

## Semidefinite Characterization and Computation of Zero-Dimensional Real Radical Ideals

Jean Bernard Lasserre · Monique Laurent ·  
Philipp Rostalski

Received: 19 September 2006 / Revised: 11 April 2007 / Accepted: 4 May 2007 /  
Published online: 23 October 2007  
© SFoCM 2007

**Abstract** For an ideal  $I \subseteq \mathbb{R}[x]$  given by a set of generators, a new semidefinite characterization of its real radical  $I(V_{\mathbb{R}}(I))$  is presented, provided it is zero-dimensional (even if  $I$  is not). Moreover, we propose an algorithm using numerical linear algebra and semidefinite optimization techniques, to compute all (finitely many) points of the real variety  $V_{\mathbb{R}}(I)$  as well as a set of generators of the real radical ideal. The latter is obtained in the form of a border or Gröbner basis. The algorithm is based on moment relaxations and, in contrast to other existing methods, it exploits the real algebraic nature of the problem right from the beginning and avoids the computation of complex components.

**Keywords** Algebraic geometry · Zero-dimensional ideal · (Real) radical ideal · Semidefinite programming

---

Communicated by Marie-Francoise Roy.

J.-B. Lasserre (✉)  
LAAS-CNRS, Toulouse, France  
e-mail: lasserre@laas.fr

J.-B. Lasserre  
Institute of Mathematics, Toulouse, France

M. Laurent  
Centrum voor Wiskunde en Informatica, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands  
e-mail: M.Laurent@cwi.nl

P. Rostalski  
Automatic Control Laboratory, ETH Zurich, Physikstrasse 3, 8092 Zurich, Switzerland  
e-mail: rostalski@control.ee.ethz.ch

**Mathematics Subject Classification (2000)** 14P05 · 13P10 · 12E12 · 12D10 · 90C22

## 1 Introduction

Algebraic computation over the reals is a highly relevant topic with many practical applications and, in particular, for finding real solutions to a system of polynomial equations. Throughout the paper,  $\mathbb{K}[x] = \mathbb{K}[x_1, \dots, x_n]$  denotes the ring of polynomials in  $n$  variables over the field  $\mathbb{K} = \mathbb{R}$  or  $\mathbb{C}$ . For an ideal  $I \subseteq \mathbb{K}[x]$ ,  $V_{\mathbb{C}}(I) := \{v \in \mathbb{C}^n \mid f(v) = 0 \forall f \in I\}$  and  $V_{\mathbb{R}}(I) := V_{\mathbb{C}}(I) \cap \mathbb{R}^n$  denote, respectively, the complex and real varieties of  $I$  and, for  $V \subseteq \mathbb{C}^n$ ,  $I(V) := \{f \in \mathbb{K}[x] \mid f(v) = 0 \forall v \in V\}$  is the vanishing ideal of the set  $V$ . The ideal  $I(V_{\mathbb{C}}(I))$  coincides with the radical ideal  $\sqrt{I}$  of  $I$  by the Nullstellensatz and  $I(V_{\mathbb{R}}(I))$  coincides with the real radical ideal  $\sqrt[\mathbb{R}]{I}$  by the Real Nullstellensatz (see Sect. 2.1 for details). The problem of finding the radical ideal  $I(V_{\mathbb{C}}(I))$  seems to be much better understood than that of finding the real radical ideal  $I(V_{\mathbb{R}}(I))$ ; see below for a brief recap on existing literature. In this paper we provide a new characterization of the real radical ideal  $I(V_{\mathbb{R}}(I))$  of an ideal  $I \subseteq \mathbb{R}[x]$ , assuming  $I$  is given by generators  $h_1, \dots, h_m \in \mathbb{R}[x]$  and  $V_{\mathbb{R}}(I)$  is finite (while  $V_{\mathbb{C}}(I)$  need not be finite). In addition, from this characterization, we also define a numerical algorithm based on semidefinite programming to compute the points of the (finite) variety  $V_{\mathbb{R}}(I)$  as well as a set of generators of the real radical ideal  $I(V_{\mathbb{R}}(I))$ . More generally, our results extend to the case of the so-called  $S$ -radical ideal  $I(V_{\mathbb{R}}(I) \cap S)$  where  $S \subseteq \mathbb{R}^n$  is defined by finitely many polynomial inequalities, assuming that  $V_{\mathbb{R}}(I) \cap S$  is finite. It turns out that a similar algorithm also works for computing  $V_{\mathbb{C}}(I)$  and the radical ideal  $I(V_{\mathbb{C}}(I))$  (assuming now  $V_{\mathbb{C}}(I)$  finite) although very good methods already exist for this latter case. In the remainder of the Introduction, after recalling some motivation and related literature on the problem of finding the (real) radical ideal, we sketch the main ingredients of our method. We already introduce some definitions but refer to Sects. 2 and 3 for additional definitions about polynomials and moment matrices.

*Motivation.* The main motivation of this work is to provide a characterization as well as an algorithm for finding the real variety and the real radical of an ideal  $I \subseteq \mathbb{R}[x]$  that takes into account the specific *real* algebraic geometric nature of the problem. Indeed, to the best of our knowledge, most basic methods for computing the real variety  $V_{\mathbb{R}}(I)$  first compute the complex variety  $V_{\mathbb{C}}(I)$ ; for this they require as basic ingredients a Gröbner basis of  $I$  and a linear basis of the vector space  $\mathbb{R}[x]/I$  and thus they work under the assumption that  $V_{\mathbb{C}}(I)$  is finite. Even if  $V_{\mathbb{C}}(I)$  is finite, but has many more complex elements than real ones, this may produce a large computational overhead. This is particularly important as the numbers of complex and real solutions may differ significantly as supported by the fewnomial theory of Khovanski [22]; see also the discussion in Bihan et al. [4, 5]. In other words, this problem of real algebraic geometry is solved via algebraic methods that do not take into account right from the beginning the real algebraic aspect of the problem. In contrast, our characterization and our algorithm do not need knowledge of a Gröbner basis of  $I$  and are real algebraic in nature, as we never compute any complex zero.

*Related Literature.* There is a large literature on the problem of finding the radical ideal  $\sqrt{I}$  of an ideal  $I$ ; see, e.g., [3, 8, 17, 19, 23, 24]. For the general (positive-dimensional) case, Krick and Logar [23] propose an efficient algorithm based on splitting and reduction to the zero-dimensional case, which is implemented, e.g., in the computer algebra package Singular [18]. In the zero-dimensional case the problem is considered to be well solved, e.g., via the following method of Seidenberg [36]:  $\sqrt{I} = \langle I \cup \{q_1, \dots, q_n\} \rangle$ , the ideal generated by  $I$  and the  $q_i$ 's, where  $q_i$  is the square-free part of the monic generator  $p_i$  of  $I \cap \mathbb{K}[x_i]$ . Finding  $p_i$  is easy once a linear basis  $\mathcal{B}$  of  $\mathbb{K}[x]/I$  is known. Namely, find the smallest integer  $k_i$  for which  $\{1, x_i, x_i^2, \dots, x_i^{k_i}\}$  is linearly dependent in  $\mathbb{K}[x]/I$ ; then this smallest linear dependence gives the polynomial  $p_i$ . Next, the polynomial  $q_i$  can be found taking derivatives and gcd-computations as  $q_i = p_i / \gcd(p_i, p_i')$ . So finding  $I(V_{\mathbb{C}}(I))$  is easy if we have a basis of  $\mathbb{K}[x]/I$ . A classical method for finding such a basis  $\mathcal{B}$  is to compute a Gröbner basis of  $I$  and the corresponding set  $\mathcal{B}$  of standard monomials. The results in the present paper show that one may alternatively find such a basis  $\mathcal{B}$  from a suitable moment matrix.

On the other hand, the problem of computing the real radical ideal is considered to be much more difficult. For instance, in their paper, which is one of the first classical references on this problem, Becker and Neuhaus [1, p. 7] write that *the computation of  $\tau$ -real parts* (thus, the real radical ideal) *is much more difficult* (than that of the ordinary radical). They give an algorithm for  $\sqrt[\mathbb{R}]{I}$  based on finding the minimal real prime ideals  $P_i$  such that  $\sqrt[\mathbb{R}]{I} = \bigcap_i P_i$ . Among other advanced algebraic manipulations, their algorithm makes intensively use of (ordinary) radical computations. For other works along similar lines see, e.g., [2, 9] and also [26] for triangular polynomial sets.

Finally, let us mention that excellent algorithms and software packages exist for computing the complex variety  $V_{\mathbb{C}}(I)$  of a zero-dimensional ideal  $I$ , e.g., by Verschelde [43], Rouillier [35]; see also related work by Reid and Zhi [33] and, e.g., the monograph [16]. For instance, Verschelde [43] proposes symbolic–numeric algorithms via homotopy continuation methods (see also [37]), whereas Rouillier [35] solves a zero-dimensional system of polynomials by giving a rational univariate representation (RUR) for its solutions, of the form  $f(t) = 0, v_1 = g_1(t)/g(t), \dots, v_n = g_n(t)/g(t)$ , where  $f, g, g_1, \dots, g_n \in \mathbb{K}[t]$  are univariate polynomials. The computation of the RUR relies in an essential way on the multiplication matrices in the quotient algebra  $\mathbb{K}[x]/I$  which thus requires the knowledge of a corresponding linear basis.

*Our Contribution.* Given an ideal  $I \subseteq \mathbb{K}[x]$  ( $\mathbb{K} = \mathbb{R}, \mathbb{C}$ ) defined by a set of generators and satisfying  $|V_{\mathbb{K}}(I)| < \infty$ , we provide a method for computing  $V_{\mathbb{K}}(I)$  as well as a border basis and a Gröbner basis of the ideal  $I(V_{\mathbb{K}}(I))$ . Our approach is based on a semidefinite programming characterization of  $I(V_{\mathbb{K}}(I))$  with the following distinguishing feature. Remarkably, 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 the geometry behind it, when this matrix is required to be positive semidefinite with maximum rank. The latter property is achieved by standard semidefinite programming algorithms. For the task of computing the real roots and the real radical ideal  $I(V_{\mathbb{R}}(I))$ , the method is real algebraic in nature, as we do not compute (implicitly or explicitly) any complex element of  $V_{\mathbb{C}}(I)$ .

Lasserre [25] already recognized that moment matrices can be used for approximating the minimum of a polynomial over a basic closed semialgebraic set and sometimes extracting global minimizers (see [21]). The present paper builds on this approach and shows how it can be applied to finding the real radical of a zero-dimensional ideal. Moreover, there are links between moment matrices and the Hermite quadratic forms used in [32] for computing the number of real roots, that were pointed out in [28].

Our approach with its specificity is best illustrated on the task of computing the real radical ideal  $I(V_{\mathbb{R}}(I))$  that we now briefly describe.

Given a sequence  $y = (y_{\alpha})_{\alpha \in \mathbb{N}^n} \in \mathbb{R}^{\mathbb{N}^n}$ , consider the *moment matrix*

$$M^{\mathbb{R}}(y) := (y_{\alpha+\beta})_{\alpha, \beta \in \mathbb{N}^n}$$

(later we will also introduce complex moment matrices  $M^{\mathbb{C}}(y)$ ,  $M^{2\mathbb{C}}(y)$ ). One may think that  $y$  and  $M^{\mathbb{R}}(y)$  are indexed by the set  $\mathbb{T}_n := \{x^{\alpha} \mid \alpha \in \mathbb{N}^n\}$  of monomials. Given a polynomial  $h \in \mathbb{R}[x]$ , set  $\text{vec}(h) := (h_{\alpha})_{\alpha \in \mathbb{N}^n}$  and define the new sequence  $hy := M^{\mathbb{R}}(y)\text{vec}(h) \in \mathbb{R}^{\mathbb{N}^n}$ . By abuse of language let us say that  $h$  lies in the kernel of  $M^{\mathbb{R}}(y)$  when  $\text{vec}(h)$  does, which enables us to view  $\text{Ker } M^{\mathbb{R}}(y)$  as a subset of  $\mathbb{R}[x]$ . The following property of moment matrices plays a central role in our approach; it is based on ideas from [12, 13, 27] and will be proved at the end of Sect. 3. Let  $I = \langle h_1, \dots, h_m \rangle$  be an ideal generated by  $h_1, \dots, h_m \in \mathbb{R}[x]$ .

**Proposition 1.1** *Assume that  $V_{\mathbb{R}}(I)$  is finite. If*

$$M^{\mathbb{R}}(y) \succeq 0, \quad M^{\mathbb{R}}(h_j y) = 0 \quad (j = 1, \dots, m), \quad (1.1)$$

*then the kernel of  $M^{\mathbb{R}}(y)$  is a real radical ideal,  $\text{rank } M^{\mathbb{R}}(y) \leq |V_{\mathbb{R}}(I)|$  and  $I(V_{\mathbb{R}}(I)) \subseteq \text{Ker } M^{\mathbb{R}}(y)$ , with equality if and only if  $M^{\mathbb{R}}(y)$  has maximum rank, equal to  $|V_{\mathbb{R}}(I)|$ .*

(In (1.1) the notation “ $\succeq 0$ ” stands for positive semidefinite.) This semidefinite characterization leads directly to an algorithm for computing  $I(V_{\mathbb{R}}(I))$ , by considering *truncated* moment matrices in place of the full (infinite) moment matrix  $M^{\mathbb{R}}(y)$ . Namely, given an integer  $t$ , let  $M_t^{\mathbb{R}}(y)$  denote the principal submatrix of  $M^{\mathbb{R}}(y)$  whose rows and columns are indexed by the set  $\mathbb{T}_{n,t} := \{x^{\alpha} \mid \alpha \in \mathbb{N}^n \text{ with } |\alpha| := \sum_i \alpha_i \leq t\}$  and set

$$d_j := \lceil \deg(h_j)/2 \rceil, \quad d := \max_{j=1, \dots, m} d_j. \quad (1.2)$$

Fix  $t \geq d$  and assume  $M_t^{\mathbb{R}}(y)$  is a maximum rank matrix satisfying

$$M_t^{\mathbb{R}}(y) \succeq 0, \quad M_{t-d_j}^{\mathbb{R}}(h_j y) = 0 \quad (j = 1, \dots, m). \quad (1.3)$$

We will show that if, moreover,

$$\text{rank } M_s^{\mathbb{R}}(y) = \text{rank } M_{s-d}^{\mathbb{R}}(y) \quad (1.4)$$

for some  $d \leq s \leq t$ , then  $I(V_{\mathbb{R}}(I))$  coincides with the ideal generated by  $\text{Ker } M_s^{\mathbb{R}}(y)$ . The same conclusion holds if

$$\text{rank } M_s^{\mathbb{R}}(y) = \text{rank } M_{s-1}^{\mathbb{R}}(y) \quad (1.5)$$

for some  $2d \leq s \leq t$ . Moreover, from the semidefinite characterizations (1.3)–(1.5), the following algebraic objects can be obtained directly from the matrix  $M_t^{\mathbb{R}}(y)$ :

- (i) Let  $\mathcal{B} \subseteq \mathbb{T}_{n,s}$  be a set indexing a maximum nonsingular principal submatrix of  $M_s^{\mathbb{R}}(y)$ . Then  $\mathcal{B}$  is a linear basis of the quotient vector space  $\mathbb{R}[x]/I(V_{\mathbb{R}}(I))$  (see Sect. 3.3).
- (ii) We can compute directly from  $M_t^{\mathbb{R}}(y)$  the matrix of any multiplication operator in  $\mathbb{R}[x]/I(V_{\mathbb{R}}(I))$  with respect to the basis  $\mathcal{B}$ , and thus compute  $V_{\mathbb{R}}(I)$  (using the eigenvalue method, see Sect. 2.2).
- (iii) When the set  $\mathcal{B}$  (as in (i)) is an order ideal (i.e., is stable under division), the matrices of the multiplication operators by  $x_1, \dots, x_n$  give directly a border basis of the ideal  $I(V_{\mathbb{R}}(I))$  (see Sect. 2.5).
- (iv) Given a graded lexicographic monomial ordering, we can find a set  $\mathcal{B}$  (as in (i)) which is precisely the set of standard monomials; the associated reduced Gröbner basis of  $I(V_{\mathbb{R}}(I))$  can then be recovered, since it is contained in the border basis. In fact, our method also applies to an arbitrary monomial ordering (see Sect. 4.4.5).
- (v) Finally, the method can also detect whether the real variety  $V_{\mathbb{R}}(I)$  is empty. Indeed,  $V_{\mathbb{R}}(I) = \emptyset$  if and only if, for some integer  $t$ , the system (1.3) admits no solution  $y$  with  $y_0 \neq 0$  (see Remark 4.8).

*Further Discussion.* An independence oracle in  $\mathbb{R}[x]/I(V_{\mathbb{R}}(I))$  is needed for our algorithm in (iv) above. The following property is a crucial ingredient. Assume that one of the conditions (1.4) or (1.5) holds and consider a set  $T \subseteq \mathbb{T}_{n,s}$ . Then,  $T$  is linearly independent in  $\mathbb{R}[x]/I(V_{\mathbb{R}}(I))$  if and only if  $T$  indexes a linearly independent set of columns of  $M_t^{\mathbb{R}}(y)$ . In view of (iv), a Gröbner basis can easily be derived *afterwards* in contrast with classical methods which compute the set of standard monomials from the Gröbner basis.

Realizing the above tasks relies only on numerical linear algebraic operations on  $M_t^{\mathbb{R}}(y)$  like evaluating the rank of certain principal submatrices. Finding a matrix satisfying (1.3) is an instance of semidefinite programming. Moreover, it is a property of most interior-point algorithms for semidefinite programming that they do find such a matrix having maximum rank (see Sect. 4.4.1 for details).

The method is iterative. Namely, if the maximum rank matrix satisfying (1.3) does not satisfy (1.4) or (1.5), then we iterate with  $t + 1$  in place of  $t$ . The method eventually terminates since we will show that (1.4) holds for  $t$  large enough.

The following two small examples illustrate how positive semidefiniteness of the matrix  $M_t^{\mathbb{R}}(y)$  allows the elimination of all complex (nonreal) roots, whose number can be much larger than the number of real roots or even infinite.

**Example 1.2** Let  $I \subseteq \mathbb{R}[x]$  be generated by  $h_i = x_i(x_i^2 + 1)$  ( $i = 1, \dots, n$ ). Then,  $V_{\mathbb{R}}(I) = \{0\}$ ,  $|V_{\mathbb{C}}(I)| = 3^n$ ,  $d_i = 2$  for all  $i$ . Assume  $y$  satisfies (1.3) for order  $t = 3$ .

Then  $M_1^{\mathbb{R}}(h, y) = 0$  implies  $y_{4e_1} = -y_{2e_1}$  and  $M_3^{\mathbb{R}}(y) \geq 0$  implies  $y_{2e_1}, y_{4e_1} \geq 0$  which in turn implies  $y_{\alpha} = 0$  for all  $\alpha \neq 0$  with  $|\alpha| \leq 5$ . (Throughout,  $e_1, \dots, e_n$  denote the standard unit vectors in  $\mathbb{R}^n$ .) Hence  $\text{rank } M_2^{\mathbb{R}}(y) = \text{rank } M_0^{\mathbb{R}}(y) = 1$ ; that is, (1.4) holds for  $s = 2$ . In fact,  $\text{Ker } M_1^{\mathbb{R}}(y)$  is spanned by  $x_1, \dots, x_n$ , the generators of  $I(V_{\mathbb{R}}(I))$ . One may argue that the ideal  $I$  is already described by a Gröbner basis. But the same conclusion also holds under the change of variables  $x = Ay$  with  $A$  being a nonsingular matrix, in which case other methods would require a Gröbner basis computation.

**Example 1.3** Let  $I \subseteq \mathbb{R}[v_1, v_2]$  be generated by  $h = v_1^2 + v_2^2$ . Then  $V_{\mathbb{R}}(I) = \{0\}$  and  $V_{\mathbb{C}}(I) = \{(v_1, v_2) \mid v_1 = \pm i v_2\}$  is infinite. Then  $M_0^{\mathbb{R}}(hy) = 0$  gives  $y_{2e_1} + y_{2e_2} = 0$  which, together with  $M_1^{\mathbb{R}}(y) \geq 0$ , implies  $y_{\alpha} = 0$  for  $\alpha \neq 0$ . Hence the maximum rank of  $M_1^{\mathbb{R}}(y)$  is equal to 1 and  $\text{Ker } M_1^{\mathbb{R}}(y)$  is spanned by  $v_1, v_2$ , the generators of  $I(V_{\mathbb{R}}(I))$ .

The method sometimes (partially) applies even if none of the rank conditions (1.4), (1.5) holds, namely, when  $M_t^{\mathbb{R}}(y)$  contains sufficient information for the construction of the (formal) multiplication matrices. More precisely, let  $M_t^{\mathbb{R}}(y)$  be a maximum rank matrix satisfying (1.3), let  $\mathcal{B} \subseteq \mathbb{T}_{n,t-1}$  index a maximum nonsingular principal submatrix of  $M_t^{\mathbb{R}}(y)$ , set  $\partial\mathcal{B} := (\bigcup_{i=1}^n x_i \mathcal{B}) \setminus \mathcal{B}$ , and assume that the two principal submatrices of  $M_t^{\mathbb{R}}(y)$  indexed by  $\mathcal{B}$  and by  $\mathcal{B} \cup \partial\mathcal{B}$  have the same rank. Then, by the results of Kehrein, Kreuzer and Robbiano [16, Chap. 4], we can construct the formal multiplication matrices and, if they commute pairwise, a set  $W \supseteq V_{\mathbb{R}}(I)$  can be computed. By checking whether the points of  $W$  satisfy all the equations  $h_j = 0$ , we can eliminate the points in  $W \setminus V_{\mathbb{R}}(I)$ . It turns out that, for most examples we have tested,  $W = V_{\mathbb{R}}(I)$  holds and we are again able to find  $I(V_{\mathbb{R}}(I))$  together with a border basis generating this ideal.

Finally, the method also applies to the task of finding the radical ideal  $I(V_{\mathbb{C}}(I))$  of a zero-dimensional ideal  $I \subseteq \mathbb{C}[x]$ . For this, instead of using the matrix  $M_t^{\mathbb{R}}(y)$  where  $y$  is a real sequence indexed by  $\mathbb{T}_{n,t}$ , we have to use a matrix  $M_t^{2\mathbb{C}}(y)$  where the argument is a complex sequence indexed by  $\mathbb{T}_{2n,t}$  (see Sect. 3.1 for details). Similar results hold as in the real case. Namely, under certain rank conditions, the ideal  $I(V_{\mathbb{C}}(I))$  can be obtained as the ideal generated by the kernel of a maximum rank complex moment matrix (see Sect. 4.3 for details). However, a drawback in the complex case is that one must in general handle matrices of larger order which leads to larger semidefinite programs, thus more difficult to solve. However, so far we do not claim that our method can compete with existing methods for finding the complex variety  $V_{\mathbb{C}}(I)$  as, e.g., [35] or [43], especially in view of the present status of SDP solvers (that we use as a black box), still in their infancy.

*Contents of the Paper.* Section 2 contains preliminaries about ideals of polynomials, in particular, about the quotient ring  $\mathbb{K}[x]/I$ , multiplication matrices, Gröbner bases and border bases. We also indicate in Sect. 2.4 an algorithm for finding the set of standard monomials from an independence oracle in  $\mathbb{K}[x]/I$ . Section 3 contains preliminaries about moment matrices, in particular, results relating (real) radical ideals and kernels of positive semidefinite moment matrices. In Sect. 4 we prove the

main results about the semidefinite characterization of the variety  $V_{\mathbb{K}}(I)$  and the associated radical ideal  $I(V_{\mathbb{K}}(I))$ . Section 4.4 gives the details and implementation of an algorithm based on the semidefinite characterization, and Sect. 5 contains several examples illustrating its behaviour.

## 2 Preliminaries on Polynomial Ideals

### 2.1 Polynomial Ideals and Varieties

Throughout,  $\mathbb{K} = \mathbb{R}$  or  $\mathbb{C}$ , and  $\mathbb{K}[x] := \mathbb{K}[x_1, \dots, x_n]$  denotes the ring of multivariate polynomials in  $n$  variables over the field  $\mathbb{K}$ . For an integer  $t \geq 0$ ,  $\mathbb{K}[x]_t$  denotes the set of polynomials of degree at most  $t$ . For a scalar  $a \in \mathbb{C}$ ,  $\bar{a}$  denotes its complex conjugate and, for a vector  $u \in \mathbb{C}^n$  (resp., a matrix  $A$ ),  $u^*$  (resp.,  $A^*$ ) denotes its conjugate transpose. Following, e.g., [10],  $x^\alpha$  denotes the monomial  $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$  (for  $\alpha \in \mathbb{N}^n$ ) and  $cx^\alpha$  is called a term (for  $c \in \mathbb{K}$ ). Let  $\mathbb{T}_n := \{x^\alpha \mid \alpha \in \mathbb{N}^n\}$  denote the set of monomials and set  $\mathbb{N}_t^n := \{\alpha \in \mathbb{N}^n \mid |\alpha| := \sum_{i=1}^n \alpha_i \leq t\}$ ,  $\mathbb{T}_{n,t} := \{x^\alpha \mid \alpha \in \mathbb{N}_t^n\}$  for  $t \in \mathbb{N}$ . Following [16, Chap. 4], a set  $\mathcal{B} \subseteq \mathbb{T}_n$  is called an *order ideal* if  $\mathcal{B}$  is stable under division, i.e., for all  $a, b \in \mathbb{T}_n$ ,  $b \in \mathcal{B}$ ,  $a|b$  implies  $a \in \mathcal{B}$ . Given an ideal<sup>1</sup>  $I \subseteq \mathbb{K}[x]$ , let

$$V_{\mathbb{C}}(I) := \{v \in \mathbb{C}^n \mid f(v) = 0 \forall f \in I\}, \quad V_{\mathbb{R}}(I) := V_{\mathbb{C}}(I) \cap \mathbb{R}^n,$$

denote its complex and real varieties, respectively. For a set  $V \subseteq \mathbb{K}^n$ , define the ideal

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

Given an ideal  $I \subseteq \mathbb{K}[x]$ , one can define the ideals  $I(V_{\mathbb{C}}(I))$  and

$$\sqrt{I} := \{f \in \mathbb{K}[x] \mid f^m \in I \text{ for some } m \in \mathbb{N} \setminus \{0\}\}$$

and, when  $I \subseteq \mathbb{R}[x]$ , one can define the ideals  $I(V_{\mathbb{R}}(I))$  and

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

Obviously,

$$I \subseteq \sqrt{I} \subseteq I(V_{\mathbb{C}}(I)), \quad I \subseteq \sqrt[\mathbb{R}]{I} \subseteq I(V_{\mathbb{R}}(I)).$$

The ideal  $I$  is said to be *radical* (resp., *real radical*) if  $I = \sqrt{I}$  (resp.,  $I = \sqrt[\mathbb{R}]{I}$ ). Obviously,  $I \subseteq I(V_{\mathbb{C}}(I)) \subseteq I(V_{\mathbb{R}}(I))$ . Hence, if  $I \subseteq \mathbb{R}[x]$  is real radical, then  $I$  is radical and, moreover,  $V_{\mathbb{C}}(I) = V_{\mathbb{R}}(I) \subseteq \mathbb{R}^n$  if  $|V_{\mathbb{R}}(I)| < \infty$ . The following lemma gives a useful characterization for (real) radical ideals.

<sup>1</sup>An ideal  $I \subseteq \mathbb{K}[x]$  is an additive subgroup of  $\mathbb{K}[x]$  such that  $fg \in I$  whenever  $f \in I$  and  $g \in \mathbb{K}[x]$ .

**Lemma 2.1** *An ideal  $I \subseteq \mathbb{K}[x]$  is radical if and only if*

$$\forall p \in \mathbb{K}[x], \quad p^2 \in I \implies p \in I, \quad (2.1)$$

*and  $I \subseteq \mathbb{R}[x]$  is real radical if and only if*

$$\forall p_1, \dots, p_k \in \mathbb{R}[x], \quad p_1^2 + \dots + p_k^2 \in I \implies p_1, \dots, p_k \in I. \quad (2.2)$$

*Proof* If  $I$  is radical, then (2.1) obviously holds. Conversely, assume that (2.1) holds; we show that  $p^m \in I \implies p \in I$  by induction on  $m \geq 2$ . If  $p^m \in I$ , then  $p^{m+1} \in I$  and thus, by (2.1),  $p^{\lceil m/2 \rceil} \in I$  which, by the induction assumption, implies  $p \in I$ . The proof for the real radical case is along the same lines and thus omitted.  $\square$

**Theorem 2.2**

- (i) Hilbert's Nullstellensatz (see, e.g., [10, §4.1])  $\sqrt{I} = I(V_{\mathbb{C}}(I))$ .
- (ii) Real Nullstellensatz (see, e.g., [7, §4.1])  $\sqrt[\mathbb{R}]{I} = I(V_{\mathbb{R}}(I))$  for an ideal  $I \subseteq \mathbb{R}[x]$ .

For a polynomial  $p \in \mathbb{R}[x]$ ,  $x \mapsto p(x) = \sum_{\alpha} p_{\alpha} x^{\alpha}$ , let  $\text{vec}(p) := (p_{\alpha})_{\alpha \in \mathbb{N}^n}$  denote the vector of its coefficients. We also let  $\text{vec}(p)$  denote the vector  $(p_{\alpha})_{\alpha \in \mathbb{N}_t^n}$  for any  $t \geq \deg(p)$ , as  $p_{\alpha} = 0$  whenever  $|\alpha| > \deg(p)$ .

Finally, given  $A \subseteq \mathbb{K}[x]$ , let  $\langle A \rangle := \{\sum_{i=1}^k u_i p_i \mid p_i \in A, u_i \in \mathbb{K}[x]\}$  denote the ideal generated by  $A$ .

## 2.2 The Algebra $\mathbb{K}[x]/I$ and Multiplication Matrices

Consider the quotient space  $\mathbb{K}[x]/I$ , whose elements are the cosets  $[f] := f + I = \{f + q \mid q \in I\}$  for  $f \in \mathbb{K}[x]$ .  $\mathbb{K}[x]/I$  is a  $\mathbb{K}$ -vector space with addition  $[f] + [g] := [f + g]$  and scalar multiplication  $\lambda[f] := [\lambda f]$ , and an algebra with multiplication  $[f][g] := [fg]$ , for  $\lambda \in \mathbb{K}$ ,  $f, g \in \mathbb{K}[x]$ . In particular, for  $h \in \mathbb{K}[x]$ , the *multiplication operator*

$$m_h : \mathbb{K}[x]/I \longrightarrow \mathbb{K}[x]/I, \\ [f] \longmapsto [hf],$$

is well defined. The following well-known result relates the cardinality of  $V_{\mathbb{C}}(I)$  and the dimension of the vector space  $\mathbb{K}[x]/I$ . See, e.g., [10], [39] for a detailed treatment of the quotient algebra  $\mathbb{K}[x]/I$ .

**Theorem 2.3** *For an ideal  $I$  in  $\mathbb{K}[x]$ ,  $|V_{\mathbb{C}}(I)| < \infty \Leftrightarrow \dim \mathbb{K}[x]/I < \infty$ . Moreover,  $|V_{\mathbb{C}}(I)| \leq \dim \mathbb{K}[x]/I$ , with equality if and only if  $I$  is radical.*

Assume  $|V_{\mathbb{C}}(I)| < \infty$  and set  $N := \dim \mathbb{K}[x]/I \geq |V_{\mathbb{C}}(I)|$ . Consider a set  $\mathcal{B} := \{b_1, \dots, b_N\} \subseteq \mathbb{K}[x]$  for which the cosets  $[b_1], \dots, [b_N]$  are pairwise distinct and  $\{[b_1], \dots, [b_N]\}$  is a basis of  $\mathbb{K}[x]/I$ ; by abuse of language we also say that  $\mathcal{B}$  itself is a basis of  $\mathbb{K}[x]/I$ . Then every  $f \in \mathbb{K}[x]$  can be written in a unique way as  $f = \sum_{i=1}^N c_i b_i + p$ , where  $c_i \in \mathbb{K}$ ,  $p \in I$ ; the polynomial  $\text{res}_{\mathcal{B}}(f) := \sum_{i=1}^N c_i b_i$  is



called the *residue of  $f$  modulo  $I$  w.r.t. the basis  $\mathcal{B}$* . In other words, the vector space  $\text{Span}_{\mathbb{K}}(\mathcal{B}) := \{\sum_{i=1}^N c_i b_i \mid c_i \in \mathbb{K}\}$  is isomorphic to  $\mathbb{K}[x]/I$ .

Given a basis  $\mathcal{B}$  of  $\mathbb{K}[x]/I$  and  $h \in \mathbb{K}[x]$ , let  $\mathcal{X}_h$  denote the matrix of the multiplication operator  $m_h$  with respect to  $\mathcal{B}$ . That is, writing  $\text{res}_{\mathcal{B}}(hb_j) = \sum_{i=1}^N a_{ij} b_i$ , the  $j$ th column of  $\mathcal{X}_h$  is the vector  $(a_{ij})_{i=1}^N$ . The following well-known result relates the points of the variety  $V_{\mathbb{C}}(I)$  to the eigenvalues and eigenvectors of  $\mathcal{X}_h$ . See, e.g., [16, Chaps. 2, 3] for a detailed treatment.

**Theorem 2.4** *Let  $h \in \mathbb{K}[x]$  and, for  $v \in V_{\mathbb{C}}(I)$ , set  $\zeta_{\mathcal{B},v} := (b_i(v))_{i=1}^N$ . The set  $\{h(v) \mid v \in V_{\mathbb{C}}(I)\}$  is the set of eigenvalues of  $\mathcal{X}_h$  and  $\mathcal{X}_h^T \zeta_{\mathcal{B},v} = h(v) \zeta_{\mathcal{B},v}$  for all  $v \in V_{\mathbb{C}}(I)$ .*

When the matrix  $\mathcal{X}_h$  is nonderogatory (i.e., all its eigenspaces are one-dimensional), one can recover the points  $v \in V_{\mathbb{C}}(I)$  from the eigenvectors of  $\mathcal{X}_h^T$ . If  $I$  is radical, then  $N = |V_{\mathbb{C}}(I)|$  and thus  $\mathcal{X}_h$  is nonderogatory whenever the values  $h(v)$  ( $v \in V_{\mathbb{C}}(I)$ ) are pairwise distinct. This is achieved with high probability if one chooses  $h = \sum_{i=1}^n a_i x_i$  for random scalars  $a_i$ .

### 2.3 Gröbner Bases and Standard Monomials

A classical basis of  $\mathbb{K}[x]/I$  is the set of standard monomials with respect to some monomial ordering ‘ $\succ$ ’ of  $\mathbb{T}_n$ . Let us recall some definitions. (See, e.g., [10] for details.) Fix a monomial ordering  $\succ$  on  $\mathbb{T}_n$ . Write also  $ax^\alpha \succ bx^\beta$  if  $x^\alpha \succ x^\beta$  and  $a, b \in \mathbb{K} \setminus \{0\}$ . For a nonzero polynomial  $f = \sum_{\alpha} f_{\alpha} x^{\alpha}$ , its *leading term*  $\text{LT}(f)$  is the maximum  $f_{\alpha} x^{\alpha}$  with respect to  $\succ$  for which  $f_{\alpha} \neq 0$ . The leading term ideal of  $I$  is  $\text{LT}(I) := \langle \text{LT}(f) \mid f \in I \rangle$  and the set

$$\mathcal{B}_{\succ} := \mathbb{T}_n \setminus \text{LT}(I) = \{x^{\alpha} \mid \text{LT}(f) \text{ does not divide } x^{\alpha} \forall f \in I\}$$

is the set of *standard monomials*. Obviously,  $\mathcal{B}_{\succ}$  is an order ideal. A finite set  $G \subseteq I$  is a *Gröbner basis* of  $I$  if  $\text{LT}(I) = \langle \text{LT}(g) \mid g \in G \rangle$ ; thus  $x^{\alpha} \in \mathcal{B}_{\succ}$  if and only if  $x^{\alpha}$  is not divisible by the leading term of any polynomial in  $G$ . A Gröbner basis always exists and it can be constructed, e.g., with the algorithm of Buchberger. Call  $G$  *reduced* if, for all  $g \in G$ , the leading coefficient of  $\text{LT}(g)$  is 1 and no term of  $g$  lies in  $\langle \text{LT}(g') \mid g' \in G \setminus \{g\} \rangle$ . Given nonzero polynomials  $f, h_1, \dots, h_m$ , the division algorithm applied to dividing  $f$  by  $h_1, \dots, h_m$  produces polynomials  $u_1, \dots, u_m, r$  satisfying  $f = \sum_{j=1}^m u_j h_j + r$ , no term of  $r$  is divisible by  $\text{LT}(h_j)$  ( $j = 1, \dots, m$ ) and  $\text{LT}(f) \succeq \text{LT}(u_j h_j)$ . Note that  $\deg(u_i h_i) \leq \deg(f)$  when the monomial ordering is a graded lexicographic ordering. When  $\{h_1, \dots, h_m\}$  is a Gröbner basis of the ideal  $I := \langle h_1, \dots, h_m \rangle$ , the remainder  $r$  is uniquely determined and belongs to  $\text{Span}_{\mathbb{K}}(\mathcal{B}_{\succ})$ ; moreover,  $f \in I \Leftrightarrow r = 0$ . Therefore, the set  $\mathcal{B}_{\succ}$  is a basis of  $\mathbb{K}[x]/I$ .

For an arbitrary basis  $\mathcal{B}$  of  $\mathbb{K}[x]/I$ , set  $d_{\mathcal{B}} := \max_{b \in \mathcal{B}} \deg(b)$ . The next result shows that  $d_{\mathcal{B}}$  is minimum when  $\mathcal{B}$  is the set of standard monomials for some graded lexicographic order.

**Lemma 2.5** *Let  $I$  be a zero-dimensional ideal in  $\mathbb{K}[x]$ . Let  $\{g_1, \dots, g_k\}$  be the Gröbner basis of  $I$  with respect to a graded lexicographic monomial ordering and let  $\mathcal{B}_{\succ}$  be the corresponding set of standard monomials. For any basis  $\mathcal{B}$  of  $\mathbb{K}[x]/I$ , we have  $d_{\mathcal{B}_{\succ}} \leq d_{\mathcal{B}}$ .*

*Proof* Set  $\mathcal{B} = \{b_1, \dots, b_N\}$ . Write  $b_i = \sum_{x^\alpha \in \mathcal{B}_>} c_{i,\alpha} x^\alpha + \sum_{h=1}^k u_h g_h$  where  $c_{i,\alpha} \in \mathbb{K}$  for  $i = 1, \dots, N$  and  $u_h \in \mathbb{K}[x]$ . Then  $\deg(u_h g_h) \leq \deg(b_i)$  (by the properties of the division algorithm as we use a graded monomial ordering). Thus,  $\deg(\sum_{x^\alpha \in \mathcal{B}_>} c_{i,\alpha} x^\alpha) \leq \deg(b_i)$ . Let  $x^{\alpha_0} \in \mathcal{B}_>$  with  $\deg(x^{\alpha_0}) = d_{\mathcal{B}_>}$ . As  $\mathcal{B}, \mathcal{B}_>$  are two bases of  $\mathbb{K}[x]/I$ , the matrix  $(c_{i,\alpha})_{i=1,\dots,N,\alpha \in \mathcal{B}_>}$  is nonsingular and thus its  $\alpha_0$ th column is nonzero. Hence  $c_{i,\alpha_0} \neq 0$  for some  $i$ . Hence  $d_{\mathcal{B}_>} = \deg(\sum_{x^\alpha \in \mathcal{B}_>} c_{i,\alpha} x^\alpha) \leq \deg(b_i) \leq d_{\mathcal{B}}$ .  $\square$

## 2.4 Finding the Set of Standard Monomials from an Independence Oracle

When  $I$  is a zero-dimensional ideal and  $>$  is a monomial ordering on  $\mathbb{T}_n$ , we describe a method for finding the set  $\mathcal{B}_>$  of standard monomials, assuming we have an oracle for checking linear independence in  $\mathbb{K}[x]/I$ . This ‘greedy sieve’ algorithm, described below in Algorithm 1, does not require knowledge of a Gröbner basis of  $I$ .

---

### Algorithm 1 The ‘greedy sieve’ algorithm

---

**Input:** A zero-dimensional ideal  $I \in \mathbb{K}[x]$ , a monomial ordering  $>$  on  $\mathbb{T}_n$ , and an integer  $s \geq 1$ .

**Output:** A set  $\mathcal{B} \subseteq \mathbb{T}_{n,s}$  linearly independent in  $\mathbb{K}[x]/I$  and satisfying  $\mathcal{B} \supseteq \mathcal{B}_> \cap \mathbb{T}_{n,s}$

- 1: Order the monomials in  $\mathbb{T}_{n,s}$  with respect to  $>$ .
  - 2: Initialize  $\mathcal{B} := \emptyset$ ,  $L := (t_1, t_2, \dots)$ , the ordered set  $\mathbb{T}_{n,s}$ .
  - 3: **while**  $\mathcal{B} \subset L$  **do**
  - 4:   Set  $t$  as the first element of  $L \setminus \mathcal{B}$
  - 5:   **if**  $\mathcal{B} \cup \{t\}$  is linearly independent in  $\mathbb{K}[x]/I$  **then**
  - 6:     Reset  $\mathcal{B} := \mathcal{B} \cup \{t\}$
  - 7:   **else**
  - 8:     Reset  $L := L \setminus t\mathbb{T}_n$  (i.e., remove from  $L$  all multiples of  $t$ ).
  - 9:   **end if**
  - 10: **end while**
  - 11: **return**  $\mathcal{B} = L$
- 

The next lemma shows correctness of Algorithm 1 and how to use it for finding the set  $\mathcal{B}_>$  of standard monomials.

**Lemma 2.6** *Let  $I$  be a zero-dimensional ideal,  $>$  a monomial ordering on  $\mathbb{T}_n$ , and  $\mathcal{B}_> = \mathbb{T}_n \setminus \text{LT}(I)$  the associated set of standard monomials. For an integer  $s \geq 1$ , let  $\mathcal{B}_s$  be the set returned by the greedy sieve algorithm applied to  $(I, >, s)$ .*

- (i)  $\mathcal{B}_s$  is linearly independent in  $\mathbb{K}[x]/I$  and satisfies  $\mathcal{B}_> \cap \mathbb{T}_{n,s} \subseteq \mathcal{B}_s$ ; in particular,  $\mathcal{B}_s = \mathcal{B}_>$  if  $\mathcal{B}_> \subseteq \mathbb{T}_{n,s}$ .
- (ii) If  $\mathcal{B}_s = \mathcal{B}_{s+1}$ , then  $\mathcal{B}_s = \mathcal{B}_>$ .
- (iii) If  $>$  is a graded monomial ordering, then  $\mathcal{B}_s \subseteq \mathcal{B}_>$ ; therefore,  $\mathcal{B}_s = \mathcal{B}_>$  if  $|\mathcal{B}_s| = \dim \mathbb{K}[x]/I$ .

*Proof* (i) Obviously, throughout the algorithm,  $\mathcal{B}$  is linearly independent in  $\mathbb{K}[x]/I$  and  $\mathcal{B} \subseteq L$ . Assume  $t_k \in (\mathcal{B}_> \cap \mathbb{T}_{n,s}) \setminus \mathcal{B}_s$ . Consider the step when the algorithm

examines  $t_k$  and let  $\mathcal{B}$  be the current set maintained by the algorithm. Then,  $\mathcal{B} \subseteq \{t_1, \dots, t_{k-1}\}$ ,  $t_k \in L \setminus \mathcal{B}$  and  $\mathcal{B} \cup \{t_k\}$  is linearly dependent in  $\mathbb{K}[x]/I$ . Hence, there exists a polynomial  $f \in I$  with  $\text{LT}(f) = t_k$ , contradicting the assumption that  $t_k \in \mathcal{B}_>$ . This shows  $\mathcal{B}_> \cap \mathbb{T}_{n,s} \subseteq \mathcal{B}_s$ . Moreover, if  $\mathcal{B}_> \subseteq \mathbb{T}_{n,s}$ , then  $\mathcal{B}_> \subseteq \mathcal{B}_s$ ; equality holds since  $|\mathcal{B}_s| \leq \dim \mathbb{K}[x]/I$  as  $\mathcal{B}_s$  is linearly independent in  $\mathbb{K}[x]/I$ , while  $|\mathcal{B}_>| = \dim \mathbb{K}[x]/I$ .

(ii) Assume  $\mathcal{B}_s = \mathcal{B}_{s+1}$ . Then, in view of (i),  $\mathcal{B}_> \cap (\mathbb{T}_{n,s+1} \setminus \mathbb{T}_{n,s}) = \emptyset$ . This implies  $\mathcal{B}_> \subseteq \mathbb{T}_{n,s}$ . Indeed, assume  $t \in \mathcal{B}_>$  has degree at least  $s+1$ ; then any divisor  $t'$  of  $t$  with degree  $s+1$  lies in  $\mathcal{B}_>$  (since  $\mathcal{B}_>$  is an order ideal) and thus  $t' \in \mathcal{B}_> \cap (\mathbb{T}_{n,s+1} \setminus \mathbb{T}_{n,s}) = \emptyset$ , a contradiction. Therefore, by (i),  $\mathcal{B}_s = \mathcal{B}_>$ .

(iii) Assume  $>$  is a graded monomial ordering and, say,  $\mathcal{B}_> \subseteq \mathbb{T}_{n,d}$  for some integer  $d$ . If  $d \leq s$ , then  $\mathcal{B}_s = \mathcal{B}_>$  by (i). If  $d \geq s+1$ , then  $\mathcal{B}_s \subseteq \mathcal{B}_d$  (since all elements of  $\mathbb{T}_{n,d} \setminus \mathbb{T}_{n,s}$  come after the elements of  $\mathbb{T}_{n,s}$  in the ordering  $>$ ) and  $\mathcal{B}_d = \mathcal{B}_>$  (by (i)), implying  $\mathcal{B}_s \subseteq \mathcal{B}_>$ .  $\square$

*Remark 2.7* Observe that, when  $>$  is not a graded monomial degree ordering, one cannot claim the inclusion  $\mathcal{B}_s \subseteq \mathcal{B}_>$ . For instance, consider the ideal  $I = \langle x^3 - 1, -y + x^2 + x + 1 \rangle$  in  $\mathbb{R}[x, y]$  and choose as monomial ordering  $>$  the lexicographic order with  $y > x$ . Then,  $\mathcal{B}_> = \{1, x, x^2\}$  is found when applying Algorithm 1 to  $(I, >, s = 2)$ ; observe that  $\mathcal{B}_2 = \mathcal{B}_3$ . However, the algorithm applied to  $(I, >, s = 1)$  returns the set  $\mathcal{B}_1 = \{1, x, y\}$ ; thus  $\mathcal{B}_1 \not\subseteq \mathcal{B}_>$ , while  $|\mathcal{B}_1| = 3 = \dim \mathbb{R}[x]/I$ .

Alternatively, one could initialize the set  $L$  in Algorithm 1 to be the full ordered set  $\mathbb{T}_n$ . Then the algorithm still terminates in finitely many steps (because  $\dim \mathbb{K}[x]/I < \infty$ ) and the set  $\mathcal{B}$  returned by the algorithm is equal to  $\mathcal{B}_>$  (using the same argument as in Lemma 2.6(i), one can show that  $\mathcal{B}_> \subseteq \mathcal{B}$ , implying  $\mathcal{B}_> = \mathcal{B}$ ).

A crucial tool for applying Algorithm 1 is having an oracle for testing linear independence in  $\mathbb{K}[x]/I$ . In our setting the oracle will work as follows: Given a subset  $\mathcal{B} \subseteq \mathbb{T}_{n,s}$ ,  $\mathcal{B}$  is linearly independent in  $\mathbb{K}[x]/I$  if and only if  $\mathcal{B}$  indexes a linearly independent set of columns of a suitable moment matrix  $M_s(y)$ . This motivates why, in our presentation of Algorithm 1, we explore the set  $\mathbb{T}_{n,s}$  of monomials of degree at most  $s$ .

## 2.5 Border Bases and Formal Multiplication Matrices

We recall results about border bases following the exposition from [16, Chap. 4]. See also [39] for details about border bases. Given an order ideal  $\mathcal{B} \subseteq \mathbb{T}_n$ , the *border* of  $\mathcal{B}$  is the set

$$\partial\mathcal{B} := \{x_i x^\beta \mid x^\beta \in \mathcal{B}, i = 1, \dots, n\} \setminus \mathcal{B}. \quad (2.3)$$

Assume  $\mathcal{B} \neq \emptyset$ , set  $N := |\mathcal{B}|$ ,  $H := |\partial\mathcal{B}|$ , and write  $\mathcal{B} = \{b_1, \dots, b_N\}$  and  $\partial\mathcal{B} = \{c_1, \dots, c_H\}$ . A set of polynomials  $G = \{g_1, \dots, g_H\}$  is called a  $\mathcal{B}$ -border prebasis if each  $g_j$  is of the form

$$g_j = c_j - \sum_{i=1}^N a_{ij} b_i \quad \text{for some } a_{ij} \in \mathbb{K}. \quad (2.4)$$

One also says that  $g_j$  is marked by the element  $c_j$  of  $\partial\mathcal{B}$ . Given a polynomial  $f$ , the border division algorithm [16, Proposition 4.2.10] produces polynomials  $u_j, r$  such that  $f = \sum_{j=1}^H u_j g_j + r$ , and  $r \in \text{Span}_{\mathbb{K}}(\mathcal{B})$ . Hence, for any ideal  $I$  containing  $G$ ,  $\mathcal{B}$  spans the  $\mathbb{K}$ -vector space  $\mathbb{K}[x]/I$ . The set  $G \subseteq I$  is said to be a  $\mathcal{B}$ -border basis of  $I$  if  $\mathcal{B}$  is linearly independent in  $\mathbb{K}[x]/I$ , i.e., if  $\mathcal{B}$  is a linear basis of  $\mathbb{K}[x]/I$ ; in that case  $G$  generates the ideal  $I$ .

Stetter [39] advocates using border bases instead of Gröbner bases since they do not depend on any monomial ordering. Border bases represent in fact an extension of the notion of Gröbner bases. Indeed, the set  $\mathbb{T}_n \setminus \mathcal{B}$  defines a monomial ideal; the elements of the minimal set of generators of this monomial ideal are called the *corners* of  $\mathcal{B}$ , which belong to  $\partial\mathcal{B}$ . When  $\mathcal{B} = \mathcal{B}_{>}$  is the set of standard monomials for some monomial ordering, there exists a unique  $\mathcal{B}_{>}$ -border basis  $G$  of  $I$  and the reduced Gröbner basis of  $I$  is the subset of  $G$  consisting of the polynomials in  $G$  that are marked by the corners of  $\mathcal{B}_{>}$ .

When  $G$  is a  $\mathcal{B}$ -border prebasis, one can mimic the construction of the multiplication matrices from the previous section in the following way. Fix  $k \in \{1, \dots, n\}$ . The *formal multiplication matrix*  $\mathcal{X}_k$  is the  $N \times N$  matrix whose  $i$ th column is defined as follows. If  $x_k b_i \in \mathcal{B}$ , say,  $x_k b_i = b_r$ , then the  $i$ th column of  $\mathcal{X}_k$  is the standard unit vector  $e_r$  (with all zero entries except 1 at the  $r$ th position). Otherwise,  $x_k b_i \in \partial\mathcal{B}$ , say,  $x_k b_i = c_j$ , then the  $i$ th column of  $\mathcal{X}_k$  is the vector  $(a_{ij})_{i=1}^N$  (compare with (2.4)). We will use the following result (see [16, Theorem 4.3.17]).

**Theorem 2.8** *Let  $\mathcal{B} \subseteq \mathbb{T}_n$  be an order ideal, let  $G$  be a  $\mathcal{B}$ -border prebasis with associated formal multiplication matrices  $\mathcal{X}_1, \dots, \mathcal{X}_n$ , and let  $J := \langle G \rangle$  be the ideal generated by  $G$ . Then,  $G$  is a border basis of  $J$  if and only if the matrices  $\mathcal{X}_1, \dots, \mathcal{X}_n$  commute pairwise. In that case,  $\mathcal{B}$  is a linear basis of  $\mathbb{K}[x]/J$  and the matrix  $\mathcal{X}_k$  represents the multiplication operator  $m_{x_k}$  of  $\mathbb{K}[x]/J$  with respect to the basis  $\mathcal{B}$ .*

**Remark 2.9** Following Mourrain [31], call  $\mathcal{B} \subseteq \mathbb{T}_n$  *connected to 1* if  $1 \in \mathcal{B}$  and any monomial in  $\mathcal{B}$  is of the form  $x_{i_1} x_{i_2} \cdots x_{i_k}$  with  $x_{i_1}, x_{i_1} x_{i_2}, \dots, x_{i_1} x_{i_2} \cdots x_{i_k} \in \mathcal{B}$ . Obviously, if  $\mathcal{B}$  is an order ideal, then  $\mathcal{B}$  is connected to 1. As shown by Mourrain [31, Theorem 3.1], the result of Theorem 2.8 remains valid in the more general setting where  $\mathcal{B}$  is connected to 1 (instead of being an order ideal). We restrict our attention in this paper to monomial bases of  $\mathbb{K}[x]/J$  that are order ideals, in particular, because we have an algorithm for finding such bases, as we just saw in the preceding section. It will be interesting to investigate the use of bases satisfying Mourrain's criterion in subsequent work.

### 3 Preliminaries on Moment Matrices

#### 3.1 Moment Matrices

Given a sequence  $y \in \mathbb{R}^{\mathbb{N}^n}$ , its *real moment matrix*  $M^{\mathbb{R}}(y)$  is the real symmetric matrix indexed by  $\mathbb{N}^n$  whose  $(\alpha, \beta)$ th entry is  $y_{\alpha+\beta}$ , for  $\alpha, \beta \in \mathbb{N}^n$ . Given a sequence

$y \in \mathbb{C}^{\mathbb{N}^{2n}}$ , its *complex moment matrix* is the matrix  $M^{2\mathbb{C}}(y)$  indexed by  $\mathbb{N}^{2n}$  whose  $(\alpha\alpha', \beta\beta')$ th entry is  $y_{\alpha'+\beta, \alpha+\beta'}$  for  $(\alpha, \alpha'), (\beta, \beta') \in \mathbb{N}^{2n}$ . If  $y$  satisfies

$$y_{\alpha'\alpha} = \overline{y_{\alpha\alpha'}} \quad \text{for } (\alpha, \alpha') \in \mathbb{N}^{2n}, \tag{3.1}$$

then  $M^{2\mathbb{C}}(y)$  is a Hermitian matrix. Let  $M^{\mathbb{C}}(y)$  denote the principal submatrix of  $M^{2\mathbb{C}}(y)$  indexed by the subset  $\{(0\alpha') \mid \alpha' \in \mathbb{N}^n\}$ ; in other words, one may think of  $M^{\mathbb{C}}(y)$  as being indexed by  $\mathbb{N}^n$  with  $(\alpha', \beta')$ th entry  $y_{\alpha'\beta'}$ ; let us call  $M^{\mathbb{C}}(y)$  a *pruned complex moment matrix*. These three types of matrices  $M^{\mathbb{K}}(y)$  ( $\mathbb{K} = \mathbb{R}, \mathbb{C}$ ) and  $M^{2\mathbb{C}}(y)$  will play a central role in our treatment. It will be convenient to think of  $M^{\mathbb{K}}(y)$  as being indexed by  $\mathbb{T}_n$  and of  $M^{2\mathbb{C}}(y)$  as being indexed by

$$\bar{\mathbb{T}}_n := \{\bar{x}^\alpha x^{\alpha'} \mid \alpha, \alpha' \in \mathbb{N}^n\} \subseteq \mathbb{C}[x, \bar{x}].$$

Thus  $\bar{\mathbb{T}}_n \sim \mathbb{T}_{2n}$  and we view  $x$  as a complex variable in the complex case. Recall that one says that ‘ $f \in \mathbb{K}[x]$  lies in the kernel of  $M^{\mathbb{K}}(y)$ ’ if  $M^{\mathbb{K}}(y) \text{vec}(f) = 0$ . Similarly, one may identify a polynomial  $(x, \bar{x}) \mapsto f(x, \bar{x}) = \sum_{\alpha, \alpha'} f_{\alpha, \alpha'} \bar{x}^\alpha x^{\alpha'}$  with its sequence of coefficients  $\text{vec}(f) = (f_{\alpha, \alpha'})_{\alpha, \alpha'}$  which allows us to say that ‘ $f \in \mathbb{C}[x, \bar{x}]$  lies in  $\text{Ker } M^{2\mathbb{C}}(y)$ ’ if  $M^{2\mathbb{C}}(y) \text{vec}(f) = 0$ .

We also need *truncated* moment matrices. For an integer  $t \geq 0$ ,  $M_t^{\mathbb{K}}(y)$  denotes the principal submatrix of  $M^{\mathbb{K}}(y)$  indexed by  $\mathbb{T}_{n,t}$  and  $M_t^{2\mathbb{C}}(y)$  denotes the principal submatrix of  $M^{2\mathbb{C}}(y)$  indexed by the set  $\bar{\mathbb{T}}_{n,t} := \{\bar{x}^\alpha x^{\alpha'} \mid \alpha, \alpha' \in \mathbb{N}^n, |\alpha| + |\alpha'| \leq t\} \sim \mathbb{T}_{2n,t}$ . Given  $h \in \mathbb{R}[x]$ ,  $h(x) = \sum_{\beta} h_{\beta} x^{\beta}$ , and  $y \in \mathbb{R}^{\mathbb{N}^n}$ , define  $hy \in \mathbb{R}^{\mathbb{N}^n}$  by

$$hy := M^{\mathbb{R}}(y) \text{vec}(h); \quad \text{that is, } (hy)_{\alpha} = \sum_{\beta} h_{\beta} y_{\alpha+\beta} \quad \text{for } \alpha \in \mathbb{N}^n.$$

Similarly, given  $h(x, \bar{x}) = \sum_{\beta, \beta'} h_{\beta\beta'} \bar{x}^{\beta} x^{\beta'} \in \mathbb{C}[x, \bar{x}]$  and  $y \in \mathbb{C}^{\mathbb{N}^{2n}}$ , define  $hy \in \mathbb{C}^{\mathbb{N}^{2n}}$  by

$$hy := M^{2\mathbb{C}}(y) \text{vec}(h); \quad \text{that is, } (hy)_{\alpha\alpha'} = \sum_{\beta, \beta'} h_{\beta\beta'} y_{\alpha'+\beta, \alpha+\beta'} \quad \text{for } \alpha, \alpha' \in \mathbb{N}^n.$$

When  $h \in \mathbb{C}[x]$  (i.e.,  $h_{\beta\beta'} = 0$  if  $\beta \neq 0$ ),  $M^{\mathbb{C}}(y) \text{vec}(h)$  is the projection of  $M^{2\mathbb{C}}(y) \text{vec}(h)$  onto the coordinates indexed by the pairs  $(\alpha, \alpha')$  with  $\alpha = 0$ .

### 3.2 Measures and Kernels of Moment Matrices

For a Hermitian matrix  $A$ , write  $A \geq 0$  if  $A$  is positive semidefinite, i.e., if  $u^* Au \geq 0$  for all  $u \in \mathbb{C}^n$  (or  $u \in \mathbb{R}^n$  when  $A$  is real valued).

*The Real Case.* For  $v \in \mathbb{C}^n$ , set  $\zeta_v := (v^\alpha)_{\alpha \in \mathbb{N}^n}$  and  $\zeta_{t,v} := (v^\alpha)_{\alpha \in \mathbb{N}_t^n}$  for an integer  $t \geq 0$ . Let  $\mu$  be a positive measure on  $\mathbb{R}^n$  with finite support; say,  $\mu = \sum_{v \in W} \lambda_v \delta_v$  where  $\lambda_v > 0$  and  $W \subseteq \mathbb{R}^n$ ,  $|W| < \infty$ . The *sequence of moments of the measure*  $\mu$  is the sequence  $y^\mu \in \mathbb{R}^{\mathbb{N}^n}$  defined by  $(y^\mu)_\alpha := \int x^\alpha d\mu = \sum_{v \in W} \lambda_v v^\alpha$  for  $\alpha \in \mathbb{N}^n$ ;

$(y^\mu)_0 = \sum_{v \in W} \lambda_v$  is the total mass of the measure, equal to 1 if  $\mu$  is a probability measure. We have

$$y^\mu = \sum_{v \in W} \lambda_v \zeta_v.$$

Moreover,  $M^{\mathbb{R}}(y^\mu) = \sum_{v \in W} \lambda_v \zeta_v \zeta_v^T \geq 0$  and

$$\text{Ker } M^{\mathbb{R}}(y^\mu) = \{f \in \mathbb{R}[x] \mid f(v) = 0 \forall v \in W\} = I(W),$$

$$\text{Ker } M_t^{\mathbb{R}}(y^\mu) = I(W) \cap \mathbb{R}[x]_t$$

(which follows from the fact that  $\text{vec}(f)^T M_t^{\mathbb{R}}(\zeta_{2t,v}) \text{vec}(f) = f(v)^2$  for  $f \in \mathbb{R}[x]_t$ ). Given polynomials  $h_1, \dots, h_m \in \mathbb{R}[x]$ , let  $d_j, d$  be defined as in (1.2) and, for  $t \geq d$ , set

$$K_t^{\mathbb{R}} := \{y \in \mathbb{R}^{\mathbb{N}_{2t}^n} \mid y_0 = 1, M_t^{\mathbb{R}}(y) \geq 0, M_{t-d_j}^{\mathbb{R}}(h_j y) = 0 (j = 1, \dots, m)\}. \quad (3.2)$$

Then,  $K_t^{\mathbb{R}}$  is a convex set which contains the vectors  $\zeta_{2t,v}$  for all  $v \in V_{\mathbb{R}}(I)$ . The following geometric observation, which indicates how the real radical ideal of  $I$  relates to the kernel of moment matrices, will play a central role in our approach.

**Lemma 3.1** *Let  $I = \langle h_1, \dots, h_m \rangle \subseteq \mathbb{R}[x]$ ,  $t \geq d$ , and let  $y \in K_t^{\mathbb{R}}$  for which  $\text{rank } M_t^{\mathbb{R}}(y)$  is maximum. Then,  $\text{Ker } M_t^{\mathbb{R}}(y) \subseteq \text{Ker } M_t^{\mathbb{R}}(z)$  for all  $z \in K_t^{\mathbb{R}}$ . Moreover,  $\text{Ker } M_t^{\mathbb{R}}(y) \subseteq I(V_{\mathbb{R}}(I))$ .*

*Proof* Let  $z \in K_t^{\mathbb{R}}$ . Then,  $y' := \frac{1}{2}(y + z) \in K_t^{\mathbb{R}}$  and  $\text{Ker } M_t^{\mathbb{R}}(y') = \text{Ker } M_t^{\mathbb{R}}(y) \cap \text{Ker } M_t^{\mathbb{R}}(z) \subseteq \text{Ker } M_t^{\mathbb{R}}(y)$ . As  $\text{rank } M_t^{\mathbb{R}}(y) \geq \text{rank } M_t^{\mathbb{R}}(y')$ , equality  $\text{Ker } M_t^{\mathbb{R}}(y) \cap \text{Ker } M_t^{\mathbb{R}}(z) = \text{Ker } M_t^{\mathbb{R}}(y)$  holds, which implies  $\text{Ker } M_t^{\mathbb{R}}(y) \subseteq \text{Ker } M_t^{\mathbb{R}}(z)$ . As  $\zeta_{2t,v} \in K_t^{\mathbb{R}}$  for all  $v \in V_{\mathbb{R}}(I)$ , this implies  $\text{Ker } M_t^{\mathbb{R}}(y) \subseteq \bigcap_{v \in V_{\mathbb{R}}(I)} \text{Ker } M_t^{\mathbb{R}}(\zeta_{2t,v})$  which in turn is contained in  $I(V_{\mathbb{R}}(I))$ .  $\square$

*The Complex Case.* Let  $\mu$  be a positive measure on  $\mathbb{C}^n$  with finite support; that is,  $\mu = \sum_{v \in W} \lambda_v \delta_v$  where  $\lambda_v > 0$  and  $W \subseteq \mathbb{C}^n$ ,  $|W| < \infty$ . One can now define the doubly indexed sequence of moments  $y^\mu \in \mathbb{C}^{\mathbb{N}^{2n}}$  of the measure  $\mu$  by  $(y^\mu)_{\alpha\alpha'} := \int \bar{x}^\alpha x^{\alpha'} d\mu = \sum_{v \in W} \lambda_v \bar{v}^\alpha v^{\alpha'}$  for  $\alpha, \alpha' \in \mathbb{N}^n$ . Thus  $y^\mu$  satisfies (3.1) and

$$y^\mu = \sum_{v \in W} \lambda_v \zeta_{\bar{v}} \otimes \zeta_v.$$

Therefore,  $M^{2\mathbb{C}}(y^\mu) = \sum_{v \in W} \lambda_v \zeta_v \otimes \zeta_{\bar{v}} (\zeta_{\bar{v}} \otimes \zeta_v)^T \geq 0$  and, in particular,  $M^{\mathbb{C}}(y^\mu) = \sum_{v \in W} \lambda_v \zeta_{\bar{v}} \zeta_v^T \geq 0$ . Moreover,

$$\text{Ker } M^{\mathbb{C}}(y^\mu) = \{f \in \mathbb{C}[x] \mid f(v) = 0 \forall v \in W\} = I(W),$$

$$\text{Ker } M^{2\mathbb{C}}(y^\mu) = \{f \in \mathbb{C}[x, \bar{x}] \mid f(v, \bar{v}) = 0 \forall v \in W\},$$

(using the fact that  $\text{vec}(f)^* M^{2\mathbb{C}}(\zeta_{\bar{v}} \otimes \zeta_v) \text{vec}(f) = |f(v, \bar{v})|^2$  for  $f \in \mathbb{C}[x, \bar{x}]$ ). Given polynomials  $h_1, \dots, h_m \in \mathbb{C}[x]$ ,  $t \geq d$ , define the sets

$$\begin{aligned} K_t^{\mathbb{C}} &:= \{y \in \mathbb{C}^{\mathbb{N}_{2t}^{2n}} \mid y_0 = 1, (3.1), M_t^{\mathbb{C}}(y) \succeq 0, \\ &\quad M_{t-d_j}^{\mathbb{C}}(h_j y) = 0 \ (j = 1, \dots, m)\}, \\ K_t^{2\mathbb{C}} &:= \{y \in \mathbb{C}^{\mathbb{N}_{2t}^{2n}} \mid y_0 = 1, (3.1), M_t^{2\mathbb{C}}(y) \succeq 0, \\ &\quad M_{t-d_j}^{2\mathbb{C}}(h_j y) = 0 \ (j = 1, \dots, m)\}. \end{aligned} \tag{3.3}$$

Hence,  $K_t^{2\mathbb{C}} \subseteq K_t^{\mathbb{C}}$  are both convex sets. The following analogue of Lemma 3.1 holds in the complex case; we omit the proof.

**Lemma 3.2** *Let  $I = \langle h_1, \dots, h_m \rangle \subseteq \mathbb{C}[x]$  and  $t \geq d$ .*

- (i) *Let  $y \in K_t^{\mathbb{C}}$  for which  $\text{rank } M_t^{\mathbb{C}}(y)$  is maximum. Then,  $\text{Ker } M_t^{\mathbb{C}}(y) \subseteq \text{Ker } M_t^{\mathbb{C}}(z)$  for all  $z \in K_t^{\mathbb{C}}$ . Moreover,  $\text{Ker } M_t^{\mathbb{C}}(y) \subseteq I(V_{\mathbb{C}}(I))$ .*
- (ii) *Let  $y \in K_t^{2\mathbb{C}}$  for which  $\text{rank } M_t^{2\mathbb{C}}(y)$  is maximum. Then,  $\text{Ker } M_t^{2\mathbb{C}}(y) \subseteq \text{Ker } M_t^{2\mathbb{C}}(z)$  for all  $z \in K_t^{2\mathbb{C}}$ . Moreover,  $\text{Ker } M_t^{\mathbb{C}}(y) \subseteq I(V_{\mathbb{C}}(I))$ .*

*Link Between the Real and Complex Cases.* As shown, e.g., in [14], the complex moment problem in  $\mathbb{C}^n$  can be reduced to the real moment problem in  $\mathbb{R}^{2n}$ . Let us sketch the main idea. For  $\alpha, \alpha' \in \mathbb{N}^n$ , define the polynomials

$$\begin{aligned} \Phi^{(\alpha\alpha')}(x, \bar{x}) &:= \left(\frac{x - \bar{x}}{2i}\right)^{\alpha} \left(\frac{x + \bar{x}}{2}\right)^{\alpha'} = \sum_{\beta\beta'} \varphi_{\beta\beta'}^{(\alpha\alpha')} \bar{x}^{\beta} x^{\beta'}, \\ \Psi^{(\alpha\alpha')}(u, v) &:= (v - iu)^{\alpha} (v + iu)^{\alpha'} = \sum_{\beta\beta'} \psi_{\beta\beta'}^{(\alpha\alpha')} u^{\beta} v^{\beta'}. \end{aligned}$$

The following can easily be verified: For all  $x \in \mathbb{C}^n$ , and all  $(u, v) \in \mathbb{R}^n$ ,

$$\overline{\Phi^{(\alpha\alpha')}(x, \bar{x})} = \Phi^{(\alpha\alpha')}(x, \bar{x}), \quad \overline{\Psi^{(\alpha\alpha')}(u, v)} = \Psi^{(\alpha'\alpha)}(u, v).$$

In addition,  $\Phi^{(\alpha\alpha'+\beta\beta')} = \Phi^{(\alpha\alpha')} \Phi^{(\beta\beta')}$ , and  $\Psi^{(\alpha\alpha'+\beta\beta')} = \Psi^{(\alpha\alpha')} \Psi^{(\beta\beta')}$ . Moreover, for every  $\alpha, \alpha' \in \mathbb{N}^n$ ,

$$\sum_{\beta\beta'} \psi_{\beta\beta'}^{(\alpha\alpha')} \Phi^{(\beta\beta')}(x, \bar{x}) = \bar{x}^{\alpha} x^{\alpha'}, \quad \sum_{\beta\beta'} \varphi_{\beta\beta'}^{(\alpha\alpha')} \Psi^{(\beta\beta')}(u, v) = u^{\alpha} v^{\alpha'}.$$

Next, given  $y \in \mathbb{C}^{\mathbb{N}^{2n}}$ , define the linear mapping  $L_y : \mathbb{C}[x, \bar{x}] \rightarrow \mathbb{C}$  by  $L_y(f) = \sum_{\beta\beta'} f_{\beta\beta'} y_{\beta\beta'}$  for  $f \in \mathbb{C}[x, \bar{x}]$  with  $f(x, \bar{x}) = \sum_{\beta\beta'} f_{\beta\beta'} \bar{x}^{\beta} x^{\beta'}$ , and the mapping  $\varphi : \mathbb{C}^{\mathbb{N}^{2n}} \rightarrow \mathbb{C}^{\mathbb{N}^{2n}}$ ,  $y \mapsto a := \varphi(y)$  with

$$a_{\alpha\alpha'} = L_y(\Phi^{(\alpha\alpha')}) = \sum_{\beta\beta'} \varphi_{\beta\beta'}^{(\alpha\alpha')} y_{\beta\beta'} \quad (\alpha\alpha' \in \mathbb{N}^{2n}). \tag{3.4}$$

Notice that  $a \in \mathbb{R}^{\mathbb{N}^{2n}}$  if  $y$  satisfies (3.1). Conversely, given  $a \in \mathbb{C}^{\mathbb{N}^{2n}}$ , let  $L_a : \mathbb{C}[u, v] \rightarrow \mathbb{C}$  be the linear mapping

$$g \left( = \sum_{\beta\beta'} g_{\beta\beta'} u^\beta v^{\beta'} \right) \mapsto L_a(g) := \sum_{\beta\beta'} g_{\beta\beta'} a_{\beta\beta'}, \quad g \in \mathbb{C}[u, v],$$

and the linear mapping  $\psi : \mathbb{C}^{\mathbb{N}^{2n}} \rightarrow \mathbb{C}^{\mathbb{N}^{2n}}$ ,  $a \mapsto y := \psi(a)$  by

$$y_{\alpha\alpha'} = L_a(\Psi^{(\alpha\alpha')}) \quad (\alpha\alpha' \in \mathbb{N}^{2n}).$$

Notice that  $y$  satisfies (3.1) whenever  $a$  is real valued. The mappings  $\varphi$  and  $\psi$  are inverse bijections between the set of sequences in  $\mathbb{C}^{\mathbb{N}^{2n}}$  satisfying (3.1) and  $\mathbb{R}^{\mathbb{N}^{2n}}$ . Based on the above observations, we can now verify that

$$M^{2\mathbb{C}}(y) \succeq 0 \iff M^{\mathbb{R}}(a) \succeq 0.$$

Assume first  $M^{2\mathbb{C}}(y) \succeq 0$  and let  $f \in \mathbb{R}^{\mathbb{N}^{2n}}$  be arbitrary. Then

$$\begin{aligned} f^T M^{\mathbb{R}}(a) f &= \sum_{\alpha\alpha', \beta\beta'} f_{\alpha\alpha'} f_{\beta\beta'} a_{\alpha\alpha'+\beta\beta'} = L_y \left( \sum_{\alpha\alpha', \beta\beta'} f_{\alpha\alpha'} f_{\beta\beta'} \Phi^{(\alpha\alpha'+\beta\beta')} \right) \\ &= L_y \left( \left( \sum_{\alpha\alpha'} f_{\alpha\alpha'} \Phi^{(\alpha\alpha')} \right)^2 \right) = \text{vec}(g^*) M^{2\mathbb{C}}(y) \text{vec}(g) \geq 0, \end{aligned}$$

with  $g(x, \bar{x}) := \sum_{\alpha\alpha'} f_{\alpha\alpha'} \Phi^{(\alpha\alpha')}(x, \bar{x})$ . This shows that  $M^{\mathbb{R}}(a) \succeq 0$ . Conversely, assume  $M^{\mathbb{R}}(a) \succeq 0$ , and let  $g \in \mathbb{C}^{\mathbb{N}^{2n}}$  be arbitrary. Then

$$\begin{aligned} g^* M^{2\mathbb{C}}(y) g &= \sum_{\alpha\alpha', \beta\beta'} \overline{g_{\alpha\alpha'}} g_{\beta\beta'} y_{\alpha'+\beta, \alpha+\beta'} \\ &= L_a \left( \sum_{\alpha\alpha', \beta\beta'} \overline{g_{\alpha\alpha'}} g_{\beta\beta'} \Psi^{(\alpha'+\beta, \alpha+\beta')} \right) = L_a(\bar{h}h), \end{aligned}$$

with  $h(u, v) := \sum_{\alpha\alpha'} g_{\alpha\alpha'} \Psi^{(\alpha\alpha')}(u, v)$ . Now  $h = h_1 + ih_2$  with  $h_1, h_2 \in \mathbb{R}[u, v]$ , and so

$$\begin{aligned} L_a(\bar{h}h) &= L_a(h_1^2 + h_2^2) \\ &= \text{vec}(h_1)^T M^{\mathbb{R}}(a) \text{vec}(h_1) + \text{vec}(h_2)^T M^{\mathbb{R}}(a) \text{vec}(h_2) \geq 0, \end{aligned}$$

which shows that  $M^{2\mathbb{C}}(y) \succeq 0$ .

Finally,  $y$  is the sequence of moments of a measure on the set  $W \subseteq \mathbb{C}^n$  if and only if  $a$  is the sequence of moments of a measure on the set  $\{(\text{Im}(v), \text{Re}(v)) \mid v \in W\} \subseteq \mathbb{R}^{2n}$ . (Use the fact that, if  $y = \zeta_{\bar{v}} \otimes \zeta_v$ , then  $a = \zeta_{(\text{Im}(v), \text{Re}(v))}$ .)



### 3.3 Flat Extensions and Finite Rank Moment Matrices

Given a Hermitian matrix  $A$  and a principal submatrix  $B$  of  $A$ , one says that  $A$  is a *flat extension* of  $B$  if  $\text{rank } A = \text{rank } B$ ; then  $A \geq 0 \Leftrightarrow B \geq 0$ . We begin with two fundamental results of Curto and Fialkow [12] about *finite rank* moment matrices, where this notion of flat extension plays a central role. See [27] for a short proof of Theorem 3.3 and [29] for an exposition of Theorem 3.4.

#### Theorem 3.3

- (i) If  $M^{\mathbb{R}}(y) \geq 0$  and  $\text{rank } M^{\mathbb{R}}(y) < \infty$ , then  $y = \sum_{v \in W} \lambda_v \zeta_v$  for some finite set  $W \subseteq \mathbb{R}^n$  and  $\lambda_v > 0$ ,  $|W| = \text{rank } M^{\mathbb{R}}(y)$ , and  $\text{Ker } M^{\mathbb{R}}(y) = I(W)$ .
- (ii) If  $M^{2\mathbb{C}}(y) \geq 0$  and  $\text{rank } M^{2\mathbb{C}}(y) < \infty$ , then  $y = \sum_{v \in W} \lambda_v \zeta_v \otimes \zeta_v$  for some finite set  $W \subseteq \mathbb{C}^n$  and  $\lambda_v > 0$ ,  $|W| = \text{rank } M^{2\mathbb{C}}(y)$ , and  $\text{Ker } M^{\mathbb{C}}(y) = I(W)$ .

#### Theorem 3.4

- (i) If  $M_t^{\mathbb{R}}(y) \geq 0$  and  $\text{rank } M_t^{\mathbb{R}}(y) = \text{rank } M_{t-1}^{\mathbb{R}}(y)$ , then  $y$  can be extended in a unique way to  $\tilde{y} \in \mathbb{R}^{\mathbb{N}^n}$  such that  $M^{\mathbb{R}}(\tilde{y})$  is a flat extension of  $M_t^{\mathbb{R}}(y)$  (and thus  $M^{\mathbb{R}}(\tilde{y}) \geq 0$ ).
- (ii) If  $M_t^{2\mathbb{C}}(y) \geq 0$  and  $\text{rank } M_t^{2\mathbb{C}}(y) = \text{rank } M_{t-1}^{2\mathbb{C}}(y)$ , then  $y$  can be extended in a unique way to  $\tilde{y} \in \mathbb{C}^{\mathbb{N}^{2n}}$  such that  $M^{2\mathbb{C}}(\tilde{y})$  is a flat extension of  $M_t^{2\mathbb{C}}(y)$  (and thus  $M^{2\mathbb{C}}(\tilde{y}) \geq 0$ ).

The following lemma taken from [12] shows that the kernel of a truncated moment matrix enjoys ideal-like properties.

#### Lemma 3.5

- (i) Let  $M_t^{\mathbb{R}}(y) \geq 0$ ,  $f, g \in \mathbb{R}[x]$ , with  $\deg(fg) \leq t - 1$ . Then,  $M_t^{\mathbb{R}}(y) \text{vec}(f) = 0 \implies M_t^{\mathbb{R}}(y) \text{vec}(fg) = 0$ .
- (ii) Let  $M_t^{2\mathbb{C}}(y) \geq 0$ ,  $f, g \in \mathbb{C}[x, \bar{x}]$ , with  $\deg(fg) \leq t - 1$ . Then,  $M_t^{2\mathbb{C}}(y) \text{vec}(f) = 0 \implies M_t^{2\mathbb{C}}(y) \text{vec}(fg) = 0$ .

*Proof* Set  $h := fg$ . (i) As  $\deg(h) \leq t - 1$  and  $M_t^{\mathbb{R}}(y) \geq 0$ , it suffices to show  $M_{t-1}^{\mathbb{R}}(y) \text{vec}(h) = 0$ . Moreover, it suffices to show the result for  $g = x_i$ ; in this latter case one can verify that, for  $\alpha \in \mathbb{N}_{t-1}^n$ ,  $(M_{t-1}^{\mathbb{R}}(y) \text{vec}(h))_{\alpha} = (M_t^{\mathbb{R}}(y) \text{vec}(f))_{\alpha+e_i} = 0$ .

(ii) Similarly, assume  $g = x_i$  or  $\bar{x}_i$ . For  $\alpha\alpha' \in \bar{\mathbb{T}}_{n,t-1}$ ,  $(M_{t-1}^{2\mathbb{C}}(y) \text{vec}(h))_{\alpha\alpha'}$  is equal to  $(M_t^{2\mathbb{C}}(y) \text{vec}(f))_{\alpha+e_i \alpha'}$  if  $g = x_i$  and to  $(M_t^{2\mathbb{C}}(y) \text{vec}(f))_{\alpha \alpha'+e_i}$  if  $g = \bar{x}_i$ , thus to 0 in both cases.  $\square$

**Proposition 3.6**  $\text{Ker } M^{\mathbb{R}}(y)$  is an ideal in  $\mathbb{R}[x]$ , which is real radical if  $M^{\mathbb{R}}(y) \geq 0$ . Assume  $M^{\mathbb{R}}(y) \geq 0$  and  $\text{rank } M^{\mathbb{R}}(y) = \text{rank } M_{t-1}^{\mathbb{R}}(y)$  for some integer  $t \geq 1$ . Then,  $\text{Ker } M^{\mathbb{R}}(y) = \langle \text{Ker } M_t^{\mathbb{R}}(y) \rangle$  and, for  $\mathcal{B} \subseteq \mathbb{T}_n$ ,  $\mathcal{B}$  indexes a (maximum) nonsingular principal submatrix of  $M^{\mathbb{R}}(y)$  if and only if  $\mathcal{B}$  is a (maximum) linearly independent subset of  $\mathbb{R}[x]/\text{Ker } M^{\mathbb{R}}(y)$ .

*Proof* We use the (easy to verify) identity

$$\text{vec}(h)^T M^{\mathbb{R}}(y) \text{vec}(pq) = \text{vec}(hq)^T M^{\mathbb{R}}(y) \text{vec}(p)$$

for  $p, q, h \in \mathbb{R}[x]$ . If  $p \in \text{Ker } M^{\mathbb{R}}(y)$ ,  $q \in \mathbb{R}[x]$ , then  $\text{vec}(h)^T M^{\mathbb{R}}(y) \text{vec}(pq) = \text{vec}(hq)^T M^{\mathbb{R}}(y) \text{vec}(p) = 0$  for all  $h \in \mathbb{R}[x]$ , which implies  $M^{\mathbb{R}}(y) \text{vec}(pq) = 0$  and thus  $pq \in \text{Ker } M^{\mathbb{R}}(y)$ . This shows that  $\text{Ker } M^{\mathbb{R}}(y)$  is an ideal. Assume now  $M^{\mathbb{R}}(y) \succeq 0$ ; we show that  $\text{Ker } M^{\mathbb{R}}(y)$  is real radical. In view of Lemma 2.1, it suffices to show that if  $\sum_{i=1}^k p_i^2 \in \text{Ker } M^{\mathbb{R}}(y)$  for some  $p_i \in \mathbb{R}[x]$ , then  $p_i \in \text{Ker } M^{\mathbb{R}}(y)$ . Indeed,  $0 = \text{vec}(1)^T M^{\mathbb{R}}(y) \text{vec}(\sum_{i=1}^k p_i^2) = \sum_{i=1}^k \text{vec}(p_i)^T M^{\mathbb{R}}(y) \text{vec}(p_i)$  implies  $\text{vec}(p_i)^T M^{\mathbb{R}}(y) \text{vec}(p_i) = 0$  and thus  $p_i \in \text{Ker } M^{\mathbb{R}}(y)$  for all  $i$ .

Assume  $\text{rank } M^{\mathbb{R}}(y) = \text{rank } M_{t-1}^{\mathbb{R}}(y) =: r$  and set  $J := \langle \text{Ker } M_t^{\mathbb{R}}(y) \rangle$ . Obviously,  $J \subseteq \text{Ker } M^{\mathbb{R}}(y)$ ; we show equality. For this, let  $\mathcal{B} \subseteq \mathbb{T}_{n,t-1}$  index an  $r \times r$  nonsingular principal submatrix of  $M^{\mathbb{R}}(y)$ . We show that, for all  $\alpha \in \mathbb{N}^n$ ,  $x^\alpha \in \text{Span}_{\mathbb{R}}(\mathcal{B}) + J$ , using induction on  $|\alpha|$ . This holds for  $|\alpha| \leq t$  by the definition of  $\mathcal{B}$ . Assume  $|\alpha| \geq t + 1$  and write  $x^\alpha = x_i x^\delta$ . By the induction assumption,  $x^\delta = \sum_{x^\beta \in \mathcal{B}} c_\beta x^\beta + q$  where  $q \in J$ ,  $c_\beta \in \mathbb{R}$ . Thus,  $x^\alpha = \sum_{x^\beta \in \mathcal{B}} c_\beta x_i x^\beta + x_i q$ . Here,  $x_i q \in J$  and  $x_i x^\beta \in \text{Span}_{\mathbb{R}}(\mathcal{B}) + J$  since  $\deg(x_i x^\beta) \leq t$ , which implies  $x^\alpha \in \text{Span}_{\mathbb{R}}(\mathcal{B}) + J$ . Thus we have shown that  $\mathbb{R}[x] = \text{Span}_{\mathbb{R}}(\mathcal{B}) + J$ . As  $\text{Ker } M^{\mathbb{R}}(y) \cap \text{Span}_{\mathbb{R}}(\mathcal{B}) = \{0\}$ , this implies easily that  $\text{Ker } M^{\mathbb{R}}(y) = J$ .

For  $\mathcal{B} \subseteq \mathbb{T}_n$ , it is obvious that  $\mathcal{B}$  indexes a nonsingular submatrix of  $M^{\mathbb{R}}(y)$  if and only if  $\mathcal{B}$  is linearly independent in  $\mathbb{R}[x]/\text{Ker } M^{\mathbb{R}}(y)$ . The last statement of the lemma now follows since  $\dim \mathbb{R}[x]/\text{Ker } M^{\mathbb{R}}(y) = r$  (as  $\text{Ker } M^{\mathbb{R}}(y)$  is radical and using the identity  $|V_{\mathbb{C}}(\text{Ker } M^{\mathbb{R}}(y))| = \text{rank } M^{\mathbb{R}}(y)$  from Theorem 3.3).  $\square$

**Proposition 3.7**  *$\text{Ker } M^{2\mathbb{C}}(y)$  is an ideal in  $\mathbb{C}[x, \bar{x}]$ . If  $M^{2\mathbb{C}}(y) \succeq 0$ , then  $\text{Ker } M^{2\mathbb{C}}(y)$  is a radical ideal in  $\mathbb{C}[x, \bar{x}]$  and thus  $\text{Ker } M^{\mathbb{C}}(y)$  is a radical ideal in  $\mathbb{C}[x]$ . Assume, moreover,  $\text{rank } M^{\mathbb{C}}(y) = \text{rank } M_{t-1}^{\mathbb{C}}(y)$  for some integer  $t \geq 1$ . Then,  $\text{Ker } M^{\mathbb{C}}(y) = \langle \text{Ker } M_t^{\mathbb{C}}(y) \rangle$  and, for  $\mathcal{B} \subseteq \mathbb{T}_n$ ,  $\mathcal{B}$  indexes a (maximum) nonsingular principal submatrix of  $M^{\mathbb{C}}(y)$  if and only if  $\mathcal{B}$  is a (maximum) linearly independent subset of  $\mathbb{C}[x]/\text{Ker } M^{\mathbb{C}}(y)$ .*

*Proof* As in the real case, we use the following (easy to verify) identities: For  $h, p, q \in \mathbb{C}[x, \bar{x}]$ ,

$$\begin{aligned} \text{vec}(h)^* M^{2\mathbb{C}}(y) \text{vec}(pq) &= \text{vec}(h\bar{p})^* M^{2\mathbb{C}}(y) \text{vec}(q), \\ \text{vec}(p)^* M^{2\mathbb{C}}(y) \text{vec}(p) &= \text{vec}(1)^* M^{2\mathbb{C}}(y) \text{vec}(p\bar{p}), \\ \text{vec}(p^2)^* M^{2\mathbb{C}}(y) \text{vec}(p^2) &= \text{vec}(p\bar{p})^* M^{2\mathbb{C}}(y) \text{vec}(p\bar{p}), \end{aligned}$$

where  $\bar{p} \in \mathbb{C}[x, \bar{x}]$  is defined as  $\bar{p}(x, \bar{x}) := \overline{p(x, \bar{x})}$ . This implies directly that  $\text{Ker } M^{2\mathbb{C}}(y)$  is an ideal. Assume now  $M^{2\mathbb{C}}(y) \succeq 0$ ; we show that  $\text{Ker } M^{2\mathbb{C}}(y)$  is radical. In view of Lemma 2.1, this follows from the following fact:

$$\begin{aligned} p^2 \in \text{Ker } M^{2\mathbb{C}}(y) &\implies 0 = \text{vec}(p^2)^* M^{2\mathbb{C}}(y) \text{vec}(p^2) = \text{vec}(p\bar{p})^* M^{2\mathbb{C}}(y) \text{vec}(p\bar{p}) \\ &\implies p\bar{p} \in \text{Ker } M^{2\mathbb{C}}(y) \end{aligned}$$

$$\begin{aligned} \implies 0 &= \text{vec}(1)^* M^{2\mathbb{C}}(y) \text{vec}(p\bar{p}) = \text{vec}(p)^* M^{2\mathbb{C}}(y) \text{vec}(p) \\ \implies p &\in \text{Ker } M^{2\mathbb{C}}(y). \end{aligned}$$

The proof for the last statements of the proposition is identical to the proof of the corresponding statements in Proposition 3.6 for the real case.  $\square$

Without the assumption  $M^{2\mathbb{C}}(y) \succeq 0$ ,  $\text{Ker } M^{\mathbb{C}}(y)$  is not necessarily an ideal in  $\mathbb{C}[x]$ . Indeed, for the sequence  $y \in \mathbb{C}^{\mathbb{N}^{2n}}$  defined by  $y_{\alpha\alpha'} := 0$  if  $\alpha = 0$  or  $\alpha' = 0$ , and  $y_{\alpha\alpha'} := 1$  otherwise,  $M^{\mathbb{C}}(y) \succeq 0$ ,  $M^{2\mathbb{C}}(y) \not\succeq 0$  and  $\text{Ker } M^{\mathbb{C}}(y)$  is not an ideal (e.g.,  $1 \in \text{Ker } M^{\mathbb{C}}(y)$  while any nonconstant monomial does not lie in  $\text{Ker } M^{\mathbb{C}}(y)$ ). We mention for further reference the following corollary, and we conclude the section with the proof of Proposition 1.1 and a lemma about the ‘(real) radical’-like property of the kernel of a positive semidefinite truncated moment matrix.

**Corollary 3.8**

- (i) Let  $M_s^{\mathbb{R}}(y) \succeq 0$  and  $\text{rank } M_s^{\mathbb{R}}(y) = \text{rank } M_{s-1}^{\mathbb{R}}(y) =: r$ . Then,  $J := \langle \text{Ker } M_s^{\mathbb{R}}(y) \rangle$  is real radical and zero-dimensional,  $\dim \mathbb{R}[x]/J = r$ ,  $J \cap \mathbb{R}[x]_s = \text{Ker } M_s^{\mathbb{R}}(y)$  and, for  $\mathcal{B} \subseteq \mathbb{T}_{n,s}$ ,  $\mathcal{B}$  indexes a (maximum) nonsingular principal submatrix of  $M_s^{\mathbb{R}}(y) \Leftrightarrow \mathcal{B}$  is (maximum) linear independent in  $\mathbb{R}[x]/J$ .
- (ii) Let  $M_s^{2\mathbb{C}}(y) \succeq 0$  and  $\text{rank } M_s^{2\mathbb{C}}(y) = \text{rank } M_{s-1}^{\mathbb{C}}(y) =: r$ . Then,  $J := \langle \text{Ker } M_s^{\mathbb{C}}(y) \rangle$  is radical,  $\dim \mathbb{C}[x]/J = r$ ,  $J \cap \mathbb{C}[x]_s = \text{Ker } M_s^{\mathbb{C}}(y)$  and, for  $\mathcal{B} \subseteq \mathbb{T}_{n,s}$ ,  $\mathcal{B}$  indexes a (maximum) nonsingular principal submatrix of  $M_s^{\mathbb{C}}(y) \Leftrightarrow \mathcal{B}$  is (maximum) linearly independent in  $\mathbb{C}[x]/J$ .

*Proof* We prove only (i). By Theorem 3.4,  $y$  has an extension  $\tilde{y} \in \mathbb{R}^{\mathbb{N}^n}$  such that  $M^{\mathbb{R}}(\tilde{y})$  is a flat extension of  $M_s^{\mathbb{R}}(y)$ . By Proposition 3.6, the ideal  $\text{Ker } M^{\mathbb{R}}(\tilde{y}) = \langle \text{Ker } M_s^{\mathbb{R}}(y) \rangle =: J$  is real radical and zero-dimensional,  $\dim \mathbb{R}[x]/J = r$ , and  $J \cap \mathbb{R}[x]_s = \text{Ker } M^{\mathbb{R}}(\tilde{y}) \cap \mathbb{R}[x]_s = \text{Ker } M_s^{\mathbb{R}}(\tilde{y}) = \text{Ker } M_s^{\mathbb{R}}(y)$ .  $\square$

*Proof of Proposition 1.1.* By Proposition 3.6,  $J := \text{Ker } M^{\mathbb{R}}(y)$  is a real radical ideal, since  $M^{\mathbb{R}}(y) \succeq 0$ . As  $0 = M^{\mathbb{R}}(h_j y) = M^{\mathbb{R}}(y) \text{vec}(h_j)$  for all  $j$ , we have  $I \subseteq J$ , which implies that  $V_{\mathbb{R}}(J) \subseteq V_{\mathbb{R}}(I)$  is finite. As  $J$  is real radical, we deduce that  $V_{\mathbb{C}}(J) = V_{\mathbb{R}}(J) \subseteq \mathbb{R}^n$ . Hence  $J$  is zero-dimensional and  $I(V_{\mathbb{R}}(I)) \subseteq J$  since  $V_{\mathbb{C}}(J) \subseteq V_{\mathbb{R}}(I)$ . Set  $r := \dim \mathbb{R}[x]/J = |V_{\mathbb{C}}(J)| \leq |V_{\mathbb{R}}(I)|$ . Let  $\mathcal{B} \subseteq \mathbb{T}_n$  be a linear basis of  $\mathbb{R}[x]/J$ ,  $|\mathcal{B}| = r$ . Then the columns of  $M^{\mathbb{R}}(y)$  indexed by  $\mathcal{B}$  form a basis of the column space of  $M^{\mathbb{R}}(y)$  and thus  $\text{rank } M^{\mathbb{R}}(y) = r$ . Moreover,  $r = |V_{\mathbb{R}}(I)|$  if and only if  $V_{\mathbb{C}}(J) = V_{\mathbb{R}}(I)$  which in turn is equivalent to  $J = I(V_{\mathbb{R}}(I))$ . Now, this maximum rank  $|V_{\mathbb{R}}(I)|$  is reached by the sequence  $y := y^\mu = \sum_{v \in V_{\mathbb{R}}(I)} \lambda_v \zeta_v$  with  $\lambda_v > 0$  which indeed satisfies (1.1).  $\square$

Finally, it is useful to observe that the kernel of a positive semidefinite truncated moment matrix enjoys the following ‘(real) radical’-like property. We omit the proof whose details are straightforward.

**Lemma 3.9**

- (i) Assume  $M_t^{\mathbb{R}}(y) \succeq 0$  and let  $p, q_j \in \mathbb{R}[x]$ ,  $f := p^{2m} + \sum_j q_j^2$  with  $m \in \mathbb{N}$ ,  $m \geq 1$ . Then,  $f \in \text{Ker } M_t^{\mathbb{R}}(y) \Rightarrow p \in \text{Ker } M_t^{\mathbb{R}}(y)$ .
- (ii) Assume  $M_t^{2\mathbb{C}}(y) \succeq 0$  and let  $p \in \mathbb{C}[x]$ ,  $m \in \mathbb{N}$ ,  $m \geq 1$ . Then,  $p^m \in \text{Ker } M_t^{2\mathbb{C}}(y) \Rightarrow p \in \text{Ker } M_t^{2\mathbb{C}}(y)$ .

#### 4 A Semidefinite Characterization of the (Real) Radical Ideal via Moment Matrices

In this section we present a semidefinite characterization of the real radical ideal  $I(V_{\mathbb{R}}(I))$  of an ideal  $I \subseteq \mathbb{R}[x]$ , as well as a numerical algorithm for computing a set of generators. It turns out that the method also applies to the radical ideal  $I(V_{\mathbb{C}}(I))$ . Our strategy is to obtain  $I(V_{\mathbb{K}}(I))$  ( $\mathbb{K} = \mathbb{R}$  or  $\mathbb{C}$ ) as the ideal generated by the kernel of some suitable moment matrix  $M_t^{\mathbb{K}}(y)$  where  $y \in K_t^{\mathbb{K}}$ . Sections 4.1–4.3 contain some results ensuring that the moment matrix  $M_t^{\mathbb{K}}(y)$  has the desirable properties for achieving this task and Sect. 4.4 describes our algorithm.

##### 4.1 Weakest Set of Conditions

Throughout,  $I = \langle h_1, \dots, h_m \rangle$  is an ideal in  $\mathbb{K}[x]$  for which we want to find the radical ideal  $I(V_{\mathbb{K}}(I))$ ,  $\mathbb{K} = \mathbb{R}$  or  $\mathbb{C}$ . Recall the definition of  $d$  in (1.2).

**Proposition 4.1** *Let  $t \geq d$ ,  $1 \leq s \leq t$ ,  $y \in K_t^{\mathbb{K}}$  for which  $\text{rank } M_t^{\mathbb{K}}(y)$  is maximum, and  $\mathcal{B} \subseteq \mathbb{T}_{n,s-1}$  index a maximum nonsingular principal submatrix of  $M_{s-1}^{\mathbb{K}}(y)$  with border  $\partial\mathcal{B}$  defined as in (2.3). Assume (i)–(iii) below hold:*

- (i)  $\mathcal{B}$  is an order ideal.
- (ii) The principal submatrix of  $M_s^{\mathbb{K}}(y)$  indexed by  $\mathcal{B} \cup \partial\mathcal{B}$  has the same rank as  $M_{s-1}^{\mathbb{K}}(y)$ ; that is, with  $\mathcal{B} := \{b_1, \dots, b_N\}$  and  $\partial\mathcal{B} := \{c_1, \dots, c_H\}$ , there exists a polynomial  $g_j \in \text{Ker } M_s^{\mathbb{K}}(y)$  of the form  $g_j(x) = c_j - \sum_{i=1}^N a_{ij}b_i$  (i.e.,  $G := \{g_1, \dots, g_H\}$  is a  $\mathcal{B}$ -border prebasis).
- (iii) The formal multiplication matrices  $\mathcal{X}_1, \dots, \mathcal{X}_n$  defined from  $G$  commute pairwise.

Then  $G$  is a border basis of  $J := \langle G \rangle \subseteq I(V_{\mathbb{K}}(I))$ ,  $\mathcal{B}$  is a linear basis of  $\mathbb{K}[x]/J$ , and one can extract (using the formal multiplication matrices) the set  $W := V_{\mathbb{C}}(J)$  which satisfies  $V_{\mathbb{K}}(I) \subseteq W$  and  $|W| \leq \text{rank } M_{s-1}^{\mathbb{K}}(y)$ . Moreover, if  $|V_{\mathbb{K}}(I)| = |W| = \text{rank } M_{s-1}^{\mathbb{K}}(y)$ , then  $V_{\mathbb{K}}(I) = W$ ,  $I(V_{\mathbb{K}}(I)) = J$ , and  $G$  is a  $\mathcal{B}$ -border basis of  $I(V_{\mathbb{K}}(I))$ .

*Proof* Theorem 2.8 gives directly that  $G$  is a border basis of the ideal  $J = \langle G \rangle$  and that  $\mathcal{B}$  is a linear basis of  $\mathbb{R}[x]/J$ . Moreover, the matrices  $\mathcal{X}_1, \dots, \mathcal{X}_n$  coincide with the multiplication matrices in  $\mathbb{R}[x]/J$  w.r.t. the basis  $\mathcal{B}$ . Thus one can compute the set  $W = V_{\mathbb{C}}(J)$  from their eigenvectors. By construction,  $J \subseteq \langle \text{Ker } M_s^{\mathbb{K}}(y) \rangle \subseteq \langle \text{Ker } M_t^{\mathbb{K}}(y) \rangle \subseteq I(V_{\mathbb{K}}(I))$ , where the last inclusion follows from Lemmas 3.1 and

3.2(i). This implies  $V_{\mathbb{K}}(I) \subseteq V_{\mathbb{C}}(J) = W$ . Moreover,  $|W| \leq \dim \mathbb{K}[x]/J = |\mathcal{B}| = \text{rank } M_{s-1}^{\mathbb{K}}(y)$ .

If  $|V_{\mathbb{K}}(I)| = |W| = \text{rank } M_{s-1}^{\mathbb{K}}(y)$ , then  $W = V_{\mathbb{K}}(I)$  and  $J$  is radical since  $\dim \mathbb{K}[x]/J = |V_{\mathbb{C}}(J)|$ , which implies  $I(V_{\mathbb{K}}(I)) = I(W) = I(V_{\mathbb{C}}(J)) = J$ .  $\square$

In the next two subsections we give simple rank conditions (4.1), (4.5), which ensure that the conditions of Proposition 4.1 hold. (See Remark 4.13 for details.) For the sake of clarity, we treat the real and complex cases separately.

#### 4.2 Characterizing and Computing the Real Radical $I(V_{\mathbb{R}}(I))$

Assume  $I = \langle h_1, \dots, h_m \rangle$  is an ideal in  $\mathbb{R}[x]$ , with  $h_1, \dots, h_m \in \mathbb{R}[x]$ .

**Proposition 4.2** *Let  $t \geq d$  and  $y \in K_t^{\mathbb{R}}$  for which  $\text{rank } M_t^{\mathbb{R}}(y)$  is maximum. If, for some  $1 \leq s \leq t$ ,*

$$\text{rank } M_s^{\mathbb{R}}(y) = \text{rank } M_{s-1}^{\mathbb{R}}(y) =: r, \tag{4.1}$$

*then  $I(V_{\mathbb{R}}(I)) \supseteq \langle \text{Ker } M_s^{\mathbb{R}}(y) \rangle =: J$ . One can compute the set  $W := V_{\mathbb{C}}(J)$  which satisfies  $V_{\mathbb{R}}(I) \subseteq W$  and  $|W| = r$ . Moreover, if  $V_{\mathbb{R}}(I) = W$ , then  $I(V_{\mathbb{R}}(I)) = J$ .*

*Proof* By Lemma 3.1,  $\text{Ker } M_s^{\mathbb{R}}(y) \subseteq \text{Ker } M_t^{\mathbb{R}}(y) \subseteq I(V_{\mathbb{R}}(I))$ , implying  $J \subseteq I(V_{\mathbb{R}}(I))$  and thus  $V_{\mathbb{R}}(I) \subseteq W$ . By Corollary 3.8(i), as  $J$  is radical,  $|W| = \dim \mathbb{R}[x]/J = r$ , and  $V_{\mathbb{R}}(I) = W$  implies  $I(V_{\mathbb{R}}(I)) = I(W) = J$ .  $\square$

One can verify (using Lemma 3.5) that, if (4.1) holds for some  $s \leq t - 2$ , then it also holds for  $s = t - 1$ . Hence it suffices to check whether (4.1) holds for  $s = t - 1$  or  $t$ . In Lemma 4.3 below, we observe that, if assumption (ii) in Proposition 4.1 holds for  $s \leq t - 1$ , then in fact (4.1) holds and thus Proposition 4.2 applies. However, it may be that Proposition 4.1 applies to the case  $s = t$  while (4.1) does not hold; see Example 5.3 (for relaxation order  $t = 2$ ) for such an instance. In Remark 4.13 below we see that the converse of the next lemma holds.

**Lemma 4.3** *In Proposition 4.1, if assumption (ii) holds for  $s \leq t - 1$  then  $\text{rank } M_{s-1}^{\mathbb{K}}(y) = \text{rank } M_s^{\mathbb{K}}(y)$ .*

*Proof* We have to show that  $\mathbb{T}_{n,s} \subseteq \text{Span}_{\mathbb{K}}(\mathcal{B}) + \text{Ker } M_s(y)$ . By the definition of  $\mathcal{B}$ , any  $x^\alpha \in \mathbb{T}_{n,s-1}$  lies in  $\text{Span}_{\mathbb{K}}(\mathcal{B}) + \text{Ker } M_{s-1}(y)$ . For  $x^\alpha \in \mathbb{T}_{n,s}$ , write  $x^\alpha = x_1 x^\delta$  where  $x^\delta \in \mathbb{T}_{n,s-1}$ . Thus  $x^\delta = \sum_{x^\beta \in \mathcal{B}} c_\beta x^\beta + p$  where  $p \in \text{Ker } M_{s-1}^{\mathbb{K}}(y)$ ,  $c_\beta \in \mathbb{K}$ . Therefore,  $x^\alpha = \sum_{x^\beta \in \mathcal{B}} c_\beta x_1 x^\beta + x_1 p$ . As  $x_1 x^\beta \in \mathcal{B} \cup \partial \mathcal{B}$ , assumption (ii) implies that  $x_1 x^\beta \in \text{Span}_{\mathbb{K}}(\mathcal{B}) + \text{Ker } M_s^{\mathbb{K}}(y)$ . As  $\deg(x_1 p) \leq s \leq t - 1$ , it follows from Lemma 3.5 that  $x_1 p \in \text{Ker } M_s^{\mathbb{K}}(y)$ . Therefore,  $x^\alpha \in \text{Span}_{\mathbb{K}}(\mathcal{B}) + \text{Ker } M_s(y)$ .  $\square$

By strengthening the rank condition (4.1), one can show that  $J = I(V_{\mathbb{R}}(I))$ , i.e., the desired real radical ideal is found.

**Proposition 4.4** *Let  $t \geq d$  and  $y \in K_t^{\mathbb{R}}$  for which  $\text{rank } M_t^{\mathbb{R}}(y)$  is maximum. Assume that, either (4.1) holds for some  $2d \leq s \leq t$ , or*

$$\text{rank } M_s^{\mathbb{R}}(y) = \text{rank } M_{s-d}^{\mathbb{R}}(y) \tag{4.2}$$

for some  $d \leq s \leq t$ . Then  $I(V_{\mathbb{R}}(I)) = \langle \text{Ker } M_s^{\mathbb{R}}(y) \rangle$  (and one can find  $V_{\mathbb{R}}(I)$ ). Moreover,  $\text{rank } M_s^{\mathbb{R}}(y) = |V_{\mathbb{R}}(I)|$ .

*Proof* In view of Proposition 4.2, there remains only to show the inclusion  $I(V_{\mathbb{R}}(I)) \subseteq J := \langle \text{Ker } M_s^{\mathbb{R}}(y) \rangle$  or, equivalently (since  $J$  is radical),  $W := V_{\mathbb{C}}(J) \subseteq V_{\mathbb{R}}(I)$ . We already know that  $W \subseteq \mathbb{R}^n$  since  $J$  is real radical and zero-dimensional (see Corollary 3.8). We now show that  $W \subseteq V_{\mathbb{C}}(I)$ . Assume first that (4.1) holds for  $s \geq 2d$ . As  $M_{t-d_j}^{\mathbb{R}}(h_j y) = 0$ , we have  $(h_j y)_{\alpha} = 0$  for all  $|\alpha| \leq 2t - 2d_j$  and thus for all  $|\alpha| \leq 2d_j$ . Hence,  $M_{2d_j}^{\mathbb{R}}(y) \text{vec}(h_j) = 0$  and thus  $h_j \in \text{Ker } M_s^{\mathbb{R}}(y)$ . Therefore,  $I \subseteq J$ , giving  $W \subseteq V_{\mathbb{C}}(I)$ .

Assume now that (4.2) holds for some  $d \leq s \leq t$ . Let  $p_v$  ( $v \in W$ ) be interpolation polynomials, i.e.,  $p_v(w) = \delta_{v,w}$  for  $v, w \in W$ . As observed in [29, Lemma 27], one can assume that  $\deg(p_v) \leq s - d$ . (Indeed, let  $\mathcal{B} \subseteq \mathbb{T}_{n,s-d}$  index a maximum nonsingular submatrix of  $M_s^{\mathbb{R}}(y)$ ; then  $\mathcal{B}$  is a basis of  $\mathbb{R}[x]/J$  by Corollary 3.8 and one can replace  $p_v$  by its residue modulo  $J$  w.r.t.  $\mathcal{B}$ .) From Theorems 3.3 and 3.4, we know that  $(y_{\alpha})_{\alpha \in \mathbb{T}_{n,2s}} = \sum_{v \in W} \lambda_v \zeta_{2s,v}$  where  $\lambda_v > 0$ . Hence,  $0 = \text{vec}(p_v)^{\top} M_{s-d_j}^{\mathbb{R}}(h_j y) \text{vec}(p_v) = h_j(v) \lambda_v$  implies  $h_j(v) = 0$  for all  $j$  and thus  $v \in V_{\mathbb{C}}(I)$ , which shows  $W \subseteq V_{\mathbb{C}}(I)$ .  $\square$

We now formulate an analogous result for the ideal  $I(V_{\mathbb{R}}(I) \cap S)$ , where  $S := \{x \in \mathbb{R}^n \mid h_{m+1}(x) \geq 0, \dots, h_{m+k}(x) \geq 0\}$  is a semialgebraic set, with  $h_{m+1}, \dots, h_{m+k} \in \mathbb{R}[x]$ . For this define the set

$$K_{t,S}^{\mathbb{R}} := K_t^{\mathbb{R}} \cap \{y \mid M_{t-d_j}(h_j y) \geq 0 \ (j = m+1, \dots, m+k)\} \quad (4.3)$$

for  $t \geq d := \max_{j=1, \dots, m+k} d_j$ .

**Proposition 4.5** *Let  $t \geq d$  and  $y \in K_{t,S}^{\mathbb{R}}$  for which  $\text{rank } M_t^{\mathbb{R}}(y)$  is maximum.*

- (i) *Assume (4.1) holds for some  $1 \leq s \leq t$ . Then  $J := \langle \text{Ker } M_s^{\mathbb{R}}(y) \rangle \subseteq I(V_{\mathbb{R}}(I) \cap S)$  and  $W := V_{\mathbb{C}}(J) \supseteq V_{\mathbb{R}}(I) \cap S$  with  $|W| = \text{rank } M_s^{\mathbb{R}}(y)$ ; moreover,  $J = I(V_{\mathbb{R}}(I) \cap S)$  if  $W = V_{\mathbb{R}}(I) \cap S$ .*
- (ii) *Assume (4.2) holds for some  $d \leq s \leq t$ . Then  $I(V_{\mathbb{R}}(I) \cap S) = \langle \text{Ker } M_s^{\mathbb{R}}(y) \rangle$ .*

*Proof* (i) The inclusion  $\text{Ker } M_t^{\mathbb{R}}(y) \subseteq I(V_{\mathbb{R}}(I) \cap S)$  follows from the maximality of the rank of  $M_t^{\mathbb{R}}(y)$  and the fact that  $\zeta_{2t,v} \in K_{t,S}^{\mathbb{R}}$  for all  $v \in V_{\mathbb{R}}(I) \cap S$ . This gives  $J \subseteq I(V_{\mathbb{R}}(I) \cap S)$  and thus  $W \supseteq V_{\mathbb{R}}(I) \cap S$ . Equality  $W = V_{\mathbb{R}}(I) \cap S$  implies  $I(V_{\mathbb{R}}(I) \cap S) = I(W) = J$  (as  $J$  radical). This concludes the proof of (i). The proof for (ii) is analogous to that of the corresponding statement in Proposition 4.4.  $\square$

To conclude we show that, when  $V_{\mathbb{R}}(I)$  is finite, then condition (4.2) is satisfied for  $t$  large enough. That is, the conclusion of Propositions 4.4 and 4.5 holds: the real radical ideal  $I(V_{\mathbb{R}}(I))$  or  $I(V_{\mathbb{R}}(I) \cap S) = \langle \text{Ker } M_s^{\mathbb{R}}(y) \rangle$  is found.

**Proposition 4.6** *Assume  $|V_{\mathbb{R}}(I)| < \infty$ .*

- (i) *If  $V_{\mathbb{R}}(I) = \emptyset$ , then  $K_{t,S}^{\mathbb{R}} = \emptyset$  for  $t$  large enough.*

(ii) If  $V_{\mathbb{R}}(I) \neq \emptyset$ , then, for  $t$  large enough, there exists  $d \leq s \leq t$  such that  $\text{rank } M_s^{\mathbb{R}}(y) = \text{rank } M_{s-d}^{\mathbb{R}}(y)$  for all  $y \in K_{t,S}^{\mathbb{R}}$ .

*Proof* Assume  $t \geq 2d$  and let  $y \in K_{t,S}^{\mathbb{R}}$ . Then, as observed in the proof of Proposition 4.4,  $h_1, \dots, h_m \in \text{Ker } M_t^{\mathbb{R}}(y)$ . We first show that, for  $t$  large enough,  $\text{Ker } M_t^{\mathbb{R}}(y)$  also contains a given basis of the ideal  $I(V_{\mathbb{R}}(I))$ .

**Claim 4.7** *Let  $\{g_1, \dots, g_k\}$  be a basis of the ideal  $I(V_{\mathbb{R}}(I))$ . There exists  $t_0 \in \mathbb{N}$  such that  $g_1, \dots, g_k \in \text{Ker } M_t^{\mathbb{R}}(y)$  for all  $t \geq t_0$ .*

*Proof* Let  $l \in \{1, \dots, k\}$ . By the Real Nullstellensatz, there exist  $m_l \in \mathbb{N}$ ,  $m_l \geq 1$ , and polynomials  $\sigma_l, u_j^{(l)}$  ( $j \leq m$ ) for which  $g_l^{2m_l} + \sigma_l = \sum_{j=1}^m u_j^{(l)} h_j$  and  $\sigma_l$  is a sum of squares. Set  $t_0 := 1 + \max_{l \leq k, j \leq m} (2d, \deg(g_l^{2m_l}), \deg(\sigma_l), \deg(u_j^{(l)} h_j))$  and let  $t \geq t_0$ . As  $\deg(u_j^{(l)} h_j) \leq t - 1$  and  $h_j \in \text{Ker } M_t^{\mathbb{R}}(y)$ , then  $u_j^{(l)} h_j \in \text{Ker } M_t^{\mathbb{R}}(y)$  by Lemma 3.5. Hence,  $g_l^{2m_l} + \sigma_l \in \text{Ker } M_t^{\mathbb{R}}(y)$  which, using Lemma 3.9(i), implies  $g_l \in \text{Ker } M_t^{\mathbb{R}}(y)$ .  $\square$

If  $V_{\mathbb{R}}(I) = \emptyset$ , then  $\{1\}$  is a basis of  $I(V_{\mathbb{R}}(I)) = \mathbb{R}[x]$ . Hence  $1 \in \text{Ker } M_t^{\mathbb{R}}(y)$ , implying  $y_0 = 0$ , which contradicts the fact that  $y_0 = 1$  for  $y \in K_{t,S}^{\mathbb{R}}$ . Therefore,  $K_{t,S}^{\mathbb{R}} = \emptyset$  for  $t \geq t_0$ , which shows (i).

Assume now  $V_{\mathbb{R}}(I) \neq \emptyset$ . Let  $\{g_1, \dots, g_k\}$  be a Gröbner basis of  $I(V_{\mathbb{R}}(I))$  for a graded monomial ordering and let  $\mathcal{B}$  be the corresponding set of standard monomials. Thus  $\mathcal{B}$  is a basis of  $\mathbb{R}[x]/I(V_{\mathbb{R}}(I))$ ; set  $d_{\mathcal{B}} := \max_{b \in \mathcal{B}} \deg(b)$  (which is well defined as  $\mathcal{B} \neq \emptyset$ ). We can write any monomial as  $x^\alpha = r^{(\alpha)} + \sum_{l=1}^k p_l^{(\alpha)} g_l$ , where  $r^{(\alpha)} \in \text{Span}_{\mathbb{R}}(\mathcal{B})$ ,  $p_l^{(\alpha)} \in \mathbb{R}[x]$  and  $\deg(p_l^{(\alpha)} g_l) \leq \deg(x^\alpha)$ . Set  $t_1 := \max(d_{\mathcal{B}} + d, t_0)$  and let  $t \geq t_1 + 1$ . Consider  $\alpha \in \mathbb{T}_{n,t_1}$ . As  $\deg(p_l^{(\alpha)} g_l) \leq t_1 \leq t - 1$  and  $g_l \in \text{Ker } M_t^{\mathbb{R}}(y)$ , we have  $p_l^{(\alpha)} g_l \in \text{Ker } M_t^{\mathbb{R}}(y)$  and thus  $x^\alpha - r^{(\alpha)} \in \text{Ker } M_t^{\mathbb{R}}(y)$ . As  $\deg(r^{(\alpha)}) \leq d_{\mathcal{B}} \leq t_1 - d$ , this shows that the  $\alpha$ th column of  $M_t^{\mathbb{R}}(y)$  is a linear combination of columns indexed by  $\mathbb{T}_{n,t_1-d}$ . Therefore,  $\text{rank } M_t^{\mathbb{R}}(y) = \text{rank } M_{t_1-d}^{\mathbb{R}}(y)$ , thus proving (ii).  $\square$

**Remark 4.8** (Detecting Existence of Real Solutions) Hence one can detect the existence of real solutions via the following criterion:

$$V_{\mathbb{R}}(I) = \emptyset \iff K_t^{\mathbb{R}} = \emptyset \quad \text{for some } t. \tag{4.4}$$

(The ‘only if’ part follows directly from Proposition 4.6(i), while the ‘if part’ follows from the fact that  $\zeta_{2t,v} \in K_t^{\mathbb{R}}$  for any  $v \in V_{\mathbb{R}}(I)$ .) Note, moreover, that, when  $V_{\mathbb{R}}(I) = \emptyset$ , none of the flat conditions (4.2), or (4.1) with  $s \geq 2d$ , can hold; indeed, under either of these two conditions, one would have  $|V_{\mathbb{R}}(I)| = \text{rank } M_s^{\mathbb{R}}(y) \geq 1$  by Proposition 4.4. Consider as an illustration the following small example:  $I = \langle h := x_1^2 + 1 \rangle \subseteq \mathbb{R}[x_1]$  with  $V_{\mathbb{R}}(I) = \emptyset$ . For  $t \geq 1$ , if  $y \in K_t$ , then  $M_1(y) \geq 0$  implies  $y_{2e_1} \geq 0$ , while  $(hy)_0 = 0$  gives  $y_{2e_1} + 1 = 0$ , yielding a contradiction. Hence,  $K_t = \emptyset$  for any  $t \geq 1$ .

*Remark 4.9* Proposition 4.6 remains valid under the weaker assumption  $|V_{\mathbb{R}}(I) \cap S| < \infty$  if, in the definition of the set  $K_{t,S}^{\mathbb{R}}$  in (4.3), we add the constraints  $M_{t-d_e}(p_e y) \geq 0$  for  $e \in \{0, 1\}^k$ , after setting  $p_e := \prod_{i=1}^k h_{m+i}^{e_i}$ . The proof is analogous, except we now prove in Claim 4.7 that  $\text{Ker } M_t^{\mathbb{R}}(y)$  contains a given basis of the ideal  $I(V_{\mathbb{R}}(I) \cap S)$ . To show this, instead of the Real Nullstellensatz, we now use the Positivstellensatz (see Stengle [38]) which in our case can be formulated in the following way: For  $g \in \mathbb{R}[x]$ ,  $g \in I(V_{\mathbb{R}}(I) \cap S)$  if and only if  $-g^{2r} = \sum_{j=1}^m u_j h_j + \sum_{e \in \{0,1\}^k} \sigma_e p_e$  for some  $r \in \mathbb{N} \setminus \{0\}$ ,  $u_j, \sigma_e \in \mathbb{R}[x]$ , with  $\sigma_e$  s.o.s.

### 4.3 Characterizing and Computing the Radical $I(V_{\mathbb{C}}(I))$

Using complex moment matrices, we can formulate analogues of Propositions 4.2, 4.4, and 4.6 for the radical ideal  $I(V_{\mathbb{C}}(I))$ ; the proofs of the first two results being similar are omitted.

**Proposition 4.10** *Let  $t \geq d$  and  $y \in K_t^{2\mathbb{C}}$  for which  $\text{rank } M_t^{2\mathbb{C}}(y)$  is maximum. If, for some integer  $1 \leq s \leq t$ ,*

$$\text{rank } M_s^{2\mathbb{C}}(y) = \text{rank } M_{s-1}^{\mathbb{C}}(y) =: r, \quad (4.5)$$

*then  $I(V_{\mathbb{C}}(I)) \supseteq \langle \text{Ker } M_s^{\mathbb{C}}(y) \rangle =: J$ . One can compute the set  $W := V_{\mathbb{C}}(J) \supseteq V_{\mathbb{C}}(I)$  which satisfies  $V_{\mathbb{C}}(I) \subseteq W$  and  $|W| = r$ . Moreover, if  $W = V_{\mathbb{C}}(I)$  then  $I(V_{\mathbb{C}}(I)) = J$ .*

**Proposition 4.11** *Let  $t \geq d$  and  $y \in K_t^{2\mathbb{C}}$  for which  $\text{rank } M_t^{2\mathbb{C}}(y)$  is maximum. Assume that, either (4.5) holds for some  $2d \leq s \leq t$ , or*

$$\text{rank } M_s^{2\mathbb{C}}(y) = \text{rank } M_{s-d}^{\mathbb{C}}(y) \quad (4.6)$$

*for some  $d \leq s \leq t$ . Then  $I(V_{\mathbb{C}}(I)) = \langle \text{Ker } M_s^{\mathbb{C}}(y) \rangle$  (and one can find  $V_{\mathbb{C}}(I)$ ).*

**Proposition 4.12** *Assume  $|V_{\mathbb{C}}(I)| < \infty$ .*

- (i) *If  $V_{\mathbb{C}}(I) = \emptyset$ , then  $K_t^{2\mathbb{C}} = \emptyset$  for  $t$  large enough.*
- (ii) *If  $V_{\mathbb{C}}(I) \neq \emptyset$ , then, for  $t$  large enough, there exists  $d \leq s \leq t$  such that  $\text{rank } M_s^{2\mathbb{C}}(y) = \text{rank } M_{s-d}^{\mathbb{C}}(y)$  for all  $y \in K_t^{2\mathbb{C}}$ .*

*Proof* Let  $t \geq 2d$  and  $y \in K_t^{2\mathbb{C}}$ . Then,  $h_1, \dots, h_m \in \text{Ker } M_t^{\mathbb{C}}(y)$ , since  $(M_t^{\mathbb{C}}(y)h_j)_{\alpha'} = (h_j y)_{0\alpha'} = 0$  for  $|\alpha'| \leq t \leq 2t - 2d_j$  by the assumption  $M_{t-d_j}^{2\mathbb{C}}(h_j y) = 0$ . Hence,  $h_j \in \text{Ker } M_t^{2\mathbb{C}}(y)$  and thus  $\overline{h_j} \in \text{Ker } M_t^{2\mathbb{C}}(y)$  too.

Let  $\{g_1, \dots, g_k\}$  be a Gröbner basis of  $I(V_{\mathbb{C}}(I))$  for a graded monomial ordering. Analogously to Claim 4.7, one can show, using Hilbert's Nullstellensatz, the existence of  $t_0 \in \mathbb{N}$  for which  $g_l \in \text{Ker } M_t^{2\mathbb{C}}(y)$  for all  $l$  and  $t \geq t_0$ . If  $V_{\mathbb{C}}(I) = \emptyset$ , then  $1 \in \text{Ker } M_t^{2\mathbb{C}}(y)$  which implies  $y_0 = 0$ , thus showing  $K_t^{2\mathbb{C}} = \emptyset$ . Assume now that  $V_{\mathbb{C}}(I) \neq \emptyset$ . Let  $\mathcal{B}$  be the basis of  $\mathbb{C}[x]/I(V_{\mathbb{C}}(I))$  for the chosen monomial ordering



and set  $d_{\mathcal{B}} := \max_{b \in \mathcal{B}} \deg(b)$  (which is well defined as  $\mathcal{B} \neq \emptyset$ ) and  $\mathcal{C} := \{\bar{b}b' \mid b, b' \in \mathcal{B}\}$ . Then any monomial  $\bar{x}^{\alpha}x^{\alpha'}$  can be written  $\bar{x}^{\alpha}x^{\alpha'} = r^{(\alpha\alpha')} + \sum_{l,l'=1}^k u_{ll'}^{(\alpha\alpha')} \bar{g}_l g_{l'}$  where  $u_{ll'}^{(\alpha\alpha')} \in \mathbb{C}[x, \bar{x}]$ ,  $r^{(\alpha\alpha')} \in \text{Span}_{\mathbb{C}}(\mathcal{C})$ , and  $\deg(u_{ll'}^{(\alpha\alpha')} \bar{g}_l g_{l'}) \leq |\alpha| + |\alpha'|$ . Let  $t_1 := \max(3d, d + 2d_{\mathcal{B}})$  and  $t \geq t_1 + 1$ . Then  $\bar{x}^{\alpha}x^{\alpha'} - r^{(\alpha\alpha')} \in \text{Ker } M_t^{2\mathbb{C}}(y)$  whenever  $|\alpha + \alpha'| \leq t_1$  which, together with  $\deg(r^{(\alpha\alpha')}) \leq 2d_{\mathcal{B}} \leq t_1 - d$ , shows that  $\text{rank } M_{t_1}^{2\mathbb{C}}(y) = \text{rank } M_{t_1-d}^{2\mathbb{C}}(y) =: r$ .

There remains to show that  $\text{rank } M_{t_1-d}^{\mathbb{C}}(y) = r$ . Applying Theorems 3.3 and 3.4, there exists  $W \subseteq \mathbb{C}^n$ ,  $|W| = r$ ,  $\lambda_v > 0$  ( $v \in W$ ) such that, if we set  $\tilde{y} := \sum_{v \in W} \lambda_v \zeta_{\bar{v}} \otimes \zeta_v$ , then  $M^{2\mathbb{C}}(\tilde{y})$  is a flat extension of  $M_{t_1}^{2\mathbb{C}}(y)$ . This implies  $M_{t_1-d}^{\mathbb{C}}(y) = \sum_{v \in W} \lambda_v \zeta_{t_1-d, \bar{v}} \zeta_{t_1-d, v}^{\top}$ . As  $h_j \in \text{Ker } M_{t_1-d}^{\mathbb{C}}(y)$  (since  $t_1 - d \geq \deg(h_j)$  as  $t_1 \geq 3d$ ), we deduce that  $h_j(v) = 0$  for all  $v \in W$  and thus  $W \subseteq V_{\mathbb{C}}(I)$ . We now show that the vectors  $\zeta_{t_1-d, v}$  ( $v \in W$ ) are linearly independent, which implies that  $\text{rank } M_{t_1-d}^{\mathbb{C}}(y) = |W| = r$ , thus concluding the proof. For this, consider interpolation polynomials  $p_v \in \mathbb{C}[x]$  ( $v \in W$ ), i.e., satisfying  $p_v(w) = \delta_{v,w}$  for  $v, w \in W$ . One may assume that  $\deg(p_v) \leq d_{\mathcal{B}}$  (replacing if necessary  $p_v$  by its residue modulo  $I(V_{\mathbb{C}}(I))$  with respect to the basis  $\mathcal{B}$ ). Assume  $\sum_{v \in W} c_v \zeta_{t_1-d, v} = 0$  for some  $c_v \in \mathbb{C}$ ; we show that all  $c_v$ 's are zero. As  $t_1 - d \geq d_{\mathcal{B}}$ , we can take the scalar product with  $\text{vec}(p_w)$  ( $w \in W$ ) which yields  $0 = \sum_{v \in W} c_v p_w(v) = c_w$ .  $\square$

*Remark 4.13* Under condition (4.1) or (4.5), the assumptions (i)–(iii) of Proposition 4.1 hold. Namely, one can construct an order ideal  $\mathcal{B} \subseteq \mathbb{T}_{n,s-1}$  indexing a maximum nonsingular principal submatrix of  $M_{s-1}^{\mathbb{K}}(y)$ . Moreover, one can choose  $\mathcal{B} = \mathcal{B}_{>}$ , the set of standard monomials for the ideal  $J := \langle \text{Ker } M_s^{\mathbb{K}}(y) \rangle$  with respect to a graded lexicographic order; this is possible since  $J$  is zero-dimensional and there is a basis in  $\mathbb{T}_{n,s-1}$  for  $\mathbb{K}[x]/J$ , which implies  $\mathcal{B}_{>} \subseteq \mathbb{T}_{n,s-1}$  by Lemma 2.5. Such a basis  $\mathcal{B}_{>}$  can be found using the greedy sieve algorithm described in Section 2.4. The execution of the algorithm requires checking whether some set  $T \subseteq \mathbb{T}_{n,s-1}$  is linearly independent in  $\mathbb{K}[x]/J$ . Using Corollary 3.8, this can be checked by testing whether  $T$  indexes a nonsingular principal submatrix of  $M_t^{\mathbb{K}}(y)$ , thus by a rank computation on  $M_t^{\mathbb{K}}(y)$ . Finally, the formal multiplication matrices as defined in Proposition 4.1 coincide with the (usual) multiplication matrices in  $\mathbb{K}[x]/J$  and thus they commute pairwise.

Therefore, the conclusion of Proposition 4.1 also applies under (4.1) or (4.5): If  $W = V_{\mathbb{K}}(I)$ , then one can construct a border basis of  $J = I(V_{\mathbb{K}}(I))$ . Moreover, when using  $\mathcal{B}_{>}$ , one can also construct the reduced Gröbner basis of  $J$  for the graded lexicographic monomial ordering. A sufficient condition for  $W = V_{\mathbb{K}}(I)$  is given above in Proposition 4.4 ( $\mathbb{K} = \mathbb{R}$ ) and Proposition 4.11 ( $\mathbb{K} = \mathbb{C}$ ).

In fact, as will be explained in Sect. 4.4.5, we can adapt this strategy to find a Gröbner basis for an arbitrary monomial ordering.

*Remark 4.14* The above results involve the matrix  $M_t^{2\mathbb{C}}(y)$  where the argument  $y \in \mathbb{C}^{\mathbb{N}^{2n}}$  is a complex sequence satisfying (3.1). As explained in Sect. 3.2 above, one may work instead with the moment matrix  $M^{\mathbb{R}}(a)$ , where  $a \in \mathbb{R}^{\mathbb{N}^{2n}}$  is the real sequence defined as in (3.4), and Propositions 4.10 and 4.11 could be reformulated in terms of real sequences only.

In fact, when the ideal  $I$  is generated by real polynomials  $h_1, \dots, h_m$ , its set  $V_{\mathbb{C}}(I)$  of complex roots is closed under complex conjugations, i.e.,  $v \in V_{\mathbb{C}}(I) \Leftrightarrow \bar{v} \in V_{\mathbb{C}}(I)$  and, for a polynomial  $f \in \mathbb{C}[x]$ ,  $f \in I(V_{\mathbb{C}}(I))$  if and only if its real and imaginary parts belong to  $I(V_{\mathbb{C}}(I))$ ; that is, it suffices to determine  $I(V_{\mathbb{C}}(I)) \cap \mathbb{R}[x]$ . For this, it suffices to consider *real valued* matrices  $M_t^{\mathbb{C}}(y)$  (or  $M_t^{2\mathbb{C}}(y)$ ), i.e., with  $y \in K_t^{\mathbb{C}} \cap \mathbb{R}^{\mathbb{N}_{2t}^{2n}}$  (or  $K_t^{2\mathbb{C}} \cap \mathbb{R}^{\mathbb{N}_{2t}^{2n}}$ ) in Propositions 4.1, 4.10, and 4.11. Indeed, one may, e.g., easily verify that Lemma 3.2 remains valid within the context of real polynomials and replacing  $K_t^{\mathbb{C}}$  (or  $K_t^{2\mathbb{C}}$ ) by  $K_t^{\mathbb{C}} \cap \mathbb{R}^{\mathbb{N}_{2t}^{2n}}$  (or  $K_t^{2\mathbb{C}} \cap \mathbb{R}^{\mathbb{N}_{2t}^{2n}}$ ). (Use here the fact that, since  $V_{\mathbb{C}}(I)$  is closed under conjugation, then  $\frac{1}{2}(\zeta_{2t,\bar{v}} \otimes \zeta_{2t,v} + \zeta_{2t,v} \otimes \zeta_{2t,\bar{v}})$  belongs to  $K_t^{2\mathbb{C}} \cap \mathbb{R}^{\mathbb{N}_{2t}^{2n}}$ .)

#### 4.4 Algorithm and Implementation

With the results of Sects. 4.1–4.3 we have all the ingredients needed to compute the radical ideals  $I(V_{\mathbb{R}}(I))$  and  $I(V_{\mathbb{C}}(I))$  of an ideal  $I$  given by its generators. We now describe the algorithm in more detail.

For convenience, let  $K_t$  (resp.,  $M_t(y)$ ) stand for  $K_t^{\mathbb{R}}$ ,  $K_t^{\mathbb{C}}$ ,  $K_t^{2\mathbb{C}}$  (resp.,  $M_t^{\mathbb{R}}(y)$ ,  $M_t^{\mathbb{C}}(y)$ ,  $M_t^{2\mathbb{C}}(y)$ ). For the task of computing  $I(V_{\mathbb{R}}(I))$ , we will use  $K_t = K_t^{\mathbb{R}}$  (and apply Propositions 4.1, 4.2, and 4.4) and for the task of computing  $I(V_{\mathbb{C}}(I))$  we use  $K_t = K_t^{\mathbb{C}}$  (and apply Proposition 4.1) or  $K_t = K_t^{2\mathbb{C}}$  (and apply Propositions 4.10 and 4.11). The algorithm consists of five main parts: For a given order  $t \geq d$ :

- (i) Find an element  $y \in K_t$  maximizing the rank of  $M_t(y)$ .
- (ii) Check the ranks of the principal submatrices of  $M_t(y)$ .
- (iii) Compute a basis for the column space of  $M_{s-1}(y)$  and the quotient space  $\mathbb{K}[x]/J$  ( $J = \langle \text{Ker } M_s(y) \rangle$ ), for suitable  $1 \leq s \leq t$ .
- (iv) Compute the formal multiplication matrices.
- (v) Construct a basis for the ideal  $J$ .

In step (ii) we search for a submatrix  $M_s(y)$  of  $M_t(y)$  satisfying Proposition 4.1(i)–(iii), or the rank condition (4.1) (resp., (4.5)), or (4.2) (resp. (4.6)). Depending on what condition is satisfied, the algorithm returns a subideal  $J \subseteq I(V_{\mathbb{K}}(I))$  together with a superset  $W \supseteq V_{\mathbb{K}}(I)$ , or the desired radical ideal  $I(V_{\mathbb{K}}(I))$  and the desired set of roots  $V_{\mathbb{K}}(I)$ . One can anyway verify a posteriori whether  $W = V_{\mathbb{K}}(I)$ , simply by checking whether  $h_j(v) = 0$  for all  $j \leq m$  and  $v \in W$ . In the sequel of this section we give more details about these different tasks.

##### 4.4.1 Finding $y \in K_t$ Maximizing the Rank of $M_t(y)$

This first task can be cast as the problem of finding a feasible solution of a semidefinite program, that has maximum rank. For details on the theory and applications of semidefinite programming the interested reader is referred, e.g., to [42, 45]. It is a known geometric property of semidefinite programs that a feasible solution has maximum rank if and only if it lies in the relative interior of the feasible region and that such a point can be found with interior-point algorithms using self-dual embedding (see, e.g., [15, 45]). Let us give some details.

Consider a general instance of a semidefinite program

$$p^* := \inf \sum_{j=1}^m b_j y_j \quad \text{s.t.} \quad \sum_{j=1}^m y_j A_j - C \succeq 0 \quad (4.7)$$

and its dual semidefinite program

$$d^* := \sup \text{Tr}(CX) \quad \text{s.t.} \quad \text{Tr}(A_j X) = b_j \quad (j = 1, \dots, m), \quad X \succeq 0. \quad (4.8)$$

Here  $A_j, C, X$  are Hermitian matrices,  $b, y \in \mathbb{R}^m$ , and  $X, y$  are the variables. Obviously,  $d^* \leq p^*$  (weak duality). There is no duality gap (i.e.,  $p^* = d^*$ ), e.g., when (4.7) is strictly feasible (i.e.,  $\exists y \in \mathbb{R}^m$  with  $\sum_{j=1}^m y_j A_j - C \succ 0$ ) or when (4.8) is strictly feasible (i.e.,  $\exists X \succ 0$  feasible for (4.8)). When (4.8) is strictly feasible and  $d^* < \infty$ , then (4.7) attains its minimum, i.e., the set of optimal solutions is nonempty. The feasible region to (4.7) is the convex set

$$K = \left\{ y \mid \sum_{j=1}^m y_j A_j - C \succeq 0 \right\} = \left\{ y \mid u^* \left( \sum_{j=1}^m y_j A_j - C \right) u \geq 0 \forall u \in \mathbb{K}^m \right\}.$$

Therefore, for  $y \in K$ ,  $y$  lies in the relative interior of  $K$  if and only if  $\text{Ker} \left( \sum_{j=1}^m y_j A_j - C \right) \subseteq \text{Ker} \left( \sum_{j=1}^m z_j A_j - C \right)$  for all  $z \in K$  or, equivalently, if  $\sum_{j=1}^m y_j A_j - C$  has maximum possible rank (same argument as for Lemma 3.1).

Semidefinite programs can be solved in polynomial time to an arbitrary precision using, e.g., the ellipsoid method, whose running time is however prohibitively high in practice. Interior-point methods are now the method of choice for solving semidefinite programs. Assuming strict feasibility of (4.7) and (4.8), interior-point algorithms construct sequences of points on the so-called central path, which has the property of converging to an optimum solution of maximum rank [20]. One can also find a maximum rank optimum solution under the weaker assumption that (4.7), (4.8) are feasible (but not necessarily strictly feasible), if  $p^*$  is attained, and  $p^* = d^* < \infty$ . Indeed, one can then construct the so-called extended self-dual embedding which is a strictly feasible semidefinite program with the property that a maximum rank optimum solution to it yields a maximum rank optimum solution to the original problem (4.7) (see, e.g., [15, Chap. 4; 45, Chap. 5]).

For our problem of finding  $y \in K_t$  maximizing rank  $M_t(y)$ , consider the semidefinite program with constant objective function 1

$$p^* := \min 1 \quad \text{s.t.} \quad M_t(y) \succeq 0, \quad M_{t-d_j}(h_j y) = 0 \quad (j = 1, \dots, m), \quad y_0 = 1, \quad (4.9)$$

where we add the condition (3.1) in the complex case. One can interpret (see, e.g., [25]) the dual of (4.9) as

$$d^* := \max \lambda \quad \text{s.t.} \quad 1 - \lambda = s + \sum_{j=1}^m q_j h_j \quad \text{with } s, q_j \text{ polynomials} \\ \deg(s), \deg(q_j h_j) \leq 2t, \quad s \text{ is s.o.s.}, \quad (4.10)$$

where ‘ $s$  is s.o.s.’ means that  $s$  can be written as a sum of squares, i.e.,  $s = \sum_h |u_h|^2$  for some polynomials  $u_h \in \mathbb{K}[x]$  or  $\mathbb{C}[x, \bar{x}]$ . Obviously, (4.9) is feasible if  $V_{\mathbb{K}}(I) \neq \emptyset$ . Moreover, (4.10) is feasible (e.g., with  $\lambda = 1$ ,  $s = q_j = 0$  as a feasible solution) and, if  $K_t \neq \emptyset$ , then  $p^* = 1$  is attained by the whole set  $K_t$  and  $p^* = d^* = 1$ . Hence an interior-point algorithm implementing the self-dual embedding technique applied to problem (4.9) is guaranteed to return the following information:<sup>2</sup> Either: (i)  $y \in K_t$  maximizing  $\text{rank } M_t(y)$ ; or (ii) a certificate that (4.9) is infeasible thus implying  $V_{\mathbb{K}}(I) = \emptyset$ . For our computations we use the semidefinite programming solver SeDuMi-1.05 [40, 41] which implements this feature. Practically, this means that the solution returned by the algorithm is very close to a maximum rank optimum solution.

*Remark 4.15* When using a semidefinite programming solver without the maximum rank property, one can recover a maximum rank solution to (4.9) from a feasible solution  $\hat{y}$  to (4.9), using the following simple iterative algorithm. Let  $u_1, \dots, u_p$  be a set of vectors that span  $\text{Ker } M_t(\hat{y})$ , set  $C := \sum_{i=1}^p u_i u_i^*$ , and consider the semidefinite program:  $\max \langle C, M_t(y) \rangle$  subject to  $y$  satisfying the constraints of (4.9). If the optimum value is equal to 0, then  $\hat{y}$  is in fact a solution of maximum rank. Otherwise, let  $y_1$  be the optimum solution returned by the solver; then  $\text{Ker } M_t(\hat{y}) \not\subseteq \text{Ker } M_t(y_1)$ . Then,  $y_2 := \frac{1}{2}(\hat{y} + y_1)$  is feasible for (4.9) and  $\text{Ker } M_t(y_2) = \text{Ker } M_t(\hat{y}) \cap \text{Ker } M_t(y_1) \subset \text{Ker } M_t(\hat{y})$ . Hence we have found a feasible solution  $y_2$  to (4.9) for which the rank of  $M_t(y_2)$  is larger than that  $M_t(\hat{y})$ . Iterate replacing  $\hat{y}$  by  $y_2$ .

#### 4.4.2 Checking Ranks of Submatrices of $M_t(y)$

Once a maximum rank matrix  $M_t(y)$  is found, one has to check if for some  $1 \leq s \leq t$  the conditions of Proposition 4.1(i)–(iii) hold, or if (4.1) (resp., (4.5)) holds, or if (4.2) (resp., (4.6)) holds. For this one has to compute the ranks of the principal submatrices  $M_s(y)$  of  $M_t(y)$  for  $s \leq t$ . Checking the rank of a matrix consisting of numerical values is computationally sensitive. This is carried out using singular value decomposition which at the same time can be used to generate a basis of the column space; see the next section for more details. The determination of the rank is done by detecting zero singular values or a decay of more than  $1e-3$  between two subsequent values, where singular values less than  $1e-8$  are declared to be zero.

#### 4.4.3 Computing a Basis for the Column Space of $M_{s-1}(y)$ and the Quotient Space $\mathbb{K}[x]/J$

We indicate here how to compute a basis of the column space of the matrix  $M_{s-1}(y)$ . Under some conditions (recall Corollary 3.8), such basis also yields a basis of the quotient space  $\mathbb{K}[x]/J$  (as before,  $J := \langle \text{Ker } M_s(y) \rangle$ ), which is needed for the computation of the multiplication matrices. The choice of this basis will have an influence

<sup>2</sup>Three options (I), (II), (III) are described in [45, Chap. 5, p. 119]; (i) corresponds to (I) and (ii) to (II), (III). Indeed, under (III) a certificate is reported that no complementary pair exists which implies, in our case, that (4.9) is infeasible, since any  $y \in K_t$  together with the solution  $\lambda = 1$ ,  $s = q_j = 0$  to (4.10) makes a complementary pair.

on the numerical stability of the extracted set  $W$  of solutions and on the properties of the basis for  $J$  as well.

*Using Singular Value Decomposition.* It is a well-known fact from linear algebra that a numerically stable way of finding an orthonormal basis  $\mathcal{B}$  for the column space of a matrix  $M$  is to use its singular value decomposition (SVD):  $M = U \Sigma V^*$ , where  $U, V$  are unitary and  $\Sigma$  is diagonal with nonnegative entries. The diagonal entries of  $\Sigma$  are the singular values of  $M$  (i.e., the square roots of the eigenvalues of  $MM^*$ ); the number of nonzero diagonal entries of  $\Sigma$  is thus equal to  $r := \text{rank } M$ . Then the set  $\{U_1, \dots, U_r\}$  of columns of  $U$  corresponding to the nonzero diagonal entries of  $\Sigma$  forms an orthonormal basis of the column space of  $M$ . As we already did perform an SVD to determine the rank of the matrix  $M := M_{s-1}(y)$ , this computation comes with no extra effort. For  $i = 1, \dots, r$ , let  $b_i := \zeta_{s-1,x}^T U_i$  be the polynomial with vector of coefficients  $\text{vec}(b_i) = U_i$ . The next lemma shows that, under some rank condition,  $\{b_1, \dots, b_r\}$  is a basis of  $\mathbb{K}[x]/J$ .

**Lemma 4.16** *Let  $\{U_1, \dots, U_r\}$  be a basis of the column space of  $M_{s-1}(y)$ , let  $b_i := \zeta_{s-1,x}^T U_i$  ( $i = 1, \dots, r$ ), and assume that the rank condition (4.1) or (4.5) holds. Then the set  $\{b_1, \dots, b_r\}$  is a basis of the quotient space  $\mathbb{K}[x]/J$ .*

*Proof* As the rank condition (4.1) or (4.5) holds, we know from Corollary 3.8 that  $\dim \mathbb{K}[x]/J = r := \text{rank } M_{s-1}(y)$  and  $J \cap \mathbb{K}_{s-1}[x] = \text{Ker } M_{s-1}(y)$ . Hence it suffices to show that  $\{b_1, \dots, b_r\}$  is linearly independent in  $\mathbb{K}[x]/J$ . For this assume  $\sum_{i=1}^r \lambda_i b_i \in J$ , i.e.,  $\zeta_{s-1,x}^T (\sum_{i=1}^r \lambda_i U_i) \in J$ . The vector  $p := \sum_{i=1}^r \lambda_i U_i$  lies in the column space of  $M_{s-1}(y)$ . On the other hand,  $p \in \text{Ker } M_{s-1}(y)$  since the corresponding polynomial  $p$  lies in  $J \cap \mathbb{K}_{s-1}[x]$ . Therefore,  $p = 0$  which implies that all  $\lambda_i = 0$ .  $\square$

*Using a ‘Greedy’ Algorithm.* If we want to compute a border basis or a Gröbner basis with our algorithm, we need a monomial basis  $\mathcal{B}$  (i.e.,  $\mathcal{B} \subseteq \mathbb{T}_n$ ) for the quotient space  $\mathbb{K}[x]/J$ . For this, it suffices to construct a set  $\mathcal{B}$  indexing a maximum principal nonsingular submatrix of  $M_{s-1}(y)$ , as  $\mathcal{B}$  is then a basis of  $\mathbb{K}[x]/J$  under the conditions of Corollary 3.8. One can apply the following simple procedure (proposed in [29]) for constructing  $\mathcal{B}$ : Scan monomials in  $\mathbb{T}_{n,s-1}$  by increasing degree, starting with  $t_0 = 1, t_1 = x_1, t_2 = x_2, \dots$ . Initialize  $\mathcal{B} := \{t_0\}$ . Let  $\mathcal{B}$  be the current set and let  $t_k$  be the current monomial to be scanned. If  $\mathcal{B} \cup \{t_k\}$  indexes a linearly independent set of columns of  $M_{s-1}(y)$ , then reset  $\mathcal{B} := \mathcal{B} \cup \{t_k\}$ , otherwise scan the next monomial  $t_{k+1}$ . This procedure is ‘greedy’ in the sense that one keeps adding as many low degree monomials as possible to the basis. One can stop as soon as  $|\mathcal{B}| = r$ . Alternatively, one may construct a reduced row echelon form of  $M_{s-1}(y)$  using Gauss Jordan elimination with partial pivoting (pivot variables serve as basis  $\mathcal{B}$ ), see [21]. One can verify afterwards whether the constructed basis  $\mathcal{B}$  is an order ideal; it turns out that this is the case in most tested instances.

The greedy sieve algorithm described earlier in Sect. 2.4 produces directly an order ideal basis. Indeed, given any graded monomial ordering  $\succ$ , we can apply it to obtain the set  $\mathcal{B} = \mathcal{B}_\succ$  of standard monomials for this ordering, forming an order ideal



basis of  $\mathbb{K}[x]/J$  (as we know from Lemma 2.5 that  $\mathcal{B}_>$  is contained in  $\mathbb{T}_{n,s-1}$  under the conditions of Corollary 3.8). See Sect. 4.4.5 for an extension to the case of an arbitrary monomial ordering.

Note that, although desirable from an algebraic point of view, monomial bases for  $\mathbb{K}[x]/J$  sometimes lead to a less accurate set  $W$  of extracted solutions as compared to those extracted with a polynomial basis  $\mathcal{B}$  based on SVD; see, e.g., Examples 5.4 and 5.5.

#### 4.4.4 Computing Formal Multiplication Matrices

Let  $\mathcal{B} = \{b_1, \dots, b_r\}$  be a basis of the column space of  $M_{s-1}(y)$ . By the assumptions of Proposition 4.1 or under the rank conditions (4.1) or (4.5), there exist scalars  $a_k^{(ij)}$  ( $k = 1, \dots, r$ ) for which  $x_i b_j - \sum_{k=1}^r a_k^{(ij)} b_k \in \text{Ker } M_s(y)$  for all  $i = 1, \dots, n$ ,  $j = 1, \dots, r$ . Then the vector  $(a_k^{(ij)})_{k=1}^r$  is the  $j$ th column of the (formal) multiplication matrix  $\mathcal{X}_i$ . We indicate how to compute  $\mathcal{X}_i$  from  $M_s(y)$ .

Suppose first that  $\mathcal{B}$  is a monomial basis, i.e.,  $\mathcal{B} \subseteq \mathbb{T}_{n,s-1}$ . Let  $M_{\mathcal{B}}$  denote the principal submatrix of  $M_s(y)$  indexed by  $\mathcal{B}$  and let  $P_{x_i}$  be the submatrix of  $M_s(y)$  whose rows are indexed by  $\mathcal{B}$  and whose columns are indexed by the set  $x_i \mathcal{B} := \{x_i b_j \mid j = 1, \dots, r\}$ . As observed in [29], we have

$$\mathcal{X}_i = M_{\mathcal{B}}^{-1} P_{x_i}. \quad (4.11)$$

Indeed, for  $b \in \mathbb{T}_{n,s}$ , let  $C_b$  denote the column of  $M_s(y)$  indexed by  $b$  restricted to the rows indexed by  $\mathcal{B}$ . Then,

$$C_{x_i b_j} = \sum_{k=1}^r a_k^{(ij)} C_{b_k} = M_{\mathcal{B}} a^{(ij)}, \quad (4.12)$$

i.e.,  $a^{(ij)} = M_{\mathcal{B}}^{-1} C_{x_i b_j}$ , which gives  $\mathcal{X}_i = M_{\mathcal{B}}^{-1} P_{x_i}$ .

Suppose now that  $\mathcal{B}$  is a polynomial basis obtained via SVD, as explained above. That is,  $b_i = \zeta_{s-1,x}^T U_i$  where  $\{U_1, \dots, U_r\}$  is an orthonormal basis of the column space of  $M_{s-1}(y)$  and thus of  $M_s(y)$  under the rank condition (4.1) or (4.5). As in the monomial case, the formal multiplication matrices can be derived from  $M_s(y)$ . Let  $\tilde{P}_{x_i}$  denote the submatrix of  $M_s(y)$  with columns indexed by  $x_i \mathbb{T}_{n,s-1}$  and with rows indexed by  $\mathbb{T}_{n,s-1}$ . Let  $U$  denote the matrix with columns  $U_1, \dots, U_r$ , and set  $P_{x_i} := U^T \tilde{P}_{x_i} U$  and  $M_{\mathcal{B}} := U^T M_{s-1}(y) U$ . Then,  $M_{\mathcal{B}}$  is nonsingular. Moreover,

$$M_{\mathcal{B}} \mathcal{X}_i = P_{x_i}, \quad (4.13)$$

which allows the computation of  $\mathcal{X}_i = M_{\mathcal{B}}^{-1} P_{x_i} = \Sigma^{-1} P_{x_i}$  where  $\Sigma$  is the diagonal matrix containing the positive singular values of  $M_{s-1}(y)$ . We verify that (4.13) holds. By construction, the polynomial  $x_i b_j - \sum_{k=1}^r a_k^{(ij)} b_k = x_i \zeta_{s-1,x}^T U_j - \sum_{k=1}^r a_k^{(ij)} \zeta_{s-1,x}^T U_k$  lies in  $\text{Ker } M_s(y)$ . This implies  $0 = \tilde{P}_{x_i} U_j - M_{s-1}(y) U a^{(ij)}$  and thus  $U^T \tilde{P}_{x_i} U_j = U^T M_{s-1}(y) U a^{(ij)} = M_{\mathcal{B}} a^{(ij)}$ , which shows that the two matrices  $P_{x_i}$  and  $M_{\mathcal{B}} \mathcal{X}_i$  have identical  $j$ th columns.

#### 4.4.5 Constructing a Basis for the Ideal $J := \langle \text{Ker } M_s(y) \rangle$

*A Linear Basis of  $\text{Ker } M_s(y)$ .* The simplest way of producing a basis for the ideal  $J = \langle \text{Ker } M_s(y) \rangle$  is simply by considering a linear basis of  $\text{Ker } M_s(y)$ . Such a basis can be found by using again an SVD for  $M_s(y)$ . Indeed, if  $M_s(y) = U \Sigma V^*$  is the SVD, then the columns  $V_i$  of  $V$  corresponding to the zero diagonal entries of  $\Sigma$  (the zero singular values of  $M_s(y)$ ) form an orthonormal basis of  $\text{Ker } M_s(y)$ . Then the polynomials  $\zeta_{s,x}^T V_i$  corresponding to the zero singular values of  $M_s(y)$  form a basis of  $J$ . A drawback of this basis however is that it is usually highly overdetermined and has a large cardinality, equal to  $|\mathbb{T}_{n,s}| - \text{rank } M_s(y)$ .

*A Border Basis.* As shown in [39, Sect. 8.2, Chap. 10], it is desirable to avoid overdetermined bases for  $J$  because it could lead to inconsistencies in the basis for numerical reasons. To avoid this drawback, border bases are proposed in [39] and their numerical properties are investigated. If during the construction of the formal multiplication matrices an order ideal basis  $\mathcal{B}$  of  $\mathbb{K}[x]/J$  was used, we deduce immediately a border basis consisting of the polynomials

$$x_i b_j - \sum_{k=1}^r a_k^{(ij)} b_k \quad \text{for } x_i b_j \in \partial \mathcal{B}. \quad (4.14)$$

*A Gröbner Basis.* If the monomial basis  $\mathcal{B}$  of  $\mathbb{K}[x]/J$  is the set of standard monomials  $\mathcal{B}_>$  with respect to a monomial ordering  $>$  obtained, e.g., with the greedy sieve algorithm, then the border basis in (4.14) is actually a Gröbner basis with respect to the monomial ordering  $>$ . When  $>$  is a graded monomial ordering then, in view of Lemma 2.5,  $\mathcal{B}_> \subseteq \mathbb{T}_{n,s}$  and thus  $\mathcal{B}_>$  can be found with Algorithm 1 applied to  $(I(V_{\mathbb{K}}(I)), \succeq, s)$ , using the following independence oracle: A subset of  $\mathbb{T}_{n,s}$  is independent in  $\mathbb{K}[x]/I(V_{\mathbb{K}}(I))$  if and only if it indexes an independent set of columns of  $M_s(y)$ . In general, when  $>$  is not a graded monomial ordering we are not assured to find  $\mathcal{B}_>$  within  $\mathbb{T}_{n,s}$ . However, we can proceed as follows. As  $M_s(y)$  is a flat extension of  $M_{s-1}(y)$ , by the results in Section 3.3, there exists an extension  $\tilde{y} \in \mathbb{R}^{\mathbb{N}_t^n}$  (for any  $t \geq s$ ) such that  $M_t(\tilde{y})$  is a flat extension of  $M_s(y)$ . As  $\langle \text{Ker } M_s(y) \rangle = \langle \text{Ker } M_t(\tilde{y}) \rangle = I(V_{\mathbb{R}}(I))$ , a subset of  $\mathbb{T}_{n,t}$  is independent in  $\mathbb{K}[x]/I(V_{\mathbb{K}}(I))$  if and only if it indexes an independent set of columns of  $M_t(\tilde{y})$ . Thus, to find  $\mathcal{B}_>$ , apply Algorithm 1 iteratively to  $t = s + 1, s + 2, \dots$  until finding  $\mathcal{B}_t = \mathcal{B}_{t+1}$ , in which case we know from Lemma 2.6(ii) that  $\mathcal{B}_> = \mathcal{B}_t$ . It remains only to address the question of how to find the flat extension  $\tilde{y}$ . The existence proof in [12] is constructive and can roughly be sketched as follows (see also [29] for details). Say we want to construct a flat extension  $C := M_{s+1}(\tilde{y})$  of  $B := M_s(y)$ , under the assumption that  $B$  is a flat extension of  $M_{s-1}(y)$ . We indicate how to construct the column  $C(\cdot, \gamma)$  of  $C$  indexed by a monomial  $x^\gamma$  of degree  $s + 1$ . Write, say,  $x^\gamma = x_i x^\beta$ . By assumption, the column  $B(\cdot, \beta)$  of  $B$  indexed by  $x^\beta$  can be expressed as a linear combination  $\sum_{|\alpha| \leq s-1} \lambda_\alpha B(\cdot, \alpha)$  of columns indexed by  $\mathbb{T}_{n,s-1}$ ; then define  $C(\cdot, \gamma)$  as  $\sum_{|\alpha| \leq s-1} \lambda_\alpha C(\cdot, \alpha + e_i)$ . Note that this construction relies on the fact that the kernel of moment matrices enjoys ideal-like properties.

#### 4.4.6 Summary of the Algorithm

Algorithm 2 below summarizes our algorithm. This algorithm has been implemented in Matlab using the Yalmip toolbox [30]. For solving the semidefinite program (4.9) the semidefinite solver SeDuMi-1.05 [40, 41] is used. As described above, and can be seen in the examples in the next section, the rank detection is the most critical task. This was the main motivation for the weaker conditions from Sect. 4.1, which extend the possibility of extracting solutions. In the examples below, this deficiency is clearly indicated in some rank sequences not exactly matching the theory.

---

#### Algorithm 2 Numerical border basis computation:

---

**Input:** Polynomial generators  $h_i$  for  $I := \langle h_1, \dots, h_m \rangle \subseteq \mathbb{K}[x]$  and relaxation order  $t \in \mathbb{N}$

**Output:** A basis for an ideal  $J \subseteq I(V_{\mathbb{K}}(I))$ , the set  $V_{\mathbb{C}}(J)$ , and a basis  $\mathcal{B}$  for the quotient ring  $\mathbb{K}[x]/J$

- 1: Solve the SDP (4.9). If the SDP is infeasible, return  $V_{\mathbb{K}}(I) = \emptyset$ . Otherwise, return a feasible solution  $y$  for which  $M_t(y)$  has maximum rank
  - 2: Compute SVD for all principal submatrices  $M_s(y)$  ( $s = 1, \dots, t$ )
  - 3: Determine rank  $M_s(y)$  ( $s = 1, \dots, t$ ) and check whether the conditions of Propositions 4.1–4.11 hold
  - 4: Fix  $s$  (for which one of Propositions 4.1–4.11 applies)
  - 5: Compute a basis  $\mathcal{B}$  of the column space of  $M_{s-1}(y)$ :
    - (a) using the SVD decomposition ( $\mathcal{B}$  is a polynomial basis)
    - (b) using a greedy algorithm ( $\mathcal{B}$  is a monomial basis)
    - (c) using a greedy sieve algorithm ( $\mathcal{B}$  is the set of standard monomials for a monomial ordering  $\succ$ )
  - 6: Compute the multiplication matrices  $\mathcal{X}_i = M_{\mathcal{B}}^{-1} P_{x_i}$
  - 7: Compute a basis for the ideal  $J$ 
    - (a) an SVD basis of  $\text{Ker } M_s(y)$  (requires  $\text{rank } M_s(y) = \text{rank } M_{s-1}(y)$ )
    - (b) a border basis of  $J$  (requires that  $\mathcal{B}$  is a monomial basis and an order ideal)
    - (c) a Gröbner basis (requires that  $\mathcal{B}$  is the corresponding set of standard monomials)
  - 8: **if** the conditions of Proposition 4.1 are met **then**
  - 9:   **return** a (border/Gröbner) basis of  $J \subseteq I(V_{\mathbb{K}}(I))$ , a basis  $\mathcal{B}$  of  $\mathbb{K}[x]/J$ , and the set  $V_{\mathbb{C}}(J)$
  - 10: **else**
  - 11:   **return** ERROR: “No extraction possible. Increase relaxation order  $t$ .”
  - 12: **end if**
- 

*Remark 4.17* In view of Propositions 4.6 and 4.12, the algorithm terminates for  $t$  large enough and finds  $J = I(V_{\mathbb{R}}(I))$  or  $I(V_{\mathbb{C}}(I))$ . The algorithm can also be used for testing existence of solutions. Let us give some details, e.g., in the real case. If at step 1 one detects infeasibility of the SDP then one can already conclude  $V_{\mathbb{R}}(I) = \emptyset$ . Suppose now the SDP is feasible. At step 4, as observed in Remark 4.8, the conditions of Proposition 4.4 cannot be met if  $V_{\mathbb{R}}(I) = \emptyset$ , but it could be that the conditions of



Proposition 4.1 or 4.2 are met. In that case one can extract a set  $W \supseteq V_{\mathbb{R}}(I)$ . Then one can simply test whether the points of  $W$  satisfy the given equations  $h_1 = \dots = h_m = 0$  to detect whether  $V_{\mathbb{R}}(I)$  is empty or not.

### 5 Numerical Examples

We present here the results of our algorithm applied to some examples, taken mainly from the literature. In each example, we specify the ideal  $I$  by its generators  $h_1, \dots, h_m$ . Let us explain Tables 1–5 below. At a given order  $t$ , let  $y$  be the optimal solution to (4.9) returned by the SDP solver. The abbreviations ‘MON’ and ‘SVD’ refer to using a *monomial* base of the quotient space, or a base found via the *SVD method*.

- The column ‘rank sequence’ shows  $(\text{rank } M_0(y), \dots, \text{rank } M_t(y))$ .
- The column ‘extract. order’ shows some numbers  $s_{\text{MON}}(r_{\text{MON}})/s_{\text{SVD}}(r_{\text{SVD}})$ . When using a monomial base,  $r_{\text{MON}}$  is the smallest order at which the extraction procedure could be carried out and  $s_{\text{MON}}$  is the order at which it was effectively carried out and gave the results reported here; analogously with the SVD method.
- The column ‘accuracy’ shows the accuracy of the returned solutions, i.e.,  $\max_{j,x} |h_j(x)|$ , where  $h_j$  runs over the generators of  $I$  and  $x$  over the extracted solutions.
- The column ‘comm. error’ shows the commutativity error for the multiplication matrices, i.e.,  $\max_{i,j=1}^n \text{abs}(\mathcal{X}_i \mathcal{X}_j - \mathcal{X}_j \mathcal{X}_i)$  (where  $\text{abs}(M)$  is the maximum absolute value of the entries of a matrix  $M$ ). If the parameter ‘comm. error’ is more than  $1e-2$ , the multiplication matrices do not commute sufficiently and we then do not extract solutions.

**Example 5.1** This simple example from [11, p. 40] has two roots, both real,

$$\begin{aligned} h_1 &= x_2^4 x_1 + 3x_1^3 - x_2^4 - 3x_1^2, \\ h_2 &= x_1^2 x_2 - 2x_1^2, \\ h_3 &= 2x_2^4 x_1 - x_1^3 - 2x_2^4 + x_1^2. \end{aligned}$$

Monomial basis of  $\mathbb{R}[x]/I(V_{\mathbb{R}}(I))$ :

$$\mathcal{B} = \{1, x_1\}.$$

**Table 1** Results for Example 5.1

Order $t$	Rank sequence	Extract. order MON/SVD	Accuracy MON/SVD	Comm. error MON/SVD
3	1 3 5 9	—	—	—
4	1 2 2 2 7	4(2)/3(2)	1.9717e-9/0.00013144	9.676e-10/3.3908e-6
5	1 2 2 2 2 8	4(2)/4(2)	2.9557e-8/3.5325e-5	1.8781e-11/1.2291e-6

Border basis for  $I(V_{\mathbb{R}}(I))$  (showing in **bold** the monomials in  $\partial\mathcal{B}$ ):

$$\begin{aligned}g_1 &= -x_1 + \mathbf{x}_1^2, \\g_2 &= -2x_1 + \mathbf{x}_2, \\g_3 &= -2x_1 + \mathbf{x}_1\mathbf{x}_2.\end{aligned}$$

Extracted real solutions  $V_{\mathbb{R}}(I)$ :

$$\begin{aligned}v_1 &= (2.12\text{e-}8, 1.91\text{e-}6), \\v_2 &= (1, 2).\end{aligned}$$

The first two polynomials  $g_1, g_2$  of the extracted border basis form a reduced Gröbner basis with respect to the graded reversed term order with  $x_1 < x_2$ . The basis of  $\sqrt{I}$  ( $= I(V_{\mathbb{R}}(I))$  as all roots are real) given in [11] has the form:

$$\begin{aligned}\{ &x_2^4x_1 + 3x_1^3 - x_2^4 - 3x_1^2, x_1^2x_2 - 2x_1^2, \\ &2x_2^4x_1 - x_1^3 - 2x_2^4 + x_1^2, x_1(x_1 - 1), x_2(-2 + x_2)\}\end{aligned}$$

and is obtained via Seidenberg's method described in the paragraph 'Related literature' in the Introduction. Computing a graded reversed Gröbner Basis of  $\sqrt{I}$  (using `tdeg` in MAPLE) leads again to the set  $\{g_1, g_2\}$  found by our method. Thus our method finds here a simpler set of generators for  $\sqrt{I}$  than the classical method of Seidenberg.

**Example 5.2** This example is taken from the polynomial testsuite [6] (see <http://www-sop.inria.fr/saga/POL/BASE/2.multipol/bifurc.html>). It has 20 complex solutions among which eight are real. This example illustrates the possibility of extracting solutions based on Proposition 4.1 in case none of the rank conditions are satisfied,

$$\begin{aligned}h_1 &= 5x_1^9 - 6x_1^5x_2 + x_1x_2^4 + 2x_1x_3, \\h_2 &= -2x_1^6x_2 + 2x_1^2x_2^3 + 2x_2x_3, \\h_3 &= x_1^2 + x_2^2 - 0.265625.\end{aligned}$$

**Table 2** Results for Example 5.2

Order $t$	Rank sequence	Extract. order MON/SVD	Accuracy MON/SVD	Comm. error MON/SVD
5	1 4 8 16 25 34	—	—	—
6	1 3 9 15 22 26 32	—	—	—
7	1 3 8 10 12 16 20 24	3(3)/—(—)	0.12786/—	0.00019754/—
8	1 4 8 8 8 12 16 20 24	4(3)/3(3)	4.6789e-5/0.00013406	4.7073e-5/0.00075005

Monomial basis of  $\mathbb{R}[x]/I(V_{\mathbb{R}}(I))$ :

$$\mathcal{B} = \{1, x_1, x_2, x_3, x_1^2, x_1x_2, x_1x_3, x_2x_3\}.$$

Border basis of  $I(V_{\mathbb{R}}(I))$ :

$$\begin{aligned} g_1 &= -0.28479x_1 + 0.44124x_1x_2 - 1.5403x_1x_3 + \mathbf{x}_1^3, \\ g_2 &= -1.7276x_3 - 0.080949x_1^2 + 8.1433x_2x_3 + \mathbf{x}_1^2\mathbf{x}_2, \\ g_3 &= -0.28763x_3 - 0.0010314x_1^2 + 0.48126x_2x_3 + \mathbf{x}_1^2\mathbf{x}_3, \\ g_4 &= -0.0015073x_1 + 0.01299x_1x_2 - 0.12111x_1x_3 + \mathbf{x}_1\mathbf{x}_2\mathbf{x}_3, \\ g_5 &= -0.26563 + x_1^2 + \mathbf{x}_2^2, \\ g_6 &= 0.019164x_1 - 0.44124x_1x_2 + 1.5403x_1x_3 + \mathbf{x}_1\mathbf{x}_2^2, \\ g_7 &= 0.022008x_3 + 0.0010314x_1^2 - 0.48126x_2x_3 + \mathbf{x}_2^2\mathbf{x}_3, \\ g_8 &= -0.0018637x_3 - 0.00067043x_1^2 + 0.026066x_2x_3 + \mathbf{x}_3^2, \\ g_9 &= -0.00015166x_1 + 0.00025958x_1x_3 + \mathbf{x}_1\mathbf{x}_3^2, \\ g_{10} &= -0.0017335x_3 + 0.01615x_2x_3 + \mathbf{x}_2\mathbf{x}_3^2. \end{aligned}$$

Extracted real solutions:

$$\begin{aligned} v_1 &= (-0.515, -0.000153, -0.0124), \\ v_2 &= (-0.502, 0.119, 0.0124), \\ v_3 &= (0.502, 0.119, 0.0124), \\ v_4 &= (0.515, -0.000185, -0.0125), \\ v_5 &= (0.262, 0.444, -0.0132), \\ v_6 &= (-2.07e-5, 0.515, -1.27e-6), \\ v_7 &= (-0.262, 0.444, -0.0132), \\ v_8 &= (-1.05e-5, -0.515, -7.56e-7). \end{aligned}$$

**Example 5.3** We now give an example for finding  $I(V_{\mathbb{R}}(I) \cap S)$ , where  $I = \langle h_1, \dots, h_4 \rangle$  with

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

**Table 3** Results for Example 5.3

Order $t$	Rank sequence	Extract. order	Accuracy	Comm. error
		MON/SVD	MON/SVD	MON/SVD
2	1 2 11	2(2)/—(—)	0.00010224/—	1.1124e-9/—
3	1 2 2 18	2(2)/2(2)	1.8985e-14/5.1015e-14	1.2212e-15/1.4155e-15
4	1 2 2 2 24	2(2)/2(2)	3.5527e-15/8.5487e-15	2.2204e-16/1.1102e-16

and  $S$  is defined by the polynomial inequalities  $-1 \leq x_1, x_2, x_3, x_4 \leq 1$ . This example, taken from [44], represents a Gaussian quadrature formula with two weights and two knots, where one is interested only in the roots lying in the box  $[-1, +1]$ .

Monomial basis of  $\mathbb{R}[x]/I(V_{\mathbb{R}}(I) \cap S)$ :

$$\mathcal{B} = \{1, x_3\}.$$

Border basis of  $I(V_{\mathbb{R}}(I) \cap S)$ :

$$\begin{aligned} g_1 &= -1 + \mathbf{x}_1, \\ g_2 &= -x_3 + \mathbf{x}_1 \mathbf{x}_3, \\ g_3 &= -1 + \mathbf{x}_2, \\ g_4 &= -x_3 + \mathbf{x}_2 \mathbf{x}_3, \\ g_5 &= -0.33333 + \mathbf{x}_3^2, \\ g_6 &= x_3 + \mathbf{x}_4, \\ g_7 &= 0.33333 + \mathbf{x}_3 \mathbf{x}_4. \end{aligned}$$

For this example the border basis is in fact a Gröbner basis, e.g., with respect to a graded lexicographic order with  $x_1 \succ x_2 \succ x_4 \succ x_3$ . Note, however, that it is not a reduced Gröbner basis since  $g_2, g_4$ , and  $g_7$  are redundant for this ordering.

Extracted real solutions  $V_{\mathbb{R}}(I) \cap S$ :

$$\begin{aligned} v_1 &= (1, 1, -0.577, 0.577), \\ v_2 &= (1, 1, 0.577, -0.577). \end{aligned}$$

**Example 5.4** This example, Katsura 5, is an example in  $\mathbb{R}^6$  with 32 complex roots, including 12 real roots. It is taken from <http://www.mat.univie.ac.at/neum/glopt/coconut/Benchmark/Library3/katsura5.mod>.

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

**Table 4** Results for Example 5.4

Order $t$	Rank sequence	Extract. order MON/SVD	Accuracy MON/SVD	Comm. error MON/SVD
1	1 7	—	—	—
2	1 6 16	—	—	—
3	1 6 12 12	—/3(3)	—/1.1928e-005	—/2.3073e-007

$$h_6 = 2x_6 + 2x_5 + 2x_4 + 2x_3 + 2x_2 + x_1 - 1.$$

We cannot extract solutions with a monomial base since the multiplication matrices do not commute, but we can extract the following real solutions using an SVD basis:

$$v_1 = (0.277, 0.226, 0.162, 0.0858, 0.0115, -0.124),$$

$$v_2 = (0.59, 0.0422, 0.327, -0.0642, -0.0874, -0.0132),$$

$$v_3 = (1, -2.8e-7, 4.7e-7, 8.81e-7, -2.79e-6, -3.69e-6),$$

$$v_4 = (0.239, 0.0608, -0.0622, -0.0233, 0.186, 0.219),$$

$$v_5 = (0.441, 0.151, 0.0225, 0.219, 0.0935, -0.207),$$

$$v_6 = (0.726, -0.0503, 0.122, 0.164, 0.11, -0.208),$$

$$v_7 = (0.462, 0.309, 0.0553, -0.102, -0.0844, 0.0917),$$

$$v_8 = (0.292, -0.101, 0.181, -0.0591, 0.193, 0.141),$$

$$v_9 = (0.753, 0.0532, 0.191, -0.114, -0.146, 0.139),$$

$$v_{10} = (0.409, -0.0732, 0.0657, -0.127, 0.252, 0.178),$$

$$v_{11} = (0.68, 0.266, -0.154, 0.0323, 0.0897, -0.0735),$$

$$v_{12} = (0.136, 0.0428, 0.0417, 0.0404, 0.0964, 0.211).$$

**Example 5.5** The following example shows the computation of the radical ideal using complex moment matrices:

$$h_1 = x_1^2 + x_2 + x_3 + 1,$$

$$h_2 = x_1 + x_2^2 + x_3 + 1,$$

$$h_3 = x_1 + x_2 + x_3^2 + 1.$$

This ideal is not radical and admits seven solutions, among which the solution  $(-1, -1, -1)$  has multiplicity two. We solve the SDP program based on the set  $K_t^{2\mathbb{C}}$  (thus using *full* complex moment matrices). The rank sequence for full and pruned matrices  $M_s^{\mathbb{C}}(y)$  and  $M_s^{2\mathbb{C}}(y)$  are shown in Table 5.

Monomial basis of  $\mathbb{C}[x]/I(V_{\mathbb{C}}(I))$ :

$$\mathcal{B} = \{1, x_1, x_2, x_3, x_1x_2, x_1x_3, x_2x_3\}.$$

**Table 5** Results for Example 5.5

Order $t$	Rank sequence $M_s^C(y), M_s^{2C}(y)$	Extract. order MON/SVD	Accuracy MON/SVD	Comm. error MON/SVD
1	(1 4), (1 7)	—	—	—
2	(1 4 7), (1 7 7)	—	—	—
3	(1 4 7 7), (1 7 7 7)	3(3)/3(3)	0.0005719/0.00022538	0.00041241/0.00043871

Border basis of  $I(V_C(I))$ :

$$g_1 = 1 + x_2 + x_3 + \mathbf{x}_1^2,$$

$$g_2 = -1 - x_1 + x_2 - x_3 + x_2x_3 + \mathbf{x}_1^2\mathbf{x}_2,$$

$$g_3 = -1 - x_1 - x_2 + x_3 + x_2x_3 + \mathbf{x}_1^2\mathbf{x}_3,$$

$$g_4 = 3.9993 - 0.99984x_1x_2 - 0.99984x_1x_3 - 0.99984x_2x_3 + \mathbf{x}_1\mathbf{x}_2\mathbf{x}_3,$$

$$g_5 = 1 + x_1 + x_3 + \mathbf{x}_2^2,$$

$$g_6 = -1 + x_1 - x_2 - x_3 + x_1x_3 + \mathbf{x}_1\mathbf{x}_2^2,$$

$$g_7 = -1 - x_1 - x_2 + x_3 + x_1x_3 + \mathbf{x}_2^2\mathbf{x}_3,$$

$$g_8 = 1 + x_1 + x_2 + \mathbf{x}_3^2,$$

$$g_9 = -1 + x_1 - x_2 - x_3 + x_1x_2 + \mathbf{x}_1\mathbf{x}_3^2,$$

$$g_{10} = -1 - x_1 + x_2 - x_3 + x_1x_2 + \mathbf{x}_2\mathbf{x}_3^2.$$

Extracted solutions (via the monomial basis):

$$v_1 = (-1 - 8.15e-11i, -1 + 4.37e-11i, -1 - 4.24e-12i) \approx (-1, -1, -1),$$

$$v_2 = (-1.16e-5 + 1.41i, 0.999 - 1.41i, 0.000654 + 1.41i) \approx (\sqrt{2}i, 1 - \sqrt{2}i, \sqrt{2}i),$$

$$v_3 = (-4.8e-5 - 1.41i, 1 + 1.41i, 0.000147 - 1.41i) \approx (-\sqrt{2}i, 1 + \sqrt{2}i, -\sqrt{2}i),$$

$$v_4 = (-9.92e-7 + 1.41i, 0.000713 + 1.41i, 0.999 - 1.41i) \approx (\sqrt{2}i, \sqrt{2}i, 1 - \sqrt{2}i),$$

$$v_5 = (-3.98e-5 - 1.41i, 0.000146 - 1.41i, 1 + 1.41i) \approx (-\sqrt{2}i, -\sqrt{2}i, 1 + \sqrt{2}i),$$

$$v_6 = (1 + 1.41i, -0.000149 - 1.41i, -0.000145 - 1.41i)$$

$$\approx (1 + \sqrt{2}i, -\sqrt{2}i, -\sqrt{2}i),$$

$$v_7 = (1 - 1.41i, 0.000103 + 1.41i, 0.000104 + 1.41i) \approx (1 - \sqrt{2}i, \sqrt{2}i, \sqrt{2}i).$$

For this example (slightly) more accurate solutions:

$$v_1 = (-1 - 2.51e-11i, -1 - 9.85e-11i, -1 - 5.99e-11i),$$

$$\begin{aligned}
v_2 &= (-1.73e-5 + 1.41i, 1 - 1.41i, -1.29e-5 + 1.41i), \\
v_3 &= (-3.78e-5 - 1.41i, 1 + 1.41i, -8.52e-5 - 1.41i), \\
v_4 &= (-2.83e-5 + 1.41i, 4.23e-5 + 1.41i, 1 - 1.41i), \\
v_5 &= (-4e-5 - 1.41i, 3.88e-5 - 1.41i, 1 + 1.41i), \\
v_6 &= (1 + 1.41i, -0.000191 - 1.41i, 6.2e-5 - 1.41i), \\
v_7 &= (1 - 1.41i, -4.61e-5 + 1.41i, 0.000104 + 1.41i),
\end{aligned}$$

could be obtained by means of the SVD-method.

## 6 Concluding Remarks

In this paper we have provided a new semidefinite characterization of the real radical ideal of an ideal  $I \subseteq \mathbb{R}[x]$  as well as an algorithm to compute all (finitely many) points of  $V_{\mathbb{R}}(I)$  and a set of generators (or a Gröbner base) of  $I(V_{\mathbb{R}}(I))$ . The main feature of our approach is its real algebraic nature as it avoids considering complex zeros, and does not need to compute a Gröbner base of  $I$ . An essential step in our algorithm consists in solving the semidefinite program (4.9). Thus our algorithm is numerical.

Let us briefly mention the *numerical* versus *numeric-symbolic* (or *arbitrary precision*) issue. Some advocate that only computation with arbitrary or guaranteed precision should be permitted while others admit some numerical imprecision; see, e.g., Revol and Rouillier [34], Stetter [39]. Clearly, being numerical in nature, the algorithm of the present paper admits some intrinsic numerical imprecision, no matter how good the SDP software packages are (or will be). At this stage, the only answer we propose in this ‘approximate vs. exact’ debate is to validate or invalidate the method by experiments. For instance, on a significant sample, compute  $J \approx I(V_{\mathbb{R}}(I))$  with our method and check afterwards by symbolic methods if  $V_{\mathbb{C}}(J) = V_{\mathbb{R}}(I)$ . On the other hand, the present algorithm is rather intended to illustrate that the new semidefinite characterizations of  $V_{\mathbb{R}}(I)$  and  $I(V_{\mathbb{R}}(I))$  are directly implementable in a relatively simple manner; clearly, its numerical features (like precision and stability) need further investigations beyond the scope of the present paper.

**Acknowledgements** We are very grateful to two referees for their careful reading and their many useful suggestions that helped us improve the presentation of the paper. In particular, we thank a referee for pointing out to us that the method can also detect the nonexistence of (real) solutions. We also thank Etienne de Klerk for helpful discussions on the self-dual embedding technique for semidefinite programming and Johan Löfberg for his support with Yalmip.

J.-B. Lasserre was supported by the French National Research Agency ANR under grant NT05-3-41612. M. Laurent was supported by The Netherlands Organization for Scientific Research grant NWO 639.032.203, and by ADONET, Marie Curie Research Training Network MRTN-CT-2003-504438.

## References

1. E. Becker and R. Neuhaus, Computation of real radicals of polynomial ideals, in *Computational Algebraic Geometry* (F. Eyssette and A. Galligo, eds.), Progress in Mathematics, Vol. 109, pp. 1–20, Birkhäuser, Boston, 1993.

2. E. Becker and J. Schmid, On the real Nullstellensatz, in *Algorithmic Algebra and Number Theory* (B. H. Matzat, G.-M. Greuel, G. Hiss, eds.), pp. 173–185, Springer, New York, 1997.
3. E. Becker and T. Wörmann, Radical computations of zero-dimensional ideals and real root counting, *Math. Comput. Simul.*, **42** (1996), 561–569.
4. F. Bihan, J. M. Rojas, and C. E. Stella, First steps in algorithmic fewnomial theory, 2004. Available from <http://www.arxiv.org/abs/math/0411107>.
5. F. Bihan and F. Sottile, New fewnomial upper bounds from Gale dual polynomial systems, *Moscow Math. J.*, **7**(3) (2007).
6. D. Bini and B. Mourrain, Polynomial test suite, 1996. Available from <http://www-sop.inria.fr/saga/POL>.
7. J. Bochnak, M. Coste, and M.-F. Roy, *Géométrie Algébrique Réelle*, Springer, New York, 1987.
8. M. Caboara, P. Conti, and C. Traverso, Yet another ideal decomposition algorithm, in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Lecture Notes in Computer Science, Vol. 1255, pp. 39–54, Springer, Berlin, 1997.
9. P. Conti and C. Traverso, Algorithms for the real radical, Preprint, 1998.
10. D. Cox, J. Little, and D. O’Shea, *Ideals, Varieties and Algorithms*, Springer, New York, 1997.
11. D. Cox, J. Little, and D. O’Shea, *Using Algebraic Geometry*, Springer, New York, 1998.
12. R. Curto and L. Fialkow, Solution of the truncated complex moment problem for flat data, *Mem. Amer. Math. Soc.* **119**(568) (1996).
13. R. Curto and L. Fialkow, The truncated complex  $K$ -moment problem, *Trans. Amer. Math. Soc.* **352** (2000), 2825–2855.
14. R. Curto and L. Fialkow, Solution of the singular quartic moment problem, *J. Oper. Theory* **48** (2002), 315–354.
15. E. de Klerk, *Aspects of Semidefinite Programming—Interior Point Algorithms and Selected Applications*, Kluwer Academic, Amsterdam, 2002.
16. A. Dickstein and I. Z. Emiris (eds.), *Solving Polynomial Equations: Foundations, Algorithms, and Applications*, Algorithms and Computation in Mathematics, Vol. 14, Springer, Berlin, 2005.
17. D. Eisenbud, C. Huneke, and W. Vasconcelos, Direct methods for primary decompositions, *Invent. Math.* **110** (1992), 207–235.
18. G.-M. Greuel, G. Pfister, and H. Schönemann, Singular 3.0. A computer algebra system for polynomial computations, Centre for Computer Algebra, University of Kaiserslautern, 2005. Available from <http://www.singular.uni-kl.de>.
19. P. Gianni, B. Trager, and G. Zacharias, Gröbner bases and primary decomposition of polynomial ideals, *J. Symb. Comput.* **6** (1988), 149–167.
20. D. Goldfarb and K. Scheinberg, Interior point trajectories in semidefinite programming, *SIAM J. Optim.* **8** (1998), 871–886.
21. D. Henrion and J. B. Lasserre, Detecting global optimality and extracting solutions in gloptiPoly, in *Positive Polynomials in Control* (D. Henrion and A. Garulli, eds.), Lectures Notes in Control and Information Sciences, Vol. 312, pp. 293–310, Springer, New York, 2005.
22. A. G. Khovanski, *Fewnomials*, Am. Math. Soc., Providence, 1991.
23. T. Krick and A. Logar, An algorithm for the computation of the radical of an ideal in the ring of polynomials, in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (New Orleans, LA, 1991), Lecture Notes in Computer Science, Vol. 539, pp. 195–205, Springer, Berlin, 1991.
24. Y. N. Lakshman and D. Lazard, On the complexity of zero-dimensional algebraic systems, in *Effective Methods in Algebraic Geometry* (T. Mora and C. Traverso, eds.), Progress in Mathematics, Vol. 94, pp. 217–226, Birkhäuser, Boston, 1991.
25. J. B. Lasserre, Global optimization with polynomials and the problem of moments, *SIAM J. Optim.* **11** (2001), 796–817.
26. J. B. Lasserre, A moment approach to analyze zeros of triangular polynomial sets, *Trans. Amer. Math. Soc.* **358** (2006), 1403–1420.
27. M. Laurent, Revisiting two theorems of Curto and Fialkow, *Proc. Amer. Math. Soc.* **133**(10) (2005), 2965–2976.
28. M. Laurent, Semidefinite representations for finite varieties, *Math. Program.* **109** (2007), 1–26.
29. M. Laurent, Moment matrices and optimization over polynomials—A survey on selected topics, Preprint, 2005. Available from <http://homepages.cwi.nl/~monique/>.
30. J. Löfberg, YALMIP: A toolbox for modeling and optimization in MATLAB, in *Proceedings of CACSD*, Taipei, Taiwan, 2004. Available from <http://control.ee.ethz.ch/~joloef/yalmip.php>.



31. B. Mourrain, A new criterion for normal form algorithms, in *Proc. Conf. AAECC-13, Honolulu, 1999* (M. Fossorier et al., eds.), Lecture Notes in Computer Science, Vol. 1719, pp. 431–443, Springer, Berlin, 1999.
32. P. Pedersen, M.-F. Roy, and A. Szpirglas, Counting real zeros in the multivariate case, in *Computational Algebraic Geometry* (F. Eyssette, A. Galligo, eds.), Progress in Mathematics, Vol. 109, pp. 203–224, Birkhäuser, Boston, 1993.
33. G. Reid and L. Zhi, Solving nonlinear polynomial system via symbolic-numeric elimination method, in *Proceedings of the International Conference on Polynomial System Solving*, 2004.
34. N. Revol and F. Rouillier, Motivations for an arbitrary precision interval arithmetic and the MPFI library, *Reliable Comput.* **11** (2005), 1–16.
35. F. Rouillier, Solving zero-dimensional systems through the rational univariate representation, *J. Appl. Algebra Eng. Commun. Comput.* **9** (1999), 433–461.
36. A. Seidenberg, Constructions in algebra, *Trans. Amer. Math. Soc.* **197** (1974), 273–313.
37. A. J. Sommese and C. W. Wampler, *The Numerical Solution of Systems of Polynomials Arising in Engineering and Science*, World Scientific, Singapore, 2005.
38. G. Stengle, A Nullstellensatz and a Positivstellensatz in semialgebraic geometry, *Math. Ann.* **207** (1974), 87–97.
39. H.J. Stetter, *Numerical Polynomial Algebra*, SIAM, Philadelphia, 2004.
40. J. F. Sturm, Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones, *Optim. Methods Softw.* **11/12** (1999), 625–653. Special issue on Interior Point Methods (CD supplement with software).
41. J. F. Sturm, Implementation of interior point methods for mixed semidefinite and second order cone optimization problems, *Optim. Methods Softw.* **17**(6) (2002), 1105–1154.
42. L. Vandenberghe and S. Boyd, Semidefinite programming, *SIAM Rev.* **38**(1) (1996), 49–95.
43. J. Verschelde, Algorithm 795: PHCpack: A general-purpose solver for polynomial systems by homotopy continuation, *ACM Trans. Math. Softw.* **25**(2) (1999), 251–276.
44. J. Verschelde and K. Gatermann, Symmetric Newton polytopes for solving sparse polynomial systems, *Adv. Appl. Math.* **16**(1) (1995), 95–127.
45. H. Wolkowicz, R. Saigal, and L. Vandenberghe (eds.), *Handbook of Semidefinite Programming*, Kluwer Academic, Boston, 2000.