Theoretical Computer Science 410 (2009) 2685–2700

Contents lists available at ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

A prolongation–projection algorithm for computing the finite real variety of an ideal

Jean B. Lasserre [a], Monique Laurent [b], Philipp Rostalski [c,*]

[a] LAAS-CNRS and Institute of Mathematics, University of Toulouse, LAAS, 7 Avenue du Colonel Roche, 31 077 Toulouse Cedex 4, France
[b] CWI, Science Park 123, 1098 XG Amsterdam, The Netherlands
[c] Automatic Control Lab., ETH Zurich, Physikstrasse 3, 8092 Zurich, Switzerland

ARTICLE INFO

Article history:
Received 23 June 2008
Received in revised form 12 January 2009
Accepted 19 March 2009
Communicated by V. Pan

Keywords:
Real solving
Finite real variety
Numerical algebraic geometry
Semidefinite optimization

ABSTRACT

We provide a real algebraic symbolic–numeric algorithm for computing the real variety $V_{\mathbb{R}}(I)$ of an ideal $I \subseteq \mathbb{R}[\mathbf{x}]$, assuming $V_{\mathbb{R}}(I)$ is finite (while $V_{\mathbb{C}}(I)$ could be infinite). Our approach uses sets of linear functionals on $\mathbb{R}[\mathbf{x}]$, vanishing on a given set of polynomials generating I and their prolongations up to a given degree, as well as on polynomials of the real radical ideal $\sqrt[\mathbb{R}]{I}$ obtained from the kernel of a suitably defined moment matrix assumed to be positive semidefinite and of maximum rank. We formulate a condition on the dimensions of projections of these sets of linear functionals, which serves as a stopping criterion for our algorithm; this new criterion is satisfied earlier than the previously used stopping criterion based on a rank condition for moment matrices. This algorithm is based on standard numerical linear algebra routines and semidefinite optimization and combines techniques from previous work of the authors together with an existing algorithm for the complex variety.

1. Introduction

Polynomial equations play a crucial role in mathematics and are widely used in an emerging number of modern applications. Recent years have witnessed a new trend in algebraic geometry and polynomial system solving, namely numerical polynomial algebra [25] or numerical algebraic geometry [24]. Algorithms in this field deal with the problem of (approximately) computing objects of interest in the classical area of algebraic geometry with a focus on polynomial root finding.

There is a broad literature for the problem of computing complex roots, that deals with numerical and symbolic algorithms, ranging from numerical continuation methods as in e.g. Verschelde [27] to exact methods as in e.g. Rouillier [22], or more general Gröbner or border bases methods; see e.g. the monograph [9] and the references therein.

In many practical applications, one is only interested in the *real* solutions of a system of polynomial equations, possibly satisfying additional polynomial inequality constraints. An obvious approach for finding all real roots of a system of polynomial equations is to first compute all complex solutions, i.e., the algebraic variety $V_{\mathbb{C}}(I)$ of the associated ideal $I \subseteq \mathbb{R}[\mathbf{x}]$, and then to sort the real variety $V_{\mathbb{R}}(I) = \mathbb{R}^n \cap V_{\mathbb{C}}(I)$ from $V_{\mathbb{C}}(I)$ afterwards. However, in many practical instances, the number of real roots is considerably smaller than the total number of roots and, in some cases, it is finite while $|V_{\mathbb{C}}(I)| = \infty$.

The literature about algorithms tailored to the problem of real solving systems of polynomial equations is by far not as broad as for the problem of computing complex roots. Often local Newton type methods or subdivision methods based

* Corresponding author. Tel.: +41 78 677 89 59.
E-mail addresses: lasserre@laas.fr (J.B. Lasserre), M.Laurent@cwi.nl (M. Laurent), rostalski@control.ee.ethz.ch (P. Rostalski).

0304-3975/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2009.03.024

on the Descartes rule of sign, on Sturm–Habicht sequences or on Hermite quadratic forms are used; see e.g. [1,19,21] for a discussion. In [12] we gave an algorithm for finding $V_{\mathbb{R}}(I)$ (assumed to be finite), and a semidefinite characterization as well as a border (or Gröbner) basis of the real radical ideal $\sqrt[\mathbb{R}]{I}$, by using linear algebra combined with semidefinite programming (SDP) techniques. We exploited the fact that all information needed to compute the above objects is contained in the so-called moment matrix (whose entries depend on the polynomials generating the ideal I) and its geometric properties when this matrix is required to be positive semidefinite with maximum rank. We use the name *(real-root) moment-matrix algorithm* for the algorithm proposed in [12]. This algorithm was later extended to the computation of all complex roots in [13]. A feature of the real-root moment-matrix algorithm is that it requires solving a sequence of SDP problems involving matrices of increasing size until a certain rank condition is satisfied. Solving the SDP problem is the computationally most demanding task in the algorithm. It is thus important to be able to terminate the algorithm as early as possible so that the size of the matrices does not grow too much. This is the motivation for the present paper where we present a new stopping condition, which is satisfied at least as early as the rank condition of [12] (and often earlier on examples). This leads to a new algorithm which we name *(real-root) prolongation–projection algorithm* since its stopping condition involves computing the dimensions of projections of certain sets of linear functionals on spaces of polynomials. This new algorithm arises by incorporating several ideas of [12,13] into an existing symbolic–numeric solver dedicated to compute $V_{\mathbb{C}}(I)$ (as described e.g. in [31]). A detailed description will be given in Section 5 but, in order to ease comparison with the moment-matrix method of [12], we now give a brief sketch of both methods.

Sketch of the real-root moment-matrix and prolongation–projection algorithms

While methods based on Gröbner bases work with the (primal) ring of polynomials $\mathbb{R}[\mathbf{x}]$, its ideals and their associated quotient spaces, we follow a dual approach here. The algorithms proposed in [12] and in this work manipulate specific subspaces of $(\mathbb{R}[\mathbf{x}])^*$, the space of linear forms dual to the ring of multivariate polynomials.

We denote by $(\mathbb{R}[\mathbf{x}]_t)^*$ the space of linear functionals on the set $\mathbb{R}[\mathbf{x}]_t$ of polynomials with degree at most t and use the notion of *moment matrix* $M_s(L) := (L(\mathbf{x}^\alpha \mathbf{x}^\beta))$ (indexed by monomials of degree at most s) for $L \in (\mathbb{R}[\mathbf{x}]_{2s})^*$. (See Section 2 for more definitions.) Say we want to compute the (finite) real variety $V_{\mathbb{R}}(I)$ of an ideal I given by a set of generators $h_1, \ldots, h_m \in \mathbb{R}[\mathbf{x}]$ with maximum degree D. A common step in both methods is to compute a maximum rank moment matrix $M_{\lfloor t/2 \rfloor}(L)$, where $L \in (\mathbb{R}[\mathbf{x}]_t)^*$ vanishes on the set $\mathcal{H}_t$ of all prolongations up to degree t of the polynomials h_j; this step is carried out with a numerical algorithm for semidefinite optimization. From that point on both methods use distinct strategies. In the moment-matrix method one checks whether the rank condition: $\operatorname{rank} M_s(L) = \operatorname{rank} M_{s-1}(L)$ holds for some $D \le s \le \lfloor t/2 \rfloor$; if so, then one can conclude that $\sqrt[\mathbb{R}]{I}$ is generated by the polynomials in the kernel of $M_s(L)$ and extract $V_{\mathbb{R}}(I)$; if not, iterate with $t+1$. In the prolongation–projection algorithm, one considers $\mathcal{G}_t$, the set obtained by adding to $\mathcal{H}_t$ prolongations of the polynomials in the kernel of $M_{\lfloor t/2 \rfloor}(L)$, its border $\mathcal{G}_t^+ := \mathcal{G}_t \cup_i x_i \mathcal{G}_t$, as well as the set $\mathcal{G}_t^\perp$ of linear functionals on $\mathbb{R}[\mathbf{x}]_t$ vanishing on $\mathcal{G}_t$, and its projections $\pi_s(\mathcal{G}_t^\perp)$ on various degrees $s \le t$. We give conditions on the dimension of these linear subspaces ensuring the computation of the real variety $V_{\mathbb{R}}(I)$ and generators for the real radical ideal $\sqrt[\mathbb{R}]{I}$. Namely, if $\dim \pi_s(\mathcal{G}_t^\perp) = \dim \pi_{s-1}(\mathcal{G}_t^\perp) = \dim \pi_s((\mathcal{G}_t^+)^\perp)$ holds for some $D \le s \le t$, then one can compute an ideal J nested between I and $\sqrt[\mathbb{R}]{I}$ so that $V_{\mathbb{R}}(I) = V_{\mathbb{R}}(J)$, with equality $J = \sqrt[\mathbb{R}]{I}$ if $\dim \pi_s(\mathcal{G}_t^\perp) = |V_{\mathbb{R}}(I)|$; if not, iterate with $t+1$.

Both algorithms are tailored to finding real roots and terminate assuming that $V_{\mathbb{R}}(I)$ is finite (while $V_{\mathbb{C}}(I)$ could be infinite). However, the order t at which the dimension condition holds is at most the order at which the rank condition holds. Hence the prolongation–projection algorithm terminates earlier than the moment-matrix method, which often permits saving a few semidefinite optimization steps with larger moment matrices (as shown on a few examples in Section 6).

Contents of the paper

Section 2 provides some basic background on polynomial ideals and moment matrices whereas Section 3 presents the basic principles behind the prolongation–projection method and Theorem 4, our main result, provides a new stopping criterion for the computation of $V_{\mathbb{R}}(I)$. Section 4 relates the prolongation–projection algorithm to the moment-matrix method of [12]. In particular, Proposition 12 shows that the rank condition used as stopping criterion in the moment-matrix method is equivalent to a strong version of the new stopping criterion; as a consequence the new criterion is satisfied at least as early as the rank condition (Corollary 13). Section 5 contains a detailed description of the algorithm whose behavior is illustrated on a few examples in Section 6.

2. Preliminaries

2.1. Polynomial ideals and varieties

We briefly introduce some notation and preliminaries for polynomials used throughout the paper and refer e.g. to [4,3] for more details.

Throughout $\mathbb{R}[\mathbf{x}] := \mathbb{R}[x_1, \ldots, x_n]$ is the ring of real polynomials in the n variables $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbb{R}[\mathbf{x}]_t$ is the subspace of polynomials of degree at most $t \in \mathbb{N}$. For $\alpha \in \mathbb{N}^n$, $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ is the monomial with exponent α and degree $|\alpha| = \sum_i \alpha_i$. For an integer $t \geq 0$, the set $\mathbb{N}^n_t = \{\alpha \in \mathbb{N}^n \mid |\alpha| \leq t\}$ corresponds to the set of monomials of degree at most t, and $\mathbb{T}^n = \{\mathbf{x}^\alpha \mid \alpha \in \mathbb{N}^n\}$, $\mathbb{T}^n_t = \{\mathbf{x}^\alpha \mid \alpha \in \mathbb{N}^n_t\}$ denote the set of all monomials and of all monomials of degree at most t, respectively. Given $S \subseteq \mathbb{R}[\mathbf{x}]$, set $x_i S := \{x_i p \mid p \in S\}$. The set

$$S^+ := S \cup x_1 S \cup \cdots \cup x_n S$$

denotes the one degree *prolongation* of S and, for $\mathcal{B} \subseteq \mathbb{T}^n$, $\partial\mathcal{B} := \mathcal{B}^+ \setminus \mathcal{B}$ is called the set of *border* monomials of $\mathcal{B}$. A set $\mathcal{B} \subseteq \mathbb{T}^n$ is said to be *connected to 1* if $1 \in \mathcal{B}$ and every monomial $m \in \mathcal{B} \setminus \{1\}$ can be written as $m = x_{i_1} \ldots x_{i_k}$ with $x_{i_1}, x_{i_1} x_{i_2}, \ldots, x_{i_1} \cdots x_{i_k} \in \mathcal{B}$. For instance, $\mathcal{B}$ is connected to 1 if it is closed under taking divisions, i.e. $m \in \mathcal{B}$ and m' divides m implies $m' \in \mathcal{B}$.

Given $h_1, \ldots, h_m \in \mathbb{R}[\mathbf{x}]$, $I = (h_1, \ldots, h_m)$ is the ideal generated by $h_1, \ldots, h_m$, its algebraic variety is

$$V_{\mathbb{C}}(I) := \left\{v \in \mathbb{C}^n \mid h_j(v) = 0 \ \forall j = 1, \ldots, m\right\}$$

and its real variety is $V_{\mathbb{R}}(I) := \mathbb{R}^n \cap V_{\mathbb{C}}(I)$. The ideal I is zero-dimensional when $V_{\mathbb{C}}(I)$ is finite. The vanishing ideal of a set $V \subseteq \mathbb{C}^n$ is the ideal

$$I(V) := \{f \in \mathbb{R}[\mathbf{x}] \mid f(v) = 0 \ \forall v \in V\}.$$

The Real Nullstellensatz [2, Chapter 4, Section 1] asserts that $I(V_{\mathbb{R}}(I))$ coincides with $\sqrt[\mathbb{R}]{I}$, the real radical of I, which is defined as

$$\sqrt[\mathbb{R}]{I} := \left\{p \in \mathbb{R}[\mathbf{x}] \;\middle|\; p^{2m} + \sum_j q_j^2 \in I \ \text{ for some } q_j \in \mathbb{R}[\mathbf{x}], m \in \mathbb{N} \setminus \{0\}\right\}.$$

Given a vector space A on $\mathbb{R}$, its dual vector space is the space $A^* = \mathrm{Hom}(A, \mathbb{R})$ consisting of all linear functionals from A to $\mathbb{R}$. Given $B \subseteq A$, set $B^\perp := \{L \in A^* \mid L(b) = 0 \ \forall b \in B\}$, and $\mathrm{Span}_{\mathbb{R}}(B) := \{\sum_{i=1}^m \lambda_i b_i \mid \lambda_i \in \mathbb{R}, b_i \in B\}$. Then $\mathrm{Span}_{\mathbb{R}}(B) \subseteq (B^\perp)^\perp$, with equality when A is finite dimensional.

For an ideal $I \subseteq \mathbb{R}[\mathbf{x}]$, the space $\mathcal{D}[I] := I^\perp = \{L \in (\mathbb{R}[\mathbf{x}])^* \mid L(p) = 0 \ \forall p \in I\}$, considered e.g. by Stetter [25], is isomorphic to $(\mathbb{R}[\mathbf{x}]/I)^*$ and $\mathcal{D}[I]^\perp = I$ when I is zero-dimensional. Recall that I is zero-dimensional precisely when $\dim \mathbb{R}[\mathbf{x}]/I < \infty$, and $|V_{\mathbb{C}}(I)| \leq \dim \mathbb{R}[\mathbf{x}]/I$ with equality precisely when $I = I(V_{\mathbb{C}}(I))$.

The canonical basis of $\mathbb{R}[\mathbf{x}]$ is the monomial set $\mathbb{T}^n$, with $\mathcal{D}_n := \{\mathbf{d}_\alpha \mid \in \mathbb{N}^n\}$ as corresponding dual basis for $(\mathbb{R}[\mathbf{x}])^*$, where

$$\mathbf{d}_\alpha(p) = \frac{1}{\prod_{i=1}^n \alpha_i!} \left(\frac{\partial^{|\alpha|}}{\partial x_1^{\alpha_1} \ldots \partial x_n^{\alpha_n}} p\right)(0) \quad \text{for } p \in \mathbb{R}[\mathbf{x}].$$

Thus any $L \in (\mathbb{R}[\mathbf{x}])^*$ can be written in the form $L = \sum_\alpha y_\alpha \mathbf{d}_\alpha$ (for some $y \in \mathbb{R}^{\mathbb{N}^n}$).

By restricting its domain to $\mathbb{R}[\mathbf{x}]_s$, any linear form $L \in (\mathbb{R}[\mathbf{x}])^*$ gives a linear form $\pi_s(L)$ in $(\mathbb{R}[\mathbf{x}]_s)^*$. Throughout we let π_s denote this projection from $(\mathbb{R}[\mathbf{x}])^*$ (or from $(\mathbb{R}[\mathbf{x}]_t)^*$ for any $t \geq s$) onto $(\mathbb{R}[\mathbf{x}]_s)^*$.

Given a zero-dimensional ideal $I \subseteq \mathbb{R}[\mathbf{x}]$, a well known method for computing $V_{\mathbb{C}}(I)$ is the so-called eigenvalue method which relies on the following theorem relating the eigenvalues of the multiplication operators in $\mathbb{R}[\mathbf{x}]/I$ to the points in $V_{\mathbb{C}}(I)$. See e.g. [3, Chapter 2, Section 4].

Theorem 1. *Let I be a zero-dimensional ideal in $\mathbb{R}[\mathbf{x}]$ and $h \in \mathbb{R}[\mathbf{x}]$. The eigenvalues of the multiplication operator*

$$\begin{array}{rccc} m_h: & \mathbb{R}[\mathbf{x}]/I & \longrightarrow & \mathbb{R}[\mathbf{x}]/I \\ & p \mod I & \mapsto & ph \mod I \end{array}$$

are the evaluations $h(v)$ of the polynomial h at the points $v \in V_{\mathbb{C}}(I)$. Moreover, given a basis $\mathcal{B}$ of $\mathbb{R}[\mathbf{x}]/I$, the eigenvectors of the matrix of the adjoint operator of m_h with respect to $\mathcal{B}$ are (up to scaling) the vectors $(b(v))_{b\in\mathcal{B}} \in \mathbb{R}^{|\mathcal{B}|}$ (for all $v \in V_{\mathbb{C}}(I)$).

The extraction of the roots via the eigenvalues of the multiplication operators requires knowledge of a basis of $\mathbb{R}[\mathbf{x}]/I$ and an algorithm for reducing a polynomial $p \in \mathbb{R}[\mathbf{x}]$ modulo the ideal I in order to construct the multiplication matrices. Algorithms using Gröbner bases can be used to perform this reduction by implementing a polynomial division algorithm (see [4, Chapter 1]) or, as we will do in this paper, generalized normal form algorithms using border bases (see [13,20,25] for details).

2.2. Moment matrices

Given $L \in (\mathbb{R}[\mathbf{x}])^*$, let Q_L denote the quadratic form on $\mathbb{R}[\mathbf{x}]$ defined by $Q_L(p) := L(p^2)$ for $p \in \mathbb{R}[\mathbf{x}]$. Q_L is said to be positive semidefinite, written as $Q_L \succeq 0$, if $Q_L(p) \geq 0$ for all $p \in \mathbb{R}[\mathbf{x}]$. Let $M(L)$ denote the matrix associated with Q_L in the canonical monomial basis of $\mathbb{R}[\mathbf{x}]$, with (α, β)-entry $L(\mathbf{x}^\alpha \mathbf{x}^\beta)$ for $\alpha, \beta \in \mathbb{N}^n$, so that

$$Q_L(p) = \sum_{\alpha,\beta \in \mathbb{N}^n} p_\alpha p_\beta L(\mathbf{x}^\alpha \mathbf{x}^\beta) = \mathrm{vec}(p)^{\mathrm{T}} M(L) \mathrm{vec}(p),$$

where $\mathrm{vec}(p)$ is the vector of coefficients of p in the monomial basis $\mathbb{T}^n$. Then $Q_L \succeq 0$ if and only if the matrix $M(L)$ is positive semidefinite. For a polynomial $p \in \mathbb{R}[\mathbf{x}]$, $p \in \mathrm{Ker}\, Q_L$ (i.e. $Q_L(p) = 0$ and so $L(pq) = 0$ for all $q \in \mathbb{R}[\mathbf{x}]$) if and only if $M(L)\mathrm{vec}(p) = 0$. Thus we may identify $\mathrm{Ker}\, M(L)$ with a subset of $\mathbb{R}[\mathbf{x}]$, namely we say that a polynomial $p \in \mathbb{R}[\mathbf{x}]$ lies in $\mathrm{Ker}\, M(L)$ if $M(L)\mathrm{vec}(p) = 0$. Then $\mathrm{Ker}\, M(L)$ is an ideal in $\mathbb{R}[\mathbf{x}]$, which is a real radical ideal when $M(L) \succeq 0$ (cf. [15,17]). For an integer $s \geq 0$, $M_s(L)$ denotes the principal submatrix of $M(L)$ indexed by $\mathbb{N}^n_s$. Then, in the canonical basis of $\mathbb{R}[\mathbf{x}]_s$, $M_s(L)$ is the matrix of the restriction of Q_L to $\mathbb{R}[\mathbf{x}]_s$, and $\mathrm{Ker}\, M_s(L)$ can be viewed as a subset of $\mathbb{R}[\mathbf{x}]_s$. It follows from an elementary property of positive semidefinite matrices that

$$M_t(L) \succeq 0 \Longrightarrow \mathrm{Ker}\, M_t(L) \cap \mathbb{R}[\mathbf{x}]_s = \mathrm{Ker}\, M_s(L) \quad \text{for } 1 \leq s \leq t, \tag{1}$$

$$M_t(L),\ M_t(L') \succeq 0 \Longrightarrow \mathrm{Ker}\, M_t(L + L') = \mathrm{Ker}\, M_t(L) \cap \mathrm{Ker}\, M_t(L'). \tag{2}$$

We now recall some results about moment matrices which played a central role in our previous work [12] and are used here again.

Theorem 2. *[5] Let $L \in (\mathbb{R}[\mathbf{x}]_{2s})^*$. If $\mathrm{rank}\, M_s(L) = \mathrm{rank}\, M_{s-1}(L)$, then there exists (a unique) $\tilde{L} \in (\mathbb{R}[\mathbf{x}])^*$ such that $\pi_{2s}(\tilde{L}) = L$, $\mathrm{rank}\, M(\tilde{L}) = \mathrm{rank}\, M_s(L)$, and $\mathrm{Ker}\, M(\tilde{L}) = (\mathrm{Ker}\, M_s(L))$.*

Theorem 3 *(Cf. [12,15]). Let $L \in (\mathbb{R}[\mathbf{x}])^*$. If $M(L) \succeq 0$ and $\mathrm{rank}\, M(L) = \mathrm{rank}\, M_{s-1}(L)$, then $\mathrm{Ker}\, M(L) = (\mathrm{Ker}\, M_s(L))$ is a zero-dimensional real radical ideal and $|V_{\mathbb{C}}(\mathrm{Ker}\, M(L))| = \mathrm{rank}\, M(L)$.*

3. Basic principles for the prolongation–projection algorithm

We present here the results underlying the prolongation–projection algorithm for computing $V_{\mathbb{K}}(I)$, $\mathbb{K} = \mathbb{R}, \mathbb{C}$. The basic techniques behind this section originally stem from the treatment of partial differential equations, see [23]. Zharkov et al. [29,30] were the first to apply these techniques to polynomial ideals. Section 3.1 contains the main result (Theorem 4). The complex case is inspired from [31] and was treated in [13]. The real case goes along the same lines, so we only give a brief sketch of the proof in Section 3.2. In Section 3.3 we indicate a natural choice for the polynomial system $\mathcal{G}$ involved in Theorem 4, which is based on the ideas of [12] and will be used in the prolongation–projection algorithm.

3.1. New stopping criterion based on prolongation/projection dimension conditions

We state the main result on which the prolongation–projection algorithm is based. We give a unified formulation for both complex/real cases.

Theorem 4. *Let $I = (h_1, \ldots, h_m)$ be an ideal in $\mathbb{R}[\mathbf{x}]$, $D = \max_j \deg(h_j)$ and s, t be integers with $1 \leq s \leq t$. Let $\mathcal{G} \subseteq \mathbb{R}[\mathbf{x}]_t$, satisfying $h_1, \ldots, h_m \in \mathcal{G}$ and $\mathcal{G} \subseteq I$ (resp., $\mathcal{G} \subseteq \sqrt[\mathbb{R}]{I}$). If $\dim \pi_s(\mathcal{G}^\perp) = 0$ then $V_{\mathbb{C}}(I) = \emptyset$ (resp., $V_{\mathbb{R}}(I) = \emptyset$). Assume now that $s \geq D$ and*

$$\dim \pi_s(\mathcal{G}^\perp) = \dim \pi_{s-1}(\mathcal{G}^\perp), \tag{3a}$$

$$\dim \pi_s(\mathcal{G}^\perp) = \dim \pi_s((\mathcal{G}^+)^\perp). \tag{3b}$$

Then there exists a set $\mathcal{B} \subseteq \mathbb{T}^n_{s-1}$ closed under taking divisions (and thus connected to 1) for which the following direct sum decomposition holds:

$$\mathbb{R}[\mathbf{x}]_s = \mathrm{Span}_{\mathbb{R}}(\mathcal{B}) \oplus (\mathbb{R}[\mathbf{x}]_s \cap \mathrm{Span}_{\mathbb{R}}(\mathcal{G})). \tag{4}$$

Let $\mathcal{B} \subseteq \mathbb{T}^n_{s-1}$ be any set connected to 1 for which (4) holds, let φ be the projection from $\mathbb{R}[\mathbf{x}]_s$ onto $\mathrm{Span}_{\mathbb{R}}(\mathcal{B})$ along $\mathbb{R}[\mathbf{x}]_s \cap \mathrm{Span}_{\mathbb{R}}(\mathcal{G})$, and let $F_0 := \{m - \varphi(m) \mid m \in \partial\mathcal{B}\}$, $J := (F_0)$. Then $\mathcal{B}$ is a basis of $\mathbb{R}[\mathbf{x}]/J$ and F_0 is a border basis of J. Moreover:

- *If $\mathcal{G} \subseteq I$ then $J = I$.*
- *If $\mathcal{G} \subseteq \sqrt[\mathbb{R}]{I}$ then*

$$V_{\mathbb{R}}(I) = V_{\mathbb{C}}(J) \cap \mathbb{R}^n; \quad J \cap \mathbb{R}[\mathbf{x}]_s = \mathrm{Span}_{\mathbb{R}}(\mathcal{G}) \cap \mathbb{R}[\mathbf{x}]_s; \quad \pi_s(\mathcal{D}[J]) = \pi_s(\mathcal{G}^\perp),$$

and in addition, $J = \sqrt[\mathbb{R}]{I}$ if $\dim \pi_s(\mathcal{G}^\perp) = |V_{\mathbb{R}}(I)|$.

This result is proved in [13] in the case when $\mathcal{G} = \mathcal{H}_t \subseteq I$, where

$$\mathcal{H}_t := \{\mathbf{x}^\alpha h_j \mid |\alpha| + \deg(h_j) \le t,\ j = 1, \ldots, m\} \tag{5}$$

consists of all prolongations to degree t of the generators h_j of I. Note however that in [13] we did not prove the existence of $\mathcal{B}$ closed under taking divisions; we include a proof in Section 3.2 below.

The proof for arbitrary $\mathcal{G} \subseteq I$ is identical to the case $\mathcal{G} = \mathcal{H}_t$. In the case $\mathcal{G} \subseteq \sqrt[\mathbb{R}]{I}$, the proof[1] is essentially analogous (except for the last claim $J = \sqrt[\mathbb{R}]{I}$ which is specific to the real case). We give a brief sketch of the proof in the next section, since this enables us to point out the impact of the various assumptions and, moreover, some technical details that are needed later in the presentation.

3.2. Sketch of proof for Theorem 4

We begin with a lemma used to show the existence of $\mathcal{B}$ closed by division in Theorem 4.

Lemma 5. *Let Y be a matrix whose columns are indexed by $\mathbb{T}^n_s$. Assume*

$$\forall \lambda \in \mathbb{R}^{|\mathbb{T}^n_{s-1}|} \quad \sum_{a \in \mathbb{T}^n_{s-1}} \lambda_a Y_a = 0 \Longrightarrow \sum_{a \in \mathbb{T}^n_{s-1}} \lambda_a Y_{x_i a} = 0, \tag{6}$$

where Y_a denotes the a-th column of Y. Then there exists $\mathcal{B} \subseteq \mathbb{T}^n_s$ which is closed under taking divisions and indexes a maximum linearly independent set of columns of Y.

Proof. Order the monomials in $\mathbb{T}^n_s$ according to a total degree monomial ordering $\prec$. Let $\mathcal{B} \subseteq \mathbb{T}^n_s$ index a maximum linearly independent set of columns of Y, which is constructed using the greedy algorithm (as described in [12]) applied to the ordering $\prec$ of the columns. Then, setting $\mathcal{B}_m := \{m' \in \mathcal{B} \mid m' \prec m\}$, $m \in \mathcal{B}$ precisely when $\mathcal{B}_m \cup \{m\}$ indexes a linearly independent set of columns of Y. We claim that $\mathcal{B}$ is closed under taking divisions. For this assume $m \in \mathcal{B}$ and $m = x_i m_1$ with $m_1 \notin \mathcal{B}$. As $m_1 \notin \mathcal{B}$, we deduce that

$$Y_{m_1} = \sum_{a \in \mathcal{B}_{m_1}} \lambda_a Y_a \quad \text{for some scalars } \lambda_a.$$

For $a \in \mathcal{B}_{m_1}$, $a \prec m_1$ implies $x_i a \prec x_i m_1 = m$, i.e., $x_i a \in \mathcal{B}_m$. Applying (6) we deduce that

$$Y_m = \sum_{a \in \mathcal{B}_{m_1}} \lambda_a Y_{x_i a},$$

which gives a linear dependency of Y_m with the columns indexed by $\mathcal{B}_m$, contradicting $m \in \mathcal{B}$. □

We now sketch the proof of Theorem 4. Set $N := \dim \pi_{s-1}(\mathcal{G}^\perp)$. If $N = 0$ then $V_{\mathbb{K}}(I) = \emptyset$ (for otherwise the evaluation at $v \in V_{\mathbb{K}}(I)$ would give a nonzero element of $\pi_{s-1}(\mathcal{G}^\perp)$). Let $\{L_1, \ldots, L_N\} \subseteq \mathcal{G}^\perp$ for which $\{\pi_{s-1}(L_1), \ldots, \pi_{s-1}(L_N)\}$ is a basis of $\pi_{s-1}(\mathcal{G}^\perp)$. Let Y be the $N \times |\mathbb{T}^n_{s-1}|$ matrix with (j, m)-th entry $L_j(m)$ for $j \le N$ and $m \in \mathbb{T}^n_{s-1}$. We verify that Y satisfies the condition (6) of Lemma 5 (replacing s by $s-1$). For this note that $\sum_{a \in \mathbb{T}^n_{s-2}} \lambda_a Y_a = 0$ if and only if $p := \sum_{a \in \mathbb{T}^n_{s-2}} \lambda_a a \in (\pi_{s-2}(\mathcal{G}^\perp))^\perp = \mathrm{Span}_{\mathbb{R}}(\mathcal{G}) \cap \mathbb{R}[\mathbf{x}]_{s-2}$ and thus $x_i p \in \mathrm{Span}_{\mathbb{R}}(\mathcal{G}^+) \cap \mathbb{R}[\mathbf{x}]_{s-1}$; in view of (3b), this implies $x_i p \in \mathrm{Span}_{\mathbb{R}}(\mathcal{G}) \cap \mathbb{R}[\mathbf{x}]_{s-1}$ and thus $\sum_{a \in \mathbb{T}^n_{s-2}} \lambda_a Y_{x_i a} = 0$. Thus we can apply Lemma 5: There exists a set $\mathcal{B}$ indexing a maximum linearly independent set of columns of Y which is closed by division. This amounts to having the direct sum decomposition:

$$\mathbb{R}[\mathbf{x}]_{s-1} = \mathrm{Span}_{\mathbb{R}}(\mathcal{B}) \oplus (\mathrm{Span}_{\mathbb{R}}(\mathcal{G}) \cap \mathbb{R}[\mathbf{x}]_{s-1}). \tag{7}$$

As $N = \dim \pi_s(\mathcal{G}^\perp)$, the set $\{\pi_s(L_1), \ldots, \pi_s(L_N)\}$ is a basis of $\pi_s(\mathcal{G}^\perp)$, and thus (4) holds. Set $F := \{m - \varphi(m) \mid m \in \mathbb{T}^n_s\}$. Obviously, $F_0 \subseteq F \subseteq \mathrm{Span}_{\mathbb{R}}(\mathcal{G}) \cap \mathbb{R}[\mathbf{x}]_s$. Moreover, one can verify (cf. [13]) that

$$\mathrm{Span}_{\mathbb{R}}(F) = \mathrm{Span}_{\mathbb{R}}(\mathcal{G}) \cap \mathbb{R}[\mathbf{x}]_s, \tag{8}$$

$$(F_0) = (F), \quad I \subseteq (F) \quad \text{if } s \ge D, \tag{9}$$

$$\varphi(x_i \varphi(x_j m)) = \varphi(x_j \varphi(x_i m)) \quad \text{for } m \in \mathcal{B} \text{ and } i, j \in \{1, \ldots, n\}. \tag{10}$$

Note that (3b) is used to show (9)–(10).

The ideal $J := (F_0)$ satisfies $I \subseteq J$ (by (9)) and $J \subseteq I$ or $J \subseteq \sqrt[\mathbb{R}]{I}$ depending on the assumption on $\mathcal{G}$. As $\mathcal{B}$ is connected to 1 and we have the commutativity property (10), we can apply [18, Theorem 3.1] and deduce that $\mathcal{B}$ is a basis of $\mathbb{R}[\mathbf{x}]/J$. The inclusion: $\mathrm{Span}_{\mathbb{R}}(\mathcal{G}) \cap \mathbb{R}[\mathbf{x}]_s \subseteq J \cap \mathbb{R}[\mathbf{x}]_s$ follows from (8)–(9), while the reverse inclusion follows from the fact that $\varphi(p) = 0$

[1] Note that if we would apply the previous result to the ideal $J := (I \cup \mathcal{G})$ and the set $\mathcal{G}$, then we would reach the desired conclusion, but under the stronger assumption $s \ge \max(D, D')$, where D' is the maximum degree of a generating set for $\mathcal{G}$.

for all $p \in J \cap \mathbb{R}[\mathbf{x}]_s$ since $\mathcal{B}$ is a basis of $\mathbb{R}[\mathbf{x}]/J$. Thus $\mathrm{Span}_{\mathbb{R}}(\mathcal{G}) \cap \mathbb{R}[\mathbf{x}]_s = J \cap \mathbb{R}[\mathbf{x}]_s$, implying $\pi_s(\mathcal{G}^\perp) = (J \cap \mathbb{R}[\mathbf{x}]_s)^\perp$. The inclusion $\pi_s(J^\perp) \subseteq (J \cap \mathbb{R}[\mathbf{x}]_s)^\perp$ is obvious, and the reverse inclusion follows from $(\pi_s(J^\perp))^\perp \subseteq (J^\perp)^\perp \cap \mathbb{R}[\mathbf{x}]_s = J \cap \mathbb{R}[\mathbf{x}]_s$, since J is zero-dimensional. Hence $\pi_s(\mathcal{G}^\perp) = \pi_s(J^\perp) = \pi_s(\mathcal{D}[J])$. Finally note that

$$\dim \pi_s(\mathcal{G}^\perp) = |\mathcal{B}| = \dim \mathbb{R}[\mathbf{x}]/J \geq |V_{\mathbb{C}}(J)| \geq |V_{\mathbb{R}}(I)|.$$

Hence, if $\dim \pi_s(\mathcal{G}^\perp) = |V_{\mathbb{R}}(I)|$, then equality holds throughout, which implies that J is real radical and thus $J = \sqrt[\mathbb{R}]{I}$. This concludes the proof of Theorem 4.

Remark 6. We indicate here what happens if we weaken some assumptions in Theorem 4.
(i) The condition $s \geq D$ is used only in (9) to show $I \subseteq (F)$. Hence if we omit the condition $s \geq D$ in Theorem 4, then we get the same conclusion except that we cannot claim $I \subseteq J$.
(ii) Consider now the case where we assume only that (3a) holds (and not (3b)). As we use (3b) to show the existence of $\mathcal{B}$ connected to 1 and to prove (9)–(10), we cannot prove the commutativity property (10), nor the equality $(F) = (F_0)$. Nevertheless, what we can do is test whether $\mathcal{B}$ is connected to 1 and whether (10) holds. If this is the case, then we can conclude that $\mathcal{B}$ is a basis of $\mathbb{R}[\mathbf{x}]/J$ where, depending on the choice of $\mathcal{G}$, the ideal $J = (F_0) \subseteq I$ or $J = (F_0) \subseteq \sqrt[\mathbb{R}]{I}$.

Furthermore, we can compute the variety $V_{\mathbb{C}}(J)$ which satisfies $V_{\mathbb{K}}(I) \subseteq V_{\mathbb{C}}(J)$ and $|V_{\mathbb{C}}(J)| \leq \dim \mathbb{R}[\mathbf{x}]/J = |\mathcal{B}|$. Then it suffices to sort out $V_{\mathbb{K}}(I)$ from $V_{\mathbb{C}}(J)$. The additional information that condition (3b) gives us is the guarantee that the commutativity property (10) holds and that we have equality $J = (F)$, thus implying $J \supseteq I$ and $V_{\mathbb{C}}(I) = V_{\mathbb{C}}(J)$ (respectively $V_{\mathbb{R}}(I) = V_{\mathbb{C}}(J) \cap \mathbb{R}^n$) if $s \geq D$.

3.3. A concrete choice for the polynomial system $\mathcal{G}$ in Theorem 4

For the task of computing $V_{\mathbb{C}}(I)$, one can choose as indicated in [13] the set $\mathcal{G} = \mathcal{H}_t$ from (5) and thus consider the linear subspace $\mathcal{K}_t := \mathcal{H}_t^\perp$ of $(\mathbb{R}[\mathbf{x}]_t)^*$. For the task of computing $V_{\mathbb{R}}(I)$, as inspired by [12], we augment $\mathcal{H}_t$ with a set $\mathcal{W}_t$ of polynomials in $\sqrt[\mathbb{R}]{I}$ obtained from the kernel of a suitable positive element in $\mathcal{H}_t^\perp$. For this, consider the convex cone

$$\mathcal{K}_{t,\succeq} := \{L \in \mathcal{H}_t^\perp \mid M_{\lfloor t/2 \rfloor}(L) \succeq 0\},$$

consisting of the elements of $\mathcal{K}_t$ that are positive, i.e. satisfy $L(p^2) \geq 0$ whenever $\deg(p^2) \leq t$. Generic elements of $\mathcal{K}_{t,\succeq}$ (defined in Lemma 7 below) play a central role; geometrically these are the elements lying in the relative interior of the cone $\mathcal{K}_{t,\succeq}$.

Lemma 7. *The following assertions are equivalent for $L^* \in \mathcal{K}_{t,\succeq}$.*

(i) $\mathrm{rank}\, M_{\lfloor t/2 \rfloor}(L^*) = \max_{L \in \mathcal{K}_{t,\succeq}} \mathrm{rank}\, M_{\lfloor t/2 \rfloor}(L)$.
(ii) $\mathrm{rank}\, M_s(L^*) = \max_{L \in \mathcal{K}_{t,\succeq}} \mathrm{rank}\, M_s(L)$ *for all* $1 \leq s \leq \lfloor t/2 \rfloor$.
(iii) $\mathrm{Ker}\, M_s(L^*) \subseteq \mathrm{Ker}\, M_s(L)$ *for all* $L \in \mathcal{K}_{t,\succeq}$ *and* $1 \leq s \leq \lfloor t/2 \rfloor$.

Then L^* is said to be generic.

Proof. Direct verification using (1)–(2). □

Hence any two generic elements $L_1, L_2 \in \mathcal{K}_{t,\succeq}$ have the same kernel, denoted by $\mathcal{N}_t$ $(= \mathrm{Ker}\, M_{\lfloor t/2 \rfloor}(L_1) = \mathrm{Ker}\, M_{\lfloor t/2 \rfloor}(L_2))$, which satisfies

$$\mathcal{N}_t \subseteq \mathcal{N}_{t'} \quad \text{if } t \leq t' \tag{11}$$

(easy verification), as well as

$$\mathcal{N}_t \subseteq \sqrt[\mathbb{R}]{I}. \tag{12}$$

(cf. [12, Lemma 3.1]). Define the set

$$\mathcal{W}_t := \{\mathbf{x}^\alpha g \mid \alpha \in \mathbb{N}^n_{\lfloor t/2 \rfloor}, g \in \mathcal{N}_t\}, \tag{13}$$

whose definition is motivated by the fact that, for $L \in (\mathbb{R}[\mathbf{x}]_t)^*$,

$$\mathcal{N}_t \subseteq \mathrm{Ker}\, M_{\lfloor t/2 \rfloor}(L) \Longleftrightarrow L \in \mathcal{W}_t^\perp. \tag{14}$$

Therefore, $\mathcal{W}_t \subseteq \sqrt[\mathbb{R}]{I}$. For the task of computing $V_{\mathbb{R}}(I)$, our choice for the set $\mathcal{G}$ in Theorem 4 is

$$\mathcal{G}_t := \mathcal{H}_t \cup \mathcal{W}_t. \tag{15}$$

Note also that

$$\mathcal{K}_{t,\succeq} \subseteq \mathcal{H}_t^\perp \cap \mathcal{W}_t^\perp = (\mathcal{H}_t \cup \mathcal{W}_t)^\perp. \tag{16}$$

In fact, as we now show, both sets in (16) have the same dimension, i.e. $(\mathcal{H}_t \cup \mathcal{W}_t)^\perp$ is the smallest linear space containing the cone $\mathcal{K}_{t,\succeq}$.

Lemma 8. $\dim \mathcal{K}_{t,\geq} = \dim(\mathcal{H}_t \cup \mathcal{W}_t)^\perp$.

Proof. Pick L^* lying in the relative interior of $\mathcal{K}_{t,\geq}$, i.e. L^* is generic, and define

$$\mathcal{P}_t := \{L \in (\mathbb{R}[\mathbf{x}]_t)^* \mid L^* \pm \epsilon L \in \mathcal{K}_{t,\geq} \text{ for some } \epsilon > 0\},$$

the linear space consisting of all possible *perturbations* at L^*. Then, $\dim \mathcal{K}_{t,\geq} = \dim \mathcal{P}_t$. One can verify that there exists an $\epsilon > 0$ such that $L^* \pm \epsilon L \in \mathcal{K}_{t,\geq}$ if and only if $L \in \mathcal{H}_t^\perp$ and $\operatorname{Ker} M_{\lfloor t/2 \rfloor}(L^*) \subseteq \operatorname{Ker} M_{\lfloor t/2 \rfloor}(L)$ (cf. e.g. [8, Thm. 31.5.3]). As the latter condition is equivalent to $L \in \mathcal{W}_t^\perp$ by (14), we find $\mathcal{P}_t = (\mathcal{H}_t \cup \mathcal{W}_t)^\perp$, which concludes the proof. □

We conclude with a characterization of $\sqrt[\mathbb{R}]{I}$ and of its dual space $\mathcal{D}[\sqrt[\mathbb{R}]{I}]$, using the sets $\mathcal{G}_t$ from (15).

Proposition 9. *With* $\mathcal{G}_t = \mathcal{H}_t \cup \mathcal{W}_t$, $\sqrt[\mathbb{R}]{I} = \bigcup_t \operatorname{Span}_{\mathbb{R}}(\mathcal{G}_t)$ *and* $\mathcal{D}[\sqrt[\mathbb{R}]{I}] = \bigcap_t \mathcal{G}_t^\perp$.

Proof. The inclusion $\bigcup_t \operatorname{Span}_{\mathbb{R}}(\mathcal{G}_t) \subseteq \sqrt[\mathbb{R}]{I}$ follows from (12). Next, for some order (t, s) we have $\sqrt[\mathbb{R}]{I} = (\operatorname{Ker} M_s(L^*))$. The proof, which relies on the existence of a finite basis for the ideal $\sqrt[\mathbb{R}]{I}$ can be found in [12]. This fact, combined with $\operatorname{Ker} M_s(L^*) \subseteq \mathcal{N}_t \subseteq \operatorname{Span}_{\mathbb{R}}(\mathcal{G}_t)$, implies the reverse inclusion $\sqrt[\mathbb{R}]{I} \subseteq \bigcup_t \operatorname{Span}_{\mathbb{R}}(\mathcal{G}_t)$. Now the equality $\sqrt[\mathbb{R}]{I} = \bigcup_t \operatorname{Span}_{\mathbb{R}} \mathcal{G}_t$ implies in turn $\mathcal{D}[\sqrt[\mathbb{R}]{I}] = \bigcap_t \mathcal{G}_t^\perp$. □

When $|V_{\mathbb{R}}(I)| < \infty$, the dual of the real radical ideal coincides in fact with the vector space spanned by the evaluations at all $v \in V_{\mathbb{R}}(I)$. Proposition 9 shows how to obtain it directly from the quadratic forms Q_L (or its matrix representation $M_{\lfloor t/2 \rfloor}(L)$) for a generic $L \in \mathcal{K}_{t,\geq}$ without a priori knowledge of $V_{\mathbb{R}}(I)$.

4. Links with the moment-matrix method

In this section we explore the links with the moment-matrix method of [12] for finding $V_{\mathbb{R}}(I)$ as well as the real radical ideal $\sqrt[\mathbb{R}]{I}$. We recall the main result of [12], underlying this method.

Theorem 10 (*[12]*). *Let L^* be a generic element of $\mathcal{K}_{t,\geq}$. Assume that*

$$\operatorname{rank} M_s(L^*) = \operatorname{rank} M_{s-1}(L^*) \tag{17}$$

for some $D \leq s \leq \lfloor t/2 \rfloor$. Then $(\operatorname{Ker} M_s(L^*)) = \sqrt[\mathbb{R}]{I}$ and any set $\mathcal{B} \subseteq \mathbb{T}^n_{s-1}$ indexing a maximum linearly independent set of columns of $M_{s-1}(L^*)$ is a basis of $\mathbb{R}[\mathbf{x}]/\sqrt[\mathbb{R}]{I}$.

4.1. Relating the rank condition and the prolongation–projection dimension conditions

We now present some links between the rank condition (17) and the conditions (3a)–(3b). First we show that the condition (3a) suffices to ensure that the rank condition (17) holds at some later order.

Proposition 11. *Let $1 \leq s \leq t$. If (3a) holds with $\mathcal{G} := \mathcal{H}_t \cup \mathcal{W}_t$, then $\operatorname{rank} M_s(L) = \operatorname{rank} M_{s-1}(L)$ for all $L \in \mathcal{K}_{t+2s,\geq}$.*

Proof. Let $L \in \mathcal{K}_{t+2s,\geq}$. We show that $\operatorname{rank} M_s(L) = \operatorname{rank} M_{s-1}(L)$. For this, pick $m, m' \in \mathbb{T}^n_s$. As in the proof of Theorem 4, (4) holds and thus we can write $m = \sum_{b\in\mathcal{B}} \lambda_b b + f$, where $\lambda_b \in \mathbb{R}, f \in \operatorname{Span}_{\mathbb{R}}(\mathcal{G})$, and $\mathcal{B} \subseteq \mathbb{T}^n_{s-1}$. (Note that (3b) was not used to derive this.) Then, $mm' = \sum_{b\in\mathcal{B}} \lambda_b m'b + m'f$. It suffices now to show that $L(m'f) = 0$. Indeed this will imply $M(L)_{m',m} = L(mm') = \sum_{b\in\mathcal{B}} \lambda_b L(m'b) = \sum_{b\in\mathcal{B}} \lambda_b M(L)_{m',b}$, that is, the mth column of $M(L)$ is a linear combination of its columns indexed by $b \in \mathcal{B}$, thus giving the desired result.

We now show that $L(m'g) = 0$ for all $g \in \mathcal{H}_t \cup \mathcal{W}_t$. By assumption, $L \in \mathcal{K}_{t+2s,\geq} \subseteq \mathcal{H}^\perp_{t+2s} \cap \mathcal{W}^\perp_{t+2s}$ (recall (16)). If $g \in \mathcal{H}_t$, then $m'g \in \mathcal{H}_{t+s} \subseteq \mathcal{H}_{t+2s}$ and thus $L(m'g) = 0$. If $g \in \mathcal{W}_t$, then $g = \mathbf{x}^\alpha h$, where $h \in \mathcal{N}_t$ and $|\alpha| \leq \lfloor t/2 \rfloor$. Hence, $m'g = m'\mathbf{x}^\alpha h$, where $\deg(m'\mathbf{x}^\alpha) \leq s + \lfloor t/2 \rfloor \leq \lfloor (2s+t)/2 \rfloor$ and $h \in \mathcal{N}_t \subseteq \mathcal{N}_{t+2s}$ (by (11)), implying $m'g \in \mathcal{W}_{t+2s}$ and thus $L(m'g) = 0$. □

We now show that the rank condition (17) is in fact equivalent to the following stronger version of the conditions (3a)–(3b) with $\mathcal{G} = \mathcal{G}_t = \mathcal{H}_t \cup \mathcal{W}_t$:

$$\dim \pi_{2s}(\mathcal{G}_t^\perp) = \dim \pi_{s-1}(\mathcal{G}_t^\perp), \tag{18a}$$

$$\dim \pi_{2s}(\mathcal{G}_t^\perp) = \dim \pi_{2s}((\mathcal{G}_t^+)^\perp). \tag{18b}$$

Proposition 12. *Let L^* be a generic element of $\mathcal{K}_{t,\geq}$ and $1 \leq s \leq \lfloor t/2 \rfloor$.*

(i) *Assume (17) holds. Then (18a) holds, and (18b) holds as well if $s \geq D$.*
(ii) *Assume (18a)–(18b) hold. Then, (17) holds, the ideal J obtained in Theorem 4 is a real radical ideal and satisfies $J = (\operatorname{Ker} M_s(L^*)) \subseteq I(V_{\mathbb{R}}(I))$ and, given $\mathcal{B} \subseteq \mathbb{T}^n_{s-1}$, $\mathcal{B}$ satisfies (7) if and only if $\mathcal{B}$ indexes a column basis of $M_{s-1}(L^*)$. Furthermore, $J = \sqrt[\mathbb{R}]{I}$ if $s \geq D$.*

The proof being a bit technical is postponed to Section 4.2. An immediate consequence of Proposition 12 is that the rank condition at order (t, s) implies the prolongation–projection dimension conditions (3a)–(3b) at the same order (t, s).

Corollary 13. *Assume $D \le s \le \lfloor t/2 \rfloor$ and let $\mathcal{G} = \mathcal{G}_t = \mathcal{H}_t \cup \mathcal{W}_t$. Then,*

$$(17) \Longleftrightarrow (18a)\text{–}(18b) \Longrightarrow (3a)\text{–}(3b).$$

Proof. Indeed, $\pi_s(\mathcal{G}_t^\perp) = \pi_s((\mathcal{G}_t^+)^\perp)$ follows directly from $\pi_{2s}(\mathcal{G}_t^\perp) = \pi_{2s}((\mathcal{G}_t^+)^\perp)$. □

It is shown in [12] that the rank condition (17) holds at order (s, t) large enough with $D \le s \le \lfloor t/2 \rfloor$. Hence the same holds for the conditions (18a)–(18b) (and thus for (3a)–(3b)), which will imply the termination of the prolongation–projection algorithm based on Theorem 4.

4.2. Proof of Proposition 12

First we note that the rank condition (17) is in fact a property of the whole cone $\mathcal{K}_{t,\ge}$ and its superset $\mathcal{G}_t^\perp = \mathcal{H}_t^\perp \cap \mathcal{W}_t^\perp$.

Lemma 14. *If (17) holds for some generic $L^* \in \mathcal{K}_{t,\ge}$, then (17) holds for* all *$L \in \mathcal{G}_t^\perp$.*

Proof. Let $L \in \mathcal{G}_t^\perp$. We have

$$\operatorname{Ker} M_s(L^*) = \operatorname{Ker} M_{\lfloor t/2 \rfloor}(L^*) \cap \mathbb{R}[\mathbf{x}]_s = \mathcal{N}_t \cap \mathbb{R}[\mathbf{x}]_s \subseteq \operatorname{Ker} M_{\lfloor t/2 \rfloor}(L) \cap \mathbb{R}[\mathbf{x}]_s \subseteq \operatorname{Ker} M_s(L), \tag{19}$$

where the first equality holds by (1), the first inclusion holds by (14), and the second one holds since $M_s(L)$ is a principal submatrix of $M_{\lfloor t/2 \rfloor}(L)$. This implies directly that $\operatorname{rank} M_s(L) = \operatorname{rank} M_{s-1}(L)$. □

We now give the proof for Proposition 12. Let L^* be a generic element of $\mathcal{K}_{t,\ge}$.

(i) Assume that (17) holds. First we show (18a), i.e. we show that $\dim \pi_{2s}(\mathcal{G}_t^\perp) = \dim \pi_{s-1}(\mathcal{G}_t^\perp)$. For this, consider the linear mapping

$$\begin{array}{rccc} \psi: & \pi_{2s}(\mathcal{G}_t^\perp) & \to & \pi_{s-1}(\mathcal{G}_t^\perp) \\ & \pi_{2s}(L) & \mapsto & \pi_{s-1}(L). \end{array}$$

As ψ is onto, it suffices to show that ψ is one-to-one. For this assume $\pi_{s-1}(L) = 0$ for some $L \in \mathcal{G}_t^\perp$. We show that $\pi_{2s}(L) = 0$, i.e. $L(\mathbf{x}^\gamma) = 0$ for all $|\gamma| \le 2s$ by induction on $|\gamma| \le 2s$. The case $|\gamma| \le s-1$ holds by assumption. Let $s \le |\gamma| \le 2s$ and write γ as $\gamma = \alpha + \beta$ where $|\alpha| = s$ and $|\beta| \le s$. By Lemma 14, $\operatorname{rank} M_s(L) = \operatorname{rank} M_{s-1}(L)$. Hence the αth column of $M_s(L)$ can be written as a linear combination of the columns indexed by $\mathbb{T}^n_{s-1}$. This gives

$M_s(L)_{\beta,\alpha} = \sum_{|\delta| \le s-1} \lambda_\delta M_s(L)_{\beta,\delta}$ for some $\lambda_\delta \in \mathbb{R}$. As $|\beta + \delta| \le |\gamma| - 1$, we have $M_s(L)_{\beta,\delta} = L(\mathbf{x}^{\beta+\delta}) = 0$ by the induction assumption, implying $L(\mathbf{x}^\gamma) = M_s(L)_{\beta,\alpha} = 0$.

We now assume moreover $s \ge D$. We show the inclusion $\pi_{2s}(\mathcal{G}_t^\perp) \subseteq \pi_{2s}((\mathcal{G}_t^+)^\perp)$, which implies (18b). Let $L \in \mathcal{G}_t^\perp$. As $\operatorname{rank} M_s(L) = \operatorname{rank} M_{s-1}(L)$, we can apply Theorem 2 and deduce the existence of $\tilde{L} \in (\mathbb{R}[\mathbf{x}])^*$ for which $\pi_{2s}(\tilde{L}) = \pi_{2s}(L)$ and $\operatorname{Ker} M(\tilde{L}) = (\operatorname{Ker} M_s(L))$. It suffices now to show that $\tilde{L} \in (\mathcal{G}_t^+)^\perp$. We show a stronger result, namely that $\tilde{L} \in I(V_\mathbb{R}(I))^\perp$. As $s \ge D$, we know from Theorem 10 that $I(V_\mathbb{R}(I)) = (\operatorname{Ker} M_s(L^*))$. Pick $p \in I(V_\mathbb{R}(I))$ and write it as $p = \sum_l u_l g_l$, where $u_l \in \mathbb{R}[\mathbf{x}]$ and $g_l \in \operatorname{Ker} M_s(L^*)$; we show that $\tilde{L}(p) = 0$. By (19), $g_l \in \operatorname{Ker} M_s(L)$ and thus, as $M_s(L) = M_s(\tilde{L})$, $g_l \in \operatorname{Ker} M_s(\tilde{L})$. Therefore, p lies in $(\operatorname{Ker} M_s(\tilde{L})) = \operatorname{Ker} M(\tilde{L})$, which gives $\tilde{L}(p) = 0$.

(ii) Assume now that (18a)–(18b) hold. Then, (3a)–(3b) holds for the pair $(t, 2s)$ (and $\mathcal{G} = \mathcal{G}_t$). Although we do not assume $2s \ge D$, the conclusion of Theorem 4 partially holds, as observed in Remark 6(i). Namely, we can find an ideal J satisfying $J \subseteq I(V_\mathbb{R}(I))$, $J \cap \mathbb{R}[\mathbf{x}]_{2s} = \operatorname{Span}_\mathbb{R}(\mathcal{G}_t) \cap \mathbb{R}[\mathbf{x}]_{2s}$, $\pi_{2s}(D[J]) = \pi_{2s}(\mathcal{G}_t^\perp)$, and $I \subseteq J$ if $2s \ge D$. Moreover, there exists a set $\mathcal{B} \subseteq \mathbb{T}^n_{s-1}$ which is a basis of $\mathbb{R}[\mathbf{x}]/J$ and satisfies the following analogue of (4):

$$\mathbb{R}[\mathbf{x}]_{2s} = \operatorname{Span}_\mathbb{R}(\mathcal{B}) \oplus (\operatorname{Span}_\mathbb{R}(\mathcal{G}_t) \cap \mathbb{R}[\mathbf{x}]_{2s}). \tag{20}$$

We show that $\operatorname{rank} M_s(L^*) = \operatorname{rank} M_{s-1}(L^*)$. As $L^* \in \mathcal{G}_t^\perp$, there exists $\tilde{L} \in D[J]$ for which $\pi_{2s}(L^*) = \pi_{2s}(\tilde{L})$. Thus $M_s(L^*) = M_s(\tilde{L})$, and $J \subseteq \operatorname{Ker} M(\tilde{L})$ since $\tilde{L} \in D[J]$. It suffices to show that $\operatorname{rank} M_s(\tilde{L}) = \operatorname{rank} M_{s-1}(\tilde{L})$. For this, as in the proof of Proposition 11, pick $m, m' \in \mathbb{T}^n_s$. Using (20), we can write $m = \sum_{b \in \mathcal{B}} \lambda_b b + f$, where $\lambda_b \in \mathbb{R}$, $f \in \operatorname{Span}_\mathbb{R}(\mathcal{G}_t) \cap \mathbb{R}[\mathbf{x}]_{2s} \subseteq J \subseteq \operatorname{Ker} M(\tilde{L})$, so that $\tilde{L}(m'm) = \sum_{b \in \mathcal{B}} \lambda_b \tilde{L}(m'b)$, which gives the desired result: $\operatorname{rank} M_s(\tilde{L}) = \operatorname{rank} M_{s-1}(\tilde{L})$.

Let $\mathcal{B}_1, \mathcal{B}_2 \subseteq \mathbb{T}^n_{s-1}$, where $\mathcal{B}_1$ satisfies (7) and $\mathcal{B}_2$ indexes a column basis of $M_{s-1}(L^*)$. Then

$$|\mathcal{B}_1| = \dim \mathbb{R}[\mathbf{x}]/J \le \operatorname{rank} M_{s-1}(L^*) \ (= |\mathcal{B}_2|) \tag{21}$$

since the columns of $M_{s-1}(L^*)$ indexed by $\mathcal{B}_1$ are linearly independent (direct verification, using (7) and the fact that $\operatorname{Ker} M_{s-1}(L^*) \subseteq \operatorname{Ker} M_{\lfloor t/2 \rfloor}(L^*) = \mathcal{N}_t \subseteq \operatorname{Span}_\mathbb{R}(\mathcal{G}_t)$). Moreover,

$$|\mathcal{B}_2| = \operatorname{rank} M_{s-1}(L^*) \le \dim \pi_{s-1}(\mathcal{G}_t^\perp) \ (= |\mathcal{B}_1|). \tag{22}$$

Indeed, as $\mathrm{Span}_{\mathbb{R}}(\mathcal{G}_t) \cap \mathbb{R}[\mathbf{x}]_{s-1} \subseteq J \cap \mathbb{R}[\mathbf{x}]_{s-1} \subseteq \mathrm{Ker}\, M_{s-1}(\tilde{L}) = \mathrm{Ker}\, M_{s-1}(L^*)$, we obtain $\mathrm{Span}_{\mathbb{R}}(\mathcal{G}_t) \cap \mathrm{Span}_{\mathbb{R}}(\mathcal{B}_2) = \{0\}$, which implies $|\mathcal{B}_2| \le \dim(\mathrm{Span}_{\mathbb{R}}(\mathcal{G}_t) \cap \mathbb{R}[\mathbf{x}]_{s-1})^{\perp} = \dim \pi_{s-1}(\mathcal{G}_t^{\perp})$. Hence, equality holds in (21) and (22). Therefore, $\mathcal{B}_1$ indexes a column basis of $M_{s-1}(L^*)$, $\mathcal{B}_2$ satisfies (7), and

$$\mathrm{rank}\, M_{s-1}(L^*) = \dim \pi_{s-1}(\mathcal{G}_t^{\perp}) = \dim \mathbb{R}[\mathbf{x}]/J.$$

As $J \subseteq \mathrm{Ker}\, M(\tilde{L})$, we deduce

$$\dim \mathbb{R}[\mathbf{x}]/\mathrm{Ker}\, M(\tilde{L}) \le \dim \mathbb{R}[\mathbf{x}]/J.$$

On the other hand,

$$\dim \mathbb{R}[\mathbf{x}]/J = \mathrm{rank}\, M_{s-1}(L^*) = \mathrm{rank}\, M_{s-1}(\tilde{L}) \le \mathrm{rank}\, M(\tilde{L}) = \dim \mathbb{R}[\mathbf{x}]/\mathrm{Ker}\, M(\tilde{L}).$$

Hence equality holds throughout. In particular, $J = \mathrm{Ker}\, M(\tilde{L})$ and $\mathrm{rank}\, M(\tilde{L}) = \mathrm{rank}\, M_{s-1}(\tilde{L})$. As $M_{s-1}(\tilde{L}) = M_{s-1}(L^*) \succeq 0$, we deduce that $M(\tilde{L}) \succeq 0$ and $J = \mathrm{Ker}\, M(\tilde{L}) = (\mathrm{Ker}\, M_s(\tilde{L})) = (\mathrm{Ker}\, M_s(L^*))$ is a real radical ideal (using Theorem 3). Finally, if $s \ge D$, then $J = (\mathrm{Ker}\, M_s(L^*)) = \sqrt[\mathbb{R}]{I}$ by Theorem 10. This concludes the proof of Proposition 12.

4.3. Two illustrative examples

We discuss two simple examples to illustrate the various notions just introduced and the role of moment matrices; the second one has infinitely many complex roots.

Example 15. Let $I = (x_1^2, x_2^2, x_1x_2) \subseteq \mathbb{R}[x_1, x_2]$, considered in [13] as an example with a non-Gorenstein algebra $\mathbb{R}[\mathbf{x}]/I$. Any $L \in \mathcal{K}_t$ $(t \ge 2)$ satisfies $L(\mathbf{x}^{\alpha}) = 0$ if $|\alpha| \ge 2$ and thus

$$M_{\lfloor t/2 \rfloor}(L) = \begin{pmatrix} a & b & c & 0 & \dots \\ b & 0 & 0 & 0 & \dots \\ c & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \quad \text{for some scalars } a, b, c,$$

where entries are indexed by $1, x_1, x_2, \dots$ Hence, $\dim \pi_2(\mathcal{K}_2) = \dim \pi_1(\mathcal{K}_2) = \dim \pi_2(\mathcal{K}_3) = 3$ and the rank stabilizes at order $(t, s) = (4, 2)$, i.e. $\mathrm{rank}\, M_2(L^*) = \mathrm{rank}\, M_1(L^*) = 2$ for generic $L^* \in \mathcal{K}_4$. When $L \in \mathcal{K}_{t,\succeq}$, the condition $M_{\lfloor t/2 \rfloor}(L) \succeq 0$ implies $b = c = 0$. Hence, for generic $L^* \in \mathcal{K}_{2,\succeq}$, $\mathcal{N}_2 := \mathrm{Ker}\, M_1(L^*)$ is spanned by the polynomials x_1 and x_2, and the rank condition (17) holds at order $(t, s) = (2, 1)$, i.e. $\mathrm{rank}\, M_1(L^*) = \mathrm{rank}\, M_0(L^*) = 1$. As $\mathrm{Span}_{\mathbb{R}}(\mathcal{G}_2)$ is spanned by the polynomials $x_1, x_2, x_1^2, x_1x_2, x_2^2$, the conditions (18a)–(18b) hold at the same order $(t, s) = (2, 1)$, i.e. $\dim \pi_2(\mathcal{G}_2^{\perp}) = \dim \pi_0(\mathcal{G}_2^{\perp}) = \dim \pi_2((\mathcal{G}_2^{\perp})^{\perp}) = 1$, as predicted by Proposition 12.

Example 16. Consider the ideal $I = (x_1^2 + x_2^2) \subseteq \mathbb{R}[x_1, x_2]$ with $V_{\mathbb{R}}(I) = \{0\}$ and $|V_{\mathbb{C}}(I)| = \infty$. As $\dim \pi_s(\mathcal{K}_t) = \dim \pi_{s-1}(\mathcal{K}_t) + 2$ for any $t \ge s \ge 2$, the conditions (3a)–(3b) never hold in the case $\mathcal{G} = \mathcal{H}_t$. On the other hand, any $L \in \mathcal{K}_{2,\succeq}$ satisfies $L(x_1^2) = L(x_2^2) = 0$, which follows from $L(x_1^2 + x_2^2) = 0$ combined with $M_1(L) \succeq 0$, giving $L(x_1^2), L(x_2^2) \ge 0$. Moreover, $L(x_1) = L(x_2) = L(x_1x_2) = 0$. Thus $\mathcal{N}_2$ is spanned by the polynomials x_1 and x_2, and the conditions (17) and (18a)–(18b) hold at order $(t, s) = (2, 1)$.

Examples 18 and 20 in Section 6 are cases where the prolongation–projection method terminates earlier than the moment-matrix method.

5. A prolongation–projection algorithm

Let us now give a brief description of our algorithm for computing $V_{\mathbb{K}}(I)$ $(\mathbb{K} = \mathbb{R}, \mathbb{C})$ based on the results of the previous section. A simple adjustment in the proposed prolongation–projection algorithm allows the computation of all complex vs. real roots. The general structure is shown in Algorithm 1. If I is an ideal given by a set of generators and $|V_{\mathbb{K}}(I)| < \infty$, this algorithm computes the multiplication matrices in $\mathbb{R}[\mathbf{x}]/J$, which thus allows the immediate computation of $V_{\mathbb{C}}(J)$ (by Theorem 1), where J is a zero-dimensional ideal satisfying $J = I$ if $\mathbb{K} = \mathbb{C}$ and $I \subseteq J \subseteq \sqrt[\mathbb{R}]{I}$ if $\mathbb{K} = \mathbb{R}$, so that $V_{\mathbb{K}}(J) = V_{\mathbb{K}}(I)$. We then comment on the key steps involved in the algorithm.

Algorithm 1 *Unified prolongation–projection algorithm for computing $V_{\mathbb{K}}(I)$:*

Require: A set $\{h_1, \ldots, h_m\}$ of generators of I and $t \geq D$.

Ensure: The multiplication matrices in $\mathbb{R}[\mathbf{x}]/J$, where $J = I$ if $\mathbb{K} = \mathbb{C}$ and $I \subseteq J \subseteq \sqrt[\mathbb{R}]{I}$ if $\mathbb{K} = \mathbb{R}$, thus enabling the computation of $V_{\mathbb{K}}(I)$.

1: Compute the matrix representation G_t of $\mathcal{G}_t$ and G_t^+ of $\mathcal{G}_t^+$.
2: Compute $\operatorname{Ker} G_t$ and $\operatorname{Ker} G_t^+$.
3: Compute $\dim \pi_s(\operatorname{Ker} G_t)$ $(= \dim \pi_s((\mathcal{G}_t)^\perp))$ and $\dim \pi_s(\operatorname{Ker} G_t^+)$ $(= \dim \pi_s((\mathcal{G}_t^+)^\perp))$ for $s \leq t$.
4: Check if (3a)–(3b) holds for some $D \leq s \leq \lfloor t/2 \rfloor$.
5: **if** yes **then**
6: **return** a basis $\mathcal{B} \subseteq \mathbb{R}[\mathbf{x}]_{s-1}$ connected to 1 and satisfying (7), and the multiplication matrices X_i in $\mathbb{R}[\mathbf{x}]/J$ represented in the basis $\mathcal{B}$.
7: **else**
8: Iterate (go to 1) replacing t by $t+1$.
9: **end if**

Remark 17. Here, $\mathcal{G}_t = \mathcal{H}_t$ (see (5)) for the task of computing $V_{\mathbb{C}}(I)$, and $\mathcal{G}_t = \mathcal{H}_t \cup \mathcal{W}_t$ (see (13)) for the task of computing $V_{\mathbb{R}}(I)$. See below for details about the matrix representations G_t and G_t^+.

Characterizing $\mathcal{G}_t$ and $\mathcal{G}_t^\perp$ via the matrix G_t

In the real case, the set $\mathcal{G}_t$ is defined as $\mathcal{G}_t = \mathcal{H}_t \cup \mathcal{W}_t$ where $\mathcal{W}_t$ is the linear space defined in (13). As we are interested in the orthogonal space $\mathcal{G}_t^\perp$, it suffices to compute a basis $\mathcal{C}_t$ of the linear space $\mathcal{N}_t$ and to define the set

$$\mathcal{S}_t := \{\mathbf{x}^\alpha g \mid |\alpha| \leq \lfloor t/2 \rfloor, g \in \mathcal{C}_t\}. \tag{23}$$

Then, $\mathcal{N}_t = \operatorname{Span}_{\mathbb{R}}(\mathcal{C}_t)$, $\mathcal{W}_t = \operatorname{Span}_{\mathbb{R}}(\mathcal{S}_t)$, and $\mathcal{G}_t^\perp = (\mathcal{H}_t \cup \mathcal{S}_t)^\perp$. Let S_t (resp., H_t) be the matrix with columns indexed by $\mathbb{T}_t^n$ and whose rows are the coefficient vectors of the polynomials in $\mathcal{S}_t$ (resp., in $\mathcal{H}_t$). In the case $\mathbb{K} = \mathbb{C}$, the set $\mathcal{G}_t = \mathcal{H}_t$ is represented by the matrix $G_t := H_t$ and, in the case $\mathbb{K} = \mathbb{R}$, the set $\mathcal{G}_t = \mathcal{H}_t \cup \mathcal{W}_t$ is represented by the matrix

$$G_t := \begin{bmatrix} H_t \\ S_t \end{bmatrix}.$$

Then the vectors in $\operatorname{Ker} G_t$ are precisely the coordinate vectors in the canonical basis of $(\mathbb{R}[\mathbf{x}]_t)^*$ of the linear forms in $\mathcal{G}_t^\perp$, i.e.

$$L \in \mathcal{G}_t^\perp \Longleftrightarrow (L(\mathbf{x}^\alpha))_{|\alpha| \leq t} \in \operatorname{Ker} G_t. \tag{24}$$

Analogously, G_t^+ is the matrix representation of $(\mathcal{H}_t \cup \mathcal{S}_t)^+$, so that $(\mathcal{G}_t^+)^\perp$ corresponds to $\operatorname{Ker} G_t^+$.

To compute the space $\mathcal{N}_t$ we need a generic element $L^* \in \mathcal{K}_{t,\geq}$. How to find such a generic element has been discussed in detail in [12, Section 4.4.1]. Let us only mention here that this task can be performed numerically using a standard semidefinite programming solver implementing a self-dual embedding strategy, see e.g. [7, Chapter 4]. For our computations we use the SDP solver SeDuMi [26].

Computing $\pi_s(\mathcal{G}_t^\perp)$ and its dimension

As shown in (24), the dual space $\mathcal{G}_t^\perp$ can be characterized in the canonical dual basis as the kernel of the matrix G_t, see e.g. [31] for details using an algorithm based on singular value decomposition. Faster implementations can be obtained e.g. using Gauss elimination. Once we have a basis of $\operatorname{Ker} G_t$, denoted say by $\{z_1, \ldots, z_M\}$, then, for any $s \leq t$, we construct the matrix Z_s whose rows are the vectors $\pi_s(z_1), \ldots, \pi_s(z_M)$, the projections onto $\mathbb{R}_s^n$ of $z_1, \ldots, z_M$. Then $\dim \pi_s(\mathcal{G}_t^\perp) = \dim \pi_s(\operatorname{Ker} G_t)$ is equal to the rank of the matrix Z_s.

Extracting solutions

In order to extract the variety $V_{\mathbb{K}}(I)$, we apply Theorem 1 which thus requires a basis $\mathcal{B}$ of the quotient space and the corresponding multiplication matrices. In the setting of Theorem 4, $\operatorname{rank} Z_s = \operatorname{rank} Z_{s-1} =: N$ and $\mathcal{B}$ is chosen such that $\mathcal{B} \subseteq \mathbb{T}_{s-1}^n$ indexes N linearly independent columns of Z_{s-1}. The first possibility to construct $\mathcal{B}$ is to use a greedy algorithm as explained in the proof of Lemma 5. Another possibility is to use Gauss–Jordan elimination with partial pivoting on Z_s (see [10]) such that each column corresponding to a monomial of degree s is expressed as a linear combination of N monomials of degree at most $s-1$. The pivot variables form a set $\mathcal{B} \subseteq \mathbb{T}_{s-1}^n$ indexing a maximum set of linearly independent columns of Z_s and their corresponding monomials serve as a (monomial) basis $\mathcal{B}$ of the quotient space (provided $\mathcal{B}$ is connected to 1). The reduced row echelon form of Z_s, interpreted as coefficient vector for some polynomials, gives the desired rewriting family, which thus enables the construction of multiplication matrices and provides a border (or Gröbner) basis (cf. [12] for details).

A second alternative proposed in [31] is to use singular value decomposition once more to obtain a basis of $\operatorname{Ker} Z_s$ and therefore a polynomial basis $\mathcal{B}$ for the quotient ring (see [31] for details). All examples presented in the next section are computed using singular value decomposition.

Table 1
Dimension table for $\pi_s(\mathscr{H}_t^\perp)$ in Example 18.

	s									
	0	1	2	3	4	5	6	7	8	9
$\dim \pi_s(\mathscr{K}_3)$	1	4	8	11	–	–	–	–	–	–
$\dim \pi_s(\mathscr{K}_4)$	1	4	8	10	12	–	–	–	–	–
$\dim \pi_s(\mathscr{K}_5)$	1	4	8	9	10	12	–	–	–	–
$\dim \pi_s(\mathscr{K}_6)$	1	4	**8**	**8**	9	10	12	–	–	–
$\dim \pi_s(\mathscr{K}_7)$	1	4	8	**8**	8	9	10	12	–	–
$\dim \pi_s(\mathscr{K}_8)$	1	4	8	8	8	8	9	10	12	–
$\dim \pi_s(\mathscr{K}_9)$	1	4	8	8	8	8	8	9	10	12

6. Numerical examples

We now illustrate the prolongation–projection algorithm on some simple examples. The algorithm has been implemented in Matlab using the Yalmip toolbox [16]. For the real-root prolongation–projection algorithm, we show the dimensions of $\pi_s(\mathscr{G}_t^\perp)$ and $\pi_s((\mathscr{G}_t^+)^\perp)$, the projections of the orthogonal complement of the set $\mathscr{G}_t = \mathscr{H}_t \cup \mathscr{W}_t$ and of its one degree prolongation. For comparison, we also sometimes show the dimension table for the complex-root version of this algorithm, and we show the values $\operatorname{rank} M_s(L^*)$ $(s \le \lfloor t/2 \rfloor)$ for a generic element $L^* \in \mathscr{K}_{t,\ge}$ used in the real moment-matrix method. To illustrate the potential savings, and at the same time facilitate a comparison between the various methods, we sometimes give more data than needed for the real root computation (then displayed in gray color). We also provide the extracted roots $v \in V_{\mathbb{K}}(I)$ and, as a measure of accuracy, the maximum evaluation $\epsilon(v) = \max_j |h_j(v)|$ taken over all input polynomials h_j at the extracted root v, as well as the commutativity error $c(\mathscr{X}) := \max_{i,j=1}^n \operatorname{abs}(\mathscr{X}_i\mathscr{X}_j - \mathscr{X}_j\mathscr{X}_i)$ of the computed multiplication matrices $\mathscr{X}_i$.

Example 18. Consider the ideal $I = (h_1, h_2, h_3) \subseteq \mathbb{R}[x_1, x_2, x_3]$, where

$$h_1 = x_1^2 - 2x_1x_3 + 5,$$
$$h_2 = x_1x_2^2 + x_2x_3 + 1,$$
$$h_3 = 3x_2^2 - 8x_1x_3,$$

with $D = 3$, $|V_{\mathbb{C}}(I)| = 8$ and $|V_{\mathbb{R}}(I)| = 2$, taken from [3, Ex. 4, p.57]. We illustrate and compare the various algorithms in this example.

Table 1 shows the dimensions of the sets $\pi_s(\mathscr{H}_t^\perp)$ for various prolongation–projection orders (t, s). Note that the conditions (3a)–(3b) hold at order $(t, s) = (6, 3)$, i.e.

$$\pi_3(\mathscr{H}_6^\perp) = \pi_2(\mathscr{H}_6^\perp) = \pi_3(\mathscr{H}_7^\perp).$$

With the complex-root prolongation–projection algorithm we can compute the following eight complex roots:

$$v_1 = \begin{bmatrix} -1.10 & -2.88 & -2.82 \end{bmatrix},$$
$$v_2 = \begin{bmatrix} 0.0767 + 2.243\mathrm{i} & 0.461 + 0.497\mathrm{i} & 0.0764 + 0.00834\mathrm{i} \end{bmatrix},$$
$$v_3 = \begin{bmatrix} 0.0767 - 2.243\mathrm{i} & 0.461 - 0.497\mathrm{i} & 0.0764 - 0.00834\mathrm{i} \end{bmatrix},$$
$$v_4 = \begin{bmatrix} -0.0815 - 0.931\mathrm{i} & 2.35 + 0.0431\mathrm{i} & -0.274 + 2.209\mathrm{i} \end{bmatrix},$$
$$v_5 = \begin{bmatrix} -0.0815 + 0.931\mathrm{i} & 2.35 - 0.0431\mathrm{i} & -0.274 - 2.20\mathrm{i} \end{bmatrix},$$
$$v_6 = \begin{bmatrix} 0.0725 + 2.24\mathrm{i} & -0.466 - 0.464\mathrm{i} & 0.0724 + 0.00210\mathrm{i} \end{bmatrix},$$
$$v_7 = \begin{bmatrix} 0.0725 - 2.24\mathrm{i} & -0.466 + 0.464\mathrm{i} & 0.0724 - 0.00210\mathrm{i} \end{bmatrix},$$
$$v_8 = \begin{bmatrix} 0.966 & -2.81 & 3.07 \end{bmatrix},$$

with a maximum error of $\max_i \epsilon(v_i) < 8\text{e-}13$ and commutativity error $c(\mathscr{X}) < 6\text{e-}13$.

Table 2 shows the dimensions of the sets $\pi_s(\mathscr{G}_t^\perp)$ and $\pi_s((\mathscr{G}_t^+)^\perp)$ with $\mathscr{G}_t = \mathscr{H}_t \cup \mathscr{W}_t$ for various prolongation–projection orders (t, s). Note that the conditions (3a)–(3b) hold at order $(t, s) = (5, 2)$, i.e.

$$\dim \pi_2(\mathscr{G}_5^\perp) = \dim \pi_1(\mathscr{G}_5^\perp) = \dim \pi_2((\mathscr{G}_5^+)^\perp).$$

With the real-root prolongation–projection algorithm we can extract the two real solutions:

$$v_1 = \begin{bmatrix} -1.101 & -2.878 & -2.821 \end{bmatrix},$$
$$v_2 = \begin{bmatrix} 0.966 & -2.813 & 3.072 \end{bmatrix},$$

with $\max_i \epsilon(v_i) < 2\text{e-}8$ and commutativity error $c(\mathscr{X}) < 3.3\text{e-}9$. Note that, since $2 = s < D = 3$, we cannot directly apply Theorem 4 to claim $V_{\mathbb{R}}(I) = V_{\mathbb{C}}(J) \cap \mathbb{R}^n$. Instead, as indicated in Remark 6(i), we can only claim $V_{\mathbb{C}}(J) \cap \mathbb{R}^n \supseteq V_{\mathbb{R}}(I)$. However,

Table 2
Dimension table for $\pi_s(\mathcal{G}_t^\perp)$ and $\pi_s((\mathcal{G}_t^+)^\perp)$ with $\mathcal{G}_t = \mathcal{H}_t \cup \mathcal{W}_t$ in Example 18.

	s							
	0	1	2	3	4	5	6	7
$\dim \pi_s(\mathcal{G}_3^\perp)$	1	4	8	11	–	–	–	–
$\dim \pi_s((\mathcal{G}_3^+)^\perp)$	1	4	8	10	12	–	–	–
$\dim \pi_s(\mathcal{G}_4^\perp)$	1	4	8	10	12	–	–	–
$\dim \pi_s((\mathcal{G}_4^+)^\perp)$	1	4	8	9	10	12	–	–
$\dim \pi_s(\mathcal{G}_5^\perp)$	1	**2**	**2**	2	3	5	–	–
$\dim \pi_s((\mathcal{G}_5^+)^\perp)$	1	2	**2**	2	3	4	6	–
$\dim \pi_s(\mathcal{G}_6^\perp)$	1	2	2	2	2	2	3	–
$\dim \pi_s((\mathcal{G}_6^+)^\perp)$	1	2	2	2	2	2	2	3

Table 3
Showing $\operatorname{rank} M_s(L^*)$ for generic $L^* \in \mathcal{K}_{t,\geq}$ in Example 18.

t	s			
	0	1	2	3
3	1	4	–	–
4	1	4	8	–
5	1	2	8	–
6	1	**2**	**2**	10

equality can be verified by evaluating the input polynomials h_j at the points $v \in V_{\mathbb{C}}(J) \cap \mathbb{R}^n$. Anyway, one can also observe that the conditions (3a)–(3b) hold at order $(t, s) = (5, 3)$, in which case one can directly conclude $V_{\mathbb{R}}(I) = V_{\mathbb{C}}(J) \cap \mathbb{R}^n$. Finally, we can even conclude $J = \sqrt[\mathbb{R}]{I}$ since $\dim \pi_s(\mathcal{G}_t^\perp) = |V_{\mathbb{R}}(I)|$ (using the last claim in Theorem 4).

The ranks of the moment matrices involved in the computation are shown in Table 3. Observe that the rank condition (17) holds at order $(t, s) = (6, 2)$, i.e.

$$\operatorname{rank} M_2(L^*) = \operatorname{rank} M_1(L^*) \quad \text{for generic } L^* \in \mathcal{K}_{6,\geq}.$$

(To be precise, as $2 = s < D = 3$, we use [12, Prop. 4.1] and check whether the extracted roots belong to $V_{\mathbb{R}}(I)$ afterwards.)

In this small example, we see that we can improve efficiency over the general complex-root algorithm if we are only interested in computing the real roots. Indeed the prolongation–projection algorithm terminates at order $(t, s) = (5, 2)$ in the real case while it terminates at order (6, 3) in the complex case, however at the price of solving an SDP in the real case. Moreover, compared to the real-root moment-matrix algorithm of [12], we save the computation of the last moment matrix $M_3(L^*)$ for $L^* \in \mathcal{K}_{6,\geq}$.

Modifying the above example by replacing each polynomial h_i by $h_i \cdot (1 + \sum_i x_1^2)$ yields an example with a positive dimensional complex variety, while the real variety is unchanged. The proposed algorithm still converges, this time at order $(t, s) = (7, 2)$ and allows the extraction of the two real roots.

Example 19. Consider the ideal $I = (h_1, h_2, h_3) \subseteq \mathbb{R}[x_1, x_2]$, where

$$h_1 = x_2^4 x_1 + 3x_1^3 - x_2^4 - 3x_1^2,$$
$$h_2 = x_1^2 x_2 - 2x_1^2,$$
$$h_3 = 2x_2^4 x_1 - x_1^3 - 2x_2^4 + x_1^2,$$

and $D = 5$, taken from [3, p.40]. The corresponding variety consists of two (real) points, one of which has multiplicity 8.

Table 4 shows the dimensions of the projections of the sets $\mathcal{G}_t^\perp$ and $(\mathcal{G}_t^+)^\perp$ with $\mathcal{G}_t = \mathcal{H}_t \cup \mathcal{W}_t$. The conditions (3a)–(3b) hold at order $(t, s) = (6, s)$ with $2 \leq s \leq 5$, i.e.

$$\dim \pi_s(\mathcal{G}_6^\perp) = \dim \pi_{s-1}(\mathcal{G}_6^\perp) = \dim \pi_s((\mathcal{G}_6^+)^\perp) \quad \text{for } 2 \leq s \leq 5,$$

the conditions (18a)–(18b) hold at order $(t, s) = (6, 2)$, i.e.

$$\dim \pi_1(\mathcal{G}_6^\perp) = \dim \pi_4(\mathcal{G}_6^\perp) = \dim \pi_4((\mathcal{G}_6^+)^\perp),$$

and the extracted roots are

Table 4
Dimension table for $\pi_s(\mathcal{G}_t^\perp)$ and $\pi_s((\mathcal{G}_t^+)^\perp)$ with $\mathcal{G}_t = \mathcal{H}_t \cup \mathcal{W}_t$ in Example 19.

	s							
	0	1	2	3	4	5	6	7
$\dim \pi_s(\mathcal{G}_5^\perp)$	1	3	5	6	8	10	–	–
$\dim \pi_s((\mathcal{G}_5^+)^\perp)$	1	3	5	6	6	8	10	–
$\dim \pi_s(\mathcal{G}_6^\perp)$	1	**2**	**2**	**2**	**2**	**2**	4	–
$\dim \pi_s((\mathcal{G}_6^+)^\perp)$	1	2	**2**	**2**	**2**	**2**	2	4

Table 5
Showing $\operatorname{rank} M_s(L^*)$ for generic $L^* \in \mathcal{K}_{t,\geq}$ in Example 19.

t	s			
	0	1	2	3
5	1	3	5	–
6	1	**2**	**2**	4

Table 6
Dimension table for $\pi_s(\mathcal{H}_t^\perp)$ in Example 19.

	s										
	0	1	2	3	4	5	6	7	8	9	10
$\dim \pi_s(\mathcal{K}_5)$	1	3	6	8	11	13	–	–	–	–	–
$\dim \pi_s(\mathcal{K}_6)$	1	3	6	8	9	11	13	–	–	–	–
$\dim \pi_s(\mathcal{K}_7)$	1	3	6	8	**9**	**9**	11	13	–	–	–
$\dim \pi_s(\mathcal{K}_8)$	1	3	6	8	9	**9**	9	11	13	–	–
$\dim \pi_s(\mathcal{K}_9)$	1	3	6	8	9	9	9	9	11	13	–
$\dim \pi_s(\mathcal{K}_{10})$	1	3	6	8	9	9	9	9	9	11	13

$$v_1 = \begin{bmatrix} -6.17\text{e-}6 & 1.10\text{e-}5 \end{bmatrix}$$
$$v_2 = \begin{bmatrix} 0.9988 & 1.9998 \end{bmatrix}$$

with an accuracy of $\epsilon(v_1) < 2\text{e-}10$ and $\epsilon(v_2) < 4\text{e-}3$ and maximum commutativity error $c(\mathcal{X}) < 3\text{e-}5$.
The ranks of the moment matrices involved in the computations are shown in Table 5. As predicted by Proposition 12, condition (17) holds at order $(t, s) = (6, 2)$, i.e.

$$\operatorname{rank} M_2(L^*) = \operatorname{rank} M_1(L^*) \quad \text{for generic } L^* \in \mathcal{K}_{6,\geq}.$$

Moreover, the returned ideal J satisfies $J = (\operatorname{Ker} M_1(L^*)) = \sqrt[\mathbb{R}]{I}$. Table 6 shows the dimensions of the projections $\pi_s(\mathcal{H}_t^\perp)$ for the complex-root prolongation–projection algorithm. The conditions (3a)–(3b) are satisfied at order $(t, s) = (7, 5)$, allowing (in principle) to extract the two roots with their corresponding multiplicities. The appearance of multiple roots requires a careful choice of the extraction procedure using multiplication operators. We employ the approach described in [6] using reordered Schur factorization. At order $(t, s) = (7, 5)$, numerical problems prevent a successful extraction despite this algorithm. However, at order $(t, s) = (8, 5)$, the multiplication matrices (on which the reordered Schur factorization method is applied) have a commutativity error of $c(\mathcal{X}) < 6.25\text{e-}16$. Thus, we can extract the root

$$v = \begin{bmatrix} 1 & 2 \end{bmatrix}$$

with accuracy $\epsilon(v) < 1.38\text{e-}14$ and the 8-fold root at the origin with an even higher accuracy of $\epsilon(v_i) < 1.75\text{e-}32$.

Note that the real version of this algorithm, working directly with the real radical of the ideal, does not require these considerations as it eliminates multiplicities.

Example 20. This example is taken from [28] and represents a Gaussian quadrature formula with two weights and two knots, namely, $I = (h_1, \ldots, h_4)$, where

$$h_1 = x_1 + x_2 - 2,$$
$$h_2 = x_1x_3 + x_2x_4,$$
$$h_3 = x_1x_3^2 + x_2x_4^2 - \frac{2}{3},$$
$$h_4 = x_1x_3^3 + x_2x_4^3,$$

Table 7
Dimension table for $\pi_s(\mathcal{G}_t^\perp)$ and $\pi_s((\mathcal{G}_t^+)^\perp)$ with $\mathcal{G}_t = \mathcal{H}_t \cup \mathcal{W}_t$ in Example 20.

	s							
	0	1	2	3	4	5	6	7
$\dim \pi_s(\mathcal{G}_4^\perp)$	1	3	7	11	20	–	–	–
$\dim \pi_s((\mathcal{G}_4^+)^\perp)$	1	3	4	8	12	23	–	–
$\dim \pi_s(\mathcal{G}_5^\perp)$	1	**2**	**2**	2	5	16	–	–
$\dim \pi_s((\mathcal{G}_5^+)^\perp)$	1	2	**2**	2	5	9	22	–
$\dim \pi_s(\mathcal{G}_6^\perp)$	1	2	2	2	2	16	18	–
$\dim \pi_s((\mathcal{G}_6^+)^\perp)$	1	2	2	2	2	2	2	2

with $D = 4$ and $|V_{\mathbb{R}}(I)| = |V_{\mathbb{C}}(I)| = 2$. Table 7 shows the dimensions for the projections of the sets $\mathcal{G}_t^\perp$ and $(\mathcal{G}_t^+)^\perp$ with $\mathcal{G}_t = \mathcal{H}_t \cup \mathcal{W}_t$ and Table 8 shows the ranks of the moment matrices $M_s(L^*)$ for generic $L^* \in \mathcal{K}_{t,\geq}$. The conditions (3a)–(3b) hold at order $(t, s) = (5, 2)$ and the extracted roots are

$$v_1 = \begin{bmatrix} 1 & 1 & -0.5774 & 0.5774 \end{bmatrix}$$
$$v_2 = \begin{bmatrix} 1 & 1 & 0.5774 & -0.5774 \end{bmatrix}.$$

with an accuracy of $\epsilon(v_1) < 2\text{e-}11$ and $\epsilon(v_2) < 2\text{e-}11$ and maximum commutativity error $c(\mathcal{X}) < 4\text{e-}14$. Here again the algorithm returns the ideal $J = \sqrt[\mathbb{R}]{I}$, since $\dim \pi_2(\mathcal{G}_5^\perp) = |V_{\mathbb{R}}(I)| = 2$. On the other hand, the moment-matrix algorithm of [12] terminates at order $(t, s) = (6, 2)$, thus later than the prolongation–projection algorithm.

Example 21. The following 6-dimensional system is taken from http://www.mat.univie.ac.at/~neum/glopt/coconut/Benchmark/Library3/katsura5.mod and is known under the name Katsura 5:

$$\begin{aligned}
h_1 &= 2x_6^2 + 2x_5^2 + 2x_4^2 + 2x_3^2 + 2x_2^2 + x_1^2 - x_1,\\
h_2 &= x_6x_5 + x_5x_4 + 2x_4x_3 + 2x_3x_2 + 2x_2x_1 - x_2,\\
h_3 &= 2x_6x_4 + 2x_5x_3 + 2x_4x_2 + x_2^2 + 2x_3x_1 - x_3,\\
h_4 &= 2x_6x_3 + 2x_5x_2 + 2x_3x_2 + 2x_4x_1 - x_4,\\
h_5 &= x_3^2 + 2x_6x_1 + 2x_5x_1 + 2x_4x_1 - x_5,\\
h_6 &= 2x_6 + 2x_5 + 2x_4 + 2x_3 + 2x_2 + x_1 - 1,
\end{aligned}$$

with $D = 2$, $|V_{\mathbb{C}}(I)| = 32$, and $|V_{\mathbb{R}}(I)| = 12$. The projection dimensions are shown in Table 9.
The solution points

$$\begin{aligned}
v_1 &= \begin{bmatrix} 1 & 8.73\text{e}{-7} & 2.14\text{e}{-6} & 2.48\text{e}{-7} & 2.23\text{e}{-6} & -1.29\text{e}{-6} \end{bmatrix},\\
v_2 &= \begin{bmatrix} 0.277 & 0.226 & 0.162 & 0.0858 & 0.0115 & -0.124 \end{bmatrix},\\
v_3 &= \begin{bmatrix} 0.136 & 0.0428 & 0.0417 & 0.0404 & 0.0964 & 0.211 \end{bmatrix},\\
v_4 &= \begin{bmatrix} 0.462 & 0.309 & 0.0553 & -0.102 & -0.0844 & 0.0917 \end{bmatrix},\\
v_5 &= \begin{bmatrix} 0.441 & 0.151 & 0.0225 & 0.219 & 0.0935 & -0.207 \end{bmatrix},\\
v_6 &= \begin{bmatrix} 0.239 & 0.0608 & -0.0622 & -0.0233 & 0.186 & 0.219 \end{bmatrix},\\
v_7 &= \begin{bmatrix} 0.753 & 0.0532 & 0.191 & -0.114 & -0.146 & 0.139 \end{bmatrix},\\
v_8 &= \begin{bmatrix} 0.726 & -0.0503 & 0.122 & 0.164 & 0.109 & -0.208 \end{bmatrix},\\
v_9 &= \begin{bmatrix} 0.409 & -0.0732 & 0.0657 & -0.127 & 0.252 & 0.178 \end{bmatrix},\\
v_{10} &= \begin{bmatrix} 0.292 & -0.101 & 0.181 & -0.0591 & 0.193 & 0.141 \end{bmatrix},\\
v_{11} &= \begin{bmatrix} 0.590 & 0.0422 & 0.327 & -0.0642 & -0.0874 & -0.0132 \end{bmatrix},\\
v_{12} &= \begin{bmatrix} 0.68 & 0.266 & -0.154 & 0.0323 & 0.0897 & -0.0735 \end{bmatrix},
\end{aligned}$$

were extracted at order $(t, s) = (6, 3)$, when conditions (3a)–(3b) were first satisfied. The maximum evaluation error was found to be $\max_i \epsilon(v_i) < 2.4\text{e-}4$ and the commutativity error $c(\mathcal{X}) < 6.2\text{e-}6$. Again the algorithm returns the ideal $J = \sqrt[\mathbb{R}]{I}$ as $\dim \pi_3(\mathcal{G}_6^\perp) = |V_{\mathbb{R}}(I)| = 12$. In this example the moment-matrix method [12] also extracts the 12 real solutions at order $(t, s) = (6, 3)$.

Table 8
Showing $\operatorname{rank} M_s(L^*)$ for generic $L^* \in \mathcal{K}_{t,\geq}$ in Example 20.

t	s			
	0	1	2	3
4	1	4	9	–
5	1	2	5	–
6	1	**2**	**2**	9

Table 9
Dimension table for $\pi_s(\mathcal{G}_t^\perp)$ and $\pi_s((\mathcal{G}_t^+)^\perp)$ with $\mathcal{G}_t = \mathcal{H}_t \cup \mathcal{W}_t$ in Example 21.

	s							
	0	1	2	3	4	5	6	7
$\dim \pi_s(\mathcal{G}_2^\perp)$	1	6	16	–	–	–	–	–
$\dim \pi_s((\mathcal{G}_2^+)^\perp)$	1	6	16	26	–	–	–	–
$\dim \pi_s(\mathcal{G}_3^\perp)$	1	6	16	26	–	–	–	–
$\dim \pi_s((\mathcal{G}_3^+)^\perp)$	1	6	16	26	31	–	–	–
$\dim \pi_s(\mathcal{G}_4^\perp)$	1	6	16	26	31	–	–	–
$\dim \pi_s((\mathcal{G}_4^+)^\perp)$	1	6	16	26	31	32	–	–
$\dim \pi_s(\mathcal{G}_5^\perp)$	1	6	16	26	31	32	–	–
$\dim \pi_s((\mathcal{G}_5^+)^\perp)$	1	6	16	26	31	32	32	–
$\dim \pi_s(\mathcal{G}_6^\perp)$	1	6	**12**	**12**	12	12	12	–
$\dim \pi_s((\mathcal{G}_6^+)^\perp)$	1	6	12	**12**	12	12	12	12

7. Conclusion

This work was motivated by the great success of numerical–algebraic methods in recent years. Incorporating features specific to *real root finding* into efficient symbolic–numeric methods may lead to more efficient algorithms for numerically computing all real roots of a given system of polynomials. The contribution of this paper is a first attempt in this direction as it implements real-algebraic features into the existing symbolic–numeric algorithm described in [31]. Concretely, the resulting algorithm uses semidefinite programming techniques in addition to standard numerical linear algebra techniques. It is not only applicable to zero-dimensional ideals, but to all problems for which the real variety is finite. An extension to zero-dimensional basic semi-algebraic subsets is also possible, along the same lines as in [12].

The new approach relies on a dual space characterization of (an approximation of) the real radical ideal, obtained by combining ideas of [12,31], but the new prolongation–projection algorithm may terminate earlier than the moment-matrix method of [12]. Although preliminary computational results are encouraging, whether the characterization at hand can lead to a new treatment of real-algebraic problems is still to be demonstrated on a larger sample of problems. An important computational issue is how to efficiently solve the underlying semidefinite program for large problems involving high degree polynomials with many variables. Exploiting sparsity in order to decrease the size of the semidefinite program is a promising direction and the work of Kojima et al. [11] and Lasserre [14] is a first important step in this direction. Strategies similar to those used in Gröbner/border basis computations can be employed to further increase efficiency of the proposed method, particularly in view of the linear algebra steps involved, e.g. the dimension tests.

Acknowledgements

We thank two referees for their careful reading and useful suggestions which helped improve the presentation of the paper.

References

[1] S. Basu, R. Pollack, M.-F. Roy, Algorithms in Real Algebraic Geometry, Springer, 2003.
[2] J. Bochnak, M. Coste, M.-F. Roy, Real Algebraic Geometry, Springer, 1998.
[3] D. Cox, J. Little, D. O'Shea, Using Algebraic Geometry, Springer, 1998.
[4] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra, Springer, 2005.
[5] R. Curto, L. Fialkow, Solution of the truncated complex moment problem for flat data, Mem. Amer. Math. Soc. 119 (568) (1996) 1–62.

[6] R.M. Corless, P.M. Gianni, B.M. Trager, A reordered Schur factorization method for zero-dimensional polynomial systems with multiple roots, in: Proc. ACM Intern. Symp. on Symbolic and Algebraic Computation, ACM Press, 1997, pp. 133–140.
[7] E. de Klerk, Aspects of Semidefinite Programming — Interior Point Algorithms and Selected Applications, Kluwer, 2002.
[8] M. Deza, M. Laurent, Geometry of Cuts and Metrics, Springer, 1997.
[9] A. Dickenstein, I.Z. Emiris (Eds.), Solving Polynomial Equations: Foundations, Algorithms, and Applications, in: Algorithms and Computation in Mathematics, vol. 14, Springer, 2005.
[10] D. Henrion, J. Lasserre, Detecting Global Optimality and Extracting Solutions in GloptiPoly, in: Positive Polynomials in Control, in: Lectures Notes in Control and Information Sciences., Springer, 2005, pp. 293–310.
[11] M. Kojima, S. Kim, H. Waki, Sparsity in sums of squares of polynomials, Math. Program. 103 (1) (2005) 45–62.
[12] J. Lasserre, M. Laurent, P. Rostalski, Semidefinite characterization and computation of real radical ideals, Found. Comput. Math. 8 (5) (2008) 607–647.
[13] J. Lasserre, M. Laurent, P. Rostalski, A unified approach for real and complex zeros of zero-dimensional ideals, in: Emerging Applications of Algebraic Geometry, in: M. Putinar, S. Sullivant (Eds.), IMA Volumes in Mathematics and its Applications, vol. 149, Springer, 2009, pp. 125–155.
[14] J.B. Lasserre, Convergent SDP-relaxations in polynomial optimization with sparsity, SIAM J. Optim. 17 (3) (2006) 822–843.
[15] M. Laurent, Revisiting two theorems of Curto and Fialkow, Proc. Amer. Math. Soc. 133 (10) (2005) 2965–2976.
[16] J. Löfberg, Yalmip : A toolbox for modeling and optimization in MATLAB, in: Proceedings of the CACSD Conference, Taipei, Taiwan, 2004.
[17] H. Möller, An inverse problem for cubature formulae, Computat. Technol. 9 (2004) 13–20.
[18] B. Mourrain, A new criterion for normal form algorithms, in: AAECC, in: LNCS, vol. 1719, 1999, pp. 430–443.
[19] B. Mourrain, F. Rouillier, M.-F. Roy, Bernstein's basis and real root isolation, in: Combinatorial and Computational Geometry, in: Mathematical Sciences Research Institute Publications, Cambridge University Press, 2005, pp. 459–478.
[20] B. Mourrain, P. Trebuchet, Generalized normal forms and polynomial system solving, in: M. Kauers (Ed.), Proc. Intern. Symp. on Symbolic and Algebraic Computation, ACM Press, New-York, 2005, pp. 253–260.
[21] V.Y. Pan, B. Murphy, R.E. Rosholt, G. Qian, Y. Tang, Real root-finding, in: SNC'07: Proceedings of the 2007 International Workshop on Symbolic–Numeric Computation, ACM Press, New York, NY, USA, 2007, pp. 161–169.
[22] F. Rouillier, Solving zero-dimensional systems through the rational univariate representation, J. Appl. Algebra Eng. Commun. Comput. 9 (5) (1999) 433–461.
[23] W. Seiler, Involution — The formal theory of differential equations and its applications in computer algebra and numerical analysis, Habilitation thesis, Department of Mathematics and Computer Science of Universität Mannheim, 2001.
[24] A. Sommese, C. Wampler, The Numerical Solution of Systems of Polynomials Arising in Engineering and Science, World Scientific Press, Singapore, 2005.
[25] H. Stetter, Numerical Polynomial Algebra, Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2004.
[26] J. Sturm, Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones, in: Interior Point Methods (CD supplement with software), Optimization Methods and Software 11–12 (1999) 625–653 (special issue).
[27] J. Verschelde, PHCPACK: A general-purpose solver for polynomial systems by homotopy continuation.
[28] J. Verschelde, K. Gatermann, Symmetric Newton polytopes for solving sparse polynomial systems, Adv. Appl. Math. 16 (1) (1995) 95–127.
[29] A. Zharkov, Y. Blinkov, Involutive bases of zero-dimensional ideals. Preprint E5-94-318, Joint Institute for Nuclear Research, Dubna, 1994.
[30] A. Zharkov, Y. Blinkov, Involutive approach to investigating polynomial systems, in: International IMACS Symposium on Symbolic Computation: New Trends and Developments, in: Math. Comp. Simul., vol. 42, 1996, pp. 323–332.
[31] L. Zhi, G. Reid, Solving nonlinear polynomial systems via symbolic–numeric elimination method, in: J. Faugère and F. Rouillier (Eds.), Proceedings of the International Conference on Polynomial System Solving, 2004, pp. 50–53.