Solving rank-constrained semidefinite programs in exact arithmetic

Simone Naldi*

September 19, 2016

Abstract

We consider the problem of minimizing a linear function over an affine section of the cone of positive semidefinite matrices, with the additional constraint that the feasible matrix has prescribed rank. When the rank constraint is active, this is a non-convex optimization problem, otherwise it is a semidefinite program. Both find numerous applications especially in systems control theory and combinatorial optimization, but even in more general contexts such as polynomial optimization or real algebra. While numerical algorithms exist for solving this problem, such as interior-point or Newton-like algorithms, in this paper we propose an approach based on symbolic computation. We design an exact algorithm for solving rank-constrained semidefinite programs, whose complexity is essentially quadratic on natural degree bounds associated to the given optimization problem: for subfamilies of the problem where the size of the feasible matrix is fixed, the complexity is polynomial in the number of variables. The algorithm works under assumptions on the input data: we prove that these assumptions are generically satisfied. We also implement it in Maple and discuss practical experiments.

KEYWORDS. Semidefinite programming, determinantal varieties, linear matrix inequalities, rank constraints, exact algorithms, computer algebra, polynomial optimization, spectrahedra, sums of squares.

*Fields Institute for Research in Mathematical Sciences - 222 College Street, M5T 3J1, Toronto, Ontario, Canada

1 Introduction

1.1 Problem statement

Let $x = (x_1, \ldots, x_n)$ denote a vector of unknowns. We consider the standard semidefinite programming problem with additional rank constraints, as follows:

$$\begin{array}{ll} (\mathrm{SDP})_r & \inf\limits_{x \in \mathbb{R}^n} \ \ell_c(x) \\ & s.t. \ \ A(x) \succeq 0, \quad \text{rank } A(x) \leq r \end{array} \tag{1}$$

Here $\ell_c(x) = c^T x$, $c \in \mathbb{Q}^n$, $A(x) = A_0 + x_1 A_1 + \cdots + x_n A_n$ is a symmetric linear matrix with $A_i \in \mathbb{S}_m(\mathbb{Q})$ (the set of symmetric matrices of size m with entries in $\mathbb{Q}$), and r is an integer, $0 \leq r \leq m$. The formula $A(x) \succeq 0$ means that $A(x)$ is positive semidefinite (*i.e.*, all its eigenvalues are nonnegative) and is called a linear matrix inequality (LMI). Remark that for $r = m$ this is the standard semidefinite programming problem since the rank constraint is inactive. Moreover, when $c = 0$ (*i.e.*, c is the zero vector), $(\mathrm{SDP})_r$ is a rank-constrained LMI. In the whole paper, we refer to $(\mathrm{SDP})_r$ as a rank-constrained semidefinite program with parameters (m, n, r).

The feasible set $\{x \in \mathbb{R}^n : A(x) \succeq 0\}$ of $(\mathrm{SDP})_m$ is denoted by $\mathscr{S}$, and is called a spectrahedron in the convex algebraic geometry literature, or equivalently LMI-set. It is a convex basic semialgebraic set. Conversely, for $r < m$, $(\mathrm{SDP})_r$ is no more a convex optimization problem, in general. Indeed, denoted by $\mathcal{D}_r = \{x \in \mathbb{C}^n : \text{rank } A(x) \leq r\}$ the determinantal variety associated to $A(x)$ of maximal rank r, the feasible set of $(\mathrm{SDP})_r$ is exactly $\mathscr{S} \cap \mathcal{D}_r \cap \mathbb{R}^n = \mathscr{S} \cap \mathcal{D}_r$.

The purpose of this paper is to design an exact algorithm for solving problem $(\mathrm{SDP})_r$. By exact, we mean that, with rational input data $(c, A_0, A_1, \ldots, A_n) \in \mathbb{Q}^n \times \mathbb{S}_m^{n+1}(\mathbb{Q})$ the output of the algorithm is either an empty list, or a finite set S encoded by a rational parametrization [29]. This is the exact algebraic representation encoded by a vector $Q = (q, q_0, q_1, \ldots, q_n) \subset \mathbb{Q}[t]$ such that q_0, q are coprime and:

$$S = \left\{ \left(\frac{q_1(t)}{q_0(t)}, \ldots, \frac{q_n(t)}{q_0(t)} \right) \in \mathbb{R}^n : q(t) = 0 \right\}. \tag{2}$$

When S is not empty, the degree of q is the algebraic degree of every element in S. When the output is not the empty list, the set S which is returned contains at least one minimizer x^* of $(\mathrm{SDP})_r$. Under general assumptions on input data, which are highlighted and discussed below, the strategy to reach our main goal is twofold:

- we prove that the *semialgebraic* optimization problem $(\mathrm{SDP})_r$ can be reduced to a (*finite*) *sequence* of *algebraic* optimization problems, that is, whose feasible set is real algebraic;
- we adapt previous techniques to design *exact algorithms* for solving the reduced algebraic optimization problems.

The coordinates of a minimizer can be approximated by intervals of arbitrary size of rational numbers, by isolating the real solutions of the univariate equation $q(t) = 0$. For complexity estimates of the real root isolation problem *cf.* [26]: these strongly depend on the degree of the polynomial q, to which we refer as the *output degree* of our algorithm. Once the output is returned, one can compute the list of minimizers

by sorting the set S with respect to the value of the objective function $\ell_c(x)$, and deleting the solutions lying out of the feasible set $\mathscr{S} \cap \mathcal{D}_r$: hence, our goal is also to give a bound for the maximal size of the output set S.

1.2 Motivations and previous work

Several problems in optimization are naturally modeled by (rank-constrained) semidefinite programming, SDP for short [1, 3]. Given $f, f_1, \ldots, f_s \in \mathbb{R}[x]$, the general polynomial optimization problem $\inf\{f(x) : \forall i\ f_i(x) \geq 0\}$ can be reduced to a sequence of semidefinite programs of increasing size (*cf.* Lasserre [20], Parrilo [27]). Since this sequence is almost always finite [23], lots of efforts have been made in order to develop efficient algorithms for SDP. Moreover, LMI and SDP conditions frequently appear in systems control theory [2]. Finding low-rank positive semidefinite matrices also concerns the completion problem for some classes of matrices in combinatorics [21]. Finally, an independent application of SDP-based techniques, but highly related to the polynomial optimization problem, is that of checking nonnegativity of multivariate polynomials. Indeed, deciding whether a given $f \in \mathbb{R}[x_1, \ldots, x_k]$ is a sum of squares of at most r polynomials (hence, nonnegative) is equivalent to a rank-constrained semidefinite program (see Section 6.2 and, *e.g.*, [28]).

The ellipsoid method [11] gives an iterative algorithm for solving any convex optimization problem, whose number of iterations is polynomial in the input parameters with fixed precision (*e.g.*, see [1]), even though it is proved to be inefficient in practice. On the other hand, the extension of Karmakar's interior-point method beyond linear programming [22] yields efficient algorithms for computing floating point approximations of a solution, implemented in several solvers such as SeDuMi, SOSTOOLS *etc.* However, these algorithms cannot, in general, manage additional determinantal conditions or non-convexity. Moreover, SDP relaxations of hard combinatorial optimization problems (as the max-cut [10]) usually discard such algebraic constraints, since they break desirable convexity properties. Moreover, interior-point algorithms cannot certify the emptiness of the feasible set or the reaching of solutions of a given rank, and can often suffer of numerical round-off errors. Remark, here, that if the standard SDP problem $(\text{SDP})_m$ has a solution x^* of rank r, then x^* is also a solution of the non-convex problem $(\text{SDP})_r$ (the viceversa is false, in general). Finally, one cannot extract information about the algebraic degree [24] of the solution with numerical methods.

In [25], Newton-like "tangent and lift" and projection methods for approximating a point at the intersection of a linear space and a manifold are proposed: the authors use this approach for solving rank constrained LMI but, in general, without guarantees of convergence, and with the request of a starting feasible point. Henrion, Safey El Din and the author proposed in [15] an exact algorithm for LMI, via suitable variants of the critical point method. This algorithm, implemented in the Maple library SPECTRA [16], has a runtime essentially quadratic on a multilinear Bézout bound on the output degree, and polynomial in n when m is fixed. This last property is shared with the algorithm in [19], which, however, cannot be used in practice, since it strongly relies on quantifier elimination techniques. The algorithm in [9] is also exact, but cannot manage semialgebraic constraints and has regularity assumptions on the input, which are not satisfied in our case. The related problem of computing witness points on determinantal algebraic sets has been addressed and solved in [12, 13, 14].

1.3 General notation

If $f = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[x]$, we denote by $\mathsf{Z}(f)$ the set of complex solutions of $f_1 = 0, \ldots, f_s = 0$, called a complex algebraic set. We also consider real solutions of polynomial equations, that is the real algebraic set $\mathsf{Z}_{\mathbb{R}}(f)$. If $S \subset \mathbb{C}^n$, the ideal of polynomials vanishing on S is denoted by $\mathsf{I}(S)$. An ideal $I \subset \mathbb{R}[x]$ is called radical if it equals its radical $\sqrt{I} = \{f \in \mathbb{R}[x] : \exists\, s \in \mathbb{N}, f^s \in I\}$. An ideal of type $\mathsf{I}(S)$ is always a radical ideal. By Hilbert's Nullstellensatz, one has $\mathsf{I}(\mathsf{Z}(I)) = \sqrt{I}$. The Jacobian matrix of partial derivatives of $\{f_1, \ldots, f_s\}$ is denoted by $Df = (\frac{\partial f_i}{\partial x_j})_{i,j}$.

An algebraic set $V \subset \mathbb{C}^n$ is called irreducible if it is not the union of two proper algebraic subsets; otherwise it is the finite union of irreducible algebraic sets $V = V_1 \cup \cdots \cup V_s$, called the irreducible components. The dimension of V is the Krull dimension of its coordinate ring $\mathbb{C}[x]/\mathsf{I}(V)$. If the V_i in the previous decomposition have the same dimension d, then V is equidimensional of dimension d. Let $V \subset \mathbb{C}^n$ be equidimensional of co-dimension c, and let $\mathsf{I}(V) = \langle f_1, \ldots, f_s \rangle$. We say that V is smooth if its singular locus, that is the algebraic set defined by $f = (f_1, \ldots, f_s)$ and by the $c \times c$ minors of Df, is empty. A set $\mathcal{E} = \mathsf{Z}(I) \setminus \mathsf{Z}(J)$ is called locally closed, and its dimension is the dimension of its Zariski closure $\mathsf{Z}(\mathsf{I}(\mathcal{E}))$.

If V is equidimensional and smooth, and if $g\colon \mathbb{C}^n \to \mathbb{C}^m$ is an algebraic map, the critical points of the restriction of g to V are denoted by $\operatorname{crit}(g, V)$, and defined by $f = (f_1, \ldots, f_s)$ and by the $c + m$ minors of $D(f, g)$. Equivalently, a point $x \in V$ is critical for g on V if and only if the differential map $dg\colon T_x V \to \mathbb{C}^m$ is not surjective (where $T_x V$ is the Zariski tangent space of V at x, *cf.* [31, Sec. 2.1.2]). The elements of $g(\operatorname{crit}(g, V))$ are the critical values, and the elements of $\mathbb{C}^m \setminus g(\operatorname{crit}(g, V))$ are the regular values of the restriction of g to V.

Let $S \subset \mathbb{R}^n$ be any set, and let $f\colon \mathbb{R}^n \to \mathbb{R}$ be a continuous function with respect to the Euclidean topology of $\mathbb{R}^n$ and $\mathbb{R}$. A point $x^* \in S$ is a local minimizer of f on S, if there exists an Euclidean open set $U \subset \mathbb{R}^n$ such that $x^* \in U$ and $f(x^*) \leq f(x)$ for every $x \in U \cap S$. A point $x^* \in S$ is a minimizer of f on S if $f(x^*) \leq f(x)$ for every $x \in S$. In particular, if $\mathcal{C} \subset S$ is a connected component of S, every minimizer of f on $\mathcal{C}$ is a local minimizer of f on S.

We finally recall the notation introduced previously. We consider $m \times m$ symmetric matrices $A_0, A_1, \ldots, A_n \in \mathbb{S}_m(\mathbb{Q})$, and a linear matrix $A(x) = A_0 + x_1 A_1 + \cdots + x_n A_n$. The convex set $\mathscr{S} = \{x \in \mathbb{R}^n : A(x) \succeq 0\}$ is called a spectrahedron. The integer $r \in \mathbb{N}$ will denote the maximal admissible rank in (1). Given an integer $p \in \mathbb{N}$, with $0 \leq p \leq r$, we denote by $\mathcal{D}_p = \{x \in \mathbb{C}^n : \operatorname{rank} A(x) \leq p\}$ the determinantal variety of maximal rank p generated by $A(x)$.

1.4 Outline of main results

We consider the rank-constrained semidefinite programming problem (1), encoded by rational data $(c, A) \in \mathbb{Q}^n \times \mathbb{S}_m^{n+1}(\mathbb{Q})$, and by the integer r related to the rank constraint. Our paper can be divided into two parts.

In the first part (Sections 2 and 3) we prove geometrical properties of problem $(\mathrm{SDP})_r$. In Section 2.1, we represent the algebraic sets $\mathcal{D}_p, p = 0, \ldots, r$, as projections of incidence varieties defined by bilinear equations, and in Proposition 1 we prove that the latter sets are generically smooth and equidimensional. The solutions of $(\mathrm{SDP})_r$ are also local minimizers of ℓ_c on $\mathcal{D}_p \cap \mathbb{R}^n$ (this is proved in Theorem 4) and are

obtained as the projection of critical points of the same map restricted to the incidence varieties (Lemma 2), which are finitely many (Proposition 3). As an outcome, we prove that a *generic* rank-constrained semidefinite program admits finitely many minimizers (Corollary 6).

The second part hosts the formal description of an algorithm for solving $(\mathrm{SDP})_r$ (Section 4) and its correctness (Theorem 7). A complexity analysis is then performed in Section 5, with explicit bounds on the size of the output set S (*cf.* (2)) computed in Proposition 8. We finally discuss the results of numerical tests performed via a first implementation of our algorithm in Section 6.

2 Preliminaries

2.1 Representation via incidence varieties

The algebraic set $\mathcal{D}_p$ will not be represented as the vanishing locus of the $(p+1)\times(p+1)$ minors of $A(x)$, mainly by two reasons. The first is that computing determinants is a difficult task. Even if this first issue could be avoided by some precomputation, the singularities of determinantal varieties appear generically. We are going to represent $\mathcal{D}_p$ as the projection of a more regular algebraic set, reviewing a classical construction.

Let V be a vector space of dimension d and let $\mathbb{G}(e,d)$ be the Grassmannian of linear subspaces of dimension e of V, with $e \leq d$. Fixed a basis of V, a point $L = \mathrm{span}(v_1,\ldots,v_e) \in \mathbb{G}(e,d)$ is represented by the $d \times e$ matrix whose columns are $v_1,\ldots,v_e$. With this in mind, we consider linear subspaces of $\mathbb{C}^m$ to model rank defects in $A(x)$.

Let $A(x) \in \mathbb{S}_m^{n+1}(\mathbb{Q})$, and let $p,r \in \mathbb{N}$, with $0 \leq p \leq r \leq m$. We denote by $Y(y) = (y_{i,j})$ a $m \times (m-p)$ matrix with unknowns entries. Then, for $x^* \in \mathbb{C}^n$, $A(x^*)$ has rank at most p, if and only if there is $y^* \in \mathbb{C}^{m(m-p)}$ such that $A(x^*)Y(y^*) = 0$, with rank $Y(y^*) = m-p$. Moreover, one can suppose that one of the maximal minors of $Y(y^*)$ is the identity matrix $\mathbb{I}_{m-p}$ (*cf.* for example [8, Sec. 2]).

For $\iota \subset \{1,\ldots,m\}$ with $\#\iota = m-p$, we denote by Y_ι the maximal minor of $Y(y)$ whose rows are indexed by ι. We deduce that $\mathcal{D}_p$ is the image under the projection $\pi_n\colon \mathbb{C}^n \times \mathbb{C}^{m(m-p)} \to \mathbb{C}^n$ of the algebraic set

$$\mathcal{V}_p = \bigcup_{\substack{\iota \subset \{1,\ldots,m\} \\ \#\iota = m-p}} \mathcal{V}_{p,\iota}$$

where $\mathcal{V}_{p,\iota} = \{(x,y) \in \mathbb{C}^n \times \mathbb{C}^{m(m-p)} : A(x)Y(y) = 0, Y_\iota = \mathbb{I}_{m-p}\}$. We call the sets $\mathcal{V}_{p,\iota}$ *incidence varieties* for $\mathcal{D}_p$. We denote by $f(A,\iota)$ (often simply by f) the polynomial system defining $\mathcal{V}_{p,\iota}$. We prove the following Proposition on the regularity of $\mathcal{V}_{p,\iota}$.

Proposition 1. *Let $\iota \subset \{1,\ldots,m\}$ with $\#\iota = m-p$.*

1. *There is a subsystem $f_{red} \subset f(A,\iota)$ of cardinality $\#f_{red} = m(m-p) + \binom{m-p+1}{2}$ such that $\mathsf{Z}(f_{red}) = \mathsf{Z}(f(A,\iota)) = \mathcal{V}_{p,\iota}$.*

2. *There is a non-empty Zariski open set $\mathscr{A} \subset \mathbb{S}_m^{n+1}(\mathbb{C})$ such that, if $A \in \mathscr{A} \cap \mathbb{S}_m^{n+1}(\mathbb{Q})$, $\mathcal{V}_{p,\iota}$ is either empty or smooth and equidimensional of co-dimension $m(m-p) + \binom{m-p+1}{2}$, and f generates a radical ideal.*

Proof. We start with Point 1. Suppose without loss of generality that $\iota = \{1, \ldots, m-p\}$, and denote by $g_{i,j}$ the $(i,j)-$th entry of the matrix $A(x)Y(y)$ where Y_ι has been substituted by $\mathbb{I}_{m-p}$. The system f_{red} is defined as follows: $f_{red} = (g_{i,j} \text{ for } i \geq j, Y_\iota - \mathbb{I}_{m-p})$. We prove now that $\mathsf{Z}(f_{red}) = \mathsf{Z}(f(A,\iota))$. If $a_{i,j}$ is the $(i,j)-$th entry of A, for $i < j$ one has that $g_{i,j} - g_{j,i} = \sum_{\ell=m-p+1}^{m} a_{i,\ell}y_{\ell,j} - a_{j,\ell}y_{\ell,i}$, since A is symmetric. Using the polynomial relations $g_{k,\ell} = 0$ for $k > m-p$ one can solve for $a_{i,\ell}$ and $a_{j,\ell}$, and deduce

$$\begin{aligned} & g_{i,j} - g_{j,i} \equiv \\ & \equiv \sum_{\ell=m-p+1}^{m} \left(- \sum_{t=m-p+1}^{m} a_{\ell,t}y_{t,i}y_{\ell,j} + \sum_{t=m-p+1}^{m} a_{\ell,t}y_{t,j}y_{\ell,i} \right) \\ & \equiv \sum_{\ell,t=m-p+1}^{m} a_{\ell,t}\left(-y_{t,i}y_{\ell,j} + y_{t,j}y_{\ell,i}\right) \equiv 0 \end{aligned}$$

modulo $\langle g_{k,\ell},\, k > m-p \rangle$. This proves Point 1.

We now give the proof of Point 2. We denote by φ the polynomial map : $\mathbb{C}^{n+m(m-p)} \times \mathbb{S}_m^{n+1}(\mathbb{C}) \to \mathbb{C}^{m(m-p)+\binom{m-p+1}{2}}$ sending (x,y,A) to $f_{red}(x,y,A)$, and let φ_A denote the section map $\varphi_A(x,y) = \varphi(x,y,A)$. Hence $\varphi_A^{-1}(0) = \mathcal{V}_{p,\iota}$. If $\varphi^{-1}(0) = \emptyset$, then for all $A \in \mathbb{S}_m^{n+1}(\mathbb{C})$, $\varphi_A^{-1}(0) = \mathcal{V}_{p,\iota} = \emptyset$, and we conclude defining $\mathscr{A} = \mathbb{S}_m^{n+1}(\mathbb{C})$.

If $\varphi^{-1}(0) \neq \emptyset$, we prove below that 0 is a regular value of φ. We deduce by Thom's Weak Transversality Theorem [30, Sec.4.2] that there exists a non-empty Zariski open set $\mathscr{A}_\iota \subset \mathbb{S}_m^{n+1}(\mathbb{C})$ such that for $A \in \mathscr{A}_\iota$, 0 is a regular value of φ_A. We finally deduce by the Jacobian Criterion [4, Th.16.19] that for $A \in \mathscr{A}_\iota$, $\mathcal{V}_{p,\iota}$ is smooth and equidimensional of co-dimension $m(m-p) + \binom{m-p+1}{2}$, and that the ideal generated by f_{red} is radical. We conclude defining $\mathscr{A} = \cap_\iota \mathscr{A}_\iota$.

Now we only have to prove that 0 is a regular value of φ. Let $D\varphi$ be the Jacobian matrix of φ. We denote by $a_{\ell,i,j}$ the variable representing the $(i,j)-$th entry of A. We consider the derivatives of elements in f_{red} with respect to:

- the variables $\eta = \{a_{0,i,j} : i \leq m-p \text{ or } j \leq m-p\}$;
- the variables $y_{i,j}$ with $i \in \iota$.

Let $(x,y,A) \in \varphi^{-1}(0)$. The submatrix of $D\varphi(x,y,A)$ containing such derivatives, contains the following non-singular blocks: the derivatives of $A(x)Y(y)$ w.r.t. elements in η, that is a unit block $\mathbb{I}_{(m-p)(m+p+1)/2}$; the derivatives of $Y_\iota - \mathbb{I}_{m-p}$, that is a unit block $\mathbb{I}_{(m-r)^2}$. These two blocks are orthogonal, and we deduce that $D\varphi$ is full rank at the point (x,y,A). Since (x,y,A) is arbitrary in $\varphi^{-1}(0)$, we conclude that 0 is a regular value of φ. □

2.2 Critical points

In this section we consider polynomial systems encoding the local minimizers of the linear function $\ell_c(x)\colon \mathbb{R}^n \to \mathbb{R}$ in (1) restricted to the determinantal variety $\mathcal{D}_p \cap \mathbb{R}^n$, with $0 \leq p \leq r$. We denote by L_c the map $L_c\colon \mathbb{R}^{n+m(m-p)} \to \mathbb{R}$ sending (x,y) to $c^T x$, that is $L_c = \ell_c \circ \pi_n$, with $\pi_n\colon \mathbb{R}^{n+m(m-p)} \to \mathbb{R}^n$, $\pi_n(x,y) = x$. With analogy to the description of $\mathcal{D}_p$ via incidence varieties of the previous section, we consider the set $\operatorname{crit}(\ell_c, \mathcal{V}_{p,\iota} \cap \mathbb{R}^{n+m(m-p)})$ of critical points of the restriction of L_c to $\mathcal{V}_{p,\iota} \cap \mathbb{R}^{n+m(m-p)}$.

Lemma 2. *Let $\mathscr{A} \subset \mathbb{S}_m^{n+1}(\mathbb{C})$ be the Zariski open set given in Proposition 1, and let $A \in \mathscr{A}$. The set of local minimizers of ℓ_c on $\mathcal{D}_p \cap \mathbb{R}^n$ is contained in the image of the union of the sets* $\operatorname{crit}(L_c, \mathcal{V}_{p,\iota})$*, for $\iota \subset \{1, \ldots, m\}$, with $\#\iota = m-p$, via the projection map $\pi_n(x, y) = x$.*

Proof. Let $\tilde{x} \in \mathbb{R}^n$ be a local minimizer of ℓ_c on $\mathcal{D}_p \cap \mathbb{R}^n$, and let $\mathcal{C}_{\tilde{x}} \subset \mathcal{D}_p \cap \mathbb{R}^n$ be the connected component containing x. Let $t = \ell_c(\tilde{x})$. Then $\ell_c(x) \geq t$ for all $x \in U \cap \mathcal{C}_{\tilde{x}}$, for some U connected open set. By definition of $\mathcal{V}_p$, and since $\tilde{x} \in \mathcal{D}_p$, there exists $\iota \subset \{1, \ldots, m-p\}$ and $\tilde{y} \in \mathbb{R}^{m(m-p)}$ such that $(\tilde{x}, \tilde{y}) \in \mathcal{V}_{p,\iota}$. Let $\mathcal{C}_{(\tilde{x},\tilde{y})}$ be the connected component of $\mathcal{V}_{p,\iota} \cap \mathbb{R}^{n+m(m-p)}$ containing $(\tilde{x}, \tilde{y})$. We claim (and prove below) that $(\tilde{x}, \tilde{y})$ is a minimizer of L_c on $\pi_n^{-1}(U) \cap \mathcal{C}_{(\tilde{x},\tilde{y})}$, hence local minimizer on $\pi_n^{-1}(U) \cap \mathcal{V}_{p,\iota}$. We deduce that $t = \ell_c(\tilde{x}) = L_c(\tilde{x}, \tilde{y})$ lies in the boundary of $L_c(\pi_n^{-1}(U) \cap \mathcal{C}_{\tilde{x},\tilde{y}})$. In particular, the differential map of L_c at x is not surjective: because $A \in \mathscr{A}$, then $\mathcal{V}_{p,\iota}$ is smooth and equidimensional, and hence $(\tilde{x}, \tilde{y}) \in \operatorname{crit}(L_c, \mathcal{V}_{p,\iota} \cap \mathbb{R}^{m(m-p)})$.

Recall that $L_c(\tilde{x}, \tilde{y}) = \ell_c(\tilde{x}) = t$, and suppose that there is $(x, y) \in \pi_n^{-1}(U) \cap \mathcal{C}_{(\tilde{x},\tilde{y})}$ such that $L_c(x, y) < t$. There exists a continuous semialgebraic map $\tau\colon [0, 1] \to \mathcal{C}_{(\tilde{x},\tilde{y})}$ such that $\tau(0) = (\tilde{x}, \tilde{y})$ and $\tau(1) = (x, y)$. We deduce that $\pi_n \circ \tau$ is also continuous and semialgebraic (since π_n is). Since $\pi_n \circ \tau(0) = \tilde{x}$ and $\pi_n \circ \tau(1) = x$, one gets $x \in U \cap \mathcal{C}_{\tilde{x}}$. Then $\ell_c(x) = L_c(x, y) < t = \ell_c(\tilde{x})$ contradicts the hypothesis that $\tilde{x}$ is a local minimizer of ℓ_c on $\mathcal{C}_{\tilde{x}}$. □

Lemma 2 states that the minimizers of ℓ_c on $\mathcal{D}_p \cap \mathbb{R}^n$ are obtained as the projection on the first n variables of the critical points of L_c over the lifted incidence variety $\mathcal{V}_p \cap \mathbb{R}^{n+m(m-p)}$. We are now going to prove that such critical points are generically finite. Let us suppose that $A \in \mathscr{A}$ (see Proposition 1), and let $c \in \mathbb{Q}^n$. We also fix a subset $\iota \subset \{1, \ldots, m\}$ of cardinality $\#\iota = m - p$.

We have denoted, in Section 2.1, by $f \subset \mathbb{Q}[x, y]$ the polynomial system defining $\mathcal{V}_{p,\iota}$, constituted by the entries of $A(x)Y(y)$ and of $Y_\iota - \mathbb{I}_{m-p}$. By Proposition 1, we deduce that f_{red}, and hence f, generates a radical ideal and defines a smooth equidimensional algebraic set of co-dimension $m(m-p) + \binom{m-p+1}{2}$. The set $\operatorname{crit}(L_c, \mathcal{V}_{p,\iota})$ is hence defined (modulo eliminating the Lagrange multipliers) by the following polynomial system:

$$\operatorname{lag}(\iota): \qquad f = 0; \quad (g, h) = z' \begin{bmatrix} Df \\ DL_c \end{bmatrix} = 0, \tag{3}$$

where $z = (z_1, \ldots, z_{(2m-p)(m-p)}, 1)$ is the vector of Lagrange multipliers: these are the classical first-order optimality conditions. In the previous notation, the vector g (resp. h) is of size n (resp. $m(m-p)$). For the sake of brevity, we say that a point $(x, y, z) \in \mathsf{Z}(\operatorname{lag}(\iota))$ has rank p, if $\operatorname{rank} A(x) = p$.

Our next goal in this section is to prove the following Proposition. It states that if the linear function ℓ_c in Problem (1) is generic, the points $x^* \in \mathcal{D}_p \cap \mathbb{R}^n$, such that $\operatorname{rank} A(x^*) = p$, that correspond to critical points (x^*, y^*) of the restriction of L_c to $\mathcal{V}_p \cap \mathbb{R}^{n+m(m-p)}$, are finitely many.

Proposition 3. *Let $\mathscr{A} \subset \mathbb{S}_m^{n+1}(\mathbb{C})$ be the Zariski open set defined by Proposition 1, and let $A \in \mathscr{A} \cap \mathbb{S}_m^{n+1}(\mathbb{Q})$. There exists a non-empty Zariski open set $\mathscr{C} \subset \mathbb{C}^n$ such that, for $c \in \mathscr{C} \cap \mathbb{Q}^n$, for every $p = 0, \ldots, r$, and for every $\iota \subset \{1, \ldots, m\}$ such that $\#\iota = m - p$, the projection of the solutions of the system $\operatorname{lag}(\iota)$ of rank p over the $x-$space is a finite set.*

In order to prove Proposition 3, we use the local description of determinantal varieties as developed in [12, Sec. 4.1] and in [13, Sec. 5.1]. This is briefly recalled below. Suppose that $x \in \mathcal{D}_p \cap \mathbb{R}^n$, with rank $A(x) = p$, and that the upper-left $p \times p$ submatrix N of $A(x)$ is non-singular (at least one of the $p \times p$ submatrices of $A(x)$ is non-singular). That is

$$A(x) = \begin{bmatrix} N & Q \\ P & R \end{bmatrix} \tag{4}$$

and $\det N \neq 0$. Suppose also w.l.o.g. that $\iota = \{1, \ldots, m-p\}$. By [12, Sec.4.1] or [14, Lemma 13], the local equations of $\mathcal{V}_{p,\iota}$ over x are given by

$$\begin{bmatrix} \mathbb{I}_p & N^{-1}Q \\ 0 & \Sigma(N) \end{bmatrix} Y(y) = 0 \qquad \text{and} \qquad Y_\iota - \mathbb{I}_{m-p} = 0, \tag{5}$$

where $\Sigma(N) = R - PN^{-1}Q$ is the Schur complement of $A(x)$ at N, well defined since N is not singular: these are elements of the local ring $\mathbb{Q}[x,y]_{\det N}$ at $I = \langle \det N \rangle$. Let $Y^{(1)}$ (resp. $Y^{(2)}$) be the matrix obtained by isolating the first p rows (resp. last $m-p$ rows) from $Y(y)$. Let U_ι be such that $U_\iota Y(y) = Y_\iota$, and let $U_\iota = U_\iota^{(1)} | U_\iota^{(2)}$ be the corresponding column subdivision of U_ι. Then (5) imply $\mathbb{I}_{m-p} = U_\iota^{(1)} Y^{(1)} + U_\iota^{(2)} Y^{(2)} = (U_\iota^{(2)} - U_\iota^{(1)} N^{-1} Q) Y^{(2)}$ and hence that both $Y^{(2)}$ and $U_\iota^{(2)} - U_\iota^{(1)} N^{-1} Q$ are invertible (in the local ring $\mathbb{Q}[x]_{\det N}$). We deduce the following equivalent form of the previous equations:

$$\begin{aligned} \tilde{f}: \qquad & Y^{(1)} + N^{-1}QY^{(2)} = 0, \quad \Sigma(N) = 0, \\ & Y^{(2)} - (U_\iota^{(2)} - U_\iota^{(1)} N^{-1} Q)^{-1} = 0, \end{aligned} \tag{6}$$

denoted by $\tilde{f}$. Up to reordering its entries, the Jacobian matrix of $\tilde{f}$ is

$$D\tilde{f} = \begin{bmatrix} D_x[\Sigma(N)]_{i,j} & 0_{(m-p)^2 \times m(m-p)} \\ \star & \mathbb{I}_{p(m-p)} \quad \star \\ & 0 \quad \mathbb{I}_{(m-p)^2} \end{bmatrix}.$$

If $A \in \mathscr{A}$, by Proposition 1 the rank of $D\tilde{f}$ equals $\#f_{red} = m(m-r) + \binom{m-r+1}{2}$ at every $x \in \mathsf{Z}(\tilde{f})$. Similarly, we localize the Lagrange system $\mathrm{lag}(\iota)$ (*cf.* (3)) by defining:

$$(\tilde{g}, \tilde{h}) = z' \begin{bmatrix} D\tilde{f} \\ DL_c \end{bmatrix}.$$

By the structure of $D\tilde{f}$, one gets $\tilde{h}_i = z_{(m-p)^2+i}$, for $i = 1, \ldots, m(m-p)$, and hence one can substitute $z_{(m-p)^2+i} = 0, i = 1, \ldots, m(m-p)$, in $(\tilde{f}, \tilde{g})$.

of Proposition 3. Let $d = m(m-p) + \binom{m-p+1}{2}$ and $e = \binom{m-p}{2}$ so that $d + e = (2m-p)(m-p) = \#z$. First, we claim that there exists a non-empty Zariski open set $\mathscr{C}_N \subset \mathbb{C}^n$ such that if $c \in \mathscr{C}_N \cap \mathbb{Q}^n$ the Jacobian matrix of the local system $(\tilde{f}, \tilde{g}, \tilde{h})$ has maximal possible rank. Here N refers to the upper left $p \times p$ submatrix of A as above. We conclude by defining $\mathscr{C} = \cap_N \mathscr{C}_N$ (where N runs over the family of $p \times p$ submatrices of A), which is non-empty and Zariski open.

The proof is similar to that of Point 2 of Proposition 1 and hence we only sketch it. Let

$$\begin{array}{rccc} \varphi: & \mathbb{C}^{n+d+e+m(m-p)} \times \mathbb{C}^n & \longrightarrow & \mathbb{C}^{n+d+e+m(m-p)} \\ & (x, y, z, c) & \longmapsto & (\tilde{f}, \tilde{g}, \tilde{h})(x, y, z, c). \end{array}$$

Then the Jacobian matrix of $(\tilde{f}, \tilde{g}, \tilde{h})$ is $D\varphi$ as a polynomial map. We prove that 0 is a regular value of φ, and apply Thom's Weak Transversality Theorem [30, Sec.4.2] as in the proof of Proposition 1. Let $(x, y, z, c) \in \varphi^{-1}(0)$ (if it does not exist, define $\mathscr{C}_N = \mathbb{C}^n$). Since polynomials in $\tilde{f}$ only depend on x and y, then $D\tilde{f}$ is a submatrix of $D\varphi$ and the columns corresponding to the derivatives with respect to z of $\tilde{f}$ are zero. Hence the rank of $D\varphi$ is at most $n + d + m(m-r)$ since $D\tilde{f}$ has e rank defects by Proposition 1 (recall that $A \in \mathscr{A}$). A $(n + d + m(m-p)) \times (n + d + m(m-p))$ full-rank submatrix of $D\varphi$ at (x, y, z, c) is given by: the derivatives with respect to: (1) x, y, (2) $c_1, \ldots, c_n$, and (3) $z_{(m-p)^2+i}, i = 1, \ldots, m(m-p)$.

Now, we can conclude the proof. Let $c \in \mathscr{C} = \cap_N \mathscr{C}_N$ (previously defined). From the previous claim, we deduce that the locally closed set $\mathcal{E} = \mathsf{Z}(\mathrm{lag}(\iota)) \cap \{(x, y, z) : \text{rank } A(x) = p\}$ is empty or equidimensional of dimension e. Let

$$\begin{array}{rccc} \pi: & \mathbb{C}^{n+m(m-p)+d+e} & \longrightarrow & \mathbb{C}^n \\ & (x, y, z) & \longmapsto & x \end{array}$$

be the projection over the $x-$space, and $x^* \in \pi(\mathcal{E})$. In particular rank $A(x^*) = p$, and there is a unique $y^* \in \mathbb{C}^{m(m-p)}$ such that $f(x^*, y^*) = 0$. We deduce that $\pi^{-1}(x^*)$ is isomorphic to the linear space defined by

$$\Big\{(z_1, \ldots, z_{d+e}) : (z_1, \ldots, z_{d+e})Df = (c', 0)\Big\}.$$

Since the rank of Df is d, $\pi^{-1}(x^*)$ is a linear space of dimension e, and by the Theorem on the Dimension of Fibers [31, Sect. 6.3, Theorem 7] $\pi_x(\mathcal{E})$ has dimension 0. □

3 From semi-algebraic to algebraic optimization

In order to prove that our algorithm is correct, we present in this section the main geometric result of this work. By the independent interest of the results of this section, we need to introduce, first, some notation.

Given $c \in \mathbb{Q}^n$ and $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$, for $0 \leq r \leq m$, we have denoted by $\mathcal{F}_r(A, c)$ the (possibly empty or infinite) set of minimizers of ℓ_c on $\mathscr{S} \cap \mathcal{D}_r$. By simplicity, we also call $\mathcal{F}_r(A, c)$ the set of minimizers of $(\mathrm{SDP})_r$. When $r = m$, $\mathcal{F}_m(A, c)$ is the convex optimal face of the spectrahedron $\mathscr{S}$ in direction c. Indeed, since every face of a spectrahedron is exposed, it is exactly defined as the set of minimizers of some semidefinite program $(\mathrm{SDP})_m$. We denote by

$$\mathcal{R}_r(A, c) = \left\{p : 0 \leq p \leq r, \exists\, x \in \mathcal{F}_r(A, c), \text{ rank } A(x) = p\right\}$$

the rank profile of $\mathcal{F}_r(A, c)$. Clearly, $\mathcal{F}_r(A, c) \neq \emptyset$ if and only if $\mathcal{R}_r(A, c) \neq \emptyset$. This is our main theorem in this section.

Theorem 4. *Suppose that $\mathcal{F}_r(A, c) \neq \emptyset$, and let $p \in \mathcal{R}_r(A, c)$. For $x^* \in \mathcal{F}_r(A, c)$ such that* rank $A(x^*) = p$, *then x^* is a local minimizer of ℓ_c on $\mathcal{D}_p \cap \mathbb{R}^n$.*

Proof. Suppose that x^* is as in the hypothesis. We denote by $\mathcal{C}^* \subset \mathcal{D}_p \cap \mathbb{R}^n$ the connected component of $\mathcal{D}_p \cap \mathbb{R}^n$ containing x^*. Hence there are three possible (non mutually exclusive) cases, that we analyze below. Recall that $p \leq r$, hence $\mathcal{D}_p \subset \mathcal{D}_r$.

First case: $\mathcal{C}^* \subset \mathscr{S}$. Hence $\mathcal{C}^* \subset \mathscr{S} \cap \mathcal{D}_p \subset \mathscr{S} \cap \mathcal{D}_r$. Since $\mathscr{S} \cap \mathcal{D}_r$ is the feasible set of $(\text{SDP})_r$ and x^* is a minimizer of $(\text{SDP})_r$, hence x^* is a minimizer of ℓ_c on $\mathcal{C}^*$. Hence it is a local minimizer of ℓ_c on $\mathcal{D}_p \cap \mathbb{R}^n$, as claimed.

Second case: There exists an open set $U \subset \mathbb{R}^n$ such that $x^* \in U$ and $U \cap (\mathcal{D}_{m-1} \setminus \mathscr{S}) = \emptyset$. This means that U intersects $\mathcal{D}_{m-1} \cap \mathbb{R}^n$ only at positive semidefinite matrices, and $U \cap \mathscr{S}$ is an open subset of $\mathscr{S}$ containing x^*. We deduce that x^* is a minimizer of ℓ_c on $U \cap \mathcal{D}_p \subset U \cap \mathscr{S}$, hence a local minimizer of ℓ_c on $\mathcal{D}_p \cap \mathbb{R}^n$.

Third case: $\mathcal{C}^* \not\subset \mathscr{S}$, and for all $U \subset \mathbb{R}^n$ open set, such that $x^* \in U$, then $U \cap (\mathcal{D}_{m-1} \setminus \mathscr{S}) \neq \emptyset$. We prove below that such a situation cannot occur. Indeed, one first deduces that, for all U as above, $U \cap (\mathcal{D}_p \setminus \mathscr{S}) \neq \emptyset$ since $\mathcal{C}^* \not\subset \mathscr{S}$. For a positive integer $d \in \mathbb{N}$, we denote by $B(x^*, 1/d)$ the open ball with center x^* and radius $1/d$, that is $B(x^*, 1/d) = \{x \in \mathbb{R}^n : \|x - x^*\| < 1/d\}$, where $\|x\|$ is the Euclidean norm of x. By hypothesis, for all $d \in \mathbb{N}$ there exists $x(d) \in B(x^*, 1/d) \cap \mathcal{D}_p$ such that $A(x(d)) \not\succeq 0$. Hence $x(d) \to x^*$ when $d \to \infty$. Denoting by $e_1(x) \leq e_2(x) \leq \cdots \leq e_m(x)$ the ordered eigenvalues of $A(x)$, one deduces that, for all $d \in \mathbb{N}$, $e_1(x(d)) < 0$ and hence $e_{m-p+1}(x(d)) \leq 0$ (since the matrix $A(x(d))$ has at least $m - p$ null eigenvalues). In particular $e_{m-p+1}(x(d)) \to e_{m-p+1}(x^*) \leq 0$ when $d \to \infty$. Since $x^* \in \mathscr{S}$, then $e_1(x^*) = \cdots = e_{m-p}(x^*) = e_{m-p+1}(x^*) = 0$, and the rank of $A(x^*)$ is at most $p - 1$, which contradicts the hypotheses. □

We prove two corollaries of Theorem 4 and of previous results, which are worth to be made explicit and highlighted.

Corollary 5. *Let $x^* \in \mathcal{F}_r(A, c)$ satisfy the following property: for all Euclidean open sets $U \subset \mathbb{R}^n$ containing x^*, U contains a singular matrix with a negative eigenvalue. Then, if $p = \text{rank } A(x^*)$, the connected component $\mathcal{C}^* \subset \mathcal{D}_p \cap \mathbb{R}^n$ containing x^* is contained in $\mathscr{S}$.*

Proof. We apply *mutatis mutandis* the argument of the Third case in the proof of Theorem 4, without the hypothesis that $\mathcal{C}^* \not\subset \mathscr{S}$. Hence we conclude that necessarily $\mathcal{C}^* \subset \mathscr{S}$. □

The second corollary gives a finiteness theorem for the set of solutions of a generic rank constrained semidefinite program (1).

Corollary 6. *Let $\mathscr{A} \subset \mathbb{S}_m^{n+1}(\mathbb{C})$ and $\mathscr{C} \subset \mathbb{C}^n$ be the Zariski open sets defined respectively in Proposition 1 and 3. If $A \in \mathscr{A} \cap \mathbb{S}_m^{n+1}(\mathbb{Q})$ and $c \in \mathscr{C} \cap \mathbb{Q}^n$, the set $\mathcal{F}_r(A, c)$ of minimizers of the rank-constrained semidefinite program $(SDP)_r$ is finite.*

Proof. Remark that $\mathcal{F}_r(A, c)$ is the union of sets $B_p \subset \mathcal{F}_r(A, c)$, for $p \in \mathcal{R}_r(A, c)$, corresponding to minimizers of rank p, that is $\mathcal{F}_r(A, c) = \cup_{p \in \mathcal{R}_r(A,c)} B_p$. We prove that B_p is finite for all $p \in \mathcal{R}_r(A, c)$.

Let $x^* \in B_p$. By Theorem 4, x^* is a local minimizer of ℓ_c on $\mathcal{D}_p \cap \mathbb{R}^n$. Since $A \in \mathscr{A}$, by Lemma 2 B_p is included in the union of the projections of the sets of critical points of L_c on $\mathcal{V}_{p,\iota}$, for $\iota \subset \{1, \ldots, m\}, \#\iota = m - p$. Since $c \in \mathscr{C}$, and since rank $A(x^*) = p$, by Proposition 3 B_p is the projection of a finite set, hence finite. □

4 The algorithm

The main algorithm described in this work is called SolveSDP.

4.1 Description

We first describe the main subroutines of SolveSDP.

CheckReg. With input $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$ and $p \leq r$, it returns `true` if for all $\iota \subset \{1,\dots,m\}$, with $\#\iota = m-p$, the set $\mathcal{V}_{p,\iota}$ is smooth and equidimensional; otherwise, it returns `false`.

Optimize. With input A, c and p, it returns the vector of ideals $(\mathrm{lag}(\iota_1),\dots,\mathrm{lag}(\iota_{\binom{m}{p}})) \subset \mathbb{Q}[x,y,z]$, where $\iota_j \subset \{1,\dots,m\}$, with $\#\iota_j = m-p$, $j = 1,\dots,\binom{m}{p}$. The set $\cup_j \mathsf{Z}(\mathrm{lag}(\iota_j))$ encodes the union of the critical points of L_c restricted to the components $\mathcal{V}_{p,\iota}$ of $\mathcal{V}_p$.

Project. With input the output of Optimize, it substitutes each ideal $\mathrm{lag}(\iota_j)$ with the elimination ideal $I_{\iota_j} = \mathrm{lag}(\iota_j) \cap \mathbb{Q}[x]$, for $j = 1,\dots,\binom{m}{p}$, returning $I = (I_{\iota_j}, i = 1,\dots,\binom{m}{p})$.

We recall the definition of rational parametrization of a finite set $S \subset \mathbb{R}^n$: this is given by a vector $Q = (q, q_0, q_1, \dots, q_n) \subset \mathbb{Q}[t]$ such that S admits a representation (2). We need to define two routines performing operations on rational parametrizations of finite sets.

RatPar. Given a zero-dimensional ideal $I_{\iota_j} \subset \mathbb{Q}[x]$, it returns a rational parametrization $Q = (q, q_0, q_1, \dots, q_n) \subset \mathbb{Q}[t]$ of I_{ι_j}. If I_{ι_j} is not zero-dimensional, it returns an error message.

Union. Given rational parametrizations $Q_1, Q_2 \subset \mathbb{Q}[t]$ encoding two finite sets $V_1, V_2 \subset \mathbb{C}^n$, it returns a rational parametrization $Q \subset \mathbb{Q}[t]$ encoding $V_1 \cup V_2$.

The following is the formal procedure of SolveSDP. We offer below a more explicit description of the algorithm for the sake of clarity.

Algorithm 1 SolveSDP

```
1: procedure SolveSDP(A, c, r)
2:     Q ← [ ]
3:     for p = 0, ..., r do
4:         if CheckReg(A, p) =false then return error
5:         I ← Project(Optimize(A, c, p))
6:         for j = 1, ..., (m choose p) do
7:             Q_{ι_j} ← RatPar(I_{ι_j})
8:             Q ← Union(Q, Q_{ι_j})
9:     return Q
```

The input is a triple (A, c, r), where $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$ is $(n+1)-$tuple of symmetric matrices with rational coefficients, $c \in \mathbb{Q}^n$ defines the linear function ℓ_c in (1) and r is the maximum admissible rank. For every value of p from 0 to r, the algorithm checks whether the regularity assumption on the incidence varieties $\mathcal{V}_{p,\iota}, \iota \subset \{1,\dots,m\}$, for $\#\iota = m-p$, holds. If this is the case, it computes rational parametrizations Q_ι of the Lagrange systems encoding the critical points of the map L_c, on the components $\mathcal{V}_{p,\iota}$ of the incidence variety $\mathcal{V}_p$. The output is a rational parametrization Q encoding the union of the finite sets defined by the Q'_ιs.

4.2 Correctness

We prove in this section that SolveSDP is correct. Our proof relies on intermediate results already stated and proved in the previous sections.

Theorem 7. *Let $\mathscr{A} \subset \mathbb{S}_m^{n+1}(\mathbb{C})$ and $\mathscr{C} \subset \mathbb{C}^n$ be the Zariski open sets defined respectively by Proposition 1 and 3. Let $A \in \mathscr{A} \cap \mathbb{S}_m^{n+1}(\mathbb{Q})$, $c \in \mathscr{C} \cap \mathbb{Q}^n$ and $0 \leq r \leq m$. Then the output of* SolveSDP *is a rational parametrization of a finite set containing all minimizers of $(SDP)_r$.*

Proof. Let (A, c, r) be the input of SolveSDP, and let $x^* \in \mathbb{R}^n$ be a solution of $(\mathrm{SDP})_r$. Let $p = \operatorname{rank} A(x^*)$. By Theorem 4, x^* is a local minimizer of ℓ_c on $\mathcal{D}_p \cap \mathbb{R}^n$. Let us denote by S the image of the union of sets $\operatorname{crit}(L_c, \mathcal{V}_{p,\iota}), \iota \subset \{1, \ldots, m\}, \#\iota = m - p$ under the projection $\pi_n(x, y) = x$, namely

$$S = \pi_n \left(\bigcup_{\#\iota = m-p} \operatorname{crit}(L_c, \mathcal{V}_{p,\iota}) \right).$$

Lemma 2 implies that $x^* \in S$. Since $A \in \mathscr{A}$, by Proposition 1 $\mathcal{V}_{p,\iota}$ is smooth and equidimensional of dimension $m(m-p) + \binom{m-p+1}{2}$. Hence, for all $\iota \subset \{1, \ldots, m\}$, with $\#\iota = m-p$, the set $\operatorname{crit}(L_c, \mathcal{V}_{p,\iota} \cap \mathbb{R}^{n+m(m-p)})$ is defined by the Lagrange system $\operatorname{lag}(\iota)$ introduced in (3). We conclude that there exists ι as above, and $y^* \in \mathbb{C}^{n+m(m-p)}$ and $z^* \in \mathbb{C}^{(2m-p)(m-p)+1}$ such that (x^*, y^*, z^*) is a solution of $\operatorname{lag}(\iota)$ of rank p (indeed, by hypothesis $\operatorname{rank} A(x^*) = p$). By Proposition 3, the solutions of rank p of $\operatorname{lag}(\iota)$ are finitely many.

Hence, respectively, the subroutines Optimize, Project and RatPar compute a rational parametrization $Q_\iota = (q^{(\iota)}, q_0^{(\iota)}, \ldots, q_n^{(\iota)}) \subset \mathbb{Q}[t]$ such that there exists $t^* \in \mathbb{R}$ such that

$$x^* = (q_1^{(\iota)}(t^*)/q_0^{(\iota)}(t^*), \ldots, q_n^{(\iota)}(t^*)/q_0^{(\iota)}(t^*)).$$

Then the output Q is a rational parametrization containing x^*. By the genericity of x^* among the solutions of $(\mathrm{SDP})_r$, we conclude. □

5 Complexity analysis

5.1 Degree bounds for the output representation

The output of SolveSDP is a rational univariate parametrization $Q = (q, q_0, q_1, \ldots, q_n) \subset \mathbb{Q}[t]$. To recover the coordinates of the minimizers of Problem (1), one can perform real root isolation on the univariate polynomial q. Hence we are interested in bounding the degree of q, which is done by the following Proposition.

Proposition 8. *Let $Q = (q, q_0, q_1, \ldots, q_n) \subset \mathbb{Q}[t]$ be the rational parametrization returned by* SolveSDP. *Then*

$$\deg q \leq \sum_{p=0}^{r} \binom{m}{p} \theta(m, n, p),$$

where

$$\theta(m, n, p) = \sum_k \binom{c_p}{n-k} \binom{n-1}{k + c_p - 1 - p(m-p)} \binom{p(m-p)}{k},$$

with $c_p = (m-p)(m+p+1)/2$.

Proof. We first prove that θ gives a bound on the degree of the ideal generated by $\mathrm{lag}(\iota)$, that is on the degree of the partial rational parametrization Q_ι. Since Q encodes the union of all algebraic sets defined by the Q'_ιs, and since the previous degree does not depend on ι, we conclude by adding all such bounds (each one multiplied by $\binom{m}{p}$, the number of subset ι of cardinality $m-p$). This relies on an equivalent construction of $\mathrm{lag}(\iota)$ which is given below.

Given $p \in \{0,\ldots,r\}$, we fix a subset $\iota \subset \{1,\ldots,m\}$ with $\#\iota = m-p$. We exploit the multilinearity of the polynomial system f defining the incidence variety $\mathcal{V}_{p,\iota}$. First, we eliminate variables $y_{i,j}$, with $i \in \iota$, by substituting $Y_\iota = \mathbb{I}_{m-p}$; we also eliminate polynomials $Y_\iota - \mathbb{I}_{m-p}$ in f_{red} (*cf.* Proposition 1). One obtains a polynomial system $\widetilde{f}$ of cardinality $c_p := (m-p)(m+p+1)/2$. Moreover, by construction, $\widetilde{f}$ is constituted by c_p polynomials of bi-degree at most $(1,1)$ with respect to the groups of variables x and

$$\overline{y} := (y_{i,j} : i \notin \iota). \tag{7}$$

We also suppose without loss of generality that the linear map ℓ_c in Problem (1) defines the projection over x_1, that is that $c = (1,0,\ldots,0)$. Hence, the system $\mathrm{lag}(\iota)$ is equivalent to the following. We consider the c_p elements in $\widetilde{f}$. Let $D\widetilde{f}$ be the Jacobian matrix of $\widetilde{f}$ w.r.t. variables $x, \overline{y}$, and let D_1 be the matrix obtained by eliminating the first column from $D\widetilde{f}$. The critical points of the projection over x_1 restricted to $\mathsf{Z}(\widetilde{f})$ are then defined by $\widetilde{f} = 0$ and by $z' D_1 = 0$, where

$$\overline{z} := (z_1,\ldots,z_{c_p-1},1) \tag{8}$$

is a non-zero vector of $c_p - 1$ Lagrange multipliers.

Hence $\mathrm{lag}(\iota)$ is equivalent to a polynomial system of

- c_p equations of bi-degree at most $(1,1,0)$ w.r.t. $x, \overline{y}, \overline{z}$;
- $n-1$ equations of bi-degree at most $(0,1,1)$ w.r.t. $x, \overline{y}, \overline{z}$;
- $p(m-p)$ equations of bi-degree at most $(1,0,1)$ w.r.t. $x, \overline{y}, \overline{z}$.

We call this new polynomial system $\widetilde{\mathrm{lag}(\iota)}$. By the Multilinear Bézout Theorem (*cf.* for example [30, Prop. 11.1.1]) the degree of $\widetilde{\mathrm{lag}(\iota)}$ is bounded above by the coefficient of $s_x^n s_y^{p(m-p)} s_z^{c_p-1}$ in

$$(s_x+s_y)^{c_p}(s_y+s_z)^{n-1}(s_x+s_z)^{p(m-p)},$$

which is exactly $\theta(m,n,p)$. □

5.2 Bounds on the arithmetic operations

Our goal in this section is to bound the number of arithmetic operations over $\mathbb{Q}$ performed by the main subroutine of SolveSDP, which is the computation of the rational parametrization Q_ι done by RatPar. Before that, we give bounds for the complexity of routines Project and Union. Let $\widetilde{\mathrm{lag}(\iota)} \subset \mathbb{Q}[x,\overline{y},\overline{z}]$ (*cf.* (7) and (8)) be the equivalent Lagrange system built in the proof of Proposition 8, and $\theta = \theta(m,n,p)$ be the bound on the degree of $\widetilde{\mathrm{lag}(\iota)}$. From [30, Chapter 10], one gets the following estimates:

- by [30, Lemma 10.1.5], Project can be performed with at most $n^2\theta(m,n,p)^2$ arithmetic operations;
- by [30, Lemma 10.1.3], Union can be performed with at most $n(\sum_{s=0}^{p}\binom{m}{s}\theta(m,n,s))^2$ arithmetic operations.

We now turn to the complexity of RatPar. Our complexity model is the symbolic homotopy algorithm for computing rational parametrization in [17]. This is a probabilistic exact algorithm for solving zero-dimensional systems via rational parametrizations, exploiting their sparsity. It allows to express the arithmetic complexity of RatPar as a function of geometric invariants of the system $\widetilde{\mathrm{lag}(\iota)}$ (mainly of its degree, which is bounded by $\theta(m,n,p)$, *cf.* Proposition 8).

We briefly recall the construction of the homotopy curve in [17]. This is similar to [13, Sec.4]. Let t be a new variable, and recall that $\widetilde{\mathrm{lag}(\iota)}$ contains quadratic polynomials with bilinear structure with respect to the three groups of variables $x, \overline{y}, \overline{z}$. Let $g \subset \mathbb{Q}[x,\overline{y},\overline{z}]$ be a new polynomial system such that: (1) $\#g = \#\widetilde{\mathrm{lag}(\iota)}$, (2) the $i-$th entry of g is a polynomial with the same monomial structure as the $i-$th entry of $\widetilde{\mathrm{lag}(\iota)}$, and (3) the solutions of g are finitely many and known. Since $\widetilde{\mathrm{lag}(\iota)}$ is bilinear in $x, \overline{y}, \overline{z}$, the system g can be obtained by considering suitable products of linear forms in, respectively, x, $\overline{y}$ and $\overline{z}$. The algorithm in [17] builds the homotopy curve $\mathsf{Z}(h)$ defined by

$$h = t\widetilde{\mathrm{lag}(\iota)} + (1-t)g \subset \mathbb{Q}[x,\overline{y},\overline{z},t].$$

In the following lemma we give a bound on the degree of the homotopy curve.

Lemma 9. *Let $\theta(m,n,p)$ be the bound on the degree of $\mathsf{Z}(\widetilde{lag(\iota)})$ computed in Proposition 8. The degree of the homotopy curve $\mathsf{Z}(h)$ is in*

$$\mathcal{O}((n + c_p + p(m-p))\min\{n, c_p\}\theta(m,n,p)).$$

Proof. The homotopy system

$$h = t\widetilde{\mathrm{lag}(\iota)} + (1-t)g$$

is bilinear in the four groups of variables $x, \overline{y}, \overline{z}, t$. Here $\#x = n, \#\overline{y} = p(m-p), \#\overline{z} = c_p - 1$, with $c_p = (m-p)(m+p+1)/2$, and $\#t = 1$. By the Multilinear Bézout Theorem (*cf.* [30, Ch. 11]), a bound for D is the sum of the coefficients of

$$q = (s_x + s_y + s_t)^{c_p}(s_y + s_z + s_t)^{n-1}(s_x + s_z + s_t)^{p(m-p)}$$

modulo $I = \langle s_x^{n+1}, s_y^{p(m-p)+1}, s_z^{c_p}, s_t^2\rangle \subset \mathbb{Z}[s_x, s_y, s_z, s_t]$. Let $q_1, q_2, q_3, q_4 \in \mathbb{Z}[s_x, s_y, s_z]$ be such that $q = q_1 + s_t(q_2 + q_3 + q_4) + u$, with s_t^2 that divides u. One gets

$$\begin{aligned}
q_1 &= (s_x + s_y)^{c_p}(s_y + s_z)^{n-1}(s_x + s_z)^{p(m-p)}\\
q_2 &= c_p(s_x + s_y)^{c_p-1}(s_y + s_z)^{n-1}(s_x + s_z)^{p(m-p)}\\
q_3 &= (n-1)(s_x + s_y)^{c_p}(s_y + s_z)^{n-2}(s_x + s_z)^{p(m-p)}\\
q_4 &= p(m-p)(s_x + s_y)^{c_p}(s_y + s_z)^{n-1}(s_x + s_z)^{p(m-p)-1}.
\end{aligned}$$

Hence $q \equiv q_1 + s_t(q_2 + q_3 + q_4) \mod I$. We compute the sum of the coefficients of $q_1, s_t q_2, s_t q_3$ and $s_t q_4$ and we conclude. The contribution of q_1 has been computed in Proposition 8, and equals $\theta(m, n, p)$.

We consider the contribution of $s_t q_2$. Let $q_2 = p_r \tilde{q}_2$. We compute the sum of the coefficients of $\tilde{q}_2$ modulo $\langle s_x^{n+1}, s_y^{p(m-p)+1}, s_z^{c_p} \rangle$. Remark that $\deg \tilde{q}_2 = n - 2 + c_p + p(m-p)$, and that the maximal powers admissible modulo I' are $s_x^n, s_y^{p(m-p)}, s_z^{c_p-1}$. Hence the contribution of $\tilde{q}_2$ is given by the sum of:

[(A)] the coefficient of $s_x^{n-1} s_y^{p(m-p)} s_z^{c_p-1}$ in $\tilde{q}_2$, that is

$$\Sigma_A = \sum_{k \in \mathcal{G}_A} \binom{c_p - 1}{n - 1 - k} \binom{n-1}{k - 1 + c_p - p(m-p)} \binom{p(m-p)}{k}$$

where $\mathcal{G}_A$ equals

$$\{\max\{0, n - c_p\} \leq k \leq \min\{n - c_p + p(m-p), p(m-p)\}\};$$

[(B)] the coefficient of $s_x^n s_y^{p(m-p)-1} s_z^{c_p-1}$ in $\tilde{q}_2$, that is

$$\Sigma_B = \sum_{k \in \mathcal{G}_B} \binom{c_p - 1}{n - k} \binom{n-1}{k - 1 + c_p - p(m-p)} \binom{p(m-p)}{k}$$

where $\mathcal{G}_B$ equals

$$\{\max\{0, n - c_p + 1\} \leq k \leq \min\{n - c_p + p(m-p), p(m-p)\}\};$$

[(C)] the coefficient of $s_x^n s_y^{p(m-p)} s_z^{c_p-2}$ in $\tilde{q}_2$, that is

$$\Sigma_C = \sum_{k \in \mathcal{G}_C} \binom{c_p - 1}{n - k} \binom{n-1}{k - 2 + c_p - p(m-p)} \binom{p(m-p)}{k}$$

where $\mathcal{G}_C$ equals

$$\{\max\{0, n - c_p + 1\} \leq k \leq \min\{n - c_p + p(m-p) + 1, p(m-p)\}\}.$$

Below, we bound the expression $c_p(\Sigma_A + \Sigma_B + \Sigma_C)$ and we conclude. By direct computation one easily checks that $\Sigma_A \leq \theta(m, n, p)$ and $\Sigma_B \leq \theta(m, n, p)$. The same does not hold for Σ_C; however, we claim that $\Sigma_C \leq (1 + \min\{n, c_p\})\, \theta(m, n, p)$ and that the contribution of q_2 is $c_p(\Sigma_A + \Sigma_B + \Sigma_C) \in O\left(c_p \min\{n, c_p\}\, \theta(m, n, p)\right)$.

We prove our claim. Let us define

$$\begin{aligned}
\chi_1 &= \max\{0, n - c_p\} \\
\chi_2 &= \min\{n - c_p + p(m-p), p(m-p)\} \\
\alpha_1 &= \max\{0, n - c_p + 1\} \\
\alpha_2 &= \min\{n - c_p + p(m-p) + 1, p(m-p)\}.
\end{aligned}$$

Remark that $\chi_1 \leq \alpha_1$ and $\chi_2 \leq \alpha_2$, and that $\theta(m, n, p)$ sums over $\chi_1 \leq k \leq \chi_2$ and Σ_C over $\alpha_1 \leq k \leq \alpha_2$.

Denote by $\varphi(k)$ the $k-$th summand of Σ_C, and by $\gamma(k)$ the $k-$th summand of $\theta(m,n,p)$. Then for all $\alpha_1 \leq k \leq \chi_2$, one gets that

$$\varphi(k) = \Psi(k)\,\gamma(k) \qquad \text{with } \Psi(k) = \frac{k-1+c_p-p(m-p)}{n-k-c_p+p(m-p)-1}.$$

When k runs in $[\alpha_1, \chi_2] \cap \mathbb{Z}$, the function $\Psi(k)$ is non-decresing monotone, and its maximum is attained in $\Psi(\chi_2)$ and is bounded by $\min\{n, c_p\}$. By that we deduce the claimed inequality $\Sigma_C \leq (1+\min\{n,c_p\})\,\theta(m,n,p)$ since if $\chi_2 < \alpha_2$ then $\chi_2 = \alpha_2 - 1$ and $\varphi(\alpha_2)$ is bounded above by $\theta(m,n,p)$.

One can use the same techniques as above to deduce that, as for q_2:

- the contribution of q_3 is in $\mathcal{O}\left(n\,\min\{n,c_p\}\,\theta(m,n,p)\right)$;
- the contribution of q_4 is in $\mathcal{O}\left(p(m-p)\,\min\{n,c_p\}\theta(m,n,p)\right)$.

□

The degree of $\mathsf{Z}(\widetilde{\mathrm{lag}(\iota)})$ and of the homotopy curve $\mathsf{Z}(h)$ are the main ingredients of the complexity bound for the algorithm [17], which is given by [17, Prop. 6.1]. We use this complexity bound in our estimate. Indeed, let us denote by

$$\begin{aligned}
\Delta_{xy} &= \{1, x_i, y_j, x_i y_j : i = 1,\ldots,n, j = 1,\ldots,p(m-p)\}\\
\Delta_{yz} &= \{1, y_j, z_k, y_j z_k : j = 1,\ldots,p(m-p), k = 1\ldots, c_p - 1\}\\
\Delta_{xz} &= \{1, x_i, z_k, x_i z_k : i = 1,\ldots,n, k = 1,\ldots,c_p - 1\}
\end{aligned}$$

the supports of polynomials in $\widetilde{\mathrm{lag}(\iota)}$. To state our complexity result for SolveSDP, we suppose that all the regularity assumptions on $A(x)$ are satisfied. We avoid in particular to consider the control subroutine CheckReg in our complexity analysis.

Theorem 10. *Suppose that $A \in \mathscr{A}$ (defined in Proposition 1). Then* SolveSDP *runs within*

$$\mathcal{O}\left(\sum_{p=0}^{r}\binom{m}{p}(npc_p(m-p))^5\theta(m,n,p)^2\right)$$

arithmetic operations over $\mathbb{Q}$, where $c_p = (m-p)(m+p+1)/2$.

Proof. Complexity bounds for subroutines Project and Union have been computed earlier in Section 5.2.

By [17, Prop.6.1], one can compute a rational parametrization of $\widetilde{\mathrm{lag}(\iota)}$ within $\mathcal{O}((\tilde{n}^2 N \log\Delta + \tilde{n}^{\omega+1})ee')$ where: $\tilde{n} = n + p(m-p) + c_p - 1$ is the number of variables in $\widetilde{\mathrm{lag}(\iota)}$; $N = c_p\#\Delta_{xy} + (n-1)\#\Delta_{yz} + p(m-p)\#\Delta_{xz} \in \mathcal{O}(npc_p(m-p))$; $\Delta = \max\{\|q\| : q \in \Delta_{xy}\cup\Delta_{yz}\cup\Delta_{xz}\} \leq \tilde{n}$; finally e is the degree of $\mathsf{Z}(\widetilde{\mathrm{lag}(\iota)})$ and e' the degree of $\mathsf{Z}(h)$, and ω is the exponent of matrix multiplication.

Applying bounds computed in Proposition 8 and Lemma 9, and since $\tilde{n} \leq N$ and $\omega \leq 3$, we conclude that RatPar runs within $\mathcal{O}(N^5\theta(m,n,p)^2)$ arithmetic operations. We conclude by recalling that for every $p = 0,\ldots,r$, the routine RatPar runs $\binom{m}{p}$ times. □

6 Experiments

We present results of our tests on a Maple implementation of the algorithm SolveSDP. We integrate this implementation in the Maple library SPECTRA [16] since the main goal of this library is to contain symbolic algorithms for semidefinite programming and related problems. A beta version of SPECTRA can be freely downloaded from the following web page:

`http://homepages.laas.fr/snaldi/software.html`

The rational parametrizations are computed using Gröbner bases via the Maple implementation of Faugère's software FGb [5], exploiting the multilinearity of Lagrange systems already exhibited in Section 5.1 (*cf.* [6] for a tailored algorithm). The regularity assumptions on the input (A, c) are also checked by testing the emptiness of complex algebraic sets, hence performing Gröbner bases computations.

In Section 6.1 we use SolveSDP to solve generic rank-constrained semidefinite programs, giving details of timings and output degrees of our implementations. In Section 6.2 we consider an application of our results for computing certificates of nonnegativity for univariate polynomials.

6.1 Random SDP

In this test, we draw $(n+1)-$tuples of random $m \times m$ symmetric linear matrices $A_0, A_1, \ldots, A_n$ with rational coefficients. The numerators and denominators of the rational entries are generated with respect to the uniform distribution in a given interval (in our case, in $\mathbb{Z} \cap [-10^3, 10^3]$). We also draw random linear forms $\ell_c = c^T x$, and we consider different rank-constrained semidefinite programs.

As explained in Section 4, the most costly routine in SolveSDP is the computation of rational parametrizations of the Lagrange systems $\mathrm{lag}(\iota)$ defined in (3), namely Step 7 in the formal description in Section 4.1. We report in Table 1 on timings (column SolveSDP) and output degrees (column Deg) relative to the computation of the rational parametrization of a single Lagrange system. Ideally, we recall that to get the total time for SolveSDP one should take the sum of these timings for $p = 0, \ldots, r$ weighted by $\binom{m}{p}$ (similarly to the complexity bound in Theorem 10).

(m,n,p)	SolveSDP	Deg	(m,n,p)	SolveSDP	Deg
$(3,3,2)$	11 s	4	$(5,3,3)$	3 s	20
$(4,3,2)$	2 s	10	$(5,4,3)$	1592 s	90
$(4,4,2)$	9 s	30	$(5,5,3)$	16809 s	207
$(4,5,2)$	29 s	42	$(5,2,4)$	7 s	20
$(4,6,2)$	71 s	30	$(5,3,4)$	42 s	40
$(4,7,2)$	103 s	10	$(5,4,4)$	42 s	40
$(4,3,3)$	10 s	16	$(5,5,4)$	858 s	16
$(4,4,3)$	21 s	8	$(6,6,3)$	704 s	112
$(5,7,2)$	25856 s	140	$(6,3,5)$	591 s	80

Table 1: Optimization over $\mathcal{D}_p \cap \mathbb{R}^n$

We remark that our implementation is able to tackle from small to medium-size input semidefinite programs and different rank constraints. As an example, for

$(m, n, p) = (5, 7, 2)$ one should compute the critical points of a general linear form over the algebraic set defined by $\binom{5}{3}\binom{5}{3} = 100$ polynomials of degree 3 in 7 variables, which is unreachable by the state-of-the-art algorithms: our implementation computes a rational parametrization of degree 140 after seven hours. Further, when the size m is fixed, the cost in terms of computation seems to reflect suitably both the growth of output degree and of the number of variables n.

Moreover, it is worth to highlight that the entries of column Deg coincide exactly with the *algebraic degree of SDP* with parameters (m, n, p), as computed in [24, Table 2]. This fact is not obvious since our algorithm builds intermediate incidence varieties whose degree is typically larger than the degree of the determinantal varieties: hence one could *a priori* expect the degree of the output representation to be larger than the expected degree (which si computed in [24]). Even though the estimate of the output degree in Proposition 8 does not depend explicitly on formulas in [24], but only on multilinear bounds, this fact is remarkable and represents a guarantee of optimality of our method.

6.2 Minimal Sum-Of-Squares certificates

In this final section, we consider an interesting application of rank-constrained semidefinite programming. Let $x = (x_1, \ldots, x_k)$ and let $f \in \mathbb{R}[x]_{2d}$ be a homogeneous polynomial of degree $2d$, for $d \geq 1$. Let $b = \{\prod_i x_i^{j_i}\}_{\sum_i j_i = d}$ be the monomial basis of $\mathbb{R}[x]_d$. The sum-of-squares (SOS) decompositions of f are parametrized by the so-called *Gram spectrahedron* of f:

$$\mathcal{G}(f) = \{X \in \mathbb{S}_{\binom{k+d-1}{d}}(\mathbb{R}) : X \succeq 0,\ f = b^T X b\},$$

and any $X \in \mathcal{G}(f)$ is called a *Gram matrix* for f. *cf.* [28]. Remark here that the constraint $f = b^T X b$ is linear in the entries of X. If $f = f_1^2 + \cdots + f_r^2$, we say that f has a SOS decomposition *of length* r. We deduce that deciding whether f has a SOS decomposition of length at most r is equivalent to the following rank-constrained semidefinite program:

$$f = b^T X b \qquad X \succeq 0 \qquad \text{rank } X \leq r.$$

We have generated nonnegative polynomials by taking sums of squares of random homogeneous polynomials of degree d. Applying SolveSDP to this subfamily of problem $(\text{SDP})_r$, we have been able to handle example with $k \leq 3$ and $2d \leq 6$, corresponding to Gram matrices of size 10. We believe that this is due to the particular sparsity of these linear matrices.

7 Final remarks

This paper addresses a fundamental problem in computational real algebraic geometry, that is rank-constrained semidefinite programming. Our algorithm is able to return an exact algebraic representation of all minimizers, with explicit bounds on its output degree and whose complexity is essentially quadratic on the mentioned degree bound. The algorithm works under assumptions on the input, which are proved to be generically satisfied. This is done by exploiting the determinantal structure of this

optimization problem, and by reducing it to linear optimization over determinantal varieties. This reduction step allows to manage (non-convex) additional rank constraints. To the best of our knowledge, this is the first exact algorithm for solving $(\mathrm{SDP})_r$.

Acknowledgments

The author would like to thank the Fields Institute for Research in Mathematical Sciences, for the financial support offert during the Thematic Program on Computer Algebra of Fall 2015, and also the participants of the program for fruitful discussions around the topic of this work.

References

[1] M. F. Anjos, J. B. Lasserre (editors). Handbook of semidefinite, conic and polynomial optimization. Int. Series in Operational Research and Management Science. V.166, Springer, NY, 2012.

[2] S. Boyd, L. El Ghaoui, E. Feron and V. Balakrishnan. Linear matrix inequalities in system and control theory. Studies in Applied Mathematics 15. SIAM, Philadelphia, 1994.

[3] S. Boyd, L. Vandenberghe. Semidefinite programming. SIAM Review, 38(1):49–95, 1996.

[4] D. Eisenbud. Commutative algebra with a view toward algebraic geometry. Springer-Verlag, New York, 1995.

[5] J.-C. Faugère. FGb: a library for computing Gröbner bases. In Mathematical Software–ICMS 2010, pp. 84–87, Springer, 2010.

[6] J.-C. Faugère, C. Mou. Fast algorithm for change of ordering of zero-dimensional Gröbner bases with sparse multiplication matrices. Proceedings of ISSAC 2011, pp. 115–122, San Jose, USA.

[7] J.-C. Faugère, P. Gianni, D. Lazard, T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. Journal of Symbolic Computation, 16(4):329–344, 1993.

[8] J.C. Faugère, M. Safey El Din, P.J. Spaenlehauer. Computing loci of rank defects of linear matrices using Grobner bases and Applications to Cryptology. Proceedings of ISSAC 2010, Munich.

[9] A. Greuet, M. Safey El Din. Probabilistic algorithm for the global optimization of a polynomial over a real algebraic set. SIAM J. Opt., 24(3):1313–1343, 2014.

[10] M. X. Goemans, D. Williamson. Improved approximation algorithms for maximum cuts and satisfiability problems using semidefinite programming. J. of the ACM 42:1115–1145, 1995.

[11] M. Grötschel, L. Lovász, A. Schrijver. Geometric algorithms and combinatorial optimization. Springer, Berlin, 1988.

[12] D. Henrion, S. Naldi, M. Safey El Din. Real root finding for determinants of linear matrices. Journal of Symbolic Computation, 74:205–238, 2016.

[13] D. Henrion, S. Naldi, M. Safey El Din. Real root finding for rank defects in linear Hankel matrices. Proceedings of ISSAC 2015, Bath, UK, 221–228, 2015.

[14] D. Henrion, S. Naldi, M. Safey El Din. Real root finding for low rank linear matrices. `hal-01159210,v.1`, June 2015.

[15] D. Henrion, S. Naldi, M. Safey El Din. Exact algorithms for linear matrix inequalities. `hal-01184320,v.1`, August 2015.

[16] D. Henrion, S. Naldi, M. Safey El Din. SPECTRA: Semidefinite Programming solved Exactly with Computation Tools of Real Algebra. Software documentation, 2015. Web page: `http://homepages.laas.fr/snaldi/software.html`.

[17] G. Jeronimo, G. Matera, P. Solernò, A. Waissbein. Deformation techniques for sparse systems. Foundations of Computational Mathematics, 9(1):1–50, 2009.

[18] E. Kaltofen, B. Li, Z. Yang, L. Zhi. Exact certification of global optimality of approximate factorizations via rationalizing sums-of-squares with floating point scalars. ISSAC 2008, 155-163.

[19] L. Khachiyan and L. Porkolab. On the complexity of semidefinite programs. J. Global Optim., 10:351–365, 1997.

[20] J.B. Lasserre. Global optimization with polynomials and the problem of moments. SIAM J. Opt., 11(3):796–817, 2001.

[21] M. Laurent, M. E. Nagy, A. Varvitsiotis. Complexity of the positive semidefinite matrix completion problem with a rank constraint. Discrete Geometry and Optimization. In Fields Institute Communications, K. Bezdek, A. Deza and Y. Ye (eds), Springer, (69)105–120, 2013.

[22] Y. Nesterov and A. Nemirovsky. Interior-point polynomial algorithms in convex programming. Studies in Applied Mathematics 13. SIAM, Philadelphia, 1994.

[23] J. Nie. Optimality conditions and finite convergence of Lasserre's hierarchy. Mathematical Programming, Ser. A, 146:97-121, 2014.

[24] J. Nie, K. Ranestad, B. Sturmfels. The algebraic degree of semidefinite programming. Mathematical Programming, Ser. A,122:379–405, 2010.

[25] R. Orsi, U. Helmke, and J. B. Moore. A Newton-like method for solving rank constrained linear matrix inequalities. Automatica, 42(11):1875-1882, 2006.

[26] V. Pan, E. Tsigaridas. Nearly optimal refinement of real roots of a univariate polynomial. hal-01105263, 2014.

[27] P. Parrilo. Semidefinite programming relaxations for semialgebraic problems. Mathematical Programming Ser.B 96(2):293–320, 2003.

[28] V. Powers, T. Woermann. An algorithm for sums of squares of real polynomials. J. Pure and Appl. Alg. 127:99–104, 1998.

[29] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. J. of Applicable Algebra in Engineering, Communication and Computing. 9(5):433–461, 1999.

[30] M. Safey El Din, É. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. Preprint arXiv:1307.7836, 2013.

[31] I. Shafarevich. Basic algebraic geometry 1. Springer, Berlin, 1977.