Journal of Symbolic Computation 72 (2016) 1–20

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

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

ARTICLE INFO

Article history:
Received 15 July 2014
Accepted 21 November 2014
Available online 18 December 2014

Keywords:
Real radical ideal
Positive-dimensional ideal
Semidefinite programming
Involutive division
Pommaret basis
δ-Regular

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.

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

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

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

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

The radical (also called complex radical) of I is

E-mail addresses: yma@mmrc.iss.ac.cn (Y. Ma), cwang@mmrc.iss.ac.cn (C. Wang), lzhi@mmrc.iss.ac.cn (L. Zhi).

http://dx.doi.org/10.1016/j.jsc.2014.12.002
0747-7171/

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

while the real radical of I is defined as

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

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, 2009b) 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 et al. (1988) and 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 (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. (2013, 2009a, 2009b), 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 $\operatorname{vec}(h) := (h_\alpha)_{\alpha \in \mathbb{N}^n}$ and define the sequence $hy := M(y)\operatorname{vec}(h) \in \mathbb{R}^{\mathbb{N}^n}$. We say that a polynomial p lies in the kernel of $M(y)$ when $M(y)p := M(y)\operatorname{vec}(p) = 0$. 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 $\mathbb{T}^n_t := \{x^\alpha \mid \alpha \in \mathbb{N}^n_t \text{ with } |\alpha| := \sum_{i=1}^n \alpha_i \le t\}$.

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 $M_t(y)\operatorname{vec}(p) = 0$, we say p lies in the kernel of $M_t(y)$, i.e.,

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

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

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

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

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

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

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

When the real algebraic variety $V_{\mathbb{R}}(I)$ is finite, 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 (2011, Example 3.2) can be used to explain the difficulty.