Moment Matrices, Border Bases and Real Radical Computation

Jean-Bernard Lasserre, Monique Laurent, Bernard Mourrain, Philipp Rostalski, Philippe Trébuchet

MOMENT MATRICES, BORDER BASES AND REAL RADICAL COMPUTATION

J.B. LASSERRE, M. LAURENT, B. MOURRAIN, PH. ROSTALSKI, AND PH. TRÉBUCHET

Abstract. In this paper, we describe new methods to compute the radical (resp. real radical) of an ideal, assuming it complex (resp. real) variety is finte. The aim is to combine approaches for solving a system of polynomial equations with dual methods which involve moment matrices and semi-definite programming. While the border basis algorithms of [17] are efficient and numerically stable for computing complex roots, algorithms based on moment matrices [12] allow the incorporation of additional polynomials, e.g., to restrict the computation to real roots or to eliminate multiple solutions. The proposed algorithm can be used to compute a border basis of the input ideal and, as opposed to other approaches, it can also compute the quotient structure of the (real) radical ideal directly, i.e., without prior algebraic techniques such as Gröbner bases. It thus combines the strength of existing algorithms and provides a unified treatment for the computation of border bases for the ideal, the radical ideal and the real radical ideal.

1. Introduction

Many problems in mathematics and science can be reduced to the task of solving zero-dimensional systems of polynomials. Existing methods for this task often compute all (real and complex) roots. However, often only real solutions are significant and one needs to sieve out all complex solutions afterwards in a separate step.

Typical approaches in this vein are the efficient homotopy continuation methods in the spirit of [21], [19], recursive intersection techniques using rational univariate representation [9] in the spirit of Kronecker's work [11], Gröbner basis approaches using eigenvector computations or rational univariate representation [5], [18], [8, chap. 4]. In the latter methods, emphasis is put on exact input and computation. Using a different approach, Mourrain and Trébuchet [17] have proposed an efficient numerical algorithm that uses border bases and the concept of *rewriting family*. In particular, in the course of this algorithm, a distinguishing and remarkable feature is a careful selection strategy for monomials serving as candidates for elements in a basis of the quotient space $\mathbb{K}[\mathbf{x}]/I$ (if $I \subset \mathbb{K}[\mathbf{x}]$ is the ideal generated by the polynomials defining the equations). As a result, at each iteration of the procedure, the candidate basis for the quotient space $\mathbb{K}[\mathbf{x}]/I$ contains only a small number of monomials (those associated with a certain *rewriting family*). Another nice feature of this approach (and in contrast with Gröbner base approaches) is its robustness with respect to perturbation of coefficients in the original system.

On the other hand, Lasserre et al. [12] have proposed an alternative numerical method, real algebraic in nature, to directly compute all real zeros *without* computing any complex zero. This approach uses well established semi-definite programming techniques and numerical linear algebra. Remarkably, all information needed is contained in the so-called quasi-Hankel *moment matrix* with rows and columns indexed by the canonical monomial basis of $\mathbb{K}[\mathbf{x}]_d$. Its entries depend on the polynomials generating the ideal I and the underlying geometry when this matrix is required to be positive semi-definite with maximum rank. A drawback of this approach is the potentially large size of the positive semi-definite moment matrices to handle in the course of the algorithm. Indeed, when the total degree is increased from d to $d+1$, the

new moment matrix to consider has its rows and columns indexed by the canonical (monomial) basis of $\mathbb{K}[\mathbf{x}]_{d+1}$.

The goal of this paper is to combine a main feature of the border basis algorithm of [17] (namely its careful selection of monomials, considered as candidates in a basis of the quotient space $\mathbb{K}[\mathbf{x}]/I$) with the semi-definite approach of [12] for computing real zeros and an approach for computing the radical ideal inspired by [10].

The main contribution of this paper is to describe a new algorithm which incorporates in the border basis algorithm the positive semi-definiteness constraint of the moment matrix, which are much easier to handle than the relaxation method of [12]. We show the termination of the computation in the case where the real radical is zero-dimensional (even in cases where the ideal is not zero-dimensional). A variant of the approach is also proposed, which yields a new algorithm to compute the (complex) radical for zero-dimensional ideals.

In this new algorithm, the rows and columns involved in the semi-definite programming problem are associated with the family of monomials (candidates for being in a basis of the quotient space) and its border, i.e., a subset of monomials much smaller than the canonical (monomial) basis of $\mathbb{R}[\mathbf{x}]_d$ considered in [12]. As a result, the (crucial) positive semi-definiteness constraint is much easier to handle and solving problem instances of size much larger than those in [12] can now be envisioned. A preliminary implementation of this new algorithm validate experimentally these improvements on few benchmarks problems.

The approach differs from previous techniques such as [1] which involve complex radical computation and factorisation or reduction to univariate polynomials, in that the new polynomials needed to describe the real radical are computed directly from the input polynomials, using SDP techniques.

The paper is organized as follows. Section 2 recalls the ingredients and properties involved in the algebraic computation. Section 3 describes duality tools and Hankel operators involved in the computation of (real) radical of ideals. In Section 4, we analyse the properties of the truncated Hankel operators. In section 5, we describe the real radical and radical algorithms and prove their correctness in section 6. Finally, Section 7 contains some illustrative examples and experimentation results of a preliminary implementation.

2. Polynomials, dual space and quotient algebra

In this section, we set our notation and recall the eigenvalue techniques for solving polynomial equations and the border basis method. These results will be used for showing the termination of the radical border basis algorithm.

2.1. **Ideals and varieties.** Let $\mathbb{K}[\mathbf{x}]$ be the set of the polynomials in the variables $\mathbf{x} = (x_1, \ldots, x_n)$, with coefficients in the field $\mathbb{K}$. Hereafter, we will choose[1] $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$. Let $\overline{\mathbb{K}}$ denotes the algebraic closure of $\mathbb{K}$. For $\alpha \in \mathbb{N}^n$, $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ is the monomial with exponent α and degree $|\alpha| = \sum_i \alpha_i$. The set of all monomials in $\mathbf{x}$ is denoted $\mathcal{M} = \mathcal{M}(\mathbf{x})$. We say that $\mathbf{x}^\alpha \leq \mathbf{x}^\beta$ if $\mathbf{x}^\alpha$ divides $\mathbf{x}^\beta$, i.e., if $\alpha \leq \beta$ coordinate-wise. For a polynomial $f = \sum_\alpha f_\alpha \mathbf{x}^\alpha$, its support is $\mathrm{supp}(f) := \{\mathbf{x}^\alpha \mid f_\alpha \neq 0\}$, the set of monomials occurring with a nonzero coefficient in f.

For $t \in \mathbb{N}$ and $S \subseteq \mathbb{K}[\mathbf{x}]$, we introduce the following sets:

- S_t is the set of elements of S of degree $\leq t$,
- $S_{[t]}$ is the set of element of S of degree exactly t,
- $\langle S \rangle = \left\{ \sum_{f \in S} \lambda_f f \mid f \in S, \lambda_f \in \mathbb{K} \right\}$ is the linear span of S,
- $(S) = \left\{ \sum_{f \in S} p_f f \mid p_f \in \mathbb{K}[\mathbf{x}], f \in S \right\}$ is the ideal in $\mathbb{K}[\mathbf{x}]$ generated by S,

[1]For notational simplicity, we will consider only these two fields in this paper, but $\mathbb{R}$ and $\mathbb{C}$ can be replaced respectively by any real closed field and any field containing its algebraic closure)

- $\langle S \,|\, t\rangle = \left\{ \sum_{f\in S_t} p_f\, f \mid p_f \in \mathbb{K}[\mathbf{x}]_{t-\deg(f)} \right\}$ is the vector space spanned by $\{\mathbf{x}^\alpha f \mid f \in S_t, |\alpha| \leq t - \deg(f)\}$,
- $S^+ := S \cup x_1 S \cup \ldots \cup x_n S$ is the prolongation of S by one degree,
- $\partial S := S^+ \setminus S$ is the border of S,
- $S^{[t]} := S^{\overbrace{+\cdots+}^{t \text{ times}}}$ is the result of applying t times the prolongation operator '$+$' on S, with $S^{[1]} = S^+$ and, by convention, $S^{[0]} = S$.

Therefore, $S_t = S \cap \mathbb{K}[\mathbf{x}]_t$, $S_{[t]} = S \cap \mathbb{K}[\mathbf{x}]_{[t]}$, $S^{[t]} = \{x^\alpha f \mid f \in S, |\alpha| \leq t\}$, $\langle S \,|\, t\rangle \subseteq (S) \cap \mathbb{K}[\mathbf{x}]_t = (S)_t$, but the inclusion may be strict.

If $\mathcal{B} \subseteq \mathcal{M}$ contains 1 then, for any monomial $m \in \mathcal{M}$, there exists an integer k for which $m \in \mathcal{B}^{[k]}$. The *$\mathcal{B}$-index* of m, denoted by $\delta_{\mathcal{B}}(m)$, is defined as the smallest integer k for which $m \in \mathcal{B}^{[k]}$.

A set of monomials $\mathcal{B}$ is said to be *connected to* 1 if $1 \in \mathcal{B}$ and for every monomial $m \neq 1$ in $\mathcal{B}$, $m = x_{i_0} m'$ for some $i_0 \in [1, n]$ and $m' \in \mathcal{B}$.

Given a vector space $E \subseteq \mathbb{K}[\mathbf{x}]$, its prolongation $E^+ := E + x_1 E + \ldots + x_n E$ is again a vector space.

The vector space E is said to be *connected to 1* if $1 \in E$ and any non-constant polynomial $p \in E$ can be written as $p = p_0 + \sum_{i=1}^n x_i p_i$ for some polynomials $p_0, p_i \in E$ with $\deg(p_0) \leq \deg(p)$, $\deg(p_i) \leq \deg(p) - 1$ for $i \in [1, n]$. Obviously, E is connected to 1 when $E = \langle \mathcal{C} \rangle$ for some monomial set $\mathcal{C} \subseteq \mathcal{M}$ which is connected to 1. Moreover, $E^+ = \langle \mathcal{C}^+ \rangle$ if $E = \langle \mathcal{C} \rangle$.

Given an ideal $I \subseteq \mathbb{K}[\mathbf{x}]$ and a field $\mathbb{L} \supseteq \mathbb{K}$, we denote by

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

its associated variety in $\mathbb{L}^n$. By convention $V(I) = V_{\overline{\mathbb{K}}}(I)$. For a set $V \subseteq \mathbb{K}^n$, we define its vanishing ideal

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

Furthermore, we denote by

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

the radical of I.

For $\mathbb{K} = \mathbb{R}$, we have $V(I) = V_{\mathbb{C}}(I)$, but one may also be interested in the subset of real solutions, namely the real variety $V_{\mathbb{R}}(I) = V(I) \cap \mathbb{R}^n$. The corresponding vanishing ideal is $I(V_{\mathbb{R}}(I))$ and the *real radical ideal* is

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

Obviously,

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

An ideal I is said to be *radical* (resp., *real radical*) if $I = \sqrt{I}$ (resp. $I = \sqrt[\mathbb{R}]{I}$). Obviously, $I \subseteq I(V(I)) \subseteq I(V_{\mathbb{R}}(I))$. Hence, if $I \subseteq \mathbb{R}[\mathbf{x}]$ is real radical, then I is radical and moreover, $V(I) = V_{\mathbb{R}}(I) \subseteq \mathbb{R}^n$ if $|V_{\mathbb{R}}(I)| < \infty$.

The following two famous theorems relate vanishing and radical ideals:

Theorem 2.1.

(i) **Hilbert's Nullstellensatz** *(see, e.g.,* [6, §4.1]*)* $\sqrt{I} = I(V_{\mathbb{C}}(I))$ *for an ideal* $I \subseteq \mathbb{C}[\mathbf{x}]$.
(ii) **Real Nullstellensatz** *(see, e.g.,* [3, §4.1]*)* $\sqrt[\mathbb{R}]{I} = I(V_{\mathbb{R}}(I))$ *for an ideal* $I \subseteq \mathbb{R}[\mathbf{x}]$.

2.2. **The quotient algebra.** Given an ideal $I \subseteq \mathbb{K}[\mathbf{x}]$, the quotient set $\mathbb{K}[\mathbf{x}]/I$ consists of all cosets $[f] := f + I = \{f + q \mid q \in I\}$ for $f \in \mathbb{K}[\mathbf{x}]$, i.e., all equivalent classes of polynomials of $\mathbb{K}[\mathbf{x}]$ modulo the ideal I. The quotient set $\mathbb{K}[\mathbf{x}]/I$ is an algebra with addition $[f]+[g] := [f+g]$, scalar multiplication $\lambda[f] := [\lambda f]$ and with multiplication $[f][g] := [fg]$, for $\lambda \in \mathbb{R}$, $f, g \in \mathbb{K}[\mathbf{x}]$.

A useful property is that, when I is zero-dimensional (i.e., $|V_{\overline{\mathbb{K}}}(I)| < \infty$) then $\mathbb{K}[\mathbf{x}]/I$ is a finite-dimensional vector space and its dimension is related to the cardinality of $V(I)$, as indicated in Theorem 2.2 below.

Theorem 2.2. *Let I be an ideal in $\mathbb{K}[\mathbf{x}]$. Then $|V_{\overline{\mathbb{K}}}(I)| < \infty \Longleftrightarrow \dim \mathbb{K}[\mathbf{x}]/I < \infty$. Moreover, $|V_{\overline{\mathbb{K}}}(I)| \leq \dim\ \mathbb{K}[\mathbf{x}]/I$, with equality if and only if I is radical.*

A proof of this theorem and a detailed treatment of the quotient algebra $\mathbb{K}[\mathbf{x}]/I$ can be found e.g., in [6], [8], [20].

Assume $|V_{\overline{\mathbb{K}}}(I)| < \infty$ and set $N := \dim \mathbb{K}[\mathbf{x}]/I$, $|V_{\overline{\mathbb{K}}}(I)| \leq N < \infty$. Consider a set $\mathcal{B} := \{b_1, \ldots, b_N\} \subseteq \mathbb{K}[\mathbf{x}]$ for which $\{[b_1], \ldots, [b_N]\}$ is a basis of $\mathbb{K}[\mathbf{x}]/I$; by abuse of language we also say that $\mathcal{B}$ itself is a basis of $\mathbb{K}[\mathbf{x}]/I$. Then every $f \in \mathbb{K}[\mathbf{x}]$ 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 $\pi_{I,\mathcal{B}}(f) := \sum_{i=1}^N c_i b_i$ is called the remainder of f modulo I, or its *normal form*, with respect to the basis $\mathcal{B}$. In other words, $\langle \mathcal{B} \rangle$ and $\mathbb{K}[\mathbf{x}]/I$ are isomorphic vector spaces.

2.2.1. *Multiplication operators.* Given a polynomial $h \in \mathbb{K}[\mathbf{x}]$, we can define the *multiplication (by h) operator* as

$$\begin{array}{rccc} \mathcal{X}_h : & \mathbb{K}[\mathbf{x}]/I & \longrightarrow & \mathbb{K}[\mathbf{x}]/I \\ & [f] & \longmapsto & \mathcal{X}_h([f]) := [hf]\,, \end{array} \tag{1}$$

Assume that $N := \dim \mathbb{K}[\mathbf{x}]/I < \infty$. Then the multiplication operator $\mathcal{X}_h$ can be represented by its matrix, again denoted $\mathcal{X}_h$ for simplicity, with respect to a given basis $\mathcal{B} = \{b_1, \ldots, b_N\}$ of $\mathbb{K}[\mathbf{x}]/I$.

Namely, setting $\pi_{I,\mathcal{B}}(hb_j) := \sum_{i=1}^N a_{ij} b_i$ for some scalars $a_{ij} \in \mathbb{K}$, the jth column of $\mathcal{X}_h$ is the vector $(a_{ij})_{i=1}^N$. Define the vector $\zeta_{\mathcal{B},v} := (b_j(v))_{j=1}^N \in \overline{\mathbb{K}}^N$, whose coordinates are the evaluations of the polynomials $b_j \in \mathcal{B}$ at the point $v \in \overline{\mathbb{K}}^n$. The following famous result (see e.g., [5, Chapter 2§4], [8]) relates the eigenvalues of the multiplication operators in $\mathbb{K}[\mathbf{x}]/I$ to the algebraic variety $V(I)$. This result underlies the so-called eigenvalue method for solving polynomial equations and plays a central role in many algorithms, also in the present paper.

Theorem 2.3. *Let I be a zero-dimensional ideal in $\mathbb{K}[\mathbf{x}]$, $\mathcal{B}$ a basis of $\mathbb{K}[\mathbf{x}]/I$, and $h \in \mathbb{K}[\mathbf{x}]$. The eigenvalues of the multiplication operator $\mathcal{X}_h$ are the evaluations $h(v)$ of the polynomial h at the points $v \in V(I)$. Moreover, $(\mathcal{X}_h)^T \zeta_{\mathcal{B},v} = h(v)\zeta_{\mathcal{B},v}$ and the set of common eigenvectors of $(\mathcal{X}_h)_{h \in \mathbb{K}[\mathbf{x}]}$ are up to a non-zero scalar multiple the vectors $\zeta_{\mathcal{B},v}$ for $v \in V(I)$.*

Throughout the paper we also denote by $\mathcal{X}_i := \mathcal{X}_{x_i}$ the matrix of the multiplication operator by the variable x_i. By the above theorem, the eigenvalues of the matrices $\mathcal{X}_i$ are the ith coordinates of the points $v \in V(I)$. Thus the task of solving a system of polynomial equations is reduced to a task of numerical linear algebra once a basis of $\mathbb{K}[\mathbf{x}]/I$ and a normal form algorithm are available, permitting the construction of the multiplication matrices $\mathcal{X}_i$.

2.3. **Border bases.** The eigenvalue method for solving polynomial equations from the above section requires the knowledge of a basis of $\mathbb{K}[\mathbf{x}]/I$ and an algorithm to compute the normal form of a polynomial with respect to this basis. In this section we will recall a general method for obtaining such a basis and a method to reduce polynomials to their normal form.

Throughout $\mathcal{B} \subseteq \mathcal{M}$ is a finite set of monomials.

Definition 2.4. *A rewriting family F for a (monomial) set $\mathcal{B}$ is a set of polynomials $F = \{f_i\}_{i \in \mathcal{I}}$ such that*

- $\mathrm{supp}(f_i) \subseteq \mathcal{B}^+$,
- *f_i has exactly* **one** *monomial in $\partial\mathcal{B}$, denoted as $\gamma(f_i)$ and called the leading monomial of f_i. (The polynomial f_i is normalized so that the coefficient of $\gamma(f_i)$ is 1.)*
- *if $\gamma(f_i) = \gamma(f_j)$ then $i = j$.*

Definition 2.5. *We say that the rewriting family F is* graded *if $\deg(\gamma(f)) = \deg(f)$ for all $f \in F$.*

Definition 2.6. *A rewriting family F for $\mathcal{B}$ is said to be* complete *in degree t if it is graded and satisfies $(\partial\mathcal{B})_t \subseteq \gamma(F)$; that is, each monomial $m \in \partial\mathcal{B}$ of degree at most t is the leading monomial of some (necessarily unique) $f \in F$.*

Definition 2.7. *Let F be a rewriting family for $\mathcal{B}$, complete in degree t. Let $\pi_{F,\mathcal{B}}$ be the projection on $\langle\mathcal{B}\rangle$ along F defined recursively on the monomials $m \in \mathcal{M}_t$ in the following way:*

- *if $m \in \mathcal{B}_t$, then $\pi_{F,\mathcal{B}}(m) = m$,*
- *if $m \in (\partial\mathcal{B})_t$ $(= (\mathcal{B}^{[1]} \setminus \mathcal{B}^{[0]})_t)$, then $\pi_{F,\mathcal{B}}(m) = m - f$, where f is the (unique) polynomial in F for which $\gamma(f) = m$,*
- *if $m \in (\mathcal{B}^{[k]} \setminus \mathcal{B}^{[k-1]})_t$ for some integer $k \geq 2$, write $m = x_{i_0} m'$, where $m' \in \mathcal{B}^{[k-1]}$ and $i_0 \in [1, n]$ is the smallest possible variable index for which such a decomposition exists, then $\pi_{F,\mathcal{B}}(m) = \pi_{F,\mathcal{B}}(x_{i_0}\, \pi_{F,\mathcal{B}}(m'))$.*

One can easily verify that $\deg(\pi_{F,\mathcal{B}}(m)) \leq \deg(m)$ for $m \in \mathcal{M}_t$. The map $\pi_{F,\mathcal{B}}$ extends by linearity to a linear map from $\mathbb{K}[\mathbf{x}]_t$ onto $\langle\mathcal{B}\rangle_t$. By construction, $f = \gamma(f) - \pi_{F,\mathcal{B}}(\gamma(f))$ and $\pi_{F,\mathcal{B}}(f) = 0$ for all $f \in F_t$. The next theorems show that, under some natural commutativity condition, the map $\pi_{F,\mathcal{B}}$ coincides with the linear projection from $\mathbb{K}[\mathbf{x}]_t$ onto $\langle\mathcal{B}\rangle_t$ along the vector space $\langle F \,|\, t\rangle$, and they introduce the notion of border bases.

Definition 2.8. *Let $\mathcal{B} \subset \mathcal{M}$ be connected to 1. A family $F \subset \mathbb{K}[\mathbf{x}]$ is a border basis for $\mathcal{B}$ if it is a rewriting family for $\mathcal{B}$, complete in all degrees, and such that $\mathbb{K}[\mathbf{x}] = \langle\mathcal{B}\rangle \oplus (F)$.*

An algorithmic way to check that we have a border basis is based on the following result, that we recall from [17]:

Theorem 2.9. *Assume that $\mathcal{B}$ is connected to 1 and let F be a rewriting family for $\mathcal{B}$, complete in degree $t \in \mathbb{N}$. Suppose that, for all $m \in \mathcal{M}_{t-2}$,*

$$\pi_{F,\mathcal{B}}(x_i\, \pi_{F,\mathcal{B}}(x_j\, m)) = \pi_{F,\mathcal{B}}(x_j\, \pi_{F,\mathcal{B}}(x_i\, m)) \quad \text{for all } i, j \in [1, n]. \tag{2}$$

Then $\pi_{F,\mathcal{B}}$ coincides with the linear projection of $\mathbb{K}[\mathbf{x}]_t$ on $\langle\mathcal{B}\rangle_t$ along the vector space $\langle F \,|\, t\rangle$; that is, $\mathbb{K}[\mathbf{x}]_t = \langle\mathcal{B}\rangle_t \oplus \langle F \,|\, t\rangle$.

Proof. Equation (2) implies that any choice of decomposition of $m \in \mathcal{M}_t$ as a product of variables yields the same result after applying $\pi_{F,\mathcal{B}}$. Indeed, let $m = x_{i_1} m' = x_{i_2} m''$ with $i_1 \neq i_2$ and $m', m'' \in \mathcal{M}_{t-1}$. Then there exists $m''' \in \mathcal{M}_{t-2}$ such that $m' = x_{i_2} m'''$, $m'' = x_{i_1} m'''$. By the relation (2) we have:

$$\begin{aligned} & \pi_{F,\mathcal{B}}(x_{i_1}\, \pi_{F,\mathcal{B}}(m')) \\ = \;& \pi_{F,\mathcal{B}}(x_{i_1}\, \pi_{F,\mathcal{B}}(x_{i_2} m''')) = \pi_{F,\mathcal{B}}(x_{i_2}\, \pi_{F,\mathcal{B}}(x_{i_1} m''')) \\ = \;& \pi_{F,\mathcal{B}}(x_{i_2}\, \pi_{F,\mathcal{B}}(m'')). \end{aligned}$$

Let us prove by induction on $l = \deg(m)$ that for a monomial $m = x_{i_1} \cdots x_{i_l} \in \mathcal{M}_t$,

$$\pi_{F,\mathcal{B}}(m) = \pi_{F,\mathcal{B}}(x_{i_1} \pi_{F,\mathcal{B}}(x_{i_1} \cdots \pi_{F,\mathcal{B}}(x_{i_l}) \cdots)), \tag{3}$$

does not depend on the order in which we take the monomials in the decomposition $m = x_{i_1} \cdots x_{i_l}$:

- Either $m \in \mathcal{B}$. As $\mathcal{B}$ is connected to 1, there exists $i' \in [1, n]$ and $m' \in \mathcal{B}_{t-1}$ such that $m = \pi_{F,\mathcal{B}}(m) = \pi_{F,\mathcal{B}}(x_{i'} m') = \pi_{F,\mathcal{B}}(x_{i'}\, \pi_{F,\mathcal{B}}(m'))$, from which we deduce (3) using the induction hypothesis applied to m' and relation (2).

- Or $m \notin \mathcal{B}$. Then, by definition of $\pi_{F,\mathcal{B}}$, there exists $i' \in [1,n]$ and $m' \in \mathcal{M}_{t-1}$ such that $\pi_{F,\mathcal{B}}(m) = \pi_{F,\mathcal{B}}(x_{i'}\,\pi_{F,\mathcal{B}}(m'))$, from which we deduce (3) in a similar way using the induction hypothesis applied to m' and relation (2).

The map $\pi_{F,\mathcal{B}}$ defines a projection of $\mathbb{K}[\mathbf{x}]_t$ on $\langle\mathcal{B}\rangle_t$. It suffices now to show that $\operatorname{Ker}\pi_{F,\mathcal{B}} = \langle F \,|\, t\rangle$. First we show that $m - \pi_{F,\mathcal{B}}(m) \in \langle F \,|\, s\rangle$ for all $m \in \mathcal{M}_s$, using induction on $s = 0,\dots,t$. The base case $s = 0$ is obvious; indeed $\pi_{F,\mathcal{B}}(1) = 1$ since $1 \in \mathcal{B}$, and $0 \in \langle F \,|\, 0\rangle$. Consider $m \in \mathcal{M}_{s+1}$. Write $m = x_{i_0}m'$ where $m' \in \mathcal{M}_s$ and $\pi_{F,\mathcal{B}}(m) = \pi_{F,\mathcal{B}}(x_{i_0}\pi_{F,\mathcal{B}}(m'))$ (recall Definition 2.7). We have:

$$m - \pi_{F,\mathcal{B}}(m) = \underbrace{x_{i_0}(m' - \pi_{F,\mathcal{B}}(m'))}_{:=q} + \underbrace{x_{i_0}\pi_{F,\mathcal{B}}(m') - \pi_{F,\mathcal{B}}(x_{i_0}\pi_{F,\mathcal{B}}(m'))}_{:=r}.$$

By the induction assumption, $m' - \pi_{F,\mathcal{B}}(m') \in \langle F \,|\, s\rangle$ and thus $q \in \langle F \,|\, s+1\rangle$. Write $\pi_{F,\mathcal{B}}(m') = \sum_{b\in\mathcal{B}_s} \lambda_b b$ ($\lambda_b \in \mathbb{K}$). Then, $r = \sum_{b\in\mathcal{B}_s} \lambda_b(x_{i_0}b - \pi_{F,\mathcal{B}}(x_{i_0}b))$, where $x_{i_0}b - \pi_{F,\mathcal{B}}(x_{i_0}b) = 0$ if $x_{i_0}b \in \mathcal{B}$, and $x_{i_0}b - \pi_{F,\mathcal{B}}(x_{i_0}b)$ is a polynomial of F_{s+1} otherwise. This implies $r \in \langle F \,|\, s+1\rangle$ and thus $m - \pi_{F,\mathcal{B}}(m) \in \langle F \,|\, s+1\rangle$. Thus we have shown that $\mathbb{K}[\mathbf{x}]_t = \langle\mathcal{B}\rangle_t + \langle F \,|\, t\rangle$. Next, observe that $\langle F \,|\, t\rangle \subseteq \operatorname{Ker}\pi_{F,\mathcal{B}}$, which follows from the fact that $F_t \subseteq \operatorname{Ker}\pi_{F,\mathcal{B}}$ together with (3). This implies that $\langle\mathcal{B}\rangle_t \cap \langle F \,|\, t\rangle = \{0\}$ and thus the equality $\langle F \,|\, t\rangle = \operatorname{Ker}\pi_{F,\mathcal{B}}$. □

In order to have a simple test and effective way to test the commutation relations (2), we introduce now the commutation polynomials.

Definition 2.10. *Let F be a rewriting family and $f, f' \in F$. Let m, m' be the smallest degree monomials for which $m\,\gamma(f) = m'\,\gamma(f')$. Then the polynomial $C(f,f') := mf - m'f' = m'\pi_{F,\mathcal{B}}(f') - m\pi_{F,\mathcal{B}}(f)$ is called the* commutation polynomial *of f, f'.*

Definition 2.11. *For a rewriting family F with respecet to $\mathcal{B}$, we denote by $C^+(F)$ the set of polynomials of the form $m\,f - m'\,f'$, where $f, f' \in F$ and $m, m' \in \{0, 1, x_1, \dots, x_n\}$ satisfy*

- *either $m\,\gamma(f) = m'\,\gamma(f')$,*
- *or $m\,\gamma(f) \in \mathcal{B}$ and $m' = 0$.*

Therefore, $C^+(F) \subset \langle\mathcal{B}^+\rangle$ and $C^+(F)$ contains all commutation polynomials $C(f,f')$ for $f, f' \in F$ whose monomial multipliers m, m' are of degree ≤ 1. The next result can be deduced using Theorem 2.9.

Theorem 2.12. *Let $\mathcal{B} \subset \mathcal{M}$ be connected to 1 and let F be a rewriting family for $\mathcal{B}$, complete in degree t. If for all $c \in C^+(F)$ of degree $\leq t$, $\pi_{F,\mathcal{B}}(c) = 0$, then $\pi_{F,\mathcal{B}}$ is the projection of $\mathbb{K}[\mathbf{x}]_t$ on $\langle\mathcal{B}\rangle_t$ along $\langle F \,|\, t\rangle$, ie. $\mathbb{K}[\mathbf{x}]_t = \langle\mathcal{B}\rangle_t \oplus \langle F \,|\, t\rangle$.*

Proof. Let us prove by induction on t that if F is complete in degree t and for all $c \in C^+(F)$ of degree $\leq t$, $\pi_{F,\mathcal{B}}(c) = 0$ then any $m \in \mathcal{M}_{t-2}$ satisfies (2), which in view of Theorem 2.9 suffices to prove the theorem.

Let us first prove that (2) holds for $m \in \mathcal{B}_{t-2}$. We distinguish several cases. If $x_i m, x_j m \in \mathcal{B}$ then (2) holds trivially. Suppose next that $x_i m, x_j m \in \partial\mathcal{B}$. Then, $f := x_i m - \pi_{F,\mathcal{B}}(x_i m)$ and $f' := x_j m - \pi_{F,\mathcal{B}}(x_j m)$ belong to F_{t-1}. As $x_j\gamma(f) = x_i\gamma(f')$, $x_j f - x_i f' \in C^+(F)$ and thus, by our assumption, $\pi_{F,\mathcal{B}}(x_j f) = \pi_{F,\mathcal{B}}(x_i f')$, which gives (2). Suppose now that $x_i m \in \partial\mathcal{B}$ and $x_j m \in \mathcal{B}$. As before $f = x_i m - \pi_{F,\mathcal{B}}(x_i m) \in F_{t-1}$. If $x_j\gamma(f) = x_i x_j m \in \mathcal{B}$ then $x_j f \in C^+(F)$ and thus $\pi_{F,\mathcal{B}}(x_j f) = 0$ gives (2). Otherwise, $x_i x_j m \in \partial\mathcal{B}$ and let $f' := x_i x_j m - \pi_{F,\mathcal{B}}(x_i x_j m) \in F_t$. Now, $x_j\gamma(f) = \gamma(f')$ implies $x_j f - f' \in C^+(F)$ and thus $\pi_{F,\mathcal{B}}(x_j f - f') = 0$ which gives again (2). This shows (2) in the case when $m \in \mathcal{B}_{t-2}$, and thus we have

$$\pi_{F,\mathcal{B}}(x_{i_2}\pi_{F,\mathcal{B}}(x_{i_1}b)) = \pi_{F,\mathcal{B}}(x_{i_1}\pi_{F,\mathcal{B}}(x_{i_2}b)) \quad \text{for all } b \in \langle\mathcal{B}\rangle_{t-2}. \tag{4}$$

Let us now consider $m \in \mathcal{M}_{t-2}\backslash\mathcal{B}_{t-2}$. By definition $\pi_{F,\mathcal{B}}(x_i\,m) = \pi_{F,\mathcal{B}}(x_{i'}\,\pi_{F,\mathcal{B}}(m'))$ for some $m' \in \mathcal{M}_{t-2}$ and $i' \in [1,n]$ such that $x_i\,m = x_{i'}\,m'$. If $i \neq i'$ there exists $m'' \in \mathcal{M}_{t-3}$ such

that $m = x_{i'}\, m'', m' = x_i\, m''$. As F is also complete in degree $t-1$ and for all $c \in C^+(F)$ of degree $\leq t-1$, $\pi_{F,\mathcal{B}}(c) = 0$, by induction hypothesis we have

$$\pi_{F,\mathcal{B}}(x_{i'}\, \pi_{F,\mathcal{B}}(x_i m'')) = \pi_{F,\mathcal{B}}(x_i\, \pi_{F,\mathcal{B}}(x_{i'} m'')),$$

so that $\pi_{F,\mathcal{B}}(x_i\, m) = \pi_{F,\mathcal{B}}(x_i\, \pi_{F,\mathcal{B}}(m))$. If $i = i'$, we have by definition $\pi_{F,\mathcal{B}}(x_i\, m) = \pi_{F,\mathcal{B}}(x_i\, \pi_{F,\mathcal{B}}(m))$.

As $\pi_{F,\mathcal{B}}(m) = m$ for $m \in \mathcal{B}_{t-2}$, we deduce that

$$\pi_{F,\mathcal{B}}(x_i m) = \pi_{F,\mathcal{B}}(x_i \pi_{F,\mathcal{B}}(m)) \text{ for all } m \in \mathcal{M}_{t-2},\ i \in [1,n]. \tag{5}$$

Now, using (5), $\pi_{F,\mathcal{B}}(x_i \pi_{F,\mathcal{B}}(x_j m))$ is equal to $\pi_{F,\mathcal{B}}(x_i \pi_{F,\mathcal{B}}(x_j \pi_{F,\mathcal{B}}(m)))$ which in turn is equal to $\pi_{F,\mathcal{B}}(x_j \pi_{F,\mathcal{B}}(x_i \pi_{F,\mathcal{B}}(m)))$ (using (4)) and thus to $\pi_{F,\mathcal{B}}(x_j \pi_{F,\mathcal{B}}(x_i m))$ (using again (5)). We can now apply Theorem 2.9 and conclude the proof. □

Theorem 2.13 (border basis, [17])**.** *Let $\mathcal{B} \subset \mathcal{M}$ be connected to 1 and let F be a rewriting family for $\mathcal{B}$, complete in any degree. Assume that $\pi_{F,\mathcal{B}}(c) = 0$ for all $c \in C^+(F)$. Then $\mathcal{B}$ is a basis of $\mathbb{K}[\mathbf{x}]/(F)$, $\mathbb{K}[\mathbf{x}] = \langle \mathcal{B} \rangle \oplus (F)$, and $(F)_t = \langle F \,|\, t \rangle$ for all $t \in \mathbb{N}$; the set F is a* border basis *of the ideal $I = (F)$ with respect to $\mathcal{B}$.*

Proof. By Theorem 2.12, $\mathbb{K}[\mathbf{x}]_t = \langle \mathcal{B} \rangle_t \oplus \langle F \,|\, t \rangle$ for all $t \in \mathbb{N}$. This implies that $\mathbb{K}[\mathbf{x}] = \langle \mathcal{B} \rangle \oplus (F)$ and thus $\mathcal{B}$ is a basis of $\mathbb{K}[\mathbf{x}]/(F)$. Let us prove that $(F)_t = \langle F \,|\, t \rangle$ for all $t \in \mathbb{N}$. Obviously, $\langle F \,|\, t \rangle \subset (F)_t$. Conversely let $p \in (F)_t$. Then $p = r + q$, where $r \in \langle \mathcal{B} \rangle_t$ and $q \in \langle F \,|\, t \rangle$. Thus $p - q \in (F) \cap \langle \mathcal{B} \rangle = \{0\}$, i.e., $p = q \in \langle F \,|\, t \rangle$. □

This implies the following characterization of border bases using the commutation property.

Corollary 2.14 (border basis, [16])**.** *Let $\mathcal{B} \subset \mathcal{M}$ be connected to 1 and let F be a rewriting family for $\mathcal{B}$, complete in any degree. If for all $m \in \mathcal{B}$ and all indices $i, j \in [1,n]$, we have:*

$$\pi_{F,\mathcal{B}}(x_i\, \pi_{F,\mathcal{B}}(x_j\, m)) = \pi_{F,\mathcal{B}}(x_j\, \pi_{F,\mathcal{B}}(x_i\, m)),$$

then $\mathcal{B}$ is a basis of $\mathbb{K}[\mathbf{x}]/(F)$, $\mathbb{K}[\mathbf{x}] = \langle \mathcal{B} \rangle \oplus (F)$, and $(F)_t = \langle F \,|\, t \rangle$ for all $t \in \mathbb{N}$.

Proof. Same proof as for Theorem 2.13, using Theorem 2.9. □

3. Hankel Operators

In this section, we analyse the properties of Hankel operators and related moment matrices, that we will need hereafter, for the moment matrix approach.

3.1. **Linear forms on the polynomial ring.** The set of $\mathbb{K}$-linear forms from $\mathbb{K}[\mathbf{x}]$ to $\mathbb{K}$ is denoted by $\mathbb{K}[\mathbf{x}]^* := \mathrm{Hom}_{\mathbb{K}}(\mathbb{K}[\mathbf{x}], \mathbb{K})$ and called the dual space of $\mathbb{K}[\mathbf{x}]$. A typical element of $\mathbb{K}[\mathbf{x}]^*$ is the evaluation at a point $\zeta \in \mathbb{K}^n$:

$$\mathbf{1}_\zeta \quad : \quad p \in \mathbb{K}[\mathbf{x}] \mapsto p(\zeta) \in \mathbb{K}.$$

Such evaluation can be composed with differentiation. Namely, for $\alpha \in \mathbb{N}^n$, the differential functional:

$$\mathbf{1}_\zeta \cdot \partial^\alpha \quad : \quad p \in \mathbb{K}[\mathbf{x}] \mapsto \left(\frac{\partial^{|\alpha|}}{\partial x_1^{\alpha_1} \dots \partial x_n^{\alpha_n}} p \right)(\zeta)$$

evaluates at ζ the derivative ∂^α of p. For $\alpha = 0$, $\mathbf{1}_\zeta \cdot \partial^0 = \mathbf{1}_\zeta$. The dual basis of the monomial basis $(\mathbf{x}^\alpha)_{\alpha \in \mathbb{N}^n}$ of $\mathbb{K}[\mathbf{x}]$ is denoted $(\mathbf{d}^\alpha)_{\alpha \in \mathbb{N}^n}$; we have $\mathbf{d}^\alpha(\mathbf{x}^\beta) = \delta_{\alpha,\beta}$. In characteristic 0, $\mathbf{d}^\alpha := \mathbf{1}_0 \cdot \frac{1}{\prod_{i=1}^n \alpha_i!} \partial^\alpha$. Any element $\Lambda \in \mathbb{K}[\mathbf{x}]^*$ can be written as $\Lambda = \sum_\alpha \Lambda(\mathbf{x}^\alpha) \mathbf{d}^\alpha$. In particular, $\mathbf{1}_\zeta = \sum_{\alpha \in \mathbb{N}^n} \zeta^\alpha \mathbf{d}^\alpha$.

For $S \subset \mathbb{K}[\mathbf{x}]$, we define

$$S^\perp := \{\Lambda \in \mathbb{K}[\mathbf{x}]^* \mid \forall p \in S\ \Lambda(p) = 0\}.$$

3.2. **Hankel operators.** The dual space $\mathbb{K}[\mathbf{x}]^*$ has a natural structure of $\mathbb{K}[\mathbf{x}]$-module which is defined as follows: $(p,\Lambda) \in \mathbb{K}[\mathbf{x}] \times \mathbb{K}[\mathbf{x}]^* \mapsto p \cdot \Lambda \in \mathbb{K}[\mathbf{x}]^*$, where

$$p \cdot \Lambda \quad : \quad q \in \mathbb{K}[\mathbf{x}] \mapsto \Lambda(pq) \in \mathbb{K}.$$

Note that, for any $\alpha, \beta \in \mathbb{N}^n$, we have

$$\begin{aligned} \mathbf{x}^\beta \cdot \mathbf{d}^\alpha &= \mathbf{d}^{\alpha-\beta} \text{ if } \alpha \geq \beta, \\ &= 0 \qquad \text{otherwise}. \end{aligned}$$

Definition 3.1. *For $\Lambda \in \mathbb{K}[\mathbf{x}]^*$, the Hankel operator H_Λ is the operator from $\mathbb{K}[\mathbf{x}]$ to $\mathbb{K}[\mathbf{x}]^*$ defined by*

$$H_\Lambda \quad : \quad p \in \mathbb{K}[\mathbf{x}] \mapsto p \cdot \Lambda \in \mathbb{K}[\mathbf{x}]^*.$$

Lemma 3.2. *For $\Lambda \in \mathbb{K}[\mathbf{x}]^*$, the matrix of the Hankel operator H_Λ with respect to the bases $(\mathbf{x}^\alpha)$ of $\mathbb{K}[\mathbf{x}]$ and $(\mathbf{d}^\beta)$ of $\mathbb{K}[\mathbf{x}]^*$ is $[H_\Lambda] = (\Lambda(\mathbf{x}^{\alpha+\beta}))$.*

Proof. Writing $\Lambda = \sum_\gamma \Lambda(\mathbf{x}^\gamma)\mathbf{d}^\gamma$, we have:

$$H_\Lambda(\mathbf{x}^\alpha) = \mathbf{x}^\alpha \cdot \Lambda = \sum_\gamma \Lambda(\mathbf{x}^\gamma)\ \mathbf{x}^\alpha \cdot \mathbf{d}^\gamma = \sum_{\gamma | \gamma \geq \alpha} \Lambda(\mathbf{x}^\gamma)\mathbf{d}^{\gamma-\alpha} = \sum_\beta \Lambda(\mathbf{x}^{\alpha+\beta})\mathbf{d}^\beta.$$

□

We now summarize some well known properties of the kernel

$$\operatorname{Ker} H_\Lambda = \{p \in \mathbb{K}[\mathbf{x}] \mid p \cdot \Lambda = 0, \ \text{ i.e., } \Lambda(pq) = 0\ \forall q \in \mathbb{K}[\mathbf{x}]\}.$$

of the Hankel operator H_Λ. Recall the definition of a Gorenstein algebra [4], [8, Chap. 8].

Definition 3.3. *An algebra $\mathcal{A}$ is called* Gorenstein *if $\mathcal{A}$ and its dual space $\mathcal{A}^*$ are isomorphic $\mathcal{A}$-modules.*

Applying this definition to $\mathcal{A} := \mathbb{K}[\mathbf{x}]/\operatorname{Ker} H_\Lambda$ yields

Lemma 3.4. *$\operatorname{Ker} H_\Lambda$ is an ideal in $\mathbb{K}[\mathbf{x}]$ and the quotient space $\mathcal{A} := \mathbb{K}[\mathbf{x}]/\operatorname{Ker} H_\Lambda$ is a Gorenstein algebra.*

Proof. Direct verification, using H_Λ as isomorphism in the proof of the second part of the lemma. □

The focus of this paper is the computation of zero-dimensional varieties, which relates to finite rank Hankel operators as shown in the following lemma.

Lemma 3.5. *The rank of the operator H_Λ is finite if and only if $\operatorname{Ker} H_\Lambda$ is a zero-dimensional ideal, in which case $\dim \mathbb{K}[\mathbf{x}]/\operatorname{Ker} H_\Lambda = \operatorname{rank} H_\Lambda$.*

Proof. Directly from the fact that, given $p_1, \ldots, p_r \in \mathbb{K}[\mathbf{x}]$, $H_\Lambda(p_1), \ldots, H_\Lambda(p_r)$ are linearly independent in $\mathbb{K}[\mathbf{x}]^*$ if and only if the cosets $[p_1], \ldots, [p_r]$ are linearly independent in $\mathbb{K}[\mathbf{x}]/\operatorname{Ker} H_\Lambda$. □

The next theorem states a fundamental result in commutative algebra, namely that all zero-dimensional polynomial ideals can be characterized using differential operators (see [8, Chap. 7], [4, Thm. 2.2.7]). For the special case of zero-dimensional Gorenstein ideals, a single differential form is enough to characterize the ideal.

Theorem 3.6. *Let $\mathbb{K} = \mathbb{C}$ and assume $\operatorname{rank} H_\Lambda = r < \infty$. Then there exist $\zeta_1, \ldots, \zeta_d \in \mathbb{C}^n$ (with $d \leq r$) and non-zero (differential) polynomials $p_1, \ldots, p_d \in \mathbb{C}[\partial]$, of the form $p_i(\partial) = \sum_{\alpha \in A_i} a_{i,\alpha}\partial^\alpha$ where $A_i \subset \mathbb{N}^n$ is finite and $a_{i,\alpha} \in \mathbb{K}$, such that*

$$\Lambda = \sum_{i=1}^{d} \mathbf{1}_{\zeta_i} \cdot p_i(\partial). \tag{6}$$

For a zero-dimensional ideal $I \subset \mathbb{K}[\mathbf{x}]$ with simple zeros $V(I) = \{\zeta_1, \ldots, \zeta_r\} \subset \mathbb{K}^n$ only, we have $I^\perp = \langle \mathbf{1}_{\zeta_1}, \ldots, \mathbf{1}_{\zeta_r} \rangle$ and the ideal I is radical as a consequence of Hilbert's Nullstellensatz.

In a similar way, we can now characterize the linear forms Λ for which $\operatorname{Ker} H_\Lambda$ is a radical ideal.

Proposition 3.7. *Let $\mathbb{K} = \mathbb{C}$ and assume that $\operatorname{rank} H_\Lambda = r < \infty$. Then, the ideal $\operatorname{Ker} H_\Lambda$ is radical if and only if*

$$\Lambda = \sum_{i=1}^{r} \lambda_i \mathbf{1}_{\zeta_i} \quad \text{with } \lambda_i \in \mathbb{K} - \{0\} \quad \text{and } \zeta_i \in \mathbb{K}^n \text{ pairwise distinct,} \tag{7}$$

in which case $\operatorname{Ker} H_\Lambda = I(\zeta_1, \ldots, \zeta_r)$ is the vanishing ideal of the ζ_i's.

Proof. Assume first that $\operatorname{Ker} H_\Lambda$ is radical with $V(\operatorname{Ker} H_\Lambda) := \{\zeta_1, \ldots, \zeta_r\} \subset \mathbb{K}^n$. This implies $\operatorname{Ker} H_\Lambda = I(V(\operatorname{Ker} H_\Lambda)) = I(\zeta_1, \ldots, \zeta_r)$. Let $p_i \in \mathbb{C}[\mathbf{x}]$ be interpolation polynomials at the points ζ_i, i.e., $p_i(\zeta_j) = \delta_{i,j}$ for $i, j \leq r$. Then the set $\{p_1, \ldots, p_r\}$ is linearly independent in $\mathcal{A} := \mathbb{K}[\mathbf{x}]/(\operatorname{Ker} H_\Lambda)$ and thus is a basis of $\mathcal{A}$. As the linear functionals Λ and $\sum_{i=1}^r \Lambda(p_i)\mathbf{1}_{\zeta_i}$ take the same values at each p_i, we obtain: $\Lambda = \sum_{i=1}^r \Lambda(p_i)\mathbf{1}_{\zeta_i}$. Moreover, $\lambda_i := \Lambda(p_i) \neq 0$, since $\operatorname{rank} H_\Lambda = r$.

Conversely assume that Λ is as in (7). The inclusion $I(\zeta_1, \ldots, \zeta_r) \subset \operatorname{Ker} H_\Lambda$ is obvious. Consider now $p \in \operatorname{Ker} H_\Lambda$ and as before let $p_i \in \mathbb{K}[\mathbf{x}]$ be interpolation polynomials at the ζ_i's. Then $0 = \Lambda(p\, p_i) = \lambda_i p(\zeta_i)$ implies $p(\zeta_i) = 0$, thus showing $p \in I(\zeta_1, \ldots, \zeta_r)$. As $\operatorname{Ker} H_\Lambda = I(\zeta_1, \ldots, \zeta_r)$ is the vanishing ideal of a set of r points, it is radical by the Hilbert Nullstellensatz. □

In a similar way, we can also characterize real radical ideals using Hankel operators.

Proposition 3.8. *Let $\mathbb{K} = \mathbb{R}$ and assume that $\operatorname{rank} H_\Lambda = r < \infty$. Then, the ideal $\operatorname{Ker} H_\Lambda$ is real radical if and only if*

$$\Lambda = \sum_{i=1}^{r} \lambda_i \mathbf{1}_{\zeta_i} \quad \text{with } \lambda_i \in \mathbb{R} - \{0\} \text{ and } \zeta_i \in \mathbb{R}^n \text{ pairwise distinct.} \tag{8}$$

Proof. If $\operatorname{Ker} H_\Lambda$ is real radical then $V(\operatorname{Ker} H_\Lambda) = \{\zeta_1, \ldots, \zeta_r\} \subset \mathbb{R}^n$, so that (7) gives (8). Conversely, if Λ is as in (8), then $\operatorname{Ker} H_\Lambda$ is real radical, since $\sum_j q_j^2 \in \operatorname{Ker} H_\Lambda$ implies $\sum_j q_j(\zeta_i)^2 = 0$ and thus $q_j(\zeta_i) = 0$, giving $q_j \in \operatorname{Ker} H_\Lambda$. □

Let us now recall a direct way to compute the radical of the ideal $\operatorname{Ker} H_\Lambda$. First, consider the quadratic form Q_Λ defined on $\mathbb{K}[\mathbf{x}]$ by

$$Q_\Lambda \quad : \quad (p, q) \in \mathbb{K}[\mathbf{x}]^2 \mapsto \Lambda(pq) \in \mathbb{K}. \tag{9}$$

Then, $Q_\Lambda(p, q) = \Lambda(pq) = H_\Lambda(p)(q) = H_\Lambda(q)(p)$ for all $p, q \in \mathbb{K}[\mathbf{x}]$, and the matrix of Q_Λ in the monomial basis $(\mathbf{x}^\alpha)$ is $[Q_\Lambda] = (\Lambda(\mathbf{x}^{\alpha+\beta}))$. We saw in Lemma 3.4 that the algebra $\mathcal{A} = \mathbb{K}[\mathbf{x}]/\operatorname{Ker} H_\Lambda$ is Gorenstein. An alternative characterisation of Gorenstein algebras states that the above quadratic form Q_Λ defines a non-degenerate inner product on $\mathcal{A}$ (see eg. [8][chap. 9]). Assume now that $\operatorname{rank} H_\Lambda = r < \infty$ so that $\dim \mathcal{A} = r$. Let $b_1, \ldots, b_r$ be a basis of $\mathcal{A}$ and let $d_1, \ldots, d_r$ be its dual basis in $\mathcal{A}$ for Q_Λ: it satisfies $\Lambda(b_i\, d_j) = \delta_{i,j}$ for $i, j \in [1, r]$. Then, for any element $a \in \mathcal{A}$, we have

$$a = \sum_{i=1}^{r} \Lambda(a\, d_i) b_i. \tag{10}$$

In particular, we have the following property:

Proposition 3.9. *Let $\Delta := \sum_{i=1}^r b_i\, d_i$. Given $h \in \mathcal{A}$, let $\mathcal{X}_h$ be the corresponding multiplication operator in $\mathcal{A}$. We have*

$$\operatorname{Trace}(\mathcal{X}_h) = \Lambda(h\Delta).$$

Proof. By relation (10), the matrix of $\mathcal{X}_h$ in the basis $(b_i)_{i\le i\le r}$ of $\mathcal{A}$ is $(\Lambda(h\,b_j\,d_i))_{1\le i,j\le r}$ and thus its trace is

$$\mathrm{Trace}(\mathcal{X}_h) = \sum_{i=1}^{r} \Lambda(h\,b_i\,d_i) = \Lambda(h\Delta).$$

□

As a direct consequence we deduce the following result (see e.g., [10]):

Theorem 3.10. *Let $\mathbb{K} = \mathbb{C}$ and assume $\operatorname{rank} H_\Lambda = r < \infty$. Let $b_1, \ldots, b_r$ be a basis of $\mathcal{A}_\Lambda$, $d_1, \ldots, d_r$ be its dual basis with respect to the inner product given by Q_Λ, and $\Delta = \sum_{i=1}^r b_i\,d_i$. Then the radical of $\operatorname{Ker} H_\Lambda$ is $\operatorname{Ker} H_{\Delta\cdot\Lambda}$.*

Proof. Let $I := \operatorname{Ker} H_\Lambda$. A polynomial h is in $\sqrt{I}$ if and only if some power of h is in I or, equivalently, if and only if $\mathcal{X}_h$ is nilpotent. By a classical algebraic property, the latter is equivalent to $\mathrm{Trace}(\mathcal{X}_h\mathcal{X}_a) = 0 = \mathrm{Trace}(\mathcal{X}_{h\,a})$ for all $a \in \mathcal{A}$. Indeed, as the operators $\mathcal{X}_h, \mathcal{X}_a$ commute, if $\mathcal{X}_h$ is nilpotent then so is $\mathcal{X}_h\mathcal{X}_a$ and we have $\mathrm{Trace}(\mathcal{X}_h\mathcal{X}_a) = 0$. Conversely if $\mathrm{Trace}(\mathcal{X}_h\mathcal{X}_a) = 0$ for all $a \in \mathcal{A}$ then, by Cayley-Hamilton identity, the characteristic polynomial $\det(\lambda I - \mathcal{X}_h)$ of $\mathcal{X}_h$ is λ^r and thus $\mathcal{X}_h$ is nilpotent. By Proposition 3.9, we deduce that $h \in \sqrt{I}$ if and only if $\Lambda(\Delta\,ha) = 0$ for all $a \in \mathcal{A}_\Lambda$, that is, if and only if $h \in \operatorname{Ker} H_{\Delta\cdot\Lambda}$. □

3.3. **Positive linear forms.** We now assume that $\mathbb{K} = \mathbb{R}$ and consider the polynomial ring $\mathbb{R}[\mathbf{x}]$. We first show that the kernel of a Hankel operator H_Λ is a real radical ideal when $\Lambda \in \mathbb{R}[\mathbf{x}]^*$ is positive. This result is crucial in the algorithm that computes the real radical of an ideal.

Definition 3.11. *We say that $\Lambda \in \mathbb{R}[\mathbf{x}]^*$ is positive, which we denote $\Lambda \succcurlyeq 0$, if $\Lambda(p^2) \geqslant 0$ for all $p \in \mathbb{R}[\mathbf{x}]$. Equivalently, we will say $H_\Lambda \succcurlyeq 0$ if $\Lambda \succcurlyeq 0$.*

We will use the following simple observation.

Lemma 3.12. *Assume $\Lambda \succcurlyeq 0$. For $p \in \mathbb{R}[\mathbf{x}]$, $\Lambda(p^2) = 0$ implies $p \in \operatorname{Ker} H_\Lambda$ and thus $\Lambda(p) = 0$. For $\Lambda, \Lambda' \succcurlyeq 0$, $\operatorname{Ker} H_{\Lambda+\Lambda'} = \operatorname{Ker} H_\Lambda \cap \operatorname{Ker} H_{\Lambda'}$.*

Proof. For any $q \in \mathbb{R}[\mathbf{x}]$, $t \in \mathbb{R}$, $\Lambda((p+tq)^2) = t^2\Lambda(q^2) + 2t\Lambda(p\,q) \geq 0$. Dividing by t and letting t go to zero yields $\Lambda(p\,q) = 0$, thus showing $p \in \operatorname{Ker} H_\Lambda$. The inclusion $\operatorname{Ker} H_\Lambda \cap \operatorname{Ker} H_{\Lambda'} \subset \operatorname{Ker} H_{\Lambda+\Lambda'}$ is obvious. Conversely, let $p \in \operatorname{Ker} H_{\Lambda+\Lambda'}$. In particular, $(\Lambda + \Lambda')(p^2) = 0$, which implies $\Lambda(p^2) = \Lambda'(p^2) = 0$ (since $\Lambda(p^2), \Lambda'(p^2) \geq 0$) and thus $p \in \operatorname{Ker} H_\Lambda \cap \operatorname{Ker} H_{\Lambda'}$. □

Proposition 3.13. *If $\Lambda \succcurlyeq 0$, then $\operatorname{Ker} H_\Lambda$ is a real radical ideal.*

Proof. Assume $\sum_i p_i^2 \in \operatorname{Ker} H_\Lambda$; we show that $p_i \in \operatorname{Ker} H_\Lambda$. Indeed, $(\sum_i p_i^2)\cdot\Lambda = 0$ implies, for all $q \in \mathbb{R}[\mathbf{x}]$, $0 = \Lambda(\sum_i p_i^2 q^2) = \sum_i \Lambda(p_i^2 q^2)$ and thus $\Lambda(p_i^2 q^2) = 0$. By Lemma 3.12, this in turn implies $\Lambda(p_i q) = 0$ and thus $p_i \in \operatorname{Ker} H_\Lambda$. □

We saw in Proposition 3.8 that the kernel of a finite rank Hankel operator H_Λ is real radical if and only if Λ is a linear combination of evaluations at real points. We next observe that Λ is positive precisely when Λ is a *conic* combination of evaluations at real points.

Proposition 3.14. *Assume $\operatorname{rank} H_\Lambda = r < \infty$. Then $\Lambda \succcurlyeq 0$ if and only if Λ has a decomposition (8) with $\lambda_i > 0$ and distinct $\zeta_i \in \mathbb{R}^n$, in which case $V(\operatorname{Ker} H_\Lambda) = \{\zeta_1, \ldots, \zeta_r\} \subset \mathbb{R}^n$.*

Proof. If $\Lambda = \sum_{i=1}^r \lambda_i \mathbf{1}_{\zeta_i}$ with $\lambda_i > 0$ and $\zeta_i \in \mathbb{R}^n$, then $\Lambda \succcurlyeq 0$ holds obviously. Conversely, assume that $\Lambda \succcurlyeq 0$ then by Proposition 3.13 the ideal $\operatorname{Ker} H_\Lambda$ is real radical. By Proposition 3.8, Λ has a decomposition (8) where $\lambda_i = \Lambda(p_i) \neq 0$, $\zeta_i \in \mathbb{R}^n$, and p_i are interpolation polynomials at the ζ_i's. As $p_i^2 - p_i \in I(\zeta_1, \ldots, \zeta_r) = \operatorname{Ker} H_\Lambda$, we have $\Lambda(p_i) = \Lambda(p_i^2) \geq 0$, which concludes the proof. □

To motivate the next section, let us recall Lemma 3.5 and observe how it specializes to truncated Hankel operators defined on subspaces of $\mathbb{K}[\mathbf{x}]$:

Lemma 3.15. *Let $\mathcal{B} = \{b_1, \ldots, b_r\} \subset \mathbb{R}[\mathbf{x}]$ and $\Lambda \in \mathbb{K}[\mathbf{x}]^*$. The operator*

$$H_\Lambda^{\mathcal{B}} : \langle \mathcal{B} \rangle \to \langle \mathcal{B} \rangle^*$$
$$p = \sum_{i=1}^{r} \lambda_i b_i \mapsto p \cdot \Lambda$$

has a trivial kernel if and only if the cosets $[b_1], \ldots, [b_r] \in \mathbb{K}[\mathbf{x}]/\operatorname{Ker} H_\Lambda$ are linearly independent in $\mathbb{K}[\mathbf{x}]/\operatorname{Ker} H_\Lambda$.

Proof. Direct verification using the fact that $\operatorname{Ker} H_\Lambda^{\mathcal{B}} = \operatorname{Ker} H_\Lambda \cap \langle \mathcal{B} \rangle$. □

Assume now that $\operatorname{Ker} H_\Lambda$ is zero-dimensional and that $\mathcal{B} = \{b_1, \ldots, b_r\} \subset \mathbb{K}[\mathbf{x}]$ is chosen so that $[b_1], \ldots, [b_r]$ form a basis of $\mathcal{A} = \mathbb{R}[\mathbf{x}]/\operatorname{Ker} H_\Lambda$. As in relation (9), we consider the quadratic form $Q_\Lambda^{\mathcal{B}}$ on $\mathcal{A}$ defined by

$$Q_\Lambda^{\mathcal{B}} \quad : \quad (p, q) \in \mathcal{A} \times \mathcal{A} \mapsto \Lambda(pq) \in \mathbb{K}.$$

Note that a matrix representation of this form can be obtained by taking the principle submatrix of $[H_\Lambda]$ indexed by $\mathcal{B}$. Following [14], we recall under which conditions the bilinear form $Q_\Lambda^{\mathcal{B}}$ relates to the Hermite form

$$T_h : \mathcal{A} \times \mathcal{A} \to \mathbb{K}$$
$$(f, g) \mapsto \operatorname{Trace}(\mathcal{X}_{fgh})$$

for some $h \in \mathcal{A}$.

Lemma 3.16. *The quadratic form associated to $Q_\Lambda^{\mathcal{B}}$ coincides with the Hermite form T_h for some $h \in \mathcal{A}$ if and only if $\operatorname{Ker} H_\Lambda$ is radical.*

Proof. See [14, Sec. 2.2]. □

4. Truncated Hankel Operators

We have seen in the previous section that the kernel of the Hankel operator associated to a positive linear form is a real radical ideal. However, in order to be able to exploit this property into an algorithm, we need to restrict our analysis to matrices of finite size. For this reason, we consider here truncated Hankel operators, which will play a central role for the construction of (real) radical ideals.

For $E \subset \mathbb{K}[\mathbf{x}]$, set $E \cdot E := \{p\, q \mid p, q \in E\}$. Suppose now $E \subset \mathbb{K}[\mathbf{x}]$ is a vector space. A linear form Λ defined on $\langle E \cdot E \rangle$ yields the map $H_\Lambda^E : E \to E^*$ by $H_\Lambda^E(p) = p \cdot \Lambda$ for $p \in E$. Thus H_Λ^E can be seen as a truncated Hankel operator, defined only on the subspace E.

Given a subspace $E_0 \subset E$, Λ induces a linear map on $\langle E_0 \cdot E_0 \rangle$ and we can consider the induced truncated Hankel operator $H_\Lambda^{E_0} : E_0 \to (E_0)^*$.

Definition 4.1. *Given vector subspaces $E_0 \subset E \subset \mathbb{K}[\mathbf{x}]$ and $\Lambda \in \langle E \cdot E \rangle^*$, H_Λ^E is said to be a flat extension of its restriction $H_\Lambda^{E_0}$ to E_0 if $\operatorname{rank} H_\Lambda^E = \operatorname{rank} H_\Lambda^{E_0}$.*

We now give some conditions ensuring that it is possible to construct a flat extension of a given truncated Hankel operator. The next result extends an earlier result of Curto-Fialkow [7]; a generalization of this result can be found in [2].

Theorem 4.2. [15] *Consider a vector subspace $E \subset \mathbb{K}[\mathbf{x}]$ and a linear function Λ on $\langle E^+ \cdot E^+ \rangle$. Assume that $E = \langle \mathcal{C} \rangle$ where $\mathcal{C} \subset \mathcal{M}$ is connected to 1 and that $\operatorname{rank} H_\Lambda^{E^+} = \operatorname{rank} H_\Lambda^E$. Then there exists a (unique) linear function $\tilde{\Lambda} \in \mathbb{K}[\mathbf{x}]^*$ which extends Λ, i.e., $\tilde{\Lambda}(p) = \Lambda(p)$ for all $p \in \langle E^+ \cdot E^+ \rangle$, and satisfying $\operatorname{rank} H_{\tilde{\Lambda}} = \operatorname{rank} H_\Lambda^{E^+}$. In other words, the truncated Hankel operator $H_\Lambda^{E^+}$ has a (unique) flat extension to a (full) Hankel operator $H_{\tilde{\Lambda}}$.*

In the following, we will deal with linear forms vanishing on a given set G of polynomials.

Definition 4.3. *Given a vector space $E \subset \mathbb{K}[\mathbf{x}]$ and $G \subset \langle E \cdot E \rangle$, define the set*

$$\mathcal{L}_{G,E} := \{\Lambda \in \langle E \cdot E \rangle^* \mid \Lambda(g) = 0 \ \forall g \in G\}. \tag{11}$$

If $\mathbb{K} = \mathbb{R}$, define

$$\mathcal{L}_{G,E,\succeq} := \{\Lambda \in \mathcal{L}_{G,E} \mid \Lambda(p^2) \geq 0 \ \forall p \in E\}. \tag{12}$$

For an integer $t \in \mathbb{N}$ and $G \subset \mathbb{K}[\mathbf{x}]_{2t}$, taking $E = \mathbb{K}[\mathbf{x}]_t$, we abbreviate our notation and set $\mathcal{L}_{G,t} := \mathcal{L}_{G,\mathbb{K}[\mathbf{x}]_t}$ and $\mathcal{L}_{G,t,\succeq} := \mathcal{L}_{G,\mathbb{K}[\mathbf{x}]_t,\succeq}$ when $\mathbb{K} = \mathbb{R}$.

4.1. **Truncated Hankel operators and radical ideals.** In this section, we assume that E is a finite dimensional vector space. The following definition for generic elements of $\mathcal{L}_{G,E}$ is justified by Theorem 4.6 below.

Definition 4.4. *Let $G \subset \langle E \cdot E \rangle$ where E is a finite dimensional subspace of $\mathbb{K}[\mathbf{x}]$. An element $\Lambda^* \in \mathcal{L}_{G,E}$ is said to be* generic *if*

$$\operatorname{rank} H_{\Lambda^*}^{E_0} = \max_{\Lambda \in \mathcal{L}_{G,E}} \operatorname{rank} H_{\Lambda}^{E_0} \tag{13}$$

for all subspaces $E_0 \subset E$.

If $\mathbb{L}$ is a field containing $\mathbb{K}$, we denote by $\mathcal{L}_{G,E}^{\mathbb{L}} := \mathcal{L}_{G,E} \otimes \mathbb{L}$, the space obtained by considering the vector spaces over $\mathbb{L}$ in (11). We recall here a classical result about generic properties over field extensions, which will be used to give a simpler proof of a result that we need from [13].

Lemma 4.5. *Let $\mathbb{K}$ be a field of characteristic 0 and $\mathbb{L}$ a field containing $\mathbb{K}$. If Λ^* is a generic element in $\mathcal{L}_{G,E}^{\mathbb{K}}$, then it is generic in $\mathcal{L}_{G,E}^{\mathbb{L}}$.*

Proof. The space of matrices H_Λ^E for $\Lambda \in \mathcal{L}_{G,E}^{\mathbb{K}}$ is a vector space spanned by a basis $H_1, \ldots, H_l$ over $\mathbb{K}$ (resp. $\mathbb{L}$). Let $u_1, \ldots, u_l$ be new variables and ρ be the maximal size of a non-zero minor $\in \mathbb{K}[\mathbf{u}]$ of $H(\mathbf{u}) := \sum_{i=1}^l u_i H_i$. Then for any value of $\mathbf{u} \in \mathbb{K}^l$ (resp. $\mathbf{u} \in \mathbb{L}^l$), the matrix $H(\mathbf{u})$ is of rank $\leq \rho$. Since $\mathbb{K}$ is of characteristic 0 there exists $\mathbf{u}_0 \in \mathbb{K}^l$ with $H(\mathbf{u}_0)$ of rank ρ, which corresponds to a generic element in $\mathcal{L}_{G,E}^{\mathbb{K}}$ and in $\mathcal{L}_{G,E}^{\mathbb{L}}$. □

Theorem 4.6. *Let E be a finite dimensional subspace of $\mathbb{K}[\mathbf{x}]$ and let $G \subset \langle E \cdot E \rangle$. Assume $\Lambda^* \in \mathcal{L}_{G,E}$ is generic, ie. satisfies (13). Then,* $\operatorname{Ker} H_{\Lambda^*}^E \subset \sqrt{(G)}$.

Proof. By Lemma 4.5, Λ^* is a generic element of $\mathcal{L}_{G,E}$ over $\mathbb{R}$ or $\mathbb{C}$ and thus we can assume that $\mathbb{K} = \overline{\mathbb{K}}$. Let $v \in V_{\overline{\mathbb{K}}}(G)$, let $\underline{\mathbf{1}}_v$ denotes the evaluation at v restricted to $\langle E \cdot E \rangle$ and let $f \in \operatorname{Ker} H_\Lambda^E$. Our objective is to show that $f(v) = 0$. Suppose for contradiction that $f(v) \neq 0$.

Notice that $\underline{\mathbf{1}}_v$ and $\Lambda' := \Lambda^* + \underline{\mathbf{1}}_v$ belong to $\mathcal{L}_{G,E}$. As $\Lambda'(f^2) = f^2(v) \neq 0$, $f \in \operatorname{Ker} H_\Lambda^E \setminus \operatorname{Ker} H_{\Lambda'}^E$ and by the maximality of the rank of H_Λ^E $\operatorname{Ker} H_{\Lambda'}^E \not\subset \operatorname{Ker} H_\Lambda^E$. Hence there exists $f' \in \operatorname{Ker} H_{\Lambda'}^E \setminus \operatorname{Ker} H_\Lambda^E$. Then, $0 = H_{\Lambda'}^E(f') = H_\Lambda^E(f') + f'(v)\underline{\mathbf{1}}_v$ implies $f'(v) \neq 0$. On the other hand,

$$0 = H_{\Lambda'}^E(f')(f) = \Lambda'(ff') = \Lambda(ff') + f(v)f'(v) = H_{\Lambda^*}^E(f)(f') + f(v)f'(v) = f(v)f'(v),$$

yielding a contradiction. □

4.2. **Truncated Hankel operators, positivity and real radical ideals.** We first give a result which relates the kernel of H_Λ^E with the real radical of an ideal (G), when Λ is positive and vanishes on a given set G of polynomials. We start with the following result, which motivates our definition of the generic property for a positive linear form.

Proposition 4.7. *For $\Lambda^* \in \mathcal{L}_{G,E,\succeq}$, the following assertions are equivalent:*

(i) $\operatorname{rank} H_{\Lambda^*}^E = \max_{\Lambda \in \mathcal{L}_{G,E,\succeq}} \operatorname{rank} H_\Lambda^E$.
(ii) $\operatorname{Ker} H_{\Lambda^*}^E \subset \operatorname{Ker} H_\Lambda^E$ *for all* $\Lambda \in \mathcal{L}_{G,E,\succeq}$.

(iii) $\operatorname{rank} H^{E_0}_{\Lambda^*} = \max_{\Lambda\in\mathcal{L}_{G,E,\succeq}} \operatorname{rank} H^{E_0}_{\Lambda}$ *for any subspace* $E_0 \subset E$.

Call $\Lambda^* \in \mathcal{L}_{G,E,\succeq}$ generic *if it satisfies any of the equivalent conditions (i)–(iii) and set*

$$\mathcal{K}_{G,E,\succeq} := \operatorname{Ker} H^E_{\Lambda^*} \quad \textit{for any generic } \Lambda^* \in \mathcal{L}_{G,E,\succeq}.$$

Proof. (i) $\Longrightarrow$ (ii): Note that $\Lambda + \Lambda^* \in \mathcal{L}_{G,E,\succeq}$ and $\operatorname{Ker} H^E_{\Lambda+\Lambda^*} = \operatorname{Ker} H^E_{\Lambda} \cap \operatorname{Ker} H^E_{\Lambda^*}$ (using Lemma 3.12). Hence, $\operatorname{rank} H^E_{\Lambda+\Lambda^*} \geq \operatorname{rank} H^E_{\Lambda^*}$ and thus equality holds. This implies that $\operatorname{Ker} H^E_{\Lambda+\Lambda^*} = \operatorname{Ker} H^E_{\Lambda^*}$ is thus contained in $\operatorname{Ker} H^E_{\Lambda}$.
(ii) $\Longrightarrow$ (iii): Given $E_0 \subset E$, we show that $\operatorname{Ker} H^{E_0}_{\Lambda^*} \subset \operatorname{Ker} H^{E_0}_{\Lambda}$. By Lemma 3.12, we have $\operatorname{Ker} H^{E_0}_{\Lambda^*} \subset \operatorname{Ker} H^E_{\Lambda^*}$ and, by the above, we have $\operatorname{Ker} H^E_{\Lambda^*} \subset \operatorname{Ker} H^E_{\Lambda}$.
The implication (iii) $\Longrightarrow$ (i) is obvious. □

Lemma 4.8. *let* $G_0 \subset G \subset \langle E \cdot E\rangle$. *Then,* $\mathcal{K}_{G_0,E,\succcurlyeq} \subset \mathcal{K}_{G,E,\succcurlyeq}$.

Proof. Let $\Lambda \in \mathcal{L}_{G,E,\succeq}$ be a generic element, so that $\operatorname{Ker} H^E_{\Lambda} = \mathcal{K}_{G,E,\succcurlyeq}$. Obviously, $\Lambda \in \mathcal{L}_{G_0,E,\succcurlyeq}$, which implies that $\operatorname{Ker} H^E_{\Lambda} \supseteq \mathcal{K}_{G_0,E,\succcurlyeq}$. □

Theorem 4.9. *Let* $G \subset \langle E \cdot E\rangle$, *where* E *is a finite dimensional subspace of* $\mathbb{R}[\mathbf{x}]$. *Then,* $\mathcal{K}_{G,E,\succcurlyeq} \subset \sqrt[\mathbb{R}]{(G)}$.

Proof. Let Λ be a generic element of $\mathcal{L}_{G,E,\succcurlyeq}$, so that $\mathcal{K}_{G,E,\succcurlyeq} = \operatorname{Ker} H^E_{\Lambda}$, and let $v \in V_{\mathbb{R}}(G)$; we show that $\operatorname{Ker} H^E_{\Lambda} \subset I(v)$. As $\underline{\mathbf{1}}_v$, the evaluation at v restricted to $\langle E \cdot E\rangle$, belongs to $\mathcal{L}_{G,E,\succcurlyeq}$, we deduce using Proposition 4.7 that $\operatorname{Ker} H^E_{\Lambda} \subset \operatorname{Ker} H^E_{\underline{\mathbf{1}}_v} \subset I(v)$. This implies $\operatorname{Ker} H^E_{\Lambda} \subset I(V_{\mathbb{R}}(G)) = \sqrt[\mathbb{R}]{G}$. □

Given a subset $F \subset \mathbb{R}[\mathbf{x}]$ and $t \in \mathbb{N}$, consider for G the prolongation $\langle F \,|\, 2t\rangle$ of F to degree $2t$, and the subspace $E = \mathbb{R}[\mathbf{x}]_t$. For simplicity in the notation we set

$$\mathcal{K}_{F,t,\succcurlyeq} := \mathcal{K}_{\langle F \,|\, 2t\rangle,\mathbb{R}[\mathbf{x}]_t,\succcurlyeq}, \tag{14}$$

which is thus contained in $\sqrt[\mathbb{R}]{(F)}$, by Theorem 4.9. The next result (from [12]) shows that equality holds for t large enough.

Theorem 4.10. [12] *Let* $F \subset \mathbb{R}[\mathbf{x}]$. *There exists* $t_0 > 0$ *such that* $(\mathcal{K}_{F,t,\succcurlyeq}) = \sqrt[\mathbb{R}]{(F)}$ *for all* $t \geq t_0$.

5. Algorithm

In this section, we describe the new algorithm to compute the (real) radical of an ideal. But before, we recall the graded moment matrix approach for computing the real radical developed in [13], and the border basis algorithm developed in [17].

5.1. **The graded moment matrix algorithm.** In the graded approach, the following family of spaces is considered:

$$\begin{aligned}\mathcal{L}_{F,t,\succeq} &:= \mathcal{L}_{\langle F \,|\, 2\,t\rangle,\mathbb{R}[\mathbf{x}]_t,\succeq}\\ &= \{\Lambda \in \mathbb{R}[\mathbf{x}]_{2\,t} \mid \forall f \in \langle F \,|\, 2\,t\rangle, \Lambda(f) = 0 \,\text{and}\, \forall p \in \mathbb{R}[\mathbf{x}]_t, \Lambda(p^2) \geq 0\}.\end{aligned}$$

For $\Lambda \in \mathcal{L}_{F,t,\succeq}$, let $H^t_{\Lambda} := H^{\mathbb{R}[\mathbf{x}]_t}_{\Lambda}$.

Algorithm 5.1 presents the graded moment matrix algorithm described in [12].

This algorithm requires in the first step to solve semi-definite programming problems on matrices of size the number of all monomials in degree t. This number is growing very quickly with the degree when the number of variables is important, which significantly slows down the performance of the method when several loops are necessary. The extension to compute the radical is also possible with this approach by doubling the variables and by embedding the problem over $\mathbb{C}^n$ in $\mathbb{R}^{2\,n}$. The correctness of the algorithm relies on Theorem 4.10 which comes from [12].

Algorithm 5.1: Graded Real Radical

Input: a finite family F of polynomials of $\mathbb{R}[\mathbf{x}]$.
Set $t := 1$ and $\delta = \max\{\deg(f), f \in F\}$;

(1) Choose a generic Λ in $\mathcal{L}_{F,t,\succeq}$;
(2) Check wether $\operatorname{rank} H_\Lambda^s = \operatorname{rank} H_\Lambda^{s+1}$ for some s such that $\delta \leq s < t$;
(3) If not, increase $t := t + 1$ and repeat from step (1);
(4) Compute $\operatorname{Ker} H_\Lambda^s$;

Output: $\sqrt[\mathbb{R}]{(F)} = (\ker H_\Lambda^s)$.

5.2. **The border basis algorithm.** Algorithm 5.2 presents the border basis algorithm described in [17]. Hereafter, we analyze shortly the different steps.

Algorithm 5.2: Border Basis

Input: a family F of polynomials of $\mathbb{K}[\mathbf{x}]$.
Set $t := 0$, $\mathcal{B} := \{1\}$, $G := \emptyset$ and $\delta = \max\{\deg(f), f \in F\}$;

(1) Compute the reduction $\tilde{F}$ of F_{t+1} on $\langle \mathcal{B} \rangle_{t+1}$ with respect to G;
(2) Set $t' := \min\{\deg(p), p \in \tilde{F}, p \neq 0\} - 1$;
(3) Compute a minimal $\tilde{G}$ such that $\langle \tilde{G} \rangle := \langle G^+, \tilde{F} \rangle \cap \langle \mathcal{B}^+ \rangle_{t'+1}$;
(4) Set $t'' = \min\{\deg(p), p \in \tilde{G} \cap \langle \mathcal{B} \rangle, p \neq 0\} - 1$; Compute $\tilde{\mathcal{B}}$ connected to 1 such that $\langle \mathcal{B}^+ \rangle_{t''+1} := \langle \tilde{\mathcal{B}} \rangle_{t''+1} \oplus \langle \tilde{G} \rangle_{t''+1}$;
(5) Compute a rewriting family G'' of $\tilde{G}_{t''+1}$ with respect to $\tilde{\mathcal{B}}_{t''+1}$;
(6) If $G'' \neq G$ or $\tilde{\mathcal{B}} \neq \mathcal{B}$ or $t'' < \delta$ then set $t := t'' + 1$, $\mathcal{B} := \tilde{\mathcal{B}}$, $G := G''$ and repeat from step (1);

Output: the border basis G of (F) with respect to $\mathcal{B}$.

In step (1), the reduction of a polynomial p by a rewriting family G for a set $\mathcal{B}$ consists of the following procedure: For each monomial $\mathbf{x}^\alpha$ of the support of p which is of the form $\mathbf{x}^\alpha = x_i \, \mathbf{x}^{\alpha'} \, \mathbf{x}^{\alpha''}$ with $\mathbf{x}^{\alpha'} \in \mathcal{B}$ and $\mathbf{x}^{\alpha''}$ of the smallest possible degree, if there exists an element $g = x_i \, \mathbf{x}^{\alpha'} - r \in G$ with $r \in \langle \mathcal{B} \rangle$, then the monomial $\mathbf{x}^\alpha$ is replaced by $\mathbf{x}^{\alpha''} \, r$. This is repeated until all monomials of the remainder are in $\mathcal{B}$.

Step (3) consists of the following steps: take the coefficient matrix $M = [M_0|M_1]$ of the polynomials in $G^+ \cup \tilde{F}$ where the block M_0 is indexed by the monomials in $\partial\mathcal{B}^+$ and the block M_1 is indexed by the monomials in $\mathcal{B}$ for a given ordering of the monomials, compute a row-echelon reduction $\tilde{M}$ of M, and deduce the polynomials of $\tilde{G}$ corresponding to the non-zero rows of $\tilde{M}$. For $p \in \tilde{G}$ corresponding to a non-zero row of $\tilde{M}$, the monomial indexing its first non-zero coefficients is denoted $\gamma(p)$. Notice that $\langle \tilde{G} \rangle := \langle G^+, \tilde{F} \rangle \cap \langle \mathcal{B}^+ \rangle_{t'+1}$ contains the elements of $C^+(G_{t'})$.

Step (4) consists

- of removing the monomials $\gamma(p)$ for $p \in \langle \tilde{G}_{t''+1} \rangle \cap \langle \mathcal{B} \rangle_{t''+1}$, and
- of adding the monomials in $\partial\mathcal{B} \setminus \{\gamma(p) \mid p \in \tilde{G}\}$ of degree $\leq t'' + 1$.

Step (5) consists of auto-reducing the polynomials $p \in \tilde{G}$ of degree $\leq t''$ so that $\gamma(p)$ is the only term of p in $\partial\tilde{\mathcal{B}}$. This is done by inverting the coefficient matrix of $\tilde{G}$ with respect to the monomials in $\partial\tilde{\mathcal{B}}$. Notice that as $\langle \mathcal{B}^+ \rangle_{t''+1} := \langle \tilde{\mathcal{B}} \rangle_{t''+1} \oplus \langle \tilde{G} \rangle_{t''+1}$, $\tilde{G}$ is complete in degree $t''+1$.

In step (6), if the test is valid then the loop start again with G a rewriting family of degree t with respect to $\mathcal{B}$, which is by definition included in $\langle \mathcal{B}^+ \rangle_t$. Thus, at each loop, $\tilde{G}$ contains G and $C^+(G) \subset \langle G^+ \rangle \cap \langle \mathcal{B}^+ \rangle_{t+1} \subset \langle \tilde{G} \rangle$.

The algorithm stops if $G'' = G$ and $\tilde{\mathcal{B}} = \mathcal{B}$ and $t \geq \delta$. Then $t'' = t$, $\tilde{G} = G$ and $C^+(G) \subset \tilde{G} = G$ is reduced to 0 by G. If G is a rewriting family complete in degree t for $\mathcal{B}$, we deduce by Theorem 2.12 that $\pi_{G,\mathcal{B}}$ is the projection of $\mathbb{K}[\mathbf{x}]_t$ on $\langle \mathcal{B} \rangle_t$ along $\langle G \,|\, t \rangle$. As $\tilde{\mathcal{B}} = \mathcal{B}$, we also have $t \geq \max\{\deg(b) \mid b \in \mathcal{B}\}$ so that G is a border basis with respect to $\mathcal{B}$. As $t \geq \delta$, the elements of F reduce to 0 by $G \subset F$. Thus $(G) = (F)$.

It is proved in [17] that this algorithm stops when the ideal (F) is zero-dimensional. Thus its output G is the border basis of the ideal (F) with respect to $\mathcal{B}$.

5.3. **$\mathbb{K}$-Radical Border Basis algorithm.** Our new radical border basis algorithm can be seen as a combination of the graded real radical algorithm and the border basis algorithm. The modification of the border basis algorithm consists essentially of generating new elements of the (real) radical of the ideal at each loop (step (1′) in Algorithm 5.3), and to use these new relations (which are in the (real) radical by Theorem 4.6 and Theorem 4.9) in step (3). In the case when $\mathbb{K} = \mathbb{C}$, a final stage is added to get the generators of the radical of a Gorenstein ideal (step (7) below).

Algorithm 5.3: $\mathbb{K}$-Radical Border Basis

Input: a family F of polynomials of $\mathbb{K}[\mathbf{x}]$.
Set $t = 0$, $\mathcal{B} = \{1\}$, and $G = \emptyset$;

(1′) *Compute a (maximal) $S \subset \mathcal{B}_{t+1}$ such that $S \cdot S$ can be reduced by G onto $\mathcal{B}_{t+1}$ and* $K := \text{GenericKernel}_{\mathbb{K}}(G, \mathcal{B}, S)$*;*
(1) Compute the reduction $\tilde{F}$ of F_{t+1} on $\langle \mathcal{B}^+ \rangle_{t+1}$ with respect to G;
(2) *Set* $t' := \min\{\deg(p), p \in \tilde{F} \cup K, p \neq 0\} - 1$*;*
(3) *Compute* $\tilde{G}$ *such that* $\langle \tilde{G} \rangle := \langle G^+, \tilde{F}, K \rangle \cap \langle \mathcal{B}^+ \rangle_{t'+1}$*;*
(4) Compute $\tilde{\mathcal{B}}$ connected to 1 and $t'' \leq t'$ maximal such that $\langle \mathcal{B}^+ \rangle_{t''+1} := \langle \tilde{\mathcal{B}} \rangle_{t''+1} \oplus \langle \tilde{G} \rangle_{t''+1}$;
(5) Compute a rewriting family G'' of $\tilde{G}_{t''+1}$ with respect to $\tilde{\mathcal{B}}$;
(6) If $G'' \neq G$ or $\tilde{\mathcal{B}} \neq \mathcal{B}$ or $t'' < \delta$ then set $t := t'' + 1$, $\mathcal{B} := \tilde{\mathcal{B}}$, $G := G''$ and repeat from step (1);
(7) *if* $\mathbb{K} = \mathbb{C}$ *then* $[G, \mathcal{B}] := \text{Socle}(G, \mathcal{B}, \Lambda)$*;*

Output: The border basis G of the ideal $\sqrt[\mathbb{K}]{(F)}$ with respect to $\mathcal{B}$.

The two new ingredients that we describe below are the function GenericKernel (see Algorithm 5.4) used to generate new polynomials in the (real) radical, and the function Socle (see Algorithm 5.5) which computes the generators of the radical from the border basis of a Gorenstein ideal when $\mathbb{K} = \mathbb{C}$.

Definition 5.1. *Given a rewriting family F with respect to $\mathcal{B}$ and $S = \{\mathbf{x}^{\beta_1}, \ldots, \mathbf{x}^{\beta_l}\}$, we define F^{red} as the following family of polynomials : For all $\mathbf{x}^{\beta_i}, \mathbf{x}^{\beta_j} \in S$ such that $\pi_{F,\mathcal{B}}(\mathbf{x}^{\beta_i+\beta_j})$ exists and is in $\langle S \cdot S \rangle$, we define $\kappa_{\beta_i+\beta_j}(\mathbf{x}) = \mathbf{x}^{\beta_i+\beta_j} - \pi_{F,\mathcal{B}}(\mathbf{x}^{\beta_i+\beta_j})$ and $\kappa_{\beta_i+\beta_j} = 0$ otherwise.*

With F^{red} as in Definition 5.1, we are going to analyze the corresponding spaces $\mathcal{L}_{F^{\text{red}},S}$, $\mathcal{L}_{F^{\text{red}},S,\succeq}$, $\mathcal{K}_{F^{\text{red}},S}$, $\mathcal{K}_{F^{\text{red}},S,\succeq}$. Notice that by construction $F^{\text{red}} \subset \langle F \,|\, t \rangle$ where $t = 2\max\{\deg(s) \mid s \in S\}$.

The construction of the generic kernel $\mathcal{K}_{F^{\text{red}},S}$ (resp., $\mathcal{K}_{F^{\text{red}},S,\succcurlyeq}$) is implemented by Algorithm 5.4. This routine is the one that is executed for finding effectively new equations in the (real) radical.

Notice that primal-dual interior point solver implementing a self dual embedding do return such a solution automatically. For a remark on how to use other solvers, see [12, Remark 4.15].

Algorithm 5.4: GenericKernel$_{\mathbb{K}}(F, \mathcal{B}, S)$

Input: A rewriting family F with respect to $\mathcal{B}$ allowing reduction for all the monomials in $S \cdot S$.

(1) If $\mathbb{K} = \mathbb{C}$, we construct an element $\Lambda \in \mathcal{L}_{F^{\mathrm{red}},S}$ such that H^S_Λ has maximal rank, by taking a generic element of the linear space $\mathcal{L}_{F^{\mathrm{red}},S}$.

(2) If $\mathbb{K} = \mathbb{R}$, we construct an element of $\Lambda \in \mathcal{L}_{F^{\mathrm{red}},S,\succcurlyeq}$ such that H^S_Λ has maximal rank, by computing an element in the relative interior of the feasible region of the following *semi-definite programming problem*:
   - $H = (h_{\alpha,\beta})_{\alpha,\beta\in S} \succcurlyeq 0$
   - H satisfies the Hankel constraints $h_{0,0} = 1$, $h_{\alpha,\beta} = h_{\alpha',\beta'}$ if $\alpha + \beta = \alpha' + \beta'$.
   - H satisfies the linear constraints $\sum_\alpha h_\alpha \kappa_{\beta,\alpha} = 0$ for all $\beta \in S \cdot S$ such that $\kappa_\beta = \sum_\alpha \kappa_{\beta,\alpha}\, \mathbf{x}^\alpha \neq 0$.

(3) Then we compute K as a basis of the kernel of H^S_Λ.

Output: A family K of polynomials in $\sqrt[\mathbb{K}]{(F)}$.

Algorithm 5.5: Socle$(G, \mathcal{B}, \Lambda)$

Input: A border basis G for $\mathcal{B}$ connected to 1 and $\Lambda \in \langle \mathcal{B}\cdot\mathcal{B}\rangle^*$ such that $H^{\mathcal{B}}_\Lambda$ is invertible.

(1) Compute a dual basis of $\mathcal{B} = \{b_1, \ldots, b_r\}$ as follows: $[d_1, \ldots, d_r] = H^{-1}[b_1, \ldots, b_r]$ where $H = (\Lambda(b_i b_j))_{1\le i,j\le r}$ is the matrix of $H^{\mathcal{B}}_\Lambda$;

(2) Compute $\Delta = \sum_{i=1}^r b_i\, d_i$ and the matrix $H_\Delta = (\Lambda(\Delta\, b_i\, b_j))_{1\le i,j\le r}$ by reduction of the elements $\Delta\, b_i\, b_j$ by G to linear combinations of elements in $\mathcal{B}$;

(3) Compute $G' = \ker H_\Delta$ and apply the normal form algorithm to $G' \cup G$ in order to deduce a basis $\tilde{\mathcal{B}} \subset \mathcal{B}$ connected to 1 and a border basis G'' for $\tilde{\mathcal{B}}$ such that $(G'') = (G' \cup G) = \sqrt{F}$.

Output: A basis $\tilde{\mathcal{B}}$ connected to 1 and a border basis G'' of $\sqrt{(F)}$ for $\tilde{\mathcal{B}}$.

6. Correctness of the algorithms

In this section, we analyse separately the correctness of the algorithm over $\mathbb{R}$ and $\mathbb{C}$.

6.1. Correctness for real radical computation.

We prove first the correctness of Algorithm 5.3 over $\mathbb{R}$.

Lemma 6.1. *If G is a rewriting family complete in degree $2\,t$ for $\mathcal{B}$, then for $\Lambda \in \langle G \,|\, 2\,t\rangle^\perp$*

$$\operatorname{Ker} H^{\mathbb{K}[\mathbf{x}]_t}_\Lambda \equiv \operatorname{Ker} H^{\mathcal{B}_t}_\Lambda \mod \langle G \,|\, t\rangle.$$

Proof. For $\Lambda \in \langle G \,|\, 2\,t\rangle^\perp$, we have

$$\begin{aligned} p \in \operatorname{Ker} H^{\mathbb{K}[\mathbf{x}]_t}_\Lambda &\Leftrightarrow \Lambda(p\,q) = 0 \ \forall q \in \mathbb{K}[\mathbf{x}]_t \\ &\Leftrightarrow \Lambda(b\,q) = 0 \ \forall q \in \mathbb{K}[\mathbf{x}]_t \text{ where } b \in \langle\mathcal{B}\rangle_t = p \mod \langle G \,|\, t\rangle \\ &\Leftrightarrow \Lambda(b\,b') = 0 \ \forall b \in \langle\mathcal{B}\rangle_t \\ &\Leftrightarrow b \in \operatorname{Ker} H^{\mathcal{B}_t}_\Lambda. \end{aligned}$$

Therefore

$$\operatorname{Ker} H^{\mathbb{K}[\mathbf{x}]_t}_\Lambda \equiv \operatorname{Ker} H^{\mathcal{B}_t}_\Lambda \mod \langle G \,|\, t\rangle,$$

which proves the equality of the two kernels modulo $\langle G \,|\, t\rangle$. □

Lemma 6.2. *If G is a rewriting family complete in degree $2\,t$ for $\mathcal{B}$, such that $\mathbb{K}[\mathbf{x}]_{2\,t} = \langle\mathcal{B}\rangle_{2\,t} \oplus \langle G \,|\, 2\,t\rangle$, then*

$$\langle \mathcal{K}_{G,t,\succeq} \,|\, t\rangle \equiv \langle \mathcal{K}_{G^{\mathrm{red}},\mathcal{B}_t,\succeq} \,|\, t\rangle \mod \langle G \,|\, t\rangle.$$

Proof. Let $\Lambda \in \langle G \,|\, 2\,t\rangle^\perp$ be a generic element such that $\mathcal{K}_{G,t,\succeq} = \operatorname{Ker} H_\Lambda^{\mathbb{K}[\mathbf{x}]_t}$. By Lemma 6.1 and Proposition 4.7, we have

$$\mathcal{K}_{G,t,\succeq} = \operatorname{Ker} H_\Lambda^{\mathbb{K}[\mathbf{x}]_t} \equiv \operatorname{Ker} H_\Lambda^{\mathcal{B}_t} \mod \langle G \,|\, t\rangle \supset \mathcal{K}_{\mathcal{B}_t,\succeq} \mod \langle G \,|\, t\rangle.$$

Conversely, let $\Lambda \in \langle G^{\mathrm{red}}\rangle^\perp$ be a generic element such that $\mathcal{K}_{G,\mathcal{B}_t,\succeq} = \operatorname{Ker} H_\Lambda^{\mathcal{B}_t}$. As $\langle G^{\mathrm{red}}\rangle \subset \langle G \,|\, 2\,t\rangle$, there exists $\tilde{\Lambda} \in \langle G \,|\, 2\,t\rangle^\perp$ which extends Λ to $\mathbb{K}[\mathbf{x}]_t$. Then we have

$$\begin{aligned} \mathcal{K}_{G,\mathcal{B}_t,\succeq} &= \operatorname{Ker} H_\Lambda^{\mathcal{B}_t} = \operatorname{Ker} H_{\tilde{\Lambda}}^{\mathcal{B}_t} \\ &\equiv \operatorname{Ker} H_{\tilde{\Lambda}}^{\mathbb{K}[\mathbf{x}]_t} \mod \langle G \,|\, t\rangle \supset \mathcal{K}_{G,t,\succeq} \mod \langle G \,|\, t\rangle. \end{aligned}$$

□

Lemma 6.3. *If Algorithm 5.3 terminates with outputs G and $\mathcal{B}$, then $(G) = \sqrt[\mathbb{R}]{(F)}$ and $\mathcal{B}$ is a basis of $\mathbb{K}[\mathbf{x}]/\sqrt[\mathbb{R}]{(F)}$.*

Proof. If the algorithm stops, all boundary polynomials of $C^+(G)$ reduce to 0 by G. By Theorem 2.12, for all t we have $\mathbb{K}[\mathbf{x}]_{2\,t} = \langle \mathcal{B}\rangle_{2\,t} \oplus \langle G \,|\, 2\,t\rangle$. As $\mathcal{K}_{G^{\mathrm{red}},\mathcal{B}_t,\succeq} = \{0\}$ by Lemma 6.2, we deduce that

$$\mathcal{K}_{G,t,\succeq} \subset \langle G \,|\, t\rangle.$$

By Theorem 4.10, there exists s_0 such that

$$(\mathcal{K}_{F,s_0,\succeq}) = \sqrt[\mathbb{R}]{I},$$

where $I = (F)$. By lemma 4.8, for $t \geq s_0$,

$$\mathcal{K}_{F,s_0,\succeq} \subset \mathcal{K}_{G,t,\succeq} \subset \langle G \,|\, t\rangle \subset \sqrt[\mathbb{R}]{I},$$

which implies that $(G) = \sqrt[\mathbb{R}]{I}$. □

Proposition 6.4. *Assume that $V_{\mathbb{R}}(F)$ is finite. Then the algorithm 5.3 terminates. It outputs a border basis G for $\mathcal{B}$ connected to 1, such that $\mathbb{R}[\mathbf{x}] = \langle \mathcal{B}\rangle \oplus (G)$ and $(G) = \sqrt[\mathbb{R}]{I}$.*

Proof. First, we are going to prove by contradiction that when the number of real roots is finite, the algorithm terminates.

Suppose that the loop goes for ever. Notice that at each step either G is extended by adding new linearly independent polynomials or it moves to degree $t+1$. Since the number of linearly independent polynomials added to G in degree $\leq t$ is finite, there is a step in the loop from which G is not modified any more. In this case, all boundary C-polynomials of elements of G of degree $\leq t$ are reduced to 0 by G_t. By Theorem 2.12, we have

$$\mathbb{R}[\mathbf{x}]_t = \langle \mathcal{B}\rangle_t \oplus \langle G_t \,|\, t\rangle. \tag{15}$$

We have assumed that the loop goes for ever, thus this property is true for any degree t. By Theorem 4.10, there exists s_0 such that

$$(\mathcal{K}_{F,s_0/2,\succeq}) = \sqrt[\mathbb{R}]{I}.$$

As any element of $\langle F \,|\, s_0\rangle$ reduces to 0 by the rewriting family G_{s_0}, we have $\langle F \,|\, s_0\rangle \subset \langle G_{s_0} \,|\, s_0\rangle$. By Lemma 4.8, we deduce that

$$\mathcal{K}_{F,s_0/2,\succeq} \quad \subset \quad \mathcal{K}_{G_{s_0},s_0/2,\succeq}.$$

For a high enough number of loops, the set G_{s_0} is not modified and we have $\mathcal{K}_{G_{s_0},\mathcal{B}_{s_0/2},\succeq} = \{0\}$. Applying Lemma 6.2 using Equation (15), we have

$$\mathcal{K}_{G_{s_0},s_0/2,\succeq} \subset \langle G_{s_0} \,|\, s_0\rangle$$

By construction $G_{s_0} \subset \sqrt[\mathbb{R}]{I}$, thus

$$(G_{s_0}) = \sqrt[\mathbb{R}]{I}.$$

Let $\mathcal{B}_0 \subset \mathbb{R}[\mathbf{x}]$ which defines a basis in $\mathbb{R}[\mathbf{x}]/\sqrt[\mathbb{R}]{I}$ and of smallest possible degree and let d_0 be the maximum degree of its elements. Then any monomial m of degree d_0+1 is equal modulo $(\sqrt[\mathbb{R}]{I})_{d_0+1}$ to an element b in $\langle \mathcal{B}_0 \rangle$ of degree $\leq d_0$.

By Theorem 2.13,

$$\langle G_{d_0+1} \,|\, d_0+1 \rangle = (\sqrt[\mathbb{R}]{I})_{d_0+1},$$

thus $m - b \in \langle G_{d_0+1} \,|\, d_0+1 \rangle$ so that any monomial of degree d_0+1 can be reduced by G to a polynomial in $\mathbb{K}[\mathbf{x}]_{d_0}$. Thus $\mathcal{B} = \cap_{f\in G}(\gamma(f))^c \subset \mathbb{R}[\mathbf{x}]_{d_0}$ is finite and the algorithm terminates.

By Lemma 6.3, the algorithm outputs a border basis G with respect to $\mathcal{B}$ connected to 1, such that $(G) = \sqrt[\mathbb{R}]{I}$. □

6.2. **Correctness for the radical computation.** In this section, we show the correctness of the algorithm for radical computation, that is with $\mathbb{K} = \mathbb{C}$.

Proposition 6.5. *Assume that $V_{\mathbb{C}}(F)$ is finite. Then the algorithm 5.3 terminates and outputs a border basis G for $\mathcal{B}$ connected to 1, such that $(G) = \sqrt{I}$ and $\mathbb{C}[\mathbf{x}] = \langle \mathcal{B} \rangle \oplus \sqrt{I}$.*

Proof. Since the family G contains the polynomials constructed by the normal form algorithm [17] and as $V_{\mathbb{C}}(I)$ is zero-dimensional, the normal form algorithm terminates and so do algorithm 5.3. When the loop stops, all boundary polynomials of $C^+(G)$ for any degree reduce to 0 by G and $\mathcal{K}_{G^{\mathrm{red}},\mathcal{B}} = \{0\}$. By Theorem 2.13, G is a border basis with respect to $\mathcal{B}$. Let $\Lambda \in \langle \mathcal{B}\cdot\mathcal{B} \rangle^*$ such that $\mathcal{K}_{G^{\mathrm{red}},\mathcal{B}} = \operatorname{Ker} H^{\mathcal{B}}_{\Lambda}$. By definition of Λ and normal form property, if $f \in \langle \mathcal{B}\cdot\mathcal{B} \rangle \cap (G)$ then f reduces to 0 by G and $\Lambda(f) = 0$. This shows that we can extend Λ to $\tilde{\Lambda} \in \mathbb{C}[\mathbf{x}]^*$ by $\tilde{\Lambda} = \Lambda$ on $\langle \mathcal{B} \rangle$ and $\tilde{\Lambda} = 0$ on (G). We deduce that $(G) = \operatorname{Ker} H_{\tilde{\Lambda}}$ and that $\mathcal{A}_\Lambda = \mathbb{C}[\mathbf{x}]/\operatorname{Ker} H_{\tilde{\Lambda}} = \mathbb{C}[\mathbf{x}]/(G)$ is Gorenstein. Let $d_1, \ldots, d_r$ be the dual basis of $\mathcal{B}$ for Q_Λ and $\Delta = \sum_{i=1}^r b_i\, d_i$. By Theorem 3.10, $\operatorname{Ker} H^{\mathcal{B}}_{\Delta\cdot\Lambda}$ computed in the function Socle, yields a new basis $\mathcal{B}'$ connected to 1 and a new border basis G' such that $(G') = \sqrt{I}$. □

7. Examples

This section contains two very simple examples which illustrate the effect of the SDP solution in one loop of the Real Radical Border Basis algorithm. The results in the next example are coming from a `C++` implementation available in the package `newmac` of the project MATHEMAGIX. It uses a version of `lapack` with templated coefficients and `sdpa` [2] with extended precision so that all the computation can be run with extended precision arithmetic.

7.1. **A univariate example.** We give here a simple example in one variable to show how the real roots can be separated from the complex roots, using this algorithm. We consider the polynomial $f = x^4 - x^3 - x + 1$ with a single real root $x = 1$ of multiplicity 2. In the routine GenericKernel of the algorithm, a 4×4 matrix H is constructed and the linear constraints deduced from the relations $x^4 \equiv x^3 + x - 1$, $x^5 \equiv x^3 + x^2 - 1$, $x^6 \equiv 2\,x^3 - 1$ modulo f imposes the following form:

$$H := \begin{pmatrix} 1 & a & b & c \\ a & b & c & c+a-1 \\ b & c & c+a-1 & c+b-1 \\ c & c+a-1 & c+b-1 & 2\,c-1 \end{pmatrix}.$$

where $a = \Lambda(x), b = \Lambda(x^2), c = \Lambda(x^3)$. The SDP solver yields the solution

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

[2] `http://sdpa.sourceforge.net/`

which kernel is $\langle x-1, x^2-x, x^3-x^2\rangle$. Thus the output of the algorithm is $(x-1)$ the real radical of (f), the basis $\mathcal{B}=\{1\}$ and the real root $x=1$.

7.2. **A very simple bivariate example.** Let $f_1 = x^2+y^2$ and $F=\{f_1\}\subset\mathbb{R}[x,y]$. The algorithm computes the following:

- $\mathcal{B}=\mathcal{M}-(y^2)$
- We compute GenericKernel in degree 1 by choosing $S=\{1,x,y\}$ with $S\cdot S\supset$ support f_1.

  The SDP problem to solve reads as follows: find $h=[a,b,c,d]\in\mathbb{R}^4$ such that

$$H=\begin{pmatrix}1 & a & b\\ a & c & d\\ b & d & -c\end{pmatrix}\succcurlyeq 0$$

  and has of maximal rank. Here $a=\Lambda(x), b=\Lambda(y), c=\Lambda(x^2), d=\Lambda(x\,y)$. The condition $H\succcurlyeq 0$ implies that
  - $c=0$,
  - $a=0, b=0, d=0$.

  and consequently that $\ker H=\langle x,y\rangle$. Thus x,y are returned by GenericKernel and added to F.
- After one iteration the border basis algorithm stops and we obtain $\mathcal{B}=\{1\}$ and $\sqrt[\mathbb{R}]{(x^2+y^2)}=(x,y)$.

7.3. **Numerical example.** The tables below compare the size of the SDP problems to solve in our approach and in the method described in [12]. The *degree* indicates the degree in the loop of the Border Basis Real radical algorithm, *n.sdp* is the size of matrices in the corresponding SDP problem and *n.constraints* the number of linear constraints involved, t is the degree of the relaxation problem in [12] and *n.sdp grad. rel.* the size of matrices in the corresponding SDP problem.

Katsura 4				
degree	*n.sdp*	*n.constraints*	t	*n.sdp grad. rel.*
2	5	5	2	56
4	11	67	2	56
6	16	176	2	56

Katsura 5				
degree	*n.sdp*	*n.constraints*	t	*n.sdp grad. rel.*
2	6	6	3	84
4	16	146	3	84
6	26	479	3	84

bifur				
degree	*n.sdp*	*n.constraints*	t	*n.sdp grad. rel.*
2	4	2	8	165
4	9	32	8	165
6	16	150	8	165
8	25	446	8	165
8	16	152	8	165
8	16	153	8	165
6	16	158	8	165
6	16	162	8	165
4	9	34	8	165
6	16	168	8	165
6	16	169	8	165
4	9	36	8	165
6	16	177	8	165
4	4	3	8	165
4	8	37	8	165

The tables below give the time for computing the real radical with the solvers `sdpa`[3] or `csdp`[4] integrated into the border basis algorithm available in the package `newmac` of MATHEMAGIX.

Example	$T_{\mathbb{R}}$	*Gen. Ker.*	*CSDP*	*SVD Drop*	*Deg*	$Deg_{\mathbb{C}}$	$N_{\mathbb{R}}$	$N_{\mathbb{C}}$	$T_{\mathbb{C}}$
Precision 90									
*kat*4	22.479s	22.281s	22.1645	$1e-12$	4	4	12	16	0.06s
*kat*5	146.49s	146.29s	145.64s	$1e-12$	5	5	16	32	0.165s
cyclo	10.839s	10.7646s	10.6243s	$1e-20$	5	5	4	16	0.03s
robot	41.84s	41.52s	41.26s	$1e-19$	6	8	4	40	1.3s
Precision 120									
*kat*4	22.557s	22.28s	22.16	$1e-14$	4	4	12	16	0.06s
*kat*5	146.59s	146.39s	145.1s	$1e-12$	5	5	16	32	0.17s
cyclo	10.839s	10.7646s	10.6243s	$1e-20$	5	5	4	16	0.03s
robot	42.884s	42.5216s	42.2447s	$1e-19$	6	8	4	40	1.4s

A precision of 90 or 120 bits is used during the computation but unfortunately the SDP solver is very, very, very slow for this precision. A strange behavior/bug of the parameter used in the relaxation of the barrier function is observed. The solution of this problem is in progress.

Example	$T_{\mathbb{R}}$	*Gen. Ker.*	$SDPA-GMP$	*SVD Drop*	*Deg*	$Deg_{\mathbb{C}}$	$N_{\mathbb{R}}$	$N_{\mathbb{C}}$	$T_{\mathbb{C}}$
Precision 90									
*kat*4	4.18s	4.12s	3.26	$1e-18$	4	4	12	16	0.06
*kat*5	26.28s	26.01s	23.16s	$1e-18$	5	5	16	32	0.165
cyclo	10, 95	10.77	10.64	$1e-20$	5	5	4	16	0.03
robot	19, 84	19.52	19.26	$1e-19$	6	8	4	40	1.3s

Using `SDPA-gmp` as the solver allows us a great improvement in efficiency though we expect futher improvements improving both the way connection with `SDPA-gmp` is operated and better tuning the parameters `SDPA`.

References

[1] E. Becker and R. R. Neuhaus. On the computation of the real radical. *Journal of Pure and Applied Algebra, 124:261280,*, 124:261280, 1998.

[3] `http://sdpa.sourceforge.net/`

[4] `https://projects.coin-or.org/Csdp/`

[2] A. Bernardi, J. Brachat, P Comon, and B. Mourrain. Multihomogeneous polynomial decomposition using moment matrices. In A. Leytkin, editor, *International Symposium on Symbolic and Algebraic Computation (ISSAC)*, page 35-42, ACM Press, 2011.
[3] J. Bochnak, M. Coste, and M.-F. Roy. *Real Algebraic Geometry*. Springer, 1998.
[4] D. Cox. Solving equations via algebra. In A. Dickenstein and I. Z. Emiris, editors, *Solving Polynomial Equations: Foundations, Algorithms, and Applications*, volume 14 of *Algorithms and Computation in Mathematics*. Springer, 2005.
[5] D.A. Cox, J.B. Little, and D.B. O'Shea. *Using Algebraic Geometry*. Springer, 1998.
[6] D.A. Cox, J.B. Little, and D.B. O'Shea. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra (Undergraduate Texts in Mathematics)*. Springer, July 2005.
[7] R.E. Curto and L. Fialkow. Solution of the truncated complex moment problem for flat data. *Memoirs of the American Mathematical Society*, 119(568):1–62, 1996.
[8] M. Elkadi and B. Mourrain. *Introduction à la résolution des systèmes d'équations algébriques*, volume 59 of *Mathématiques et Applications*. Springer-Verlag, 2007.
[9] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner Free Alternative for Solving Polynomial Systems. *Journal of Complexity*, 17(1):154–211, 2001.
[10] I. Janovitz-Freireich, A. Szántó, B. Mourrain, and L. Ronyai. Moment matrices, trace matrices and the radical of ideals. In *ISSAC '08: Proceedings of the twenty-first international symposium on Symbolic and algebraic computation*, pages 125–132, New York, NY, USA, 2008. ACM.
[11] L. Kronecker. Grundzüge einer Arithmetischen Theorie de Algebraischen Grössen. *Journal Reine Angew Mathematik*, 92:1–122, 1882.
[12] J.B. Lasserre, M. Laurent, and P. Rostalski. Semidefinite characterization and computation of real radical ideals. *Foundations of Computational Mathematics*, 8(5):607–647, 2008.
[13] J.B. Lasserre, M. Laurent, and P. Rostalski. A unified approach for real and complex zeros of zero-dimensional ideals. In M. Putinar and S. Sullivant, editors, *Emerging Applications of Algebraic Geometry.*, volume 149, pages 125–156. Springer, 2009.
[14] M. Laurent. Semidefinite representations for finite varieties. *Math. Progr*, 109:1–26, 2007.
[15] M. Laurent and B. Mourrain. A generalized flat extension theorem for moment matrices. *Arch. Math. (Basel)*, 93(1):87–98, July 2009.
[16] B. Mourrain. A new criterion for normal form algorithms. In M. Fossorier, H. Imai, Shu Lin, and A. Poli, editors, *Proc. AAECC*, volume 1719 of *LNCS*, pages 430–443. Springer, Berlin, 1999.
[17] B. Mourrain and P. Trébuchet. Generalized normal forms and polynomials system solving. In M. Kauers, editor, *ISSAC: Proceedings of the ACM SIGSAM International Symposium on Symbolic and Algebraic Computation*, pages 253–260, 2005.
[18] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Journal of Applicable Algebra in Engineering, Communication and Computing*, 9(5):433–461, 1999.
[19] A.J. Sommese and C.W. Wampler. *The Numerical Solution of Systems of Polynomials Arising in Engineering and Science*. World Scientific Press, Singapore, 2005.
[20] H.J. Stetter. *Numerical Polynomial Algebra*. SIAM, USA, 2004.
[21] J. Verschelde. PHCPACK: A general-purpose solver for polynomial systems by homotopy continuation.

J.B. Lasserre, LAAS, Toulouse, France

Monique Laurent, CWI, Amsterdam, Netherland

Bernard Mourrain, GALAAD INRIA, Sophia Antipolis, France

Philipp Rolstalki, University of Berkeley, USA

Philippe Trébuchet, LIP6, University Paris VI, France