Computing real radicals by moment optimization

Lorenzo Baldi, Bernard Mourrain

Computing real radicals by moment optimization

Lorenzo Baldi & Bernard Mourrain
Inria Méditerranée, Université Côte d'Azur,
Sophia Antipolis, France

ABSTRACT

We present a new algorithm for computing the real radical of an ideal I and, more generally, the S-radical of I, which is based on convex moment optimization. A truncated positive generic linear functional σ vanishing on the generators of I is computed solving a Moment Optimization Problem (MOP). We show that, for a large enough degree of truncation, the annihilator of σ generates the real radical of I. We give an effective, general stopping criterion on the degree to detect when the prime ideals lying over the annihilator are real and compute the real radical as the intersection of real prime ideals lying over I.

The method involves several ingredients, that exploit the properties of generic positive moment sequences. A new efficient algorithm is proposed to compute a graded basis of the annihilator of a truncated positive linear functional. We propose a new algorithm to check that an irreducible decomposition of an algebraic variety is real, using a generic real projection to reduce to the hypersurface case. There we apply the Sign Changing Criterion, effectively performed with an exact MOP. Finally we illustrate our approach in some examples.

KEYWORDS

real radical, moments, positive polynomial, convex optimization, orthogonal polynomials, numerical algorithm

ACKNOWLEDGMENTS

This work is supported by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Actions, grant agreement 813211 (POEMA).

1 INTRODUCTION

In many "real world" problems which can be modeled by polynomial constraints, the solutions with real coordinates are generally analyzed with particular attention. Efficient algebraic methods have been developed over the years to solve such systems of polynomial constraints, including Grobner basis, border basis, resultants, triangular sets, homotopy continuation. But all these methods involve implicitly the complex roots of the polynomial systems and their complexity depends on the degree (and multiplicity) of the underlying complex algebraic varieties.

Finding equations vanishing on the real solutions without computing all the complex roots is a challenging question. This means computing the vanishing ideal of the real solutions of an ideal I, that is, its real radical $\sqrt[\mathbb{R}]{I}$.

Several approaches have been proposed to compute the real radical. Some of these methods are reducing to univariate problems [5, 6, 29, 36], or exploiting quantifier elimination techniques [15], or using infinitesimals [31] or triangular sets and regular chains [12, 39].

Sums-of-Squares convex optimisation and moment matrices are used in [20, 21] to compute real radicals, when the set of real solutions is finite. Some properties of ideals associated to semidefinite programming relaxations are analysed in [33], involving the simple point criterion. In [25] a stopping criterion is presented to verify that a Pommaret basis has been computed from the kernels of moment matrices involved in Sum of Squares relaxation. In [10], a test based on sum-of-square decomposition is proposed to verify that polynomials vanishing on a subset of the semi-algebraic set are in the real radical.

In [32], an algorithm based on rational representations of equidimensional components of algebraic varieties and singular locus recursion is presented and its complexity is analysed.

We present a new algorithm for computing the real radical of an ideal I and, more generally, the S-radical of I, which is based on convex moment optimization. An interesting feature of the approach is that it does not involve the complex solutions, which are not on a real component of the algebraic variety $\mathcal{V}(I)$. Section 2 recalls the relationship between vanishing ideals and radicals for real and complex algebraic varieties.

Generators of the real radical of I are computed from a truncated generic positive linear functional σ vanishing on the generators of I. This truncated linear functional is computed by solving a Moment Optimization Problem (MOP), as summarized in Section 3.

We show that, for a large enough degree of truncation, the annihilator of σ generates the real radical of I, suggesting an algorithm which will compute the annihilator of a generic positive linear functional for increasing degrees. The flat extension property (see e.g. [14, 22]) gives a stopping criterion in the zero-dimensional case (see e.g. [20, 21]). But the question remained open for positive-dimensional real varieties (see e.g. [23, § 4.3], [25]).

In this work, we give a new effective stopping criterion to detect when the prime ideals associated to the annihilator are real and compute equations for the minimal real prime ideals lying over I.

The method involves several ingredients, that exploit the properties of generic non-negative moment sequences.

A new efficient algorithm is proposed in Section 4 to compute a graded basis of the annihilator of a truncated non-negative linear functions. A new algorithm is presented in Section 5 to check that an irreducible decomposition of an algebraic variety is real, using a generic real projection to reduce to the hypersurface case. We apply the Sign Changing Criterion, effectively performed with an exact MOP.

The complete algorithm for computing the real radical of an ideal I as the intersection of real prime ideals is presented in Section 6.

In Section 7, we illustrate the algorithm by some effective numerical computation on examples, where the real radical differs significantly from the ideal I.

2 VARIETIES AND RADICALS

Let $f_1, \dots, f_s \in \mathbb{C}[x_1, \dots, x_n] = \mathbb{C}[\mathrm{x}]$ and let $I = (\mathrm{f}) \subset \mathbb{C}[\mathrm{x}]$ be the ideal generated $\mathrm{f} = \{f_1, \dots, f_s\}$. The algebraic variety defined by f is denoted $V = \mathcal{V}_{\mathbb{C}}(I) = \{\xi \in \mathbb{C}^n \mid f_i(\xi) = 0, i = 1, \dots, s\}$. It decomposes into an union of irreducible components $V = \cup_{i=1}^{l} V_i$ where $V_i = \mathcal{V}_{\mathbb{C}}(\mathfrak{p}_i)$ with $\mathfrak{p}_i$ a prime ideal of $\mathbb{C}[\mathrm{x}]$. An irreducible variety V is an algebraic variety which cannot be decomposed into an union of algebraic varieties distinct from V.

The Hilbert Nullstellensatz states that the vanishing ideal $\mathcal{I}(V) = \{p \in \mathbb{C}[\mathrm{x}] \mid \forall \xi \in V, p(\xi) = 0\}$ of an algebraic variety $V \subset \mathbb{C}^n$ is the radical

$$\sqrt{I} = \{p \in \mathbb{C}[\mathrm{x}] \mid \exists m \in \mathbb{N},\ p^m \in I\}$$

(see e.g. [13]). This implies that $\sqrt{I} = \cap_{i=1}^{l} \mathfrak{p}_i$. We say that I is radical if $I = \sqrt{I}$.

Considering now equations $\mathrm{f} = \{f_1, \dots, f_s\} \subset \mathbb{R}[\mathrm{x}]$ with real coefficients, the real variety defined by f is $V_{\mathbb{R}} = \mathcal{V}_{\mathbb{C}}(I) \cap \mathbb{R}^n = \mathcal{V}_{\mathbb{R}}(I) = \{\xi \in \mathbb{R}^n \mid f_i(\xi) = 0, i = 1, \dots, s\}$. The vanishing ideal of $V_{\mathbb{R}}$ is $\mathcal{I}(V_{\mathbb{R}}) = \{p \in \mathbb{R}[\mathrm{x}] \mid \forall \xi \in V_{\mathbb{R}},\ p(\xi) = 0\}$. Let $\Sigma^2 = \{\sum_j p_j^2,\ p_j \in \mathbb{R}[\mathrm{x}]\}$ be the sums of squares of polynomials of $\mathbb{R}[\mathrm{x}]$. The real Nullstellensatz states that $\mathcal{I}(\mathcal{V}_{\mathbb{R}}(I))$ is the real radical of I, defined as:

$$\sqrt[\mathbb{R}]{I} = \{p \in \mathbb{R}[\mathrm{x}] \mid \exists m \in \mathbb{N}, s \in \Sigma^2 \text{ s.t. } p^{2m} + s \in I\}$$

(see e.g. [26, p. 26], [8, p. 85]). If $I = \sqrt[\mathbb{R}]{I}$ then we say that I is a *real* or *real radical* ideal. The real radical of I contains $\sqrt{I}$ and is the intersection of real prime ideals $\mathfrak{p}_i$ in $\mathbb{R}[\mathrm{x}]$ containing I, corresponding to the real irreducible components of $\mathcal{V}_{\mathbb{R}}(I)$. The example $f = x_1^2 + x_2^2$ such that $I = (f) = \sqrt{I}$ and $\sqrt[\mathbb{R}]{I} = (x_1, x_2)$ shows that the radical and real radical ideals can define algebraic varieties of different dimensions.

Sets $S = \{\xi \in \mathbb{R}^n \mid f_1(\xi) = 0, \dots, f_s(\xi) = 0, g_1(\xi) \geq 0, \dots, g_r(\xi) \geq 0\}$ with $f_i, g_j \in \mathbb{R}[\mathrm{x}]$ are called basic semi-algebraic sets. The real Nullstellensatz for S states that the vanishing ideal $\mathcal{I}(S)$ is the S-radical of $I = (\mathrm{f})$:

$$\sqrt[S]{I} = \{p \in \mathbb{R}[\mathrm{x}] \mid \exists m \in \mathbb{N}, (s_\alpha) \in (\Sigma^2)^{\{0,1\}^r} \text{ s.t. } p^{2m} + \sum_\alpha s_\alpha \mathrm{g}^\alpha \in I\}$$

(see e.g. [26, th. 2.2.1], [8, cor. 4.4.3], [17], [37]). The S-radical $\sqrt[S]{I}$ is related to the real radical of an extended ideal I_S defined by introducing slack variables $s_1, \dots, s_r$ for each non-negativity constraint defining S: $I_S = (f_1, \dots, f_s, g_1 - s_1^2, \dots, g_r - s_r^2) \subset \mathbb{R}[x_1, \dots, x_n, s_1, \dots, s_r]$. Namely, we have $\sqrt[S]{I} = \sqrt[\mathbb{R}]{I_S} \cap \mathbb{R}[\mathrm{x}]$ (by the Real Nullstellensatz, see e.g. [8, p. 91]). Therefore, in the following we will focus on the computation of the real radical of $I = (\mathrm{f})$ and apply this transformation for the computation of S-radicals.

To describe the irreducible components of a variety $\mathcal{V}_{\mathbb{C}}(f_1, \dots, f_s)$ defined by equations $f_1, \dots, f_s \in \mathbb{R}[\mathrm{x}]$, we use tools from Numerical Algebraic Geometry, namely a description of irreducible components by witness sets. A witness set of an irreducible algebraic variety $V \subset \mathbb{C}^n$ is a triple $W = (\mathrm{f}, L, S)$ where $\mathrm{f} \subset \mathcal{I}(V)$, L is a generic linear space of dimension $n - \dim(V)$ given by $\dim(V)$ linear equations and $S = L \cap V \subset \mathbb{C}^n$ is a finite set of $\deg(V)$ points. Given equations $\mathrm{f} = \{f_1, \dots, f_s\} \subset \mathbb{R}[\mathrm{x}]$, a numerical irreducible decomposition of $\mathcal{V}_{\mathbb{C}}(\mathrm{f})$ can be computed as a collection of witness sets $W_i = (\mathrm{h}_i, L_i, S_i)$ such that each irreducible component V_i of V is described by one and only one witness set W_i and all sample sets S_i are pairewise disjoint. Several methods, based on homotopy techniques, have been developed over the past to compute such decomposition. See e.g. [4, 16, 35].

The witness set W of an (irreducible) algebraic variety V, can be used to compute defining equations $\mathrm{h} = \{h_1, \dots, h_n\} \subset \mathbb{C}[\mathrm{x}]$ such that $\mathcal{V}_{\mathbb{C}}(\mathrm{h}) = V$. Homotopy techniques are employed to generate enough sample points on V. The equations h_i are then computed by projection of the sample points onto $\leq n + 1$ generic linear spaces of dimension $(\dim(V) + 1)$ and by interpolation. See e.g. [35], for more details.

The numerical irreducible decomposition of $\mathcal{V}_{\mathbb{C}}(\mathrm{f})$ as a collection of witness sets provides a description of all the irreducible components V_i associated to the isolated primary components Q_i of $I = (\mathrm{f})$ [2]. To check that these primary components are reduced and thus prime (i.e. $\sqrt{Q_i} = Q_i$), it is enough to check that the Jacobian of f is of rank $n - \dim V_i$ (Jacobian criterion) at one of the sample points of the witness set W_i, describing the irreducible component $V_i = \mathcal{V}(P_i)$.

Checking that $I = (\mathrm{f})$ has no embedded component can also be done by numerical irreducible decomposition of deflated ideals, as described in [18]. We are not going to use this deflation technique to check non-embedded components.

3 MOMENT RELAXATIONS

3.1 Linear functionals

We describe the dual of polynomial rings (see for instance [28] for more details). For $\sigma \in (\mathbb{R}[\mathrm{x}])^* = \hom_{\mathbb{R}}(\mathbb{R}[\mathrm{x}], \mathbb{R}) = \{\, \sigma \colon \mathbb{R}[\mathrm{x}] \to \mathbb{R} \mid \sigma \text{ is } \mathbb{R}\text{-linear} \,\}$, we denote $\langle \sigma, f \rangle = \sigma(f)$ the application of σ to $f \in \mathbb{R}[\mathrm{x}]$. Recall that $(\mathbb{R}[\mathrm{x}])^* \cong \mathbb{R}[[\mathrm{y}]] \coloneqq \mathbb{R}[[y_1, \dots, y_n]]$, with the isomorphism given by: $\sigma \mapsto \sum_{\alpha \in \mathbb{N}^n} \langle \sigma, \mathrm{x}^\alpha \rangle \frac{\mathrm{y}^\alpha}{\alpha!}$, where $\{\frac{\mathrm{y}^\alpha}{\alpha!}\}$ is the dual basis to $\{\mathrm{x}^\alpha\}$, i.e. $\langle \mathrm{y}^\alpha, \mathrm{x}^\beta \rangle = \alpha!\, \delta_{\alpha,\beta}$. With this basis we can also identify $\sigma \in (\mathbb{R}[\mathrm{x}])^*$ with its sequence of coefficients $(\sigma_\alpha)_\alpha$, where $\sigma_\alpha \coloneqq \langle \sigma, \mathrm{x}^\alpha \rangle$.

If $\sigma \in (\mathbb{R}[\mathrm{x}])^*$ and $g \in \mathbb{R}[\mathrm{x}]$, we define the *convolution of g and σ* as $g \star \sigma \coloneqq \sigma \circ m_g \in (\mathbb{R}[\mathrm{x}])^*$ where m_g is the operator of multiplication by g on the polynomials (i.e. $\langle g \star \sigma, f \rangle = \langle \sigma, gf \rangle\ \forall f$). The operation $\star$ defines an $\mathbb{R}[\mathrm{x}]$-module structure on $\mathbb{R}[[\mathrm{y}]]$. We define the *Hankel operator* $H_\sigma \colon \mathbb{R}[\mathrm{x}] \to (\mathbb{R}[\mathrm{x}])^*,\ g \mapsto g \star \sigma$ and the *annihilator* $\mathrm{Ann}(\sigma) = \ker H_\sigma \colon g \in \mathrm{Ann}(\sigma) \iff H_\sigma(g) = 0 \iff g \star \sigma = 0$.

We describe these operations in coordinates. If $\sigma = (\sigma_\alpha)_\alpha$ and $g = \sum_\alpha g_\alpha \mathrm{x}^\alpha$ then $g \star \sigma = (\sum_\beta g_\beta \sigma_{\alpha+\beta})_\alpha$; the matrix H_σ in the basis $\{\mathrm{x}^\alpha\}$ and $\{\frac{\mathrm{y}^\alpha}{\alpha!}\}$ is $H_\sigma = (\sigma_{\alpha+\beta})_{\alpha,\beta}$.

3.2 Truncation

We introduce the same operations in a finite dimensional setting, considering only polynomials of bounded degree. If $A \subset \mathbb{R}[\mathrm{x}]$, $A_d \coloneqq \{\, f \in A \mid \deg f \leq d \,\}$. In particular $\mathbb{R}[\mathrm{x}]_d$ is the vector space of polynomials of degree $\leq d$. If $\sigma \in (\mathbb{R}[\mathrm{x}])^*$ (resp. $\sigma \in (\mathbb{R}[\mathrm{x}]_r)^*, r \geq t$) then $\sigma^{[t]} \in (\mathbb{R}[\mathrm{x}]_t)^*$ denotes its restriction to $\mathbb{R}[\mathrm{x}]_t$; moreover if $B \subset (\mathbb{R}[\mathrm{x}])^*$ (resp. $B \subset (\mathbb{R}[\mathrm{x}]_r)^*,\ r \geq t$) then $B^{[t]} \coloneqq \{\, \sigma^{[t]} \in (\mathbb{R}[\mathrm{x}]_t)^* \mid \sigma \in B \,\}$.

If $\sigma \in (\mathbb{R}[\mathrm{x}]_t)^*$ and $g \in \mathbb{R}[\mathrm{x}]_t$, then $g \star \sigma \coloneqq \sigma \circ m_g \in (\mathbb{R}[\mathrm{x}]_{t - \deg g})^*$. If $\sigma \in (\mathbb{R}[\mathrm{x}])^*$ (or $\sigma \in (\mathbb{R}[\mathrm{x}]_r)^*,\ r \geq 2t$), then we define $H_\sigma^t \colon \mathbb{R}[\mathrm{x}]_t \to (\mathbb{R}[\mathrm{x}]_t)^*,\ g \mapsto (g \star \sigma)^{[t]}$. We have

$(g \star \sigma)^{[2t]} = 0 \iff H^t_{g\star\sigma} = 0$: in analogy to the infinite dimensional setting we define $\mathrm{Ann}_d(\sigma) := \ker H^d_\sigma$.

For $\mathrm{h} = h_1, \ldots, h_r \subset \mathbb{R}[\mathrm{x}]$ we define $\langle \mathrm{h} \rangle_t := \left\{ \sum_{i=1}^r f_i h_i \in \mathbb{R}[\mathrm{X}]_t \mid f_i \in \mathbb{R}[\mathrm{X}]_{t-\deg h_i} \right\}$, the elements of $(\mathrm{h})_t$ generated in degree $\leq t$.

3.3 Positive linear functionals and generic elements

Let $A \subset \mathbb{R}[\mathrm{x}]$ (resp. $A \subset \mathbb{R}[\mathrm{x}]_t$). We define $A^\perp := \left\{ \sigma \in (\mathbb{R}[\mathrm{x}])^* \mid \langle \sigma, f \rangle = 0 \ \forall f \in A \right\}$ (resp. $A^\perp := \left\{ \sigma \in (\mathbb{R}[\mathrm{x}]_t)^* \mid \langle \sigma, f \rangle = 0 \ \forall f \in A \right\}$). Notice that $\sigma \in \langle \mathrm{h} \rangle_t^\perp$ (resp. $(\mathrm{h})^\perp$) if and only if $(h \star \sigma)^{[t-\deg h]} = 0 \ \forall h \in \mathrm{h}$ (resp. $h \star \sigma = 0 \ \forall h \in \mathrm{h}$).

We say that $\sigma \in (\mathbb{R}[\mathrm{x}]_{2t})^*$ is *positive semidefinite* (psd) $\iff$ H^t_σ is psd, i.e. $\langle H^t_\sigma(f), f \rangle = \langle \sigma, f^2 \rangle \geq 0 \ \forall f \in \mathbb{R}[\mathrm{x}]_t$. If σ is pds then $\langle \sigma, f^2 \rangle = 0 \Rightarrow f \in \mathrm{Ann}_t(\sigma)$ [20, 3.12]

For $G \subset \mathbb{R}[\mathrm{x}]_t$ we finally define the closed convex cone:

$$\mathcal{L}_t(G) := \{ \sigma \in (\mathbb{R}[\mathrm{x}]_t)^* \mid \sigma \text{ is psd and } \forall g \in (G \cdot \Sigma^2)_t \ \langle \sigma, g \rangle \geq 0 \},$$

see [3] for more details. In particular $\mathcal{L}_t(\pm\mathrm{h}) = \{ \sigma \in \langle \mathrm{h} \rangle_t^\perp \mid \sigma \text{ is psd} \}$. We use $\mathcal{L}(G)$ for the infinite dimensional case. Notice that $\mathcal{L}(G)^{[t]} \subset \mathcal{L}_t(G) \ \forall t$.

Linear functionals of special importance are evaluations e_ξ defined as $\langle \mathrm{e}_\xi, f \rangle = f(\xi)$. For $\xi \in \mathcal{V}_\mathbb{R}(\mathrm{h})$ we have $\mathrm{e}_\xi \in \mathcal{L}(\pm\mathrm{h})$.

Definition 3.1. We say that $\sigma^* \in \mathcal{L}_t(\pm\mathrm{h})$ is *generic* if $\mathrm{rank}\, H^t_{\sigma^*} = \max\{\mathrm{rank}\, H^t_\eta \mid \eta \in \mathcal{L}_t(\pm\mathrm{h})\}$.

Genericity is characterized as follows, see e.g. [20, prop. 4.7]:

Proposition 3.2. *Let $\sigma \in \mathcal{L}_{2t}(\pm\mathrm{h})$. The following are equivalent:*

(i) σ is generic;
(ii) $\mathrm{Ann}_t(\sigma) \subset \mathrm{Ann}_t(\eta) \ \forall \eta \in \mathcal{L}_{2t}(\mathrm{g})$;
(iii) $\forall d \leq t$, we have: $\mathrm{rank}\, H^d_\sigma = \max\{\mathrm{rank}\, H^d_\eta \mid \eta \in \mathcal{L}_{2t}(\pm\mathrm{h})\}$.

Generic elements can be used to compute the real radical of ideals, see [30, th. 7.39]. We give in Theorem 3.3 a proof of this result. See also [3, th. 3.16] for a generalisation to quadratic modules.

Theorem 3.3. *Let $\sigma^* \in \mathcal{L}_{2d}(\pm\mathrm{h})$ be generic and $I = (\mathrm{h})$. Then for every $d \geq \deg \mathrm{h}$ we have $I \subset (\mathrm{Ann}_d(\sigma^*)) \subset \sqrt[\mathbb{R}]{I}$. Moreover for d big enough $(\mathrm{Ann}_d(\sigma^*)) = \sqrt[\mathbb{R}]{I}$.*

Proof. The inclusion $I \subset (\mathrm{Ann}_d(\sigma^*))$ is clear since $\mathrm{h} \subset \mathrm{Ann}_d(\sigma^*)$ by definition. Now let $J = \sqrt[\mathbb{R}]{I}$. Notice that, for $\xi \in \mathbb{R}^n$, $\mathrm{Ann}_d(\mathrm{e}_\xi) = \mathcal{I}(\xi)_d = (x_1 - \xi_1, \ldots, x_n - \xi_n)_d$. Moreover, if $\xi \in \mathcal{V}_\mathbb{R}(I)$, then $\mathrm{e}_\xi^{[2d]} \in \mathcal{L}_{2d}(\pm\mathrm{h})$. Then, since σ^* is generic:

$$\mathrm{Ann}_d(\sigma^*) \subset \bigcap_{\xi \in \mathcal{V}_\mathbb{R}(I)} \mathrm{Ann}_d(\mathrm{e}_\xi) = \bigcap_{\xi \in \mathcal{V}_\mathbb{R}(I)} \mathcal{I}(\xi)_d = J_d,$$

and thus $(\mathrm{Ann}_d(\sigma^*)) \subset J$.

For the second part, let $g_1, \ldots, g_k$ be generators of J. By the Real Nullstellensatz, $\forall i$ there exists $m_i \in \mathbb{N}, s_i \in \Sigma^2$ such that $g_i^{2m_i} + s_i \in I$. Then for d big enough and $\sigma \in \mathcal{L}_{2d}(\pm\mathrm{h})$ we have $\langle \sigma^{[2d]}, g_i^{2m_i} + s_i \rangle = 0$, thus $\langle \sigma^{[2d]}, g_i^{2m_i} \rangle = 0$ and $g_i \in \mathrm{Ann}_d(\sigma)$. This implies $J \subset (\mathrm{Ann}_d(\sigma))$ for all $\sigma \in \mathcal{L}_{2d}(\pm\mathrm{h})$, and in particular for $\sigma = \sigma^*$ generic. □

The goal of the paper is to find an effective algorithm, based on Theorem 3.3, to compute $\sqrt[\mathbb{R}]{I}$. In the case of a finite real variety, the flat extension criterion [20, 21] certifies that $(\mathrm{Ann}_d(\sigma^*)) = \sqrt[\mathbb{R}]{I}$ for some $d \in \mathbb{N}$. We will focus in the positive dimensional case, when such a criterion cannot apply.

3.4 Polynomial Optimization and Exactness

Let $f, \mathrm{g} \in \mathbb{R}[\mathrm{x}]$. The goal of Polynomial Optimization is to find:

$$f^* := \inf \left\{ f(x) \in \mathbb{R} \mid x \in \mathbb{R}^n, \ g_i(x) \geq 0 \ \text{ for } i = 1, \ldots, s \right\}. \quad (1)$$

that is the infimum f^* of the *objective function* f on the *basic semi-algebraic set* $S := \{ x \in \mathbb{R}^n \mid g_i(x) \geq 0 \ \text{ for } i = 1, \ldots, s \}$. In particular we will consider the case of equalities $h_i = 0$, obtained as $\pm h_i \geq 0$. To solve problem (1) Lasserre [19] proposed to use two hierarchies of finite dimensional convex cones depending on an order $d \in \mathbb{N}$. We describe the Moment Matrix hierarchy and the property of *exactness*, see [3] for more details.

Definition 3.4. We define the *MoM relaxation of order d* of problem (1) as $\mathcal{L}_{2d}(\mathrm{g})$ and the infimum:

$$f^*_{\mathrm{MoM},d} := \inf \left\{ \langle \sigma, f \rangle \in \mathbb{R} \mid \sigma \in \mathcal{L}_{2d}(\mathrm{g}), \ \langle \sigma, 1 \rangle = 1 \right\}. \quad (2)$$

We will call Problem (2) a *Moment Optimization Problem* (MOP). It can be efficiently solved by semidefinite programming, using interior point methods. Taking $f = 1$, these methods yield an interior point of $\mathcal{L}_{2d}(\mathrm{g})$, that is a *generic* element σ^* in $\mathcal{L}_{2d}(\mathrm{g})$.

Usually we are interested in minimizers of f with bounded norm, i.e. minimizers in some closed ball defined by $r - \|\mathrm{x}\|^2 \geq 0$ (*Archimedean condition*). If the Archimedean condition and some regularity conditions at the minimizers of f hold (known as *Boundary Hessian Conditions* or BHC), the MoM relaxation is *exact*: for some $d \in \mathbb{N}$ the minimum is reached, i.e. $f^* = f^*_{\mathrm{MoM},d}$, and we can effectively recover the minimizers (see [3, th. 4.8]). Using the flat extention criterion for the Hankel matrix H^d_σ (associated to a minimizing moment sequence σ) we can effectively test exactness. As BHC hold generically, exactness is also generic (see [3, cor. 4.9]).

4 ORTHOGONAL POLYNOMIALS AND ANNIHILATOR

To compute the real radical, we need to compute a basis of the annihilator of a truncated positive linear functional $\sigma \in \mathbb{R}[\mathrm{x}]^*_{2d}$ such that $\langle \sigma, p^2 \rangle \geq 0$ for $p \in \mathbb{R}[\mathrm{x}]_d$. In this section, we describe an efficient algorithm to compute a basis of $\mathrm{Ann}_d(\sigma) = \{p \in \mathbb{R}[\mathrm{x}]_d \mid p \star \sigma = 0\} = \{p \in \mathbb{R}[\mathrm{x}]_d \mid \langle \sigma, p^2 \rangle = 0\}$. It is a Gram-Schmidt orthogonalization process, using the inner product $\langle \cdot, \cdot \rangle_\sigma$ defined, for $p, q \in \mathbb{R}[\mathrm{x}]_d$, by

$$\langle p, q \rangle_\sigma := \langle \sigma, p\, q \rangle.$$

By ordering the monomials basis of $\mathbb{R}[\mathrm{x}]_d$ and projecting successively a monomial x^α onto the space spanned by the previous monomials, we construct monomial basis $\mathrm{b} = \{\mathrm{x}^\beta\}$ of $\mathbb{R}[\mathrm{x}]_d / \mathrm{Ann}_d(\sigma)$, a corresponding basis of orthogonal polynomials $\mathrm{p} = (p_\beta)$ and a basis $\mathrm{k} = (k_\gamma)$ of $\mathrm{Ann}_d(\sigma)$. The orthogonal polynomials are such that

$$\langle p_\beta, p_{\beta'} \rangle_\sigma = \begin{cases} > 0 & \text{if } \beta = \beta' \\ 0 & \text{otherwise,} \end{cases}$$

and for all β, γ, we have $\langle p_\beta, k_\gamma \rangle_\sigma = \langle k_\gamma, k_\gamma \rangle_\sigma = 0$.

To compute these polynomials, we use a projection defined on the orthogonal of the space spanned by orthogonal polynomials $\mathrm{p} = [p_1, \ldots, p_l]$ such that $\langle p_i, p_i\rangle_\sigma > 0$ and $\langle p_i, p_j\rangle_\sigma = 0$ if $i \neq j$, as follows: for $f \in \mathbb{R}[\mathrm{x}]_d$,

$$\mathrm{proj}(f, \mathrm{p}) = f - \sum_{i=1}^{l} \frac{\langle f, p_i\rangle_\sigma}{\langle p_i, p_i\rangle_\sigma} p_i.$$

By construction, we have $\langle \mathrm{proj}(f, \mathrm{p}), p_i\rangle_\sigma = 0$ for $i = 1, \ldots, l$. In practice, the implementation of this projection is done by the so-called Modified Gram-Schmidt projection algorithm, which is known to have a better numerical behavior than the direct Gram-Schmidt orthogonalization process [38][Lecture 8].

To compute a basis of $\mathrm{Ann}_d(\sigma)$, we choose a monomial ordering $\prec$ compatible with the degree (e.g. the graded reverse lexicographic ordering) and build the list of monomials s of degree $\leq d$ in increasing order for this ordering $\prec$. Algorithm 4.1 choses incrementally a new monomial in the list s and projects it on the space spanned by the previous orthogonal polynomials. The new monomials computed by the function $\mathrm{next}(\mathrm{s}, \mathrm{b}, \mathrm{l})$ are the lowest monomials of s not in b and not divisible by a monomial of l.

Algorithm 4.1: Orthogonal polynomials and annihilator of σ

Input: a positive linear functional $\sigma \in \mathbb{R}[\mathrm{x}]^*_{2d+2}$.

- Let $\mathrm{b} := []$; $\mathrm{p} := []$; $\mathrm{k} := []$; $\mathrm{l} := []$; $\mathrm{n} := [1]$; $\mathrm{s} := [\mathrm{x}^\alpha, |\alpha| \leq d]$;
- while $\mathrm{n} \neq \emptyset$ do
  - for each $\mathrm{x}^\alpha \in \mathrm{n}$,
    - (i) $p_\alpha := \mathrm{proj}(\mathrm{x}^\alpha, \mathrm{p})$;
    - (ii) compute $v_\alpha = \langle p_\alpha, p_\alpha\rangle_\sigma$;
    - (iii) if $v_\alpha \neq 0$ then add x^α to b; add p_α to p; else add $k_\alpha := p_\alpha$ to k; add x^α to l; end;
  - $\mathrm{n} := \mathrm{next}(\mathrm{s}, \mathrm{b}, \mathrm{d})$;

Output:

- a basis $\mathrm{k} = [k_\gamma]_{\mathrm{x}^\gamma \in \mathrm{l}}$ of the annihilator $\mathrm{Ann}_d(\sigma)$ and their leading monomials $\mathrm{l} = [\mathrm{x}^\gamma]$;
- a basis of orthogonal polynomials $\mathrm{p} = [p_{\beta_i}]$, $\mathrm{m} = [m_{\beta_i}]$;
- a monomial set $\mathrm{b} = [\mathrm{x}^{\beta_1}, \ldots, \mathrm{x}^{\beta_r}]$.

By construction, the vector space spanned by b and p are equal at each loop of the algorithm. As the function $\mathrm{next}(\mathrm{s}, \mathrm{b}, \mathrm{l})$ outputs the least monomials in s, greater than b and not divisible by the monomials in l, the monomials in n are greater than the monomials in b. Thus, the leading term of $k_\gamma \in \mathrm{k}$ is x^γ.

Let k, l, p, b denote the output of Algorithm 4.1. For $\alpha \in \mathbb{N}^n$, let $(\mathrm{k})_{\leq\alpha}$ be the vector space spanned by the elements of the form $\mathrm{x}^\delta k_\gamma$ with $\delta + \gamma \preceq \alpha$. Similarly, $\mathrm{p}_{\leq\alpha}$ is the set of $p_\beta \in \mathrm{p}$ such that $\beta \preceq \alpha$. We prove that k is a Grobner basis of $\mathrm{Ann}_d(\sigma)$, that is any element of $\mathrm{Ann}_d(\sigma)$ reduces to 0 by k:

Proposition 4.1. *Let $\sigma \in \mathbb{R}[\mathrm{x}]^*_{2d+2}$, k, p be the output of Algorithm 4.1. For $\mathrm{x}^\alpha \in (\mathrm{l})_d$, i.e. divisible by a monomial in l and of degree $|\alpha| \leq d$, $p_\alpha = \mathrm{proj}(\mathrm{x}^\alpha, \mathrm{p}_{\leq\alpha})$ is in $(\mathrm{k})_{\leq\alpha} \subset \mathrm{Ann}_d(\sigma)$.*

Proof. Let us prove it by induction on the ordering of α. The lowest element in $(\mathrm{l})_d$ is a monomial x^γ of l. As $k_\gamma = \mathrm{proj}(\mathrm{x}^\gamma, \mathrm{p}_{\beta\leq\gamma})$ is such that $\langle k_\gamma, k_\gamma\rangle_\sigma = \langle \sigma, k_\gamma^2\rangle = 0, k_\gamma = \mathrm{proj}(\mathrm{x}^\gamma, \mathrm{p}_{\beta\leq\gamma}) \in (\mathrm{k})_{\leq\gamma} \subset \mathrm{Ann}_d(\sigma)$. The induction hypothesis is true for the lowest monomial of $(\mathrm{l})_d$.

Assume that it is true for $\mathrm{x}^{\alpha'} \in (\mathrm{l})_d$ and let α be the next monomial in $(\mathrm{l})_d$ for the monomial ordering $\prec$. Then, there exists $\mathrm{x}^{\alpha''} \in (\mathrm{l})_{\leq\alpha'}$ and $i_0 \in 1, \ldots, n$ such that $x_{i_0}\mathrm{x}^{\alpha''} = \mathrm{x}^\alpha$. As $p_\alpha - x_{i_0} p_{\alpha''}$ has a leading term smaller that x^α, it can be written as a linear combination of $p_{\alpha'} = \mathrm{proj}(\mathrm{x}^{\alpha'}, \mathrm{p}_{\prec\alpha'})$ with $\alpha' \prec \alpha$. More precisely, we have

$$p_\alpha = x_{i_0} p_{\alpha''} + \sum_{\delta\prec\alpha, \mathrm{x}^\delta \in (\mathrm{l})_d} \lambda_\delta\, p_\beta + \sum_{\beta\prec\alpha, \mathrm{x}^\beta \in \mathrm{b}} \mu_\beta\, p_\beta,$$

for some $\lambda_\delta, \mu_\beta \in \mathbb{R}$.

By induction hypothesis, $p_{\alpha''}, p_\delta \in (\mathrm{k})_{\leq\alpha'} \subset (\mathrm{k})_{\leq\alpha} \subset \mathrm{Ann}_d(\sigma)$. Moreover, as $p_{\alpha''} \in \mathrm{Ann}_d(\sigma) \subset \mathrm{Ann}_{d+1}(\sigma)$, for any $p \in \mathbb{R}[\mathrm{x}]_d$ we have $\langle x_{i_0} p_{\alpha''}, p\rangle_\sigma = \langle p_{\alpha''}, x_{i_0}\, p\rangle_\sigma = 0$. This shows that $x_{i_0} p_{\alpha''} \in (\mathrm{k})_{\leq\alpha} \cap \mathrm{Ann}_d(\sigma)$.

By definition of $p_\alpha = \mathrm{proj}(\mathrm{x}^\alpha, \mathrm{p}_{\prec\alpha})$, $\langle p_\alpha, p_\beta\rangle_\sigma = 0$ for $\mathrm{x}^\beta \in \mathrm{b}_{\prec\alpha}$ so that $\mu_\beta = \frac{\langle p_\alpha, p_\beta\rangle_\sigma}{\langle p_\beta, p_\beta\rangle_\sigma} = 0$ and $p_\alpha \in (\mathrm{k})_{\leq\alpha} \cap \mathrm{Ann}_d(\sigma)$.

As $(\mathrm{k})_{\leq\alpha} = (\mathrm{k})_{\leq\alpha'} + \langle p_\alpha\rangle$, we have $(\mathrm{k})_{\leq\alpha} \subset \mathrm{Ann}_d(\sigma)$, which proves the induction hypothesis for α and concludes the proof of the proposition. □

This proposition explains why the function $\mathrm{next}(\mathrm{s}, \mathrm{b}, \mathrm{l})$ only outputs the least monomial in s, greater than b and not divisible by the monomials in l. This algorithm is an optimization of Algorithm 4.1 in [28] or Algorithm 3.2 in [27]. It strongly exploits the positivity of the linear functional σ and improves significantly the performance. We will illustrate its behavior in Section 7.

Remark 4.2. *When the real variety $\mathcal{V}_\mathbb{R}(\mathrm{f})$ is finite, the flat extension test on the rank of H^k_σ can be replaced by testing that the set l of initial terms contains a power of each variable x_i. This is equivalent to the fact that $\mathbb{R}[\mathrm{x}]/(\mathrm{k})$ is finite dimensional or equivalently that the rank of H^d_σ is constant for $d \gg 0$.*

5 REAL IRREDUCIBLE COMPONENTS

We introduce an effective algorithm for testing real radicality in the irreducible case.

5.1 Genericity

Let $\mathbb{C}^N$ be the N-dimensional affine space and $\mathbb{C}[t_1, \ldots, t_N] = \mathbb{C}[\mathrm{t}]$ be its coordinate (polynomial) ring. We say that a property holds *generically* in $\mathbb{C}^N$ if there exists finitely many nonzero polynomials $\phi_1, \ldots, \phi_l \in \mathbb{C}[\mathrm{t}]$ such that, for $\xi \in \mathbb{C}^N$, when $\phi_1(\xi) \neq 0, \ldots, \phi_l(\xi) \neq 0$ the property holds for ξ.

In particular we will consider linear maps $A \in \hom_\mathbb{C}(\mathbb{C}^n, \mathbb{C}^{k+1})$ as elements in $\mathbb{C}^{n(k+1)}$ in the natural way, and thus talk about *generic linear maps*.

5.2 Smooth Complex and Real Zeros

We recall the definition of *smooth zero*. We refer to [34] for the complex case and to [26] for the real case.

We say that a variety $V \subset \mathbb{C}^n$ is *defined over* $\mathbb{R}$, if $\mathcal{I}(V)$ is generated by a family of polynomials with coefficient in $\mathbb{R}$. For $A \subset \mathbb{C}^n$ we denote by $\mathrm{cl}(A)$ its Zariski closure.

Hereafter $\mathbb{K}$ denotes a field of characteristic 0 and $\overline{\mathbb{K}}$ its algebraic closure.

Definition 5.1. Let $I = (f_1, \ldots, f_m) \subset \mathbb{K}[\mathrm{x}]$ be a prime ideal and $V = \mathcal{V}_{\overline{\mathbb{K}}}(I)$. We say that $\xi \in \mathcal{V}_{\mathbb{K}}(I)$ is a *smooth zero* of I if $\operatorname{rank} \mathrm{Jac}(f_1, \ldots, f_m)(\xi) = n - \dim V$.

For $\mathbb{K} = \mathbb{C}$ the mapping $V \mapsto \mathcal{I}_{\mathbb{C}}(V)$ is a bijection between irreducible varieties in $\mathbb{C}^n$ and prime ideals. Moreover, for a prime ideal I, smooth zeros of I and smooth points of $\mathcal{V}_{\mathbb{C}}(I)$ coincide, and they are dense. On the other hand for $\mathbb{K} = \mathbb{R}$ the mapping $V \mapsto \mathcal{I}_{\mathbb{R}}(V)$ is a bijection between irreducible varieties in $\mathbb{R}^n$ and prime ideals which are real radical. For prime ideals I which are not real radical, smooth zeros of I are not dense in $\mathcal{V}_{\mathbb{R}}(I)$.

Example 5.2. Here are examples of reducible and irreducible algebraic varieties with dense complex smooth points but with no real smooth point.

- $I = (x^2 + y^2) \subset \mathbb{R}[x, y]$ is a prime, non real radical ideal, as $\mathcal{V}_{\mathbb{R}}(I) = \{(0, 0)\}$ and $\sqrt[\mathbb{R}]{I} = (x, y)$. I does not have smooth real zeros. Notice that $(x^2+y^2) \subset \mathbb{C}[x, y]$ is not prime, since $x^2 + y^2 = (x + iy)(x - iy)$.
- $I = (x^2 + y^2 + z^2) \subset \mathbb{R}[x, y, z]$ is a prime, non real radical ideal, as $\mathcal{V}_{\mathbb{R}}(I) = \{(0, 0, 0)\}$ and $\sqrt[\mathbb{R}]{I} = (x, y, z)$. I does not have smooth real zeros. In this case $(x^2+y^2+z^2) \subset \mathbb{C}[x, y, z]$ is prime, since $x^2 + y^2 + z^2$ is irreducible over $\mathbb{C}$.

We recall criterions for testing whether a prime ideal $I \subset \mathbb{R}[\mathrm{x}]$ is real radical or not.

Theorem 5.3 (Simple Point Criterion [26, th. 12.6.1]). *Let I be a prime ideal of $\mathbb{R}[\mathrm{x}]$. The following are equivalent:*

- *I is a real radical ideal;*
- *$I = \mathcal{I}(\mathcal{V}_{\mathbb{R}}(I))$;*
- *$\mathrm{cl}(\mathcal{V}_{\mathbb{R}}(I)) = \mathcal{V}_{\mathbb{C}}(I)$;*
- *I has a smooth real zero.*

Definition 5.4. If $V \subset \mathbb{C}^n$ then $V_{\mathbb{R}}$ denotes the real points of V, i.e. $V_{\mathbb{R}} = V \cap \overline{V} = V \cap \mathbb{R}^n$.

Let $V \subset \mathbb{C}^n$ be an irreducible variety defined over $\mathbb{R}$ and $I \subset \mathbb{R}[\mathrm{x}]$ the ideal defined by its real generators. If follows from Theorem 5.3 that $V_{\mathbb{R}} = \mathcal{V}_{\mathbb{R}}(I)$ is Zariski dense in V if and only if I is a real radical ideal. In this case we say that V is *real*.

For hypersurfaces there exists another criterion based on the change of sign of the defining polynomial.

Theorem 5.5 (Sign Changing Criterion [26, th. 12.7.1]). *Let $f \in \mathbb{R}[\mathrm{x}]$ be an irreducible polynomial. The following are equivalent:*

- *(f) is a real radical ideal;*
- *(f) has a smooth real point (i.e. there exists $\xi \in \mathcal{V}_{\mathbb{R}}(I)$ such that $\nabla f(\xi) \neq 0$);*
- *the polynomial f changes sign in $\mathbb{R}^n$ (i.e. there exists $x, y \in \mathbb{R}^n$ such that $f(x)f(y) < 0$).*

5.3 Test for Real Radicality

We reduce the problem of testing real radicaly to the hypersurface case, and then use the Simple Point Criterion. For that prupose we project $V \subset \mathbb{C}^n$, irreducible variety of dimension k, on a linear subspace $\mathbb{C}^{k+1} \subset \mathbb{C}^n$, in such a way V and $\mathrm{cl}(\pi(V))$ are *birational*. (see [34, p. 38] for the definition).

It is classical that every irreducible (affine) variety is birational to an hypersurface. We recall briefly this result to show that we can choose a generic projection as birational morphism, as done for the geometric resolution or rational representation, see for instance [24] or [9].

Lemma 5.6. *Let $V \subset \mathbb{C}^n$ be an irreducible varierty of dimension k and $\pi \colon \mathbb{C}^n \to \mathbb{C}^{k+1}$ be a generic projection. Then V is birational to $\pi(V)$, i.e. $V \cong \mathrm{cl}(\pi(V))$.*

Proof. (sketch) The birational morphism in [34, p. 39] can be given as a generic projection. Indeed we can choose algebraically independent elements $l_1, \ldots, l_k$ generic linear forms in the indeterminates x (see for instance [9, p. 488]). The choice of the primitive element l_{k+1} is generic (see for instance [1, th. 15.8.1]: one can choose l_{k+1} as a generic linear form). Then $l_1, \ldots, l_{k+1}$ define the projection $\pi \colon \mathbb{C}^n \to \mathbb{C}^{k+1}$, $\xi \mapsto (l_1(\xi), \ldots, l_{k+1}(\xi))$ and V is birational to $\mathrm{cl}(\pi(V))$. □

We choose a generic projection defined over $\mathbb{R}$. In this case we show that V has a smooth real point if and only if $\mathrm{cl}(\pi(V))$ has a smooth real point, using the following propositions.

Proposition 5.7. *Let $V \subset \mathbb{C}^n$ be an irreducible varierty defined over $\mathbb{R}$ of dimension k, and let $\pi \colon \mathbb{C}^n \to \mathbb{C}^{k+1}$ be a generic projection defined over $\mathbb{R}$. Then $\mathrm{cl}(\pi(V))$ is defined over $\mathbb{R}$ and if V has a smooth real point then $\mathrm{cl}(\pi(V))$ has a smooth real point.*

Proof. Let $\pi \colon \mathbb{C}^n \to \mathbb{C}^{k+1}$ be a generic projection defined over $\mathbb{R}$. As V is defined over $\mathbb{R}$, $\mathrm{cl}(\pi(V))$ is also defined over $\mathbb{R}$ since $\mathcal{I}(\pi(V))$ is the elimination ideal $(\mathcal{I}(V) + (\mathrm{x} - \pi(\mathrm{y})))\cap\mathbb{R}[\mathrm{y}]$, where $\mathrm{y} = y_1, \ldots, y_{k+1}$ are coordinates of $\mathbb{C}^{k+1}$ (see [13]).

If V has a smooth real point then $V_{\mathbb{R}}$ is Zariski dense in V by Theorem 5.3. Then $\pi(V_{\mathbb{R}})$ is Zariski dense in $\pi(V)$. Since π is defined over $\mathbb{R}$ we have that $\pi(V_{\mathbb{R}}) \subset (\pi(V))_{\mathbb{R}}$ and $(\pi(V))_{\mathbb{R}}$ is Zariski dense in $\pi(V)$. Then $\mathrm{cl}((\pi(V))_{\mathbb{R}}) = \mathrm{cl}(\pi(V))$ and by Theorem 5.3 $\mathrm{cl}(\pi(V))$ has a smooth real point. □

Proposition 5.8. *Let $V \subset \mathbb{C}^n$ be an irreducible variety defined over $\mathbb{R}$ of dimension k without smooth real points. Then, for a generic projection $\pi \colon \mathbb{C}^n \to \mathbb{C}^{k+1}$ defined over $\mathbb{R}$, $\mathrm{cl}(\pi(V))$ is defined over $\mathbb{R}$ and has no smooth real points.*

Proof. By Proposition 5.7, $\mathrm{cl}(\pi(V))$ is defined over $\mathbb{R}$.

Assume now that $\mathrm{cl}(\pi(V))$ has a smooth real point. Since V is generically birational to $\pi(V)$ (Lemma 5.6), the preimage of a generic smooth point in $\pi(V)$ is a single point in V, which is smooth. If π is defined over $\mathbb{R}$ then this smooth point $p \in V$ is real since $\pi(p) = \overline{\pi(p)} = \pi(\overline{p})$ implies that $p = \overline{p}$, showing that V has a smooth real point. □

Proposition 5.9. *Let $V \subset \mathbb{C}^n$ be an irreducible variety not defined over $\mathbb{R}$ of dimension k. If $\pi \colon \mathbb{C}^n \to \mathbb{C}^{k+1}$ is a generic projection defined over $\mathbb{R}$ then $\mathrm{cl}(\pi(V))$ is not defined over $\mathbb{R}$.*

Proof. V is not defined over $\mathbb{R}$ if and only if $V \neq \overline{V}$. Thus there exists $p \in V$ such that $\overline{p} \notin V$. Then for $\pi \colon \mathbb{C}^n \to \mathbb{C}^{k+1}$ a generic

projection, we have $\pi(\overline{p}) \notin \mathrm{cl}(\pi(V))$ (see e.g. [7, sec. 3]). As π is defined over $\mathbb{R}$, we have $\pi(p) \in \mathrm{cl}(\pi(V))$ and $\overline{\pi(p)} = \pi(\overline{p}) \notin \mathrm{cl}(\pi(V))$. Therefore, $\mathrm{cl}(\pi(V)) \neq \overline{\mathrm{cl}(\pi(V))}$ and $\mathrm{cl}(\pi(V))$ is not defined over $\mathbb{R}$. □

Theorem 5.10. *Let $V \subset \mathbb{C}^n$ be an irreducible variety of dimension k. Then V is defined over $\mathbb{R}$ and has a smooth real point if and only if, for $\pi\colon \mathbb{C}^n \to \mathbb{C}^{k+1}$ generic projection defined over $\mathbb{R}$, $\mathrm{cl}(\pi(V))$ is defined over $\mathbb{R}$ and has a smooth real point.*

Proof. If V has a smooth real point then we apply Proposition 5.7 to conclude that $\mathrm{cl}(\pi(V))$ has a smooth real point. If V is defined over $\mathbb{R}$ but has no smooth real point, we apply Proposition 5.8 and deduce that $\mathrm{cl}(\pi(V))$ has no smooth real points. Finally, if V is not defined over $\mathbb{R}$ we apply Proposition 5.9 to show that $\mathrm{cl}(\pi(V))$ is not defined over $\mathbb{R}$. □

Corollary 5.11. *Let $V \subset \mathbb{C}^n$ be an irreducible variety of dimension k, and $\pi\colon \mathbb{C}^n \to \mathbb{C}^{k+1}$ a generic projection defined over $\mathbb{R}$. Then the following are equivalent:*

(i) V is defined over $\mathbb{R}$ and the real generators of $\mathcal{I}(V)$ define a real radical ideal in $\mathbb{R}[\mathrm{x}]$;
(ii) $\mathcal{I}(\pi(V))$ is generated by a real polynomial, irreducible over $\mathbb{C}$, which changes sign in $\mathbb{R}^{k+1}$.

Proof. By Theorem 5.3, real generators of $\mathcal{I}(V)$ define a real radical ideal if and only if V has a smooth real point . Then $(i) \iff (ii)$ follows from Theorem 5.10 and Theorem 5.5. □

We finally describe the algorithm for testing real radicality.

Algorithm 5.1: Test real radicality

Input: An irreducible variety $V \subset \mathbb{C}^n$ of dim. k and $\varepsilon, r > 0$.

(i) Fix a generic projection $\pi\colon \mathbb{C}^n \to \mathbb{C}^{k+1}$;
(ii) Compute the irreducible polynomial h defining $\mathrm{cl}(\pi(V))$;
(iii) If h is not real return false;
(iv) Choose a generic point $\xi \in \mathbb{R}^{k+1}$ such that $h(\xi) \neq 0$;
(v) $s := \mathrm{sign}(h(\xi))$;
(vi) Let $f = \|\mathrm{x} - \xi\|^2$. Solve the MOP:

$$f^*_{\mathrm{MoM},d} = \inf\{\langle \sigma, f\rangle \mid \sigma \in \mathcal{L}_{2d}(\pm(h + s\varepsilon), r^2 - f),\ \langle \sigma, 1\rangle = 1\};$$

(vii) Extract a minimizer η and check that $h(\xi)h(\eta) < 0$.

Output: False if the MOP is not feasible, true if the MOP is feasible and $h(\xi)h(\eta) < 0$.

In step (i) we fix a generic real projection such that V is birational to $\mathrm{cl}(\pi(V))$ (Lemma 5.6).

In steps (ii) and (iii) we compute a minimal degree polynomial h of the hypersurface $\mathrm{cl}(\pi(V))$, scaled so that one of its coefficients is 1 and stop if it has non real coefficients.

In steps (iv), (v) and (vi) we check if the real polynomial h defines a real radical ideal, using Theorem 5.5. We find $\xi \in \mathbb{R}^{k+1}$ where h is not vanishing, and then search another point where h has opposite sign, by Moment Optimization.

If h does not change sign then $\mathcal{V}_{\mathbb{R}}(h + s\varepsilon) = \emptyset$ and the MOP will not be feasible (see for instance [21]).

On the other hand if h changes sign there exist $\eta \in \mathbb{R}^{k+1}$ such that $h(\xi)h(\eta) < 0$. If $\|\eta - \xi\| < r$ and $0 < \varepsilon \leq f(\eta)$ then the MOP has a solution. For generic ξ the minimizer will be a unique smooth point, the MOP will be exact (since we added the ball constraint $r^2 - f \leq 0$, the Archimedean property holds and generecally the MOM relaxation is exact), and we can certify that h changes sign. The constraint $r^2 - \|\mathrm{x} - \xi\|^2 \geq 0$ is not necessary if $\mathcal{V}_{\mathbb{R}}(h)$ is compact, since in this case the Archimedean hypothesis is already satisfied.

The correctness of Algorithm 5.1 follows from Corollary 5.11.

5.4 Test

We test Algorithm 5.1 for two simple cases, using the Julia packages `MomentTools.jl` and `MultivariateSeries.jl`.

Example 5.12. We check that the irreducible polynomial $h = x^2 + y^2 \in \mathbb{R}[x, y]$ defines an ideal $I = (h)$ that is not real radical. We randomly choose $\xi = (-1.5667884102749219, -0.5028780359864093)$, where $h(\xi) > 0$. We check that h does not change sign, detecting the infeasibility of the optimization problem.

```
X = @polyvar x y
h = x^2 + y^2
s = sign(f(X => xi))
dist = sum((xi - vec(X)).^2)
e = 0.01
v, M = minimize(dist, [h+s*e], [9 - dist],
                                  X, 4, optimizer);
```

The termination status `termination_status(M.model)` of the optimization:

```
INFEASIBLE::TerminationStatusCode = 2
```

shows the infeasibility of the moment optimization program and that I is not real radical.

In the same way we detect the sign change. For $h = x^2 + y^2 - 1$ and ξ as above, we find $\eta = (-0.9473807839956285, -0.30408822493309284)$ and $h(\xi)h(\eta) < 0$.

In the previous examples we could avoid the ball constraint $r^2 - \|\mathrm{x} - \xi\|^2 \leq 0$, since in these cases $\mathcal{V}_{\mathbb{R}}(h)$ is compact and the Archimedean condition is already satisfied.

6 COMPUTING THE REAL RADICAL

With the main ingredients, we can now describe the algorithm for computing the real radical of an ideal $I = (\mathrm{f})$, presented as the intersection of real prime ideals. The steps, summarised in Algorithm 6.1, are detailed hereafter.

In step (ii) we compute a generic element of $\mathcal{L}_{2d+2}(\pm\mathrm{f})$ solving a MOP with a constant objective function.

In step (iii) we use Algorithm 4.1 to compute the graded basis k.

In step (iv) we find the irreducible components of the variety $\mathcal{V}_{\mathbb{C}}(\mathrm{k})$, described by witness sets (see e.g. [4]). The embedded components of (k) are not recovered by this technique.

In step (v) we control if the irreducible components of $\mathcal{V}_{\mathbb{C}}(\mathrm{k})$ are real, using Algorithm 5.1.

Algorithm 6.1: Real radical

Input: Polynomials $\mathrm{f} = (f_1, \ldots, f_s) \subset \mathbb{R}[\mathrm{x}]$.
$d := \max(\deg(\mathrm{f}_i), i = 1, \ldots, s) - 1$; success := false;
Repeat until success
(i) $d := d + 1$
(ii) Compute a generic element σ^* of $\mathcal{L}_{2d+2}(\pm\mathrm{f})$
(iii) Compute a graded basis k of $\mathrm{Ann}_d(\sigma^*)$ (Algorithm 4.1)
(iv) Compute the numerical irreducible components V_i of $V_{\mathbb{C}}(\mathrm{k})$ (described by witness sets)
(v) For each component V_i, check that V_i is real (Algorithm 5.1). If not repeat from step (i).
(vi) success := true
(vii) For each component V_i compute defining equations $\mathrm{h}_i = \{h_{i,1}, \ldots, h_{i,n+1}\}$ of V_i
Output: The polynomials h_i generating the minimal real prime ideals $\mathfrak{p}_i$ lying over (f).

In step (vii), the equations defining V_i are obtained from $n+1$ generic projections. In particular, the equation of a generic projection of V_i used in step (ii) of Algorithm 5.1 provides one of the defining equation, say $h_{i,1}$.

We prove the correctness of the algorithm. By Theorem 3.3 we have $\mathcal{V}_{\mathbb{R}}(\mathrm{k}) = \mathcal{V}_{\mathbb{R}}(\mathrm{f})$ for $d \geq \max(\deg(\mathrm{f}))$. Let $\mathfrak{p}_i = (\mathrm{h}_i)$ in step (vii). By construction $\mathcal{V}_{\mathbb{R}}(\mathrm{k}) = \bigcup_i (V_i)_{\mathbb{R}} = \bigcup_i \mathcal{V}_{\mathbb{R}}(\mathfrak{p}_i) = \mathcal{V}_{\mathbb{R}}(\bigcap_i \mathfrak{p}_i)$. If step (v) succeeds, all the $\mathfrak{p}_i$'s are real radical, and thus $\bigcap_i \mathfrak{p}_i$ is real radical. Since $\mathcal{V}_{\mathbb{R}}(\mathrm{f}) = \mathcal{V}_{\mathbb{R}}(\bigcap_i \mathfrak{p}_i)$, by the Real Nullstellensatz $\bigcap_i \mathfrak{p}_i = \sqrt[\mathbb{R}]{\mathrm{f}}$ and the $\mathfrak{p}_i$ are the real prime ideal lying over (f). The loop stops for some $d \gg 0$ by Theorem 3.3.

Algorithm 6.1 computes the minimal real prime ideals lying over (f), but does not check that the equations k define a real radical ideal. If the ideal (k) has no embedded component and the prime ideals $\mathfrak{p}_i$ are of multiplicity 1 (checked with the Jacobian criterion for h at a witness point of $\mathfrak{p}_i$), then the success of step (v) implies that $\mathrm{k} = \mathrm{Ann}_d(\sigma^*)$ defines the real radical of (f).

Algorithm 6.1 can be simplified in the case where $\mathcal{V}_{\mathbb{R}}(\mathrm{f})$ is finite. We can check that $(\mathrm{k}) = \sqrt[\mathbb{R}]{\mathrm{f}}$, for $\mathrm{k} = \mathrm{Ann}_d(\sigma^*)$, using the flat extension criterion. We can also detect this condition with the initial of k, see Remark 4.2. In this case, σ^* extends to a positive linear functional on $\mathbb{R}[\mathrm{x}]$ and $(\mathrm{k}) = \sqrt[\mathbb{R}]{\mathrm{f}}$.

Similarly, when the ideal (k) is prime, one only needs to check that it is real (using Algorithm 5.1 on a generic projection), steps (iv), (vii) can be skipped and we obtain $(\mathrm{k}) = \sqrt[\mathbb{R}]{\mathrm{f}}$. When (k) is real radical, the algorithm can even output directly $(\mathrm{k}) = \sqrt[\mathbb{R}]{\mathrm{f}}$.

7 EXAMPLES

We illustrate Algorithm 6.1, with the Julia package `MomentTools.jl`[1], using the Semi-Definite Programm optimizer `Mosek`.

7.1 The isolated singular locus of a real surface

Example 7.1. Let $f = -10z^4 + x^3 - 3x^2z + 3xz^2 + 20yz^2 - z^3 - 10x^2 + 20xz - 10y^2 - 10z^2, g = 5 - (x^2 + y^2 + z^2)$ and $S = \{\, \xi \in \mathbb{R}^3 \mid f(\xi) = 0,\ g(\xi \geq 0) \,\}$. We want to compute the S-radical of $I = (f)$, which is equal to $(z - x, x^2 - y)$.

[1] https://gitlab.inria.fr/AlgebraicGeometricModeling/MomentTools.jl

```
X = @polyvar x y z
f = -10*z^4 + x^3 - 3*x^2*z + 3*x*z^2 + 20*y*z^2
         - z^3 - 10*x^2 + 20*x*z - 10*y^2 - 10*z^2
g = 5 - (x^2+y^2+z^2)
v, M = minimize(one(f),[f], [g], X, 6, optimizer)
sigma = get_series(M)[1]
L = monomials(X,seq(0:3))
K,In,P,B = annihilator(sigma, L)
```

We compute a generic positive linear functional σ (by optimising the constant function 1 on S), a graded basis K of $(\mathrm{Ann}_d(\sigma))$, the initial monomials `In` of K, a basis P of $\frac{\mathbb{R}[\mathrm{x}]}{(\mathrm{Ann}_d(\sigma))}$ orthogonal with respect to $\langle\cdot,\cdot\rangle_\sigma$ and a monomial basis B of $\frac{\mathbb{R}[\mathrm{x}]}{(\mathrm{Ann}_d(\sigma))}$. The elements of K are:

```
-0.999999935776211x - 2.027089868945844e-9y + z
                            + 1.9280308682132505e-9
x² - 1.9114608711668615e-8x - 0.9999998601127081y
                            - 2.6012502193917264e-7
```

These polynomials define a parametrisation of parabola and thus generate a real radical ideal. They are approximation of the generators of the S-radical of I within an error `3.e-7`.

Example 7.2. We compute equations for the hold of the Whitney umbrella. Let $f = x^2 - y^2 z, g = 1 - (x^2 + y^2 + (z+2)^2)$ and $S = \{\, \xi \in \mathbb{R}^3 \mid f(\xi) = 0,\ g(\xi \geq 0) \,\}$. We compute the S-radical of $I = (f)$, which is equal to (x, y). Proceding as above, we obtain for K, the polynomials:

```
x + 3.1388489268444904e-21
y + 3.6567022687420305e-21
```

These polynomials are a good approximation of the generators (x, y) of the real radical, defining the singular locus of the Whitney umbrella.

7.2 Components of different dimensions

Example 7.3. This example is taken from [30, ex. 9.6]. We want to compute the real radical of $I = (f_1, f_2, f_3) \subset \mathbb{R}[x, y, z]$, where:

$$f_1 = x^2 + x\,y - x\,z - x - y + z$$
$$f_2 = x\,y + 2\,y^2 - y\,z - x - 2\,y + z$$
$$f_3 = x\,z + y\,z - z^2 - x - y + z.$$

Its variety has three irreducible components, two lines and a point, defined by the real prime ideals $\mathfrak{p}_1 = (x-z, y)$, $\mathfrak{p}_2 = (x-z+1, y-1)$ and $\mathfrak{m} = (x-1, y-1, z-1)$. In the primary decomposition of I there is an embedded component $\mathfrak{m}'$, corresponding to the point $(1, 0, 1) \in \mathcal{V}(\mathfrak{p}_1)$ which has multiplicity two. The real radical of I is $\sqrt[\mathbb{R}]{I} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m} = (y^2 - y, x^2 - 2xz + z^2 + x - z, xz + yz - z^2 - x - y + z, xy + xz - z^2 - 2x - y + 2z)$.

We compute $\sqrt[\mathbb{R}]{I}$ as described in the algorithm.

```
v, M = minimize(one(f1),[f1,f2,f3], [], X, 8, optimizer)
sigma = get_series(M)[1]
L = monomials(X,seq(0:3))
K,I,P,B = annihilator(sigma, L)
```

The elements of K are:

```
-0.9999999985579915x² - 0.9999999940764733xy + xz +
      0.9999999838152133x + 0.9999999868597321y -
      0.9999999838041349z - 2.550976860304921e-10
4.386341684978274e-7x² + 3.2135911001749273e-7xy + y²
```

```
       - 8.511512801700947e-7x - 1.0000008530709377y
       + 9.888494964176088e-7z - 5.851033908621897e-8
8.763853490689755e-7x² - 0.9999993625797754xy + yz +
      0.9999983122334805x - 1.6948939787209127e-6y -
        0.9999980367703514z - 1.1680315895740145e-7
-0.9999991215344914x² - 1.99999935020258xy + z² +
           2.99999828318184x + 1.9999982828997438y -
          2.999998007995895z - 1.1724998920381591e-7
```

which are approximately (within an error of `1.e-6`) generators of $\sqrt[\mathbb{R}]{I}$.

Example 7.4. This example is taken from [11, 8.2]. We want to compute the real radical of $I = (f_1, f_2, f_3) \subset \mathbb{R}[x, y, z]$, where:

$$f_1 = xyz$$
$$f_2 = z(x^2 + y^2 + z^2 + y)$$
$$f_3 = y(y + z).$$

The associated complex variety has four irreducible components: two conjugates lines intersecting in the origin, another line (double for f) and a point. The real variety is given by a line $\mathfrak{p} = (y, z)$ and a point $\mathfrak{m} = (x, 2y + 1, 2x - 1)$. The real radical is $\sqrt[\mathbb{R}]{I} = \mathfrak{p} \cap \mathfrak{m} = (yx, z + y, y^2 + \frac{y}{2})$. A direct check shows that these polynomials generate a real radical ideal.

We compute $\sqrt[\mathbb{R}]{I}$ as described above and obtain for `K`:

```
-6.53338688785662e-19x + 0.9995827809845268y + z
                       - 0.00020850768649473272
-1.4685109255649737e-19x² + xy + 5.9730164512226755e-6x
      + 2.1320912413237275e-19y + 1.0655056374451632e-19
-2.268705086623265e-6x² + y² + 1.88498770272315e-19x +
             0.4998194337295852y + 4.384653173789382e-6
```

approximating (within an error of `5.e-4`) the generators of $\sqrt[\mathbb{R}]{I}$.

7.3 Limitations

Algorithm 6.1 is a symbolic-numeric algorithm, which output depends on the quality of the numerical tools that are involved. In particular, the numerical quality of the generic positive linear functional σ^*, produced by a SDP solver, impacts the computation of generators of the real radical. This computation depends on a threshold used to determine when a polynomial is in annihilator. A detailled analysis of the numerics behind the algorithm as well as bounds analysing its complexity are left for futur investigations.

REFERENCES

[1] Michael Artin. 2017. *Algebra* (2 edizione ed.). Pearson College Div, New York, New York.

[2] M. F. Atiyah and I. G. MacDonald. 1994. *Introduction To Commutative Algebra*. Avalon Publishing.

[3] Lorenzo Baldi and Bernard Mourrain. 2020. Exact Moment Representation in Polynomial Optimization. (2020). https://hal.archives-ouvertes.fr/hal-03082531 preprint.

[4] Daniel J. Bates, Jonathan D. Haunstein, Andrew J. Sommese, and Charles W. Wampler. 2013. *Numerically Solving Polynomial Systems with Bertini*. Society for Industrial and Applied Mathematics, USA.

[5] E. Becker and R. Neuhaus. 1993. Computation of Real Radicals of Polynomial Ideals. In *Computational Algebraic Geometry (Progress in Mathematics)*, Frédéric Eyssette and André Galligo (Eds.). Birkhäuser, Boston, MA, 1–20.

[6] Eberhard Becker and Joachim Schmid. 1999. On the Real Nullstellensatz. In *Algorithmic Algebra and Number Theory*, B. Heinrich Matzat, Gert-Martin Greuel, and Gerhard Hiss (Eds.). Springer, Berlin, Heidelberg, 173–185.

[7] Cristina Blanco, Gabriela Jeronimo, and Pablo Solernó. 2004. Computing generators of the ideal of a smooth affine algebraic variety. *Journal of Symbolic Computation* 38, 1 (2004), 843–872.

[8] Jacek Bochnak, Michel Coste, and Marie-Francoise Roy. 1998. *Real Algebraic Geometry*. Springer-Verlag, Berlin Heidelberg.

[9] Alin Bostan, Frédéric Chyzak, Marc Giusti, Romain Lebreton, Grégoire Lecerf, Bruno Salvy, and Éric Schost. 2017. *Algorithmes Efficaces en Calcul Formel* (1° edizione ed.). Frédéric Chyzak.

[10] Daniel A. Brake, Jonathan D. Hauenstein, and Alan C. Liddell. 2016. Validating the Completeness of the Real Solution Set of a System of Polynomial Equations. In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*. ACM, Waterloo ON Canada, 143–150.

[11] Daniel A. Brake, Jonathan D. Hauenstein, and Alan C. Liddell. 2016. Validating the Completeness of the Real Solution Set of a System of Polynomial Equations. In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation (ISSAC '16)*. Association for Computing Machinery, New York, NY, USA, 143–150.

[12] Changbo Chen, James H. Davenport, John P. May, Marc Moreno Maza, Bican Xia, and Rong Xiao. 2013. Triangular Decomposition of Semi-Algebraic Systems. *Journal of Symbolic Computation* 49 (2013), 3–26.

[13] David A. Cox, John B. Little, and Donal O'Shea. 2015. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra* (fourth edition ed.). Springer, Cham Heidelberg New York Dordrecht London.

[14] Raúl E. Curto and Lawrence A. Fialkow. 1998. *Flat Extensions of Positive Moment Matrices: Recursively Generated Relations*. American Mathematical Soc.

[15] A. Galligo and N. Vorobjov. 1995. Complexity of Finding Irreducible Components of a Semialgebraic Set. *Journal of Complexity* 11, 1 (1995), 174–193.

[16] Jonathan D. Hauenstein, Andrew J. Sommese, and Charles W. Wampler. 2011. Regenerative Cascade Homotopies for Solving Polynomial Systems. *Appl. Math. Comput.* 218, 4 (2011), 1240–1246.

[17] Jean-Louis Krivine. 1964. Anneaux préordonnés. *Journal d'analyse mathématique* 12 (1964), p. 307–326.

[18] Robert Krone and Anton Leykin. 2017. Numerical Algorithms for Detecting Embedded Components. *Journal of Symbolic Computation* 82 (2017), 1–18.

[19] Jean B. Lasserre. 2001. Global Optimization with Polynomials and the Problem of Moments. *SIAM Journal on Optimization* 11, 3 (2001), 796–817.

[20] Jean-Bernard Lasserre, Monique Laurent, Bernard Mourrain, Philipp Rostalski, and Philippe Trébuchet. 2013. Moment matrices, border bases and real radical computation. *Journal of Symbolic Computation* 51 (2013), 63–85.

[21] Jean Bernard Lasserre, Monique Laurent, and Philipp Rostalski. 2008. Semidefinite Characterization and Computation of Zero-Dimensional Real Radical Ideals. *Foundations of Computational Mathematics* 8, 5 (2008), 607–647.

[22] Monique Laurent and Bernard Mourrain. 2009. A Generalized Flat Extension Theorem for Moment Matrices. *Archiv der Mathematik* 93, 1 (2009), 87–98.

[23] Monique Laurent and Philipp Rostalski. 2012. The Approach of Moments for Polynomial Equations. In *Handbook on Semidefinite, Conic and Polynomial Optimization*, Miguel F. Anjos and Jean B. Lasserre (Eds.). Springer US, Boston, MA, 25–60.

[24] Grégoire Lecerf. 2003. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *Journal of Complexity* 19, 4 (2003), 564–596.

[25] Yue Ma, Chu Wang, and Lihong Zhi. 2016. A Certificate for Semidefinite Relaxations in Computing Positive-Dimensional Real Radical Ideals. *Journal of Symbolic Computation* 72 (2016), 1–20.

[26] Murray Marshall. 2008. *Positive Polynomials and Sums of Squares*. American Mathematical Soc.

[27] Bernard Mourrain. 2017. Fast algorithm for border bases of Artinian Gorenstein algebras. In *ISSAC'17 – International Symposium on Symbolic and Algebraic Computation*. ACM New York, NY, USA, Kaiserslautern, Germany, 333–340.

[28] Bernard Mourrain. 2018. Polynomial–Exponential Decomposition From Moments. *Foundations of Computational Mathematics* 18, 6 (2018), 1435–1492.

[29] Rolf Neuhaus. 1998. Computation of Real Radicals of Polynomial Ideals — II. *Journal of Pure and Applied Algebra* 124, 1-3 (1998), 261–280.

[30] Philipp Rostalski. 2009. *Algebraic moments: real root finding and related topics*. Doctoral Thesis. ETH Zurich. Accepted: 2017-06-13T08:51:18Z.

[31] Marie-Francoise Roy and Nicolai Vorobjov. 2002. The Complexification and Degree of a Semi-Algebraic Set. *Mathematische Zeitschrift* 239 (2002), 131–142.

[32] Mohab Safey El Din, Zhi-Hong Yang, and Lihong Zhi. 2021. Computing Real Radicals and S-Radicals of Polynomial Systems. *Journal of Symbolic Computation* 102 (2021), 259–278.

[33] Yoshiyuki Sekiguchi, Tomoyuki Takenawa, and Hayato Waki. 2013. Real Ideal and the Duality of Semidefinite Programming for Polynomial Optimization. *Japan Journal of Industrial and Applied Mathematics* 30, 2 (2013), 321–330.

[34] Igor R. Shafarevich. 2013. *Basic Algebraic Geometry 1: Varieties in Projective Space* (3 ed.). Springer-Verlag, Berlin Heidelberg.

[35] Andrew J. Sommese, Jan Verschelde, and Charles W. Wampler. 2001. Numerical Decomposition of the Solution Sets of Polynomial Systems into Irreducible Components. *SIAM J. Numer. Anal.* 38, 6 (2001), 2022–2046.

[36] Silke J Spang. 2008. A Zero-Dimensional Approach to Compute Real Radicals. *Computer Science Journal of Moldova* 16, 1 (2008), 64–92.
[37] Gilbert Stengle. 1974. A Nullstellensatz and a Positivstellensatz in Semialgebraic Geometry. *Math. Ann.* 207, 2 (1974), 87–97.
[38] Lloyd N. Trefethen and David Bau. 1997. *Numerical Linear Algebra.* SIAM.
[39] Bican Xia and Lu Yang. 2002. An Algorithm for Isolating the Real Solutions of Semi-Algebraic Systems. *Journal of Symbolic Computation* 34, 5 (2002), 461–477.