For instance, Theorem 19 in Section 3.1 gives such a reprentation result in the case when the description of K involves a set of polynomial equations generating a zero-dimensional radical ideal. We will treat in detail in Section 5 the convergence properties of the bounds p_t^* and ρ_t^* and the conditions permitting to give an optimality certificate and to extract global minimizers.

Two software packages have been developped for the optimization of polynomials over semialgebraic sets. The first one is *GlotiPoly*, developped by Henrion and Lasserre (see [16]), which relies on the program (16) involving moment matrices. The second one is

SOSTOOLS, developped by Prajna et al. (see [34]), and relies on sums of squares of polynomials. Both packages use SeDuMi, a software developped by Jos Sturm for solving semidefinite programs using interior-point algorithms.

3 Algebraic Preliminaries

3.1 Polynomial ideals and varieties

We group here some preliminaries on polynomial ideals and varieties. For more information, see, e.g., [1], [8], [9], [46].

Let I be an ideal in $\mathbb{R}[x_1,\ldots,x_n]$; that is, $I \subseteq \mathbb{R}[x_1,\ldots,x_n]$ is closed under addition and satisfies: $fg \in I$ whenever $f \in I$ and $g \in \mathbb{R}[x_1,\ldots,x_n]$. Given polynomials $h_1,\ldots,h_m$, $\langle h_1,\ldots,h_m\rangle := \{\sum_{j=1}^m u_j h_j \mid u_1,\ldots,u_m \in \mathbb{R}[x_1,\ldots,x_n]\}$ denotes the *ideal generated by* $h_1,\ldots,h_m$. By the finite basis theorem, any ideal in $\mathbb{R}[x_1,\ldots,x_n]$ admits a finite set of generators. The set

$$V(I) := \{x \in \mathbb{C}^n \mid f(x) = 0 \ \forall f \in I\}$$

is called the (complex) variety associated to I. Thus, if I is generated by $h_1,\ldots,h_m$, then $V(I)$ is the set of common complex zeros of $h_1,\ldots,h_m$. Observe that $V(I)$ is closed under complex conjugation, i.e., $\overline{v} \in V(I)$ for all $v \in V(I)$, since I consists of polynomials with real coefficients. Throughout, $\overline{z}$ denotes the complex conjugate of $z \in \mathbb{C}$. When $V(I)$ is finite, the ideal I is said to be *zero-dimensional.*

Given $V \subseteq \mathbb{C}^n$, the following sets

$$I(V) := \{f \in \mathbb{R}[x_1,\ldots,x_n] \mid f(x) = 0 \ \forall v \in V\},$$

$$\sqrt{I} := \{f \in \mathbb{R}[x_1,\ldots,x_n] \mid f^k \in I \text{ for some integer } k \geq 1\}$$

are again ideals in $\mathbb{R}[x_1,\ldots,x_n]$, which obviously contain the ideal I when $V = V(I)$.

Theorem 16 (Hilbert's Nullstellensatz) $\sqrt{I} = I(V(I))$.

The ideal I is said to be *radical* when $I = \sqrt{I}$. Therefore,

$$I \text{ is radical} \iff \begin{array}{l}\text{the only polynomials vanishing at all points of } V(I)\\ \text{are the polynomials in } I.\end{array} \tag{19}$$

Roughly speaking, the ideal I is radical if all points of $V(I)$ have single multiplicity. For instance, the ideal $I := \langle x^2\rangle$ is not radical since $V(I) = \{0\}$ and $x \in I(V(I)) \setminus I$. The following result relates the cardinality of $V(I)$ and the dimension of the quotient vector space $\mathbb{R}[x_1,\ldots,x_n]/I$.

Theorem 17 *The ideal I is zero-dimensional (i.e., $|V(I)| < \infty$) if and only if the vector space $\mathbb{R}[x_1,\ldots,x_n]/I$ is finite dimensional. Moreover, $|V(I)| \leq \dim\ \mathbb{R}[x_1,\ldots,x_n]/I$, with equality if and only if the ideal I is radical.*

We give the proof of Theorem 17 at the end of this section. One of the ingredients in the proof is the following result about interpolation polynomials, which we will need at several occasions in the paper.

Lemma 18 *Let $V \subseteq \mathbb{C}^n$ with $|V| < \infty$. There exist polynomials $p_v \in \mathbb{C}[x_1, \ldots, x_n]$ (for $v \in V$) satisfying $p_v(v) = 1$ and $p_v(u) = 0$ for all $u \in V \setminus \{v\}$; we call them* interpolation polynomials at the points of V. *Moreover, if V is closed under complex conjugation, then we may assume that $p_{\overline{v}} = \overline{p_v}$ for all $v \in V$.*

PROOF. Fix $v \in V$. For $u \in V$, $u \neq v$, pick an index $i_u \in \{1, \ldots, n\}$ for which $u_{i_u} \neq v_{i_u}$ and define the polynomial $p_v(x) := \prod_{u \in V \setminus \{v\}} \frac{x_{i_u} - u_{i_u}}{v_{i_u} - u_{i_u}}$. Then the polynomials p_v $(v \in V)$ satisfy the lemma. If $\overline{V} = V$, then we can choose the interpolation polynomials in such a way that $p_{\overline{v}} = \overline{p_v}$ for all $v \in V$. Indeed, for $v \in V \cap \mathbb{R}^n$, simply replace p_v by its real part and, for $v \in V \setminus \mathbb{R}^n$, pick p_v as before and choose $p_{\overline{v}} := \overline{p_v}$. ∎

We also need a few basic definitions about monomial orderings and Groebner bases. A *monomial ordering* '$<$' is a total ordering of the set of monomials x^α $(\alpha \in \mathbb{Z}^n_+)$ which is a well-ordering and satisfies the condition: $x^\alpha < x^\beta \Longrightarrow x^{\alpha+\gamma} < x^{\beta+\gamma}$. Examples of monomial ordering are the *lexicographic order* '$<_{lex}$', where $x^\alpha <_{lex} x^\beta$ if $\alpha < \beta$ for a lexicographic order on $\mathbb{Z}^n_+$, or the *graded lexicographic order* '$<_{grlex}$', where $x^\alpha <_{grlex} x^\beta$ if $|\alpha| < |\beta|$, or $|\alpha| = |\beta|$ and $x^\alpha <_{lex} x^\beta$.

Fix a monomial ordering on $\mathbb{R}[x_1, \ldots, x_n]$. For a nonzero polynomial $f(x) = \sum_\alpha f_\alpha x^\alpha$, its *terms* are the quantities $f_\alpha x^\alpha$ with $f_\alpha \neq 0$ and its *leading term* $\mathrm{LT}(f)$ is defined as $f_\alpha x^\alpha$, where x^α is the maximum (with respect to the given ordering) monomial for which $f_\alpha \neq 0$. Let I be an ideal in $\mathbb{R}[x_1, \ldots, x_n]$. A finite subset $G \subseteq I$ is called a *Groebner basis* of I if the leading term of every nonzero polynomial in I is divisible by the leading term of some polynomial in G. It is known that a Groebner basis always exists. A monomial x^α is called a *standard monomial* if it not divisible by the leading term of any polynomial in I or, equivalently, if x^α is not divisible by the leading term of any poynomial in a Groebner basis. Let $\mathcal{S}$ denote the set of standard monomials and $\mathcal{B}$ the set of their exponents; that is, $\mathcal{S} = \{x^\beta \mid \beta \in \mathcal{B}\}$.

Once a monomial ordering is fixed, one can apply the division algorithm. Let $h_1, \ldots, h_m$ and f be nonzero polynomials. If one divides f by the polynomials $h_1, \ldots, h_m$, one obtains polynomials $u_1, \ldots, u_m$ and r satisfying $f = \sum_{j=1}^m u_j h_j + r$, no term of r is divisible by $\mathrm{LT}(h_j)$ $(j = 1, \ldots, m)$ if $r \neq 0$, and $\deg(f) \geq \deg(u_j h_j)$ if $u_j \neq 0$. Hence, when the polynomials $h_1, \ldots, h_m$ form a Groebner basis of the ideal I, the remainder r is uniquely determined and it is a linear combination of the set of standard monomials; that is, $r(x) = \sum_{x^\beta \in \mathcal{B}} r_\beta x^\beta$ with $r_\beta \in \mathbb{R}$. Moreover, $f \in I$ if and only if $r = 0$. This shows that $\mathbb{R}[x_1, \ldots, x_n]/I$ and $\mathbb{R}^{|\mathcal{B}|}$ are isomorphic vector spaces and thus

$$\dim \mathbb{R}[x_1, \ldots, x_n]/I = |\mathcal{B}| = \# \text{ standard monomials.} \tag{20}$$

Hence, if I is zero-dimensional, the set $\mathcal{S}$ of standard monomials (w.r.t. some monomial ordering) is a basis of $\mathbb{R}[x_1,\ldots,x_n]/I$. Therefore, for any polynomial $f \in \mathbb{R}[x_1,\ldots,x_n]$, there exists a unique $\lambda^{(f)} \in \mathbb{R}^{|\mathcal{B}|}$ for which the polynomial $f - \sum_{\beta\in\mathcal{B}} \lambda_\beta^{(f)} x^\beta$ belongs to I; $\sum_{\beta\in\mathcal{B}} \lambda_\beta^{(f)} x^\beta$ is called the *residue* of f modulo I w.r.t. the standard monomial basis. In particular, there exist interpolation polynomials p_v ($v \in V(I)$) where each p_v is a linear combination of standard monomials (replacing if necessary each p_v by its residue modulo $\mathcal{S}$).

Consider, for instance, the ideal $I := \langle x_i^2 - x_i \mid i = 1,\ldots,n\rangle$. Its variety is $V(I) = \{0,1\}^n$, its set of standard monomials is $\mathcal{S} := \{\prod_{i\in I} x_i \mid I \subseteq \{1,\ldots,n\}\}$, and thus I is a radical zero-dimensional ideal.

We can now prove Theorem 17.

Proof of Theorem 17. Assume $k := \dim \mathbb{R}[x_1,\ldots,x_n]/I < \infty$. Then, the set $\{1, x_1, \ldots, x_1^k\}$ is linearly dependent in $\mathbb{R}[x_1,\ldots,x_n]/I$. Thus there exist scalars $\lambda_0,\ldots,\lambda_k$ (not all zero) for which the polynomial $f(x) := \sum_{h=0}^k \lambda_h x_1^h$ belongs to I. Thus, for $v \in V(I)$, $f(v) = 0$, which implies that v_1 takes only finitely many values. Applying the same reasoning to the other coordinates, we deduce that $V(I)$ is finite.

Assume now $|V(I)| < \infty$. Say, $\{v_1 \mid v \in V(I)\} = \{a_1,\ldots,a_k\}$. Then the polynomial $f(x) := \prod_{h=1}^k (x_1 - a_h)$ belongs to $I(V(I))$. By Theorem 16, $f \in \sqrt{I}$, i.e., $f^m \in I$ for some integer m. As the leading term of f^m, equal to $LT(f^m) = x_1^{km}$, does not divide any standard monomial, it follows that $\beta_1 < km$ for any standard monomial x^β. Applying the same reasoning to the other coordinates, we deduce that the set of standard monomials is finite. In view of (20), this shows that $\dim \mathbb{R}[x_1,\ldots,x_n]/I < \infty$.

Assume $V(I)$ is finite. Partition $V(I)$ into $S \cup T \cup \overline{T}$, where $S := V(I) \cap \mathbb{R}^n$ and $T \cup \overline{T} = V(I) \setminus \mathbb{R}^n$. Let p_v ($v \in V(I)$) be interpolation polynomials at the points of $V(I)$; by Lemma 18, we may assume that $p_v \in \mathbb{R}[x_1,\ldots,x_n]$ for $v \in S$, $p_v = q_v + ih_v$, $p_{\overline{v}} = q_v - ih_v$ for $v \in T$, where $q_v, h_v \in \mathbb{R}[x_1,\ldots,x_n]$ (and i is the complex root of -1). One can easily verify that $\mathcal{A} := \{p_v \mid v \in S\} \cup \{q_v,\ h_v \mid v \in T\}$ is linearly independent in $\mathbb{R}[x_1,\ldots,x_n]/I$, i.e., if the polynomial $\sum_{v\in S} a_v p_v + \sum_{v\in T} b_v q_v + c_v h_v$ (where $a_v, b_v, c_v \in \mathbb{R}$) belongs to I then all scalars a_v, b_v, c_v are equal to 0. This shows that $\dim \mathbb{R}[x_1,\ldots,x_n]/I \geq |V(I)|$. Moreover, if I is radical, then the set $\mathcal{A}$ is a basis of $\mathbb{R}[x_1,\ldots,x_n]/I$. Indeed, for any $f \in \mathbb{R}[x_1,\ldots,x_n]$, the polynomial $f(x) - \sum_{v\in V(I)} f(v) p_v$ belongs to I, since it vanishes at all $v \in V(I)$ (applying (19)). Therefore, $\dim \mathbb{R}[x_1,\ldots,x_n]/I = |V(I)|$ if I is radical. Finally, if I is not radical, there exists a polynomial $f \in I(V(I)) \setminus I$ and it is easy to verify that the set $\mathcal{A} \cup \{f\}$ is linearly independent in $\mathbb{R}[x_1,\ldots,x_n]/I$. ∎

The algebraic tools just introduced here also permit to show the following result of Parrilo [33] giving a sum of squares decomposition for every polynomial nonnegative on a finite variety assuming radicality of the associated ideal.

Theorem 19 *[33] Consider the semialgebraic set*

$$K := \{x \in \mathbb{R}^n \mid h_1(x) = 0, \ldots, h_m(x) = 0, h_{m+1}(x) \geq 0, \ldots, h_{m+k}(x) \geq 0\}, \tag{21}$$

where $h_1, \ldots, h_{m+k} \in \mathbb{R}[x_1, \ldots, x_n]$ and $k \geq 0$. Assume that the ideal $I := \langle h_1, \ldots, h_m \rangle$ is zero-dimensional and radical. Then every nonnegative polynomial on K belongs to $\Sigma_{put}(K)$, i.e., is of the form $u_0 + \sum_{j=1}^{m+k} u_j h_j$ where $u_j \in \mathbb{R}[x_1, \ldots, x_n]$ and $u_0, u_{m+1}, \ldots, u_{m+k}$ are sums of squares.

PROOF. Partition $V = V(I)$ into $S \cup T \cup \bar{T}$, where $S = V \cap \mathbb{R}^n$, $T \cup \bar{T} = V \setminus \mathbb{R}^n$. Suppose first that f is a real polynomial nonnegative on the set S. For $v \in S \cup T$, let $\gamma_v = \sqrt{f(v)}$ (thus, $\gamma_v \in \mathbb{R}_+$ if $v \in S$) and define the real polynomials $q_v := \gamma_v p_v$ $(v \in S)$ and $q_v := \gamma_v p_v + \overline{\gamma_v p_v}$ $(v \in T)$. The polynomial $f - \sum_{v \in S \cup T} (q_v)^2$ vanishes at all points of V; hence it belongs to I, since I is radical. This shows that $f = \sigma + q$, where σ is a sum of squares and $q \in I$.

Suppose now that f is nonnegative on the set K. We define real polynomials s_0, $s_{m+1}, \ldots, s_{m+k}$ taking the following prescribed values at the points in V. If $v \in V \setminus S$, or if $v \in S$ and $f(v) \geq 0$, $s_0(v) = f(v)$ and $s_j(v) = 0$ $(j = m+1, \ldots, m+k)$. Otherwise, $v \notin K$ and thus $h_{j_v}(v) < 0$ for some $j_v \in \{m+1, \ldots, m+k\}$; then $s_{j_v}(v) = \frac{f(v)}{h_{j_v}(v)}$ and $s_0(v) = s_j(v) = 0$ for all remaining j. Then, each of $s_0, s_{m+1}, \ldots, s_{m+k}$ is nonnegative on S; by the above, $s_j = \sigma_j + q_j$, where σ_j is a sum of squares and $q_j \in I$. By construction, the polynomial $f - s_0 - \sum_{j=m+1}^{m+k} s_j h_j$ vanishes at all points of V and thus belongs to I. Therefore, $f - \sigma_0 - \sum_{j=m+1}^{m+k} \sigma_j h_j \in I$. ∎

Corollary 20 *Assume K is as in (21) and $h_1, \ldots, h_m$ generate a zero-dimensional radical ideal. Then the programs (1), (11) and (13) have the same optimum values; that is, $\rho^* = p^* = p_{\min}$.*

PROOF. Directly from Theorem 19, analogously to the proof of Theorem 15. ∎

3.2 Solving systems of polynomial equations

We will encounter in this paper (within the extraction procedure for global minimizers of polynomial optimization problems) the problem of solving a system of polynomial equations:

$$h_1(x) = 0, \ldots, h_m(x) = 0,$$

asssuming the ideal $I := \langle h_1, \ldots, h_m \rangle$ is zero-dimensional and radical. This problem has received considerable attention in the literature; see, e.g., [46] for a detailed account on various methods for solving this problem. We present the so-called eigenvalue method (also known as the Stetter-Möller method) which relates the points of $V(I)$ to the eigenvalues of the multiplication operator.

Given $h \in \mathbb{R}[x_1, \ldots, x_n]$,

$$\begin{array}{cccc} m_h : & \mathbb{R}[x_1, \ldots, x_n]/\mathcal{I} & \longrightarrow & \mathbb{R}[x_1, \ldots, x_n]/\mathcal{I} \\ & f \mod I & \longmapsto & fh \mod I \end{array} \tag{22}$$

is the 'multiplication by h' operator. Suppose we are given a basis $\mathcal{S}_{\mathcal{A}} := \{x^\alpha \mid \alpha \in \mathcal{A}\}$ of $\mathbb{R}[x_1, \ldots, x_n]/I$. Then we can define the matrix M_h of the operator m_h w.r.t. this basis. Thus M_h is the $|\mathcal{A}| \times |\mathcal{A}|$ matrix whose β-th column is the vector $\lambda^{(hx^\beta)} \in \mathbb{R}^{|\mathcal{A}|}$, giving the residue w.r.t. $\mathcal{S}_{\mathcal{A}}$ of the product hx^β, for $\beta \in \mathcal{A}$. When $h(x) = x_i$, the multiplication matrices M_{x_i} are also known as the *companion matrices* of the ideal $\mathcal{I}$. As the matrices $M_{x_1}, \ldots, M_{x_n}$ pairwise commute, they generate a commutative algebra $\mathbb{R}[M_{x_1}, \ldots, M_{x_n}]$, which is isomorphic to the ring $\mathbb{R}[x_1, \ldots, x_n]/\mathcal{I}$ via the correspondance $x_i \longmapsto M_{x_i}$. It is easy to verify that, for $h(x) = \sum_\alpha h_\alpha x^\alpha$, $M_h = \sum_\alpha h_\alpha M_{x_1}^{\alpha_1} \cdots M_{x_n}^{\alpha_n}$. The next result shows that the coordinates of the points $v \in V$ can be obtained from the eigenvalues of the companion matrices.

Theorem 21 (Stickelberger's theorem) *Let $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$ is a zero-dimensional radical ideal, let $\mathcal{S}_{\mathcal{A}} = \{x^\alpha \mid \alpha \in \mathcal{A}\}$ be a basis of $\mathbb{R}[x_1, \ldots, x_n]/I$, and let M_{x_i} the matrix of the multiplication operator m_{x_i} w.r.t. the basis $\mathcal{S}_{\mathcal{A}}$. Set $\zeta_{\mathcal{A},v} := (v^\alpha)_{\alpha \in \mathcal{A}}$ and let $p_v \in \mathbb{C}[x_1, \ldots, x_n]$ ($v \in V(I)$) be interpolation polynomials at the points of $V(I)$, where each p_v is assumed to be a linear combination of monomials in the basis $\mathcal{S}_{\mathcal{A}}$. Then, the eigenvalues of M_{x_i} are v_i (for $v \in V(I)$) with respective left eigenvector p_v and right eigenvector $\zeta_{\mathcal{A},v}$. That is,*

$$M_{x_i} p_v = v_i p_v, \;\; M_{x_i}^T \zeta_{\mathcal{A},v} = v_i \zeta_{\mathcal{A},v} \quad \forall v \in V(I). \tag{23}$$

PROOF. As I is radical, M_{x_i} is a matrix of size $|\mathcal{A}| = |V(I)|$. Hence, (23) implies that v_i (for $v \in V(I)$) are all the eigenvalues of M_{x_i}. Fix $v \in V(I)$ and set $p_v(x) := \sum_{\beta \in \mathcal{B}} a_\beta x^\beta$, $q := M_{x_i} p_v \in \mathbb{R}^{|\mathcal{B}|}$. The identity $q = v_i p_v$ will hold if we can show that the two polynomials $q(x) := \sum_{\gamma \in \mathcal{B}} q_\gamma x^\gamma$ and $v_i p_v(x)$ coincide. It suffices to show that $q(u) = v_i p_v(u)$ for all $u \in V(I)$. Indeed, if so, then the polynomial $q(x) - v_i p_v(x)$ belongs to I (since I is radical) and thus it is identically zero (since it is a linear combination of standard monomials). By the definition of M_{x_i}, $q = M_{x_i} p_v = \sum_{\beta \in \mathcal{B}} a_\beta \lambda^{(x_i x^\beta)}$ and thus $q(x) = \sum_{\gamma, \beta \in \mathcal{B}} a_\beta \lambda_\gamma^{(x_i x^\beta)} x^\gamma$. As $x^\beta x_i \equiv \sum_{\gamma \in \mathcal{B}} \lambda_\gamma^{(x_i x^\beta)} x^\gamma$ modulo I, $q(x) \equiv \sum_{\beta \in \mathcal{B}} a_\beta x^\beta x_i = x_i p_v(x)$ modulo I. Therefore, for $u \in V(I)$, $q(u) = p_v(u) u_i = p_v(u) v_i$.

Fix $\beta \in \mathcal{A}$ and let $\lambda \in \mathbb{C}^{|\mathcal{A}|}$ be the β-th column of M_{x_i}. That is, $x^\beta x_i - \sum_{\alpha \in \mathcal{A}} \lambda_\alpha x^\alpha \in I$, implying $v^\beta v_i = \sum_{\alpha \in \mathcal{A}} \lambda_\alpha v^\alpha$. In other words, $\zeta_{\mathcal{A},v}^T \lambda = v_i v^\beta$ for all $v \in V(I)$, which shows $M_{x_i}^T \zeta_{\mathcal{A},v} = v_i \zeta_{\mathcal{A},v}$. ∎

Let us indicate how to recover the points $v \in V(I)$ from the right eigenvectors vectors $\zeta_{\mathcal{A},v}$ of the multiplication matrices M_{x_i}. Note that, if several distinct points $v \in V(I)$ have the same i-th coordinate v_i, then the corresponding eigenspace of M_{x_i} has dimension larger than one and it is not clear how to recognize the eigenvector $\zeta_{\mathcal{A},v}$. Corless, Gianni, and Trager [7] propose the following strategy. Pick a polynomial $h \in \mathbb{R}[x_1, \ldots, x_n]$ which is a random linear combination of the monomials $x_1, \ldots, x_n$. Then, with high probability, the values $h(v)$ (for $v \in V(I)$) are all distinct. As these are precisely the eigenvalues of M_h, this means then that the right eigenspaces of the multiplication matrix M_h are all one-dimensional and thus spanned by the vectors $\zeta_{\mathcal{A},v}$ (for $v \in V(I)$). Once we know the vector $\zeta_{\mathcal{A},v}$ (or a scalar multiple of it), it is not hard to recover $v = (v_1, \ldots, v_n)$. Consider, e.g., the first coordinate v_1. If $x_1 \in \mathcal{S}_{\mathcal{A}}$, then v_1 can be read immediately from $\zeta_{\mathcal{A},v}$. Else, x_1 can be expressed as $\sum_{\alpha \in \mathcal{A}} \lambda_\alpha x^\alpha$ modulo I (for some scalars λ_α), implying $v_1 = \sum_{\alpha \in \mathcal{A}} \lambda_\alpha v^\alpha$, which can thus be computed from $\zeta_{\mathcal{A},v}$.

4 Results about Moment Matrices

We group here several results about moment matrices, which will have important applications to the optimization problem (1) over polynomials, in particular, for formulating optimality certificates and for extracting global minimizers.

4.1 Basic result about finite rank moment matrices

We have seen in Lemma 6 (iii) that, if a sequence $y \in \mathbb{Z}^{\mathbb{Z}^n_+}$ has a nonnegative r-atomic representing measure, then its moment matrix $M(y)$ is positive semidefinite and its rank is at most r. Curto and Fialkow [10] show that the rank of $M(y)$ is in fact *equal* to r and they show that the implication holds as an equivalence. More precisely, the following holds, which extends Theorem 9.

Theorem 22 *[10] Let $y \in \mathbb{R}^{\mathbb{Z}^n_+}$.*

(i) *If $M(y) \succeq 0$ and $M(y)$ has finite rank r, then y has a unique representing measure μ. Moreover, μ is r-atomic.*

(ii) *If y has an r-atomic representing measure, then $M(y) \succeq 0$ and $M(y)$ has rank r.*

The starting point of our proof is the fact that the kernel of a positive semidefinite (infinite) moment matrix is a radical ideal in $\mathbb{R}[x_1, \ldots, x_n]$; see Lemma 23 below. This property enables us to give a simpler proof for Theorem 22, which uses an algebraic tool (Hilbert's Nullstellensatz) in place of the tools from functional analysis (the spectral theorem and the Riesz representation theorem) used in the original proof of Curto and Fialkow [10].

Consider a moment matrix $M(y)$ where $y \in \mathbb{R}^{\mathbb{Z}^n_+}$. As $M(y)$ is indexed by $\mathbb{Z}^n_+$ (or equivalently by the monomials x^α for $\alpha \in \mathbb{Z}^n_+$), any vector $f = (f_\alpha)_\alpha$ in the kernel of $M(y)$ can be identified with the polynomial $f(x) = \sum_\alpha f_\alpha x^\alpha$. In this way, we may say that 'a polynomial p lies in the kernel of $M(y)$', and the kernel of $M(y)$ can be seen as a subset I of $\mathbb{R}[x_1, \ldots, x_n]$. Making this identification enables us, for instance, to claim in the next result that 'the kernel of $M(y)$ is an ideal in $\mathbb{R}[x_1, \ldots, x_n]$' (a fact observed by Curto and Fialkow [10]), or that 'the kernel is a radical ideal' when $M(y) \succeq 0$ (a fact observed by Laurent [26]).

Lemma 23 *The kernel $I := \{p \in \mathbb{R}[x_1, \ldots, x_n] \mid M(y)p = 0\}$ of a moment matrix $M(y)$ is an ideal in $\mathbb{R}[x_1, \ldots, x_n]$. If, moreover, $M(y) \succeq 0$, then I is a radical ideal.*

PROOF. We apply Lemma 4. Say $f \in I$ and $g \in \mathbb{R}[x_1, \ldots, x_n]$. For any $h \in \mathbb{R}[x_1, \ldots, x_n]$, $h^T M(y)(fg) = (hg)^T M(y) f = 0$, implying that $fg \in I$. Assume now $f^2 \in I$; we show that $f \in I$, which shows that I is radical. Indeed, $0 = f^T M(y) f = 1^T M(y)(f^2) = 0$, which implies $M(y)f = 0$, i.e., $f \in I$, since $M(y) \succeq 0$. ∎

We now prove Theorem 22. Assertion (ii) follows easily from (i) and Lemma 6 (iii). We now prove (i). Assume that $M(y) \succeq 0$ and let $r := \text{rank } M(y) < \infty$. By Lemma 23, $I := \text{Ker } M(y)$ is a radical ideal in $\mathbb{R}[x_1, \ldots, x_n]$.

Let $\mathcal{A}_0 \subseteq \mathbb{Z}_+^n$ be a subset indexing a maximum nonsingular principal submatrix of $M(y)$ and let M_0 denote the submatrix of $M(y)$ with rows and columns in $\mathcal{A}_0$; thus $|\mathcal{A}_0| = r$ and M_0 is nonsingular.

Lemma 24 *The set $\{x^\alpha \mid \alpha \in \mathcal{A}_0\}$ is a basis of the space $\mathbb{R}[x_1, \ldots, x_n]/I$.*

PROOF. The set $\{x^\alpha \mid \alpha \in \mathcal{A}_0\}$ is linearly independent in $\mathbb{R}[x_1, \ldots, x_n]/I$ since, if $\sum_{\alpha \in \mathcal{A}_0} \lambda_\alpha x^\alpha \in I$, then $M_0 \lambda = 0$ implying $\lambda = 0$. The set $\{x^\alpha \mid \alpha \in \mathcal{A}_0\}$ spans $\mathbb{R}[x_1, \ldots, x_n]/I$ since, for any $\beta \in \mathbb{Z}_+^n$, the β-th column of $M(y)$ can be written as a linear combination of its columns indexed by $\mathcal{A}_0$; that is, $x^\beta \equiv \sum_{\alpha \in \mathcal{A}_0} \lambda_\alpha x^\alpha \mod I$ for some scalars λ_α. ∎

Therefore, $r = |\mathcal{A}_0| = \dim \mathbb{R}[x_1, \ldots, x_n]/I$. By Theorem 17, $\dim \mathbb{R}[x_1, \ldots, x_n]/I = r = |V(I)|$, where $V(I) = \{x \in \mathbb{C}^n \mid f(x) = 0 \ \forall f \in I\}$ is the variety associated to I. Partition the set $V := V(I)$ into $S \cup T \cup \overline{T}$ where $S = V \cap \mathbb{R}^n$. Let p_v ($v \in V$) be interpolation polynomials with $p_{\overline{v}} = \overline{p_v}$ for $v \in V$. Let Z be the $|\mathbb{Z}_+^n| \times |V|$ matrix whose columns are the Zeta vectors $\zeta_v = (v^\alpha)_{\alpha \in \mathbb{Z}_+^n}$ (for $v \in V$), and let $\tilde{Z}$ be the $|V| \times |\mathbb{Z}_+^n|$ matrix whose rows are the vectors p_v ($v \in V$). Thus, $\tilde{Z} Z = I$.

Lemma 25 $M(y) = Z \text{diag}(\tilde{Z} y) Z^T$.

PROOF. Given $\alpha, \beta \in \mathbb{Z}_+^n$, one has to verify that $y_{\alpha+\beta} = \sum_{v \in V} v^\alpha v^\beta \sum_\gamma (p_v)_\gamma y_\gamma$. This follows from the fact that the polynomial $x^{\alpha+\beta} - \sum_{v \in V} v^\alpha v^\beta p_v(x)$ belongs to I since it vanishes at all points of V (and I is radical). ∎

Lemma 26 *$V(I) \subseteq \mathbb{R}^n$ and $\mu_0 := \sum_{v \in V(I)} p_v^T M(y) p_v \delta_v$ is a representing measure for y.*

PROOF. W.r.t. the partition $V(I) = S \cup T \cup \overline{T}$ and using Lemma 25, Z, $\tilde{Z}y$ and $M(y)$ can be written as

$$Z = \begin{array}{c} \begin{array}{ccc} S & T & \overline{T} \end{array} \\ \begin{pmatrix} A & B & \overline{B} \end{pmatrix} \end{array}, \quad \tilde{Z} y = \begin{array}{c} S \\ T \\ \overline{T} \end{array} \begin{pmatrix} a \\ b \\ \overline{b} \end{pmatrix}, \quad M(y) = \begin{pmatrix} A & B & \overline{B} \end{pmatrix} \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & \overline{b} \end{pmatrix} \begin{pmatrix} A^T \\ B^T \\ \overline{B}^T \end{pmatrix}$$

where A, B, a, b have real entries. Hence, $M(y) = A\mathrm{diag}(a)A^T + B\mathrm{diag}(b)B^T + \overline{B\mathrm{diag}(b)B^T}$. The term $A\mathrm{diag}(a)A^T$ can be written as $CC^T - DD^T$, where C, D are real matrices and the number of columns of C (resp., D) is the number of $v \in S$ with $a_v > 0$ (resp., $a_v < 0$). Setting $\sqrt{b} := (\sqrt{b_v})_{v \in V}$ and decomposing $B\mathrm{diag}(\sqrt{b})$ into its real and imaginary parts, $B\mathrm{diag}(b)B^T + \overline{B\mathrm{diag}(b)B^T}$ can be written as $EE^T - FF^T$, where E, F are real matrices with as many columns as the number of $v \in T$ with $b_v \neq 0$. Therefore, $M(y) = (CC^T + EE^T) - (DD^T + FF^T)$ is the difference of two positive semidefinite matrices. As $M(y) \succeq 0$, the kernel of $CC^T + EE^T$ is contained in the kernel of $M(y)$; that is, rank $M(y) \leq \mathrm{rank}(CC^T + EE^T) \leq |\{v \in S \mid a_v > 0\}| + |\{v \in T \mid b_v \neq 0\}|$. On the other hand, rank $M(y) = r = |V(I)| = |S| + 2|T|$. Therefore, $T = \emptyset$ and $a_v > 0$ for all $v \in S$, which implies that $V(I) \subseteq \mathbb{R}^n$, $M(y) = \sum_{v \in V(I)} a_v \zeta_v \zeta_v$, and $a_v = p_v^T M(y) p_v$ for all $v \in V(I)$. That is, $\mu_0 := \sum_{v \in V(I)} a_v \delta_v$ is a representing measure for y, which shows the lemma. ∎

The previous lemma shows the existence of an r-atomic measure μ_0 for y. We now verify the unicity of such measure. Say, μ is another representing measure for y. By Lemma 6, $r = \mathrm{rank}\ M(y) \leq s = |supp(\mu)|$; moreover, $supp(\mu) \subseteq V(I)$, implying $s \leq |V(I)| = r$. Thus, $r = s$, $supp(\mu) = V(I)$, and μ coincides with the measure μ_0 from Lemma 26. This concludes the proof of Theorem 22.

At that point, we make an observation, which will be useful for the proof of Theorem 36 below.

Lemma 27 *Assume $M(y) \succeq 0$ and $r = \mathrm{rank}\ M(y) < \infty$. Let μ be the representing measure for y, whose support is $V(I)$, where $I = \mathrm{Ker}\ M(y)$. If, for some integer $t \geq 1$, $\mathrm{rank}\ M_t(y) = r$, then there exist interpolation polynomials p_v ($v \in V(I)$) having degree at most t.*

PROOF. As rank $M_t(y) = \mathrm{rank}\ M(y)$, one can choose a basis $\{x^\alpha \mid \alpha \in \mathcal{A}_0\}$ of $\mathbb{R}[x_1, \ldots, x_n]/I$, where $\mathcal{A}_0$ is a subset of S_t. (Recall Lemma 24.) Let p_v ($v \in V(I)$) be interpolation polynomials at the points of $V(I)$. Replacing each p_v by its residue modulo I w.r.t. the basis $\{x^\alpha \mid \alpha \in \mathcal{A}_0\}$, we may assume that $\deg p_v \leq t$. ∎

By Lemma 23, the kernel of an infinite moment matrix is an ideal in $\mathbb{R}[x_1, \ldots, x_n]$. Although the kernel of a *truncated* moment matrix $M_t(y)$ cannot be claimed to be an ideal in $\mathbb{R}[x_1, \ldots, x_n]$, it yet enjoys the following 'truncated ideal like' properties, which will play an essential role in the proof of Theorem 32.

Lemma 28 *Assume that $M_t(y) \succeq 0$ and let f, g be two polynomials with product $h := fg$.*

(i) *If* $\deg(h) \leq t - 1$, *then* $M_t(y)f = 0 \Longrightarrow M_t(y)h = 0$.

(ii) *If* $\mathrm{rank}\ M_t(y) = \mathrm{rank}\ M_{t-1}(y)$ *and* $\deg(h) \leq t$, *then* $M_t(y)f = 0 \Longrightarrow M_t(y)h = 0$.

The proof uses the following easy fact about the kernel of a positive semidefinite matrix.

Lemma 29 *Let* $X = \begin{pmatrix} A & B \\ B^T & C \end{pmatrix} \succeq 0$, *where* X *is* $n \times n$, A *is* $p \times p$, C *is* $q \times q$, $n = p + q$.

(i) *For* $x \in \mathbb{R}^p$, $Ax = 0 \Longrightarrow X \begin{pmatrix} x \\ 0 \end{pmatrix} = 0$.

(ii) *Assume* X *is a flat extension of* A, *i.e.,* rank X = rank A. *For* $x \in \mathbb{R}^p$, $y \in \mathbb{R}^q$,

$$Ax + By = 0 \Longrightarrow X \begin{pmatrix} x \\ y \end{pmatrix} = 0.$$

Proof. (i) $Ax = 0 \Longrightarrow 0 = x^T A x = \begin{pmatrix} x^T & 0 \end{pmatrix} X \begin{pmatrix} x \\ 0 \end{pmatrix}$, which implies $X \begin{pmatrix} x \\ 0 \end{pmatrix} = 0$, as $X \succeq 0$.
(ii) By assumption, $B = AW$, $C = B^T W = W^T A W$ for some matrix W, and $0 = Ax + By = Ax + AWy$. Then, $B^T x + Cy = W^T(Ax + AWy) = 0$, giving $X \begin{pmatrix} x \\ y \end{pmatrix} = 0$. ∎

Proof of Lemma 28. It suffices to show the result for $g(x) = x_i$ since the general result follows from repeated applications of this special case. Then, $h(x) = \sum_\alpha f_\alpha x^{\alpha + e_i} = \sum_{\alpha | \alpha \geq e_i} f_{\alpha - e_i} x^\alpha$. For $\alpha \in S_{t-1}$, we have:

$$(M_t(y)h)_\alpha = \sum_\gamma h_\gamma y_{\alpha+\gamma} = \sum_{\gamma | \gamma \geq e_i} f_{\gamma - e_i} y_{\alpha+\gamma} = \sum_\gamma f_\gamma y_{\alpha+\gamma+e_i} = (M_t(y)f)_{\alpha+e_i} = 0.$$

In view of Lemma 29, this implies that $M_t(y)h = 0$ in both cases (i), (ii). ∎

4.2 Further results about moment matrices

Theorem 22 characterizes the infinite sequences having a finite atomic representing measure. The next question is to characterize the *truncated* sequences $y \in \mathbb{R}^{S_{2t}}$ having a finite atomic representing measure μ. It turns out that for a truncated sequence, the existence of a representing measure implies the existence of another one with a finite support (this is not true for infinite sequences). This result, due to Bayer and Teichmann [2], strengthens an earlier result of Putinar [39] which assumed the existence of a measure with a compact support.

Theorem 30 *[2] If a truncated sequence* $y \in \mathbb{R}^{S_{2t}}$ *has a representing measure, then it has one which is finitely atomic with at most* $\binom{n+2t}{2t}$ *atoms.*

Proof. Assume $y \in \mathbb{R}^{S_{2t}}$ has a representing measure μ and let $S := supp(\mu)$. We show that y has another finite atomic representing measure having at most $\binom{n+2t}{2t}$ atoms. For this, let $\mathcal{C}$ denote the cone generated by the vectors $\zeta_{2t,x} = (x^\alpha)_{\alpha \in S_{2t}}$ for $x \in S$. Then $\mathcal{C}$ is a a convex cone, whose closure $\overline{\mathcal{C}}$ is a closed convex cone in $\mathbb{R}^{S_{2t}}$. Therefore $\overline{\mathcal{C}}$ is equal to the intersection of its supporting halfspaces; say,

$$\overline{\mathcal{C}} = \{z \in \mathbb{R}^{S_{2t}} \mid c^T z \leq 0 \ \forall c \in I\}$$

for some $I \subseteq \mathbb{R}^{|S_{2t}|}$. Obviously, $y \in \overline{\mathcal{C}}$ since, for any $c \in I$,

$$c^T y = \sum_\alpha c_\alpha y_\alpha = \int_S (\sum_\alpha c_\alpha x^\alpha) \mu(dx) \leq 0$$

as $\sum_\alpha c_\alpha x^\alpha = c^T \zeta_{2t,x} \leq 0$ for all $x \in S$. Moreover,

$$y \text{ belongs to the relative interior of } \overline{\mathcal{C}}. \tag{24}$$

Indeed, consider a supporting hyperplane $c^T z \leq 0$ ($c \in I$) that does not contain $\overline{\mathcal{C}}$; we show that $c^T y < 0$. For this, assume $c^T y = 0$ and set $X := \{x \in S \mid c^T \zeta_{2t,x} < 0\}$, $X_k := \{x \in S \mid c^T \zeta_{2t,x} \leq -\frac{1}{k}\}$ for $k \geq 1$ integer. Then, $X \neq \emptyset$ and $X = \cup_{k \geq 1} X_k$. We have:

$$0 = c^T y = \int_X c^T \zeta_{2t,x} \mu(dx) = \int_{X_k} c^T \zeta_{2t,x} \mu(dx) + \int_{X \setminus X_k} c^T \zeta_{2t,x} \mu(dx),$$

implying $0 \geq \int_{X \setminus X_k} c^T \zeta_{2t,x} \mu(dx) = -\int_{X_k} c^T \zeta_{2t,x} \mu(dx) \geq \frac{1}{k} \mu(X_k)$ and thus $\mu(X_k) = 0$. This shows that $\mu(X) = 0$. Therefore, $S \setminus X = S \cap \{x \mid c^T \zeta_{2t,x} = 0\}$ is a closed set whose complement $(\mathbb{R}^n \setminus S) \cup X$ has measure 0, which contradicts the definition of the support of μ. Therefore, (24) holds and thus y belongs to the cone $\mathcal{C}$. Using Caratheodory's theorem, we deduce that y can be written as a conic combination of at most $|S_{2t}| = \binom{n+2t}{2t}$ vectors $\zeta_{2t,x}$; that is, y has an atomic representing measure with at most $\binom{n+2t}{2t}$ atoms. ∎

By Lemma 6 (i), a necessary condition for the existence of a finite atomic reprenting measure for $y \in \mathbb{R}^{S_{2t}}$ is that the moment matrix $M_t(y)$ has rank at most $|supp(\mu)|$. Theorem 34 below gives a characterization for the existence of a *minimum* atomic measure, i.e., satisfying $|supp(\mu)| = \text{rank } M_t(y)$. Then Theorem 35 deals with the general case of existence of a finite atomic representing measure. In both results, the following notion of flat extension plays a central role.

Definition 31 *Let X be a symmetric matrix with block decomposition $X = \begin{pmatrix} A & B \\ B^T & C \end{pmatrix}$. One says that X is a* flat extension *of A if* rank X = rank A *or, equivalently, if $B = AW$ and $C = B^T W = W^T A W$ for some matrix W. Observe that, if X is a flat extension of A, then $X \succeq 0 \Longleftrightarrow A \succeq 0$.*

Theorem 32 below provides a key result about flat extensions of moment matrices. It permits (under some 'flat extension' assumption) to extend a truncated sequence $y \in \mathbb{R}^{S_{2t}}$ with $M_t(y) \succeq 0$ to an infinite sequence $y \in \mathbb{R}^{\mathbb{Z}_+^n}$ with $M(y) \succeq 0$ having finite rank, and thus to apply the tools developped for infinite moment sequences (e.g, Theorem 22) to truncated sequences.

Theorem 32 *[10] Let $y \in \mathbb{R}^{S_{2t}}$ for which $M_t(y) \succeq 0$ and $M_t(y)$ is a flat extension of $M_{t-1}(y)$. Then, one can extend y to a (unique) vector in $\mathbb{R}^{S_{2t+2}}$, again denoted by y, in such a way that $M_{t+1}(y)$ is a flat extension of $M_t(y)$.*

We delay the proof of Theorem 32, which is a bit technical, till the Appendix. Theorem 32, combined with Theorem 22, imply directly the next corollary and Theorem 34 below.

Corollary 33 *[10] Given $y \in \mathbb{R}^{S_{2t}}$, assume that $M_t(y) \succeq 0$ and that $M_t(y)$ is a flat extension of $M_{t-1}(y)$. Then, one can extend y to a vector in $\mathbb{R}^{\mathbb{Z}_+^n}$ which is the sequence of moments of a finite atomic nonnegative measure on $\mathbb{R}^n$.*

Theorem 34 *[10] The following assertions are equivalent for $y \in \mathbb{R}^{S_{2t}}$.*

(i) *y has a* (rank $M_t(y)$)*-atomic representing measure.*

(ii) *$M_t(y) \succeq 0$ and one can extend y to a vector $y \in \mathbb{R}^{S_{2t+2}}$ in such a way that $M_{t+1}(y)$ is a flat extension of $M_t(y)$.*

Theorem 35 *[11] The following assertions are equivalent for $y \in \mathbb{R}^{S_{2t}}$.*

(i) *y has a representing measure [equivalently, a finite atomic representing measure].*

(ii) *$M_t(y) \succeq 0$ and there exists an integer $k \geq 0$ for which y can be extended to a vector $y \in \mathbb{R}^{S_{2(t+k+1)}}$ in such a way that $M_{t+k}(y) \succeq 0$ and $M_{t+k+1}(y)$ is a flat extension of $M_{t+k}(y)$.*

Moreover, one can assume $k \leq \binom{n+2t}{2t} - t$ in (ii).

Proof. Assume that (i) holds. In view of Theorem 30, y has an r-atomic representing measure μ for some $r \geq 1$. Then, y can be extended to $y \in \mathbb{R}^{\mathbb{Z}_+^n}$ with μ as representing measure. Therefore, by Theorem 22 (ii), $M(y) \succeq 0$ and rank $M(y) = r$. Let $k \geq 0$ be the smallest integer for which rank $M_{t+k}(y) = r$. Then, $M_{t+k+1}(y)$ is a flat extension of $M_{t+k}(y)$, showing (iii).

Assume that (ii) holds. By Theorem 32, y can be extended to $y \in \mathbb{R}^{\mathbb{Z}_+^n}$ in such a way that $M(y)$ has a finite rank. Therefore, y has a finite atomic representing measure by Theorem 22 (i).

We now verify that one may choose $k \leq \binom{n+2t}{2t} - t$ in (iii). For this, let $k \geq 0$ be the smallest integer for which rank $M_{t+k}(y) = r$. Then, rank $M_{t+k+1}(y) =$ rank $M_{t+k}(y)$. If $k = 0$, then $k \leq \binom{n+2t}{2t} - t$ holds. Assume $k \geq 1$. Then, rank $M_{s+1}(y) \geq$ rank $M_s(y) + 1$ for all $1 \leq s \leq t+k-1$. This implies that rank $M_{t+k}(y) \geq t+k$ and, thus, $k \leq r-t \leq \binom{n+2t}{2t}-t$. ∎

Curto and Fialkow [12] extend the above two results to truncated sequences having a finite atomic representing measure whose support is contained in a prescribed semialgebraic set K. We derive them from Theorems 34 and 35 using the short argument from [26].

Theorem 36 *[12] Let $y \in \mathbb{R}^{\mathcal{S}_{2t}}$, let K be the set from (4), and set $d := \max_{j=1,\dots,m} d_j$. The following assertions are equivalent.*

(i) *y has a* (rank $M_t(y)$)*-atomic nonnegative representing measure whose support is contained in K.*

(ii) *$M_t(y) \succeq 0$ and y can be extended to a vector $y \in \mathbb{R}^{\mathcal{S}_{2(t+d)}}$ in such a way that $M_{t+d}(y)$ is a flat extension of $M_t(y)$ and $M_t(h_j * y) \succeq 0$ for $j = 1, \dots, m$.*

In that case, the representing measure μ is unique and, setting $r_j :=$ rank $M_t(h_j * y)$, exactly $r - r_j$ of the atoms in the support of μ belong to the set of roots of the polynomial $h_j(x)$.

Proof. The implication (i) $\Longrightarrow$ (ii) follows from Theorem 34 ((i) $\Longrightarrow$ (ii)) together with Lemma 6 (ii). Conversely, assume that (ii) holds and set $r :=$ rank $M_t(y)$. In view of Theorem 34 ((ii) $\Longrightarrow$ (i)) (and its proof), y has an r-atomic representing measure μ; say, $\mu = \sum_{v \in S} \lambda_v \delta_v$ where $\lambda_v > 0$, $|S| = r$. We prove that $S \subseteq K$; that is, $h_j(v) \geq 0$ for all $v \in S$. By Lemma 27, there exist interpolation polynomials p_v ($v \in S$) having degree at most t. Then, $p_v^T M_t(h_j * y) p_v = \sum_{u \in V} (p_v(u))^2 h_j(u) \lambda_u = h_j(v) \lambda_v \geq 0$, since $M_t(h_j * y) \succeq 0$. This implies that $h_j(v) \geq 0$ for all $j = 1, \dots, m$, $v \in V$; that is, the measure μ is supported by the set K.

We now verify that $r - r_j$ of the points of S are zeros of the polynomial $h_j(x)$. Denote again by $y \in \mathbb{R}^{\mathbb{Z}_+^n}$ the (infinite) sequence of moments of the measure μ and denote again by $h_j * y$ the (infinite) sequence of moments of the measure $\mu_j := \sum_{v \in S} \lambda_v h_j(v) \delta_v$. Thus, y (resp., $h_j * y$) is an extension of the given vector y (resp., $h_j * y$). By Theorem 34 (ii), rank $M(h_j * y) = |\{v \in S \mid h_j(v) > 0\}|$. We now verify that $M(h_j * y)$ is a flat extension of $M_t(h_j * y)$, which implies that $r_j = |\{v \in S \mid h_j(v) > 0\}|$, giving the desired result. For this we note that Ker $M(y) \subseteq$ Ker $M(h_j * y)$. Indeed, if $p \in$ Ker $M(y)$ then, using Lemma 4, $p^T M(h_j * y) p = (p h_j)^T M(y) p = 0$. Now, as $M(y)$ is a flat extension of $M_t(y)$, it follows that $M(h_j * y)$ is a flat extension of $M_t(h_j * y)$ too. ∎

Theorem 37 *[12] Let K be the set from (4), and $d := \max_{j=1,\dots,m} d_j$. The following assertions are equivalent for $y \in \mathbb{R}^{\mathcal{S}_{2t}}$.*

(i) *y has a representing measure whose support is finite and contained in K.*

(ii) *$M_t(y) \succeq 0$ and there exists an integer $k \geq 0$ for which y can be extended to a vector $y \in \mathbb{R}^{\mathcal{S}_{2(t+k+d)}}$ in such a way that $M_{t+k}(y) \succeq 0$, $M_{t+k+1}(y)$ is a flat extension of $M_{t+k}(y)$, and $M_{t+k}(h_j * y) \succeq 0$ for $j = 1, \ldots, m$.*

PROOF. ∎

5 Application to Optimization

Let us consider again the optimization problem (1). In Section 2.3, we have defined the dual semidefinite hierarchies (16) (based on moment matrices) and (17) (based on sums of squares of polynomials), giving lower bounds p_t^* and ρ_t^* satisfying

$$\rho_t^* \leq p_t^* \leq p_{\min}$$

for $t \geq \max(d, d_1, \ldots, d_m)$. We raised several issues: asymptotic/finite convergence to $p_{\min}$, optimality certificate, extraction of global minimizers. We now explain how the results about moment matrices from Section 4 permit to give (partial) answers to these questions.

5.1 Asymptotic/finite convergence

To start with, recall Theorem 15 showing that Putinar's result (Theorem 14) implies the asymptotic convergence of ρ_t^*, p_t^* to $p_{\min}$ as $t \to \infty$, assuming the semialgebraic set satisfies (10).

We now present a class of problems for which finite convergence can be proved, namely, when the description of the semialgebraic set K contains a set of equations $h_1(x) = 0$, $\ldots$, $h_m(x) = 0$ generating a zero-dimensional ideal J. Theorem 38 below is taken from Laurent [25], except (iii) in the radical case which follows from Theorem 19 (from Parrilo [33]).

This result applies, for instance, to the 0/1 case when the equations $x_i^2 - x_i = 0$ ($i = 1, \ldots, n$) are present in the description of the semialgebraic set K; then, $K \subseteq \{0,1\}^n$ and we find the finite convergence result proven by Lasserre [22]. In the 0/1 case, other combinatorial methods have been proposed for constructing hierarchies of bounds; in particular, by Sherali and Adams [44], Lovász and Schrijver [27]. It turns out that the hierachy of bounds p_t^* refines these other hierarchies; see Laurent [24].

The finite convergence result applies, more generally, to the case when K is a discrete grid, i.e., when $K = K_1 \times \ldots \times K_n$ (each $K_i \subseteq \mathbb{R}$ finite), considered by Lasserre [23].

Theorem 38 *[25] Consider the problem (1) of minimizing a polynomial p over the semialgebraic set $K = \{x \in \mathbb{R}^n \mid h_j(x) = 0 \ (j = 1, \ldots, m),\ h_j(x) \geq 0 \ (j = m+1, \ldots, m+k)\}$ (as in (21)). Let J denote the ideal generated by $h_1, \ldots, h_m$ and assume that J is zero-dimensional. Then,*

(i) $\rho^* = p^* = p_{\min}$.

(ii) $p_{\min} = p_t^*$ *for t large enough.*

(iii) *If J is radical, or if $h_1, \ldots, h_m$ form a Groebner basis of J, then $\rho_t^* = p_t^* = p_{\min}$ for t large enough.*

PROOF. (i) follows from Theorem 15 since the set K satisfies (10). Indeed, the polynomial $p := -\sum_{j=1}^m h_j^2$ belongs to $\Sigma_{put}(K)$ and $\{x \in \mathbb{R}^n \mid p(x) \geq 0\} = V(J) \cap \mathbb{R}^n$ is compact (since finite).

Alternatively, the equality $p^* = p_{\min}$ follows from Theorem 22. Let us give the argument, since the latter result is more elementary than Putinar's result (used for Theorem 15). Assume $y_0 = 1$, $M(y) \succeq 0$, $M(h_j * y) = 0$ ($j = 1, \ldots, m$) and $M(h_j * y) \succeq 0$ ($j \geq m+1$). Then, for $j = 1, \ldots, m$, $0 = h_j * y = M(y)h_j$, which implies that $J \subseteq I :=$ Ker $M(y)$. Hence, $V(I) \subseteq V(J)$ is finite and thus $\dim \mathbb{R}[x_1, \ldots, x_n]/I < \infty$, which implies that rank $M(y) < \infty$. By Theorem 22 (and its proof), $V(I) \subseteq \mathbb{R}^n$ and y has a finite atomic measure μ supported by $V(I)$; say, $\mu = \sum_{v \in V(I)} \lambda_v \delta_v$ with $\lambda_v > 0$. Remains to verify that $S \subseteq K$, i.e., $h_j(v) \geq 0$ for $j \geq m+1$ and $v \in V(I)$. Let p_v ($v \in V(I)$) be (real) interpolation polynomials at the points of $V(I)$. Then, $p_v^T M(h_j * y) p_v = \lambda_v h_j(v)$, which implies $h_j(v) \geq 0$ for $j \geq m+1$. Thus $V(I) \subseteq K$, implying $p^T y \geq p_{\min}$. Therefore, $p^* \geq p_{\min}$, giving equality $p^* = p_{\min}$.

We now prove (ii). Let $\mathcal{B} := \{b_1, \ldots, b_s\}$ be a set of polynomials forming a basis of $\mathbb{R}[x_1, \ldots, x_n]/J$ and set $d_{\mathcal{B}} := \max_{i=1,\ldots,s} \deg(b_i)$. With $d_0 = \lceil \deg p/2 \rceil$, $d_j = \lceil \deg h_j/2 \rceil$, set $t_0 := \max(d_0, d_{\mathcal{B}} + 1, d_{\mathcal{B}} + \max_{j \geq m+1} d_j, 2 \max_{j=1,\ldots,m} d_j)$. Fix $\alpha \in S_{t_0}$. Then, $f^{(\alpha)}(x) := x^\alpha - \sum_{r=1}^s \lambda_r^{(\alpha)} b_r \in J$ for some scalars $\lambda_r^{(\alpha)}$. Thus, $f^{(\alpha)}(x) = \sum_{j=1}^m u_j^{(\alpha)} h_j$ for some polynomials $u_j^{(\alpha)} \in \mathbb{R}[x_1, \ldots, x_n]$. Set

$$T_0 := \max(t_0, 1 + \deg(u_j^{(\alpha)} h_j \text{ for } \alpha \in S_{t_0},\ j = 1, \ldots, m).$$

We show that $p_t^* = p_{\min}$ for $t \geq T_0$. For this assume $y_0 = 1$, $M_t(y) \geq 0$, $M_{t-d_j}(h_j * y) = 0$ ($j = 1, \ldots, m$), $M_{t-d_j}(h_j * y) \succeq 0$ ($j \geq m+1$). We show that y has a representing measure supported by K. As $t \geq 2d_j$ for $j \leq m$, we deduce from $M_{t-d_j}(h_j * y) = 0$ that $M_t(y)h_j = 0$. Fix $\alpha \in S_{t_0}$. For $j \leq m$, as $\deg(u_j^{(\alpha)} h_j) \leq T_0 - 1 \leq t - 1$, we can apply Lemma 28 and deduce that $M_t(y)(u_j^{(\alpha)} h_j) = 0$. Therefore, $M_t(y) f^{(\alpha)} = 0$ for all $\alpha \in S_{t_0}$. Going back to the definition of $f^{(\alpha)}$, this shows that every column of $M_t(y)$ can be expressed as a linear combination of its columns indexed by monomials in $S_{d_{\mathcal{B}}}$. That is, $M_t(y)$ is a flat extension of $M_{d_{\mathcal{B}}}(y)$. As $t \geq d_{\mathcal{B}} + 1$, we deduce from Corollary 33 that y has a finite atomic representing measure, say, $\mu = \sum_{v \in S} \lambda_v \delta_v$ with $\delta_v > 0$ and $S \subseteq \mathbb{R}^n$. Remains to show that $S \subseteq K$. For $j \leq m$, $M_t(y)h_j = 0$ implies that $0 = h_j M_t(y) h_j = \sum_{v \in S} \lambda_v h_j(v)^2$ and thus $h_j(v) = 0$ for all $v \in S$. Hence, $S \subseteq V(J)$. As above, let p_v ($v \in S$) be interpolation polynomials at the points of S. As $S \subseteq V(J)$, we can replace each p_v by its residue q_v modulo J w.r.t. the basis $\mathcal{B}$. In this way we obtain a set of interpolation polynomials q_v ($v \in S$) having degree at most $d_\mathcal{B}$. For $j \geq m+1$, $d_\mathcal{B} \leq t - d_j$ and thus $0 \leq q_v^T M_{t-d_j}(h_j * y) q_v = \lambda_v h_j(v)$ implies $h_j(v) \geq 0$. Therefore, $S \subseteq K$ and we can conclude that $p^T y \geq p_{\min}$, giving $p_t^* \geq p_{\min}$ and thus equality $p_t^* = p_{\min}$.

We now prove (iii), assuming $h_1, \ldots, h_m$ form a Groebner basis of J. Let $\epsilon > 0$ and $t \geq \max(d_0, d_1, \ldots, d_m, d_\mathcal{B}, d_\mathcal{B} + d_{m+1}, \ldots, d_\mathcal{B} + d_{m+k})$. We show that $\rho_t^* \geq p_{\min} - \epsilon$. Letting ϵ go to 0, this gives $\rho_t^* \geq p_{\min}$ and thus equality $\rho_t^* = p_t^* = p_{\min}$. The polynomial $p(x) - p_{\min} + \epsilon$ is positive on K. By Theorem 14, $p(x) - p_{\min} + \epsilon = u_0 + \sum_{j=m+1}^{m+k} u_j h_j + q$, where $u_0, u_{m+1}, \ldots, u_{m+k}$ are sums of squares and $q \in J$. Such a decomposition exists where each u_j is a sum of squares of polynomials that are linear combinations of members of the basis $\mathcal{B}$. Thus we may assume that $\deg(u_0) \leq 2d_\mathcal{B} \leq 2t$, $\deg(u_j h_j) \leq 2(d_\mathcal{B} + d_j) \leq 2t$. Hence, $\deg(q) \leq 2t$. As $h_1, \ldots, h_m$ form a Groebner basis of J, one can find (using the division algorithm) a decomposition $q = \sum_{j=1}^m u_j h_j$ with $\deg(u_j h_j) \leq 2t$. Therefore, $p_{\min} - \epsilon$ is feasible for the program (17), which implies $p_{\min} - \epsilon \leq \rho_t^*$. ∎

5.2 Optimality certificate

The result of Curto and Fialkow from Theorem 36 is used by Henrion and Lasserre [17] for formulating a stopping criterion for the hierarchy (16), namely, for producing a certificate that the relaxation (16) of order t in fact solves the original problem (1) at optimality.

Theorem 39 *Let $y \in \mathbb{R}^{\mathcal{S}_{2t}}$ be an optimum solution to the program (16), $d_j = \lceil \deg(h_j)/2 \rceil$, and $d = \max(d_1, \ldots, d_m)$. If*

$$\text{rank } M_t(y) = \text{rank } M_{t-d}(y), \tag{25}$$

then $p_t^* = p_{\min}$.

Proof. By assumption, $M_t(y) \succeq 0$, rank $M_t(y) =$ rank $M_{t-d}(y) =: r$, $M_{t-d}(h_j * y) \succeq 0$ for $j = 1, \ldots, m$. Therefore, by Theorem 36, we can conclude that y has an r-atomic representing measure $\mu = \sum_{i=1}^r \lambda_i \delta_{v_i}$, where $v_i \in K$, $\lambda_i > 0$ and $\sum_{i=1}^r \lambda_i = 1$ (since $y_0 = 1$). Hence, $p_t^* = p^T y = \sum_{i=1}^r \lambda_i p(v_i) \geq p_{\min}$, as $p(v_i) \geq p_{\min}$ for all i. On the other hand, $p_{\min} \geq p_t^*$. This implies that $p_{\min} = p_t^*$ and that each v_i is a minimizer of $p(x)$ over the set K. ∎

Henrion and Lasserre [17] also propose a procedure for extracting a global optimizer of $p(x)$ over the set K when the assumption (25) is satisfied. This procedure is incorporated in the optimization software GloptiPoly. We describe it in the next section.

5.3 Extracting global minimizers

We present here the method proposed by Henrion and Lasserre [17] for finding global minimizers to problem (1) (asuming (25) holds), whose details fit nicely within the algebraic setting developped in Section 4.1 for positive semidefinite moment matrices of finite rank.

We assume throughout this section that $y \in \mathbb{R}^{S_{2t}}$ is an optimum solution to the program (16) satisfying the rank condition (25). As the proof of Theorem 39 shows, $p_t^* = p_{\min}$ and y has an r-atomic representing measure $\mu = \sum_{i=1}^r \lambda_i \delta_{v_i}$, where $\lambda_i > 0$, $\sum_{i=1}^r \lambda_i = 1$, $r = \text{rank } M_t(y)$, and the points $v_1, \ldots, v_r$ are global minimizers of $p(x)$ over the set K. The question we now address is how to find the v_i's knowing only the optimum moment matrix $M_t(y)$.

Denote also by y the (infinite) sequence of moments of the measure μ. Then, $M(y) \succeq 0$, $r = \text{rank } M(y)$, and $\{v_1, \ldots, v_r\} = V(I)$, where $I := \text{Ker } M(y)$ (by the results in Section 4.1). Therefore, $v_1, \ldots, v_r$ are the common zeros to the polynomials in I. (In fact, it is not difficult to check that I is equal to the ideal generated by Ker $M_t(y)$; therefore, the v_i's are the common zeros to a set of polynomials forming a linear basis of Ker $M_t(y)$.) As the ideal I is zero-dimensional radical, we can apply the eigenvalue technique from Section 3.2 for finding its variety $V(I) = \{v_1, \ldots, v_r\}$. We now describe in more detail how the eigenvalue technique applies to our problem. Our description differs in some steps from the original method of Henrion and Lasserre and it follows the implementation described by Jibetean and Laurent [19].

In a first step, we determine a subset $\mathcal{A}_0 \subseteq \mathbb{Z}_+^n$ indexing a maximum nonsingular principal submatrix of $M_t(y)$. Thus, $|\mathcal{A}_0| = \text{rank } M_t(y) = r$ and the set $\mathcal{S}_{\mathcal{A}_0} = \{x^\alpha \mid \alpha \in \mathcal{A}_0\}$ is a basis of $\mathbb{R}[x_1, \ldots, x_n]/I$ (by Lemma 24). We find such set $\mathcal{A}_0$ in a 'greedy manner', by computing the successive ranks of the north-east corner principal submatrices of $M_t(y)$. Starting from the constant monomial 1, we insert in $\mathcal{A}_0$ as many low degree monomials as possible.

In a second step, we construct the multiplication matrices M_{x_i} (for $i = 1, \ldots, n$). Here, M_{x_i} is defined as the matrix of the 'multiplication by x_i' operator m_{x_i} (recall (22)) with respect to the basis $\mathcal{S}_{\mathcal{A}_0}$ of $\mathbb{R}[x_1, \ldots, x_n]/I$. That is, for $\beta \in \mathcal{A}_0$, the β-th column of M_{x_i} contains the residue of the monomial $x_i x^\beta$ modulo I w.r.t. the basis $\mathcal{S}_{\mathcal{A}_0}$.

Lemma 40 *Let M_0 denote the principal submatrix of $M_t(y)$ indexed by $\mathcal{A}_0$ and let U_i denote the submatrix of $M_t(y)$ whose rows are indexed by $\mathcal{A}_0$ and whose columns are indexed by the set $x_i\mathcal{A}_0 := \{x_i x^\alpha \mid \alpha \in \mathcal{A}_0\}$. Then, $M_{x_i} = M_0^{-1} U_i$.*

Proof. For $\alpha \in \mathcal{A}_0$, let C_α denote the α-th column of $M_t(y)$. Fix $\beta \in \mathcal{A}_0$. Let C denote the column of $M_t(y)$ indexed by $x^\beta x_i$, let $\tilde{C} := (C_\alpha)_{\alpha \in \mathcal{A}_0}$ the corresponding column of U_i, and let $\lambda = (\lambda_\alpha)_{\alpha \in \mathcal{A}_0}$ be the scalars permitting to express C as $C = \sum_{\alpha \in \mathcal{A}_0} \lambda_\alpha C_\alpha$. In other words, the polynomial $x^\beta x_i - \sum_{\alpha \in \mathcal{A}_0} \lambda_\alpha x^\alpha$ belongs to the kernel of $M_t(y)$ and thus to I, which means that the β-th column of M_{x_i} is equal to λ. As $M_0 \lambda = \tilde{C}$, we deduce that $\lambda = M_0^{-1} \tilde{C}$, which gives the identity $M_{x_i} = M_0^{-1} U_i$. ∎

In view of Theorem 21, the right eigenvectors of M_{x_i} are the vectors $\zeta_{\mathcal{A}_0,v} = (v^\alpha)_{\alpha\in\mathcal{A}_0}$ with respective eigenvalues v_i (for $v \in V(I)$). Therefore, for a polynomial $h \in \mathbb{R}[x_1,\ldots,x_n]$, the eigenvalues of the multiplication matrix M_h are $h(v)$ for $v \in V(I)$. Thus, if the values $h(v)$ for $v \in V(I)$ are all distinct, the right eigenspaces of M_h are 1-dimensional and spanned by the vectors $\zeta_{\mathcal{A}_0,v}$ (for $v \in V(I)$). In that case, one can recover the vectors $\zeta_{\mathcal{A}_0,v}$ from the right eigenvectors of M_h. Then it is easy - in fact, immediate if $\mathcal{A}_0$ contains the monomials $x_1,\ldots,x_n$ - to recover the components of v from the vector $\zeta_{\mathcal{A}_0,v} = (v^\alpha)_{\alpha\in\mathcal{A}_0}$. Following the strategy of Corless, Gianni, and Trager [7], choose h as a random linear combination of the monomials $x_1,\ldots,x_n$; then, with high probability, the values $h(v)$ at the distinct points of $V(I)$ are all distinct.

We illustrate the method on some examples. See [21], [17] for more examples.

Example 41 Consider the problem:

$$\begin{array}{ll} \min & p(x) = -25(x_1-2)^2 - (x_2-2)^2 - (x_3-1)^2 \\ & \qquad\qquad -(x_4-4)^2 - (x_5-1)^2 - (x_6-4)^2 \\ \text{s.t.} & (x_3-3)^2 + x_4 \geq 4, \;\; (x_5-3)^2 + x_6 \geq 4 \\ & x_1 - 3x_2 \leq 2, \;\; -x_1 + x_2 \leq 2, \; x_1 + x_2 \leq 6, \\ & x_1 + x_2 \geq 2, \; 1 \leq x_3 \leq 5, \; 0 \leq x_4 \leq 6, \\ & 1 \leq x_5 \leq 5, \; 0 \leq x_6 \leq 10, \; x_1, x_2 \geq 0 \end{array}$$

GloptiPoly finds the optimum value -310 and a global minimizer $(5,1,5,0,5,10)$ at the relaxation of order $t = 2$. This involves then the computation of a SDP with 209 variables, one semidefinite constraint involving a matrix of size 28 (namley, $M_2(y) \succeq 0$) and 16 semidefinite constraints involving matrices size 7 (namely, $M_1(h_j * y) \succeq 0$, corresponding to the 16 constraints $h_j(x) \geq 0$ of degree 1 or 2).

order t	bound p_t^*	solution extracted
1	unbounded	none
2	-310	(5,1,5,0,5,10)

Example 42 Consider the problem

$$\begin{array}{ll} \min & p(x) = -x_1 - x_2 \\ \text{s.t.} & x_2 \leq 2x_1^4 - 8x_1^3 + 8x_1^2 + 2 \\ & x_2 \leq 4x_1^4 - 32x_1^3 + 88x_1^2 - 96x_1 + 36 \\ & 0 \leq x_1 \leq 3, \; 0 \leq x_2 \leq 4 \end{array}$$

GloptiPoly solves the problem at optimality at the relaxation of order $t = 4$.

order t	bound p_t^*	solution extracted
2	-7	none
3	-6.6667	none
4	-5.5080	(2.3295,3.1785)

References

[1] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in Real Algebraic Geometry.* Springer, 2003.

[2] C. Bayer and J. Teichmann. The proof of Tchakaloff's theorem. Preprint, 2005.

[3] C. Berg, J.P.R. Christensen, and C.U. Jensen. A remark on the multidimensional moment problem. *Mathematische Annalen*, 243:163–169, 1979.

[4] C. Berg, J.P.R. Christensen, and P. Ressel. Positive definite functions on Abelian semigroups. *Mathematische Annalen*, 223:253–272, 1976.

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

[6] A.M. Cohen, H. Cuypers, and H. Sterk (eds.). *Some Tapas of Computer Algebra.* Springer, Berlin, 1999.

[7] R.M. Corless, P.M. Gianni, B.M. Trager. A reordered Schur factorization method for zero-dimensional polynomial systems with multiple roots. *Proceedings ACM International Symposium Symbolic and Algebraic Computations*, Maui, Hawaii, 133–140, 1997.

[8] D. A. Cox, J. B. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer, 1997.

[9] D. A. Cox, J. B. Little, and D. O'Shea. *Using Algebraic Geometry.* Graduate Texts in Mathematics, Number 185, Springer, New York, 1998.

[10] R.E. Curto and L.A. Fialkow. Solution of the truncated complex moment problem for flat data. *Memoirs of the American Mathematical Society,* vol. 119, n. 568, 1996.

[11] R.E. Curto and L.A. Fialkow. Flat extensions of positive moment matrices: recursively generated relations. *Memoirs of the American Mathematical Society,* vol. 136, n. 648, 1998.

[12] R.E. Curto and L.A. Fialkow. The truncated complex K-moment problem. *Transactions of the American Mathematical Society*, 352:2825–2855, 2000.

[13] B. Fuglede. The multidimensional moment problem. *Expositiones Mathematicae*, 1:47–65, 1983.

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

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

[16] D. Henrion and J.-B. Lasserre. GloptiPoly: Global optimization over polynomials with Matlab and SeDuMi. *ACM Transactions Math. Soft.*, 29:165–194, 2003.

[17] D. Henrion and J.-B. Lasserre. Detecting global optimality and extracting solutions in GloptiPoly. In *Positive Polynomials in Control, D. Henrion and A. Garulli*, eds., Lecture Notes on Control and Information Sciences, Vol. 312, pages 293–310. Springer Verlag, Berlin, January 2005.

[18] T. Jacobi and A. Prestel. Distinguished representations of strictly positive polynomials. *Journal für die Reine und Angewandte Mathematik*, 532:223–235, 2001.

[19] D. Jibetean and M. Laurent. Semidefinite approximations for global unconstrained polynomial optimization. *SIAM Journal on Optimization*, to appear.

[20] H. Landau. Classic background of the moment problem. In *Moments in Mathematics*, Proceedings of Symposia in Applied Mathematics, vol. 37, pages 1–15, AMS, Providence, 1987.

[21] J.B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on Optimization*, 11:796–817, 2001.

[22] J.B. Lasserre. An explicit exact SDP relaxation for nonlinear $0-1$ programs. In K. Aardal and A.M.H. Gerards, eds., *Lecture Notes in Computer Science*, 2081:293–303, 2001.

[23] J.B. Lasserre. Polynomials nonnegative on a grid and discrete representations. *Transactions of the American Mathematical Society*, 354:631–649, 2001.

[24] M. Laurent. A comparison of the Sherali-Adams, Lovász-Schrijver and Lasserre relaxations for 0-1 programming. *Mathematics of Operations Research*, 28(3):470–496, 2003.

[25] M. Laurent. Semidefinite representations for finite varieties. *Mathematical Programming*, to appear.

[26] M. Laurent. Revisiting two theorems of Curto and Fialkow on moment matrices. *Proceedings of the American Mathematical Society* 133(10):2965–2976, 2005.

[27] L. Lovász and A. Schrijver. Cones of matrices and set-functions and $0-1$ optimization. *SIAM Journal on Optimization*, 1:166–190, 1991.

[28] T.S. Motzkin and E.G. Straus. Maxima for graphs and a new proof of a theorem of Túran. *Canadian Journal of Mathematics* 17: 533–540, 1965.

[29] K.G. Murty and S.N. Kabadi. Sone NP-complete problems in quadratic and nonlinear programming. *Mathematical Programming*, 39:117–129, 1987.

[30] Y. Nesterov. Squared functional systems and optimization problems. In J.B.G. Frenk, C. Roos, T. Terlaky, and S. Zhang, eds., *High Performance Optimization*, pages 405–440. Kluwer Academic Publishers, 2000.

[31] P.A. Parrilo. *Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization.* PhD thesis, California Institute of Technology, May 2000.

[32] P.A. Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Mathematical Programming B*, 96:293–320, 2003.

[33] P.A. Parrilo. An explicit construction of distinguished representations of polynomials nonnegative over finite sets. Preprint, ETH, Zürich, 2002.

[34] S. Prajna, A. Papachristodoulou, and P.A. Parrilo. SOSTOOLS (Sums of squares optimization toolbox for MATLAB) User's guide. Available at http://control.ee.ethz.ch/ parrilo/sostools/index.html

[35] V. Powers and B. Reznick. A new bound for Pólya's theorem with applications to polynomials positive on polyhedra. *Journal of Pure and Applied Algebra*, 164 (1-2):221–229, 2001.

[36] V. Powers and T. Wörmann. An algorithm for sums of squares of real polynomials. *Journal of Pure and Applied Algebra*, 127:99–104, 1998.

[37] A. Prestel and C.N. Delzell. *Positive Polynomials - From Hilbert's 17th Problem to Real Algebra.* Springer, Berlin, 2001.

[38] M. Putinar. Positive polynomials on compact semi-algebraic sets. *Indiana University Mathematics Journal*, 42:969–984, 1993.

[39] M. Putinar. A note on Tchakaloff's theorem. *Proceedings of the American Mathematical Society*, 125:2409–2414, 1997.

[40] B. Reznick. Some concrete aspects of Hilbert's 17th problem. In *Real Algebraic Geometry and Ordered Structures*, C.N. Delzell and J.J. Madden, eds., *Contemporary Mathematics* 253: 251–272, 2000.

[41] K. Schmüdgen. The K-moment problem for compact semi-algebraic sets. *Mathematische Annalen*, 289:203–206, 1991.

[42] M. Schweighofer. On the complexity of Schmüdgen's Positivstellensatz. *Journal of Complexity* 20(4):529–543, 2004.

[43] M. Schweighofer. Optimization of polynomials on compact semialgebraic sets. *SIAM Journal on Optimization* 15(3):805–825, 2005.

[44] H.D. Sherali and W.P. Adams. A hierarchy of relaxations between the continuous and convex hull representations for zero-one programming problems. *SIAM Journal on Discrete Mathematics*, 3:411–430, 1990.

[45] N.Z. Shor. An approach to obtaining global extremums in polynomial mathematical programming problems. *Kibernetika*, 5:102–106, 1987.

[46] B. Sturmfels. *Solving Systems of Polynomial Equations.* CBMS, Regional Conference Series in Mathematics, Number 97, AMS, Providence, 2002.

[47] H. Wolkowicz, R. saigal, L. Vandeberghe (eds.). *Handbook of Semidefinite Programming*, Kluwer, 2000.

Appendix

We give here the proof of Theorem 32. We begin with a characterization of moment matrices.

Lemma 43 *Let M be a symmetric matrix indexed by S_t. Then, M is a moment matrix, i.e., $M = M_t(y)$ for some sequence $y \in \mathbb{R}^{S_{2t}}$, if and only if the following holds:*

(i) $M_{\alpha,\beta} = M_{\alpha-e_i,\beta+e_i}$ *for all $\alpha, \beta \in S_t$, $i \in \{1,\ldots,n\}$ such that $\alpha_i \geq 1$, $|\beta| \leq t-1$.*

(ii) $M_{\alpha,\beta} = M_{\alpha-e_i+e_j,\beta+e_i-e_j}$ *for all $\alpha, \beta \in S_t$, $i, j \in \{1,\ldots,n\}$ such that $\alpha_i, \beta_j \geq 1$, $|\alpha| = |\beta| = t$.*

Proof. The 'if part' being obvious, we show the 'only if' part. That is, we assume that (i), (ii) hold and we show that $M(\alpha,\beta) = M(\alpha',\beta')$ whenever $\alpha+\beta = \alpha'+\beta'$. For this we use induction on the parameter $\delta_{\alpha\beta,\alpha'\beta'} := \min(\|\alpha-\alpha'\|_1, \|\beta-\beta'\|_1)$. If $\delta_{\alpha\beta,\alpha'\beta'} = 0$, then $(\alpha,\beta) = (\alpha',\beta')$ and there is nothing to prove. If $\delta_{\alpha\beta,\alpha'\beta'} = 1$, then the result holds by assumption (i). Assume now that $\delta_{\alpha\beta,\alpha'\beta'} \geq 2$.

Consider first the case when $|\alpha|+|\beta| \leq 2t-1$. As $\alpha \neq \alpha'$ we may assume without loss of generality that $\alpha'_i \geq \alpha_i+1$ for some i, implying $\beta'_i \leq \beta_i-1$. Define $(\alpha'',\beta'') := (\alpha-e_i, \beta+e_i)$. Then, $\delta_{\alpha\beta,\alpha''\beta''} = \delta_{\alpha\beta,\alpha'\beta'} - 1$. If $|\beta'| \leq t-1$, then $M_{\alpha,\beta} = M_{\alpha'',\beta''}$ by the induction assumption and $M_{\alpha'',\beta''} = M_{\alpha',\beta'}$ by (i), implying the desired result. Assume now that $|\beta'| = t$ and thus $|\alpha'| \leq t-1$. Then, $|\alpha| - |\alpha'| = t - |\beta| \geq 0$ and thus $\alpha_i \geq \alpha'_i + 1$ for some i, yielding $\beta'_i \geq \beta_i + 1$. Define $(\alpha'',\beta'') := (\alpha'+e_i, \beta'-e_i)$. Then $\delta_{\alpha\beta,\alpha''\beta''} = \delta_{\alpha\beta,\alpha'\beta'} - 1$. Therefore, $M_{\alpha,\beta} = M_{\alpha'',\beta''}$ by the induction assumption and $M_{\alpha'',\beta''} = M_{\alpha',\beta'}$ by (i), implying the desired result.

We can now suppose that $|\alpha| = |\beta| = |\alpha'| = |\beta'| = t$. Hence, $\alpha'_i \geq \alpha_i + 1$ for some i and $\beta'_j \geq \beta_j + 1$ for some j; moreover $i \neq j$. Define $(\alpha'',\beta'') := (\alpha'-e_i+e_j, \beta'+e_i-e_j)$. Then, $\delta_{\alpha\beta,\alpha''\beta''} = \delta_{\alpha\beta,\alpha'\beta'} - 2$. Therefore, $M_{\alpha,\beta} = M_{\alpha'',\beta''}$ by the induction assumption and $M_{\alpha'',\beta''} = M_{\alpha',\beta'}$ by (ii), implying the desired result. ∎

We now prove Theorem 32. Set $X := M_t(y) = \begin{pmatrix} A & B \\ B^T & C \end{pmatrix}$, where $A := M_{t-1}(y)$. By assumption, X is a flat extension of A. Our objective is to construct a flat extension $Y := \begin{pmatrix} X & D \\ D^T & E \end{pmatrix}$ of X, which is a moment matrix. As we explain below, Lemma 28 (ii) plays a central role in this construction. In what follows we use the following notation: For a matrix M and a column index α, M_α denotes the column of M indexed by α.

As X is a flat extension of A, we can choose a subset $\mathcal{B} \subseteq S_{t-1}$ indexing a maximum nonsingular principal submatrix of X. Then any column of X can be decomposed in a unique way as a linear combination of columns indexed by the set $\mathcal{B}$. That is, for any $\alpha \in S_t$, there exists a unique set of scalars $a_\beta^{(\alpha)}$ ($\beta \in \mathcal{B}$) for which

$$X_\alpha = \sum_{\beta \in \mathcal{B}} a_\beta^{(\alpha)} X_\beta. \tag{26}$$

We now explain how to define the matrix Y, i.e., the matrices D and E. Take $\gamma \in S_{t+1}$ with $|\gamma| = t+1$. Say, $\gamma_i \geq 1$ for some $i = 1, \ldots, n$. As observed above, the column $X_{\gamma - e_i}$ of X indexed by $\gamma - e_i \in S_t$, can be written as

$$X_{\gamma - e_i} = \sum_{\beta \in \mathcal{B}} a_\beta^{(\gamma - e_i)} X_\beta. \tag{27}$$

In other words, the polynomial $p(x) := x^{\gamma - e_i} - \sum_{\beta \in \mathcal{B}} a_\beta^{(\gamma - e_i)} x^\beta$ has its coefficient vector p lying in the kernel of X. For $q(x) := p(x) x_i$, it follows from Lemma 28 (ii) that q belongs to the kernel of Y, the desired flat extension of X. Therefore, the following identity should hold:

$$Y_\gamma = \sum_{\beta \in \mathcal{B}} a_\beta^{(\gamma - e_i)} Y_{\beta + e_i}. \tag{28}$$

In particular, we should define the γ-th column of D in the following way:

$$D_\gamma = \sum_{\beta \in \mathcal{B}} a_\beta^{(\gamma - e_i)} X_{\beta + e_i}. \tag{29}$$

And, in turn, the γ-th column of E should be given by:

$$E_\gamma = \sum_{\beta \in \mathcal{B}} a_\beta^{(\gamma - e_i)} (D^T)_{\beta + e_i}. \tag{30}$$

We verify that the above definitions for the matrices D and E are *good*, i.e., that the definitions (29), (30) do not depend on the choice of the index i for which $\gamma_i \geq 1$.

Lemma 44 *Defining D, E as explained above, via (27), (29), (30), is a* good *definition.*

Proof. let $\gamma \in S_{t+1}$ with $|\gamma| = t+1$ and assume that $\gamma_i, \gamma_j \geq 1$ for two distinct indices $i, j = 1, \ldots, n$. Let

$$v := \sum_{\beta \in \mathcal{B}} a_\beta^{(\gamma - e_i)} X_{\beta + e_i}, \quad w := \sum_{\beta \in \mathcal{B}} a_\beta^{(\gamma - e_j)} X_{\beta + e_j}$$

be the corresponding two candidate definitions for D_γ via (29). We show that they produce the same answer; that is, $v = w$. By Lemma 29, it suffices to show that $v_\alpha = w_\alpha$ for $\alpha \in S_{t-1}$. Given $\alpha \in S_{t-1}$, we have:

$$v_\alpha = \sum_{\beta \in \mathcal{B}} a_\beta^{(\gamma - e_i)} X_{\alpha, \beta + e_i} = \sum_{\beta \in \mathcal{B}} a_\beta^{(\gamma - e_i)} X_{\alpha + e_i, \beta} = \left(\sum_{\beta \in \mathcal{B}} a_\beta^{(\gamma - e_i)} X_\beta \right)_{\alpha + e_i} = X_{\alpha + e_i, \gamma - e_i} = X_{\alpha, \gamma}.$$

Similarly, $w_\alpha = X_{\alpha,\gamma}$, showing $v = w$.

Let $\delta \in S_{t+1}$ with $|\delta| = t+1$ and let

$$v := (\sum_{\beta \in \mathcal{B}} a_\beta^{(\gamma - e_i)} (D^T)_{\beta + e_i})_\delta, \quad w := (\sum_{\beta \in \mathcal{B}} a_\beta^{(\gamma - e_j)} (D^T)_{\beta + e_j})_\delta$$

be the two candidate values for the entry $E_{\delta,\gamma}$ obtained via (30); we show that $v = w$. For this, pick an index r for which $\delta_r \geq 1$. We have:

$$\begin{aligned} v &= \left(\sum_{\beta \in \mathcal{B}} a_\beta^{(\gamma - e_i)} (D^T)_{\beta + e_i} \right)_\delta = \sum_{\beta \in \mathcal{B}} a_\beta^{(\gamma - e_i)} (D_\delta)_{\beta + e_i} \\ &= \sum_{\beta \in \mathcal{B}} a_\beta^{(\gamma - e_i)} \left(\sum_{\beta' \in \mathcal{B}} a_{\beta'}^{(\delta - e_r)} X_{\beta' + e_r} \right)_{\beta + e_i} \\ &= \sum_{\beta' \in \mathcal{B}} a_{\beta'}^{(\delta - e_r)} \left(\sum_{\beta \in \mathcal{B}} a_\beta^{(\gamma - e_i)} X_{\beta + e_i} \right)_{\beta' + e_r}. \end{aligned}$$

Similarly,

$$w = \sum_{\beta' \in \mathcal{B}} a_{\beta'}^{(\delta - e_r)} \left(\sum_{\beta \in \mathcal{B}} a_\beta^{(\gamma - e_j)} X_{\beta + e_j} \right)_{\beta' + e_r}.$$

Now, we just saw above that the two inner summations are equal, which shows $v = w$. ∎

We now verify that the matrix Y is a moment matrix, i.e., that Y satisfies the conditions (i), (ii) from Lemma 43.

Lemma 45 *$Y_{\gamma,\delta} = Y_{\gamma+e_i, \delta - e_i}$ for $\gamma, \delta \in S_{t+1}$ with $\delta_i \geq 1$ and $|\gamma| \leq t$.*

Proof. Suppose first that $|\gamma| \leq t-1$. We can assume that $|\delta| = t+1$ (else, the result holds since X is a moment matrix). We have:

$$Y_{\gamma,\delta} = (Y_\delta)_\gamma = \left(\sum_{\beta \in \mathcal{B}} a_\beta^{(\delta - e_i)} Y_{\beta + e_i} \right)_\gamma = \sum_{\beta \in \mathcal{B}} a_\beta^{(\delta - e_i)} X_{\gamma, \beta + e_i},$$

$$Y_{\gamma + e_i, \delta - e_i} = (Y_{\delta - e_i})_{\gamma + e_i} = \left(\sum_{\beta \in \mathcal{B}} a_\beta^{(\delta - e_i)} Y_\beta \right)_{\gamma + e_i} = \sum_{\beta \in \mathcal{B}} a_\beta^{(\delta - e_i)} X_{\gamma + e_i, \beta} = Y_{\gamma,\delta}.$$

Suppose now that $|\gamma| = t$, $|\delta| \leq t$. Then,

$$Y_{\gamma,\delta} = X_{\gamma,\delta} = (X_\gamma)_\delta = \left(\sum_{\beta\in\mathcal{B}} a_\beta^{(\gamma)} X_\beta\right)_\delta = \sum_{\beta\in\mathcal{B}} a_\beta^{(\gamma)} X_{\beta,\delta},$$

$$Y_{\gamma+e_i,\delta-e_i} = (Y_{\gamma+e_i})_{\delta-e_i} = \left(\sum_{\beta\in\mathcal{B}} a_\beta^{(\gamma)} Y_{\beta+e_i}\right)_{\delta-e_i} = \sum_{\beta\in\mathcal{B}} a_\beta^{(\gamma)} X_{\beta+e_i,\delta-e_i} = Y_{\gamma,\delta}.$$

Suppose finally that $|\gamma| = t$, $|\delta| = t+1$. Then,

$$\begin{gathered} Y_{\gamma,\delta} = (Y_\gamma)_\delta = \left(\sum_{\beta\in\mathcal{B}} a_\beta^{(\gamma)} Y_\beta\right)_\delta = \sum_{\beta\in\mathcal{B}} a_\beta^{(\gamma)} (Y_\delta)_\beta \\ = \sum_{\beta\in\mathcal{B}} a_\beta^{(\gamma)} \left(\sum_{\beta'\in\mathcal{B}} a_{\beta'}^{(\delta-e_i)} Y_{\beta'+e_i}\right)_\beta = \sum_{\beta,\beta'\in\mathcal{B}} a_\beta^{(\gamma)} a_{\beta'}^{(\delta-e_i)} X_{\beta'+e_i,\beta} \end{gathered}$$

and

$$\begin{gathered} Y_{\gamma+e_i,\delta-e_i} = (Y_{\delta-e_i})_{\gamma+e_i} = \left(\sum_{\beta'\in\mathcal{B}} a_{\beta'}^{(\delta-e_i)} Y_{\beta'}\right)_{\gamma+e_i} \\ = \sum_{\beta'\in\mathcal{B}} a_{\beta'}^{(\delta-e_i)} (Y_{\gamma+e_i})_{\beta'} = \sum_{\beta'\in\mathcal{B}} a_{\beta'}^{(\delta-e_i)} \left(\sum_{\beta\in\mathcal{B}} a_\beta^{(\gamma)} Y_{\beta+e_i}\right)_{\beta'} \\ = \sum_{\beta,\beta'\in\mathcal{B}} a_{\beta'}^{(\delta-e_i)} a_\beta^{(\gamma)} X_{\beta+e_i,\beta'} = Y_{\gamma,\delta}. \end{gathered}$$

∎

Lemma 46 *$Y_{\gamma,\delta} = Y_{\gamma-e_j+e_i,\delta+e_j-e_i}$ for $\gamma, \delta \in S_{t+1}$ with $\gamma_j \geq 1$, $\delta_i \geq 1$, $|\gamma| = |\delta| = t+1$.*

PROOF. We have:

$$\begin{gathered} Y_{\gamma,\delta} = (Y_\gamma)_\delta = \left(\sum_{\beta\in\mathcal{B}} a_\beta^{(\gamma-e_j)} Y_{\beta+e_j}\right)_\delta = \sum_{\beta\in\mathcal{B}} a_\beta^{(\gamma-e_j)} (Y_\delta)_{\beta+e_j} \\ = \sum_{\beta\in\mathcal{B}} a_\beta^{(\gamma-e_j)} \left(\sum_{\beta'\in\mathcal{B}} a_{\beta'}^{(\delta-e_i)} Y_{\beta'+e_i}\right)_{\beta+e_j} = \sum_{\beta,\beta'\in\mathcal{B}} a_\beta^{(\gamma-e_j)} a_{\beta'}^{(\delta-e_i)} X_{\beta+e_j,\beta'+e_i}, \end{gathered}$$

and

$$\begin{gathered} Y_{\gamma-e_j+e_i,\delta+e_j-e_i} = (Y_{\gamma-e_j+e_i})_{\delta+e_j-e_i} = \left(\sum_{\beta\in\mathcal{B}} a_\beta^{(\gamma-e_j)} Y_{\beta+e_i}\right)_{\delta+e_j-e_i} \\ = \sum_{\beta\in\mathcal{B}} a_\beta^{(\gamma-e_j)} (Y_{\delta-e_j+e_i})_{\beta+e_i} = \sum_{\beta\in\mathcal{B}} a_\beta^{(\gamma-e_j)} \left(\sum_{\beta'\in\mathcal{B}} a_{\beta'}^{(\delta-e_i)} Y_{\beta'+e_j}\right)_{\beta+e_i} \\ = \sum_{\beta,\beta'\in\mathcal{B}} a_\beta^{(\gamma-e_j)} a_{\beta'}^{(\delta-e_i)} X_{\beta+e_i,\beta'+e_j} = Y_{\gamma,\delta}. \end{gathered}$$

∎