Exact algorithms for semidefinite programs with degenerate feasible set*

Didier Henrion† Simone Naldi‡ Mohab Safey El Din§

2018

Abstract

Let $A_0, \ldots, A_n$ be $m \times m$ symmetric matrices with entries in $\mathbb{Q}$, and let $A(x)$ be the linear pencil $A_0 + x_1 A_1 + \cdots + x_n A_n$, where $x = (x_1, \ldots, x_n)$ are unknowns. The linear matrix inequality (LMI) $A(x) \succeq 0$ defines the subset of $\mathbb{R}^n$, called spectrahedron, containing all points x such that $A(x)$ has non-negative eigenvalues. The minimization of linear functions over spectrahedra is called semidefinite programming (SDP). Such problems appear frequently in control theory and real algebra, especially in the context of nonnegativity certificates for multivariate polynomials based on sums of squares.

Numerical software for solving SDP are mostly based on the interior point method, assuming some non-degeneracy properties such as the existence of interior points in the admissible set. In this paper, we design an exact algorithm based on symbolic homotopy for solving semidefinite programs without assumptions on the feasible set, and we analyze its complexity. Because of the exactness of the output, it cannot compete with numerical routines in practice but we prove that solving such problems can be done in polynomial time if either n or m is fixed.

1 Introduction

Let $x = (x_1, \ldots, x_n)$ be variables, and $A_0, A_1, \ldots, A_n$ $m \times m$ symmetric matrices with entries in the field $\mathbb{Q}$ of rational numbers. The goal of this article is to design algorithms for solving the semidefinite programming (SDP) problem

$$\inf \ell(x) \quad \text{s.t.} \quad x \in \mathscr{S}(A) \tag{1.1}$$

where $\ell(x) = \ell_1 x_1 + \cdots + \ell_n x_n$ is a linear function and $\mathscr{S}(A)$ is the solution set in $\mathbb{R}^n$ of the linear matrix inequality (LMI)

$$A(x) \coloneqq A_0 + x_1 A_1 + \cdots + x_n A_n \succeq 0. \tag{1.2}$$

*Mohab Safey El Din is supported by the ANR grant ANR-17-CE40-0009 Galop and the PGMO grant Gamma.

†LAAS-CNRS, Université de Toulouse, CNRS, Toulouse, France; Faculty of Electrical Engineering, Czech Technical University in Prague, Czech Republic.

‡Univ. Limoges, XLIM, UMR 7252; F-87000 Limoges, France

§Sorbonne Université, CNRS, INRIA, Laboratoire d'Informatique de Paris 6, LIP6, Équipe PolSys, 4 place Jussieu, F-75252, Paris Cedex 05, France.

In the previous formula, the constraint $A(x) \succeq 0$ means that $A(x)$ is positive semidefinite, that is, that all its eigenvalues are non-negative. The set $\mathscr{S}(A)$, called *spectrahedron*, is a convex and basic semi-algebraic, as affine section of the cone of positive semidefinite matrices.

Linear matrix inequalities and semidefinite programs appear frequently in several applied domains, *e.g.* for stability queries in control theory [11]. They also appear as a central object in convex algebraic geometry and real algebra for computing certificates of non-negativity based on sums of squares [8, 9] following the technique popularized notably by the seminal work of Lasserre [22] and Parrilo [26]. Since the LMI $A(x) \succeq 0$ defines the feasible set of SDP, LMI is also known as the SDP feasibility problem.

Even though SDP can be solved in polynomial time to a fixed accuracy via the ellipsoid algorithm, the complexity status of this problem in the Turing or in the real numbers model is still an open question in computer science (see [27, 2]). On the other hand, very few algebraic methods that can represent an alternative to classical approaches from optimization theory have been developed.

In this paper, we aim at designing a symbolic algorithm for solving the SDP in (1.1), without any assumption on the feasible set $\mathscr{S}(A)$, but with genericity assumptions on the objective function ℓ. It returns an algebraic representation of a feasible solution.

1.1 State of the art

Numerical methods have been developed for solving SDP problems, the most efficient of which are based on the interior point method [24]. This amounts to constructing an algebraic primal-dual curve called *central path*, whose points (x_μ, y_μ) are solutions to the quadratic semi-algebraic problems

$$A(x)Y(y) = \mu\,\mathbb{I}_m \qquad A(x) \succeq 0 \qquad Y(y) \succeq 0. \tag{1.3}$$

Above, $Y(y)$ must be read as a square matrix lying in a space of matrices dual to that of $A(x)$. For small but positive μ, when the LMI has strictly feasible solutions, the points x_μ lie in the interior of $\mathscr{S}(A)$, and converge to a boundary point for $\mu \to 0^+$. Moreover, barrier logarithmic functions have been extended from the classical setup of linear programming to the semidefinite cone, and can be used to solve (1.1) when $\mathscr{S}(A)$ has interior points.

By the way, there are several obstacles to interior-point strategies. First, $\mathscr{S}(A)$ has empty interior in several situations, for instance when $\mathscr{S}(A)$ consists of sums-of-squares certificates of a polynomial with rational coefficients that does not admit rational certificates, see [34] for a class of such examples. Moreover, as proved in [15], when classical assumptions on the given SDP fail to be satisfied, for instance in absence of strict complementarity, the central path might fail to converge to the optimal face. Finally, even in presence of interior points, it is hard to estimate the degree of the central path (that represents a complexity measure for path-following methods) in practical situations and explicit examples of central paths with exponential curvature have been computed [1].

The several existing variants of the interior-point algorithm are implemented in software running in finite precision, to cite a few SeDuMi [36], SDPT3 [37] and MOSEK [3]. The expected running time is essentially polynomial in $n, m, \log(\eta^{-1})$ (where η is the precision) and in the bit-length of the input [4, Ch.1,Sec.1.4]. Whereas these numerical routines run quite efficiently on huge instances, they may fail on degenerate situations, even on medium

or small size problems. This has motivated for instance the development of floating point libraries for SDP working in extended precision [21].

Symbolic computation has been used in the context of SDP to tackle several related problems. First, it should be observed that $\mathscr{S}(A)$ is a semi-algebraic set in $\mathbb{R}^n$ defined by sign conditions on the coefficients of the characteristic polynomial $t \mapsto det(t\,\mathbb{I}_m - A(x))$. Hence, classical real root finding algorithms for semi-algebraic sets such as [6, 7, 29, 5] can be used to solve SDP exactly. Using such algorithms leads to solve SDP in time $m^{O(n)}$. Algorithms for solving diophantine problems on linear matrix inequalities have been developed in [14, 33].

More recently, algorithms for solving exactly *generic* LMI [17, 19] and *generic* rank-constrained SDP [23] have been designed, with runtime polynomial in n (the number of variables, or equivalently the dimension of the affine section defining $\mathscr{S}(A)$) if m (the size of the matrix) is fixed. Because of the high degrees needed to encode the output [25], they cannot compete with numerical software but on small size problems offer a nice complement to these techniques in situations where numerical issues are encountered. In both cases, genericity assumptions on the input are required. This means that for some special problems (lying in some Zariski closed subset of the space spanned by the entries of matrices A_i), these algorithms cannot be applied.

1.2 Outline of the main contributions

In this paper, we remove the genericity assumptions on the feasible set $\mathscr{S}_A$ of the input SDP that were required in our previous work [17], and we show that optimization of generic linear functions over $\mathscr{S}_A$ can be performed without significant extra cost from the complexity viewpoint.

Our precise contributions are as follows.

- We design an algorithm for solving the SDP in (1.1) without any assumption on the defining matrix $A(x)$, with genericity assumptions on the objective function;
- we prove that this algorithm uses a number of arithmetic operations which is polynomial in n when m is fixed, and viceversa;
- we report on examples showing the behaviour of the algorithm on small-size but degenerate instances.

The main tool is the construction of a homotopy acting on the matrix representation $A(x)$ rather than on the classical complementarity conditions as in (1.3). This allows to preserve the LMI structure along the perturbation.

We use similar techniques from real algebraic geometry as those in [17], based on transversality theory [12], to prove genericity properties of the perturbed systems. We also investigate closedness properties of linear maps restricted to semi-algebraic sets in a more general setting in Section 2, generalizing similar statements for real algebraic sets in [30, 16].

1.3 General notation

For a matrix of polynomials $f \in \mathbb{R}[x]^{s\times t}$ in $x = (x_1, \ldots, x_n)$, we denote by $Z(f)$ the complex algebraic set defined by the entries of f. If $f \in \mathbb{R}[x]^s$, the Jacobian matrix of f is denoted

by $Df := \left(\frac{\partial f_i}{\partial x_j}\right)_{ij}$. A set $S \subset \mathbb{R}^n$ defined by sign conditions on a finite list of polynomials is called a basic semi-algebraic set, and a finite union of such sets is called a semi-algebraic set.

Let $\mathbb{S}_m(\mathbb{Q})$ be the space of $m \times m$ symmetric matrices with entries in $\mathbb{Q}$, and $\mathbb{S}_m^+(\mathbb{Q})$ the cone of positive semidefinite matrices in $\mathbb{S}_m(\mathbb{Q})$. Let $A(x) = A_0 + \sum_{i=1}^n x_i A_i$, with $A_i \in \mathbb{S}_m(\mathbb{Q})$. One can associate to $A(x)$ the hierarchy of algebraic sets

$$\mathcal{D}_r(A) = \{x \in \mathbb{R}^n : \operatorname{rank} A(x) \leq r\}, \quad r = 1, \ldots, m-1$$

defined by the minors of $A(x)$ of a fixed size. The set $\mathcal{D}_r$ is called a determinantal variety. We recall the definition of incidence variety in the context of semidefinite programming, introduced by the authors in [17]. For $r \in \{1, \ldots, m-1\}$, let $Y = Y(y)$ be a $m \times (m-r)$ matrix of unknowns $y_{i,j}$. Let $\iota \subset \{1, \ldots, m\}$ be a subset of cardinality $m-r$, and Y_ι the submatrix of Y corresponding to lines in ι. The *incidence variety* for $\mathcal{D}_r(A)$ is the algebraic set

$$\mathcal{V}_{r,\iota}(A) = \{(x, y) \in \mathbb{C}^n \times \mathbb{C}^{m(m-r)} : A(x)Y(y) = 0, Y_\iota = \mathbb{I}_{m-r}\}.$$

We have defined previously the spectrahedron $\mathscr{S}(A) = \{x \in \mathbb{R}^n : A(x) \succeq 0\}$, associated to $A(x)$.

Let $B \in \mathbb{S}_m(\mathbb{Q})$ and $\varepsilon \in [0, 1]$. In this paper, we consider a 1-parameter family of linear matrices

$$A(x) + \varepsilon B = (A_0 + \varepsilon B) + \sum x_i A_i$$

perturbing $A(x)$ in direction B.

2 Preliminaries

In this section, we prove some results of topological nature on spectrahedra and their deformations. Before doing that, we need to recall basics about infinitesimals and Puiseux series rings. More details can be found in [7].

An infinitesimal ε is a positive element which is transcendental over $\mathbb{R}$ and smaller than any positive real number. The Puiseux series field $\mathbb{R}\langle\varepsilon\rangle = \{\sum_{i \geq i_0} a_i \varepsilon^{i/q} \mid i_0 \in \mathbb{Z}, q \in \mathbb{N} - \{0\}\}$ is a real closed one [10, Ex.1.2.3]. An element $z = \sum_{i \geq i_0} a_i \varepsilon^{i/q}$ is bounded over $\mathbb{R}$ if $i_0 \geq 0$. In that case, one says that its limit when ε tends to 0 is a_0 and we write it $\lim_\varepsilon z$. The $\lim_\varepsilon$ operator is a ring homomorphism between $\mathbb{R}\langle\varepsilon\rangle$ and $\mathbb{R}$. We extend it over $\mathbb{R}\langle\varepsilon\rangle^n$ coordinatewise. Also given a subset $Q \subset \mathbb{R}\langle\varepsilon\rangle^n$, we denote by $\lim_\varepsilon Q$ the subset of $\mathbb{R}^n$ of points which are the images by $\lim_\varepsilon$ of bounded elements in Q.

Given a semi-algebraic set $S \subset \mathbb{R}^n$ defined by a semi-algebraic formula with coefficients in $\mathbb{R}$, we denote by $\mathsf{ext}(S, \mathbb{R}\langle\varepsilon\rangle)$ the solution set of that formula in $\mathbb{R}\langle\varepsilon\rangle^n$.

For a linear pencil $A(x) = A_0 + x_1 A_1 + \cdots + x_n A_n$ of $m \times m$ symmetric linear matrices and a $m \times m$ positive definite matrix B, we consider the spectrahedron $\mathscr{S}(A + \varepsilon B)$ in $\mathbb{R}\langle\varepsilon\rangle$. Our first result relates $\mathscr{S}(A) \subset \mathbb{R}^n$ with $\mathscr{S}(A + \varepsilon B) \subset \mathbb{R}\langle\varepsilon\rangle^n$.

Lemma 1 *Using the above notation, $\mathscr{S}(A)$ is included in (the interior of) $\mathscr{S}(A + \varepsilon B)$.*

Proof : If $\mathscr{S}(A) = \emptyset$, there is nothing to prove. Let $x^* \in \mathscr{S}(A)$. By definition of positive semi-definiteness, for any vector $v \in \mathbb{R}^m$, $v^t A(x^*) v \geq 0$. Since ε is a positive infinitesimal and

B is positive definite, we deduce that for any vector $v \in \mathbb{R}^m \setminus \{0\}$, $0 < v^t A(x^*)v + v^t \varepsilon B v = v^t(A(x^*)+\varepsilon B)v$. We deduce that $A+\varepsilon B$ is positive definite at x^*, hence x^* is in (the interior of) $\mathscr{S}(A+\varepsilon B)$, as requested. □

Further, we identify the set of linear forms $\ell = \ell_1 x_1 + \cdots + \ell_n x_n$ with $\mathbb{C}^n$, the linear form ℓ being identified to the point $\ell_1, \ldots, \ell_n$. By a slight abuse of notation we also denote by ℓ the map $x \mapsto \ell(x)$.

Lemma 2 *Let $\mathbf{R}$ be a real closed field, $\mathbf{C}$ be an algebraic closure of $\mathbf{R}$ and $S \subset \mathbf{R}^n$ be a closed semi-algebraic set. There exists a non-empty Zariski open set $\mathscr{L}(S) \subset \mathbf{C}^n$ such that for $\ell \in \mathscr{L}(S) \cap \mathbf{R}^n$, $\ell(S)$ is closed for the Euclidean topology.*

Proof : Our proof is by induction on the dimension of S. When S has dimension 0, the statement is immediate.

We let now $d \in \mathbb{N} \setminus \{0\}$, assume that the statement holds for semi-algebraic sets of dimension less than d and that S has dimension d. By [10, Th.2.3.6], it can be partitioned as a finite union of closed semi-algebraically connected semi-algebraic manifolds $S_1, \ldots, S_N$. Note that each S_i is still semi-algebraic. We establish below that there exist non-empty Zariski open sets $\mathscr{L}(S_i) \subset \mathbf{C}^n$ such that for $\ell \in \mathscr{L}(S_i) \cap \mathbf{R}^n$, $\ell(S_i)$ is closed for the Euclidean topology. Taking the intersections of those finitely many non-empty Zariski open set is then enough to define $\mathscr{L}(S)$.

Let $1 \leq i \leq N$. If the dimension of S_i is less than d, we apply the induction assumption and we are done. Assume now that S_i has dimension d. Let $V \subset \mathbf{C}^n$ be the Zariski closure of S_i and C be the semi-algebraically connected component of $V \cap \mathbf{R}^n$ which contains S_i. By [18, Prop.17], there exists a non-empty Zariski open set $\Lambda_{1,i} \subset \mathbf{C}^n$ such that for $\ell \in \Lambda_{1,i} \cap \mathbf{R}^n$, $\ell(C)$ is closed.

By definition of C and using [10, Ch.2.8], C has dimension d, as S_i. We denote by $T_i \subset \mathbf{R}^n$ the boundary of S_i. Observe that it is a closed semi-algebraic set of dimension less than d [10, Ch.2.8]. Using the induction assumption, we deduce that there exists a non-empty Zariski open set $\Lambda_{2,i} \subset \mathbf{C}^n$ such that for $\ell \in \Lambda_{2,i} \cap \mathbf{R}^n$, $\ell(T_i)$ is closed. We claim that one can define $\mathscr{L}(S_i)$ as the intersection $\Lambda_{1,i} \cap \Lambda_{2,i}$, i.e. for $\ell \in \mathscr{L}(S_i) \cap \mathbf{R}^n$, $\ell(S_i)$ is closed.

Indeed, assume that the boundary of $\ell(S_i)$ is not empty (otherwise there is nothing to prove) and take a in this boundary. Without loss of generality, assume also that for all $x \in S_i$, $\ell(x) \geq a$. We need to prove that $a \in S_i$.

Assume first that for all $\eta > 0$, $\ell^{-1}([a, a+\eta])$ has a non-empty intersection with T_i. Since $\ell(T_i)$ is closed by construction, we deduce that there exists $x \in T_i$ such that $\ell(x) = a$. Since S_i is closed by construction and T_i is its boundary, we deduce that $x \in S_i$ and then that $a \in \ell(S_i)$.

Assume now that for some $\eta > 0$, $\ell^{-1}([a, a+\eta])$ has an empty intersection with T_i. Then, we deduce that $\ell^{-1}([a, a+\eta]) \cap S_i = \ell^{-1}([a, a+\eta]) \cap C$. Besides, since $\ell(C)$ is closed, there exists $x \in C$ such that $\ell(x) = a$. Because, $\ell^{-1}([a, a+\eta]) \cap S_i = \ell^{-1}([a, a+\eta]) \cap C$, we deduce that $x \in S_i$ which ends the proof. □

Lemma 3 *Let $A(x)$ be as above and let B be a positive definite $m \times m$ matrix. There exists a non-empty Zariski open set $\mathscr{U}_1 \subset \mathbb{C}^n$ such that for $\ell \in \mathscr{U}_1 \cap \mathbb{R}^n$ the following holds:*

- *$\ell(\mathscr{S}(A))$ is closed for the Euclidean topology*
- *$\ell(\mathscr{S}(A+\varepsilon B))$ is closed for the Euclidean topology.*

Proof : If $\mathscr{S}(A) = \emptyset$, there is nothing to prove. Since $\mathscr{S}(A) \subset \mathbb{R}^n$ is a closed semi-algebraic set, one can apply Lemma 2 and deduce that there exists a non-empty Zariski open set $\mathscr{U}_1' \subset \mathbb{C}^n$ such that for $\ell \in \mathscr{U}_1' \cap \mathbb{R}^n$, $\ell(\mathscr{S}(A))$ is closed for the Euclidean topology.

The spectrahedron $\mathscr{S}(A + \varepsilon B) \subset \mathbb{R}\langle\varepsilon\rangle^n$ is also a closed semi-algebraic set. Applying Lemma 2 with $\mathbf{R} = \mathbb{R}\langle\varepsilon\rangle$, one deduces that there exists a non-empty Zariski open set $\mathscr{U}_\varepsilon'' \subset \mathbb{C}\langle\varepsilon\rangle^n$ such that for $\ell \in \mathscr{U}_\varepsilon'' \cap \mathbb{R}\langle\varepsilon\rangle^n$, $\ell(\mathscr{S}(A+\varepsilon B))$ is closed for the Euclidean topology. Since any non-empty Zariski open set $\mathscr{U}_\varepsilon'' \subset \mathbb{C}\langle\varepsilon\rangle^n$ contains a non-empty Zariski open set of $\mathbb{C}^n$, we pick one such set, denoted by $\mathscr{U}_1''$ and take finally $\mathscr{U}_1 = \mathscr{U}_1' \cap \mathscr{U}_1''$. □

Lemma 4 *Let ℓ in $\mathscr{U}_1 \cap \mathbb{R}^n$ where $\mathscr{U}_1$ is the non-empty Zariski open set defined in Lemma 3.*

Assume that there exists $x^* \in \mathscr{S}(A)$ such that $\ell(x^*)$ lies in the boundary of $\ell(\mathscr{S}(A))$. Then, there exists $x_\varepsilon^* \in \mathscr{S}(A + \varepsilon B)$ such that $\ell(x_\varepsilon^*)$ lies in the boundary of $\ell(\mathscr{S}(A + \varepsilon B))$ and $\lim_\varepsilon x_\varepsilon^* = x^*$.

Viceversa, if $x_\varepsilon^* \in \mathscr{S}(A+\varepsilon B)$ lies in the boundary of $\ell(\mathscr{S}(A+\varepsilon B))$, and $\mathscr{S}(A) \neq \emptyset$, then $\ell(\lim_\varepsilon x_\varepsilon^*)$ lies in the boundary of $\ell(\mathscr{S}(A))$.

Proof : Fix $r \in \mathbb{R}$ positive and let $B(x^*, r)$ be the ball centered at x^* of radius r. Further we abuse notation by denoting $\mathsf{ext}(\mathscr{S}(A), \mathbb{R}\langle\varepsilon\rangle)$ by $\mathscr{S}(A)$.

Recall that $\mathscr{S}(A)$ is contained in $\mathscr{S}(A + \varepsilon B)$ (Lemma 1) and observe that $\mathscr{S}(A + \varepsilon B)$ is infinitesimally close to $\mathscr{S}(A)$ (because of the continuity of the eigenvalues of $A(x) + \varepsilon B$ when x ranges over $\mathscr{S}(A + \varepsilon B)$).

This implies that there exists ρ_ε in the boundary of $\ell(\mathscr{S}(A + \varepsilon B) \cap \mathsf{ext}(B(x^*, r)))$ and which is infintesimally close $\ell(x^*)$. Since $\mathscr{S}(A + \varepsilon B) \cap \mathsf{ext}(B(x^*, r)$ is closed and bounded, $\ell(\mathscr{S}(A + \varepsilon B) \cap \mathsf{ext}(B(x^*, r))$ is closed for the Euclidean topology. Then, there exists $x_\varepsilon^* \in \mathscr{S}(A + \varepsilon B) \cap \mathsf{ext}(B(x^*, r)$ such that $\ell(x_\varepsilon^*) = \rho_\varepsilon$. Since this is true for any $r \in \mathbb{R}$ positive, we deduce the equality $\lim_\varepsilon x_\varepsilon^* = x^*$.

Viceversa, suppose that $x_\varepsilon^* \in \mathscr{S}(A + \varepsilon B)$ is such that $\ell(x_\varepsilon^*)$ lies in the boundary of $\ell(\mathscr{S}(A+\varepsilon B))$. Hence $\ell(x_\varepsilon^*)$ minimizes ℓ on $\mathscr{S}(A+\varepsilon B)$. Let $y \in \mathscr{S}(A)$. From Lemma 1, we know that $y \in \mathscr{S}(A+\varepsilon B)$. Since orders are preserved under limit, and by the continuity of ℓ, we get that

$$\ell(x^*) = \ell(\lim_\varepsilon x_\varepsilon^*) = \lim_\varepsilon \ell(x_\varepsilon^*) \leq \lim_\varepsilon \ell(y) = \ell(y).$$

By the arbitrarity of y we deduce that x^* minimizes ℓ on $\mathscr{S}(A)$, hence $\ell(x^*)$ lies in the boundary of $\ell(\mathscr{S}(A))$. □

3 Homotopy for semidefinite systems

We consider the original linear matrix inequality $A(x) \succeq 0$ and its solution set $\mathscr{S}(A)$. In this section, we prove that one gets regularity properties under the the deformation of $\mathscr{S}(A)$ described in the previous sections.

3.1 Regularity of perturbed incidence varieties

Let $B \in \mathbb{S}_m(\mathbb{Q})$ and $\varepsilon \in [0, 1]$. We say that $A + \varepsilon B$ is *regular* if, for every $r = 1, \ldots, m$ and $\iota \subset \{1, \ldots, m\}$ with $\sharp\iota = m-r$, the algebraic set $\mathcal{V}_{r,\iota}(A+\varepsilon B)$ is smooth and equidimensional, of co-dimension $m(m-r) + \binom{m-r+1}{2}$ in $\mathbb{C}^{n+m(m-r)}$.

The following proposition states that such a property holds almost everywhere if the perturbation follows a generic direction.

Proposition 5 *There exists a non-empty Zariski open set $\mathscr{B}_1 \subset \mathbb{S}_m(\mathbb{C})$ such that, for all $r \in \{0,\dots,m\}$, $\iota \subset \{1,\dots,m\}$ with $\sharp\iota = m-r$, and for $B \in \mathscr{B}_1 \cap \mathbb{S}_m(\mathbb{Q})$, the following holds. For every $\varepsilon \in (0,1]$, out of a finite set, the matrix $A+\varepsilon B$ is regular.*

Proof : We suppose w.l.o.g. that r is fixed and $\iota = \{1,\dots,m-r\}$. Let $\mathfrak{B}$ be an unknown $m\times m$ symmetric matrix. For $\varepsilon \in (0,1]$, we get a matrix $A+\varepsilon\mathfrak{B} = A(x)+\varepsilon\mathfrak{B}$, which is bilinear in the two groups of variables $x, \mathfrak{B}$. Let $f^{(\varepsilon)} = f^{(\varepsilon)}(x,y,\mathfrak{B})$ be the polynomial system given by the $(i,j)-$entries of $(A+\varepsilon\mathfrak{B})Y$ with $i \geq j$, and by all entries of $Y_\iota - \mathbb{I}_{m-r}$. By [17, Lemma 3.2], $Z(f^{(\varepsilon)}) = Z((A+\varepsilon\mathfrak{B})Y, Y_\iota - \mathbb{I}_{m-r})$, and remark that $\sharp f^{(\varepsilon)} = m(m-r) + \binom{m-r+1}{2}$.

We now proceed with a transversality argument. Consider the map (with abuse of notation)

$$\begin{array}{rccc} f^{(1)}: & \mathbb{C}^n \times \mathbb{C}^{m(m-r)} \times \mathbb{C}^{\binom{m+1}{2}} & \longrightarrow & \mathbb{C}^{m(m-r)+\binom{m-r+1}{2}} \\ & (x,y,\mathfrak{B}) & \longmapsto & f^{(1)}(x,y,\mathfrak{B}). \end{array}$$

We claim that 0 is a regular value of the map $f^{(1)}$ (the claim is proved in the last paragraph). This implies by Thom's Weak Transversality [31, Prop. B.3] that there is a Zariski open set $\mathscr{B}_{r,\iota} \subset \mathbb{S}_m(\mathbb{C})$ such that, if $B \in \mathscr{B}_{r,\iota}$, then 0 is a regular value of the section map $(x,y) \mapsto f^{(1)}(x,y,B)$.

We define $\mathscr{B}_1 := \cap_r \cap_\iota \mathscr{B}_{r,\iota}$, which is a finite intersection of Zariski open sets, hence Zariski open. Now, for a fixed $B \in \mathscr{B}_1$, consider the line tB, $t \in \mathbb{R}$, in $\mathbb{S}_m(\mathbb{C})$. Let $F_1 \in \mathbb{C}[\mathfrak{B}]$ be the generator of the ideal of all polynomials vanishing over the algebraic hypersurface $\mathbb{S}_m(\mathbb{C}) \setminus \mathscr{B}_1$. Then, since $B \in \mathscr{B}_1$ by construction, $t \mapsto F_1(tB)$ does not vanish identically, hence it vanishes exactly $\deg F_1$ many times (counting multiplicities). We deduce that, $\varepsilon B \in \mathscr{B}_1$ except for finitely many values of ε. We conclude that for all r and ι, $\mathcal{V}_{r,\iota}(A+\varepsilon B)$ is smooth and equidimensional of co-dimension $\sharp f^{(\varepsilon)} = m(m-r) + \binom{m-r+1}{2}$, for $\varepsilon \in (0,1]$ except for finitely many values.

We prove now our claim. It follows by argument similar to the proof of [17, Prop.3.4]. Consider the derivatives of polynomials in $f^{(1)}(x,y,\mathfrak{B})$ with respect to the $(i,j)-$entries of $\mathfrak{B}$, with either $i \leq m-r$ or $j \leq m-r$, and those with respect to $y_{i,j}$ with $i \in \iota$. It is straightforward to check that this gives a maximal submatrix of the jacobian matrix $Df^{(1)}$ whose determinant is non-zero, proving that 0 is actually a regular value of $f^{(1)}$. □

3.2 Critical points on perturbed LMI

Let $B \in \mathbb{S}_m(\mathbb{Q})$ and let $A+\varepsilon B$ be the perturbed linear pencil defined above. For a fixed $\varepsilon < 1$, we consider the stratification of the hypersurface $Z(\det(A+\varepsilon B))$ given by the varieties $\mathcal{D}_r(A+\varepsilon B)$ of multiple rank defects of $A+\varepsilon B$, and their lifted incident sets $\mathcal{V}_{r,\iota}(A+\varepsilon B)$.

For $r < m$ and $\iota \subset \{1,\dots,m\}$ with $\sharp\iota = m-r$, let $c := m(m-r) + \binom{m-r+1}{2}$. We recall from the proof of Proposition 5 that $f^{(\varepsilon)} \in \mathbb{R}[x,y]^c$ consists of the $(i,j)-$entries of $A^{(\varepsilon)}Y$ with $i \geq j$, and by all entries of $Y_\iota - \mathbb{I}_{m-r}$. We define the *Lagrange system* $\mathrm{Lag}_{r,\iota}(A+\varepsilon B)$ as follows:

$$\begin{gathered} f_i^{(\varepsilon)}(x,y) = 0, \quad i = 1,\dots,c \\ \sum_{i=1}^{c} z_i \nabla f_i^{(\varepsilon)}(x,y) = \begin{pmatrix} \ell \\ 0 \end{pmatrix} \end{gathered} \tag{3.1}$$

where $\ell : \mathbb{R}^n \to \mathbb{R}$ is linear. As in Section 2, we abuse the notation of ℓ, and identifying it with the vector $(\ell_1, \ldots, \ell_n) \in \mathbb{R}^n$ giving $\ell(x) = \ell_1 x_1 + \cdots + \ell_n x_n$, hence $\ell = \nabla \ell$.

The set $Z(f^{(\varepsilon)}) = \mathcal{V}_{r,\iota}(A + \varepsilon B)$ is smooth for generic B thanks to Proposition 5. Hence a solution (x^*, y^*, z^*) of system (3.1) is a critical point (x^*, y^*) of the restriction of ℓ to $\mathcal{V}_{r,\iota}(A + \varepsilon B)$, equipped with a Lagrange multiplier $z^* \in \mathbb{C}^c$. Such a solution is called *of rank* r if rank $(A(x^*) + \varepsilon B) = r$.

Proposition 6 *There are two non-empty Zariski-open sets $\mathscr{B}_2 \subset \mathbb{S}_m(\mathbb{C})$ and $\mathscr{C}_2 \subset \mathbb{C}^n$ such that, for $B \in \mathscr{B}_2 \cap \mathbb{S}_m(\mathbb{Q})$, $\ell \in \mathscr{C}_2 \cap \mathbb{Q}^n$, and $\varepsilon \in (0, 1]$ out of a finite set, the following holds. Suppose that ℓ has a minimizer or maximizer x^*_ε on $\mathscr{S}(A + \varepsilon B)$. The projection on the $x-$space of the union, for $\iota \subset \{1, \ldots, m\}$, $\sharp\iota = m - r$, of the solution sets of rank r of system* (3.1)*, is finite and contains x^*_ε.*

Proof : Let $r \leq m - 1$ and $\iota \subset \{1, \ldots, m\}$. Recall by [23, Th. 4] that a minimizer or a maximizer x^* for the SDP $\inf\{\ell(x) : A(x) + \varepsilon B \succeq 0\}$, with rank $(A(x^*) + \varepsilon B) = r$, is a critical point of the restriction of ℓ to $\mathcal{D}_r(A + \varepsilon B)$. Moreover, [23, Lem. 2] implies that such critical points can be computed as projection on the $x-$space, of the critical points of the restriction of ℓ to $\mathcal{V}_{r,\iota}(A + \varepsilon B)$, for some ι (here we mean the extension $(x, y) \mapsto \ell(x)$ of ℓ to the $(x, y)-$space). Thus we only need to prove the finiteness of solutions of rank r of system (3.1), for a generic perturbation matrix B and a generic linear function ℓ, *uniformly* on ε.

We denote by $g^{(\varepsilon)} = z^T D f^{(\varepsilon)} - (\ell, 0)^T$ (the polynomials in the second row of (3.1)). The system $(f^{(\epsilon)}, g^{(\epsilon)})$ is square, for a fixed ϵ. Consider the polynomial map $(f^{(1)}, g^{(1)})$ sending $(x, y, \mathfrak{B}, z, \mathfrak{l})$ to $(f^{(1)}(x, y, \mathfrak{B}), g^{(1)}(x, y, \mathfrak{B}, z, \mathfrak{l}))$, where $\mathfrak{B}$ and $\mathfrak{l}$ are variables for B and ℓ, of the right size. As in the proof of Proposition 5, for generic B the rank of $Df^{(1)}$ is maximal. Hence, following *mutatis mutandis* the proof of [23, Prop.3], we conclude that the jacobian matrix of $(f^{(1)}, g^{(1)})$ has full rank at every point in $Z(f^{(1)}, g^{(1)})$ of rank r. Hence there exist non-empty Zariski open sets $\mathscr{B}_{r,\iota} \subset \mathbb{S}_m(\mathbb{C}), \mathscr{C}_{r,\iota} \subset \mathbb{C}^n$ such that if $(B, \ell) \in \mathscr{B}_{r,\iota} \times \mathscr{C}_{r,\iota}$ then system (3.1) has finitely many solutions of rank r, for $\varepsilon = 1$. We define $\mathscr{B}_2 \coloneqq \cap_r \cap_\iota \mathscr{B}_{r,\iota}$ and $\mathscr{C}_2 \coloneqq \cap_r \cap_\iota \mathscr{C}_{r,\iota}$ and we conclude the same disregarding r and ι.

Let $F_2 \in \mathbb{C}[\mathfrak{B}, \mathfrak{l}]$ be the generator of the ideal of all polynomials vanishing over $(\mathbb{S}_m(\mathbb{C}) \times \mathbb{C}^n) \setminus (\mathscr{B}_2 \times \mathscr{C}_2)$. Then $F_2(B, \ell) \neq 0$, which implies that $t \mapsto F_2(tB, \ell)$ has finitely many roots, hence $(\varepsilon B, \ell) \in (\mathscr{B}_2 \times \mathscr{C}_2)$ almost everywhere in $(0, 1]$. We conclude the proof by defining the claimed finite set as the union of (1) the set of roots of F_2 and (2) the finite set constructed in Proposition 5. □

Note that the transversality techniques used in the proofs of Propositions 5 and 6 are non-constructive. Indeed they prove the existence of the *discriminants* $F_1 \in \mathbb{C}[\mathfrak{B}]$ and $F_2 \in \mathbb{C}[\mathfrak{B}, \mathfrak{l}]$, but do not construct them effectively. If we knew F_1, F_2 one could use separation bounds for real roots of univariate polynomials (*e.g.* [20]) to get upper bounds for the minimum of the finite sets.

3.3 The degree of the homotopy curve

We consider the Lagrange system (3.1), $r < m$ and $\iota \subset \{1, \ldots, m\}$ with $\sharp\iota = m - r$. For a given homotopy parameter $\varepsilon \in (0, 1)$ out of the union of the finite sets defined in Propositions 5 and 6, the system has finitely many solutions of rank r. When ε converges to 0, these solutions draw a (possibly reducible) semi-algebraic curve. This can also be seen as a semi-algebraic subset of dimension 1 in $\mathbb{R}\langle\varepsilon\rangle^n$. We denote this curve by $\mathcal{C}_{r,\iota}$.

Contrarily to the classical homotopy based on the central path, whose points lie in the interior of the feasible set, we have constructed homotopy curves containing optimal solutions of given rank of perturbed semidefinite programs. This allows to derive degree bounds that depend on this rank.

Proposition 7 *Let r, ι be fixed, let $\mathcal{C}_{r,\iota}$ be the curve of solutions or rank r of the Lagrange system* (3.1)*, for positive small enough ε, and $Zar(\mathcal{C}_{r,\iota})$ be its complex Zariski closure. Then*

$$\deg Zar(\mathcal{C}_{r,\iota}) \leq (1 + 2r(m-r)) \cdot \theta_1$$

where

$$\theta_1 = \sum_k \binom{c}{n-k}\binom{n}{c+k-r(m-r)}\binom{r(m-r)}{k} \tag{3.2}$$

Proof : We first compute a polynomial system equivalent to (3.1). We make the substitution $Y_\iota = \mathbb{I}_{m-r}$ that eliminates variables $\{y_{i,j} : i \in \iota\}$ in the vector $f^{(\varepsilon)}$ defining the incidence variety $\mathcal{V}_{r,\iota}(A + \varepsilon B)$, hence we suppose $f^{(\varepsilon)} \in \mathbb{Q}[\varepsilon, x, \overline{y}]^c$, with $c = m(m-r) - \binom{m-r}{2} = \frac{(m-r)(m+r+1)}{2}$ and $\overline{y} = \{y_{i,j} : i \notin \iota\}$. (Indeed, $\binom{m-r}{2}$ is the number of redundancies eliminated by [17, Lemma 3.2] recalled in the proof of Proposition 5.) Above we have intentionally abused of the notation of $f^{(\varepsilon)}$ and c. Next, the new polynomials f_i do not depend on $y \setminus \overline{y}$. Hence, defining $g \coloneqq \sum_{i=1}^c z_i \nabla f_i^{(\varepsilon)}(x, \overline{y}) - (\nabla \ell, 0)^T \in \mathbb{Q}[\varepsilon, x, \overline{y}, z]$, with $z = (z_1, \ldots, z_c)$, one has $\sharp g = \sharp x + \sharp \overline{y} = n + r(m-r)$.

We conclude that the Lagrange system (3.1) is given after reduction by the entries of $f^{(\varepsilon)}$ and g, that are multilinear in the three groups of variables $\xi \coloneqq (\varepsilon, x), \overline{y}$ and z. The multidegree with respect to $(\xi, \overline{y}, z)$ is respectively

- $\mathrm{mdeg}_{(\xi,\overline{y},z)}(f_i^{(\varepsilon)}) = (1, 1, 0)$, for $i = 1, \ldots, c$
- $\mathrm{mdeg}_{(\xi,\overline{y},z)}(g_i) = (0, 1, 1)$, for $i = 1, \ldots, n$
- $\mathrm{mdeg}_{(\xi,\overline{y},z)}(g_{n+j}) = (1, 0, 1)$, for $j = 1, \ldots, r(m-r)$

We compute below a multilinear Bézout bound of $\deg \mathrm{Zar}(\mathcal{C}_{r,\iota})$ (see [31, App.H.1]). This is given by the sum of the coefficients of the polynomial

$$P = (s_1 + s_2)^c (s_2 + s_3)^n (s_1 + s_3)^{r(m-r)}$$

modulo the monomial ideal $I = \langle s_1^{n+2}, s_2^{r(m-r)+1}, s_3^{c+1} \rangle$. Since the maximal admissible power modulo I of s_1 (resp. of s_2, s_3) is $n+1$ (resp. $r(m-r), c$) and since P is homogeneous of degree $c + n + r(m-r)$ we get

$$P \equiv \theta_1 s_1^n s_2^{r(m-r)} s_3^c + \theta_2 s_1^{n+1} s_2^{r(m-r)-1} s_3^c + \theta_3 s_1^{n+1} s_2^{r(m-r)} s_3^{c-1}$$

modulo I, where $\theta_i = \theta_i(m, n, r)$ are the corresponding coefficiens in the expansion of P, hence the bound is $\theta_1 + \theta_2 + \theta_3$. Just by expanding P and by solving a linear system over $\mathbb{Z}$ one gets the expression in (3.2), within the range $0 \leq k \leq \min\{n - c + r(m-r), r(m-r)\}$. A similar formula holds for θ_2 where $n - k + 1$ substitutes $n - k$ in the first binomial coefficient. We deduce that

$$\theta_2 \leq \max_k \left\{ \frac{c - n + k}{n - k + 1} \right\} \theta_1 \leq r(m-r)\theta_1.$$

Moreover the expression of θ_3 equals that of θ_2 except for the second binomial coefficient which is smaller, hence $\theta_3 \leq \theta_2 \leq r(m-r)\theta_1$, and we conclude. □

Recall that the algorithm in [17] solves LMI under genericity properties that cannot be assumed in the context of this paper. It avoids the use of homotopy. We expect that in degenerate situations the degree of the homotopy curve will exceed that of the univariate representation computed in the regular case. We prove that this degree gap is controlled, namely, that the extra factor is linear in n and in the rank-corank coefficient $r(m-r)$.

Proposition 8 *Let $\theta = \theta(m,n,r)$ be the bound computed in [17, Prop.5.1]. For all r and ι as above,* $\deg Zar(\mathcal{C}_{r,\iota}) \leq (1+2r(m-r))\, n\theta$.

Proof : Let θ_1 be the expression in (3.2). We prove that $\theta_1 \leq n\theta$ and we conclude. Indeed, let $\theta = \sum_k a_k$ and $\theta_1 = \sum_k b_k$. Then

$$\frac{b_k}{a_k} = \frac{n}{c+k-r(m-r)}$$

that does not exceed n for all k. Hence $\theta_1 \leq \sum_k n a_k = n\theta$. □

4 Algorithm

4.1 Description

This section contains the formal description of a homotopy-based algorithm for solving the semidefinite program in (1.1), called DegenerateSDP.

We first define the data structures we use to represent algebraic sets of dimension 0 and 1 during the algorithm. A *zero-dimensional parametrization* of a finite set $W \subset \mathbb{C}^n$ is a vector $Q = (q_0, q_1, \ldots, q_n, q) \in \mathbb{Q}[t]^{n+2}$ such that q_0, q are coprime and

$$W = \{a \in \mathbb{C}^n : a_i = q_i(t)/q_0(t), q(t) = 0, \exists t \in \mathbb{R}\}\,.$$

Similarly a *one-dimensional parametrization* of a curve $\mathcal{C} \subset \mathbb{C}^n$ is a vector $Q = (q_0, q_1, \ldots, q_n, q) \in \mathbb{Q}[t,u]^{n+2}$ with q_0, q coprime and

$$\mathcal{C} = \{a \in \mathbb{C}^n : a_i = q_i(t,u)/q_0(t,u), q(t,u) = 0, \exists t,u \in \mathbb{R}\}\,.$$

Abusing notation we denote by $Z(Q)$ the sets in the right part of the previous equalities. If Q is a list of parametrizations, $Z(Q)$ denotes the union of $Z(Q_i)$ for Q_i in Q, and every $x^* \in Z(Q)$ is encoded by $(Q, [a_*, b_*])$, where $a_*, b_* \in \mathbb{Q}$ and $[a_*, b_*]$ is a separating interval for the root that corresponds to x^*. These representations for finite sets and curves are standard in real algebraic geometry, and are called parametrizations in the sequel. By convention, ( ) is a parametrization for $\emptyset$.

We also define the following subroutines manipulating this kind of representations:

- ODP. With input a polynomial system $f = (f_1, \ldots, f_s)$ defining a one-dimensional algebraic set $Z(f)$, and a set of variables x, it returns a one-dimensional parametrization of the projection of $Z(f)$ on the $x-$space.

- CUT. Given a one-dimensional parametrization Q of the zero set $Z(f) \subset \mathbb{C}^{n+1}$ of polynomials $f_1, \ldots, f_s \in \mathbb{Q}[\varepsilon, x]$, it returns a zero-dimensional parametrization of the projection on the $x-$space of the limit of $Z(f)$ for $\varepsilon \to 0^+$.

- UNION. Given two parametrizations Q_1, Q_2, it returns a parametrization Q such that $Z(Q) = Z(Q_1) \cup Z(Q_2)$.

The input of DEGENERATESDP is the $m \times m$ $n-$variate symmetric linear matrix $A(x)$ defining the spectrahedron $\mathscr{S}(A)$, and a linear form ℓ. The output is a list $Q = [Q_1, \ldots, Q_{m-1}]$ of zero-dimensional parametrizations containing a solution x^* to the original LMI (with the corresponding interval $[a_*, b_*]$ of rational numbers), or ( ), which means that the original SDP (1.1) is either infeasible ($\mathscr{S}(A) = \emptyset$) or that the infimum in (1.1) equals $-\infty$.

Below we describe each step of the algorithm.

1: **procedure** DEGENERATESDP(A, ℓ)
2: Generate $B \in \mathbb{S}_m(\mathbb{Q})$
3: $Q \leftarrow [\,]$
4: **for** $r = 1, \ldots, m-1$ **do**
5: $Q_r \leftarrow (1)$
6: **for** $\iota \subset \{1, \ldots, m\}$ with $\sharp\iota = m - r$ **do**
7: $L \leftarrow \mathrm{Lag}_{r,\iota}(A + \varepsilon B)$
8: $Q_{r,\iota} \leftarrow \mathsf{ODP}(L, x)$
9: $Q_r \leftarrow \mathsf{UNION}(Q_r, Q_{r,\iota})$
10: $Q \leftarrow [Q, \mathsf{CUT}(Q_r)]$
11: **if** $\mathscr{S}(A) \cap Z(Q) = \emptyset$ **then return** ( )
12: **return** $(Q, [a_*, b_*])$

Note that ε in the previous formal description is treated as variable, so that the polynomials in L at step 7 define a curve. Remark that all solutions satisfy $\det A(x) = 0$ hence $\operatorname{rank} A(x) \leq m - 1$.

We show in Theorem 9 that DEGENERATESDP is correct and computes solutions to the original linear matrix inequality as limits of perturbed solutions. We use the results of Sections 2 and 3 and refer to the notation of Zariski open sets constructed in Lemma 3 and 4, and in Proposition 5 and 6.

Theorem 9 *Let A be a $m \times m$ $n-$variate symmetric linear matrix. Let $B \in \mathscr{B}_1 \cap \mathscr{B}_2 \cap \mathbb{S}_m^+(\mathbb{Q})$, and $\ell \in \mathscr{C}_1 \cap \mathscr{C}_2 \cap \mathbb{Q}^n$.*

A. If $A(x^*) = 0$ for some $x^* \in \mathbb{R}^n$, then x^* is a minimizer in (1.1) or ℓ is unbounded from below on $\mathscr{S}_A$.

B. Otherwise, $Q = $ DEGENERATESDP(A, ℓ) fulfils the following condition. If $x^* \in \mathscr{S}(A)$ is a minimizer in (1.1) then $x^* \in \mathscr{S}(A) \cap Z(Q)$. Viceversa, if $\mathscr{S}(A) \neq \emptyset$, and ℓ is not unbounded from below on $\mathscr{S}(A)$, then $\mathscr{S}(A) \cap Z(Q)$ contains a minimizer in (1.1).

Proof : First, suppose that $A(x^*) = 0$ for some $x^* \in \mathbb{R}^n$. Then $A_0 = -\sum_i x_i^* A_i$, hence $A(x) = (x_1 - x_1^*)A_1 + \cdots + (x_n - x_n^*)A_n$. We deduce that $\mathscr{S}_A$ is the image under the

translation $x \mapsto x + x^*$ of a cone, that is: either $\mathscr{S}_A = \{x^*\}$, in which case $\ell \equiv \ell(x^*)$ on $\mathscr{S}_A$, and x^* is a minimizer for (1.1), or $\mathscr{S}_A$ is an unbounded convex cone with origin in x^*. In the second case, since ℓ is linear, either its infimum on $\mathscr{S}_A$ is attained at the origin x^*, or its maximum is attained in x^* and ℓ is unbounded from below on $\mathscr{S}_A$.

We prove the first sentence in (B). Assume that $x^* \in \mathscr{S}(A)$ is a minimizer in (1.1). Then $\ell(x^*)$ lies in the boundary of $\ell(\mathscr{S}(A))$. By Lemma 4, we get that there exists $x^*_\varepsilon \in \mathscr{S}(A+\varepsilon B)$ such that $\ell(x^*_\varepsilon)$ lies in the boundary of $\ell(\mathscr{S}(A+\varepsilon B))$ and $\lim_\varepsilon x^*_\varepsilon = x^*$. Hence for $\varepsilon > 0$, x^*_ε is a minimizer of ℓ on $\ell(\mathscr{S}(A+\varepsilon B)) \subset \mathbb{R}^n$. By Proposition 6, there exists $r \in \{1, \ldots, m-1\}$, $\iota \subset \{1, \ldots, m\}$ with $\sharp\iota = m - r$, y^*_ε and z^*_ε, such that $(x^*_\varepsilon, y^*_\varepsilon, z^*_\varepsilon)$ is a solution of the Lagrange system $\mathrm{Lag}_{r,\iota}(A + \varepsilon B)$. We deduce that for $\varepsilon > 0$, x^*_ε is parametrized by the one-dimensinal parametrization $Q_{r,\iota} = \mathsf{ODP}(L)$ computed at step 8 of DegenerateSDP, hence by Q_r. We deduce that Q parametrizes the limit $x^* = \lim_\varepsilon x^*_\varepsilon$, that is $x^* \in \mathscr{S}(A) \cap Z(Q)$.

We finally come to the second sentence in (B). Since ℓ is not unbounded on $\mathscr{S}(A)$, and $\mathscr{S}(A) \neq 0$, then the same holds for ℓ on $\mathscr{S}(A + \varepsilon B)$. By Lemma 3, $\ell(\mathscr{S}(A))$ and $\ell(\mathscr{S}(A + \varepsilon B))$ are closed intervals. We deduce that the boundary of $\ell(\mathscr{S}(A + \varepsilon B))$ is non-empty. Let x^*_ε be such that $\ell(x^*_\varepsilon)$ lies in the boundary of $\ell(\mathscr{S}(A + \varepsilon B))$. Since $\mathscr{S}(A) \neq \emptyset$, by 4 $x^* \coloneqq \lim_\varepsilon x^*_\varepsilon \in \mathscr{S}(A) \cap Z(Q)$ is such that $\ell(x^*)$ lies in the boundary of $\ell(\mathscr{S}(A))$, hence a minimizer of the SDP in (1.1). □

To conclude, we make explicit the following fact that follows from Theorem 9. Recall that a generic linear form over a non-empty convex set is either unbounded from below ($\inf \ell = -\infty$) or its infimum is attained. Theorem 9 implies that if ℓ is a generic linear form, then $\mathscr{S}(A) \cap Z(Q) = \emptyset$ if and only if $\mathscr{S}(A) = \emptyset$ or ℓ is unbounded from below on $\mathscr{S}(A)$. We conclude that up to genericity assumptions on the linear form, the algorithm is correct, since it returns a non-empty rational parametrization if and only if problem (1.1) has a feasible solution.

4.2 Complexity analysis

This section contains a rigourous analysis of the arithmetic complexity of DegenerateSDP. Let us first give an overview of the algorithms that are used to perform the subroutines in DegenerateSDP.

The computation of a one-dimensional parametrization of the homotopy curve $\mathrm{Zar}(\mathcal{C}_{r,\iota})$ at step 8, that is the routine ODP, is done in two steps. First, we instantiate the system $\mathrm{Lag}_{r,\iota}(A + \varepsilon B)$ to a generic $\varepsilon = \bar{\varepsilon}$. By Proposition 6 we deduce that the obtained system is zero-dimensional. We use [32] to compute a zero-dimensional rational parametrization of this system.

The second steps consists in *lifting* the parameter ε and in computing a *parametric geometric resolution* of $\mathrm{Lag}_{r,\iota}(A+\varepsilon B)$ with the algorithm in [35], that is, a parametric analogue of [13]. In our context, there is only one parameter, that is ε.

The routine CUT can be performed via the algorithm in [28] and, finally, the cost of the routine UNION is given in [31, Lem.G.3].

To keep notations simple, let $L = (L_1, \ldots, L_N) \in \mathbb{Q}[\varepsilon, t_1, \ldots, t_N]$ be the polynomials defining the Lagrange system (3.1), in the reduced form as in the proof of Proposition (7). Hence $N = c + n + r(m - r)$, where $c = (m - r)(m + r + 1)/2$. The complex algebraic set $\mathrm{Zar}(\mathcal{C}_{r,\iota}) = Z(L)$ is a curve whose degree is bounded by Proposition 7.

Theorem 10 *Let L and N be as above. Under the assumptions of Theorem 9, the output $Q = \text{DegenerateSDP}(A, \ell)$ is returned within*

$$\widetilde{O}\left(n \sum_r \binom{m}{r} r(m-r) N^4 \theta^2\right)$$

arithmetic operations over $\mathbb{Q}$, where $\widetilde{O}(T) = O(T \log^a(T))$ for some a and $\theta \leq \binom{m^2+n}{n}^3$.

Proof : Let $\overline{\varepsilon} \in (0,1)$ be generic, and let $\overline{L}$ be equal to the system L where ε is instantiated to $\overline{\varepsilon}$. Let θ be the value computed in [17, Prop.5.1], that bound the number of solution of $\overline{L} = 0$ in $\mathbb{C}^N$. By the same proposition one gets

$$\theta \leq \binom{c+n}{n}^3 \leq \binom{m(m-r)+n}{n}^3,$$

from which the claimed bound uniform in r.

Let $\overline{L}' = (\overline{L}'_1, \ldots, \overline{L}'_N)$ be a polynomial vector of lenght N such that $\overline{L}'_i$ has the same multilinear structure as $\overline{L}_i$, for $i = 1, \ldots, N$. Let $H(T, t_1, \ldots, t_N) = T\overline{L} + (1-T)\overline{L}'$. By [32, Prop.5], the complexity of computing a univariate representation of $Z(\overline{L})$ is in $\widetilde{O}(N^3\theta\theta')$ where $\theta' = \deg, Z(H)$. By [17, Lem.5.4], $\theta' \in O(N \min\{n, c\}\theta)$. Hence the complexity of the first step of ODP is in

$$\widetilde{O}(\min\{n, c\} N^4 \theta^2).$$

Next, let $\pi : \mathbb{C}^{N+1} \to \mathbb{C}$ be the projection $(\varepsilon, t_1, \ldots, t_N) \mapsto \varepsilon$. By [17, Prop.5.1], a generic fiber of π has degree bounded by θ. Proposition 8 implies that $\deg \text{Zar}(\mathcal{C}_{r,\iota})$ is bounded above by $(1 + 2r(m-r))\, n\theta$. We apply the bound in [35, Cor.1], and we get a complexity in

$$\widetilde{O}\left(nr(m-r)N^4\theta^2\right),$$

for the parametric resolution step in ODP. By [32, Lem.13], the complexity of CUT is in $\widetilde{O}\left(N^3\theta\theta'\right)$, hence in

$$\widetilde{O}\left(\min\{n, c\} N^4 \theta^2\right).$$

The complexity of UNION is in $\widetilde{O}(N\theta^2)$ at each step, by [31, Lem.G.3]. This shows that the most expensive step is the lifting step.

The previous complexity bounds depend on r, and hold for all $r = 1, \ldots, m$, and for all index subsets $\iota \subset \{1, \ldots, m\}$. We conclude by summing up with weight $\binom{m}{r}$, the number of subsets $\iota \subset \{1, \ldots, m\}$ of cardinality $m - r$. □

We note that N can be bounded above by $n + 2m^2$ uniformly in r. The complexity of DegenerateSDP given by Theorem 10 is polynomial in n when m is fixed. Moreover, for a generic perturbation matrix B, [17, Lem.3.1] allows to deduce the inequality $n \geq \binom{m-r+1}{2}$: this implies that when n is fixed, then m is bounded above and hence the complexity is still polynomial.

5 Example

In this final section we develop a degenerate example in low dimension, showing how our algorithm works from a geometric viewpoint.

Consider the 2×2 semidefinite representation of a point $(p_1, p_2) \in \mathbb{R}^2$:

$$\left\{ (x_1, x_2) \in \mathbb{R}^2 : A(x) \coloneqq \begin{pmatrix} p_1 - x_1 & x_2 - p_2 \\ x_2 - p_2 & x_1 - p_1 \end{pmatrix} \succeq 0 \right\} = \{(p_1, p_2)\}.$$

The interior of $\mathscr{S}(A) \coloneqq \{(p_1, p_2)\}$ in $\mathbb{R}^2$ is empty, and moreover $\mathscr{S}(A)$, corresponding to the intersection of the $2-$dimensional linear space of matrices in the pencil $A(x)$ with the the $3-$dimensional cone of 2×2 symmetric matrices, has co-dimension 2 in $\mathbb{R}^2$.

We first construct the incidence varieties $\mathcal{V}_{r,\iota}(A)$. For $r = 0$, the incidence variety is smooth, but for $r = 1$ and $\iota = \{1\}$, this is the following algebraic curve in $\mathbb{C}^3$

$$\mathcal{V}_{1,\{1\}} = Z((x_2 - p_2)y + p_1 - x_1, (x_1 - p_1)y + x_2 - p_2)$$

having two complex singularities lifting (p_1, p_2), precisely at $(p_1, p_2, \pm\mathfrak{i})$, with $\mathfrak{i}^2 = -1$.

According to Proposition 5, we can desingularize the varieties $\mathcal{V}_{r,\iota}(A)$ by applying a sufficiently generic homotopy

$$A + \varepsilon B = \begin{pmatrix} p_1 - x_1 & x_2 - p_2 \\ x_2 - p_2 & x_1 - p_1 \end{pmatrix} + \varepsilon \begin{pmatrix} b_{11} & b_{12} \\ b_{12} & b_{22} \end{pmatrix}$$

perturbing the constant term of A. The set $\mathcal{V}_{r,\iota}(A + \varepsilon B)$ is smooth and equidimensional for generic B, and the expected number of critical points of the restriction of a generic linear function $\ell(x_1, x_2) = \ell_1 x_1 + \ell_2 x_2$ is finite for each ε.

In Figure 1 we plot the semi-algebraic curve of solutions to the perturbed systems for a fixed linear objective function. Eliminating variables y and z from the Lagrange system $\mathrm{Lag}_{r,\iota}(A + \varepsilon B)$, one gets a one-dimensional complex curve, representing the Zariski closure of the red curves in Figure 1.

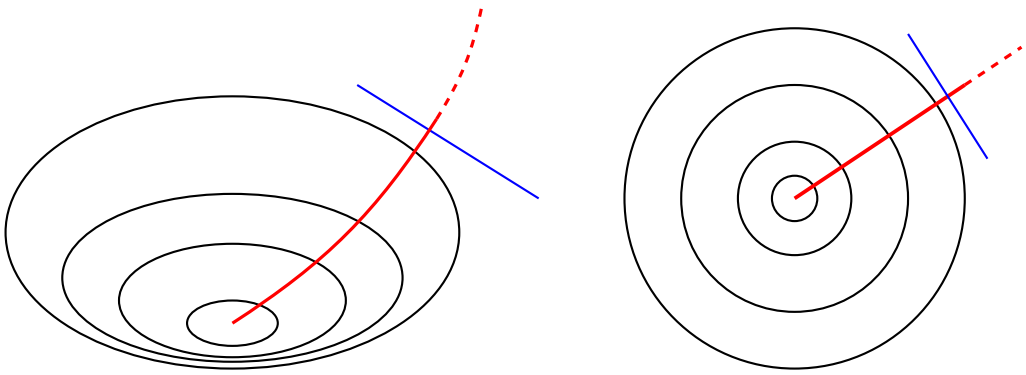

Figure 1: Homotopy curves in red and linear objective function in blue, for generic B (left) and for $B = \mathbb{I}_2$ (right)

For the special choice $B = \mathbb{I}_2$, the real trace of the homotopy curve is the line orthogonal to ℓ, that is parallel to the zero set of $\ell^\perp(x_1, x_2) = \ell_2 x_1 - \ell_1 x_2$ and passing through (p_1, p_2), while if B is drawn randomly the homotopy curve has degree 2. For instance, for $(p_1, p_2) = (1, 1)$, the homotopy curve constructed by DegenerateSDP is given by the equality

$$2241769\, x_1^2 + 115046296\, x_1 x_2 + 65669911\, x_2^2 - 119529834\, x_1 - 246386118\, x_2 + 182957976 = 0$$

where $\ell(x_1, x_2) = 88x_1 - 94x_2$ is the objective function, and with perturbation matrix

$$B = \begin{pmatrix} 80 & -68 \\ -68 & 109 \end{pmatrix}.$$

We finally remark that, even if the choice $B = \mathbb{I}_2$ exhibits a degenerate behaviour in the sense described above, from the point of view of the homotopy constructed in this work $B = \mathbb{I}_2$ exhibits a generic behaviour: one can check by hand that the incidence variety $\mathcal{V}_{r,\iota}(A + \varepsilon\mathbb{I}_2)$ is singular if and only if $\varepsilon = 0$. Indeed, $\mathcal{V}_{r,\iota}(A + \varepsilon\mathbb{I}_2)$ is defined by the vanishing of $f^{(\varepsilon)} = (\varepsilon - x_1 + x_2 y, x_2 + \varepsilon y + x_1 y)$, and the 2×2 minors of $Df^{(\varepsilon)}$ combined with $f^{(\varepsilon)} = 0$ imply that $y = \pm\mathfrak{i}$ and $0 = x_2 = \varepsilon - x_1 = \varepsilon + x_1$ hence $x_1 = x_2 = \varepsilon = 0$.

References

[1] X. Allamigeon, P. Benchimol, S. Gaubert, and M. Joswig, *Long and winding central paths*, arXiv preprint arXiv:1405.4161, (2014).

[2] X. Allamigeon, S. Gaubert, and M. Skomra, *Solving generic nonarchimedean semidefinite programs using stochastic game algorithms*, Proceedings of ISSAC 2016, Waterloo, Canada, (2016).

[3] E. Andersen and K. Andersen, *Mosek: High performance software for large-scale lp, qp, socp, sdp and mip*, __, March, (2013).

[4] M. Anjos and J.-B. Lasserre, *Introduction to semidefinite, conic and polynomial optimization*, in Handbook on semidefinite, conic and polynomial optimization, Springer, 2012, pp. 1–22.

[5] B. Bank, M. Giusti, J. Heintz, and M. Safey El Din, *Intrinsic complexity estimates in polynomial optimization*, Journal of Complexity, (2014), pp. –.

[6] S. Basu, R. Pollack, and M.-F. Roy, *A new algorithm to find a point in every cell defined by a family of polynomials*, in Quantifier elimination and cylindrical algebraic decomposition, Springer-Verlag, 1998.

[7] ——, *Algorithms in real algebraic geometry*, vol. 10 of Algorithms and Computation in Mathematics, Springer-Verlag, second ed., 2006.

[8] G. Blekherman, *Nonnegative polynomials and sums of squares*, Journal of the American Mathematical Society, 25 (2012), pp. 617–635.

[9] G. Blekherman, P. Parrilo, and R. Thomas, *Semidefinite optimization and convex algebraic geometry*, vol. 13, Siam, 2013.

[10] J. Bochnak, M. Coste, and M.-F. Roy, *Real algebraic geometry*, vol. 36 of Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer-Verlag, 1998.

[11] S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan, *Linear matrix inequalities in system and control theory*, vol. 15, Siam, 1994.

[12] M. Demazure, *Bifurcations and catastrophes: geometry of solutions to nonlinear problems*, Springer Science & Business Media, 2013.

[13] M. Giusti, G. Lecerf, and B. Salvy, *A Gröbner-free alternative for polynomial system solving*, Journal of Complexity, 17 (2001), pp. 154–211.

[14] Q. Guo, M. Safey El Din, and L. Zhi, *Computing rational solutions of linear matrix inequalities*, in ISSAC'13, 2013, pp. 197–204.

[15] M. Halická, E. de Klerk, and C. Roos, *On the convergence of the central path in semidefinite optimization*, SIAM Journal on Optimization, 12 (2002), pp. 1090–1099.

[16] D. Henrion, S. Naldi, and M. Safey El Din, *Real root finding for determinants of linear matrices*, Journal of Symbolic Computation, 74 (2015), pp. 205–238.

[17] ——, *Exact algorithms for linear matrix inequalities*, SIAM J. Optim., 26 (2016), pp. 2512–2539.

[18] D. Henrion, S. Naldi, and M. Safey El Din, *Exact algorithms for linear matrix inequalities*, SIAM Journal on Optimization, 26 (2016), pp. 2512–2539. cited By 0.

[19] D. Henrion, S. Naldi, and M. Safey El Din, *Spectra: a Maple library for solving linear matrix inequalities in exact arithmetic*, Optimization Methods and Software, (2017).

[20] A. Herman, H. Hong, and E. Tsigaridas, *Improving Root Separation Bounds*, Journal of Symbolic Computation, (2017). (to appear).

[21] M. Joldes, J.-M. Muller, and V. Popescu, *Implementation and performance evaluation of an extended precision floating-point arithmetic library for high-accuracy semidefinite programming*, ARITH 2017, London, UK, July 24-26 2017, (2017).

[22] J.-B. Lasserre, *Global optimization with polynomials and the problem of moments*, SIAM J. Optim., 11 (2001), pp. 796–817.

[23] S. Naldi, *Solving rank-constrained semidefinite programs in exact arithmetic*, vol. 20-22-July-2016, Association for Computing Machinery, 2016, pp. 357–364.

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

[25] J. Nie, K. Ranestad, and B. Sturmfels, *The algebraic degree of semidefinite programming*, Mathematical Programming, 122 (2010), pp. 379–405.

[26] P. Parrilo, *Semidefinite programming relaxations for semialgebraic problems*, Mathematical Programming Ser.B, 96 (2003), pp. 293–320.

[27] M. Ramana, *An exact duality theory for semidefinite programming and its complexity implications*, Mathematical Programming, 77 (1997), pp. 129–162.

[28] F. Rouillier, M.-F. Roy, and M. Safey El Din, *Finding at least one point in each connected component of a real algebraic set defined by a single equation*, J. Complexity, 16 (2000), pp. 716–750.

[29] M. Safey El Din, *Testing sign conditions on a multivariate polynomial and applications*, Mathematics in Computer Science, 1 (2007), pp. 177–207.

[30] M. Safey El Din and E. Schost, *Polar varieties and computation of one point in each connected component of a smooth real algebraic set*, in ISSAC'03, ACM, 2003, pp. 224–231.

[31] M. Safey El Din and E. Schost, *A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets*, Journal of the ACM, 63 (2017).

[32] M. Safey El Din and É. Schost, *Bit complexity for multi-homogeneous polynomial system solving - application to polynomial minimization*, Journal of Symbolic Computation, 87 (2018), pp. 176 – 206.

[33] M. Safey El Din and L. Zhi, *Computing rational points in convex semialgebraic sets and sum of squares decompositions*, SIAM Journal on Optimization, 20 (2010), pp. 2876–2889.

[34] C. Scheiderer, *Sums of squares of polynomials with rational coefficients.*, Journal of the European Mathematical Society, 18 (2016), pp. 1495–1513.

[35] É. Schost, *Computing parametric geometric resolutions*, Applicable Algebra in Engineering, Communication and Computing, 13 (2003), pp. 349–393.

[36] J. F. Sturm, *Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones*, Optim. Methods Softw., 11/12 (1999), pp. 625–653.

[37] K.-C. Toh, M. Todd, and R. Tütüncü, *Sdpt3 – a matlab software package for semidefinite programming, version 1.3*, Optimization methods and software, 11 (1999), pp. 545–581.