A Certificate for Semidefinite Relaxations in Computing Positive-Dimensional Real Radical Ideals

Yue Ma, Chu Wang, Lihong Zhi

Key Lab of Mathematics Mechanization, AMSS
Beijing 100190, China

Abstract

For an ideal I with a positive-dimensional real variety $V_{\mathbb{R}}(I)$, based on moment relaxations, we study how to compute a Pommaret basis which is simultaneously a Gröbner basis of an ideal J generated by the kernel of a truncated moment matrix and satisfying $I \subseteq J \subseteq I(V_{\mathbb{R}}(I)), V_{\mathbb{R}}(I) = V_{\mathbb{C}}(J) \cap \mathbb{R}^n$. We provide a certificate consisting of a condition on coranks of moment matrices for terminating the algorithm. For a generic δ-regular coordinate system, we prove that the condition is satisfiable in a large enough order of moment relaxations.

Keywords: Real radical ideal, positive-dimensional ideal, semidefinite programming, involutive division, Pommaret basis, δ-regular.

1. Introduction

Finding real solutions of a polynomial system is a classical mathematical problem with wide applications. Let $I = \langle h_1, \ldots, h_m \rangle \subseteq \mathbb{R}[x] := \mathbb{R}[x_1, \ldots, x_n]$ be an ideal generated by polynomials $h_1, \ldots, h_m \in \mathbb{R}[x]$. Its complex and real algebraic varieties are defined as

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

The vanishing ideal of a set $V \subseteq \mathbb{C}^n$ is an ideal

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

Email addresses: yma@mmrc.iss.ac.cn (Yue Ma), cwang@mmrc.iss.ac.cn (Chu Wang), lzhi@mmrc.iss.ac.cn (Lihong Zhi)

The radical (also called complex radical) of I is

$$\sqrt{I} := \left\{ f \in \mathbb{C}[x] \,\middle|\, f^k \in I \ \text{ for some } k \in \mathbb{N} \right\},$$

while the real radical of I is defined as

$$\sqrt[\mathbb{R}]{I} := \left\{ f \in \mathbb{R}[x] \,\middle|\, f^{2k} + \sum_{i=1}^{r} q_i^2 \in I \ \text{ for some } k \in \mathbb{N},\, q_1, \ldots, q_r \in \mathbb{R}[x] \right\}.$$

Clearly, they satisfy the inclusion $I \subseteq \sqrt{I} \subseteq \sqrt[\mathbb{R}]{I}$. An ideal I is called *radical* (resp. *real radical*) if $I = \sqrt{I}$ (resp. $I = \sqrt[\mathbb{R}]{I}$). According to the Real Nullstellensatz Bochnak et al. (1998), the vanishing ideal $I(V_{\mathbb{R}}(I))$ of the zero set $V_{\mathbb{R}}(I)$ is a real radical ideal and $I(V_{\mathbb{R}}(I)) = \sqrt[\mathbb{R}]{I}$.

There exist numerical algorithms Janovitz-Freireich et al. (2012); Lasserre et al. (2009a,b) and symbolic algorithms Becker and Wörmann (1996); Gianni et al. (1988) for computing the radical ideal of a zero-dimensional ideal I. For the general case of I being positive-dimensional, a commonly used technique is to reduce the problem to the zero-dimensional case, like in Gianni, Trager and Zacharias Gianni et al. (1988) and Krick and Logar Krick and Logar (1991).

The problem of computing the real radical ideal $\sqrt[\mathbb{R}]{I}$ is typically much more difficult than computing $\sqrt{I}$. Becker and Neuhaus Becker and Neuhaus (1993) proposed a symbolic algorithm based on the primary decomposition to compute $\sqrt[\mathbb{R}]{I}$ (see also Neuhaus (1998); Silke (2007a); Xia and Yang (2002); Zeng (1999)). Some interesting algorithms based on critical point methods were proposed in Aubry et al. (2002); Bank et al. (2001); Basu et al. (1997); Safey El Din and Schost (2003) to compute a point on each semi-algebraically connected component of real algebraic varieties.

A new approach based on moment relaxations has been proposed by Lasserre et al. Lasserre et al. (2013, 2009a,b); Laurent and Rostalski (2010) for computing $\sqrt[\mathbb{R}]{I}$ when I has a zero-dimensional real variety. Hereby we briefly describe this interesting approach.

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

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

is a real symmetric matrix whose rows and columns are indexed by the set $\mathbb{T}^n := \{x^\alpha \mid \alpha \in \mathbb{N}^n\}$ of monomials. Given a polynomial $h \in \mathbb{R}[x]$, we set $\mathrm{vec}(h) := (h_\alpha)_{\alpha \in \mathbb{N}^n}$ and define the sequence $hy := M(y)\mathrm{vec}(h) \in \mathbb{R}^{\mathbb{N}^n}$. We say

that a polynomial p lies in the kernel of $M(y)$ when $M(y)p := M(y)\mathrm{vec}(p) = 0$. Given a truncated moment sequence $y = (y_\alpha)_{\alpha\in\mathbb{N}^n_{2t}} \in \mathbb{R}^{\mathbb{N}^n_{2t}}$, it defines a *truncated moment matrix*

$$M_t(y) := (y_{\alpha+\beta})_{\alpha,\beta\in\mathbb{N}^n_t}$$

indexed by the set $\mathbb{T}^n_t := \{x^\alpha \mid \alpha \in \mathbb{N}^n_t \text{ with } |\alpha| := \Sigma^n_{i=1}\alpha_i \le t\}$.

We work with the space $\mathbb{R}[x]_t$ of polynomials of the degree smaller than or equal to t. For a polynomial $p \in \mathbb{R}[x]_t$, if $M_t(y)\mathrm{vec}(p) = 0$, we say p lies in the kernel of $M_t(y)$, i.e.,

$$\ker M_t(y) := \{p \in \mathbb{R}[x]_t \mid M_t(y)\mathrm{vec}(p) = 0\}. \tag{1}$$

Let $I = \langle h_1, \ldots, h_m\rangle \subseteq \mathbb{R}[x]$ be an ideal and set

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

For $t \ge d$, we define the set

$$\mathcal{K}_t := \{y \in \mathbb{R}^{\mathbb{N}^n_{2t}} \mid y_0 = 1, M_t(y) \succeq 0, M_{t-d_j}(h_j y) = 0, j = 1, \ldots, m\}. \tag{3}$$

An element $y \in \mathcal{K}_t$ is *generic* if $M_t(y)$ has maximum rank over $\mathcal{K}_t$. We denote

$$\mathcal{K}^{gen}_t := \{y \in \mathcal{K}_t \mid \text{ rank } M_t(y) \text{ is maximum over } \mathcal{K}_t\}. \tag{4}$$

When the real algebraic variety $V_\mathbb{R}(I)$ is finite, Lasserre et al. Lasserre et al. (2008) used the flat extension (a rank condition of moment matrices in Curto and Fialkow (1996)) as a certificate to check whether polynomials in $\ker M_s(y)$ $(1 \le s \le t)$ for a generic element $y \in \mathcal{K}_t$ generate the real radical ideal $I(V_\mathbb{R}(I))$. When $V_\mathbb{R}(I)$ is positive-dimensional, this certificate does not work. The following example given by Fialkow in (Fialkow, 2011, Example 3.2) can be used to explain the difficulty.

Example 1. *Consider $M_3(y)$ defined by*

$$M_3(y) = \begin{pmatrix}
1 & 0 & 0 & 1 & 2 & 5 & 0 & 0 & 0 & x \\
0 & 1 & 2 & 0 & 0 & 0 & 2 & 5 & 14 & 42 \\
0 & 2 & 5 & 0 & 0 & x & 5 & 14 & 42 & 132 \\
1 & 0 & 0 & 2 & 5 & 14 & 0 & 0 & x & 0 \\
2 & 0 & 0 & 5 & 14 & 42 & 0 & x & 0 & 0 \\
5 & 0 & x & 14 & 42 & 132 & x & 0 & 0 & 0 \\
0 & 2 & 5 & 0 & 0 & x & 5 & 14 & 42 & 132 \\
0 & 5 & 14 & 0 & x & 0 & 14 & 42 & 132 & r \\
0 & 14 & 42 & x & 0 & 0 & 42 & 132 & r & s \\
x & 42 & 132 & 0 & 0 & 0 & 132 & r & s & t
\end{pmatrix}.$$

With an ordering on the variables $x_1 \prec x_2$, we use the graded reverse lexicographic order (Definition 2) in assigning orders of monomials $x_1^{\alpha_1} x_2^{\alpha_2}, 0 \leq \alpha_1 + \alpha_2 \leq 3$ and sorting rows and columns of the moment matrix $M_3(y)$. When $x = 0, r = 429, s = 1422, t = 4798$, we have $M_3(y) \succeq 0$, $rank M_3(y) = 9$ and $\ker M_3(y) = \{x_2 - x_1^3\}$. Unlike the zero-dimensional case, although the kernel of the moment matrix $M_3(y)$ consists of only one polynomial $x_2 - x_1^3$ which is already a Gröbner basis of the real radical ideal $I = I(V_{\mathbb{R}}(I)) = \langle x_2 - x_1^3 \rangle$, it has been shown by Fialkow Fialkow (2011) that the truncated moment sequence $y \in \mathcal{K}_3$ can not be extended to the next order, i.e. y has no representing measure.

The motivation of this paper is to provide a certificate for checking $\langle \ker M_t(y) \rangle = I(V_{\mathbb{R}}(I))$ when $V_{\mathbb{R}}(I)$ is positive-dimensional. Unfortunately, we still can not solve this open problem (Laurent and Rostalski, 2010, §2.4.3). However, we provide a certificate (7) based on the geometric involutivity theory Scott (2006); Scott et al. (2009); Seiler (2010) for checking whether we have obtained a weak Pommaret basis (also a Gröbner basis) of an ideal $J = \langle \ker M_{t-2}(y) \rangle$ satisfying $I \subseteq J \subseteq I(V_{\mathbb{R}}(I))$ under graded reverse lexicographic order. A (weak) Pommaret basis is a special instance of the Gröbner basis which allows for directly reading off the depth, the projective dimension and the Castelnuovo-Mumford regularity of a module. When the real algebraic variety $V_{\mathbb{R}}(I)$ is positive-dimensional, we will succeed in all the examples presented in Section 4 in showing that the computed basis is a Pommaret basis of the real radical ideal $I(V_{\mathbb{R}}(I))$. In general, it is still not possible to prove that the kernel of the moment matrix satisfying the certificate (7) generates a real radical ideal.

The paper is organized as follows. In Section 2, we review some preliminary backgrounds about elementary algebraic geometry, moment matrices, involutive divisions and involutive bases. In Section 3, we propose a certificate for terminating the algorithm and prove that it works for positive-dimensional real algebraic varieties under a δ-regular coordinate system. In Section 4, we present computational results for a set of examples taken from Rostalski (2009); Scott et al. (2009); Seiler (2002); Stetter (2004). Some open questions and ongoing work are given in Section 5.

2. Preliminaries

We introduce some notation and preliminaries about polynomials, matrices, semidefinite programs and involutive bases. Given $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$, the ring of multivariate polynomials in n variables over the field $\mathbb{K}$ is denoted by $\mathbb{K}[x] := \mathbb{K}[x_1, \ldots, x_n]$. For an integer $t \geq 0$, $\mathbb{K}[x]_t$ denotes the set of polynomials of degree at most t. $\mathbb{N}$ denotes the set of nonnegative integers and we set $\mathbb{N}^n_t := \{\alpha \in \mathbb{N}^n \mid |\alpha| := \Sigma_{i=1}^n \alpha_i \leq t\}$ for $t \in \mathbb{N}$. For $\alpha \in \mathbb{N}^n$, x^α denotes the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ whose total degree is $|\alpha| := \Sigma_{i=1}^n \alpha_i$. All monomials are included in $\mathbb{T}^n := \{x^\alpha \mid \alpha \in \mathbb{N}^n\}$ and $\mathbb{T}^n_t := \{x^\alpha \mid \alpha \in \mathbb{N}^n_t\}$ consists of monomials with degrees bounded by $t \in \mathbb{N}$. Consider a polynomial $p \in \mathbb{K}[x]$, $p = \Sigma_{\alpha \in \mathbb{N}^n} p_\alpha x^\alpha$, where there are only finitely many nonzero $p_\alpha \in \mathbb{K}$, its leading term $\mathrm{lt}_\prec(p)$ is the maximum term x^α with respect to a monomial order $\prec$ for which $p_\alpha \neq 0$. We denote by $\langle \mathrm{lt}_\prec(I) \rangle$ the ideal generated by leading terms of polynomials in I. The symbol $[x]_t$ denotes the sequence consisting of all monomials of degree at most t:

$$[x]_t := [1, x_1, \cdots, x_n, x_1^2, x_1 x_2, \cdots, x_1^t, x_1^{t-1} x_2, \cdots, x_n^t].$$

2.1. Properties of Moment Matrices

The kernel of a moment matrix is particularly useful as it has the following properties, see Curto and Fialkow (1996); Lasserre et al. (2008); Laurent (2005, 2009); Möller (2004).

Lemma 1. *(Lasserre et al., 2008, Proposition 3.6) Let* $\ker M(y) := \{p \in \mathbb{R}[x] \mid M(y)\mathrm{vec}(p) = 0\}$ *be the kernel of a moment matrix* $M(y)$*. Then* $\ker M(y)$ *is an ideal in* $\mathbb{R}[x]$*. Moreover, if* $M(y) \succeq 0$*, then* $\ker M(y)$ *is a real radical ideal.*

The kernel of the truncated moment matrix $M_t(y)$ is not an ideal, but under certain conditions, it has the following properties.

Proposition 1. *(Lasserre et al., 2008, Lemma 3.5, 3.9) Let* $y \in \mathbb{R}^{\mathbb{N}^n_{2t}}$ *and assume that its truncated moment matrix* $M_t(y)$ *is positive semidefinite.*

(i) If $f, g \in \mathbb{R}[x]$ *with* $\deg(fg) \leq t - 1$*, then* $f \in \ker M_t(y) \implies fg \in \ker M_t(y)$*.*

(ii) For a polynomial $p \in \mathbb{R}[x]$*, if* $p^{2k} + \sigma \in \ker M_t(y)$ *for some* $k \in \mathbb{N}$ *and* $\sigma \in \sum \mathbb{R}[x]^2$*, then* $p \in \ker M_t(y)$*.*

(iii) We have $\ker M_t(y) \cap \mathbb{R}[x]_s = \ker M_s(y) \quad$ *for* $1 \leq s \leq t$.

Generic elements of $\mathcal{K}_t$ have useful properties. The following results are cited from (Lasserre et al., 2008, Lemma 3.1) and (Rostalski, 2009, Lemma 7.28, 7.39).

Proposition 2. *Assume* $y \in \mathcal{K}_t^{gen}$ *is generic.*

(i) For all $1 \leq s \leq t$, *we have* $\ker M_s(y) \subseteq \sqrt[\mathbb{R}]{I}$ *and* $\ker M_s(y) \subseteq \ker M_s(z)$ *for all* $z \in \mathcal{K}_t$.

(ii) If $t \leq t'$ *and* $y' \in \mathcal{K}_{t'}^{gen}$, *then* $\ker M_t(y) \subseteq \ker M_{t'}(y')$.

(iii) For every finite basis $\{g_1, \ldots, g_k\}$ *of the real radical ideal* $\sqrt[\mathbb{R}]{I}$, *there exists* $t_0 \in \mathbb{N}$ *such that* $g_1, \ldots, g_k \in \ker M_t(z)$ *for all* $z \in \mathcal{K}_t$ *and* $t \geq t_0$.

(iv) It holds that $\langle \ker M_t(y) \rangle = \sqrt[\mathbb{R}]{I}$ *if* t *is sufficiently large.*

2.2. Involutive Divisions and Involutive Bases

When the real algebraic variety $V_{\mathbb{R}}(I)$ is zero-dimensional, Lasserre et al. Lasserre et al. (2013, 2008) proposed new approaches based on moment relaxations for computing Gröbner bases or border bases of the real radical ideal $\sqrt[\mathbb{R}]{I}$. For the positive-dimensional real variety $V_{\mathbb{R}}(I)$, we can also compute its Gröbner bases. Stimulated by the work in Lasserre et al. (2009a) and Reid and Zhi (2009); Scott (2006); Scott et al. (2009), we propose a new approach based on the completion to involution to compute a Pommaret basis of an ideal nested between I and $\sqrt[\mathbb{R}]{I}$. A Pommaret basis is automatically a Gröbner basis for the given term order. It contains extra information such as the Castelnuovo-Mumford regularity. Moreover, we provide a new stopping criterion for the algorithm which is based on the classical Cartan's test for involution from the theory of exterior differential systems. We now introduce some basic concepts from the classical theory of involutive systems for polynomial systems. For background, see Seiler (2002, 2010).

Definition 1. *Let* $\nu = [\nu_1, \ldots, \nu_n] \in \mathbb{N}^n$ *be the multi index of a monomial* x^ν. *If* k *is the smallest value such that* $\nu_k \neq 0$, *then the class of* ν *or* x^ν *is* k, *written by* $\mathrm{cls}(\nu) = k$ *or* $\mathrm{cls}(x^\nu) = k$. *The class of a polynomial* f *which is denoted by* $\mathrm{cls}(f)$ *is* k, *if the class of its leading term* $\mathrm{cls}(\mathrm{lt}_\prec(f)) = k$.

We say that a term order *respects classes*, if for monomials x^μ and x^ν of the same total degree, $\mathrm{cls}(\mu) < \mathrm{cls}(\nu)$ implies $x^\mu \prec x^\nu$. An important example of a class respecting ordering is the *graded reverse lexicographic* order $\prec_{\mathrm{tdeg}}$.

Definition 2. *With an ordering on the variables $x_1 \prec \cdots \prec x_n$, the graded reverse lexicographic order $\prec_{\mathrm{tdeg}}$ is defined by $x^\alpha \prec_{\mathrm{tdeg}} x^\beta$, if $|\alpha| < |\beta|$, or $|\alpha| = |\beta|$ and the first non-vanishing entry of the multi index $\alpha - \beta$ is positive.*

Throughout the paper, we use $\prec_{\mathrm{tdeg}}$ in assigning orders of monomials, and sorting rows and columns of a moment matrix $M_t(y)$. The set $\mathbb{N}^n$ equipped with the addition is an Abelian monoid. For any multi index $\nu \in \mathbb{N}^n$, we introduce its cone $\mathcal{C}(\nu) = \nu + \mathbb{N}^n$, i.e. the set of all multi indices that can be reached from ν by adding another multi index. We say that ν *divides* μ, written $\nu|\mu$ if $\mu \in \mathcal{C}(\nu)$.

Definition 3. *(Seiler, 2010, Definition 3.1.1) An involutive division L is defined on the monoid $(\mathbb{N}^n, +)$. For any finite subset $\mathcal{B} \subseteq \mathbb{N}^n$ and any $\nu \in \mathbb{N}^n$, we are given a set $N_{L,\mathcal{B}}(\nu) \subseteq \{1, \ldots, n\}$ and the corresponding set $L(\nu, \mathcal{B}) = \{\mu \in \mathbb{N}^n \mid \forall j \notin N_{L,\mathcal{B}}(\nu) : \mu_j = 0\}$, which is a submonoid of $\mathbb{N}^n$. Moreover the following two conditions on the involutive cones $\mathcal{C}_{L,\mathcal{B}}(\nu) = \nu + L(\nu, \mathcal{B}) \subseteq \mathbb{N}^n$ must hold:*

(i) If $\mathcal{C}_{L,\mathcal{B}}(\mu) \cap \mathcal{C}_{L,\mathcal{B}}(\nu) \neq \emptyset$ for some $\mu, \nu \in \mathcal{B}$, then $\mathcal{C}_{L,\mathcal{B}}(\mu) \subseteq \mathcal{C}_{L,\mathcal{B}}(\nu)$ or $\mathcal{C}_{L,\mathcal{B}}(\nu) \subseteq \mathcal{C}_{L,\mathcal{B}}(\mu)$.

(ii) If $\mathcal{B}' \subset \mathcal{B}$, then $N_{L,\mathcal{B}}(\nu) \subseteq N_{L,\mathcal{B}'}(\nu)$ for all $\nu \in \mathcal{B}'$.

An arbitrary multi index $\mu \in \mathbb{N}^n$ is involutively divisible by $\nu \in \mathcal{B}$, written $\nu \mid_{L,\mathcal{B}} \mu$, if $\mu \in \mathcal{C}_{L,\mathcal{B}}(\nu)$. In this case ν is called an involutive divisor of μ.

Definition 4. *(Seiler, 2010, Example 3.1.7) The Pommaret division L is defined by assigning the multiplicative indices $N_{L,\mathcal{B}}(\nu)$ according to a simple rule: if $\mathrm{cls}(\nu) = k$, then we set $N_{L,\mathcal{B}}(\nu) = \{1, \ldots, k\}$.*

Remark 1. *The Pommaret division is a globally defined division as the assignment of the multiplicative indices to a multi index $\nu \in \mathcal{B}$ is independent of the set $\mathcal{B}$. The Pommaret division is an involutive division by (Seiler, 2010, Lemma 3.1.8).*

Definition 5. *(Seiler, 2010, Definition 3.1.9) The involutive span of a finite set $\mathcal{B} \subset \mathbb{N}^n$ is*

$$\langle \mathcal{B} \rangle_L = \bigcup_{\nu \in \mathcal{B}} \mathcal{C}_{L,\mathcal{B}}(\nu). \tag{5}$$

The set $\mathcal{B}$ is called weakly involutive for the division L or a weak involutive basis of the monoid ideal $\langle \mathcal{B} \rangle$, if $\langle \mathcal{B} \rangle_L = \langle \mathcal{B} \rangle$. The set $\mathcal{B}$ is a strong involutive basis or for short an involutive basis, if the union (5) is disjoint, i.e., the intersections of the involutive cones are empty.

For a polynomial $f \in \mathbb{K}[x]$ and a term order $\prec$, we select its leading term $\mathrm{lt}_\prec(f) = x^\mu$ with the leading exponent $\mathrm{le}_\prec(f) = \mu$.

Definition 6. *(Seiler, 2010, Definition 3.4.1) Let $I \subseteq \mathbb{K}[x]$ be an ideal. A finite set $\mathcal{H} \subset I$ is a weak involutive basis of I for an involutive division L on $\mathbb{N}^n$, if $\mathrm{le}_\prec(\mathcal{H})$ is a weak involutive basis of the monoid ideal $\mathrm{le}_\prec(I)$. The set $\mathcal{H}$ is an involutive basis of I, if $\mathrm{le}_\prec(\mathcal{H})$ is an involutive basis of $\mathrm{le}_\prec(I)$ and two distinct elements of $\mathcal{H}$ never possess the same leading exponents.*

Not every ideal in $\mathbb{K}[x]$ possesses a finite Pommaret basis (see Seiler (2010)).

Definition 7. *(Seiler, 2010, Definition 4.3.1) A coordinate system is called δ-regular for the ideal $I \subseteq \mathbb{K}[x]$ and the term order $\prec$, if I possesses a finite Pommaret basis for the term order $\prec$.*

Theorem 1. *(Seiler, 2010, Theorem 4.3.15) Every polynomial ideal $I \subseteq \mathbb{K}[x]$ possesses a finite Pommaret basis for a term order $\prec$ in some suitably chosen coordinate systems.*

Definition 8. *(Seiler, 2010, Definition 3.4.2) Let $\mathcal{F} \subset \mathbb{K}[x] \backslash \{0\}$ be a finite set of polynomials and L be an involutive division on $\mathbb{N}^n$. We assign to each element $f \in \mathcal{F}$ a set of multiplicative variables*

$$X_{L,\mathcal{F},\prec}(f) = \{x_i \mid i \in N_{L,\mathrm{le}_\prec \mathcal{F}}(\mathrm{le}_\prec f)\}.$$

The involutive span of $\mathcal{F}$ is then the set

$$\langle \mathcal{F} \rangle_{L,\prec} = \sum_{f \in \mathcal{F}} \mathbb{K}[X_{L,\mathcal{F},\prec}(f)] \cdot f \subseteq \langle \mathcal{F} \rangle.$$

Theorem 2. *(Seiler, 2010, Theorem 3.4.4) Let $I \subseteq \mathbb{K}[x]$ be a nonzero ideal, $\mathcal{H} \subset I \backslash \{0\}$ a finite set and L an involutive division on $\mathbb{N}^n$. Then the following two statements are equivalent.*

(i) The set $\mathcal{H} \subset I$ is a weak involutive basis of I with respect to L and $\prec$.

(ii) Every polynomial $f \in I$ can be written in the form

$$f = \sum_{h \in \mathcal{H}} P_h \cdot h \tag{6}$$

with coefficients $P_h \in \mathbb{K}[X_{L,\mathcal{H},\prec}(h)]$ satisfying $\mathrm{lt}_\prec(P_h \cdot h) \preceq \mathrm{lt}_\prec(f)$ for all polynomials $h \in \mathcal{H}$ such that $P_h \neq 0$.

$\mathcal{H}$ is an involutive basis, if and only if the representation (6) is unique.

Remark 2. *Definition 5, Definition 6 and the representation (6) in Theorem 2 imply immediately that any weak involutive basis is a Gröbner basis.*

Corollary 1. *(Seiler, 2010, Corollary 3.4.5) Let $\mathcal{H}$ be a weak involutive basis of the ideal $I \subseteq \mathbb{K}[x]$. Then $\langle \mathcal{H} \rangle_{L,\prec} = I$. If $\mathcal{H}$ is even an involutive basis of I, then I considered as a $\mathbb{K}$-linear space possesses a direct sum decomposition $I = \bigoplus_{h \in \mathcal{H}} \mathbb{K}[X_{L,\mathcal{H},\prec}(h)] \cdot h$.*

Proposition 3. *(Seiler, 2010, Proposition 3.4.7) Let $I \subseteq \mathbb{K}[x]$ be an ideal and $\mathcal{H} \subset I$ be a weak involutive basis of I for the involutive division L. Then there exists a subset $\mathcal{H}' \subseteq \mathcal{H}$ which is an involutive basis of I.*

Definition 9. *If we regard $\mathbb{K}[x]$ as a linear space, then the ideal I and the truncated ideal $I_t = I \cap \mathbb{K}[x]_t$ are both subspaces in $\mathbb{K}[x]$. We say that the set $G = \{g_1, \ldots, g_s\}$ is a reduced basis of I_t, if it is a linear independent basis of I_t and all polynomials in G have different leading monomials with respect to a given term order.*

3. Computing a Pommaret Basis

In this section, we present an algorithm as well as a certificate for computing a Pommaret basis for an ideal J, s.t. $I \subseteq J \subseteq I(V_{\mathbb{R}}(I))$ when $V_{\mathbb{R}}(I)$ is positive-dimensional.

3.1. The Certificate

Let $I = \langle h_1, \ldots, h_m \rangle \subseteq \mathbb{R}[x]$ be an ideal and $d := \max_{1 \le j \le m} d_j$, $d_j := \lceil \deg(h_j)/2 \rceil$. For each $t \ge d$, recall the notions

$$\mathcal{K}_t := \{y \in \mathbb{R}^{\mathbb{N}^n_{2t}} \mid y_0 = 1, M_t(y) \succeq 0, M_{t-d_j}(h_j y) = 0, j = 1, \ldots, m\},$$

and

$$\mathcal{K}_t^{gen} := \{y \in \mathcal{K}_t \mid \operatorname{rank} M_t(y) \text{ is maximum over } \mathcal{K}_t\}.$$

For a moment matrix $M_t(y)$ of order t, the truncated moment matrix $M_{t-\ell}(y)$ for $\ell < t$ is the order $t - \ell$ principal submatrix of $M_t(y)$ indexed by $\alpha, \beta \in \mathbb{N}^n_{t-\ell}$.

Let α_j denote the number of class j polynomials of degree $t-2$ exactly in a reduced basis of $\ker M_{t-2}(y)$. Although the reduced bases of $\ker M_{t-2}(y)$ are not unique, they have the same set of leading terms since they can be represented linearly by each other. Therefore, the quantity $\sum_{j=1}^n j\alpha_j$ does not depend on the choice of the reduced basis of $\ker M_{t-2}(y)$. Moreover, according to Proposition 1, $\ker M_t(y) \cap \mathbb{R}[x]_s = \ker M_s(y)$ for $1 \le s \le t$, at Step 2 of Algorithm 1, a reduced basis of $\ker M_{t-2}(y)$ is obtained by selecting all polynomials of degree at most $t-2$ in a reduced basis of $\ker M_{t-1}(y)$.

Theorem 3. *Let $I = \langle h_1, \ldots, h_m \rangle \subseteq \mathbb{R}[x]$ be an ideal. Consider an integer $t \ge 2d$ and let y be a generic element of $\mathcal{K}_t^{gen}$. Assume that the following relation*

$$\sum_{j=1}^{n} j\alpha_j = \operatorname{corank} M_{t-1}(y) - \operatorname{corank} M_{t-2}(y) \tag{7}$$

holds. Then a reduced basis of the null space of $M_{t-2}(y)$ is a weak Pommaret basis for $J = \langle \ker M_{t-2}(y) \rangle$ under the monomial ordering $\prec_{\text{tdeg}}$ and

$$I \subseteq J \subseteq I(V_{\mathbb{R}}(I)),\ V_{\mathbb{R}}(I) = V_{\mathbb{C}}(J) \cap \mathbb{R}^n. \tag{8}$$

The proof of Theorem 3 follows from Proposition 2 and Theorem 4 whose proofs are given in Section 3.3.

In our algorithm, we need to find an element y in $\mathcal{K}_t$ maximizing the rank of $M_t(y)$. As pointed out in Lasserre et al. (2008), this could be done typically by solving the semidefinite program

$$\min \quad 0 \quad \text{s.}t. \quad y \in \mathcal{K}_t \tag{9}$$

with interior-point algorithms using self-dual embedding, see Vandenberghe and Boyd (1996); Wolkowicz et al. (2000).

3.2. An Algorithm for Computing a Pommaret Basis

We list the main steps of our algorithm based on solving (9) for computing a Pommaret basis of the ideal $J = \langle \ker M_{t-2}(y) \rangle$ nested between I and $I(V_{\mathbb{R}}(I))$.

Algorithm 1. *Computing a Pommaret basis of an ideal J such that $I \subseteq J \subseteq I(V_{\mathbb{R}}(I))$.*

Input: *A set of polynomials $\{h_1, \ldots, h_m\}$ generating I and the monomial ordering $\prec_{\text{tdeg}}$ on variables $x_1, \ldots, x_n$.*

Output: *A Pommaret basis for $\langle \ker M_{t-2}(y) \rangle$ under the monomial ordering $\prec_{\text{tdeg}}$.*

Step 1 *For $t \geq 2d$, compute a generic element $y \in \mathcal{K}_t$ by solving (9).*

Step 2 *Compute a reduced basis of* $\ker M_{t-1}(y)$.

- *A reduced basis $\{g_1, \ldots, g_{s+r}\}$ of* $\ker M_{t-2}(y)$ *is obtained by choosing all polynomials of degree at most $t-2$ in the reduced basis of* $\ker M_{t-1}(y)$, *where* $\deg(g_i) = t-2$ *for* $1 \leq i \leq s$ *and* $\deg(g_i) < t-2$ *for $s+1 \leq i \leq s+r$.*
- *Compute the value of $\sum_{j=1}^{n} j\alpha_j$, where α_j counts the number of class j polynomials in $\{g_1, \ldots, g_s\}$.*

Step 3 *Compute* $\operatorname{corank} M_{t-1}(y) - \operatorname{corank} M_{t-2}(y)$ *by calculating the number of polynomials of degree $t-1$ in the reduced basis of* $\ker M_{t-1}(y)$.

Step 4 *Test whether the condition (7) is satisfied.*

- *If yes, then $\{g_1, \ldots, g_{s+r}\}$ is a weak Pommaret basis for $\langle \ker M_{t-2}(y) \rangle$ and can be reduced further to a Pommaret basis.*
- *Otherwise, let $t := t+1$ and go to Step 1.*

In Section 3.3, we prove that Algorithm 1 is correct and terminates in a finite number of steps in a δ-regular coordinate system for $\sqrt[\mathbb{R}]{I}$. The algorithm has been implemented in Matlab using the GloptiPoly toolbox Henrion and Lasserre (2003) and we demonstrate its performance on a set of examples given in Section 4.

3.3. Justification of The Certificate

Our main goal in this section is to prove that Algorithm 1 is correct and it terminates after a finite number of steps in a δ-regular coordinate system for $\sqrt[\mathbb{R}]{I}$.

Assumption 1. *Let $I = \langle h_1, \ldots, h_m \rangle \subseteq \mathbb{R}[x]$ be an ideal. Suppose there exists an integer $t \geq 2d$ satisfying the condition (7) for $y \in \mathcal{K}_t^{gen}$. Let $\{g_1, \ldots, g_{s+r}\}$ be a reduced basis of $\ker M_{t-2}(y)$, where*

$$\deg(g_i) = t-2 \text{ for } 1 \leq i \leq s, \text{ and } \deg(g_i) < t-2 \text{ for } s+1 \leq i \leq s+r.$$

Lemma 2. *Under Assumption 1, the polynomial set*

$$\{x_1 g_1, \ldots, x_{j_1} g_1, \ldots, x_1 g_s, \ldots, x_{j_s} g_s, g_1, \ldots, g_{s+r}\}$$

is a reduced basis of $\ker M_{t-1}(y)$, where $j_i = \mathrm{cls}(g_i)$ for $i = 1, \ldots, s$.

Proof. For $k = 1, \ldots, n$, $i = 1, \ldots, s+r$, since $\deg(x_k g_i) \leq t-1$, by Proposition 1 (i), we have $x_k g_i \in \ker M_{t-1}(y)$. In fact, since each polynomial in $\{g_1, \ldots, g_{s+r}\}$ has different leading terms, according to Definition 9, the polynomials

$$x_1 g_1, \ldots, x_{j_1} g_1, \ldots, x_1 g_s, \ldots, x_{j_s} g_s \tag{10}$$

all have distinct leading terms of degree $t-1$. Hence they are linearly independent. Suppose there are α_j polynomials of class j in $\{g_1, \ldots, g_s\}$, then polynomials in (10) yield $\sum_{j=1}^{n} j\alpha_j$ linearly independent polynomials of degree $t-1$ in $\ker M_{t-1}(y)$. On the other hand, the number of linearly independent polynomials of degree $t-1$ in a reduced basis of $\ker M_{t-1}(y)$ equals to $\operatorname{corank} M_{t-1}(y) - \operatorname{corank} M_{t-2}(y)$. Hence, the condition (7) and Proposition 1 (iii) imply that the conclusion is true. □

Remark 3. *Under Assumption 1, for any polynomial $f \in \ker M_{t-1}(y)$, we can express it as a linear combination:*

$$f = \sum_{k=1}^{s} \sum_{i=1}^{\mathrm{cls}(g_k)} c_{ik} x_i g_k + \sum_{k=1}^{s+r} \lambda_k g_k, \tag{11}$$

where $c_{ik} \in \mathbb{R}$ and $\mathrm{lt}_{\prec}(c_{ik} x_i g_k) \preceq_{\mathrm{tdeg}} \mathrm{lt}_{\prec}(f)$ for $1 \leq i \leq \mathrm{cls}(g_k)$ and $1 \leq k \leq s$, $\lambda_k \in \mathbb{R}$ and $\mathrm{lt}_{\prec}(\lambda_k g_k) \preceq_{\mathrm{tdeg}} \mathrm{lt}_{\prec}(f)$ for $1 \leq k \leq s+r$. Note that every polynomial in $\{x_1 g_1, \ldots, x_{j_1} g_1, \ldots, x_1 g_s, \ldots, x_{j_s} g_s, g_1, \ldots, g_{s+r}\}$ has a

different leading term. Under the graded monomial ordering $\prec_{\text{tdeg}}$, there is only one $c_{i_0k_0} \neq 0$ with $\text{lt}_\prec(x_{i_0}g_{k_0}) = \text{lt}_\prec(f)$ if not all c_{ik} are zeros. If all c_{ik} are zero, then there exists only one index $1 \leq k \leq s+r$ such that $\lambda_k \neq 0$ and $\text{lt}_\prec(g_k) = \text{lt}_\prec(f)$. This property is very important and will be used in the proofs of theorems below.

Lemma 3. *Under Assumption 1, for all monomials x^μ and polynomials g_j with $\deg(g_j) < t-2$, $j = s+1, \ldots, s+r$, the polynomial $x^\mu g_j$ can be expressed as*

$$x^\mu g_j = \sum_{k=1}^{s} h_k g_k + \sum_{k=s+1}^{s+r} \lambda_k g_k, \tag{12}$$

where $h_k \in \mathbb{R}[x]$ and $\lambda_k \in \mathbb{R}$ satisfying $\text{lt}_\prec(h_k g_k) \preceq_{\text{tdeg}} \text{lt}_\prec(x^\mu g_j)$, $k = 1, \ldots, s$ and $\text{lt}_\prec(\lambda_k g_k) \preceq_{\text{tdeg}} \text{lt}_\prec(x^\mu g_j)$, $k = s+1, \ldots, s+r$.

Proof. If $\deg(x^\mu g_j) \leq t-1$, by Proposition 1 (i), we have $x^\mu g_j \in \ker M_{t-1}(y)$. According to Remark 3, we have the expression (12). Otherwise, we set $x^\mu = x^{\mu_1}x^{\mu_2}$ such that $\deg(x^{\mu_2}g_j) = t-1$. Hence, we have

$$\begin{aligned} x^\mu g_j = x^{\mu_1}x^{\mu_2}g_j &= x^{\mu_1}(\sum_{k=1}^{s} h_k g_k + \sum_{k=s+1}^{s+r} \lambda_k g_k) \\ &= \sum_{k=1}^{s} x^{\mu_1} h_k g_k + \sum_{k=s+1}^{s+r} \lambda_k x^{\mu_1} g_k. \end{aligned}$$

We can repeat the above reduction on $x^{\mu_1}g_k$ for $s+1 \leq k \leq s+r$. Since $\deg(x^{\mu_1}) < \deg(x^\mu)$, after a finite number of steps, we have the expected form (12). □

Theorem 4. *Under Assumption 1, a reduced basis $\{g_1, \ldots, g_{s+r}\}$ of $\ker M_{t-2}(y)$ is a weak Pommaret basis of the ideal $\langle \ker M_{t-2}(y) \rangle$.*

Proof. We show that any polynomial $f \in \langle \ker M_{t-2}(y) \rangle$ can be represented as

$$f = \sum_{k=1}^{s} h_k g_k + \sum_{k=s+1}^{s+r} \lambda_k g_k, \tag{13}$$

where $\lambda_k \in \mathbb{R}$ and $h_k \in \mathbb{R}[x_1, \ldots, x_{\text{cls}(g_k)}]$. Since $\text{lt}_\prec(h_k g_k)$ and $\text{lt}_\prec(g_k)$ are all different for $1 \leq k \leq s+r$, if f satisfies (13), then we have $\text{lt}_\prec(h_k g_k) \preceq_{\text{tdeg}} \text{lt}_\prec(f)$ for $1 \leq k \leq s$ and $\text{lt}_\prec(\lambda_k g_k) \preceq_{\text{tdeg}} \text{lt}_\prec(f)$ for $s+1 \leq k \leq s+r$.

Therefore, according to Theorem 2, the polynomial set $\{g_1, \ldots, g_{s+r}\}$ is a weak Pommaret basis of the ideal $\langle \ker M_{t-2}(y) \rangle$.

Since $\{g_1, \ldots, g_{s+r}\}$ is a reduced basis of $\ker M_{t-2}(y)$, every polynomial $f \in \langle \ker M_{t-2}(y) \rangle$ can be represented as

$$f = \sum_{j=1}^{s+r} h_j g_j,$$

where $h_j \in \mathbb{R}[x],\ j = 1, \ldots, s+r$. Hence, we only need to show that each polynomial $x^\mu g_j$ for $\mu \in \mathbb{N}^n$ and $1 \leq j \leq s+r$ can be written as (13).

Set $f = x^\mu g_j$. If $\deg(f) \leq t-1$, by Lemma 2, we have the expected expression (13) directly. Otherwise, we prove by the induction on its leading term $\mathrm{lt}_\prec(f) = t_0$, i.e., we assume that $f = x^\mu g_j$ has the expected expression (13) as long as $\mathrm{lt}_\prec(f) \prec_{\mathrm{tdeg}} t_0$ for $\mu \in \mathbb{N}^n$ and $1 \leq j \leq s+r$, we show it has the expected expression when $\mathrm{lt}_\prec(f) = t_0$.

If $x^\mu \in \mathbb{R}[x_1, \ldots, x_{\mathrm{cls}(g_j)}]$, nothing needs to be proved. Otherwise, without loss of generality, let x_{i_1} be a non-multiplicative variable in x^μ with respect to g_j, i.e. $i_1 \notin \{1, \ldots, \mathrm{cls}(g_j)\}$. Since $\deg(g_j) \leq t-2,\ j = 1, \ldots, s+r$, by Proposition 1 (i), we have $x_{i_1} g_j \in \ker M_{t-1}(y)$. By Lemma 2 and Remark 3, we have

$$\begin{aligned} f = x^\mu g_j &= \big(x^\mu / x_{i_1}\big)\ x_{i_1} g_j \\ &= \big(x^\mu / x_{i_1}\big)\big(\sum_{k=1}^{s} \sum_{i=1}^{\mathrm{cls}(g_k)} c_{ik} x_i g_k + \sum_{k=1}^{s+r} \lambda_k g_k\big) \\ &= \sum_{k=1}^{s} \sum_{i=1}^{\mathrm{cls}(g_k)} c_{ik} \big(x^\mu / x_{i_1}\big) x_i g_k + \sum_{k=1}^{s+r} \lambda_k \big(x^\mu / x_{i_1}\big) g_k. \end{aligned} \tag{14}$$

According to Remark 3, there are two cases:

(i) if all $c_{ik} = 0$, there exists only one $1 \leq j_1 \leq s+r$, such that $\lambda_{j_1} \neq 0$ and $\mathrm{lt}_\prec(\lambda_{j_1} \big(x^\mu / x_{i_1}\big) g_{j_1}) = t_0$;

(ii) otherwise, there exist $1 \leq j_1 \leq s$ and $1 \leq i_2 \leq \mathrm{cls}(g_{j_1})$ such that $c_{i_2 j_1} \neq 0$ and $\mathrm{lt}_\prec(c_{i_2 j_1} \big(x^\mu / x_{i_1}\big) x_{i_2} g_{j_1}) = t_0$.

In both cases, all other terms in (14) have leading terms of order less than t_0, which can be expressed as (13) by induction. Moreover, above two cases

do not exist simultaneously. Therefore, we only need to check whether the polynomial $\lambda_{j_1}\big(x^\mu/x_{i_1}\big)g_{j_1}$ in case (i) or $c_{i_2j_1}\big(x^\mu/x_{i_1}\big)x_{i_2}g_{j_1}$ in case (ii) has the representation (13).

In case (i), if $x^\mu/x_{i_1} \in \mathbb{R}[x_1,\ldots,x_{\mathrm{cls}(g_{j_1})}]$ then we obtain the representation (13). Otherwise, we repeat the reduction to the polynomial $\big(x^\mu/x_{i_1}\big)g_{j_1}$. Since $\mathrm{lt}_\prec(\lambda_{j_1}\big(x^\mu/x_{i_1}\big)g_{j_1}) = \mathrm{lt}_\prec(x^\mu g_j) = t_0$, we have $\deg(g_j) < \deg(g_{j_1})$, i.e.,

$$\mathrm{lt}_\prec(g_j) \prec_{\mathrm{tdeg}} \mathrm{lt}_\prec(g_{j_1}).$$

In case (ii), if $x^\mu/x_{i_1} \in \mathbb{R}[x_1,\ldots,x_{\mathrm{cls}(g_{j_1})}]$, since x_{i_2} is a multiplicative variable of $\mathrm{lt}_\prec(g_{j_1})$, then $\big(x^\mu/x_{i_1}\big)x_{i_2} \in \mathbb{R}[x_1,\ldots,x_{\mathrm{cls}(g_{j_1})}]$. Hence, we obtain the representation (13). Otherwise, since x_{i_1} is a non-multiplicative variable of $\mathrm{lt}_\prec(g_j)$ and x_{i_2} is a multiplicative variable of $\mathrm{lt}_\prec(g_{j_1})$, we have

$$\mathrm{cls}(g_j) < \mathrm{cls}(x_{i_1}), \quad \mathrm{cls}(x_{i_2}) \leq \mathrm{cls}(g_{j_1}).$$

Because $\mathrm{lt}_\prec(c_{i_2j_1}\big(x^\mu/x_{i_1}\big)x_{i_2}g_{j_1}) = t_0$, we have $\mathrm{lt}_\prec(x_{i_2}g_{j_1}) = \mathrm{lt}_\prec(x_{i_1}g_j)$ and

$$\mathrm{cls}(x_{i_2}) = \mathrm{cls}(x_{i_2}g_{j_1}) = \mathrm{cls}(x_{i_1}g_j) < \mathrm{cls}(x_{i_1}). \tag{15}$$

This implies that $x_{i_2} \prec_{\mathrm{tdeg}} x_{i_1}$. If $\mathrm{lt}_\prec(g_{j_1}) \preceq_{\mathrm{tdeg}} \mathrm{lt}_\prec(g_j)$, we have $\mathrm{lt}_\prec(x_{i_2}g_{j_1}) \prec_{\mathrm{tdeg}} \mathrm{lt}_\prec(x_{i_1}g_j)$ which leads to a contradiction. Therefore, we can deduce that

$$\mathrm{lt}_\prec(g_j) \prec_{\mathrm{tdeg}} \mathrm{lt}_\prec(g_{j_1}).$$

In both cases, if the reduction does not stop, we will obtain a sequence of polynomials satisfying

$$\mathrm{lt}_\prec(g_j) \prec_{\mathrm{tdeg}} \mathrm{lt}_\prec(g_{j_1}) \prec_{\mathrm{tdeg}} \cdots \prec_{\mathrm{tdeg}} \mathrm{lt}_\prec(g_{j_i}) \prec_{\mathrm{tdeg}} \mathrm{lt}_\prec(g_{j_{i+1}}) \prec_{\mathrm{tdeg}} \cdots \prec_{\mathrm{tdeg}} t_0.$$

Since the number of polynomials with strictly increasing leading terms bounded by $\mathrm{lt}_\prec(f) = t_0$ is finite, the above procedure will stop in a finite number of steps and we obtain the expected form (13) for f. □

Theorem 5. *In a δ-regular coordinate system for $\sqrt[\mathbb{R}]{I}$, after a finite number of steps, Algorithm 1 will terminate and return an integer $t \geq 2d$ which satisfies the condition (7) for an element $y \in \mathcal{K}_t^{gen}$.*

Proof. In a δ-regular coordinate system, we have a finite Pommaret basis $\mathcal{H} = \{h_1,\ldots,h_s\}$ for the real radical ideal $I(V_\mathbb{R}(I))$. According to Proposition

2 (iii), we can conclude that there exists an integer t_1 such that the Pommaret basis $\{h_1, \ldots, h_s\}$ is contained in $\ker M_t(y)$ for all $y \in \mathcal{K}_t$ and $t \geq t_1$.

Since $\mathcal{H}$ is a Pommaret basis of $I(V_{\mathbb{R}}(I))$, according to Corollary 1, for $t \geq t_1 + 2$, we have the following decomposition:

$$I(V_{\mathbb{R}}(I))_{t-2} = \bigoplus_{h_k \in \mathcal{H}} \mathbb{R}[x_1, \ldots, x_{\mathrm{cls}(h_k)}]_{t-2-\deg(h_k)} \cdot h_k. \tag{16}$$

Let

$$T = \{x^u h_k \mid x^u \in \mathbb{R}[x_1, \ldots, x_{\mathrm{cls}(h_k)}],\ \deg(x^u) \leq t - 2 - \deg(h_k), 1 \leq k \leq s\}. \tag{17}$$

According to Proposition 1 (i), $T \subseteq \ker M_{t-2}(y)$. Therefore, by (16) and (17), we have

$$I(V_{\mathbb{R}}(I))_{t-2} \subseteq \ker M_{t-2}(y).$$

On the other hand, y is a generic element, by Proposition 2 (i), we have

$$\ker M_{t-2}(y) \subseteq I(V_{\mathbb{R}}(I))_{t-2}.$$

Hence, we have $\ker M_{t-2}(y) = I(V_{\mathbb{R}}(I))_{t-2}$ and the decomposition:

$$\ker M_{t-2}(y) = \bigoplus_{h_k \in \mathcal{H}} \mathbb{R}[x_1, \ldots, x_{\mathrm{cls}(h_k)}]_{t-2-\deg(h_k)} \cdot h_k. \tag{18}$$

Since $\mathcal{H}$ is a Pommaret basis of $I(V_{\mathbb{R}}(I))$, according to Definition 6, each polynomial in T has a different leading term. Therefore T is actually a reduced basis of $\ker M_{t-2}(y)$. By Theorem 3, it suffices to show that the condition (7) holds for the polynomials in T.

Similar to the decomposition (18), we can show that there exists a direct sum decomposition of $\ker M_{t-1}(y)$:

$$\ker M_{t-1}(y) = \bigoplus_{h_k \in \mathcal{H}} \mathbb{R}[x_1, \ldots, x_{\mathrm{cls}(h_k)}]_{t-1-\deg(h_k)} \cdot h_k. \tag{19}$$

For a polynomial $f \in \ker M_{t-1}(y)$ with $\deg(f) = t - 1$, according to (19), we

have the following equalities:

$$\begin{aligned} f &= \sum_{k=1}^{s} \sum_{0\le|\mu|\le t-1-\deg(h_k)} c_{\mu k} x^{\mu} h_k \ \ (\text{note that } x^{\mu} \in \mathbb{R}[x_1, \ldots, x_{\mathrm{cls}(h_k)}]) \\ &= \sum_{k=1}^{s} \sum_{|\mu|=t-1-\deg(h_k)} c_{\mu k} x^{\mu} h_k + \sum_{k=1}^{s} \sum_{0\le|\mu|\le t-2-\deg(h_k)} c_{\mu k} x^{\mu} h_k \\ &= \sum_{k=1}^{s} \sum_{|\mu|=t-1-\deg(h_k)} c_{\mu k} x_{\mathrm{cls}(x^{\mu})} \big(x^{\mu}/x_{\mathrm{cls}(x^{\mu})}\big) h_k + \sum_{k=1}^{s} \sum_{0\le|\mu|\le t-2-\deg(h_k)} c_{\mu k} x^{\mu} h_k. \end{aligned}$$

Since $x_{\mathrm{cls}(x^{\mu})}$ is always a multiplicative variable for the polynomial $\big(x^{\mu}/x_{\mathrm{cls}(x^{\mu})}\big)h_k \in T$, we know that each polynomial in $\ker M_{t-1}(y)$ can be represented by the polynomials in T and T_1, where

$$T_1 = \{x_i g \mid 1 \le i \le \mathrm{cls}(g),\ g \in T, \deg(g) = t-2\}.$$

The polynomials in T_1 and T have different leading terms, hence $T \cup T_1$ is a linearly independent basis of $\ker M_{t-1}(y)$. Moreover, T is a reduced basis of $\ker M_{t-2}(y)$, and T_1 consists of all linearly independent polynomials with degree $t-1$ in $\ker M_{t-1}(y)$. We can deduce that the number of polynomials in T_1 is equal to $\operatorname{corank} M_{t-1}(y) - \operatorname{corank} M_{t-2}(y)$. On the other hand, let α_j denote the number of polynomials of class j and degree $t-2$ in T. Since the set T_1 is constructed by multiplying polynomials in T of degree $t-2$ by their multiplicative variables only, the total number of polynomials in T_1 is equal to $\sum_{j=1}^{n} j\alpha_j$. Therefore, the condition (7) is satisfied. □

3.4. An Extension to $I(V_{\mathbb{R}}(I) \cap \mathcal{A})$

Consider the semialgebraic set

$$\mathcal{A} := \{x \in \mathbb{R}^n \mid f_1(x) \ge 0, \ldots, f_s(x) \ge 0\}, \tag{20}$$

where $f_1, \ldots, f_s \in \mathbb{R}[x]$. The $\mathcal{A}$-variety $V_{\mathcal{A}}(I)$ denotes the intersection

$$V_{\mathcal{A}}(I) = V_{\mathbb{R}}(I) \cap \mathcal{A}.$$

For every $\nu \in \{0,1\}^s$, we denote the product $f^{\nu} := f_1^{\nu_1} f_2^{\nu_2} \cdots f_s^{\nu_s}$.

Definition 10. *Marshall (2008) The $\mathcal{A}$-radical of an ideal I is defined as*

$$\sqrt[\mathcal{A}]{I} := \left\{ p \in \mathbb{R}[x] \,\middle|\, p^{2k} + \sum_{\nu \in \{0,1\}^s} \sigma_\nu f^\nu \in I \quad \text{for some } k \in \mathbb{N},\, \sigma_\nu \in \sum \mathbb{R}[x]^2 \right\}.$$

The ideal I is called $\mathcal{A}$-radical if $I = \sqrt[\mathcal{A}]{I}$.

Theorem 6. *(Stengle, 1994, Semialgebraic Nullstellensatz) Let I be an ideal in $\mathbb{R}[x]$ and $\mathcal{A}$ be defined by (20). Then $\sqrt[\mathcal{A}]{I}$ is an $\mathcal{A}$-radical ideal and $\sqrt[\mathcal{A}]{I} = I(V_{\mathbb{R}}(I) \cap \mathcal{A})$.*

To compute the $\mathcal{A}$-radical ideal $\sqrt[\mathcal{A}]{I}$, we consider the set

$$\mathcal{K}_{t,\mathcal{A}} := \mathcal{K}_t \cap \left\{ y \in \mathbb{R}^{\mathbb{N}^n_{2t}} : M_{t-d_{f^\nu}}(f^\nu y) \succeq 0,\ \forall \nu \in \{0,1\}^s \right\}, \tag{21}$$

where $d_{f^\nu} = \lceil \deg(f^\nu)/2 \rceil$. Clearly, the set $\mathcal{K}_{t,\mathcal{A}}$ is a restriction of $\mathcal{K}_t$. The definition of the set $\mathcal{K}_{t,\mathcal{A}}$ is motivated by the polynomials in $\sqrt[\mathcal{A}]{I}$ and the Semialgebraic Nullstellensatz. The generic elements of $\mathcal{K}_{t,\mathcal{A}}$ are similarly defined to be the elements of the set

$$\mathcal{K}^{gen}_{t,\mathcal{A}} := \{ y \in \mathcal{K}_{t,\mathcal{A}} : \operatorname{rank} M_t(y) \text{ is maximum over } \mathcal{K}_{t,\mathcal{A}} \}.$$

Lemma 4. *(Lasserre et al., 2008, Remark 4.9). Let $\{g_1, \ldots, g_k\}$ be a set of generators for the ideal $\sqrt[\mathcal{A}]{I}$. Then there exists $t_0 \in \mathbb{N}$ such that $g_1, \ldots, g_k \in \ker M_t(y)$ for all $y \in \mathcal{K}_{t,\mathcal{A}}$ and $t \geq t_0$.*

According to Lemma 4, it is easy to show that there exists $t_0 \in \mathbb{N}$ such that $\langle \ker M_t(y) \rangle = \sqrt[\mathcal{A}]{I}$ for all $y \in \mathcal{K}^{gen}_{t,\mathcal{A}}$ and $t \geq t_0$. Hence, for t large enough, the information about $\sqrt[\mathcal{A}]{I}$ will be contained in the projection of a generic element $y \in \mathcal{K}_{t,\mathcal{A}}$. Thus, propositions and theorems discussed above are true for generic elements y in $\mathcal{K}_{t,\mathcal{A}}$.

The following theorem can be seen as a variant of Theorem 3 for the semi-algebraic set $\mathcal{A}$. The proof uses exactly the same reasoning as in Theorem 4 and Theorem 5 after replacing $\mathcal{K}_t$ and $\sqrt[\mathbb{R}]{I}$ by $\mathcal{K}_{t,\mathcal{A}}$ and $\sqrt[\mathcal{A}]{I}$ respectively.

Theorem 7. *Suppose the condition (7) holds for a generic element $y \in \mathcal{K}_{t,\mathcal{A}}$, and $t \geq 2d$. Then a reduced basis of the null space of $M_{t-2}(y)$ is a weak Pommaret basis of $\langle \ker M_{t-2}(y) \rangle$ under the monomial ordering $\prec_{\text{tdeg}}$ and*

$$I \subseteq \langle \ker M_{t-2}(y) \rangle \subseteq I(V_{\mathbb{R}}(I) \cap \mathcal{A}).$$

Remark 4. *For computing a Pommaret basis of* $\langle \ker M_{t-2}(y)\rangle$*, we add the defining polynomials* $\{f_1,\ldots,f_s\}$ *of the semialgebraic set* $\mathcal{A}$ *to the input of the above algorithm and additional constraints* $M_{t-d_{f^\nu}}(f^\nu y)\succeq 0$ *for all* $\nu\in\{0,1\}^s$ *to the semidefinite program (9).*

4. Numerical Examples

We present here the results obtained by applying Algorithm 1 to some examples taken from Rostalski (2009); Scott et al. (2009); Seiler (2002); Stetter (2004) and others. For a given tolerance τ, we define the numerical rank of a matrix to be k, if its singular values satisfy $\sigma_1\geq\cdots\geq\sigma_k>\tau>\sigma_{k+1}$ or $\sigma_k/\sigma_{k+1}>10^3$. Spang implemented in SINGULAR Decker et al. (2012) a symbolic algorithm realrad for computing the real radical of an arbitrary ideal over transcendental extension of the rational numbers Silke (2007b). Since the algorithm realrad is based on Wu-Ritt's characteristic set method and Gröbner basis computation, it has double-exponential complexity. Our algorithm is based on semidefinite programming and numerical linear algebra, it has polynomial complexity. However, the results we computed may contain numerical errors. Using realrad, we can verify that Examples 2, 3, 5 are real radical ideals, i.e. $I=\sqrt[\mathbb{R}]{I}$ and Examples 4, 6 are not real radical ideals, i.e. $I\subset\sqrt[\mathbb{R}]{I}$.

Example 2. *Consider the 2-dimensional ideal* $I=\langle h_1,h_2,h_3\rangle$ *taken from (Stetter, 2004, p.397, Eq. (9.60)) where*

$$\begin{aligned}h_1&=x_1^2+x_1x_2-x_1x_3-x_1-x_2+x_3,\\ h_2&=x_1x_2+x_2^2-x_2x_3-x_1-x_2+x_3,\\ h_3&=x_1x_3+x_2x_3-x_3^2-x_1-x_2+x_3.\end{aligned}$$

The rank and corank sequences for truncated moment matrices $M_{t-\ell}(y)$ *are shown in Table 1 and 2. We set* $\tau=10^{-5}$ *and* $x_1\prec_{\text{tdeg}}x_2\prec_{\text{tdeg}}x_3$*. For t=4, we have*

$$\sum_{j=1}^{3}j\alpha_j=6,\ \textit{and}\ \operatorname{corank}M_{4-1}-\operatorname{corank}M_{4-2}=6.$$

Hence, the condition (7) is satisfied. The Pommaret basis computed by Algorithm 1 for $t=4$ *is*

$$\begin{aligned}\{x_1+x_2-x_3-x_1^2-x_1x_2+x_1x_3,x_1+x_2-x_3-x_1x_2-x_2^2+x_2x_3,\\ 3x_1+3x_2-3x_3-x_1^2-2x_1x_2-x_2^2+x_3^2\}.\end{aligned}$$

From Table 3, we note that the condition (7) is also satisfied for $t = 5, 6, 7$. *For this example, using the function* realrad, *we can show that* $I = \langle \ker M_{4-2}(y) \rangle = \sqrt[\mathbb{R}]{I}$, *and a reduced basis of* $\ker M_{4-2}(y)$ *is a Pommaret basis of* $\sqrt[\mathbb{R}]{I}$. *Hence, the condition (7) can be satisfied by arbitrary* $t \geq 4$.

Table 1: The rank of $M_{t-\ell}(y)$

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=4	16	11	7
t=5	22	16	11
t=6	29	22	16
t=7	37	29	22

Table 2: The corank of $M_{t-\ell}(y)$

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=4	19	9	3
t=5	34	19	9
t=6	55	34	19
t=7	83	55	34

Table 3: The α_j of a reduced basis of $\ker M_{t-2}(y)$

Order	α_1	α_2	α_3	$\sum_{j=1}^{3} j\alpha_j$
t=4	1	1	1	1×1+2×1+3×1=6
t=5	3	2	1	1×3+2×2+3×1=10
t=6	6	3	1	1×6+2×3+3×1=15
t=7	10	4	1	1×10+2×4+3×1=21

Example 3. *Consider the polynomial system* $P = \{h_1, h_2\}$ *in (Scott et al., 2009, p.20, Ex 1.4.6), where*

$$h_1 = x_1^2 - x_2,$$
$$h_2 = x_1 x_2 - x_3.$$

For the term order $x_3 \prec_{\text{tdeg}} x_1 \prec_{\text{tdeg}} x_2$, *we have* $\text{cls}(x_1) = 2$, $\text{cls}(x_2) = 3$, $\text{cls}(x_3) = 1$. *Let* $\tau = 10^{-8}$, *the rank and corank sequences for truncated moment matrices* $M_{t-\ell}(y)$ *are shown in Table 4 and 5.*

For t=4, we have

$$\sum_{j=1}^{3} j\alpha_j = 7, \text{ and } \operatorname{corank} M_{4-1} - \operatorname{corank} M_{4-2} = 7.$$

Table 4: The rank of $M_{t-\ell}(y)$

Order	$\ell=0$	$\ell=1$	$\ell=2$
t=3	12	7	4
t=4	16	10	7
t=5	20	13	10

Table 5: The corank of $M_{t-\ell}(y)$

Order	$\ell=0$	$\ell=1$	$\ell=2$
t=3	8	3	0
t=4	19	10	3
t=5	36	22	10

Table 6: The α_j of a reduced basis of $\ker M_{t-2}(y)$

Order	α_1	α_2	α_3	$\sum_{j=1}^{3} j\alpha_j$
t=3	0	0	0	1×0+2×0+3×0=0
t=4	0	2	1	1×0+2×2+3×1=7
t=5	3	3	1	1×3+2×3+3×1=12

Hence, the condition (7) is satisfied. The Pommaret basis computed by Algorithm 1 for $t=4$ is

$$\{x_1^2 - x_2, x_1x_2 - x_3, x_2^2 - x_1x_3\},$$

which is also the basis of $\sqrt[\mathbb{R}]{I}$ computed by the function realrad*. Moreover, since $x_2^2 - x_1x_3 = x_1(x_1x_2 - x_3) - x_2(x_1^2 - x_2)$, we have $I = \langle \ker M_{4-2}(y)\rangle = \sqrt[\mathbb{R}]{I}$.*

Example 4. *Consider the ideal $I = \langle h_1, h_2\rangle$ in (Rostalski, 2009, p.123, Ex 7.41) with*

$$\begin{aligned} h_1 &= x_1^2 + x_2^2 + x_3^2 - 2, \\ h_2 &= x_1^2 + x_2^2 - x_3. \end{aligned}$$

Applying the function realrad*, we obtain generators*

$$\{x_3 - 1, x_1^2 + x_2^2 - 1\} \tag{22}$$

of the real radical ideal $\sqrt[\mathbb{R}]{I}$. Since $x_3 - 1$ is not in the ideal I, we can deduce that I is strictly contained in $\sqrt[\mathbb{R}]{I}$, i.e. $I \subset \sqrt[\mathbb{R}]{I}$. Let $\tau = 10^{-8}$ and $x_1 \prec_{\text{tdeg}} x_2 \prec_{\text{tdeg}} x_3$, the rank and corank sequences for truncated moment matrices $M_{t-\ell}(y)$ are shown in Table 7 and 8.

Table 7: The rank of $M_{t-\ell}(y)$

Order	$\ell=0$	$\ell=1$	$\ell=2$
t=3	7	5	3
t=4	9	7	5
t=5	11	9	7
t=6	13	11	9

Table 8: The corank of $M_{t-\ell}(y)$

Order	$\ell=0$	$\ell=1$	$\ell=2$
t=3	13	5	1
t=4	26	13	5
t=5	45	26	13
t=6	71	45	26

Table 9: The α_j of a reduced basis of $\ker M_{t-2}(y)$

Order	α_1	α_2	α_3	$\sum_{j=1}^{3} j\alpha_j$
t=3	0	0	1	1×0+2×0+3×1=3
t=4	1	2	1	1×1+2×2+3×1=8
t=5	4	3	1	1×4+2×3+3×1=13
t=6	8	4	1	1×8+2×4+3×1=19

For t=4, we have

$$\sum_{j=1}^{3} j\alpha_j = 8, \text{ and } \operatorname{corank} M_{4-1} - \operatorname{corank} M_{4-2} = 8.$$

Hence, the condition (7) is satisfied. The Pommaret basis computed by Algorithm 1 for $t = 4$ is

$$\{-1 + x_3, -1 + x_1^2 + x_2^2\}, \tag{23}$$

which is the same as the basis (22) of $\sqrt[\mathbb{R}]{I}$ computed by realrad*. Therefore, we have $\langle \ker M_{4-2}(y) \rangle = \sqrt[\mathbb{R}]{I}$, and the reduced basis (23) of $\ker M_{4-2}(y)$ is a Pommaret basis of $\sqrt[\mathbb{R}]{I}$. Hence, the condition (7) can be satisfied by arbitrary $t \geq 4$.*

Example 5. *Consider the ideal $I = \langle h_1, h_2, h_3 \rangle$ in (Seiler, 2002, p.61, Ex 2.4.12), where*

$$\begin{aligned} h_1 &= x_3^2 + x_2x_3 - x_1^2, \\ h_2 &= x_1x_3 + x_1x_2 - x_3, \\ h_3 &= x_2x_3 + x_2^2 + x_1^2 - x_1. \end{aligned}$$

Let $\tau = 10^{-7}$ and the term order be $x_1 \prec_{\text{tdeg}} x_2 \prec_{\text{tdeg}} x_3$. The rank and corank sequences for the truncated moment matrices $M_{t-\ell}(y)$ are shown in Table 10 and 11.

Table 10: The rank of $M_{t-\ell}(y)$

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=4	13	10	7
t=5	16	13	10
t=6	19	16	13
t=7	22	19	16

Table 11: The corank of $M_{t-\ell}(y)$

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=4	22	10	3
t=5	40	22	10
t=6	65	40	22
t=7	98	65	40

Table 12: The α_j of a reduced basis of $\ker M_{t-2}(y)$

Order	α_1	α_2	α_3	$\sum_{j=1}^{3} j\alpha_j$
t=4	1	1	1	1×1+2×1+3×1=6
t=5	4	2	1	1×4+2×2+3×1=11
t=6	8	3	1	1×8+2×3+3×1=17
t=7	13	4	1	1×13+2×4+3×1=24

The condition (7) can not be satisfied for t from 4 to 7. Actually, Seiler showed in Seiler (2002) that the coordinates (x_1, x_2, x_3) are not δ-regular for the ideal I. However, if we perform the linear transformation suggested in Seiler (2002), $\tilde{x}_1 = x_3$, $\tilde{x}_2 = x_2 + x_3$, $\tilde{x}_3 = x_1$, after an auto-reduction, we obtain the polynomial system $\tilde{P} = \{\tilde{x}_1\tilde{x}_2 - \tilde{x}_3^2, \tilde{x}_2\tilde{x}_3 - \tilde{x}_1, \tilde{x}_2^2 - \tilde{x}_3\}$.

Let $\tilde{I}$ be the ideal generated by $\tilde{P}$. The generators of $\sqrt[\mathbb{R}]{\tilde{I}}$ computed by the function realrad *are*

$$\{\tilde{x}_1\tilde{x}_2 - \tilde{x}_3^2, \tilde{x}_2\tilde{x}_3 - \tilde{x}_1, \tilde{x}_2^2 - \tilde{x}_3, \tilde{x}_3^3 - \tilde{x}_1^2\}. \tag{24}$$

Since $\tilde{x}_3^3 - \tilde{x}_1^2 = -\tilde{x}_3(\tilde{x}_1\tilde{x}_2 - \tilde{x}_3^2) + \tilde{x}_1(\tilde{x}_2\tilde{x}_3 - \tilde{x}_1)$, we can deduce that $\tilde{I} = \sqrt[\mathbb{R}]{\tilde{I}}$.

Choosing an ordering $\tilde{x}_1 \prec_{\text{tdeg}} \tilde{x}_2 \prec_{\text{tdeg}} \tilde{x}_3$ and $\tau = 10^{-8}$, the rank and corank sequences for the truncated moment matrices $M_{t-\ell}(y)$ are shown in Table 13 and 14.

Table 13: The rank of $M_{t-\ell}(y)$

Order	$\ell=0$	$\ell=1$	$\ell=2$
t=4	13	10	7
t=5	16	13	10
t=6	19	16	13

Table 14: The corank of $M_{t-\ell}(y)$

Order	$\ell=0$	$\ell=1$	$\ell=2$
t=4	22	10	3
t=5	40	22	10
t=6	65	40	22

Table 15: The α_j of a reduced basis of $\ker M_{t-2}(y)$

Order	α_1	α_2	α_3	$\sum_{j=1}^{3} j\alpha_j$
t=4	0	2	1	1×0+2×2+3×1=7
t=5	3	3	1	1×3+2×3+3×1=12
t=6	7	4	1	1×7+2×4+3×1=18

For t=4, we have

$$\sum_{j=1}^{3} j\alpha_j = 7, \text{ and } \operatorname{corank} M_{4-1} - \operatorname{corank} M_{4-2} = 7.$$

Hence, the condition (7) is satisfied. The Pommaret basis computed by Algorithm 1 for $t = 4$ is

$$\{\tilde{x}_1\tilde{x}_2 - \tilde{x}_3^2, \tilde{x}_2\tilde{x}_3 - \tilde{x}_1, \tilde{x}_2^2 - \tilde{x}_3\}. \tag{25}$$

By (24), we know that (25) is also a Pommaret basis of $\sqrt[\mathbb{R}]{\tilde{I}}$.

Example 6. *Consider the ideal $I = \langle h_1, h_2\rangle$, where*

$$\begin{aligned} h_1 &= (x_1 - x_2)(x_1 + x_2)^2(x_1 + x_2^2 + x_2), \\ h_2 &= (x_1 - x_2)(x_1 + x_2)^2(x_1^2 + x_2^2). \end{aligned}$$

Applying the function realrad*, we obtain a generator set*

$$\{x_1^2 - x_2^2\} \tag{26}$$

of $\sqrt[\mathbb{R}]{I}$. Since $x_1^2 - x_2^2$ is not in the ideal I, we can deduce that I is strictly contained in $\sqrt[\mathbb{R}]{I}$, i.e. $I \subset \sqrt[\mathbb{R}]{I}$.

Table 16: The rank of $M_{t-\ell}(y)$

Order	$\ell=0$	$\ell=1$	$\ell=2$
t=7	15	13	11
t=8	17	15	13
t=9	19	17	15

Table 17: The corank of $M_{t-\ell}(y)$

Order	$\ell=0$	$\ell=1$	$\ell=2$
t=7	21	15	10
t=8	28	21	15
t=9	36	28	21

Table 18: The α_j of a reduced basis of $\ker M_{t-2}(y)$

Order	α_1	α_2	$\sum_{j=1}^{2} j\alpha_j$
t=7	3	1	1×3+2×1=5
t=8	4	1	1×4+2×1=6
t=9	5	1	1×5+2×1=7

Let $\tau = 10^{-4}$ and $x_1 \prec_{\text{tdeg}} x_2$, the rank and corank sequences for the truncated moment matrices $M_{t-\ell}(y)$ are shown in Table 16 and 17.

For t=7, we have

$$\sum_{j=1}^{2} j\alpha_j = 5, \text{ and } \operatorname{corank} M_{7-1} - \operatorname{corank} M_{7-2} = 5.$$

Hence, the condition (7) is satisfied. The Pommaret basis computed by Algorithm 1 for $t = 7$ is

$$\{-x_1^2 + x_2^2\}. \tag{27}$$

By (26) and (27), we have shown that $\langle \ker M_{7-2}(y) \rangle = \sqrt[\mathbb{R}]{I}$, and the reduced basis (27) is a Pommaret basis of $\sqrt[\mathbb{R}]{I}$.

It should be noticed that for this example, if we set tolerance $\tau < 10^{-4}$, the rank and corank sequences for the truncated moment matrices $M_{t-\ell}(y)$ will be completely different from those shown in Table 16 and 17, and we can not get $\{-x_1^2 + x_2^2\}$ as a Pommaret basis of $\sqrt[\mathbb{R}]{I}$.

Example 7. *We compute $I(V_{\mathbb{R}}(I) \cap \mathcal{A})$ for $I = \langle h_1, h_2 \rangle$,*

$$\begin{aligned} h_1 &= (x_1 - x_2)(x_1 + x_2)(x_1 + x_2^2 + x_2), \\ h_2 &= (x_1 - x_2)(x_1 + x_2)(x_1^2 + x_2^2), \end{aligned}$$

and

$$\mathcal{A} = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 \geq 1,\ x_2 \geq 1\}.$$

Let us set $\tau = 10^{-8}$ *and* $x_1 \prec_{\text{tdeg}} x_2$*, the rank and corank sequences for the truncated moment matrices* $M_{t-\ell}(y)$ *with* $y \in \mathcal{K}_{t,\mathcal{A}}$ *are shown in Table 19 and 20.*

Table 19: The rank of $M_{t-\ell}(y)$

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=6	8	6	5
t=7	9	7	6
t=8	10	8	7

Table 20: The corank of $M_{t-\ell}(y)$

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=6	20	15	10
t=7	27	21	15
t=8	35	28	21

Table 21: The α_j of a reduced basis of $\ker M_{t-2}(y)$

Order	α_1	α_2	$\sum_{j=1}^{2} j\alpha_j$
t=6	3	1	1×3+2×1=5
t=7	4	1	1×4+2×1=6
t=8	5	1	1×5+2×1=7

For t=6, we have

$$\sum_{j=1}^{2} j\alpha_j = 5, \text{ and } \operatorname{corank} M_{6-1} - \operatorname{corank} M_{6-2} = 5.$$

Hence, the condition (7) is satisfied. The Pommaret basis we obtain by Algorithm 1 for $t = 6$ *is*

$$\{-x_1 + x_2\}$$

for $I(V_{\mathbb{R}}(I) \cap \mathcal{A})$*.*

5. Concluding Remarks

In this paper we present a semidefinite characterization for computing a Pommaret basis of an ideal J, where J is generated by polynomials in the kernel of a truncated moment matrix and satisfies $I \subseteq J \subseteq I(V_{\mathbb{R}}(I))$. Our approach is stimulated by the previous work in Lasserre et al. (2008, 2009a); Laurent and Rostalski (2010); Reid and Zhi (2009); Rostalski (2009);

Scott (2006); Scott et al. (2009); Seiler (2002). By combining the geometric involutive theory with the results on positive semidefinite moment matrices, we introduce a new stopping condition (7) for the semidefinite program (9) and prove the finite termination of the algorithm in a δ-regular coordinate system. Although we still could not provide a certificate to check whether $J = \langle \ker M_{t-2}(y) \rangle = I(V_{\mathbb{R}}(I)$, it is interesting to show some related work below which might lead to a solution to this problem in future.

Remark 5. *In zero-dimensional case, if the flat extension condition is satisfied at $s \leq t$, i.e. $rank\, M_s(y) = rank\, M_{s-1}(y)$ for $y \in \mathcal{K}_t^{gen}$, then $\langle \ker M_s(y) \rangle = I(V_{\mathbb{R}}(I))$ and $\operatorname{corank} M_s(y) - \operatorname{corank} M_{s-1}(y) = \binom{n+s-1}{s}$, which means that monomials of degree s all appear in the reduced basis of $\ker M_s(y)$. Hence we have $\sum_{j=1}^{n} j\alpha_j = \binom{n+s}{s+1}$ for $\ker M_s(y)$.*

If $s < t-1$, by the ideal-like property given in Proposition 1(i), we can show that $rank\, M_s(y) = rank\, M_{s+1}(y)$, i.e. $\operatorname{corank} M_{s+1}(y) - \operatorname{corank} M_s(y) = \binom{n+s}{s+1}$. Therefore, our condition (7) is satisfied for $\ker M_s(y)$ and a reduced basis of $\ker M_s(y)$ is a weak Pommaret basis for $J = \langle \ker M_s(y) \rangle = I(V_{\mathbb{R}}(I))$ under the monomial ordering $\prec_{\text{tdeg}}$.

If $s = t-1$, using Proposition 1(i) and Proposition 2(ii), it is straightforward to show that the flat extension condition is also satisfied at s for $y' \in \mathcal{K}_{t+1}^{gen}$, i.e. $rank\, M_s(y') = rank\, M_{s-1}(y')$. Hence, $rank\, M_s(y') = rank\, M_{s+1}(y')$, and the condition (7) will be satisfied at $M_s(y')$ and $J = \langle \ker M_s(y') \rangle = I(V_{\mathbb{R}}(I))$. If $s = t$, similarly, we can show that the condition (7) will be satisfied at $M_s(y'')$ for $y'' \in \mathcal{K}_{t+2}^{gen}$ and $J = \langle \ker M_s(y'') \rangle = I(V_{\mathbb{R}}(I))$.

Remark 6. *From the tables in Section 4, we can check that the condition (7) can be satisfied by higher order moment matrices once it is satisfied at order t. Moreover, we can also check that the condition*

$$rank\, M_{t'-\ell}(y_1) = rank\, M_{(t'+1)-(\ell+1)}(y_2),\ \text{for } t' \geq t,\ \ell = 1, 2 \tag{28}$$

is satisfied for $y_1 \in \mathcal{K}_{t'}^{gen}$ and $y_2 \in \mathcal{K}_{t'+1}^{gen}$. However, in general we can not guarantee this property. It is clear that if both (7) and (28) hold for all higher order moment matrices, then for all $k \geq 0$ and all generic $y \in \mathcal{K}_{t+k}^{gen}$, we have

$$rank\, M_{t+k-\ell}(y) = HP^{aff}_{\sqrt[\mathbb{R}]{I}}(t+k-\ell), \tag{29}$$

where $HP^{aff}_{\sqrt[\mathbb{R}]{I}}(t+k-\ell)$ is the affine Hilbert polynomial of $\sqrt[\mathbb{R}]{I}$ which counts the dimension of polynomials of $\mathbb{K}[x]_{\leq t+k-\ell}$ not lying in $\sqrt[\mathbb{R}]{I}_{\leq t+k-\ell}$ (Ma, 2012,

Theorem 5.20). Therefore, a reduced basis of $\ker M_{t-\ell}(y)$ *is a weak Pommaret basis for* $J = \langle \ker M_{t-\ell}(y) \rangle = I(V_{\mathbb{R}}(I))$ *under the monomial ordering* $\prec_{\text{tdeg}}$ *(Ma, 2012, Theorem 5.21).*

Remark 7. *Let* $I = \langle h_1, \ldots, h_m \rangle$*, and* $\dim(I) = s > 0$*. For each polynomial* $f \in \sqrt[\mathbb{R}]{I}$*, there exist* $t, r \in \mathbb{N}$ *and polynomials* $q_1, \ldots, q_r, p_1, \ldots, p_m \in \mathbb{R}[x]$ *such that*

$$f^{2\tau} + \sum_{i=1}^{r} q_i^2 = \sum_{i=1}^{m} p_i h_i. \tag{30}$$

Some interesting bounds $D(n, \deg(f), s)$ *for* $\deg(p_i h_i), i = 1, \ldots, m$ *have been given in Henri et al. (2014); Schmid (1998, 2000). Suppose we know the degree upper bound* k_1 *for the generators of* $\sqrt[\mathbb{R}]{I}$*, then we have* $\deg(p_i h_i) \leq k_2 = D(n, k_1, s)$*. By (30) and Proposition 1(ii), we know that all generators of* $\sqrt[\mathbb{R}]{I}$ *will be included in* $\ker M_{k_2}(y)$*. Therefore, if the condition (7) is satisfied at* $t - 2 > k_2$ *then a reduced basis of* $\ker M_{t-2}(y)$ *is a weak Pommaret basis for* $J = \langle \ker M_{t-2}(y) \rangle = I(V_{\mathbb{R}}(I))$ *under the monomial ordering* $\prec_{\text{tdeg}}$*.*

In general, it is difficult to estimate the degree upper bound k_1 *for the generators in* $\sqrt[\mathbb{R}]{I}$*. We know that the Castelnuovo-Mumford regularity of a homogenous ideal is* q *if and only if the ideal has in some suitably chosen coordinates a Pommaret basis of degree* q *for the graded reverse lexicographic order (Seiler, 2010, Theorem 5.5.15). Therefore, the Pommaret basis we computed for* $J = \langle \ker M_{t-2}(y) \rangle$ *can be used to bound the degree of the generators of* $I(V_{\mathbb{R}}(I))$ *in some cases Ravi (1990).*

Finally, we wish to mention that results computed by semidefinite programming and numerical linear algebra are approximate. Therefore, our condition (7) can only be checked with respect to a given tolerance. For improperly chosen tolerance, we might not be able to give a meaningful answer.

Acknowledgement We are most grateful to Jiawang Nie for many constructive remarks to improve the presentation of the paper. Yue Ma, Chu Wang and Lihong Zhi are partially supported by a NKBRPC 2011CB302400, and the Chinese National Natural Science Foundation under grant NSFC 91118001, 60911130369 and 60821002/F02. This work is supported by National Institute for Mathematical Sciences 2014 Thematic Program on Applied Algebraic Geometry in Daejeon, South Korea. We would also like to acknowledge many helpful comments and suggestions from the referees.

Aubry, P., Rouillier, F., Din, M. S. E., 2002. Real solving for positive dimensional systems. J. Symbolic Comput. 34 (6), 543–560.

Bank, B., Giusti, M., Heintz, J., Mbakop, G., 2001. Polar varieties and efficient real elimination. Math. Z. 238 (1), 115–144.

Basu, S., Pollack, R., Roy, M.-F., 1997. On computing a set of points meeting every cell defined by a family of polynomials on a variety. J. Complexity 13 (1), 28–37.

Becker, E., Neuhaus, R., 1993. Computation of real radicals of polynomial ideals. In: Computational algebraic geometry (Nice, 1992). Vol. 109 of Progr. Math. Birkhäuser Boston, Boston, MA, pp. 1–20.

Becker, E., Wörmann, T., 1996. Radical computations of zero-dimensional ideals and real root counting. Math. Comput. Simulation 42 (4-6), 561–569, symbolic computation, new trends and developments (Lille, 1993).

Bochnak, J., Coste, M., Roy, M.-F., 1998. Real algebraic geometry. Vol. 36 of Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer-Verlag, Berlin.

Curto, R., Fialkow, L., 1996. Solution of the truncated complex moment problem for flat data. Memoirs of the American Mathematical Society 119 (568), 1–62.

Decker, W., Greuel, G.-M., Pfister, G., Schönemann, H., 2012. SINGULAR 3-1-6 — A computer algebra system for polynomial computations. `http://www.singular.uni-kl.de`.

Fialkow, L., 2011. Solution of the truncated moment problem with variety $y = x^3$. Trans. Amer. Math. Soc. 363, 3133–3165.

Gianni, P., Trager, B., Zacharias, G., 1988. Gröbner bases and primary decomposition of polynomial ideals. J. Symbolic Comput. 6 (2/3), 149–167.

Henri, L., Daniel, P., Marie-Francoise, R., 2014. An elementary recursive bound for effective positivstellensatz and Hilbert 17-th problem, preprint. URL `http://arxiv.org/abs/1404.2338`

Henrion, D., Lasserre, J., 2003. GloptiPoly: Global optimization over polynomials with Matlab and SeDuMi. ACM Trans. Math. Softw. 29 (2), 165–194.

Janovitz-Freireich, I., Mourrain, B., Rónyai, L., Szántó, A., Jan. 2012. On the computation of matrices of traces and radicals of ideals. J. Symbolic Comput. 47, 102–122.

Krick, T., Logar, A., 1991. 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). Vol. 539 of Lecture Notes in Comput. Sci. Springer, Berlin, pp. 195–205.

Lasserre, J., Laurent, M., Mourrain, B., Rostalski, P., Trébuchet", P., 2013. Moment matrices, border bases and real radical computation. J. Symbolic Comput. 51, 63 – 85.

Lasserre, J., Laurent, M., Rostalski, P., 2008. Semidefinite characterization and computation of zero-dimensional real radical ideals. Foundations of Computational Mathematics 8, 607–647.

Lasserre, J., Laurent, M., Rostalski, P., 2009a. A prolongation-projection algorithm for computing the finite real variety of an ideal. Theoretical Computer Science 410 (27-29), 2685–2700.

Lasserre, J., Laurent, M., Rostalski, P., 2009b. A unified approach to computing real and complex zeros of zero-dimensional ideals. In: Emerging applications of algebraic geometry. Vol. 149 of IMA Vol. Math. Appl. Springer, New York, pp. 125–155.

Laurent, M., 2005. Revisiting two theorems of Curto and Fialkow on moment matrices. Proceedings of the American Mathematical Society 133 (10), 2965–2976.

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

Laurent, M., Rostalski, P., 2010. The approach of moments for polynomial equations. In: Anjos, M. F., Lasserre, J. B. (Eds.), Handbook on Semidefinite, Cone and Polynomial Optimization. Vol. 166 of International Series in Operations Research and Management Science. Springer.

Ma, Y., 2012. Polynomial optimization via low-rank matrix completion and semidefinite programming. `http://www.mmrc.iss.ac.cn/~lzhi/Thesis_yma.pdf`, Ph.D. thesis, Chinese Academy of Sciences.

Marshall, M., 2008. Positive polynomials and sums of squares. Vol. 146 of Mathematical Surveys and Monographs. American Mathematical Society.

Möller, H., 2004. An inverse problem for cubature formulae. Computational Technologies 9 (13-20).

Neuhaus, R., 1998. Computation of real radicals of polynomial ideals. II. J. Pure Appl. Algebra 124 (1-3), 261–280.

Ravi, M., 1990. Regularity of ideals and their radicals. manuscripta mathematica 68 (1), 77–87.

Reid, G., Zhi, L., 2009. Solving polynomial systems via symbolic-numeric reduction to geometric involutive form. J. Symbolic Comput. 44 (3), 280–291.

Rostalski, P., 2009. Algebraic moments-Real Root Finding and Related topics. Ph.D. thesis, ETH Zurich.

Safey El Din, M., Schost, E., 2003. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In: Proceedings of the 16th international symposium on Symbolic and algebraic computation. ISSAC '03. ACM, New York, NY, USA, pp. 224–231.

Schmid, J., 1998. On the degree complexity of hilbert's 17th problem and the real nullstellensatz. Habilitationsschrift, Universität Dortmund.

Schmid, J., 2000. On the complexity of the real nullstellensatz in the 0-dimensional case. Journal of Pure and Applied Algebra 151 (3), 301–308.

Scott, R., 2006. Approximate Gröbner bases. Master thesis, University of Western Ontario, Canada.

Scott, R., Reid, G., Wu, W., Zhi, L., 2009. Geometric involutive bases and applications to approximate commutative algebra. In: Approximate commutative algebra. Texts Monogr. Symbol. Comput. SpringerWienNewYork, Vienna, pp. 99–124.

Seiler, W., 2002. Involution - the formal theory of differential equations and its applications in computer algebra and numerical analysis. Habilitation thesis, Univ. of Mannheim.

Seiler, W., 2010. Involution: The Formal Theory of Differential Equations and its Applications in Computer Algebra. Vol. 25 of Algorithms and Computation in Mathematics. Springer-Verlag.

Silke, S., 2007a. On the computation of the real radical. Ph.D. thesis, Technische Universität Kaiserslautern.

Silke, S., 2007b. `realrad.lib`. A SINGULAR 3-1-6 library for computing the real radicals. `http://www.singular.uni-kl.de`.

Stengle, G., 1994. A nullstellensatz and positivstellensatz in semialgebraic geometry. Math. Ann. 207, 87–97.

Stetter, H., 2004. Numerical polynomial algebra. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA.

Vandenberghe, L., Boyd, S., 1996. Semidefinite programming. SIAM Rev. 38 (1), 49–95.

Wolkowicz, H., Saigal, R., Vandenberghe, L., 2000. Handbook of Semidefinite Programming: Theory, Algorithms, and Applications. International Series in Operations Research & Management Science. Springer US.

Xia, B., Yang, L., 2002. An algorithm for isolating the real solutions of semialgebraic systems. J. Symbolic. Comput. 34 (5), 461–477.

Zeng, G., 1999. Computation of generalized real radicals of polynomial ideals. Sci. China Ser. A 42 (3), 272–280.