An SDP-based method for the real radical ideal membership test

Greg Reid
Department of Applied Mathematics
University of Western Ontario
London, Canada
reid@uwo.ca

Fei Wang, Henry Wolkowicz
Department of Combinatorcs & Optimization
University of Waterloo
Waterloo, Canada
f49wang@uwaterloo.ca, hwolkowicz@uwaterloo.ca

***Abstract*—Let V be the set of real solutions of a system of multivariate polynomial equations with real coefficients. The real radical ideal (RRI) of V is the infinite set of multivariate polynomials that vanish on V. We give theoretical results that yield a finite step numerical algorithm for testing if a given polynomial is a member of this RRI.**

The paper exploits recent work that connects solution sets of such real polynomial systems with solution sets of semidefinite programming, SDP, problems involving moment matrices. We take advantage of an SDP technique called facial reduction. This technique regularizes our problem by projecting the feasible set onto the so-called *minimal face*. Also, we use the Douglas-Rachford iterative approach which has advantages over traditional interior point methods for our application.

If V has finitely many real solutions, then our method yields known results: a basis and membership test for the RRI. In the case where the set V has real solution components of positive dimension, and given an input polynomial of degree d, our method can also decide RRI membership via a truncated geometric involutive basis of degree d.

Examples are given to illustrate our approach and its advantages that remove multiplicities and sums of squares that cause ill-conditioning for real solutions of polynomial systems.

***Keywords*-real radical, moment matrix, facial reduction, Douglas-Rachford, semidefinite programming, geometric involutive basis.**

I. Introduction

The fundamental objects of real polynomial solving are sets of their real solutions (varieties) and their associated *real radical ideals, RRI*. In comparison to the less realistic but theoretically easier case of complex solution sets and radical ideals over $\mathbb{C}$, much less is known about the real case. In a remarkable series of recent papers it was shown that (generators of) the RRI of a real polynomial system with finitely many solutions can be determined by computing the kernel of so-called moment matrices arising from a *semidefinite programming, SDP*, e.g., [19], [25]. This RRI is generated by a feasibility problem of a system of real polynomials having only real roots that are free of multiplicities. The RRI is thus useful for regularizing numerical solutions of such systems and avoiding the cost of computing non-real roots.

Our work, similar to that of [21], [22] is motivated by the important open problem for the positive dimensional case. In this paper we show that certain aspects of such generating sets, namely their members up to any truncated degree, can be determined in the positive dimensional case. We also show that facial reduction combined with the Douglas-Rachford iterative scheme can be used to significantly improve efficiency and accuracy.

We note that the determination of real solutions of polynomial equations is frequently required in many applications such as mechanical design, chemistry, robotics, etc. For such problems, people usually care only about the real solutions. The real radical ideal is free of sum of squares and multiplicities; and ensures that its generators accurately reflect the geometry of its associated real solution set. Thus when applying Newton's method or critical point methods, the Jacobian matrix is non-singular and numerical difficulties are substantially reduced. Hence a main motivation is to reduce and regularize a given polynomial system without losing the real solutions that are of interest.

A. Preliminaries

Suppose $x = (x_1, ..., x_n) \in \mathbb{R}^n$ and consider a system of m multivariate polynomials with real coefficients: $P = \{p_1(x), p_2(x), ..., p_m(x)\} \subseteq \mathbb{R}[x]$, the ring of polynomials over $\mathbb{R}$. Its solution set or variety is

$$V_{\mathbb{R}}(p_1, ..., p_m) = \{x \in \mathbb{R}^n : p_j(x) = 0,\ 1 \le j \le m\}.$$

The ideal generated by $P = \{p_1, ..., p_m\} \subseteq \mathbb{R}$ is:

$$\langle P \rangle_{\mathbb{R}} = \{f_1 p_1 + ... + f_m p_m : f_j \in \mathbb{R}[x], 1 \le j \le m\},$$

and its associated radical ideal over $\mathbb{R}$ is defined as

$$\sqrt[\mathbb{R}]{\langle P \rangle_{\mathbb{R}}} := \{f \in \mathbb{R}[x] : \exists\, q_j \in \mathbb{R}[x], t \in \mathbb{N}^+ \text{with } f^{2t} + \Sigma_{j=1}^{s} q_j^2 \in \langle P \rangle_{\mathbb{R}}\}$$

Example I.1. *For $P = \{(x^2+y^2)(x-y-1)^2\}$ the solution set is easily computed as $V_{\mathbb{R}}(P) = \{(0,0)\} \cup \{(x, x-1) : x \in \mathbb{R}\}$ and $\sqrt[\mathbb{R}]{\langle P \rangle_{\mathbb{R}}} = \langle x(x-y-1), y(x-y-1)\rangle_{\mathbb{R}}$.*

Another approach recently developed by Hauenstein et al. [8] is based on verifying the *completeness* of a real solution set S. Suppose $I = \langle P \rangle_{\mathbb{R}}$ and $S \subseteq V_{\mathbb{R}}(I)$, then the vanishing ideal of S, denoted by $\mathcal{I}(S)$, satisfies $\sqrt[\mathbb{R}]{I} \subseteq \mathcal{I}(S)$. If we can verify $\mathcal{I}(S) \subseteq \sqrt[\mathbb{R}]{I}$, then $\mathcal{I}(S) = \sqrt[\mathbb{R}]{I}$ and S is complete. In other words, a real radical membership verification is needed. However, in [8] one can not certify $\mathcal{I}(S) \not\subseteq \sqrt[\mathbb{R}]{I}$ and the membership verification is not guaranteed to terminate in finitely many steps. In this paper, we propose an effective approach for the real radical membership verification motivated by the above open problem.

Our approach also builds on the method of moment matrices. A key step is to solve the problem of the following type for X

$$\mathcal{A}(X) = b, \quad X \in \mathcal{S}_+^k, X \text{ is maximum rank}, \tag{I.1}$$

where $\mathcal{S}_+^k$ denotes the convex cone of $k \times k$ real symmetric positive semidefinite matrices, and $\mathcal{A} : \mathcal{S}_+^k \to \mathbb{R}^l$ is a linear transformation which enforces the moment matrix structure for X.

The standard regularity assumption for (I.1) is the *Slater constraint qualification* or strict feasibility assumption:

$$\text{there exists } X \text{ with } \mathcal{A}(X) = b, \quad X \in \operatorname{int} \mathcal{S}_+^k =: \mathcal{S}_{++}^k. \tag{I.2}$$

We let $X \succeq 0, \succ 0$ denote $X \in \mathcal{S}_+^k, \in \operatorname{int} \mathcal{S}_+^k$, respectively. It is well known that the Slater condition for SDP holds generically, e.g., [15]. Surprisingly, many SDP problems arising from particular applications, and in particular our polynomial system applications, are marginally infeasible, i.e., fail to satisfy strict feasibility. This is exactly the case for our moment matrices approach. This creates difficulties with numerical algorithms such as interior point solvers and the maximum rank cannot be computed accurately.

In this paper, we use facial reduction first introduced by Borwein and Wolkowicz [6], [7]. This effectively regularizes the SDP moment problem associated with the input polynomial system so that it satisfies the strict feasibility constraint. We then use the *geometric involutive basis* to check if the kernel of the moment matrix is a truncated ideal (ideal-like). This leads to a method to compute the generators of real radicals up to any given degree d. Therefore we can numerically determine the real radical membership as well as the completeness of the real solution subset S.

II. Real radical and moment matrices

A fundamental result e.g., [2] is:

Theorem II.1 (Real nullstellensatz). *For any ideal $I \subseteq \mathbb{R}[x]$ we have $\sqrt[\mathbb{R}]{I} = \mathcal{I}(V_{\mathbb{R}}(I))$. Equivalently*

$$\sqrt[\mathbb{R}]{\langle P \rangle_{\mathbb{R}}} = \{f(x) \in \mathbb{R}[x] : f(x) = 0 \ \text{ for all } \ x \in V_{\mathbb{R}}(P)\}.$$

Remark II.1. *An ideal $I \subseteq \mathbb{R}[x]$ is real radical if and only if for all $p_1, \cdots, p_m \in \mathbb{R}[x]$:*

$$p_1^2 + \cdots + p_m^2 \in I \Longrightarrow p_1, \cdots, p_m \in I. \tag{II.1}$$

For these and related results see e.g., [2] and the references therein. Next we introduce *moment matrices*, which are central for the computation of RRI.

Definition II.1 (Moment matrix [20]). *Let $\lambda \in \mathbb{R}[x]^*$ be a linear form that maps a polynomial to a real number. The symmetric matrix*

$$M(\lambda) := (\lambda(x^\alpha x^\beta))_{\alpha,\beta \in \mathbb{N}^n} \tag{II.2}$$

is called the moment matrix of λ where $\mathbb{N} = \{0, 1, 2, \cdots\}$.

Similarly, we define the truncated moment matrix.

Definition II.2 (Truncated moment matrix [20]). *Given a linear form $\lambda_d \in (\mathbb{R}[x]_{2d})^*$, the truncated moment matrix of λ_d is:*

$$M(\lambda_d) := (\lambda_d(x^\alpha x^\beta))_{\alpha,\beta \in \mathbb{N}_d^n} \tag{II.3}$$

where $\mathbb{N}_d^n = \{\gamma \in \mathbb{N}^n : |\gamma| = \Sigma_{j=1}^n \gamma_j \leq d\}$.

Example II.1. *Suppose $\lambda_1 \in \mathbb{R}[x, y]_{2d}^*$ for $d = 1$. Then*

$$M(\lambda_1) = \begin{bmatrix} u_{00} & u_{10} & u_{01} \\ u_{10} & u_{20} & u_{11} \\ u_{01} & u_{11} & u_{02} \end{bmatrix}. \tag{II.4}$$

Without loss, we assume $u_{00} = 1$ throughout this paper.

The kernel of a positive semidefinite truncated moment matrix has the following *real radical* type property:

Lemma II.1. *[20] Assume $M(\lambda_d) \succeq 0$ and let $p, q_j \in \mathbb{R}[x]$, $f := p^{2m} + \sum_j q_j^2$ with $m \in \mathbb{N}$, $m \geq 1$. Then, $f \in \ker M(\lambda_d) \Rightarrow p \in \ker M(\lambda_d)$.*

We note that there is a bijective correspondence between vectors $v \in \ker M(\lambda_d)$ and polynomials given by $v \mapsto \mathbb{P}(v) = v^T (x^\alpha)_{\alpha \in \mathbb{N}^n}$ where $(x^\alpha)_{\alpha \in \mathbb{N}^n}$ is the vector of all monomials of degree $\leq d$ ordered in the same way as the rows of the moment matrix. We now introduce the following important theorems about the kernel of a positive semidefinite moment matrix.

Theorem II.2 ([18, Lemma 3.1]). *Suppose that the ideal $I = \langle f_1, \dots f_m \rangle_{\mathbb{R}}$ with $\max_i(\deg(f_i)) = d$ and let B be the coefficient matrix of $\{f_1, \dots f_m\} \subseteq \mathbb{R}[x]$. Let $M(\lambda_d)$ be a truncated moment matrix such that $B^T \cdot M(\lambda_d) = 0$ and $M(\lambda_d) \succeq 0$. If the rank of $M(\lambda_d)$ is maximum then*

$$\mathbb{P}(\ker M(\lambda_d)) \subseteq \sqrt[\mathbb{R}]{I}. \tag{II.5}$$

Theorem II.3 (Flat extension [11]). *Assume $M(\lambda_d) \succeq 0$. Then the following statements are equivalent:*

- *There exists an extension moment matrix $M(\lambda_{d+1}) \succeq 0$ such that* $\operatorname{rank} M(\lambda_d) = \operatorname{rank} M(\lambda_{d+1})$.
- $\ker M(\lambda_d)$ *is ideal-like.*

Finally, in the zero-dimensional case, we have the following important result that relates the real radical ideal and moment matrices.

Lemma II.2 ([18, Theorem 3.4, Corollary 3.8]). *Assume $M(\lambda_d) \succeq 0$ and $\operatorname{rank} M(\lambda_d) = \operatorname{rank} M(\lambda_{d-1}) = r$. Then we have $J = \langle \mathbb{P}(\ker M(\lambda_d)) \rangle_{\mathbb{R}}$ is real radical and zero-dimensional. One can extend λ_d to $\lambda = \sum_{i=1}^r \alpha_i \lambda_{v_i} \in \mathbb{R}[x]^*$ where $\alpha_i > 0$ and $\{v_1, \dots, v_r\} = V_{\mathbb{R}}(\mathbb{P}(\ker M(\lambda_d)))$. Furthermore $\lambda = \lambda_d$ when λ is restricted to $\mathbb{R}[x]_{2d}$.*

Example II.2. *Consider the polynomial $p = x^4 - 2$ of degree 4. In matrix form, the polynomial is represented by its coefficient matrix $B = [-2, 0, 0, 0, 1]^T$.*

The truncated moment matrix is the following:

$$M(\lambda_2) = \begin{pmatrix} u_0 & u_1 & u_2 & u_3 & u_4 \\ u_1 & u_2 & u_3 & u_4 & u_5 \\ u_2 & u_3 & u_4 & u_5 & u_6 \\ u_3 & u_4 & u_5 & u_6 & u_7 \\ u_4 & u_5 & u_6 & u_7 & u_8 \end{pmatrix} \tag{II.6}$$

Then we solve the following semidefinite programming problem:

$$B^T \cdot M = 0, M \succeq 0, \operatorname{rank}(M) \text{ is maximum.} \tag{II.7}$$

The solution moment matrix is:

$$M(\lambda_2) = \begin{pmatrix} 1 & 0 & \sqrt{2} & 0 & 2 \\ 0 & \sqrt{2} & 0 & 2 & 0 \\ \sqrt{2} & 0 & 2 & 0 & 2\sqrt{2} \\ 0 & 2 & 0 & 2\sqrt{2} & 0 \\ 2 & 0 & 2\sqrt{2} & 0 & 4 \end{pmatrix}. \tag{II.8}$$

The kernel corresponds to the generating set

$$\{\sqrt{2} - x^2, 2 - x^4, \sqrt{2}x - x^3\} \tag{II.9}$$

The moment matrix satisfies $\operatorname{rank} M(\lambda_1) = \operatorname{rank} M(\lambda_2) = 2$ and the kernel generates the correct real radical ideal.

III. Computation of generators of the real radical up to a given degree

Based on the maximum rank moment matrix, the geometric involutive form [24], the results of Curto and Fialkow [11] and Lasserre et al. [18] we give an algorithm for computing the real radical up to a given degree d. Throughout this section we consider a system of multivariate polynomials $\{f_1, \cdots, f_m\} \subseteq \mathbb{R}[x_1, x_2, ..., x_n]$ of degree $d = \max_i(\deg(f_i))$. The associated real ideal is denoted

$$I := \langle f_1, f_2, ..., f_m \rangle_{\mathbb{R}} \tag{III.1}$$

and its associated real radical ideal is denoted by $\sqrt[\mathbb{R}]{I}$.

In particular we solve the following problem:

Problem III.1. *Given a system of multivariate polynomials $P = \{f_1, \cdots, f_m\} \subseteq \mathbb{R}[x_1, x_2, ..., x_n]$ with associated ideal $I = \langle P \rangle_{\mathbb{R}}$ and an integer d we give an algorithm to compute:*

$$\left(\sqrt[\mathbb{R}]{I}\right)_{(\leq d)} := \{f \in \sqrt[\mathbb{R}]{I} : \deg(f) \leq d\}. \tag{III.2}$$

We will represent $\left(\sqrt[\mathbb{R}]{I}\right)_{(\leq d)}$ by polynomials corresponding to vectors in $\ker M(\lambda_d)$ where $M(\lambda_d)$ is the truncated moment matrix to degree d as defined in Definition II.2. In order to obtain our main result we will require that $\ker M(\lambda_d)$ is *ideal-like* as defined by Curto and Fialkow [11].

Definition III.1 (Ideal-like truncated moment matrix [11])**.** *The kernel of a truncated moment matrix $M(\lambda_d)$ is ideal-like of degree d if the following two conditions are satisfied:*

- *If $f_1, f_2 \in \mathbb{P}(\ker M(\lambda_d))$ then $f_1 + f_2 \in \mathbb{P}(\ker M(\lambda_d))$.*
- *If $f \in \mathbb{P}(\ker M(\lambda_d))$ and $g \in \mathbb{R}[x]$ has $\deg(fg) \leq d$, then $fg \in \mathbb{P}(\ker M(\lambda_d))$.*

The ideal-like property is denoted as RG in [11].

Our main result which relates the real radical and the kernel of the moment matrix in the positive dimensional case is:

Theorem III.1. *Suppose an ideal $I = \langle f_1, \dots f_m \rangle_{\mathbb{R}}$ is given with $\max_i(\deg(f_i)) = d$ and let B be the coefficient matrix of $\{f_1, \dots f_m\} \subseteq \mathbb{R}[x]$. Let $M(\lambda_d)$ be a truncated moment matrix such that $B^T \cdot M(\lambda_d) = 0$ and $M(\lambda_d) \succeq 0$. If the rank of $M(\lambda_d)$ is maximum and* $\ker M(\lambda_d)$ *is ideal-like then*

$$\mathbb{P}(\ker M(\lambda_d)) = \left(\sqrt[\mathbb{R}]{I}\right)_{(\leq d)}. \tag{III.3}$$

To prove the above theorem, we will need Theorem II.2, Theorem II.3 and Lemma II.2.

Proof: Suppose $\ker M(\lambda_d)$ is *ideal-like*, $M(\lambda_d) \succeq 0$ and $M(\lambda_d)$ has maximum rank together with the other assumptions in Theorem III.1. Our goal is to show that

$$\mathbb{P}(\ker M(\lambda_d)) = \left(\sqrt[\mathbb{R}]{I}\right)_{(\leq d)}.$$

First by Theorem II.2, the following direction is obvious:

$$\mathbb{P}(\ker M(\lambda_d)) \subseteq \left(\sqrt[\mathbb{R}]{I}\right)_{(\leq d)}.$$

So we only need to show

$$\mathbb{P}(\ker M(\lambda_d)) \supseteq \left(\sqrt[\mathbb{R}]{I}\right)_{(\leq d)}.$$

By Theorems II.3 and II.2, λ_d can be extended to λ_{d+1} such that $J = \langle \mathbb{P} \ker(M(\lambda_{d+1})) \rangle_{\mathbb{R}}$ is real radical and zero-dimensional. Since $I \subseteq J$, we have $\sqrt[\mathbb{R}]{I} \subseteq J$. By Theorem II.2, one can extend λ_d to $\lambda = \sum_{i=1}^r \alpha_i \lambda_{v_i} \in \mathbb{R}[x]^*$ where $\alpha_i > 0$ and $\{v_1, \dots, v_r\} = V_{\mathbb{R}}(\mathbb{P}(\ker M(\lambda_{d+1}))) = V_{\mathbb{R}}(J)$ and λ_{v_i} is an evaluation mapping at v_i such that $\lambda_{v_i}(f) = f(v_i)$. Thus $\lambda_d = \sum_{i=1}^r \alpha_i \lambda_{v_i}^{(d)}$ where $\lambda_{v_i}^{(d)}$ is the truncated linear form of λ_{v_i}. Since $\sqrt[\mathbb{R}]{I} \subseteq J$, we have $\{v_1, \dots, v_r\} \subseteq V_{\mathbb{R}}(\sqrt[\mathbb{R}]{I})$.

Now we can prove the other inclusion:

$$\mathbb{P}(\ker M(\lambda_d)) \supseteq \left(\sqrt[\mathbb{R}]{I}\right)_{(\leq d)}.$$

So we let $g \in \left(\sqrt[\mathbb{R}]{I}\right)_{(\leq d)}$ and we want to show that $g \in \mathbb{P}(\ker M(\lambda_d))$, that is to show that $\text{vec}(g)^T M(\lambda_d) = 0$.

Since $g \in \sqrt[\mathbb{R}]{I}$ with $\deg(g) \leq d$, we can conclude $g(v_i) = 0, i = 1, \dots, r$. Therefore, we have $g^2(v_i) = \text{vec}(g)^T M(\lambda_{v_i}^{(d)}) \text{vec}(g) = 0$. Since $M(\lambda_{v_i}^{(d)}) \succeq 0$, we have $\text{vec}(g)^T M(\lambda_{v_i}) = 0$ for $i = 1, \dots, r$. Hence $\sum_{i=1}^r \alpha_i \text{vec}(g)^T M(\lambda_{v_i}^{(d)}) = 0$, so $\text{vec}(g)^T M(\lambda_d) = 0$ and $g \in \mathbb{P} \ker M(\lambda_d)$ which is what we wanted to show. ■

By Theorem III.1, the "ideal-like" property is important. Given a polynomial system P, we can compute its *geometric involutive form, GIF*, which returns an involutive basis of the ideal generated by P. The symbolic-numeric version of the geometric involutive form algorithm, denoted as `GIF`, was first described and implemented in Wittkopf and Reid [29]. Note the `GIF` algorithm obtains polynomials in a form that satisfies the ideal-like property, so $P = \texttt{GIF}(P)$ implies P is "ideal-like". The details of the `GIF` algorithm, including, prolongations and projections, can be found in our earlier work [24]. The algorithm for computing the maximum rank solution will be discussed in the next section. We now state our complete algorithm to Problem III.1:

Algorithm 1: RealRadical(P, d)

Input($P = \{f_1, \dots, f_m\} \subseteq \mathbb{R}[x]$, $x \in \mathbb{R}^n$*, an integer* $d \geq \deg(P)$.)
Set P' to be the prolongation of P to degree d.
repeat
  $B :=$ CoeffMtx(P').
  Solve for maximum rank moment matrix $M(\lambda_d)$ such that $B^T M(\lambda_d) = 0, M(\lambda_d) \succeq 0$ using Algorithm 2 described in the next section.
  $P'' := \mathbb{P}(\ker M(\lambda_d))$.
  Compute $\texttt{GIF}(P'')$.
  Project/ Prolong $\texttt{GIF}(P'')$ to degree d:
  $P' := \texttt{GIF}(P'')_{(\leq d)}$.
until $\dim P' = \dim P''$;
Output(P'*, a basis for* $\{f \in \sqrt[\mathbb{R}]{\langle P \rangle_{\mathbb{R}}} : \deg(f) \leq d\}$.)

Lemma III.1. *Algorithm 1 is correct.*

Proof: By lemma II.2, at each iteration, we have $P'' \subseteq \left(\sqrt[\mathbb{R}]{\langle P \rangle_{\mathbb{R}}}\right)_{(\leq d)}$. Therefore $P' := \texttt{GIF}(P'')_{(\leq d)} \subseteq \left(\sqrt[\mathbb{R}]{\langle P \rangle_{\mathbb{R}}}\right)_{(\leq d)}$. When Algorithm 1 stops, $P' = P'' = \texttt{GIF}(P)$ is "ideal-like". So by Theorem III.1, we have $P' = \left(\sqrt[\mathbb{R}]{\langle P' \rangle_{\mathbb{R}}}\right)_{(\leq d)}$.

Since $\langle P\rangle_{\mathbb{R}} \subseteq \langle P'\rangle_{\mathbb{R}}$, we have $\left(\sqrt[\mathbb{R}]{\langle P\rangle_{\mathbb{R}}}\right)_{(\leq d)} \subseteq P'$. Therefore, we proved $\left(\sqrt[\mathbb{R}]{\langle P\rangle_{\mathbb{R}}}\right)_{(\leq d)} = P'$. ∎

Remark III.1 (Real radical membership verification)**.** *Given a polynomial $g \in \mathbb{R}[x]$ with $\deg(g) \leq d$ and a polynomial system P, the problem for determining whether $g \in \sqrt[\mathbb{R}]{\langle P\rangle_{\mathbb{R}}}$ or not is equivalent to checking if g lies in* RealRadical*(P, d) which can be done using simple linear algebra. The termination of Algorithm 1 is guaranteed by the finite descending chain property of the Noetherian ring $\mathbb{R}[x]$.*

IV. SDP and facial reduction

Semidefinite programming and facial reduction are important tools for efficiently obtaining the accurate maximum rank moment matrix as required by Algorithm 1 in Section III.

Recall that we denote positive semidefinite and positive definite matrices using $A \succeq 0, A \succ 0$, respectively.

Definition IV.1 (Trace inner product)**.** *Given $A, B \in \mathcal{S}^k$, the trace inner product is $\langle A, B\rangle = \operatorname{trace}(AB) = \sum_{ij} A_{ij}B_{ij}$.*

Definition IV.2. *Suppose $A_1, ..., A_l \in \mathcal{S}^k$. The constraint linear map $\mathcal{A} : \mathcal{S}^k \to \mathbb{R}^l$ is*

$$\mathcal{A}(X) := \big(\langle A_1, X\rangle, ..., \langle A_l, X\rangle\big)^T \in \mathbb{R}^l,\ X \in \mathcal{S}^k. \qquad \text{(IV.1)}$$

The adjoint operator of $\mathcal{A}$, denoted $\mathcal{A}^* : \mathbb{R}^l \to \mathcal{S}^k$, is the unique linear map that satisfies

$$\langle \mathcal{A}^*(y), X\rangle = \langle y, \mathcal{A}(X)\rangle, \forall X \in \mathcal{S}^k, \forall y \in \mathbb{R}^l, \qquad \text{(IV.2)}$$

and is explicitly given by: $\mathcal{A}^*(y) := \sum_{i=1}^{l} y_i A_i$.[1]

Definition IV.3. *Given a matrix $H = (a_{ij})_{1\leq i,j\leq k} \in \mathbb{R}^{k\times k}$, define vec$(H)$ to be the vectorization of H columnwise, i.e.,*

$$vec(H) = \big(a_{11}, a_{12}, \ldots, a_{1k}, a_{21}, a_{22}, \ldots, a_{k1}, \ldots, a_{kk}\big)^T \in \mathbb{R}^{k^2}.$$

The matrix representation of the linear operator $\mathcal{A}$, denoted as A, is $A = [\operatorname{vec}(A_1), ..., \operatorname{vec}(A_l)]^T \in \mathbb{R}^{l\times k^2}$.

A. Facial structure and minimal face

The following results can be found in e.g., [6], [7], [9], [14], [23].

Definition IV.4. *Given convex cones F, K and $F \subseteq K$, we call F a face of K, and write $F \trianglelefteq K$ if*

$$x, y \in K, x + y \in F \implies x, y \in F.$$

Given a nonempty convex subset S of K, the minimal face *of K containing S is defined to be the intersection of all faces of K containing S and is denoted* face(S).

Definition IV.5. *Let F be a face of $\mathcal{S}_+^k$. The* conjugate face *of F is $F^c := \{Z \in \mathcal{S}_+^k : Z \cdot X = 0, \forall X \in F\}$. The dual cone of F, is $F^* := \{Z \in \mathcal{S}^k : Z \cdot X \succeq 0, \forall X \in F\}$.*

The following classical results about facial structure can be found in e.g., [30].

Lemma IV.1. *Let $F \trianglelefteq \mathcal{S}_+^k$ and $X \in \operatorname{relint} F$. Let $X = \begin{bmatrix} U & V\end{bmatrix}\begin{bmatrix} D_r & 0 \\ 0 & 0\end{bmatrix}\begin{bmatrix} U & V\end{bmatrix}^T$, $D_r \in \mathcal{S}_{++}^r$ be the orthogonal spectral decomposition. Then*

$$F = U\mathcal{S}_+^r U^T, \quad F^c = V\mathcal{S}_+^{n-r}V^T.$$

Lemma IV.2. *Let $F \trianglelefteq \mathcal{S}_+^k$ and $W \in \mathcal{S}_+^k$. Then both $\mathcal{S}_+^k \cap \{W\}^\perp$ and $F \cap \{W\}^\perp$ are faces of $\mathcal{S}_+^k$.*[2]

B. Facial reduction

We consider our feasible SDP set $F_P := \{X \in \mathcal{S}^k : \mathcal{A}(X) = b, X \succeq 0\}$. Clearly F_P is a convex subset of $\mathcal{S}^k$. The following theorem gives information on the facial structure of F_P.

Theorem IV.1 ([23, SDP version of Lemma 28.4])**.** *Let*

$$F_{\min} := \operatorname{face}(F_P) \trianglelefteq F \trianglelefteq \mathcal{S}_+^k.$$

Then

$$\left\{ \begin{array}{ll} I. & \mathcal{A}(X) = b, X \in F \\ II. & b^T y = 0,\ Z = \mathcal{A}^* y \in F^* \setminus F^\perp \end{array} \right\} \Rightarrow X \in \{Z\}^\perp \cap F \subset F.$$

In addition, $F = F_{\min}$ if and only if (II) has no solution.

The matrix Z is called an *exposing vector*. Each time (II) is solved, an exposing vector Z is obtained and can be used to update $F \leftarrow \{Z\}^\perp \cap F$. Repeating this process until (II) is infeasible yields a finite sequence of faces containing F_P: $F_0 \supset F_1 \supset F_2 \supset \cdots \supset F_{\min} \supset F_p$, where $F_0 = \mathcal{S}_+^k$ and $F_{i+1} = F_i \cap \{Z_i\}^\perp$. This iteration process to find the minimal face $F_{\min}$ is called *facial reduction* and is guaranteed to terminate in at most $k - 1$ iterations [28]. The minimal number of facial reductions is called the *singularity degree*, [27].

C. Facial reduction maximum rank algorithm

Our facial reduction algorithm follows from Theorem IV.1. We use the following Lemmas to convert $(I), (II)$ of Theorem IV.1 to equivalent problems that are easier and more practical to solve. The proofs of these Lemmas can be found in Appendix A, page 8.

Lemma IV.3. *Let $F := U\mathcal{S}_+^r U^T \trianglelefteq \mathcal{S}_+^k, U \in \mathbb{R}^{k\times r}$, and U full column rank. Then*

$$\exists X \in F,\ \mathcal{A}(X) = b \iff \exists \bar{X} \in \mathcal{S}_+^r,\ U^T \mathcal{A} U(\bar{X}) = b,$$

where $U^T \mathcal{A} U$ is a linear operator from $\mathcal{S}^r$ to $\mathbb{R}^l$ defined as

$$(U^T\mathcal{A}U)(\bar{X}) = \big(\langle U^T A_1 U, X\rangle, ..., \langle U^T A_l U, X\rangle\big)^T, \bar{X} \in \mathcal{S}^r.$$

Lemma IV.4. *Let $F := U\mathcal{S}_+^r U^T \trianglelefteq \mathcal{S}_+^k, U \in \mathbb{R}^{k\times r}$, and U full column rank. Then the following two statements are equivalent:*

$$\exists y : Z = \mathcal{A}^*(y) \in F^* \setminus F^\perp,\ b^T y = 0 \qquad \text{(IV.3)}$$
$$\exists y : 0 \neq \bar{Z} = (U^T\mathcal{A}U)^*(y) \succeq 0,\ b^T y = 0. \qquad \text{(IV.4)}$$

Lemma IV.5. *Let Z be an exposing vector as in* (IV.3) *and let $\bar{Z}$ be as in* (IV.4)*. Let V be full column rank with* $\operatorname{range}(V) = \operatorname{null}(\bar{Z})$*. Let $F := U\mathcal{S}_+^r U^T \trianglelefteq \mathcal{S}_+^k, U \in \mathbb{R}^{k\times r}$. Then*

$$\{Z\}^\perp \cap F = UV\mathcal{S}_+^{\bar{r}} V^T U^T.$$

Recall in Algorithm 1, we need to find $M(\lambda_d)$ such that $B^T M(\lambda_d) = 0, M(\lambda_d) \succeq 0$. All such moment matrices form a

[1] Here $\langle y, \mathcal{A}(X)\rangle = y^T\mathcal{A}(X)$ is the standard vector inner product.

[2] Here $\{W\}^\perp$ denotes the orthogonal complement.

convex subset of $\mathbb{R}^{k\times k}$, the moment matrices $M(\lambda_d)$ form an affine subspace defined by $\mathcal{A}(X) = b$. The construction of $\mathcal{A}$ is described in [24]. So the set $\{M(\lambda_d) : B^T M(\lambda_d) = 0, M(\lambda_d) \succeq 0\}$ can be converted to a convex set $\mathcal{F}_p := \{X \in \mathcal{S}^k : \mathcal{A}(X) = b, B^T X = 0, X \succeq 0\}$. The algorithm to find maximum rank solutions of $\mathcal{F}_p$ needed in Algorithm 1 is summarized in the following Algorithm 2.

Algorithm 2: Facial reduction on the primal.

Input($\mathcal{A} : \mathcal{S}^k \to \mathbb{R}^l, b \in \mathbb{R}^l, B \in \mathbb{R}^{k\times m},\ j = 1.$)
repeat
  If $j = 1$, set $Z = BB^T$, $U = I$. Else,

$$\text{find} \quad 0 \neq Z = \sum_{i=1}^{l} A_i y_i \succeq 0, b^T y = 0 : y \in \mathbb{R}^l. \quad \text{(IV.5)}$$

  Find a basis V for null(Z).
  Update $\mathcal{A}$ by setting $A_i \leftarrow V^T A_i V, i = 1 \ldots l$.
  Update U by setting $U \leftarrow U \cdot V$.
  $j = j + 1$.
until (IV.5) *has unique solution* $Z = 0$;
Solve $\mathcal{A}(P) = b, P \succ 0$. Set $X := UPU^T$.
Output(*a maximum rank solution* X)

Lemma IV.6 (Maximum rank)**.** *Algorithm 2 returns a maximum rank solution of* $\mathcal{F}_p$.

Proof: (We outline a proof. More details for a similar facial reduction approach can be found in e.g., [7].) Each nonzero exposing vector results in a reduction to an equivalent SDP of smaller dimension. This is done until no further progress can be made. The finite convergence uses the above results in Lemmas IV.3, IV.4, IV.5 and Theorem IV.1. ∎

Remark IV.1 (Singularity degree)**.** *Recall that the minimum number of facial reduction steps is called the* singularity degree*. In Section VII below we show that instances with singularity degree greater than 1 can be accurately solved with the facial reduction heuristic. For more details, see e.g., [13], [27].*

V. A Special Case for Determining the Positive Dimensional Real Radical

An important open problem in real algebraic geometry is to determine an integer d such that $\left(\sqrt[\mathbb{R}]{I}\right)_{(\le d)}$ actually generates the whole real radical $\sqrt[\mathbb{R}]{I}$. Our theorem on the determination of the real radical up to finite degree is illustrated graphically in Figure V.1. Here suppose $F = \{f_1, ..., f_m\} \subset \mathbb{R}[x]$ and we applied Algorithm 1 RealRadical(F, d) for a given d, and that the resulting system has leading monomials shown as the corners of the black monomial staircase. See [10] for the description of such diagrams. Then the system is prolonged and the kernel of its moment matrix is examined for new generators at degrees $d+1, d+2, \ldots$. The only way that this is not a complete generating set for the real radical (and that our conjecture fails), is that there is a minimum degree $d' > d$ where after prolongation to d' new generators are determined that lie outside simple prolongations of the black leading generators. These have leading monomials shown in red. Sometimes the completeness of the generating set at degree d can be checked by a critical point calculation. For example, if

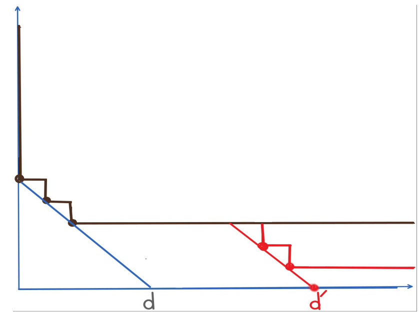

Figure V.1. In the Figure, the black monomial staircase represents the leading monomials of the generators of the real radical determined to degree d by RealRadical(P, d). The only way these can fail to be a complete set of generators for the real radical is that there is a minimum degree $d' > d$ where additional generators with leading monomials of exactly degree d' shown in red are found outside black monomial staircase.

the critical point method shows that the variety is real positive dimensional, then this could rule out the existence of the red staircase predicting a 0-dimensional real variety. In particular, if the number of red circles in Figure V.1 is 1 and the variety of F is real positive dimensional, then RealRadical(F, d) returns the generators of $\sqrt[\mathbb{R}]{\langle F\rangle_{\mathbb{R}}}$. We get the following

Theorem V.1. *Given a system of multivariate polynomials* $F = \{f_1, \cdots, f_m\} \subseteq \mathbb{R}[x_1, x_2, ..., x_n]$ *with associated ideal* $I = \langle F\rangle$ *and an integer* d*. Let* $G = \{g_1, ..., g_k\} \subset \mathbb{R}[x]$ *be the output of Algorithm 1 RealRadical(F, d) applied to* F *and let* s *be the number of linearly independent polynomials of degree* d *in* G*. If* $s = \binom{d+n-1}{n-1} - 1$ *and the variety of* F *is real positive dimensional, then we have*

$$\sqrt[\mathbb{R}]{\langle F\rangle_{\mathbb{R}}} = \langle G\rangle_{\mathbb{R}}. \quad \text{(V.1)}$$

Proof: By Theorem III.1, we get $\left(\sqrt[\mathbb{R}]{\langle F\rangle_{\mathbb{R}}}\right)_{(\le d)} = \text{span}_{\mathbb{R}}\, G$. Now suppose that the result fails, i.e., suppose that $\sqrt[\mathbb{R}]{\langle F\rangle_{\mathbb{R}}} \supset \langle G\rangle_{\mathbb{R}}$, and there exists a $d' > d$ such that $(\langle H\rangle_{\mathbb{R}})_{(\le d')} \subset \left(\sqrt[\mathbb{R}]{\langle F\rangle_{\mathbb{R}}}\right)_{(\le d')}$, where H is the prolongation of G to degree d'. Therefore there exists a polynomial $\tilde{g} \in \text{span}_{\mathbb{R}}\, \bar{G}$ but with $g \notin \text{span}_{\mathbb{R}}\, H$ and with $\deg(\tilde{g}) = d' > d$, where $\bar{G} = \{\bar{g}_1, ..., \bar{g}_l\}$ spans $\left(\sqrt[\mathbb{R}]{\langle F\rangle_{\mathbb{R}}}\right)_{(\le d')}$.

Now assume the number of linearly independent polynomials of degree d' in H is t and the number of linearly independent polynomials of degree d' in $\bar{G}$ is $\bar{t}$. Then $t < \bar{t}$ because of the existence of $\tilde{g}$. By a simple combinatorial argument, the number of distinct monomials of degree d in n variables is $\binom{d+n-1}{n-1}$. Since G is already involutive and $s = \binom{d+n-1}{n-1} - 1$, we have $t = \binom{d'+n-1}{n-1} - 1$ as well. Also clearly $\bar{t} \le \binom{d'+n-1}{n-1}$. Therefore we conclude that $\bar{t} = \binom{d'+n-1}{n-1}$. This means that $\sqrt[\mathbb{R}]{\langle F\rangle_{\mathbb{R}}}$ is a 0-dimensional real variety, a contradiction with the assumption that the variety of F is real positive dimensional. ∎

VI. Numerical Computational Issues

In Algorithm 2, we need to solve two subproblems: the auxiliary problem (IV.5); and the primal problem after facial reduction $\mathcal{A}(P) = b, P \succ 0$. Essentially, we need to find the intersection between an affine subspace (linear constraints) and a positive semidefinite cone. The two problems can be solved efficiently by well-known interior point solvers. However, these interior-point solvers are not the appropriate choice for our problem as illustrated by the examples in Section VII, below. When solving the auxiliary problem (IV.5), interior point based methods can yield small positive eigenvalues which makes the facial reduction steps very unstable as it is difficult to distinguish which eigenvalues are zero.

We consider the *Douglas-Rachford reflection-projection* (DR) method e.g., [1], [5], [12]. This method involves projections and reflections between two convex sets. These two convex sets are the affine subspace and the positive semidefinite cone in our case. There are also other projection-based methods, such as the simpler method of *alternating projection* [16]. We prefer the DR method for our application as it displayed better convergence properties in our tests. Moreover, we can project onto the semidefinite cone with a specific rank of our choice in order to avoid small eigenvalues in the solution of the auxiliary problem (IV.5). The convergence rate of the DR method is studied by Bauschke et al [3], [4]. Also, unlike the alternating projection method, which is likely to converge to the boundary of the cone, the DR method is likely to converge to the interior of the cone which is needed in Algorithm 2 for solving $\mathcal{A}(P) = b, P \succ 0$.

VII. Numerical results

We used MATLAB version 2015a. The computations were carried out on a desktop with ubuntu 12.04 LTS, Intel Core™2 Quad CPU Q9550 @ 2.83 GHz × 4, 8GB RAM, 64-bit OS, x64-based processor.

In Examples VII.1, VII.2 we see that the algorithm solves the problems of singularity degree 2. The next two examples VII.3,VII.4 of higher singularity degree were not solved accurately in previous attempts [24]. We show here that additional facial reductions steps resulted in accurate solutions. In all our examples tested, d is chosen to be the degree of the input system. Only one iteration of Algorithm 1 is needed. Therefore `GIF` is only called once. We conjecture that this is true in general.

Example VII.1 (Reducible cubic)**.**

$$(x+y)(x^2+y^2+2). \tag{VII.1}$$

Note that the second factor has no real roots, so it is discarded and the real radical is generated by $(x+y)$*. The moment matrix corresponding to* (VII.1) *is a* 10×10 *matrix. The coefficient matrix* B *is* $[0,2,2,0,0,0,1,1,1,1]^T$*. Using Algorithm 1, after two facial reduction steps, we obtain a maximum rank* 4 *moment matrix with residual less than* 10^{-14} *in less than* 200 *DR iterations.*[3] *The output approximates the real radical ideal generated by* $(x+y)$ *and its prolongations to degree* 3*.*

Example VII.2 (Reducible quintic)**.**

$$(1+x+y)(x^4+y^4+2). \tag{VII.2}$$

The moment matrix corresponding to (VII.2) *is a* 21×21 *matrix. We solve this problem using Algorithm 1. Algorithm 1 can get* 14 *decimal accuracy and a maximum rank moment matrix of rank* 6 *in about* 1300 *DR iterations with* 2 *facial reduction steps. The output approximates the real radical ideal generated by* $(1+x+y)$ *and its prolongations to degree* 5*.*

Example VII.3 (Two variable geometric polynomial with 3 facial reductions)**.**

$$1+(x+y)+(x+y)^2+(x+y)^3. \tag{VII.3}$$

The moment matrix corresponding to (VII.3) *is a* 10×10 *matrix. The coefficient matrix* B *is* $[2,2,2,1,0,1,1,1,1,1]^T$*.*

After 3 *facial reductions, the face is reduced to dimension* 4 *and the moment matrix is obtained with residual* 10^{-13}*. The eigenvalues of the final moment matrix are* $4.70, 3.48, 0.89, 0.59, 0,0,0,0,0,0$ *which gives the correct maximum rank of* 4*.*

Application of Algorithm 1 yields the correct generators of the real radical $\langle 1+x+y\rangle$ *up to degree 3.*

Example VII.4 ([8])**.**

$$f = \{2yz-y,\ 2y^2+y,\ xy,\ 4x^2z+4z^3+y\}. \tag{VII.4}$$

The generators of the real radical is [8]:

$$\{z^2+y/2, yz-y/2, y^2+y/2, xz, xy, y+z\},$$

which is the same as the output of Algorithm 1. The moment matrix of this problem is a 20×20 *matrix. We use Algorithm 2 to solve for the maximum rank moment matrix. The sizes of the SDP problem are* $\{20,16,14,8\}$ *after* 3 *facial reductions. The residual of the auxiliary problem at each facial reduction is* $10^{-15}, 10^{-14}$*. (The first facial reduction is done using a MATLAB eigenvalue decomposition so we do not include the residual.) The moment matrix is solved with residual* 10^{-13} *and the maximum rank is* 8*.*

	min # FR	rank (FR)	sing. deg.	Res(FR)	Res(CVX)
Ex VII.1	2	10, 9, 4	2	10^{-14}	10^{-9}
Ex VII.2	2	21, 20, 6	2	10^{-14}	10^{-9}
Ex VII.3	3	10, 9, 7, 4	3	10^{-13}	10^{-9}
Ex VII.4	3	20, 16, 14, 8	3	10^{-13}	10^{-9}

Table VII.1: **Comparison between facial reduction and SeDuMi (1)** Here: "min (max) # FR" means minimal (maximum) number of facial reductions in our tests; "rank(FR)" means the size of the problem after each facial reduction, the first one is the size of the original problem; "Singlty deg" is the singularity degree of the SDP problem after the 1st facial reduction; "Res(FR)" is the residual of the final moment matrix using facial reduction and DR iterations (Algorithm 2); "Res(CVX)" is the residual of the final moment matrix using CVX(SeDuMi).

We then compare Algorithm 2 with the traditional interior point solver SeDuMi using CVX, e.g., [17]. In the computations for

	max rank	res each FR	# DR each FR	Time
Ex VII.1	4	$10^{-15}, 10^{-15}$	120, 7	0.11s
Ex VII.2	6	$10^{-15}, 10^{-14}$	267, 6	0.26s
Ex VII.3	4	$10^{-15}, 10^{-14}, 10^{-15}$	260, 143, 1	0.16s
Ex VII.4	8	$10^{-15}, 10^{-14}, 10^{-14}$	625, 437, 29	0.48s

Table VII.2: **Comparison between facial reduction and SeDuMi (2)** "max rank" is the maximum rank of the moment matrix; "res each FR" is the residual of solving the corresponding SDP problem by DR after each facial reduction; " # DR each FR" is the number of DR iterations to solve the corresponding SDP problem after each facial reduction.

[3]Note that each DR iteration is extremely inexpensive relative to interior point iterations.

	min # FR	rank (FR)	Run time	# DR each FR	Res(FR)
Ex VII.5	2	10, 9, 4	0.09s	120, 7	10^{-14}
Ex VII.6	2	21, 20, 6	0.23s	245, 6	10^{-13}
Ex VII.7	3	10, 9, 7, 4	0.30s	260, 146, 1	10^{-13}
Ex VII.8	3	20, 16, 14, 8	0.58s	616, 452, 29	10^{-13}

Table VII.3: **Perturbations**

the above examples and Table VII.1,VII.2, the traditional interior point SDP solver SeDuMi(CVX) performed relatively poorly in computing the maximum rank moment matrices. In contrast, with facial reduction and the DR method, we get much better accuracy and also the correct maximum rank.

A. Perturbed examples

In this subsection, we study how small perturbations affect our Algorithm 2. The computational results are shown in Table VII.3.

Example VII.5 (Perturbed Reducible cubic)**.**

$$(x+y)(x^2+y^2+0.000001xy+2). \tag{VII.5}$$

Example VII.6 (Perturbed Reducible quintic)**.**

$$(1+x+y)(x^4+y^4+0.000001xy+2). \tag{VII.6}$$

Example VII.7.

$$1+1.000001(x+y)+0.999999(x+y)^2+1.000001(x+y)^3. \tag{VII.7}$$

Example VII.8.

$$f=\{2yz-y+\epsilon,\ 2y^2+y-\epsilon,\ xy+\epsilon,\ 4x^2z+4z^3+y-\epsilon\}, \tag{VII.8}$$

where $\epsilon = 1\times 10^{-14}$.

In examples VII.5 VII.6 and VII.5 where the coefficients of the real radical ideal change continuously with respect to the changes of the input polynomial system, Algorithm 2 has the same performance on the examples as on the ones without perturbation. For example VII.8 where theoretically the real radical ideal can be very different under small perturbations, Algorithm 2 still works very well if the perturbation is smaller than the residual of the final moment matrix.

VIII. Conclusion

SDP feasibility problems typically involve the intersection of the convex cone of semidefinite matrices with a linear manifold. Their importance in applications has led to the development of many specific algorithms. However these feasibility problems are often marginally infeasible, i.e., they do not satisfy strict feasibility as is the case for our polynomial applications. Such problems are *ill-posed* and *ill-conditioned*.

This paper is part of a series in which we exploit facial reduction and apply it to finding real solutions to systems of real polynomial and differential equations. The current work is directed at guaranteeing the maximal rank property and the ideal-like condition to ensure all the generators of the real radical up to a given degree are captured. It also establishes the first examples of additional facial reduction that are effective in practice for polynomial systems.

This builds on our work in [24] in which we introduced facial reduction, for the class of SDP problems arising from analysis and solution of systems of real polynomial equations for real solutions. Facial reduction yields an equivalent smaller regularized problem for which there are strictly feasible points. Facial reduction also reduces the size of the moment matrices occurring in the application of SDP methods. For example the determination of a $k\times k$ moment matrix for a problem with m linearly independent constraints is reduced to a $(k-m)\times(k-m)$ moment matrix by one facial reduction. The high accuracy required by facial reduction and also the ill-conditioning commonly encountered in numerical polynomial algebra [26] motivated us to implement the Douglas-Rachford appproach [24].

A fundamental open problem is to generalize the work of [19], [25] to positive dimensional ideals. In essence, this requires the determinations of a degree bound d such that $\left(\sqrt[\mathbb{R}]{I}\right)_{(\leq d)}$ actually generates the whole real radical $\sqrt[\mathbb{R}]{I}$. At the current stage, there is no practical degree bound when I is real positive dimensional. In section V, we only give an answer for a special case.

Recently, Hauenstein et al [8] have made progress on this fundamental open problem by using sample points determined by Hauenstein critical point algorithm. This is able to certify the generators of the real radical ideal in some cases. Our results Theorem III.1 enables the determination of the generators up to a given degree. Thus we give an answer to the open problem of real radical ideal membership test left in [8]. Potentially, the efficiency for computing the sample points can also be improved which will be described in a subsequent work.

References

[1] F.J.A. Artacho, J.M. Borwein, and M.K. Tam. Recent results on Douglas-Rachford methods. *Serdica Mathematical Journal*, 39:313–330, 2013. 6

[2] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in Real Algebraic Geometry*, volume 10 of *Algorithms and Computation in Math*. Springer-Verlag, 2 edition, 2006. 2

[3] H.H. Bauschke, J.Y. Bello Cruz, T.T.A. Nghia, H.M. Phan, and X. Wang. The rate of linear convergence of the Douglas-Rachford algorithm for subspaces is the cosine of the Friedrichs angle. *J. Approx. Theory*, 185:63–79, 2014. 6

[4] H.H. Bauschke and D. Noll. On the local convergence of the Douglas-Rachford algorithm. *Arch. Math. (Basel)*, 102(6):589–600, 2014. 6

[5] J.M. Borwein and M.K. Tam. A Cyclic Douglas–Rachford Iteration Scheme. *J. Optim. Theory Appl.*, 160(1):1–29, 2014. 6

[6] J.M. Borwein and H. Wolkowicz. Facial reduction for a cone-convex programming problem. *J. Austral. Math. Soc. Ser. A*, 30(3):369–380, 1980/81. 2, 4

[7] J.M. Borwein and H. Wolkowicz. Regularizing the abstract convex program. *J. Math. Anal. Appl.*, 83(2):495–530, 1981. 2, 4, 5

[8] D. Brake, J. Hauenstein, and A. Liddell. Numerically validating the completeness of the real solution set of a system of polynomial equations. *Procedings of the 41th International Symposium on Symbolic and Algebraic Computation*, 2016. 1, 6, 7

[9] Y-L. Cheung, S. Schurr, and H. Wolkowicz. Preprocessing and regularization for degenerate semidefinite programs. In D.H. Bailey, H.H. Bauschke, P. Borwein, F. Garvan, M. Thera, J. Vanderwerff, and H. Wolkowicz, editors, *Computational and Analytical Mathematics, In Honor of Jonathan Borwein's 60th Birthday*, volume 50 of *Springer Proceedings in Mathematics & Statistics*, pages 225–276. Springer, 2013. 4

[10] D. Cox, J. Little, and D. O'shea. *Ideals, varieties, and algorithms*, volume 3. Springer, 1992. 5

[11] R.E Curto and L.A Fialkow. Solution of the truncated complex moment problem for flat data-introduction. *Memoirs of the American Mathematical Society*, 119(568):1, 1996. 2, 3

[12] J. Douglas, JR and H.H. Rachford, JR. On the numerical solution of heat conduction problems in two and three space variables. *Trans. Amer. Math. Soc.*, 82:421–439, 1956. 6

[13] D. Drusvyatskiy, G. Li, and H. Wolkowicz. Alternating projections for ill-posed semidenite feasibility problems. Technical report, University of Waterloo, Waterloo, Ontario, 2014. submitted Sept. 2014, 12 pages. 5

[14] D. Drusvyatskiy, G. Pataki, and H. Wolkowicz. Coordinate shadows of semi-definite and euclidean distance matrices. *Math. Programming*, 25(2):1160–1178, 2015. ArXiv:1405.2037.v1. 4

[15] M. Dür, B. Jargalsaikhan, and G. Still. The Slater condition is generic in linear conic programming. Technical report, University of Trier, Trier, Germany, 2012. 2

[16] R. Escalante and M. Raydan. *Alternating projection methods*, volume 8 of *Fundamentals of Algorithms*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2011. 6

[17] M. Grant and S. Boyd. CVX: Matlab software for disciplined convex programming, version 1.21. http://cvxr.com/cvx, April 2011. 6

[18] J.B. Lasserre, M. Laurent, and P. Rostalski. Semidefinite characterization and computation of zero-dimensional real radical ideals. *Foundations of Computational Mathematics*, 8(5):607–647, 2008. 2, 3

[19] J.B. Lasserre, M. Laurent, and P. Rostalski. A prolongation–projection algorithm for computing the finite real variety of an ideal. *Theoretical Computer Science*, 410(27):2685–2700, 2009. 1, 7

[20] M. Laurent and P. Rostalski. The approach of moments for polynomial equations. In Miguel F. Anjos and Jean B. Lasserre, editors, *Handbook on semidefinite, conic and polynomial optimization*, International Series in Operations Research & Management Science, 166, pages 25–60. Springer, New York, 2012. 2

[21] Y. Ma. *Polynomial Optimization via Low-rank Matrix Completion and Semidefinite Programming*. PhD thesis, Academy of Mathematics and Systems Science, Chinese Academy of Science, 2012. 1

[22] Y. Ma, C. Wang, and L. Zhi. A certificate for semidefinite relaxations in computing positive dimensional real varieties. *Journal of Symbolic Computation*, 72:1 – 20, 2016. 1

[23] G. Pataki. Strong duality in conic linear programming: facial reduction and extended duals. In David Bailey, Heinz H. Bauschke, Frank Garvan, Michel Thera, Jon D. Vanderwerff, and Henry Wolkowicz, editors, *Computational and analytical mathematics*, volume 50 of *Springer Proc. Math. Stat.*, pages 613–634. Springer, New York, 2013. 4

[24] G. Reid, F. Wang, H. Wolkowicz, and W. Wu. Semidefinite Programming and facial reduction for Systems of Polynomial Equations. *Preprint arXiv:1504.00931v1*, 2015. 3, 5, 6, 7

[25] F. Sottile. *Real solutions to equations from geometry*, volume 57 of *University Lecture Series*. American Mathematical Society, Providence, RI, 2011. 1, 7

[26] Hans J. Stetter. *Numerical polynomial algebra*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2004. 7

[27] J.F. Sturm. Error bounds for linear matrix inequalities. *SIAM J. Optim.*, 10(4):1228–1248 (electronic), 2000. 4, 5

[28] L. Tunçel. *Polyhedral and semidefinite programming methods in combinatorial optimization*, volume 27 of *Fields Institute Monographs*. American Mathematical Society, Providence, RI, 2010. 4

[29] A.D. Wittkopf and G.J. Reid. Fast differential elimination in c: The cdiffelim environment. *Computer Physics Communications*, 139(2):192–217, 2001. 3

[30] H. Wolkowicz, R. Saigal, and L. Vandenberghe, editors. *Handbook of semidefinite programming*. International Series in Operations Research & Management Science, 27. Kluwer Academic Publishers, Boston, MA, 2000. Theory, algorithms, and applications. 4

Appendix

A. Proof of Lemma IV.3

First suppose there exists $X = UMU^T$ satisfying $\mathcal{A}(X) = b$, then we have $U^T\mathcal{A}U(M) = \mathcal{A}(UMU^T) = b$ due to the cyclic property of the trace product.

For the other direction, suppose there exists $\bar{X}$ satisfying $U^T\mathcal{A}U(\bar{X}) = b$, let $X = U\bar{X}^TU^T$ then it is easy to see $\mathcal{A}(X) = b$ as well.

B. Proof of Lemma IV.4

Suppose (IV.3) holds, there exists $Z = \sum_{i=1}^{l} A_i y \in F^*$ which means $\langle Z, UMU^T\rangle \succeq 0$ for all $M \in \mathcal{S}_+^r$ and $\langle U^TZU, M\rangle \succeq 0$ for all $M \in \mathcal{S}_+^r$. Also $Z \notin F^\perp$ which means $\langle U^TZU, M\rangle \neq 0$ for some $M \in \mathcal{S}_+^r$ which indicates $U^TZU \neq 0$.

Now suppose (IV.4) holds, since $\bar{Z} = U^TZU \succeq 0$, we have $\langle Z, UMU^T\rangle = \langle U^TZU, M\rangle \succeq 0$ for all $M \in \mathcal{S}_+^r$. Hence $Z \in F^*$. Since $\bar{Z} \neq 0$, we have $Z \notin \text{null}(U^T)$ so $Z \notin F^\perp$.

C. Proof of Lemma IV.5

First suppose $X = UV\bar{M}V^TU^T$, then we have $\langle Z, X\rangle = \langle U^TZU, V\bar{M}V^T\rangle = 0$ which means $ZX = 0$ since $Z \succeq 0, X \succeq 0$. So $X \in \{Z\}^\perp$ and $X \in F$.

For the other direction, if $X \in F$, then $X = UMU^T$ for some $M \in \mathcal{S}_+^r$. If $X \in \{Z\}^\perp$, then $XZ = 0$ which means $\langle X, Z\rangle = \langle M, U^TZU\rangle = \langle M, \bar{Z}\rangle = 0 \Rightarrow M\bar{Z} = 0$. Hence $M = V\bar{M}V^T$ for $V = \text{null}(\bar{Z})$ and $X = UV\bar{M}V^TU$ for some $\bar{M} \in \mathcal{S}_+^{\bar{r}}$.