Algebraic certificates for the truncated moment problem

Didier Henrion, Simone Naldi, Mohab Safey El Din

Algebraic certificates for the truncated moment problem

Didier Henrion[1,2], Simone Naldi[3], Mohab Safey El Din[4]

February 13, 2023

Abstract

The truncated moment problem consists of determining whether a given finite-dimensional vector of real numbers $\boldsymbol{y}$ is obtained by integrating a basis of the vector space of polynomials of bounded degree with respect to a non-negative measure on a given set K of a finite-dimensional Euclidean space. This problem has plenty of applications *e.g.* in optimization, control theory and statistics. When K is a compact semialgebraic set, the duality between the cone of moments of non-negative measures on K and the cone of non-negative polynomials on K yields an alternative: either $\boldsymbol{y}$ is a moment vector, or $\boldsymbol{y}$ is not a moment vector, in which case there exists a polynomial strictly positive on K making a linear functional depending on $\boldsymbol{y}$ vanish. Such a polynomial is an *algebraic certificate* of moment unrepresentability. We study the complexity of computing such a certificate using computer algebra algorithms.
Keywords: moments, sums of squares, semialgebraic sets, real algebraic geometry, algorithms, complexity.

1 Introduction

Problem statement Let $\boldsymbol{x} = (x_1, \ldots, x_n)$ be variables, $\mathbb{R}[\boldsymbol{x}]$ be the ring of n-variate real polynomials and for $d \in \mathbb{N}$, let $\mathbb{R}[\boldsymbol{x}]_{\leq d}$ be the vector space of real polynomials of degree at most d. The multivariate monomial with exponent $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ is denoted by $\boldsymbol{x}^{\boldsymbol{\alpha}} := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, and its total degree by $|\boldsymbol{\alpha}| = \alpha_1 + \cdots + \alpha_n$. For $\boldsymbol{g} = (g_1, \ldots, g_k) \in \mathbb{R}[\boldsymbol{x}]^k$, the *basic semialgebraic set* associated with $\boldsymbol{g}$ is

$$S(\boldsymbol{g}) = \{\boldsymbol{a} \in \mathbb{R}^n : g_1(\boldsymbol{a}) \geq 0, \ldots, g_k(\boldsymbol{a}) \geq 0\}. \tag{1}$$

Given $n, d \in \mathbb{N}$ and a sequence of real numbers $\boldsymbol{y} = (y_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \mathbb{N}^n_d}$ indexed by $\mathbb{N}^n_d = \{\boldsymbol{\alpha} \in \mathbb{N}^n : \sum_{i=1}^n \alpha_i \leq d\}$, the *truncated moment problem* (below TMP) is the question of deciding

[1]CNRS, LAAS, Université de Toulouse, France.
[2]Faculty of Electrical Engineering, Czech Technical University in Prague, Czechia.
[3]Université de Limoges, CNRS, XLIM, Limoges, France.
[4]Sorbonne Université, LIP6, Paris, France.

whether there exists a nonnegative Borel measure μ on $\mathbb{R}^n$, with support in $K = S(\boldsymbol{g})$, and such that

$$y_{\boldsymbol{\alpha}} = \int_K x^{\boldsymbol{\alpha}} \, d\,\mu, \qquad \text{for all } \boldsymbol{\alpha} \in \mathbb{N}^n_d, \tag{2}$$

If this is the case, one says that $\boldsymbol{y}$ is *moment-representable on* K. More generally, the monomial basis can be replaced by another linear basis of $\mathbb{R}[\boldsymbol{x}]_{\leq d}$, (*e.g.* Chebyshev polynomials). The TMP is the truncated version of the classical *full moment problem* [18, 33].

Overview and state of the art The TMP is of central importance in data science. It is at the heart of several questions in optimization, control theory or statistics, to mention just a few application domains. It is a key ingredient to the moment-SOS (sum of squares) approach [13] which consists of solving numerically non-convex non-linear problems at the price of solving a family of finite-dimensional conic optimization (typically semidefinite programming) problems. Mathematical foundations of the moment problem were recently surveyed in [33, 10].

The TMP can be interpreted as a *decision problem of the first order theory of the reals*, in which case, the input-output data structure is as follows. The input is encoded by a finite-dimensional real vector $\boldsymbol{y}$, whose coordinates are indexed by a basis of the vector space of n-variate polynomials of degree $\leq d$, together with finitely-many polynomial inequalities defining a basic semialgebraic set $K \subset \mathbb{R}^n$. The output is a decision yes/no whether $\boldsymbol{y}$ is obtained by integrating the basis with respect to a non-negative measure supported on K.

When K is compact, the TMP is dual, in the convex analysis sense, to the problem of determining whether a polynomial is non-negative on the semialgebraic set K. This latter problem is at the heart of the development of real algebra in the twentieth century. Whereas deciding nonnegativity of a polynomial of degree at least four can be challenging (NP-complete problems can be cast as instances of such positivity problems [19]), there exist algebraic certificates based on SOS for deciding strict positivity under compactness-like assumptions that can be computed by solving a semidefinite programming (SDP) problem [27]. For positivity over compact basic semialgebraic sets, these certificates have the form of linear combinations with SOS coefficients of polynomials that are explicitly nonnegative on K [28, 32]. The size of the SDP is determined by the degree of the SOS-representation. Seminal papers [29, 26] have started to investigate the complexity of SDP in the context of rational arithmetic. More recent work is based on the determinantal structure of semidefinite programs [14].

The specific case study of computation of SOS certificates have recently received a lot of attention from the computer algebra community [16, 17, 14, 15, 20] especially for the question whether certificates exist over the rational numbers [25, 30, 12, 31]. In this work we make use of quantifier elimination for determining bounds on the complexity of computing certificates for unrepresentability by using quantitative results from [2]. These also rely on recent advances in the complexity analysis of Putinar Positivstellensatz [1].

Note that these non-negativity problems can be solved with computer algebra algorithms which are root-finding algorithms, hence which do not provide algebraic certificates of non-negativity but do provide witnesses (real points) of negativity whenever they exist. The first family of algorithms for doing so is based on the so-called Cylindrical Algebraic Decomposition [8]. It has complexity which is doubly exponential in the number of variables, which would lead, in the context of TMP, to complexity bounds that are doubly exponential in $n + \binom{n+d}{d}$. The second family of algorithms, named critical point method, initiated by [11], has complexity which is singly exponential in the number of variables (see [3] and references therein).

The purpose of this communication is to leverage on these achievements and initiate the study and development of *computer algebra algorithms for solving the truncated moment problem for basic semialgebraic sets.*

Overview of the contribution In the wake of the mentioned duality with moments, the existence of SOS-certificates for nonnegative polynomials in the dual side, suggests that similar certificates might be used for the TMP on the primal side.

On the one hand, when a measure exists whose partial moments coincide with $\boldsymbol{y}$, the measure itself is the natural algebraic proof that allows the user to verify directly that $\boldsymbol{y}$ is moment-representable. On the other hand, this paper shows the existence of explicit algebraic certificates of unrepresentability: these have the form of positive polynomials on K admitting a positivity certificate and orthogonal to the vector $\boldsymbol{y}$.

Our contribution is based on the fact that the TMP, as a decision problem, is equivalent to the feasibility of a convex conic program in a finite dimensional vector space. More precisely, the question is whether the interior of $\mathscr{P}(K)_d$, the cone of polynomials nonnegative on K of degree at most d, intersects the vanishing locus of the Riesz functional $\mathscr{L}_{\boldsymbol{y}} : \mathbb{R}[x]_{\leq d} \to \mathbb{R}$ defined by $\mathscr{L}_{\boldsymbol{y}} \left(\sum p_{\boldsymbol{\alpha}} x^{\boldsymbol{\alpha}}\right) = \sum p_{\boldsymbol{\alpha}} y_{\boldsymbol{\alpha}}$.

When K is compact, Tchakaloff's Theorem [35] states that $\boldsymbol{y}$ is moment-representable whenever $\mathscr{L}_{\boldsymbol{y}}$ is nonnegative on $\mathscr{P}(K)_d$, in other words, if the mentioned conic program is *weakly feasible.* In this case there exists an atomic measure $\mu = \sum_{i=1}^{s} c_i \delta_{x_i}$ whose moment sequence of degree $\leq d$ is $\boldsymbol{y}$: such measure is a (real) solution of a highly structured polynomial system of type multivariate Vandermonde, which we do not investigate here. On the other side of the coin, $\boldsymbol{y}$ is not moment-representable exactly when the conic program is *strongly feasible*: in algebraic terms, this means that there exists a polynomial $p \in \mathscr{P}(K)_d$, (strictly) positive on K, in the kernel of $\mathscr{L}_{\boldsymbol{y}}$.

In our contribution we study algorithmic aspects of the computation of such *unrepresentability algebraic certificates* when $\boldsymbol{y}$ is not moment-representable. First, we show that if the quadratic module corresponding to the description of K is archimedean, such certificates exist. We define an integer invariant called the unrepresentability degree which measures the complexity of computing such certificate. We give bounds on such degree that only depend on the input size of our algorithm. When the input vector $\boldsymbol{y}$ is defined over $\mathbb{Q}$, and if it is not moment-representable, we show that there exists a rational certificate of unrepresentability.

2 Preliminaries

2.1 Nonnegative polynomials

Let $K \subset \mathbb{R}^n$. A polynomial $f \in \mathbb{R}[\boldsymbol{x}]$ is called *nonnegative* on K if $f(\boldsymbol{a}) \geq 0$ for all $\boldsymbol{a} \in K$ and *positive* if $f(\boldsymbol{a}) > 0$ for all $\boldsymbol{a} \in K$. We denote by

$$\mathscr{P}(K)_d = \{f \in \mathbb{R}[\boldsymbol{x}]_{\leq d} : f(\boldsymbol{a}) \geq 0, \forall \boldsymbol{a} \in K\}$$

the convex cone of polynomials of degree $\leq d$, nonnegative on K. If K is semialgebraic, then $\mathscr{P}(K)_d$ is also semialgebraic by the theorem of Tarski on quantifier elimination over the reals [34].

We denote by $\Sigma_n \subset \mathbb{R}[\boldsymbol{x}]$ the *cone of sums of squares* of polynomials, and by $\Sigma_{n,2d} = \Sigma_n \cap \mathbb{R}[\boldsymbol{x}]_{\leq 2d}$ its degree-$2d$ part (remark that $\Sigma_{n,2d+1} = \Sigma_{n,2d}$). The cone $\Sigma_{n,2d}$ is full-dimensional in $\mathbb{R}[\boldsymbol{x}]_{\leq 2d}$ and is contained in $\mathscr{P}(\mathbb{R}^n)_{2d}$.

Testing membership in cones of nonnegative polynomials over semialgebraic sets can be challenging. Indeed, testing nonnegativity of polynomials of degree ≥ 4 is NP-hard [19, Sec. 1.1]. Nevertheless $\mathscr{P}(K)_d$ contains subcones that can be represented via linear matrix inequalities, thus testing membership in these subcones can be cast as a *semidefinite programming (SDP) problem.*

Examples of such subsets are quadratic modules: for $K = S(\boldsymbol{g})$ as in (1) and $d \in \mathbb{N}$, and denoting $g_0 := 1$, we define the *quadratic module* associated with $\boldsymbol{g}$ and its *truncation of order d* respectively by:

$$Q(\boldsymbol{g}) = \left\{\sum_{i=0}^{k} \sigma_i g_i : \sigma_i \in \Sigma_n\right\} \quad \text{and}$$
$$Q(\boldsymbol{g})[d] = \left\{\sum_{i=0}^{k} \sigma_i g_i : \sigma_i \in \Sigma_n, \deg(\sigma_i g_i) \leq d\right\}.$$

If $f \in Q(\boldsymbol{g})$, we call the polynomials $[\sigma_0, \sigma_1, \ldots, \sigma_k]$ in an expression $f = \sum_{i=0}^{k} \sigma_i g_i$ a *SOS-certificate for $f \in Q(\boldsymbol{g})$*. The sets $Q(\boldsymbol{g})$ and $Q(\boldsymbol{g})[d]$ depend on the polynomials $\boldsymbol{g}$ in the description of K. Denoted by $Q(g)_d := Q(\boldsymbol{g}) \cap \mathbb{R}[\boldsymbol{x}]_{\leq d}$, by construction one has $Q(\boldsymbol{g})[d] \subset Q(\boldsymbol{g})_d$ but, in general, this inclusion is strict: in other words, for some $\boldsymbol{g}$ there exists a polynomial $f \in Q(\boldsymbol{g})$, of degree d, such that in any certificate $f = \sum_{i=0}^{k} \sigma_i g_i$, at least one product $\sigma_i g_i$ has degree $> d$.

It is not even true that $Q(\boldsymbol{g})_d \subset Q(\boldsymbol{g})[D]$ for possibly large D: these quadratic modules are called stable.

Definition 1 ([21, Sec. 4.1]) *For $d \in \mathbb{N}$, a quadratic module $Q(\boldsymbol{g})$ is called* stable in degree *d if there exists D such that $Q(\boldsymbol{g})_d \subset Q(\boldsymbol{g})[D]$. It is called* stable *if it is stable in every $d \in \mathbb{N}$ (we call the function $D = D(d)$ a* stability function *for $Q(\boldsymbol{g})$).*

Stability in a given degree depends on the generators $\boldsymbol{g}$ whereas stability depends only on the quadratic module $Q(\boldsymbol{g})$ and is equivalent to the existence of degree bounds for the representation $f = \sum_i \sigma_i g_i \in Q(\boldsymbol{g})$ that only depend on the degree of f, see for instance [23]. One example of stable quadratic module is the cone $\Sigma_{n,2d} = Q(0)_{2d}$: indeed, every polynomial in $\Sigma_{n,2d}$ is a sum of squares of polynomials of degree at most d, that is, $Q(0)_{2d} = Q(0)[2d]$ and hence $D(2d) = D(2d+1) = 2d$ is a stability function for Σ_n.

As well as $\Sigma_{n,2d}$, truncated quadratic modules are *semidefinite representable sets*, that is linear images of feasible sets of SDP problems (also known as projected spectrahedra or spectrahedral shadows in the literature): given a description $\boldsymbol{g}$ for $K = S(\boldsymbol{g})$, computing one polynomial in $Q(\boldsymbol{g})[D]$ amounts to solving a single SDP problem (*cf.* Section 3.3).

Definition 2 ([28]) *A quadratic module $Q(\boldsymbol{g})$ is called archimedean if there exists $u \in Q(\boldsymbol{g})$ such that $S(u)$ is compact.*

Remark that if $Q(\boldsymbol{g})$ is archimedean, then $S(\boldsymbol{g}) \subset S(u)$ thus $S(\boldsymbol{g})$ is compact. Archimedeanity and stability are often mutually exclusive properties, indeed, for $n \geq 2$, an archimedean quadratic module is not stable.

Theorem 1 (Putinar's Positivstellensatz [28]) *Let $K = S(\boldsymbol{g})$ be non empty, and assume $Q(\boldsymbol{g})$ is archimedean. Then every polynomial positive on K belongs to $Q(\boldsymbol{g})$.*

The problem of bounding the degree D of the summands in a Putinar certificate $f = \sum_{i=0}^{k} \sigma_i g_i$ for a polynomial $f \in \mathscr{P}(K)_d$, is called the *effective* Putinar Positivstellensatz, see [24, 1]. The work [1] gives a bound for D as a function of d, n, of the polynomial f and of geometrical parameters of K, see [1, Th. 1.7], *cf.* Section 4.

2.2 Moments

A *nonnegative Borel measure* (below *measure*, for short) μ is a bounded nonnegative linear functional on the σ-algebra of Borel sets $\mathscr{B}(\mathbb{R}^n)$. The *support* of μ is the complement of the largest open Borel set $A \in \mathscr{B}(\mathbb{R}^n)$ such that $\mu(A) = 0$, denoted by $\operatorname{supp}(\mu)$.

Let $K \subset \mathbb{R}^n$ be a Euclidean closed set. A measure μ is *supported* on K if $\operatorname{supp}(\mu) \subset K$ (in particolar it satisfies $\mu(\mathbb{R}^n \setminus K) = 0$). For $\boldsymbol{u} \in K$, we denote by $\delta_{\boldsymbol{u}}$ the Dirac measure supported on the singleton $\{\boldsymbol{u}\}$. A finite linear combinations $\sum_{i=1}^{s} c_i \delta_{\boldsymbol{u}_i}$ of s Dirac measures is called s-*atomic*: its support is $\operatorname{supp}(\sum_{i=1}^{s} c_i \delta_{\boldsymbol{u}_i}) = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_s\}$.

For $\boldsymbol{\alpha} \in \mathbb{N}^n$, the *(monomial) moment of exponent* $\boldsymbol{\alpha}$ of μ is the real number $\int_K \boldsymbol{x}^{\boldsymbol{\alpha}} \, \mathrm{d}\mu(\boldsymbol{x})$ as in (2). We say that μ satisfying (2) is a *representing measure* for the sequence $\boldsymbol{y} = (y_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \mathbb{N}^n_d}$. If K is compact, the Stone-Weierstrass Theorem implies that a measure is uniquely determined by its (infinite-dimensional) sequence of monomial moments, see [21, Cor. 3.3.1].

In this work, we address the following inverse problem for semialgebraic sets:

Problem 1 (Truncated Moment Problem [33, Ch. 17-18]) *Let $K \subset \mathbb{R}^n$ be a basic closed semialgebraic set. Given a finite sequence $\boldsymbol{y} = (y_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \mathbb{N}^n_d}$ of real numbers, determine whether $\boldsymbol{y}$ admits a representing measure supported on K.*

For $\boldsymbol{y} = (y_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha}\in\mathbb{N}^n}$, the matrix $M_d(\boldsymbol{y}) = (y_{\boldsymbol{\alpha}+\boldsymbol{\beta}})_{\boldsymbol{\alpha},\boldsymbol{\beta}\in\mathbb{N}^n_d}$ is called the *moment matrix of order* d of $\boldsymbol{y}$. We recall that we denote by $\mathscr{L}_{\boldsymbol{y}} : \mathbb{R}[\boldsymbol{x}]_{\leq d} \to \mathbb{R}$ the *Riesz functional associated with* $\boldsymbol{y}$, defined by $\mathscr{L}_{\boldsymbol{y}}(\boldsymbol{x}^{\boldsymbol{\alpha}}) = y_{\boldsymbol{\alpha}}$ and extended linearly on $\mathbb{R}[\boldsymbol{x}]_{\leq d}$.

Let now $K = S(\boldsymbol{g})$ be a basic closed semialgebraic set, and let

$$\mathscr{M}(K)_d = \Big\{\boldsymbol{y} = (y_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha}\in\mathbb{N}^n_d} \in \mathbb{R}^m : \exists\, \mu, \operatorname{supp}(\mu) \subset K, \\ \forall \boldsymbol{\alpha} \in \mathbb{N}^n_d,\, y_{\boldsymbol{\alpha}} = \int_K \boldsymbol{x}^{\boldsymbol{\alpha}} d\mu(\boldsymbol{x})\Big\}$$

denote the set of moments of order up to d of nonnegative Borel measures with support in K. The set $\mathscr{M}(K)_d$ is in general not closed, as shown by the following example.

Example 1 ([7, Rem. 3.147]) *Let $n = 1, d = 4$ and $\boldsymbol{y} = (1, 0, 0, 0, 1)$. Its second moment matrix $M_2(\boldsymbol{y})$ is positive semidefinite but the vector $\boldsymbol{y}$ is not representable by a nonnegative univariate measure, indeed $y_2 = 0$ but $y_4 \neq 0$. Thus $\boldsymbol{y} \notin \mathscr{M}(\mathbb{R})_4$. Nevertheless $\boldsymbol{y} \in \overline{\mathscr{M}(\mathbb{R})_4}$, the Euclidean closure of $\mathscr{M}(\mathbb{R})_4$: indeed $\boldsymbol{y} = \lim_{\epsilon\to 0} \boldsymbol{y}_\epsilon$ where $\boldsymbol{y}_\epsilon = (1, 0, \epsilon^2, 0, 1)$ is the sequence of moments of degree ≤ 4 of the $3-$atomic measure*

$$\mu_\epsilon = \frac{\epsilon^4}{2}\left(\delta_{\frac{1}{\epsilon}} + \delta_{-\frac{1}{\epsilon}}\right) + (1 - \epsilon^4)\delta_0$$

□

Let $V^\vee$ be the dual vector space of a real vector space V, that is the set of $\mathbb{R}$-linear functionals $L : V \to \mathbb{R}$. If $C \subset V$ is a convex cone, the set $C^* = \{L \in V^\vee : L(\boldsymbol{a}) \geq 0,\, \forall \boldsymbol{a} \in C\}$ is called the dual cone of C. It is straightforward to see that $\mathscr{M}(K)_d \subset \mathscr{P}(K)^*_d$, and a non-trivial result is that equality holds for K compact:

Theorem 2 (Tchakaloff's Theorem [35]) *Let $K \subset \mathbb{R}^n$ be compact and $d \in \mathbb{N}$. Then*

$$\mathscr{M}(K)_d = \mathscr{P}(K)^*_d = \{\boldsymbol{y} \in \mathbb{R}^m : \mathscr{L}_{\boldsymbol{y}}(p) \geq 0,\, \forall p \in \mathscr{P}(K)_d\}.$$

Theorem 2 is a finite-dimensional version of the Riesz-Haviland Theorem [9]. It is often used in the moment-SOS hierarchy, see [13, Lemma 1.7]. A modern statement and proof can be found *e.g.* in [19, Theorem 5.13], see also [4].

3 An algorithm for the moment problem

We describe an algorithm based on semidefinite programming that solves Problem 1 for compact basic semialgebraic sets.

To do that, we first give a characterization of the interior of cones of nonnegative polynomials on compact sets $K \subset \mathbb{R}^n$ (Section 3.1). Next we interpret Problem 1 as a conic feasibility problem and prove that its solvability is related to the feasibility type of the program (Section 3.2). Finally we describe our algorithm in Section 3.3.

3.1 Interior of $\mathscr{P}(K)_d$

Let $K \subset \mathbb{R}^n$ be non-empty. For $f \in \mathbb{R}[\boldsymbol{x}]$, we denote by $f^* := \inf_{x \in K} f(x)$, possibly $-\infty$.

It is straightforward to construct examples of positive polynomials $f \in \mathscr{P}(K)$, on a non-compact set K, such that $f \notin \operatorname{Int}(\mathscr{P}(K))$ even if $f^* > 0$ (for instance $1 = \lim_{\epsilon \to 0} 1 - \epsilon x$ so $1 \notin \operatorname{Int}(\mathscr{P}(\mathbb{R})_2)$). More generally, positive sum-of-squares polynomials of degree $< d$ lie in the boundary of the cone of nonnegative polynomials of degree $\leq d$ (*cf.* [7, §4.4.3]).

The next folklore lemma shows that, for compact sets, the interior of $\mathscr{P}(K)_d$ is exactly the set of positive polynomials over K.

Lemma 1 *Let $K \subset \mathbb{R}^n$ be non-empty, and let $d \in \mathbb{N}$. Then Int($\mathscr{P}(K)_d$) $\subset \{f \in \mathbb{R}[\boldsymbol{x}]_{\leq d} : f^* > 0\}$. If K is compact, equality holds, and Int($\mathscr{P}(K)_d$) consists of exactly those polynomials in $\mathbb{R}[\boldsymbol{x}]_{\leq d}$ that are positive on K.*

Proof: If $f \in \mathbb{R}[\boldsymbol{x}]_{\leq d}$ is such that $f^* \leq 0$, then $(f - \epsilon)^* = f^* - \epsilon < 0$ for all $\epsilon > 0$, thus $f - \epsilon \notin \mathscr{P}(K)_d$ for all $\epsilon > 0$, hence $f \notin \operatorname{Int}(\mathscr{P}(K)_d)$, which proves the sought inclusion $\subset$.

Now assume K is compact, and let $f \notin \operatorname{Int}(\mathscr{P}(K)_d)$. Then f is in the closure of the complement of $\mathscr{P}(K)_d$ in $\mathbb{R}[\boldsymbol{x}]_{\leq d}$, that is, f is the pointwise limit $f = \lim_{k \to \infty} f_k$ of polynomials $f_k \notin \mathscr{P}(K)_d$, in particular, satisfying $f_k^* < 0$ for all k. Since K is compact, $f_k^* = \min_{x \in K} f_k(x) = f_k(x_k)$ for some $x_k \in K$. Let $\overline{x} \in K$ be a limit point of $\{x_k\}_k$, which exists by Bolzano-Weierstrass Theorem. Thus up to extracting a subsequence, one has $0 \geq \lim_k f_k^* = \lim_k f_k(x_k) = f(\overline{x}) \geq f^*$, which shows the inclusion $\supset$, thus the equality $\operatorname{Int}(\mathscr{P}(K)_d) = \{f \in \mathbb{R}[\boldsymbol{x}]_{\leq d} : f^* > 0\}$. Since the infimum of a polynomial function on a compact set is its minimum, one has $f^* > 0$ if and only if $\min_{x \in K} f(x) > 0$ if and only if f is positive on K, as claimed. □

Remark 1 *Theorem 1 and Lemma 1 ensure that if $Q(\boldsymbol{g})$ is archimedean, then Int($\mathscr{P}(K)_d$) $\subset Q(\boldsymbol{g}) \cap \mathbb{R}[\boldsymbol{x}]_{\leq d} \subset \mathscr{P}(K)_d$. Thus under this assumption, [1, Th. 1.7] yields a degree bound $D = D(d, n, f, K)$ such that if $f \in$ Int($\mathscr{P}(K)_d$) then $f \in Q_D(\boldsymbol{g})$. Since $Q_D(\boldsymbol{g})$ is semidefinite representable, it can be sampled through semidefinite programming: solving such optimization problem yields an element of the boundary of $Q_D(\boldsymbol{g})$, thus this might not be sufficient to compute an element of Int($\mathscr{P}(K)_d$).*

The following Corollary shows that one can get elements of $\operatorname{Int}(\mathscr{P}(K)_d)$ as well through semidefinite programming, from the knowledge of a polynomial description $\boldsymbol{g}$ of K.

Corollary 1 *Let $\boldsymbol{g}$ be such that $Q(\boldsymbol{g})$ is archimedean, and let $K = S(\boldsymbol{g})$. Let $f \in$ Int($\mathscr{P}(K)_d$) and $0 < \delta < f^* = \min_K f$. Then $\frac{1}{\delta} f - 1 \in$ Int($\mathscr{P}(K)_d$) and there exist $\sigma_0^\delta, \sigma_1^\delta, \ldots, \sigma_k^\delta \in \Sigma_n$ such that*

$$\frac{1}{\delta} f - 1 = \sigma_0^\delta + \sum_i \sigma_i^\delta g_i.$$

Proof: The polynomial $f - \delta$ is positive on K, thus by Lemma 1, $f - \delta \in \mathrm{Int}(\mathscr{P}(K)_d)$ and hence $(f-\delta)/\delta = \frac{1}{\delta} f - 1 \in \mathrm{Int}(\mathscr{P}(K)_d)$, since $\mathrm{Int}(\mathscr{P}(K)_d)$ is a cone. Since $\frac{1}{\delta} f - 1$ is positive on K, we conclude by Theorem 1. $\square$

Corollary 1 can be rephrased as follows: if $Q(\boldsymbol{g})$ is archimedean and $0 < \delta < f^* = \min_K f$, then $f/\delta \in 1 + Q(\boldsymbol{g})$. Remark that (unless $Q(\boldsymbol{g})$ is stable in the degree of f) the degrees of the SOS-multipliers for a SOS-certificate $f/\delta \in 1 + Q(\boldsymbol{g})$ depend on δ and might be larger than the degrees for a SOS-certificate $f \in Q(\boldsymbol{g})$.

3.2 Moment problem as conic feasibility

Let $C \subset V$ be a convex cone with non-empty interior, and let $L \subset V$ be an affine space. The *conic program* associated with C and L is called *feasible* if $L \cap C \neq \emptyset$, otherwise *infeasible*. It is called *strongly feasible* if $L \cap \mathrm{Int}(C) \neq \emptyset$, and *weakly feasible* if it is feasible but not strongly.

If L is a linear space (that is if $0 \in L$) then $\{0\} \subset (L \cap C)$, thus $L \cap C$ is always feasible. If L is a hyperplane, then the corresponding program is weakly feasible if and only if $L \cap C$ is a proper face of C and in this case L is called a *supporting hyperplane* for C: geometrically, C is contained in one of the two closed half-spaces bounded by L, and L is tangent to the boundary of C.

Proposition 1 *Let $\boldsymbol{y} = (y_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \mathbb{N}^n_d} \in \mathbb{R}^m$, $m = \binom{n+d}{d}$ with $\boldsymbol{y}_0 > 0$. Let $\mathscr{L}_{\boldsymbol{y}} \in (\mathbb{R}[\boldsymbol{x}]_{\leq d})^\vee$ be the Riesz functional of $\boldsymbol{y}$, and $L_{\boldsymbol{y}} = \{p \in \mathbb{R}[\boldsymbol{x}]_{\leq d} : \mathscr{L}_{\boldsymbol{y}}(p) = 0\}$. Let $K = S(\boldsymbol{g}) \subset \mathbb{R}^n$. The following are equivalent:*

- A_1. *$\boldsymbol{y} \in \mathscr{M}(K)_d$;*
- A_2. *The conic program $L_{\boldsymbol{y}} \cap \mathscr{P}(K)_d$ is weakly feasible;*
- A_3. *There exist $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_s \in K$, with $s \leq m$, such that $\boldsymbol{y}$ admits a representing measure μ with supp$(\mu) = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_s\}$ and $L_{\boldsymbol{y}} \cap \mathscr{P}(K)_d = \{p \in \mathscr{P}(K)_d : p(\boldsymbol{u}_1) = 0, \ldots, p(\boldsymbol{u}_s) = 0\}$.*

Moreover, the following are equivalent and are strong alternatives to A_1-A_2-A_3:

- B_1. *$\boldsymbol{y} \notin \mathscr{M}(K)_d$;*
- B_2. *The conic program $L_{\boldsymbol{y}} \cap \mathscr{P}(K)_d$ is strongly feasible.*

Proof: The fact that A_1 and B_1 are strong alternatives is obvious, and the fact that the program $L_{\boldsymbol{y}} \cap \mathscr{P}(K)_d$ is always feasible (indeed, $L_{\boldsymbol{y}}$ is linear) implies that A_2 and B_2 are strong alternatives. Hence we only have to prove the equivalence of A_1, A_2 and A_3.

We first prove that A_1 is equivalent to A_3. For $\boldsymbol{u} \in K$, denote by $\lambda_{\boldsymbol{u}} = (\boldsymbol{u}^{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \mathbb{N}^n_d} \in \mathscr{M}(K)_d$ the sequence of moments of order $\leq d$ of the Dirac measure $\delta_{\boldsymbol{u}}$. By [33, Th. 17.2], $\boldsymbol{y}$ admits a representing measure supported on K, if and only if it admits a representing atomic measure

$\mu = \sum_{i=1}^{s} c_i \delta_{\boldsymbol{u}_i}$, where $s \le \dim \mathbb{R}[\boldsymbol{x}]_{\le d} = \binom{n+d}{d}$ and for some $c_i > 0$ and $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_s \in K$. For every $p \in \mathbb{R}[\boldsymbol{x}]_{\le d}$, one deduces

$$\mathscr{L}_{\boldsymbol{y}}(p) = \int_K p \, d\mu = \sum_{i=1}^{s} c_i p(\boldsymbol{u}_i)$$

and thus $p \in L_{\boldsymbol{y}}$ if and only if $\sum_{i=1}^{s} c_i p(\boldsymbol{u}_i) = 0$: then for $p \in \mathscr{P}(K)_d$, we conclude that p must vanish on $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_s\}$. We deduce that A_1 and A_3 are equivalent.

We prove now that A_1 and A_2 are equivalent. By Theorem 2, we know that A_1 holds if and only if $\mathscr{L}_{\boldsymbol{y}}$ is non-negative over $\mathscr{P}(K)_d$: this is the case if and only if the cone $\mathscr{P}(K)_d$ is contained in the closed half-space $L_{\boldsymbol{y}}^+ = \{p \in \mathbb{R}[\boldsymbol{x}]_{\le d} : \mathscr{L}_{\boldsymbol{y}}(p) \ge 0\}$, and since $0 \in L_{\boldsymbol{y}}$, this is equivalent to $L_{\boldsymbol{y}}$ being a supporting hyperplane and the program being weakly feasible. □

When the conic program in Proposition 1 is weakly feasible, the set $L_{\boldsymbol{y}} \cap \mathscr{P}(K)_d$ is an exposed and proper face of $\mathscr{P}(K)_d$ defined by vanishing on the finite set defined in Item A_3. See also [5] and [7, Sec. 4.4]. On the contrary, if the conic program is strongly feasible, we give the following definition.

Definition 3 *Let $\boldsymbol{y} \notin \mathscr{M}(K)_d$. A polynomial $p \in L_{\boldsymbol{y}} \cap \mathrm{Int}(\mathscr{P}(K)_d)$ is called a unrepresentability certificate for $\boldsymbol{y}$ in K.*

Corollary 2 shows how to compute explicit unrepresentability certificates for Problem 1.

Corollary 2 *Assume that $Q(\boldsymbol{g})$ is archimedean and that conditions B_1-B_2 of Proposition 1 hold. There exists $p \in \mathrm{Int}(\mathscr{P}(K)_d)$ such that $p \in 1 + Q(\boldsymbol{g})$, $\mathscr{L}_{\boldsymbol{y}}(p) = 0$ and $p^* > 1$ is arbitrarily large.*

Proof: Property B_2 of Proposition 1 ensures that there exists $f \in L_{\boldsymbol{y}} \cap \mathrm{Int}(\mathscr{P}(K)_d)$, that is f is positive over K and $\mathscr{L}_{\boldsymbol{y}}(f) = 0$. Let $0 < \delta < f^*$, and let $p = \frac{1}{\delta} f \in \mathrm{Int}(\mathscr{P}(K)_d)$. From Corollary 1 we get that $p - 1 \in Q(\boldsymbol{g})$, that is, $p \in 1 + Q(\boldsymbol{g})$. Moreover $\mathscr{L}_{\boldsymbol{y}}(p) = \frac{1}{\delta}\mathscr{L}_{\boldsymbol{y}}(f) = 0$, and $p^* = f^*/\delta > 1$ is arbitrarily large. □

Remark 2 *If $\boldsymbol{y} \in \mathbb{Q}^m$, then p in Corollary 2 can be chosen with rational coefficients. Indeed, the hyperplane $L_{\boldsymbol{y}}$ is defined by an equation with rational coefficients, and $L_{\boldsymbol{y}} \cap \mathrm{Int}(\mathscr{P}(K)_d)$ is a non-empty open subset of $L_{\boldsymbol{y}}$, hence it contains a rational point f. Choosing $\delta \in \mathbb{Q}$ in the proof of Corollary 2 is thus sufficient to get a rational certificate.*

Nevertheless, let us recall from [31] that there exist polynomials in $\mathbb{Q}[\boldsymbol{x}]$, that are sums of squares as elements of $\mathbb{R}[\boldsymbol{x}]$ but not as elements of $\mathbb{Q}[\boldsymbol{x}]$. In our context, this means that the rational unrepresentability certificate p might not admit rational certificates of positivity showing that $p \in 1 + Q(\boldsymbol{g})$ (see also [22] for the existence of rational certificates in conic programming).

Any polynomial p as in Corollary 2 is such that $p - 1 \in Q(\boldsymbol{g})$. In particular, there exists $D > 0$ such that $p - 1 \in Q(\boldsymbol{g})[D]$, that is $p \in 1 + Q(\boldsymbol{g})[D]$. Bounds for D are given, *e.g.*, in [1, Th. 1.7]. Below we give a bound on D as a function of the input of Algorithm 1, see Definition 4 and Section 4.

The following example shows that the certificate of Corollary 2 might exist in non-archimedean contexts.

Example 2 *The vector $\boldsymbol{y} = (1, 1, 0)$ is not a univariate moment vector (indeed the moment matrix $M_1(\boldsymbol{y}) = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ is not positive semidefinite). Remark that $\mathbb{R} = S(0)$ and $Q(0) = \Sigma_n$ is not archimedean, but an unrepresentability certificate in the spirit of Corollary 2 exists. Indeed $\mathscr{L}_{\boldsymbol{y}}(p_0 + p_1 x + p_2 x^2) = p_0 + p_1$ and the following identity holds for all $p \in L_{\boldsymbol{y}}$:*

$$p_0 - p_0 x + p_2 x^2 = 1 + \begin{pmatrix} 1 & x \end{pmatrix} \begin{pmatrix} p_0 - 1 & -\frac{p_0}{2} \\ -\frac{p_0}{2} & p_2 \end{pmatrix} \begin{pmatrix} 1 \\ x \end{pmatrix}.$$

The identity is a SOS-certificate for $p \in 1 + Q(\boldsymbol{g})$ if and only if the Gram matrix on the right hand side is positive semidefinite. This yields a spectrahedral representation of the set of unrepresentability certificates of $\boldsymbol{y}$:

$$\left\{ p \in \mathbb{R}[\boldsymbol{x}]_{\leq 2} : p_1 = -p_0, \left(\begin{smallmatrix} p_0 - 1 & -\frac{p_0}{2} \\ -\frac{p_0}{2} & p_2 \end{smallmatrix}\right) \succeq 0 \right\}$$

For instance the polynomial $p = 2 - 2x + x^2 = 1 + (1 - x)^2 \in (1 + Q(0)) \cap L_{\boldsymbol{y}}$.

We remark that the existence of such p implies $\boldsymbol{y} \notin \mathscr{M}(\mathbb{R})_2$. Indeed, if $\boldsymbol{y} \in \mathscr{M}(\mathbb{R})_2$, then by A_3 of Proposition 1, there would exist a representing measure with finite support, thus one would have $\boldsymbol{y} \in \mathscr{M}([-R, R])_2$ for some $R > 0$. Now, since $1 + Q(0) \subset 1 + Q(R^2 - x^2)$ for every $R > 0$, we deduce that $p \in 1 + Q(R^2 - x^2)$, thus $p \in Int(\mathscr{P}([-R, R])_2)$ (according to Lemma 1) and thus $\boldsymbol{y} \notin \mathscr{M}([-R, R])_2$, for every $R > 0$ (by B_2, Proposition 1). □

The polynomial p in Example 2, together with its positivity certificate $1 + (1 - x)^2$, allows to check rigourously the unrepresentability of $\boldsymbol{y} = (1, 1, 0)$. Nevertheless, in general the archimedianity hypothesis cannot be dropped, as shown in Example 3.

Example 3 *Let $\boldsymbol{y} = (1, 0, 0, 0, 1)$ be the vector of Example 1, with $\boldsymbol{g} = 0$. The semidefinite program in Corollary 2 is infeasible: indeed $Q(0) = \Sigma_n$ and it is easy to check that there is no polynomial $p = \sum_{i=0}^{4} p_i x^i$ satisfying*

$$\begin{aligned} \mathscr{L}_{\boldsymbol{y}}(p) = p_0 + p_4 = 0 \\ p = 1 + \begin{pmatrix} 1 & x & x^2 \end{pmatrix} X \begin{pmatrix} 1 & x & x^2 \end{pmatrix}^T \\ X \succeq 0. \end{aligned}$$

Indeed, the constraints imply that $p_4 = -p_0 = -(1 + X_{11}) < 0$, thus p is negative at infinity, in particular, $p \notin \mathscr{P}(\mathbb{R})$.

Nevertheless for every $R > 0$, with $\boldsymbol{g} = (R - x, R + x)$, Corollary 2 ensures that there exists $p_R \in 1 + Q(R - x, R + x)$ such that $\mathscr{L}_{\boldsymbol{y}}(p_R) = 0$, that certifies that $\boldsymbol{y} \notin \mathscr{M}([-R, R])_4$: the polynomial p_R is any solution of the following parametric linear matrix inequality with $\sigma_0, \sigma_1, \sigma_2 \in \Sigma_1$:

$$p_0 + p_1 x + p_2 x^2 + p_3 x^3 - p_0 x^4 = 1 + \sigma_0 + \sigma_1 (R - x) + \sigma_2 (R + x).$$

The fact that $\boldsymbol{g} = (R - x, R + x)$ *is the natural description of* $[-R, R]$ *(see [21, Sec. 2.7]) implies that* $Q(\boldsymbol{g})$ *is stable, with stability function* $D(d) = d$ *(see e.g. [33, Prop. 3.3]), and hence one can assume* $\sigma_0 \in \Sigma_{1,4}$ *and* $\sigma_1, \sigma_2 \in \Sigma_{1,2}$. □

We terminate this series of examples with a bivariate one.

Example 4 *Let* $n = 2, d = 6$ *and let* $\boldsymbol{y} = (y_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \mathbb{N}_6^2}$ *be the vector in* $\mathbb{R}^{28}$ *whose non-zero entries are*

$$\begin{aligned} y_{00} &= 32 & y_{22} &= 30 \\ y_{20} = y_{02} &= 34 & y_{60} = y_{06} &= 128 \\ y_{40} = y_{04} &= 43 & y_{42} = y_{24} &= 28. \end{aligned}$$

We claim that there is no nonnegative Borel measure supported on the unit ball $K = \{\boldsymbol{a} = (a_1, a_2) \in \mathbb{R}^2 : a_1^2 + a_2^2 \leq 1\}$ *whose moments up to degree 6 agree with* $\boldsymbol{y}$. *Remark that the semialgebraic set* $K = S(1 - x_1^2 - x_2^2)$ *is compact and* $Q(1 - x_1^2 - x_2^2)$ *is archimedean, in particular it is not stable. We give below in Example 5 an unrepresentability certificate of small degree certifying that* $\boldsymbol{y} \notin \mathscr{M}(K)_d$, *proving our claim.* □

3.3 SDP-based algorithm

The results of Section 3.2 yield the following alternatives for Problem 1. Given $\boldsymbol{y} = (\boldsymbol{y}_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \mathbb{N}_d^n}$ and $K = S(\boldsymbol{g})$, according to Proposition 1:

- either $\boldsymbol{y} \notin \mathscr{M}(K)_d$, in which case a certificate of unrepresentability is given by a polynomial $p \in \mathrm{Int}(\mathscr{P}(K)_d)$ such that $\mathscr{L}_{\boldsymbol{y}}(p) = 0$ (Corollary 2)
- or $\boldsymbol{y} \in \mathscr{M}(K)_d$, in which case there exists an atomic measure $\mu = \sum_{i=1}^s c_i \delta_{\boldsymbol{u}_i}$ representing $\boldsymbol{y}$ (Property A_3 in Proposition 1).

We describe our main algorithm.

Algorithm 1 certify_moment

Input:

- $n, d \in \mathbb{N}$
- *A vector* $\boldsymbol{y} \in \mathbb{R}^m$, *with* $m = \binom{n+d}{d}$
- *Polynomials* $\boldsymbol{g} = (g_1, \ldots, g_k) \in \mathbb{R}[\boldsymbol{x}]^k$
- *A threshold* $D \in \mathbb{N}$

Output:

- *Either* (p, Σ) *where* $p \in \mathbb{R}[\boldsymbol{x}]_{\leq d}$ *satisfies Corollary 2, and* $\Sigma \in \Sigma_n^{k+1}$ *is a certificate for* $p \in 1 + Q(\boldsymbol{g})[D]$
- *or a measure* $\mu = \sum c_i \delta_{\boldsymbol{u}_i}$ *satisfying* A_3 *in Proposition 1*

1: $(p, \Sigma) \leftarrow$ **find_certificate**$(n, d, \boldsymbol{y}, \boldsymbol{g}, D)$
2: ***if*** $p \neq []$ ***then return*** (p, Σ)
3: ***return*** **find_measure**$(n, d, \boldsymbol{y}, \boldsymbol{g})$

Algorithm 1 depends on two subroutines. The first one, **find_certificate** at Step 1, returns, if it exists, an unrepresentability certificate $p \in \mathbb{R}[\boldsymbol{x}]_{\leq d}$ for $\boldsymbol{y}$, together with a SOS-certificate for p as element of $1 + Q(\boldsymbol{g})[D]$.

Algorithm 2 find_certificate

```
1: p ← [], Σ ← [], g_0 ← 1
2: Find p ∈ R[x]_{≤d} and σ_0, σ_1, ..., σ_k ∈ Σ_n such that
     • L_y(p) = 0
     • p = 1 + Σ_{i=0}^{k} σ_i g_i, deg(σ_i g_i) ≤ D
3: Σ ← [σ_0, σ_1, ..., σ_k]
4: return (p, Σ)
```

Algorithm 2 can be performed by solving one (finite-dimensional) SDP feasibility program whose unknowns are $p, \sigma_0, \sigma_1, \ldots, \sigma_k$. First, the constraint $\mathscr{L}_{\boldsymbol{y}}(p) = 0$ is linear in p. Next, denoting $\delta_i = \lfloor (D - \deg(g_i))/2 \rfloor$, the constraints $\sigma_i \in \Sigma_n$ and $\deg(\sigma_i g_i) \leq D$ are equivalent to the existence of a symmetric matrix $X_i \succeq 0$, of size $\binom{\delta_i+n}{n}$, such that $\sigma_i = v^T X_i v$, where v is a linear basis of $\mathbb{R}[\boldsymbol{x}]_{\delta_i}$. Finally the constraint $p = 1 + Q(\boldsymbol{g})[D]$ in Step 2 is affine linear in p and in the entries of $X_0, X_1, \ldots, X_k$. We give upper bounds for the value of D in Section 4.

The second routine, **find_measure**, is called if and only if Algorithm 1 reaches Step 3. It returns a s-atomic measure representing the vector $\boldsymbol{y}$, for some $s \leq \binom{n+d}{d}$.

Algorithm 3 find_measure

```
s = 1
while s ≤ binom(n+d, d) do
    Find c ∈ R^s and U = (u_1, ..., u_s) ∈ (R^n)^s s.t.
     • u_1, ..., u_s ∈ S(g)
     • c_1 u_1^α + ··· + c_s u_s^α = y_α for all α ∈ N^n_d
    if solution exists then return (c, U)
    s ← s + 1
```

The routine **find_measure** can be performed by existing algorithms computing one point per connected component of basic semialgebraic sets applied to the set of elements $(\boldsymbol{c}, \boldsymbol{U}) \in \mathbb{R}^s \times (\mathbb{R}^n)^s$ satisfying the inequalities defining K and the polynomial equations $\sum_i c_i \boldsymbol{u}_i^{\boldsymbol{\alpha}} = y_{\boldsymbol{\alpha}}$, $\boldsymbol{\alpha} \in \mathbb{N}^n_d$. The equations have a multivariate Vandermonde structure. A precise complexity analysis of **find_measure** is left to future work.

We define now an integer function of the input of Problem 1.

Definition 4 *Let $K = S(\boldsymbol{g})$ and $\boldsymbol{y} \notin \mathscr{M}(K)_d$. The* unrepresentability degree *of $\boldsymbol{y}$ in K is the minimum integer $D = D(n, d, \boldsymbol{y}, \boldsymbol{g})$ such that there exists $p \in 1 + Q(\boldsymbol{g})[D]$ satisfying*

$\mathscr{L}_{\boldsymbol{y}}(p) = 0$.

The unrepresentability degree is well defined, according to Corollary 2. We prove the correctness of Algorithm 1.

Theorem 3 (Correctness) *Let $\boldsymbol{y} = (y_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha}\in\mathbb{N}^n_d}$, and let $\boldsymbol{g} = (g_1, \ldots, g_k) \in \mathbb{R}[\boldsymbol{x}]^k$ be such that $Q(\boldsymbol{g})$ is archimedean. There exists $D = D(n, d, \boldsymbol{y}, \boldsymbol{g}) \in \mathbb{N}$ such that Algorithm 1 with input $(n, d, \boldsymbol{y}, \boldsymbol{g}, D)$ terminates and is correct.*

Proof: Let $K = S(\boldsymbol{g})$. Since $Q(\boldsymbol{g})$ is archimedean, K is compact and by Lemma 1, $\mathrm{Int}(\mathscr{P}(K)_d) = \{p \in \mathbb{R}[\boldsymbol{x}]_{\leq d} : p(\boldsymbol{a}) > 0, \forall\, \boldsymbol{a} \in K\}$. By Theorem 1, if a polynomial is positive on K, then it belongs to $Q(\boldsymbol{g})$. We deduce that $\mathrm{Int}(\mathscr{P}(K)_d) \subset Q(\boldsymbol{g}) \cap \mathbb{R}[\boldsymbol{x}]_{\leq d} \subset \mathscr{P}(K)_d$.

We claim that for $D \in \mathbb{N}$ large enough, then $\boldsymbol{y} \notin \mathscr{M}(K)_d$ if and only if **certify_moment** returns a polynomial p at Step 2, that is, if and only if the semidefinite program at Step 1 is feasible.

Assume $\boldsymbol{y} \notin \mathscr{M}(K)_d$ and let D the unrepresentability degree of $\boldsymbol{y}$ in K. By Corollary 2, there exists a polynomial $p \in 1 + Q(\boldsymbol{g})[D] \subset \mathrm{Int}(\mathscr{P}(K)_d)$, such that $\mathscr{L}_{\boldsymbol{y}}(p) = 0$. In other words, **find_certificate** returns (p, Σ) with $p \neq []$, and hence Algorithm 1 returns its output at Step 2.

For the reverse implication, suppose that the semidefinite program at Step 1 is feasible for some degree D. Let $p \in \mathbb{R}[\boldsymbol{x}]_{\leq d}$ be a solution of such program. Then $p = 1 + q$ for some $q \in Q(\boldsymbol{g})[D]$, in particular, $p^* \geq 1$ on K, that is, p is positive on K. Since $\mathscr{L}_{\boldsymbol{y}}(p) = 0$, and by compactness of K, one has $p \in \mathrm{Int}(\mathscr{P}(K)) \cap L_{\boldsymbol{y}}$ and again applying Proposition 1 one concludes $\boldsymbol{y} \notin \mathscr{M}(K)_d$. This proves the claim.

Finally, remark that this also shows that $\boldsymbol{y} \in \mathscr{M}(K)_d$ if and only if **certify_moment** reaches Step 3. If this is the case, **find_measure** computes the support and the weights of an s-atomic measure representing $\boldsymbol{y}$: such measure exists for some $s \leq \binom{n+d}{d}$, according to Proposition 1. □

4 Bound on the unrepresentability degree

A priori bounds on the degree of Putinar certificates that only depend on the degree of the polynomial exist for stable quadratic modules. Nevertheless, stability and archimedeanity properties are mutually exclusive in dimension $n \geq 2$.

In this section we give general bounds for the unrepresentability degree of a vector $\boldsymbol{y} \notin \mathscr{M}(K)_d$ in a compact basic semialgebraic set $K = S(\boldsymbol{g})$. A key ingredient to do this is the use of already existing quantitative analysis of computer algebra algorithms performing quantifier elimination over the reals.

We first recall the following bound on the degree of a Putinar representation of a polynomial in $\mathrm{Int}(\mathscr{P}(K)_d)$, for an archimedean quadratic module $Q(\boldsymbol{g})$, given in [1]. Let

$f \in \mathrm{Int}(\mathscr{P}(K)_d)$. We denote by $\epsilon(f) := f^*/\|f\|$ where

$$f^* = \min_{\boldsymbol{a} \in K} f(\boldsymbol{a}) \qquad \text{and} \qquad \|f\| = \max_{\boldsymbol{a} \in [-1,1]^n} f(\boldsymbol{a}).$$

Under the following assumptions:

- $1 - \sum_i x_i^2 \in Q(\boldsymbol{g})$
- $\|g_i\| \leq \frac{1}{2}$ for all $i = 1, \ldots, k$

then by [1, Th. 1.7] there exists a function $\gamma = \gamma(n, \boldsymbol{g})$ such that $f \in Q(\boldsymbol{g})[D]$ for D of the order of

$$\gamma(n, \boldsymbol{g})\, d^{3.5\text{Ł}n}\, \epsilon(f)^{-2.5\text{Ł}n} \tag{3}$$

where $\mathfrak{c}$ and Ł are the Łojasiewicz coefficients as they are defined in [1, Def. 2.4].

Let now $(n, d, \boldsymbol{y}, \boldsymbol{g})$ be the input of Algorithm 1. We assume in the whole section that $\boldsymbol{y} \in \mathbb{Q}^N$, with $N = \binom{n+d}{d}$, that the basic semialgebraic set $K = S(\boldsymbol{g}) \subset \mathbb{R}^n$ is defined by polynomial inequalities $\boldsymbol{g} = (g_1, \ldots, g_k) \subset \mathbb{Q}[\boldsymbol{x}]^k$ and that $Q(\boldsymbol{g})$ is archimedean.

Assume $\boldsymbol{y} \notin \mathscr{M}(K)_d$, and let $p \in 1 + Q(\boldsymbol{g})$ satisfy $\mathscr{L}_{\boldsymbol{y}}(p) = 0$ and $p^* = 1 + m$ for some arbitrary constant $m > 0$. Such unrepresentability certificate exists by Corollary 2. From (3), one has that $p \in 1 + Q(\boldsymbol{g})[D]$ with D depending on

$$\epsilon(p-1) = \frac{p^* - 1}{\|p - 1\|} \geq \frac{1}{1 + \|p\|}$$

where the last inequality derives from Corollary 2 choosing without loss of generality $m = 1$. In the following, we provide an upper bound B on $\|p\|$: this will yield a lower bound on $\epsilon(p-1)$, hence an upper bound on D.

As already said, in order to do that, we consider the formulation in terms of quantifier elimination over the reals that solves the truncated moment problem in the sense of Proposition 1 and Corollary 2, and we use quantitative results on quantifier elimination over the reals from [3].

Consider the following formula with quantified variables $\boldsymbol{x} = (x_1, \ldots, x_n)$ and parameters the unknown coefficients $\{p_{\boldsymbol{\alpha}} : \boldsymbol{\alpha} \in \mathbb{N}^n_d\}$ of a polynomial $p \in \mathbb{R}^N$:

$$\mathscr{L}_{\boldsymbol{y}}(p) = 0 \;\; \wedge \;\; \left(\forall \boldsymbol{x} \in \mathbb{R}^n \quad \bigwedge_{i=1}^{k} g_i(\boldsymbol{x}) \geq 0 \Rightarrow p(\boldsymbol{x}) > 1 \right). \tag{4}$$

Lemma 2 *Let $S \subset \mathbb{R}^N$ be the semialgebraic set defined by the quantifier-free formula obtained from (4) after eliminating the quantified variables. Then S is an open subset of $L_{\boldsymbol{y}}$ with respect to the induced topology.*

Proof: For $p \in \mathbb{R}[\boldsymbol{x}]_{\leq d}$ and $A \subset \mathbb{R}[\boldsymbol{x}]_{\leq d}$, we denote by $p+A := \{p+q : q \in A\}$. Since $Q(\boldsymbol{g})$ is archimedean, K is compact and according to Lemma 1, $\mathrm{Int}(\mathscr{P}(K)_d)$ consists exactly of polynomials that are positive on K. Thus $S = L_{\boldsymbol{y}} \cap (1 + \mathrm{Int}(\mathscr{P}(K)_d))$. Moreover by Proposition 1, we know that $L_{\boldsymbol{y}} \cap \mathrm{Int}(\mathscr{P}(K)_d)$ is non-empty and open in $L_{\boldsymbol{y}}$. Now since $L_{\boldsymbol{y}}$ is a linear space intersecting $\mathrm{Int}(\mathscr{P}(K)_d)$, which is an open convex cone, so does the affine space $-1+L_{\boldsymbol{y}}$. Thus $T = (-1+L_{\boldsymbol{y}}) \cap \mathrm{Int}(\mathscr{P}(K)_d)$ is open in $-1+L_{\boldsymbol{y}}$ and hence $S = 1+T$ is open in $1+(-1+L_{\boldsymbol{y}}) = L_{\boldsymbol{y}}$. □

Observe that the constraint $\mathscr{L}_{\boldsymbol{y}}(p) = 0$ in (4) is linear in p and $\boldsymbol{y} \neq 0$. Thus one of the coefficients of p, say $p_{\boldsymbol{\alpha}'}$, can be eliminated, yielding an formulation of the quantifier elimination problem (4):

$$\forall \boldsymbol{x} \in \mathbb{R}^n \quad \bigwedge_{i=1}^{k} g_i(\boldsymbol{x}) \geq 0 \Rightarrow \tilde{p}(\boldsymbol{x}) > 1 \tag{5}$$

where $\tilde{p}$ is the polynomial obtained when substituting $p_{\boldsymbol{\alpha}'}$ in p by a linear form in the other coefficients $p_{\boldsymbol{\alpha}}$ using $\mathscr{L}_{\boldsymbol{y}}(p) = 0$. Below we abuse of notation and consider the set S defined in Lemma 2 and by the previous formulae as embedded in $L_{\boldsymbol{y}}$ identified with $\mathbb{R}^{N-1}$. We conclude that the set S has non-empty interior in $\mathbb{R}^{N-1}$.

We denote by

$$d_{\boldsymbol{g}} = \max_i \left\{ \deg(g_i), i = 1, \ldots, k \right\}$$

and by $\tau_{\boldsymbol{g}}$ the maximum bit size of the coefficients of the g_i's. Note that we can multiply in (5) the polynomials g_i by the (positive) least commun multiple of the denominators of their coefficients to obtain equivalent inequalities but with coefficients in $\mathbb{Z}$. These least common multiples have height bounded by $(\binom{n+d_{\boldsymbol{g}}}{n} + 1)\tau_{\boldsymbol{g}}$.

Further, we denote by $\tau_{\boldsymbol{y}}$ the maximum bit size of the coefficients of $\boldsymbol{y}$. As above, the equation $\mathscr{L}_{\boldsymbol{y}}(p) = 0$ can be rewritten with coefficients in $\mathbb{Z}$ of bit size bounded by $(N+1)\tau_{\boldsymbol{y}}$. We set

$$\tau = \max\left((N+1)\tau_{\boldsymbol{y}}, \left(\binom{n+d_{\boldsymbol{g}}}{n} \right) \tau_{\boldsymbol{g}} \right). \tag{6}$$

Note that τ is a bound on the integer coefficients of the polynomial constraints in (5) once we have multiplied each of them by the least common multiple of the denominators of their coefficients.

Finally, let $\delta = \max(d+1, d_{\boldsymbol{g}})$. Note that δ dominates the maximum degree of the polynomial constraints in (5), indeed, the polynomial $\tilde{p} \in \mathbb{R}[\boldsymbol{x}, p_{\boldsymbol{\alpha}} : \boldsymbol{\alpha} \in \mathbb{N}^n_d]$ has degree d in $\boldsymbol{x}$ and has degree 1 with respect to its unknown coefficients.

Proposition 2 *There exists $\tilde{p} \in S$ with $\|\tilde{p}\| \leq B$ for B in*

$$\tau^{O(1)} \left(k(\delta+1)\right)^{O(n(N-1))}.$$

Proof: We start by providing some quantitative bounds on the quantifier-free formula which defines $S \subset \mathbb{R}^{N-1}$ obtained by eliminating the quantified variables $\boldsymbol{x} = (x_1, \ldots, x_n)$ in (5). By [3, Theorem 14.16] such a formula satisfies the following properties

- It can be obtained with polynomials of degree lying in $(\delta+1)^{O(n)}$;
- the bit size of the coefficients of these polynomials lies in $\tau(\delta+1)^{O(n(N-1))}$;
- this formula is a disjunction of $k^{n+1}\delta^{O(n)}$ conjunctions of $k^{n+1}\delta^{O(n)}$ disjunctive formulas of polynomial inequalities involving $k^{n+1}\delta^{O(n)}$ polynomials.

Recall that since S is open, it coincides with its interior $\operatorname{Int}(S)$. We aim at computing one point with rational coordinates in S. To do this, we just put these disjunctions in closed form, replace non-strict inequalities by strict inequalities and call an algorithm for computing at least one point with rational coordinates in S; see e.g. [2, Theorem 4.1.2].

Note that the input to such an algorithm is a system of polynomial strict inequalities in $\mathbb{R}[p_{\boldsymbol{\alpha}} : \boldsymbol{\alpha} \in \mathbb{N}_d^n]$ of degree $(\delta+1)^{O(n)}$ with bit size coefficients in $\tau(\delta+1)^{O(n(N-1))}$. By [2, Theorem 4.1.2], if the semialgebraic set defined by the input is non-empty, then it outputs a point with rational coordinates of bit size bounded by $\tau^{O(1)}\left(k(\delta+1)\right)^{O(n(N-1))}$.

All in all, this bounds the bit size of the coefficients of some polynomial $\tilde{p} \in S$ (with rational coordinates). Since the number of these coefficients is $N-1$, the 2-norm of $\tilde{p}$ still lies in

$$\tau^{O(1)}\left(k(\delta+1)\right)^{O(n(N-1))}.$$

Finally, observe that $\|\tilde{p}\| = \min_{\boldsymbol{a}\in[-1,1]^n} \tilde{p}(\boldsymbol{a})$ is bounded above by the 2-norm of $\tilde{p}$. □

Corollary 3 *Let $\tau_{\boldsymbol{y}}$ and $\tau_{\boldsymbol{g}}$ bound the bit-size of $\boldsymbol{y}$ and $\boldsymbol{g}$, respectively, and let $d_{\boldsymbol{g}}$ be a bound on the degrees of $g_1, \ldots, g_k$. Let τ be as in (6) and $\delta = \max\{d+1, d_{\boldsymbol{g}}\}$. If $\boldsymbol{y} \notin \mathscr{M}(K)_d$, then the degree of unrepresentability of $\boldsymbol{y}$ in K is in*

$$\gamma(n,\boldsymbol{g})\, d^{3.5\text{Ł}n}\, \tau^{O(\text{Ł}n)}\, \left(k(\delta+1)\right)^{O(\text{Ł}n^2(N-1))}.$$

Proof: With the notation introduced in (3), by Corollary 2, there exists $p \in 1 + Q(\boldsymbol{g})[D]$ and by applying [1, Th. 1.7] and Proposition 2, the degree D is bounded above by

$$\begin{aligned}
&\gamma(n,\boldsymbol{g})\, d^{3.5\text{Ł}n}\, \epsilon(p-1)^{-2.5\text{Ł}n}\\
&\le \gamma(n,\boldsymbol{g})\, d^{3.5\text{Ł}n}\, (1+\|p\|)^{2.5\text{Ł}n}\\
&\le \gamma(n,\boldsymbol{g})\, d^{3.5\text{Ł}n}\, \left(\tau^{O(1)}\left(k(\delta+1)\right)^{O(n(N-1))}\right)^{2.5\text{Ł}n}\\
&= \gamma(n,\boldsymbol{g})\, d^{3.5\text{Ł}n}\, \tau^{O(\text{Ł}n)}\, \left(k(\delta+1)\right)^{O(\text{Ł}n^2(N-1))}
\end{aligned}$$

□

We terminate with a bivariate example showing that the bound of Corollary 3 is usually quite pessimistic.

Example 5 (Example 4 continued) *Let $\boldsymbol{y} \in \mathbb{R}^{28}$ be the vector defined in Example 4. Consider the polynomial*

$$p = 1 + \frac{8}{9}(1 - x_1^2 - x_2^2)$$

One checks that $p \in 1 + Q(1 - x_1^2 - x_2^2)$ and $\mathscr{L}_{\boldsymbol{y}}(p) = y_{00}(1+\frac{8}{9}) - \frac{8}{9}(y_{20}+y_{02}) = 0$. Since $K = S(1 - x_1^2 - x_2^2)$ is compact, p certifies that the conic program defined in Proposition 1 is strongly feasible, in other words, that $\boldsymbol{y} \notin \mathscr{M}(K)_d$. □

5 Conclusions and perspectives

The goal of this work was to undertake a systematic analysis of the computational complexity of the truncated moment problem on semialgebraic sets. Preliminary results concern the existence of algebraic certificates for vectors that are not representable as moments of measures, and upper bounds on the degree of SOS representations of these certificates.

Our contribution offers several challenges and research directions in the computational aspects of the truncated moment problem, let us mention a few. One of these is the need of efficient algorithms for classes of polynomial systems with Vandermonde structure as that defined in the routine **find_measure**.

A second one is to refine the quantifier-elimination bound given in Corollary 3. Unlike the viewpoint of the so-called effective Putinar Positivstellensatz introduced in [1], for which degree bounds depend on the polynomial itself, it is clear from our analysis that for the complexity analysis of the TMP one needs to give uniform degree bounds that only depend on the input of the TMP. One way of getting such uniform bounds is to consider manifestly positive polynomials such as those in $1 + Q(\boldsymbol{g})$ for compact $K = S(\boldsymbol{g})$.

A final perspective is to extend our analysis to the more general case of basic closed semialgebraic sets, not necessarily compact (see *e.g.* [6] and [4,]).

6 Acknowledgments

The authors thank Lorenzo Baldi for discussions concerning the degree bounds of SOS-certificates. This work is supported by the European Commission Marie Sklodowska-Curie Innovative Training Network POEMA (Polynomial Optimization, Efficiency through Moments and Algebra, 2019-2023); by the Agence Nationale de la Recherche (ANR), grant agreements ANR-18-CE33-0011 (SESAME), ANR-19-CE40-0018 (De Rerum Natura), ANR-21-CE48-0006-01 (HYPERSPACE); by the joint ANR-Austrian Science Fund FWF grant agreement ANR-19-CE48-0015 (ECARP); by the EOARD-AFOSR grant agreement FA8665-20-1-7029.

References

[1] L. Baldi, B. Mourrain. On the effective Putinar's Positivstellensatz and moment approximation. Mathematical Programming, 2022.

[2] S. Basu, R. Pollack, M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. Journal of the ACM 43(6):1002–1045, 1996.

[3] S. Basu, R. Pollack, M.-F. Roy. Algorithms in real algebraic geometry. 2nd Ed. Algorithms and Computation in Mathematics, Vol. 10, Springer, 2006.

[4] G. Blekherman, L.A. Fialkow. The core variety and representing measures in the truncated moment problem. Journal of Operator Theory 84(1):185–209, 2020.

[5] G. Blekherman, S. Iliman, M. Kubitzke. Dimensional differences between faces of the cones of nonnegative polynomials and sums of squares. International Mathematics Research Notices, 18:8437–8470, 2015.

[6] G. Blekherman, J.-B. Lasserre. The truncated K-moment problem for closure of open sets. J. Funct. Anal. 263(11):3604–3616, 2012.

[7] G. Blekherman, P. A. Parrilo, R. R. Thomas. Semidefinite optimization and convex algebraic geometry, SIAM, 2012.

[8] G. E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. Lecture Notes in Comput. Sci. 33:134–183, Springer, 1975.

[9] R. E. Curto, L. A. Fialkow. An analogue of the Riesz-Haviland theorem for the truncated moment problem. J. Funct. Anal. 255(10):2709–2731, 2008.

[10] L. A. Fialkow. The truncated K-moment problem: a survey. In Operator theory: the state of the art. Theta Ser. Adv. Math. 18(25–51), Theta, 2016.

[11] D. Grigoriev, N. Vorobjov. Solving systems of polynomials inequalities in subexponential time. J. Symbolic Computation 5:37–64, 1988.

[12] Q. Guo, M. Safey EI Din, L. Zhi. Computing rational solutions of linear matrix inequalities. Proc. Int. Symp. Symbolic and Algebraic Comput. (ISSAC) 197–204, 2013.

[13] D. Henrion, M. Korda, J.-B. Lasserre. The moment-SOS hierarchy. World Scientific, 2020.

[14] D. Henrion, S. Naldi, M. Safey El Din. Exact algorithms for linear matrix inequalities. SIAM J. Optim. 26(4):2512–2539, 2016.

[15] D. Henrion, S. Naldi, M. Safey El Din. SPECTRA–a Maple library for solving linear matrix inequalities in exact arithmetic. Optim. Methods and Software 34(1):62–78, 2019.

[16] E. Kaltofen, B. Li, Z. Yang, L. Zhi. Exact certification of global optimality of approximate factorizations via rationalizing sums-of-squares with floating point scalars. Proc. Int. Symp. Symbolic and Algebraic Comput. (ISSAC), 155–164, 2008.

[17] E. Kaltofen, B. Li, Z. Yang, L. Zhi. Exact certification in global polynomial optimization via sums-of-squares of rational functions with rational coefficients. J. Symbolic Comput. 47(1):1–15, 2012.

[18] S. Kuhlmann, M. Marshall. Positivity, sums of squares and the multi-dimensional moment problem. Trans. Amer. Math. Soc. 354(11):4285–4301, 2002.

[19] M. Laurent. Sums of squares, moment matrices and optimization over polynomials. In Emerging applications of algebraic geometry. IMA Vol. Math. Appl. 149:157–270, Springer, 2009.

[20] V. Magron, M. Safey El Din. On exact Reznick, Hilbert-Artin and Putinar's representations. J. Symbolic Comput. 107:221–250, 2021.

[21] M. Marshall. Positive polynomials and sums of squares. Amer. Math. Soc. 2008.

[22] S. Naldi, R. Sinn. Conic programming: infeasibility certificates and projective geometry. J. Pure Appl. Algebra 225(7):106605, 2021.

[23] T. Netzer. Stability of quadratic modules. Manuscripta Mathematica 129(2):251–271, 2009.

[24] J. Nie, M. Schweighofer. On the complexity of Putinar's Positivstellensatz. J. Complexity 23(1):135–150, 2007.

[25] H. Peyrl, P. A. Parrilo. Computing sum of squares decompositions with rational coefficients. Theoretical Computer Science 409(2):269–281, 2008.

[26] L. Porkolab, L. Khachiyan. On the complexity of semidefinite programs. J. Global Optim. 10(4):351–365, 1997.

[27] V. Powers, T. Wörmann. An algorithm for sums of squares of real polynomials. J. Pure Appl. Algebra 127(1):99–104, 1998.

[28] M. Putinar. Positive polynomials on compact semi-algebraic sets. Indiana Univ. Math. J. 42(3):969–984, 1993.

[29] M. V. Ramana. An exact duality theory for semidefinite programming and its complexity implications. Math. Prog. 77:129–162, 1997.

[30] M. Safey El Din, L. Zhi. Computing rational points in convex semialgebraic sets and sum of squares decompositions. SIAM J. Optim. 20(6):2876–2889, 2010.

[31] C. Scheiderer. Sums of squares of polynomials with rational coefficients. J. Europ. Math. Soc. 18(7):1495–1513, 2016.

[32] K. Schmüdgen. The K-moment problem on compact semi-algebraic sets. Math. Ann. 289:203–206, 1991.

[33] K. Schmüdgen. The moment problem. Springer, 2017.

[34] A. Tarski. A decision method for elementary algebra and geometry. Univ. California Press, 1951.

[35] V. Tchakaloff. Formules de cubatures mécaniques à coefficients non négatifs. Bull. Sci. Math. 81(2):123–134, 1957.