Exact algorithms for linear matrix inequalities

Didier Henrion, Simone Naldi, Mohab Safey El Din

Exact algorithms for linear matrix inequalities

Didier Henrion* Simone Naldi† Mohab Safey El Din‡

September 9, 2016

Abstract

Let $A(x) = A_0 + x_1A_1 + \cdots + x_nA_n$ be a linear matrix, or pencil, generated by given symmetric matrices $A_0, A_1, \ldots, A_n$ of size m with rational entries. The set of real vectors x such that the pencil is positive semidefinite is a convex semi-algebraic set called spectrahedron, described by a linear matrix inequality (LMI). We design an exact algorithm that, up to genericity assumptions on the input matrices, computes an exact algebraic representation of at least one point in the spectrahedron, or decides that it is empty. The algorithm does not assume the existence of an interior point, and the computed point minimizes the rank of the pencil on the spectrahedron. The degree d of the algebraic representation of the point coincides experimentally with the algebraic degree of a generic semidefinite program associated to the pencil. We provide explicit bounds for the complexity of our algorithm, proving that the maximum number of arithmetic operations that are performed is essentially quadratic in a multilinear Bézout bound of d. When m (resp. n) is fixed, such a bound, and hence the complexity, is polynomial in n (resp. m). We conclude by providing results of experiments showing practical improvements with respect to state-of-the-art computer algebra algorithms.

Keywords: linear matrix inequalities, semidefinite programming, computer algebra algorithms, symbolic computation, polynomial optimization.

1 Introduction

Let $\mathbb{S}_m(\mathbb{Q})$ be the vector space of $m \times m$ symmetric matrices with entries in $\mathbb{Q}$. Let $A_0, A_1, \ldots, A_n \in \mathbb{S}_m(\mathbb{Q})$ and $A(x) = A_0 + x_1A_1 + \cdots + x_nA_n$ be the associated *linear matrix*, $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$. We also denote the tuple $(A_0, A_1, \ldots, A_n)$ by $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$. For $x \in \mathbb{R}^n$, $A(x)$ is symmetric, with real entries, and hence its eigenvalues are real numbers.

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

†LAAS-CNRS, Université de Toulouse, CNRS, Toulouse, France.

‡Sorbonne Universités, UPMC Univ Paris 06, CNRS, INRIA Paris Center, LIP6, Equipe PolSys, F-75005, Paris, France.

The central object of this paper is the subset of $x \in \mathbb{R}^n$ such that the eigenvalues of $A(x)$ are all nonnegative, that is the *spectrahedron*

$$\mathscr{S} = \{x \in \mathbb{R}^n : A(x) \succeq 0\}.$$

Here $\succeq 0$ means "positive semidefinite" and $A(x) \succeq 0$ is called a *linear matrix inequality* (LMI). The set $\mathscr{S}$ is convex closed basic semi-algebraic. This paper addresses the following decision problem for the spectrahedron $\mathscr{S}$:

Problem 1 (Feasibility of semidefinite programming) *Compute an exact algebraic representation of at least one point in $\mathscr{S}$, or decide that $\mathscr{S}$ is empty.*

We present a probabilistic exact algorithm for solving Problem (1). The algorithm depends on some assumptions on input data that are specified later. If $\mathscr{S}$ is not empty, the expected output is a *rational parametrization* (see e.g. [55]) of a finite set $\mathcal{Z} \subset \mathbb{C}^n$ meeting $\mathscr{S}$ in at least one point x^*. This is given by a vector $(q_0, \ldots, q_{n+1}) \subset \mathbb{Z}[t]^{n+2}$ and a linear form $\lambda = \lambda_1 x_1 + \cdots + \lambda_n x_n \in \mathbb{Q}[t]$ such that $\deg(q_{n+1}) = \sharp\mathcal{Z}$, $\deg(q_i) < \deg(q_{n+1})$ for $0 \leq i \leq n$, $\gcd(q_{n+1}, q_0) = 1$ and $\mathcal{Z}$ coincides with the set

$$\{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid t = \lambda_1 x_1 + \cdots + \lambda_n x_n, q_{n+1}(t) = 0, x_i = q_i(t)/q_0(t)\} \qquad (1)$$

A few remarks on this representation are in order. Usually, q_0 is taken as $\frac{\partial q_{n+1}}{\partial t}$ for a better control on the size of the coefficients [14, Theorem 1] – see also the introductory discussion of that theorem in [14]. More precisely, if D bounds the degrees of a finite family of polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$ defining $\mathcal{Z}$ and h bounds the bit size of their coefficients and those of λ, then the coefficients of a rational parametrization encoding $\mathcal{Z}$ have bit size bounded by hD^n.

This is to be compared with polynomial parametrizations where the rational fractions q_i/q_0 are replaced by polynomials p_i; they are obtained by inverting q_0 w.r.t. q_{n+1} using the extended Euclidean algorithm. That leads to polynomials p_i with bit size bounded by hD^{2n}.

In order to compute such representations, the usual and efficient strategy is to compute first the image of such representations in a prime field and next use a Newton-Hensel lifting to recover the integers. According to [23, Lemma 4] and the above bounds, the cost of lifting integers is log-linear in the output size. Since in the case of polynomial parametrizations, the output size may be D^n times larger than in the case of rational parametrizations, rational parametrizations are easier to compute. In addition, observe from [45, Lemma 3.4 and Theorem 3.12] that isolating boxes for the real points in $\mathcal{Z}$ from rational or polynomial representations have the same bit complexity (e.g. cubic in the degree of q and log-linear in the maximum bit size of the coefficients in the parametrization).

As an outcome of designing our algorithm, we also compute the minimum rank attained by the pencil on the spectrahedron. Moreover, since the points in $\mathcal{Z}$ are in one-to-one correspondence with the roots of q_{n+1}, from this representation the coordinates of the feasible point $x^* \in \mathscr{S}$ can be computed with arbitrary precision by isolating the corresponding solution t^* of the univariate equation $q_{n+1}(t) = 0$. If $\mathscr{S}$ is empty, the expected output is the empty list.

1.1 Motivations

Semidefinite programming models a large number of problems in the applications [53, 10, 8]. This includes one of the most important questions in computational algebraic geometry, that is the general polynomial optimization problem. Indeed, Lasserre [42] proved that the problem of minimizing a polynomial function over a semi-algebraic set can be relaxed to a sequence of primal-dual semidefinite programs called LMI relaxations, and that under mild assumptions the sequence of solutions converge to the original minimum. Generically, solving a non-convex polynomial optimization problem amounts to solving a finite-dimensional convex semidefinite programming problem [47]. Numerical algorithms following this approach are available and, typically, guarantees of their convergence are related to the feasibility (or strict feasibility) of the LMI relaxations. It is, in general, a challenge to obtain exact algorithms for deciding whether the feasible set of a semidefinite programming (SDP) problem

$$\min_{x\in\mathbb{R}^n} \sum_{i=1}^{n} c_i x_i \qquad \text{s.t. } A(x) \succeq 0 \tag{2}$$

is empty or not. The feasible set of the SDP (2) is defined by an LMI and hence it is a spectrahedron. Problem (1) amounts to solving the feasibility problem for semidefinite programming, in exact arithmetic: given a $\mathbb{Q}-$definable semidefinite program as in (2) (that is, we suppose that the coefficients of $A(x)$ have rational entries), decide whether the feasible set $\mathscr{S} = \{x \in \mathbb{R}^n : A(x) \succeq 0\}$ is empty or not, and compute exactly at least one feasible point. We would like to emphasize the fact that we do not assume the existence of an interior point in $\mathscr{S}$. Quite the opposite, we are especially interested in degenerate cases for which the maximal rank achieved by the pencil $A(x)$ in $\mathscr{S}$ is small.

This work is a first step towards an exact approach to semidefinite programming. In particular, a natural perspective of this work is to design exact algorithms for deciding whether the minimum in (2) is attained or not, and for computing such a minimum in the affirmative case. While the number of iterations performed by the ellipsoid algorithm [27] to compute the approximation of a solution of (2) is polynomial in the number of variables, once the accuracy is fixed, no analogous results for exact algorithms are available. Moreover, since the intrinsic complexity of the optimization problem (2) is related to its algebraic degree δ as computed in [48, 24], the paramount goal is to design algorithms whose runtime is polynomial in δ. The algorithm of this paper shows experimentally such an optimal behavior with respect to δ.

We finally recall that solving LMIs is a basic subroutine of computer algorithms in systems control and optimization, especially in linear systems robust control [9, 33], but also for the analysis or synthesis of nonlinear dynamical systems [67], or in nonlinear optimal control with polynomial data [37, 11].

1.2 Contribution and outline

We design a computer algebra algorithm for solving the feasibility problem of semidefinite programming, that is Problem (1), in exact arithmetic. Let us clarify that we do not

claim that an exact algorithm can be competitive with a numerical algorithm in terms of admissible size of input problems: indeed, SDP solvers based on interior-point methods [7, 46] can nowadays handle inputs with a high number of variables that are out of reach for our algorithms. Our contribution can be summarized as follows:

1. we show that the geometry of spectrahedra understood as semi-algebraic sets with determinantal structure can be exploited to design dedicated computer algebra algorithms;

2. we give explicit complexity and output-degree upper bounds for computer algebra algorithms solving exactly the feasibility problem of semidefinite programming; our algorithm is probabilistic and works under assumptions on the input, which are generically satisfied;

3. we provide results of practical experiments showing the gain in terms of computational timings of our contribution with respect to the state of the art in computer algebra;

4. remarkably, our algorithm does not assume that the input spectrahedron $\mathscr{S} = \{x \in \mathbb{R}^n : A(x) \succeq 0\}$ is full-dimensional, and hence it can tackle also examples with empty interior.

The main idea is to exploit the relation between the geometry of spectrahedra, and that of the determinantal varieties associated to the input symmetric pencil $A(x)$. Let us introduce, for $r = 0, \ldots, m-1$, the algebraic sets

$$\mathcal{D}_r = \{x \in \mathbb{C}^n : \text{rank } A(x) \leq r\}.$$

These define a nested sequence $\mathcal{D}_0 \subset \mathcal{D}_1 \subset \cdots \subset \mathcal{D}_{m-1}$. The dimension of $\mathcal{D}_r$ for generic linear matrices A is known, and equals $n - \binom{m-r+1}{2}$ (see Lemma 4). The Euclidean boundary $\partial\mathscr{S}$ of $\mathscr{S}$ is included in the real trace of the last algebraic set of the sequence: $\partial\mathscr{S} \subset \mathcal{D}_{m-1} \cap \mathbb{R}^n$. In particular, for $x \in \partial\mathscr{S}$, the matrix $A(x)$ is singular and one could ask which elements of the real nested sequence $\mathcal{D}_0 \cap \mathbb{R}^n \subset \cdots \subset \mathcal{D}_{m-1} \cap \mathbb{R}^n$ intersect $\partial\mathscr{S}$.

Notation 1 *If $\mathscr{S} = \{x \in \mathbb{R}^n : A(x) \succeq 0\}$ is not empty, we define the integer $r(A) = \min\{\text{rank } A(x) : x \in \mathscr{S}\}$.*

When $\mathscr{S}$ is not empty, $r(A)$ equals the minimum integer r such that $\mathcal{D}_r \cap \mathbb{R}^n$ intersects $\mathscr{S}$. We present our first main result, which states that $\mathscr{S}$ contains at least one of the connected components of the real algebraic set $\mathcal{D}_{r(A)} \cap \mathbb{R}^n$. We denote by $\mathbb{S}_m^{n+1}(\mathbb{Q}) = \mathbb{S}_m(\mathbb{Q}) \times \cdots \times \mathbb{S}_m(\mathbb{Q})$ the $(n+1)-$fold Cartesian product of $\mathbb{S}_m(\mathbb{Q})$.

Theorem 2 (Smallest rank on a spectrahedron) *Suppose that $\mathscr{S} \neq \emptyset$. Let $\mathcal{C}$ be a connected component of $\mathcal{D}_{r(A)} \cap \mathbb{R}^n$ such that $\mathcal{C} \cap \mathscr{S} \neq \emptyset$. Then $\mathcal{C} \subset \mathscr{S}$ and hence $\mathcal{C} \subset (\mathcal{D}_{r(A)} \setminus \mathcal{D}_{r(A)-1}) \cap \mathbb{R}^n$.*

We give a proof of Theorem 2 in Section 2. From Theorem 2, we deduce the following mutually exclusive conditions on the input symmetric linear pencil A: either $\mathscr{S} = \emptyset$, or $\mathscr{S}$ contains one connected component $\mathcal{C}$ of $\mathcal{D}_{r(A)} \cap \mathbb{R}^n$. Consequently, an exact algorithm whose output is one point in the component $\mathcal{C} \subset \mathscr{S} \cap \mathcal{D}_{r(A)}$ would be sufficient for our goal. Motivated by this fact, we design in Section 3.2 an exact algorithm computing one point in each connected component of $\mathcal{D}_r \cap \mathbb{R}^n$, for $r \in \{0, \ldots, m-1\}$.

The strategy to compute sample points in $\mathcal{D}_r \cap \mathbb{R}^n$ is to build an algebraic set $\mathcal{V}_r \subset \mathbb{C}^{n+m(m-r)}$ whose projection on the first n variables is contained in $\mathcal{D}_r$. This set is defined by the incidence bilinear relation $A(x)Y(y) = 0$ where $Y(y)$ is a full-rank $m \times (m-r)$ linear matrix whose columns generate the kernel of $A(x)$ (*cf.* Section 3.1). Unlike $\mathcal{D}_r$, the incidence variety $\mathcal{V}_r$, up to genericity conditions on the matrices $A_0, A_1, \ldots, A_n$, turns to be generically smooth and equidimensional. The next theorem presents a complexity result for an exact algorithm solving Problem (1) under these genericity assumptions.

Theorem 3 (Exact algorithm for LMI) *Suppose that for $0 \leq r \leq m-1$, the incidence variety $\mathcal{V}_r$ is smooth and equidimensional and that its defining polynomial system generates a radical ideal. Suppose that $\mathcal{D}_r$ has the expected dimension $n - \binom{m-r+1}{2}$. There is a probabilistic algorithm that takes A as input and returns:*

1. *either the empty list, if and only if $\mathscr{S} = \emptyset$, or*
2. *a vector x^* such that $A(x^*) = 0$, if and only if the linear system $A(x) = 0$ has a solution, or*
3. *a rational parametrization $q = (q_0, \ldots, q_{n+1}) \subset \mathbb{Z}[t]$ such that there exists $t^* \in \mathbb{R}$ with $q_{n+1}(t^*) = 0$ and:*
   - *$A(q_1(t^*)/q_0(t^*), \ldots, q_n(t^*)/q_0(t^*)) \succeq 0$ and*
   - *$\operatorname{rank} A(q_1(t^*)/q_0(t^*), \ldots, q_n(t^*)/q_0(t^*)) = r(A)$.*

The number of arithmetic operations performed are in

$$O^{\sim}\left(n\binom{\frac{m^2+m}{2}+n}{n}^6 \sum_{r \leq m-1}\binom{m}{r}\left(n+(m-r)(m+3r)\right)^7\right).$$

If $\mathscr{S} \neq \emptyset$, the degree of q is in $\mathcal{O}\left(\binom{\frac{m^2+m}{2}+n}{n}^3\right)$.

An important aspect of our contribution can be read from the complexity and degree bounds in Theorem 3: indeed, remark that when m is fixed, both the output degree and the complexity of the algorithm are polynomial functions of n. Viceversa, by the constraint $n \geq \binom{m-r+1}{2}$ (given by Lemma 4), one also easily deduces that when n is fixed, the complexity is polynomial in m.

The algorithm of Theorem 3 is described in Section 3. Its probabilistic nature comes from random changes of variables performed during the procedure, allowing to put the sets $\mathcal{D}_r$

in generic position. We prove that for generic choices of parameters the output of the algorithm is correct.

A complexity analysis is performed in Section 5. Bounds in Theorem 3 are explicit expressions involving m and n. These are computed by exploiting the multilinearity of intermediate polynomial systems generated during the procedure, and are not sharp in general. By experiments on randomly generated symmetric pencils, reported in Section 6, we observe that the output degree coincides with the algebraic degree of generic semidefinite programs, that is with data given in [48, Table 2]: this evidences the optimality of our approach. We did not succeed in proving exact formulas for such degrees.

1.3 Related works

On input A, $\mathscr{S}$ can be defined by m polynomial inequalities in $\mathbb{Q}[x_1, \ldots, x_n]$ of degree $\leq m$ (see e.g. [51]). As far as we know, the state-of-the-art for designing algorithms deciding the emptiness of $\mathscr{S}$ consists only of algorithms for deciding the emptiness of general semi-algebraic sets; our contribution being the first attempt to exploit structural properties of the problem, e.g. through the smallest rank property (Theorem 2).

A first algorithmic solution to deciding the emptiness of general semi-algebraic sets is given by Cylindrical Algebraic Decomposition algorithm [12]; however its runtime is doubly exponential in the number n of variables. The first singly exponential algorithm is given in [26], and has led to a series of works (see e.g. [54, 31]) culminating with algorithms designed in [5] based on the so-called critical points method. This method is based on the general idea which consists in computing minimizers/maximizers of a well-chosen function reaching its extrema in each connected component of the set under study. Applying [5] to problem (1) requires $m^{O(n)}$ bit operations. Note that our technique for dealing with sets $\mathcal{V}_r$ is based on the idea underlying the critical point method. Also, in the arithmetic complexity model, our complexity estimates are more precise (the complexity constant in the exponent is known) and better. This technique is also related to algorithms based on polar varieties for grabbing sample points in semi-algebraic sets; see for example [2, 3, 58, 59] and its application to polynomial optimization [25].

To get a purely algebraic certificate of emptiness for $\mathscr{S}$, one could use the classical approach by Positivstellensatz [43, 52, 64]. As a snake biting its tail, this would lead to a family, or hierarchy, of semidefinite programs [42]. Bounds for the degree of Positivstellensatz certificates are exponential in the number of variables and have been computed in [65] for Schmudgen's, and in [49] for Putinar's formulation. In the recent remarkable result [44], a uniform 5−fold exponential bound for the degree of the Hilbert 17th problem is provided. In [41], an emptiness certificate dedicated to the spectrahedral case, by means of special quadratic modules associated to these sets, is obtained.

All the above algorithms do not exploit the particular structure of spectrahedra understood as determinantal semi-algebraic sets. In [40], the authors showed that deciding emptiness of $\mathscr{S}$ can be done in time $\mathcal{O}(nm^4) + m^{\mathcal{O}(\min(n,m^2))}$, that is in polynomial time in m (resp. linear time in n) if n (resp. m) is fixed. The main drawback of this algorithm is that it is based on general procedures for quantifier elimination, and hence it does not lead to efficient practical implementations. Note also that the complexity constant in the

exponent is still unknown.

Also, in [28], a version of [57] dedicated to spectrahedra exploiting some of their structural properties, decides whether a linear matrix inequality $A(x) \succeq 0$ has a rational solution, that is whether $\mathscr{S}$ contains a point with coordinates in $\mathbb{Q}$. Remark that such an algorithm is not sufficient to solve our problem, since, in some degenerate but interesting cases, $\mathscr{S}$ is not empty but does not contain rational points: in Section 6.2 we will illustrate the application of our algorithm to one of these examples.

As suggested by the smallest rank property, determinantal structures play an important role in our algorithm. This structure has been recently exploited in [18] and [22] for the fast computation of Gröbner bases of zero-dimensional determinantal ideals and computing zero-dimensional critical loci of maps restricted to varieties in the generic case.

Exploiting determinantal structures for determinantal situations remained challenging for a long time. In [34] we designed a dedicated algorithm for computing sample points in the real solution set of the determinant of a square linear matrix. This has been extended in [36] to real algebraic sets defined by rank constraints on a linear matrix. Observe that this problem looks similar to the ones we consider thanks to the smallest rank property. As in this paper, the traditional strategy consists in studying incidence varieties for which smoothness and regularity properties are proved under some *genericity assumptions* on the input linear matrix.

Hence, in the case of symmetric matrices, these results cannot be used anymore. Because of the structure of the matrix, the system defining the incidence variety involves too many equations; some of them being redundant. Hence, these redundancies need to be eliminated to characterize critical points on incidence varieties in a convenient way. In the case of Hankel matrices, the special structure of their kernel provides an efficient way to do that. This case study is done in [35]. Yet, the problem of eliminating these redundancies remained unsolved in the general symmetric case and this is what we do in Section 3 which is the starting point of the design of our dedicated algorithm.

1.4 Basic notation

We refer to [6, 13, 30, 16] for the algebraic-geometric background of this paper. We recall below some basic definitions and notation. We denote by $\mathbb{M}_{p,q}(\mathbb{Q})$ the space of $p \times q$ rational matrices, and $\mathrm{GL}_n(\mathbb{C})$ the set of $n \times n$ non-singular matrices. The transpose of $M \in \mathbb{M}_{p,q}(\mathbb{Q})$ is M^T. The cardinality of a finite set T (resp. the number of entries of a vector v) are denoted by $\sharp T$ (resp. $\sharp v$).

Let $x = (x_1, \ldots, x_n)$. A vector $f = (f_1, \ldots, f_s) \subset \mathbb{Q}[x]$ is a polynomial system, $\langle f \rangle \subset \mathbb{Q}[x]$ its ideal and $Z(\langle f \rangle) = \{x \in \mathbb{C}^n : f_i(x) = 0, i = 1, \ldots, s\}$ the associated algebraic set. Sets $Z(\langle f \rangle)$ define the collection of closed sets of the Zariski topology of $\mathbb{C}^n$. The intersection of a Zariski closed and a Zariski open set is called a locally closed set. For $M \in \mathrm{GL}_n(\mathbb{C})$ and $\mathcal{Z} \subset \mathbb{C}^n$, let $M^{-1}\mathcal{Z} = \{x \in \mathbb{C}^n : M\,x \in \mathcal{Z}\}$. With $I(S)$ we denote the ideal of polynomials vanshing on $S \subset \mathbb{C}^n$.

Let $f = (f_1, \ldots, f_s) \subset \mathbb{Q}[x]$. Its Jacobian matrix is denoted by $Df = (\partial f_i/\partial x_j)_{i,j}$. An algebraic set $\mathcal{Z} \subset \mathbb{C}^n$ is irreducible if $\mathcal{Z} = \mathcal{Z}_1 \cup \mathcal{Z}_2$ where $\mathcal{Z}_1, \mathcal{Z}_2$ are algebraic sets,

implies that either $\mathcal{Z} = \mathcal{Z}_1$ or $\mathcal{Z} = \mathcal{Z}_2$. Any algebraic set is the finite union of irreducible algebraic sets, called its irreducible components. The codimension c of an irreducible algebraic set $\mathcal{Z} \subset \mathbb{C}^n$ is the maximum rank of Df on $\mathcal{Z}$, where $I(\mathcal{Z}) = \langle f \rangle$. Its dimension is $n - c$. If all the irreducible components of $\mathcal{Z}$ have the same dimension, we say that $\mathcal{Z}$ is equidimensional. The dimension of an algebraic set $\mathcal{Z}$ is the maximum of the dimensions of its irreducible components, and it is denoted by $\dim \mathcal{Z}$. The degree of an equidimensional algebraic set $\mathcal{Z}$ of codimension c is the maximum cardinality of finite intersections $\mathcal{Z} \cap \mathcal{L}$ where $\mathcal{L}$ is a linear space of dimension c. The degree of an algebraic set is the sum of the degrees of its equidimensional components.

Let $\mathcal{Z} \subset \mathbb{C}^n$ be equidimensional of codimension c, and let $I(\mathcal{Z}) = \langle f_1, \ldots, f_s \rangle$. The singular locus of $\mathcal{Z}$, denoted by $\operatorname{sing}(\mathcal{Z})$, is the algebraic set defined by $f = (f_1, \ldots, f_s)$ and by all $c \times c$ minors of Df. If $\operatorname{sing}(\mathcal{Z}) = \emptyset$ we say that $\mathcal{Z}$ is smooth, otherwise singular. The points in $\operatorname{sing}(\mathcal{Z})$ are called singular, while points in $\operatorname{reg}(\mathcal{Z}) = \mathcal{Z} \setminus \operatorname{sing}(\mathcal{Z})$ are called regular. Let $\mathcal{Z} \subset \mathbb{C}^n$ be smooth and equidimensional of codimension c, and let $I(\mathcal{Z}) = \langle f_1, \ldots, f_s \rangle$. Let $g : \mathbb{C}^n \to \mathbb{C}^m$ be an algebraic map. The set of critical points of the restriction of g to $\mathcal{Z}$ is the algebraic set denote by $\operatorname{crit}(g, \mathcal{Z})$ and defined by $f = (f_1, \ldots, f_s)$ and by all $c + m$ minors of the Jacobian matrix $D(f, g)$. The points in $g(\operatorname{crit}(g, \mathcal{Z}))$ are called critical values, while points in $\mathbb{C}^m \setminus g(\operatorname{crit}(g, \mathcal{Z}))$ are called the regular values, of the restriction of g to $\mathcal{Z}$.

2 The smallest rank on a spectrahedron

We prove Theorem 2, which relates the geometry of linear matrix inequalities to the rank stratification of the defining symmetric pencil. We believe that the statement of this theorem is known to the community of researchers working on real algebraic geometry and semidefinite optimization; however, we did not find any explicit reference in the literature.

Proof of Theorem 2: By assumption, the rank of $A(x)$ on $\mathscr{S}$ is greater or equal than $r(A)$. We consider the vector function $e = (e_1, \ldots, e_m) : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ where $e_1(x) \leq \ldots \leq e_m(x)$ are the ordered eigenvalues of $A(x)$. Let $\mathcal{C}$ be a connected component of $\mathcal{D}_{r(A)} \cap \mathbb{R}^n$ such that $\mathcal{C} \cap \mathscr{S} \neq \emptyset$, and let $x \in \mathcal{C} \cap \mathscr{S}$. One has $\operatorname{rank} A(x) = r(A)$ and $e_1(x) = \ldots = e_{m-r(A)}(x) = 0 < e_{m-r(A)+1}(x) \leq \ldots \leq e_m(x)$. Suppose *ad absurdum* that there exists $y \in \mathcal{C}$ such that $y \notin \mathscr{S}$. In particular, one eigenvalue of $A(y)$ is strictly negative.

Let $g\colon [0,1] \to \mathcal{C}$ be a continuous semi-algebraic map such that $g(0) = x$ and $g(1) = y$. This map exists since $\mathcal{C}$ is a connected component of a real algebraic set. The image $g([0,1])$ is compact and semi-algebraic. Let

$$T = \{t \in [0,1] : g(t) \in \mathscr{S}\} = g^{-1}(g([0,1]) \cap \mathscr{S}).$$

Since g is continuous, $T \subset [0,1]$ is closed. So it is a finite union of closed intervals. Since $0 \in T$ ($g(0) = x \in \mathscr{S}$) there exists $t_0 \in [0,1]$ and $N \in \mathbb{N}$ such that $[0, t_0] \in T$ and for all $p \geq N$, $t_0 + \frac{1}{p} \notin T$. One gets that $g(t_0) = \tilde{x} \in \mathscr{S}$ and that for all $p \geq N$, $g(t_0 + \frac{1}{p}) = \tilde{x}_p \notin \mathscr{S}$. By definition, $\tilde{x}, \tilde{x}_p \in \mathcal{C} \subset \mathcal{D}_{r(A)} \cap \mathbb{R}^n$ for all $p \geq N$, and since $\tilde{x} \in \mathscr{S}$, we get $\operatorname{rank} A(\tilde{x}) = r(A)$ and $\operatorname{rank} A(\tilde{x}_p) \leq r(A)$ for all $p \geq N$. We also get that

rank $A(g(t)) = r(A)$ for all $t \in [0, t_0]$. We finally have $\tilde{x}_p \to \tilde{x}$ when $p \to +\infty$, since g is continuous. There exists a map

$$\varphi\colon \Big\{p \in \mathbb{N} : p \geq N\Big\} \to \mathbb{Z}$$

which assigns to p the index of eigenvalue-function among $e_1, \ldots, e_m$ corresponding to the maximum strictly negative eigenvalue of $A(\tilde{x}_p)$, if it exists, otherwise it assigns 0. Remark that since rank $A(\tilde{x}_p) \leq r(A)$ for all p, then $\varphi(p) \leq r(A)$ for all p. In other words, the eigenvalues of $A(\tilde{x}_p)$ satisfy

$$\begin{aligned} e_1(\tilde{x}_p) \leq \ldots \leq e_{\varphi(p)}(\tilde{x}_p) < 0 = e_{\varphi(p)+1}(\tilde{x}_p) = \ldots = e_{\varphi(p)+m-r(A)}(\tilde{x}_p) \\ 0 \leq e_{\varphi(p)+m-r(A)+1}(\tilde{x}_p) \leq \ldots \leq e_m(\tilde{x}_p), \end{aligned}$$

for $p \geq N$. Since the sequence $\{\varphi(p)\}_{p \geq N}$ is bounded, up to taking a subsequence, it admits at least a limit point by the Bolzano-Weierstrass Theorem [4, Th. 3.4.8], this point is an integer, and $j \mapsto \varphi(j)$ is constant for large j. Suppose that there exists a limit point $\ell > 0$, and let $\{p_j\}_{j \in \mathbb{N}}$ such that $\varphi(p_j) \to \ell$ and that for $j \geq N'$, $j \mapsto \varphi(p_j)$ is constant. Thus, $0 = e_{\ell+1}(\tilde{x}_{p_j}) = \ldots = e_{\ell+m-r(A)}(\tilde{x}_{p_j})$ for all $j \geq N'$. Since $\tilde{x}_{p_j} \to \tilde{x}$, and since $e_1, \ldots, e_m$ are continuous functions, we obtain that $\ell = 0$ is the unique limit point of φ, hence φ converges to 0. Hence $\varphi \equiv 0$ for large p. This contradicts the fact that $\tilde{x}_p \notin \mathscr{S}$ for large p.

We conclude that the set $\mathcal{C} \setminus \mathscr{S}$ is empty, that is $\mathcal{C} \subset \mathscr{S}$. By the minimality of the integer $r(A)$ in $\{\text{rank } A(x) : x \in \mathscr{S}\}$, one deduces that $\mathcal{C} \subset (\mathcal{D}_{r(A)} \setminus \mathcal{D}_{r(A)-1}) \cap \mathbb{R}^n$. □

3 Algorithm

Our algorithm is called SolveLMI, and it is presented in Section 3.3. Before, we describe in Section 3.2 its main subroutine LowRankSym, which is of recursive nature and computes one point per connected component of the real algebraic set $\mathcal{D}_r \cap \mathbb{R}^n$. We start, in the next section, with some preliminaries.

3.1 Preliminaries

Expected dimension of low rank loci

We first recall a known fact about the dimension of $\mathcal{D}_r$, when A is a generic symmetric pencil.

Lemma 4 *There exists a non-empty Zariski open subset $\mathscr{A} \subset \mathbb{S}_m^{n+1}(\mathbb{C})$ such that, if $A \in \mathscr{A} \cap \mathbb{S}_m^{n+1}(\mathbb{Q})$, for all $r = 0, \ldots, m-1$, the set $\mathcal{D}_r$ is either empty or it has dimension $n - \binom{m-r+1}{2}$.*

Proof : The proof is classical and can be found *e.g.* in [1, Prop. 3.1]. □

Incidence varieties

Let $A(x)$ be a symmetric $m \times m$ linear matrix, and let $0 \leq r \leq m-1$. Let $y = (y_{i,j})_{1 \leq i \leq m, 1 \leq j \leq m-r}$ be unknowns. Below, we build an algebraic set whose projection on the $x-$space is contained in $\mathcal{D}_r$. Let

$$Y(y) = \begin{pmatrix} y_{1,1} & \cdots & y_{1,m-r} \\ \vdots & & \vdots \\ y_{m,1} & \cdots & y_{m,m-r} \end{pmatrix},$$

and let $\iota = \{i_1, \ldots, i_{m-r}\} \subset \{1, \ldots, m\}$, with $\sharp \iota = m-r$. We denote by Y_ι the $(m-r) \times (m-r)$ sub-matrix of $Y(y)$ obtained by isolating the rows indexed by ι. There are $\binom{m}{r}$ such matrices. We define the set

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

We denote by $f(A, \iota)$, or simply by f, when there is no ambiguity on ι, the polynomial system defining $\mathcal{V}_r(A, \iota)$. We often consider linear changes of variables x: for $M \in \mathrm{GL}_n(\mathbb{C})$, $f(A \circ M, \iota)$ denotes the entries of $A(M\,x)Y(y)$ and $Y_\iota - \mathbb{I}_{m-r}$, and by $\mathcal{V}_r(A \circ M, \iota)$ its zero set. We also denote by $U_\iota \in \mathbb{M}_{m-r,m}(\mathbb{Q})$ the full rank matrix whose entries are in $\{0, 1\}$, and such that $U_\iota Y(y) = Y_\iota$. By simplicity we call U_ι the *boolean matrix* with multi-index ι.

By definition, the projection of $\mathcal{V}_r(A, \iota)$ on the first n variables is contained in $\mathcal{D}_r$. We remark the similarity between the relation $A(x)Y(y) = 0$ and the so-called *complementarity condition* for a couple of primal-dual semidefinite programs, see for example [48, Th. 3]. The difference in our model is that the special size of $Y(y)$ and the affine constraint $Y_\iota = \mathbb{I}_{m-r}$ force a rank condition on $Y(y)$ and hence on $A(x)$.

Eliminating redundancies

The system $f(A, \iota)$ contains redundancies induced by polynomial relations between its generators. These relations can be explicitly eliminated in order to obtain a minimal polynomial system defining $\mathcal{V}_r$.

Lemma 5 *Let $M \in \mathrm{GL}_n(\mathbb{C})$. Let $\iota \subset \{1, \ldots, m\}$, with $\sharp \iota = m-r$. Let $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$, and $f \in \mathbb{Q}[x, y]^{m(m-r)+(m-r)^2}$ be the polynomial system defined in Section 3.1. Then we can explicitly construct a subsystem $f_{red} \subset f$ of length $m(m-r) + \binom{m-r+1}{2}$ such that $\langle f_{red} \rangle = \langle f \rangle$.*

Proof : In order to simplify notations and without loss of generality we suppose $M = \mathbb{I}_n$ and $\iota = \{1, \ldots, m-r\}$. We substitute $Y_\iota = \mathbb{I}_{m-r}$ in $A(x)Y(y)$, and we denote by $g_{i,j}$ the $(i, j)-$th entry of the resulting matrix. We denote by f_{red} the following system:

$$f_{red} = (g_{i,j} \text{ for } i \geq j,\ Y_\iota - \mathbb{I}_{m-r})\,.$$

We claim that, for $1 \leq i \neq j \leq m-r$, $g_{i,j} \equiv g_{j,i} \mod \langle g_{k,\ell}, k > m-r \rangle$, which implies that f_{red} verifies the statement. Let $a_{i,j}$ denote the $(i,j)-$th entry of $A(x)$. Let $i < j$ and write

$$g_{i,j} = a_{i,j} + \sum_{\ell=m-r+1}^{m} a_{i,\ell} y_{\ell,j} \text{ and } g_{j,i} = a_{j,i} + \sum_{\ell=m-r+1}^{m} a_{j,\ell} y_{\ell,i}.$$

We deduce that $g_{i,j} - g_{j,i} = \sum_{\ell=m-r+1}^{m} a_{i,\ell} y_{\ell,j} - a_{j,\ell} y_{\ell,i}$ since A is symmetric. Also, modulo the ideal $\langle g_{k,\ell},\, k > m-r \rangle$, and for $\ell \geq m-r+1$, one can explicit $a_{i,\ell}$ and $a_{j,\ell}$, by using polynomial relations $g_{\ell,i} = 0$ and $g_{\ell,j} = 0$, as follows:

$$\begin{aligned} g_{i,j} - g_{j,i} &\equiv \sum_{\ell=m-r+1}^{m} \left(- \sum_{t=m-r+1}^{m} a_{\ell,t} y_{t,i} y_{\ell,j} + \sum_{t=m-r+1}^{m} a_{\ell,t} y_{t,j} y_{\ell,i} \right) \equiv \\ &\equiv \sum_{\ell,t=m-r+1}^{m} a_{\ell,t} \left(-y_{t,i} y_{\ell,j} + y_{t,j} y_{\ell,i} \right) \equiv 0 \mod \langle g_{k,\ell},\, k > m-r \rangle . \end{aligned}$$

The previous congruence concludes the proof. □

We prove below in Proposition 7 and in Corollary 11 that, up to genericity assumptions, the ideal $\langle f \rangle = \langle f_{red} \rangle$ is radical and that $\sharp f_{red}$ matches the codimension of $\mathcal{V}_r$. In the next example, we explicitly write down the redundancies shown in Lemma 5 for a simple case.

Example 6 *We consider a 3×3 symmetric matrix of unknowns, and the kernel corresponding to the configuration $\{1,2\} \subset \{1,2,3\}$. Let*

$$\begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \\ f_{31} & f_{32} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_4 & x_5 \\ x_3 & x_5 & x_6 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ y_{31} & y_{32} \end{pmatrix}.$$

We consider the classes of polynomials f_{12}, f_{21} modulo $\langle f_{31}, f_{32} \rangle$, deducing the following linear relation: $f_{12} - f_{21} = y_{32}x_3 - y_{31}x_5 \equiv y_{31}x_6y_{32} - y_{32}x_6y_{31} = 0$.

Lagrange systems

Let $f(A,\iota)$ be the polynomial system defining $\mathcal{V}_r(A,\iota)$. We set $c = m(m-r) + \binom{m-r+1}{2}$ and $e = \binom{m-r}{2}$, so that $\mathcal{V}_r$ is defined by $c = \sharp f_{red}$ polynomial equations, and $e = \sharp f - c$ is the number of redundancies eliminated by Lemma 5. We define, for $M \in \mathrm{GL}_n(\mathbb{C})$, the polynomial system $\ell = \ell(A \circ M, \iota)$, given by the coordinates of the map

$$\begin{aligned} \ell : \ \mathbb{C}^n \times \mathbb{C}^{m(m-r)} \times \mathbb{C}^{c+e} &\longrightarrow \mathbb{C}^{n+m(m-r)+c+e} \\ (x,y,z) &\longmapsto \left(f(A \circ M, \iota), z^T Df(A \circ M, \iota) - (e_1^T, 0) \right), \end{aligned}$$

where $e_1 \in \mathbb{Q}^n$ is the first column of the identity matrix $\mathbb{I}_n$. We also define $\mathcal{Z}(A \circ M, \iota) = Z(\ell(A \circ M, \iota))$. When $\mathcal{V}_r(A \circ M, \iota)$ is smooth and equidimensional, $\mathcal{Z}(A \circ M, \iota)$ encodes the critical points of the restriction of $\Pi_1(x,y) = x_1$ to $\mathcal{V}_r(A \circ M, \iota)$.

Output representation

The output of the algorithm is a rational parametrization $(q_0, \ldots, q_{n+1}) \subset \mathbb{Z}[t]$ such that the finite set defined in (1) contains at least one point on the spectrahedron $\mathscr{S}$.

3.2 Real root finding for symmetric low rank loci

We describe the main subroutine LowRankSym, which is a variant for symmetric pencils of the algorithms in [34, 35, 36]. Its output is a finite set meeting each connected component of $\mathcal{D}_r \cap \mathbb{R}^n$. It takes advantage of the particular properties of the incidence varieties over a symmetric low rank locus, as highlighted by Lemma 5.

Properties

We define the following properties for a given $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$:

Property P_1. We say that A satisfies P_1 if, for all $\iota \subset \{1, \ldots, m\}$, with $\sharp\iota = m - r$, the incidence variety $\mathcal{V}_r(A, \iota)$ is either empty or smooth and equidimensional.

Property P_2. We say that A satisfies P_2 if, for all r, $\mathcal{D}_r$ has the expected dimension $n - \binom{m-r+1}{2}$. Property P_2 holds generically in $\mathbb{S}_m^{n+1}(\mathbb{Q})$, as shown by Lemma 4.

We also define the following property for a polynomial system $f \subset \mathbb{Q}[x]$ and a Zariski open set $\mathscr{O} \subset \mathbb{C}^n$:

Property Q. Suppose that $f \subset \mathbb{Q}[x]$ generates a radical ideal and that it defines an algebraic set of codimension c, and let $\mathscr{O} \subset \mathbb{C}^n$ be a Zariski open set. We say that f satisfies Q in $\mathscr{O}$, if the rank of Df is c in $Z(\langle f \rangle) \cap \mathscr{O}$.

Formal description of LowRankSym

The formal description of our algorithm is given next. It consists of a main algorithm which checks the genericity hypotheses, and of a recursive sub-algorithm called LowRankSymRec.

LowRankSym

Input: $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$, encoded by the $m(m+1)(n+1)/2$ entries of $A_0, A_1, \ldots, A_n$, and an integer $1 \leq r \leq m-1$;

Output: Either the empty list [ ], if and only if $\mathcal{D}_r \cap \mathbb{R}^n = \emptyset$, or an error message stating that the genericity assumptions are not satisfied, or a rational parametrization $q = (q_0, \ldots, q_{n+1}) \subset \mathbb{Z}[t]$, such that for every connected component $\mathcal{C} \subset \mathcal{D}_r \cap \mathbb{R}^n$, with $\mathcal{C} \cap \mathcal{D}_{r-1} = \emptyset$, there exists $t^* \in Z(q_{n+1}) \cap \mathbb{R}$ with $(q_1(t^*)/q_0(t^*), \ldots, q_n(t^*)/q_0(t^*)) \in \mathcal{C}$.

Procedure LowRankSym(A, r)

1. if $n < \binom{m-r+1}{2}$ then
   - if $\dim \mathcal{D}_r = -1$ then return [ ], else return("the input is not generic");
2. for $\iota \subset \{1, \ldots, m\}$ with $\sharp\iota = m - r$ do
   - if IsReg$((A, \iota)) =$ `false` then return("the input is not generic");
3. return(LowRankSymRec(A, r)).

Procedure LowRankSymRec(A, r)

1. choose $M \in \mathrm{GL}_n(\mathbb{Q})$;
2. $q \leftarrow$ [ ]; for $\iota \subset \{1, \ldots, m\}$ with $\sharp\iota = m - r$ do
   - $q_\iota \leftarrow$ Image(Project(RatPar$(\ell(A \circ M, \iota))), M^{-1})$;
   - $q \leftarrow$ Union(q, q_ι);
3. choose $t \in \mathbb{Q}$; $A \leftarrow (A_0 + tA_1, A_2, \ldots, A_n)$;
4. $q' \leftarrow$ Lift(LowRankSymRec$(A, r), t)$;
5. return(Union(q, q')).

The routines appearing in the previous algorithm are described next:

- IsReg. *Input:* $A \in \mathbb{S}_m^{n+1}(\mathbb{Q}), \iota \subset \{1, \ldots, m\}$; *Output:* `true` if $\mathcal{V}_r(A, \iota)$ is empty or smooth and equidimensional of codimension $m(m-r) + \binom{m-r+1}{2}$, `false` otherwise.
- Project. *Input:* A rational parametrization of $\ell(A \circ M, \iota) \subset \mathbb{Q}[x, y, z]$; *Output:* an error message if the projection of $\mathcal{Z}(A \circ M, \iota) \cap \{(x, y, z) : \operatorname{rank} A(M\,x) = r\}$ on the $x-$space is not finite; otherwise a rational parametrization of this projection.

- RatPar. *Input:* $\ell(A \circ M, \iota) \subset \mathbb{Q}[x, y, z]$; *Output*: a rational parametrization of $\ell(A \circ M, \iota)$.
- Image. *Input:* a rational parametrization of a set $\mathcal{Z} \subset \mathbb{Q}[x_1, \ldots, x_N]$ and a matrix $M \in \mathrm{GL}_N(\mathbb{Q})$; *Output:* a rational parametrization of $M^{-1}\mathcal{Z} = \{x \in \mathbb{C}^N : M\,x \in \mathcal{Z}\}$.
- Union. *Input:* two rational parametrizations encoding $\mathcal{Z}_1, \mathcal{Z}_2 \subset \mathbb{Q}[x_1, \ldots, x_N]$; *Output:* a rational parametrization of $\mathcal{Z}_1 \cup \mathcal{Z}_2$.
- Lift. *Input:* a rational parametrization of a set $\mathcal{Z} \subset \mathbb{Q}[x_1, \ldots, x_N]$, and $t \in \mathbb{C}$; *Output:* a rational parametrization of $\{(t, x) : x \in \mathcal{Z}\}$.

3.3 Main algorithm: description

The input of SolveLMI is a linear matrix $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$, and the algorithm makes use of algorithm LowRankSym described previously, as a subroutine. The formal description is the following.

SolveLMI

Input: $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$, encoded by the $m(m+1)(n+1)/2$ entries of $A_0, A_1, \ldots, A_n$;

Output: Either the empty list [ ], if and only if $\{x \in \mathbb{R}^n : A(x) \succeq 0\}$ is empty; or an error message stating that the genericity assumptions are not satisfied, or, otherwise, either a vector $x^* = (x_1^*, \ldots, x_n^*)$ such that $A(x^*) = 0$, or a rational parametrization $q = (q_0, \ldots, q_{n+1}) \subset \mathbb{Z}[t]$, such that there exists $t^* \in Z(q_{n+1}) \cap \mathbb{R}$ with $A(q_1(t^*)/q_0(t^*), \ldots, q_n(t^*)/q_0(t^*)) \succeq 0$.

Procedure SolveLMI(A)

1. $x^* \leftarrow$ SolveLinear(A); if $x^* \neq$ [ ] then return(x^*);
2. for r from 1 to $m-1$ do:
   - $q \leftarrow$ LowRankSym(A, r);
   - if $q =$ "the input is not generic" then return(q);
   - if $q \neq$ [ ] then $b \leftarrow$ CheckLMI(A, q);
   - if $b =$ `true` then return(q);
3. return([ ], "the spectrahedron is empty").

The different subroutines of SolveLMI are described next:

- SolveLinear. *Input*: $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$; *Output* the empty list if $A(x) = 0$ has no solution, otherwise x^* such that $A(x^*) = 0$;
- CheckLMI. *Input*: $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$ and a rational parametrization $q \subset \mathbb{Z}[t]$; *Output*: `true` if $A(q_1(t^*)/q_0(t^*), \ldots, q_n(t^*)/q_0(t^*)) \succeq 0$ is satisfied for some $t^* \in Z(q_{n+1}) \cap \mathbb{R}$, `false` otherwise.

3.4 Main algorithm: correctness

We prove in Theorem 10 that SolveLMI returns a correct output if genericity properties on input data and on random parameters chosen during its execution are satisfied; the proof relies on some preliminary results that are described before. The proofs of these intermediate results share some techniques with [34, 35, 36] and are given in Section 4.

Intermediate results

The first result is a regularity theorem for the incidence varieties $\mathcal{V}_r(A, \iota)$. We focus on property P_1 for the input matrix A (*cf.* Section 3.2).

Proposition 7 *Let $m, n, r \in \mathbb{N}$, with $0 \leq r \leq m-1$.*

1. *There exists a non-empty Zariski-open set $\mathscr{A} \subset \mathbb{S}_m^{n+1}(\mathbb{C})$ such that if $A \in \mathscr{A} \cap \mathbb{S}_m^{n+1}(\mathbb{Q})$, then A satisfies P_1;*
2. *if A satisfies P_1, there exists a non-empty Zariski open set $\mathscr{T} \subset \mathbb{C}$ such that if $t \in \mathscr{T} \cap \mathbb{Q}$, then $(A_0 + tA_1, A_2, \ldots, A_n)$ satisfies P_1.*

Next, we prove that the projection of $\mathcal{Z}(A \circ M, \iota) \cap \{(x, y, z) : \operatorname{rank} A(M\,x) = r\}$ over the $x-$space is finite and that this set meets the critical points of the restriction of the map $\Pi_1 \colon (x, y) \to x_1$ to $\mathcal{V}_r(A, \iota)$.

Proposition 8 *Let $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$ satisfy P_1. Then there exists a non-empty Zariski open set $\mathscr{M}_1 \subset \mathrm{GL}_n(\mathbb{C})$ such that, if $M \in \mathscr{M}_1 \cap \mathbb{M}_{n,n}(\mathbb{Q})$, for all $\iota \subset \{1, \ldots, m\}$, with $\sharp\iota = m-r$, the following holds:*

1. *The system $\ell(A \circ M, \iota)$ satisfies Q in $\{(x, y, z) : \operatorname{rank} A(M\,x) = r\}$;*
2. *the projection of $\mathcal{Z}(A \circ M, \iota) \cap \{(x, y, z) : \operatorname{rank} A(M\,x) = r\}$ on the $x-$space is empty or finite;*
3. *the projection of $\mathcal{Z}(A \circ M, \iota) \cap \{(x, y, z) : \operatorname{rank} A(M\,x) = r\}$ on (x, y) contains the set of critical points of the restriction of $\Pi_1 \colon (x, y) \to x_1$ to $\mathcal{V}_r(A \circ M, \iota) \cap \{(x, y) : \operatorname{rank} A(M\,x) = r\}$.*

Finally, we show, after a generic linear change of variables x, closure properties of the projection maps $\pi_i(x) = (x_1, \ldots, x_i)$ restricted to $\mathcal{D}_r$. Also, in order to compute sample points on the connected components of $\mathcal{D}_r \cap \mathbb{R}^n$ not meeting $\mathcal{D}_{r-1}$, the next proposition shows that to do that it is sufficient to compute critical points on the incidence variety $\mathcal{V}_r$.

Proposition 9 *Let $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$ satisfy P_1, and let $d = \dim \mathcal{D}_r$. There exists a non-empty Zariski open set $\mathscr{M}_2 \subset \mathrm{GL}_n(\mathbb{C})$ such that if $M \in \mathscr{M}_2 \cap \mathbb{M}_{n,n}(\mathbb{Q})$, for any connected component $\mathcal{C} \subset \mathcal{D}_r \cap \mathbb{R}^n$, the following holds:*

1. *for $i = 1, \ldots, d$, $\pi_i(M^{-1}\mathcal{C})$ is closed; further, for $t \in \mathbb{R}$ lying on the boundary of $\pi_1(M^{-1}\mathcal{C})$, then $\pi_1^{-1}(t) \cap M^{-1}\mathcal{C}$ is finite;*
2. *let t lie on the boundary of $\pi_1(M^{-1}\mathcal{C})$: for $x \in \pi_1^{-1}(t) \cap M^{-1}\mathcal{C}$, such that $\operatorname{rank} A(M\,x) = r$, there exists $\iota \subset \{1, \ldots, m\}$, with $\sharp\iota = m - r$, and $(x, y) \in \mathcal{V}_r(A \circ M, \iota)$, such that $\Pi_1(x, y) = t$.*

Theorem of correctness

Let $A \in \mathbb{S}_{m,m}^{n+1}(\mathbb{Q})$ be the input of SolveLMI. We say that hypothesis H holds if:

- A and all parameters generated by SolveLMI belong to the Zariski open sets defined in Proposition 7, 8 and 9, for all recursive steps of LowRankSym;
- A satisfies Property P_2.

We can now state the correctness theorem for SolveLMI.

Theorem 10 (Correctness of SolveLMI) *Suppose that H holds. Let $\mathscr{S} = \{x \in \mathbb{R}^n : A(x) \succeq 0\}$ be the spectrahedron associated to A. Then two alternatives hold:*

1. *$\mathscr{S} = \emptyset$: hence the output of SolveLMI with input A is the empty list;*
2. *$\mathscr{S} \neq \emptyset$: hence the output of SolveLMI with input A is either a vector x^* such that $A(x^*) = 0$, if it exists; or a rational parametrization $q = (q_0, \ldots, q_{n+1}) \subset \mathbb{Z}[t]$ such that there exists $t^* \in Z(q_{n+1}) \cap \mathbb{R}$ with:*
   - *$A(q_1(t^*)/q_0(t^*), \ldots, q_n(t^*)/q_0(t^*)) \succeq 0$ and*
   - *$\operatorname{rank} A(q_1(t^*)/q_0(t^*), \ldots, q_n(t^*)/q_0(t^*)) = r(A)$ (cf. Notation 1).*

Proof : Suppose $A(x) = 0$ has a solution. Hence, at Step 1 of SolveLMI, SolveLinear with input A returns a vector x^* such that $A(x^*) = 0$. We deduce that $x^* \in \mathscr{S} \neq \emptyset$ and that the rank of A attains its minimum on $\mathscr{S}$ at x^*. We deduce that, if $A(x) = 0$ has at least one solution, the algorithm returns a correct output.

Suppose now that either $\mathscr{S}$ is empty, or $r(A) \geq 1$. We claim that LowRankSym is correct, in the following sense: with input (A, r), with A satisfying P_1, the output is a rational

parametrization whose solutions meet each connected component $\mathcal{C}$ of $\mathcal{D}_r \cap \mathbb{R}^n$ such that $\mathcal{C} \cap \mathcal{D}_{r-1} = \emptyset$.

We assume for the moment this claim, and consider two possible alternatives:

1. $\mathscr{S} = \emptyset$. Consequently, CheckLMI outputs `false` at each iteration of Step 2 in SolveLMI. Thus the output of SolveLMI is the empty list, and correctness follows.

2. $\mathscr{S} \neq \emptyset$. Denote by $\mathcal{C}$ a connected component of $\mathcal{D}_{r(A)} \cap \mathbb{R}^n$ such that $\mathcal{C} \cap \mathscr{S} \neq \emptyset$. By Theorem 2, we deduce that $\mathcal{C} \subset \mathscr{S}$, and that $\mathcal{C} \cap \mathcal{D}_{r(A)-1} = \emptyset$. Let q be the output of LowRankSym at Step 2 of SolveLMI. By our claim, q defines a finite set whose solutions meet $\mathcal{C}$, hence $\mathscr{S}$. Consequently, CheckLMI returns `true` at Step 2, and hence the algorithm stops returning the correct output q.

We end the proof by showing that LowRankSym is correct. This is straightforwardly implied by the correctness of the recursive subroutine LowRankSymRec, which is proved below by using induction on the number of variables n.

For $n < \binom{m-r+1}{2}$, since H holds, then A satisfies P_r. Hence $\mathcal{D}_r$ is empty, and LowRankSym returns the correct answer [ ] (the empty list).

Let $n \geq \binom{m-r+1}{2}$, and let (A, r) be the input. The induction hypothesis implies that for any $\tilde{A} \in \mathbb{S}^n_m(\mathbb{Q})$ satisfying P_1, then LowRankSymRec with input $(\tilde{A}, r)$ returns a rational parametrization of a finite set meeting each connected component $\tilde{\mathcal{C}} \subset \tilde{\mathcal{D}}_r \cap \mathbb{R}^{n-1}$ such that $\tilde{\mathcal{C}} \cap \tilde{\mathcal{D}}_{r-1} = \emptyset$, with $\tilde{\mathcal{D}}_r = \{x \in \mathbb{R}^{n-1} : \operatorname{rank} \tilde{A}(x) \leq r\}$. Let $\mathcal{C} \subset \mathcal{D}_r \cap \mathbb{R}^n$ be a connected component with $\mathcal{C} \cap \mathcal{D}_{r-1} = \emptyset$, and let M be the matrix chosen at Step 1. Hence, since H holds, by Proposition 9 the set $\pi_1(M^{-1}\mathcal{C})$ is closed in $\mathbb{R}$. There are two possible scenarios.

First case. Suppose that $\pi_1(M^{-1}\mathcal{C}) = \mathbb{R}$, let $t \in \mathbb{Q}$ be the rational number chosen at Step 3 of LowRankSymRec, and let $\tilde{A} = (A_0 + tA_1, A_2, \ldots, A_n) \in \mathbb{S}^n_m(\mathbb{Q})$. We deduce that $\pi_1^{-1}(t) \cap M^{-1}\mathcal{C} \neq \emptyset$ is the union of some connected components of the algebraic set $\tilde{\mathcal{D}}_r = \{x \in \mathbb{R}^{n-1} : \operatorname{rank} \tilde{A}(x) \leq r\}$ not meeting $\tilde{\mathcal{D}}_{r-1}$. Also, since A satisfies P_1, so does $A \circ M$; by Proposition 7, then $\tilde{A}$ satisfies P_1. By the induction assumption, LowRankSymRec with input $(\tilde{A}, r)$ returns at least one point in each connected component $\tilde{\mathcal{C}} \subset \tilde{\mathcal{D}}_r \cap \mathbb{R}^{n-1}$ not meeting $\tilde{\mathcal{D}}_{r-1}$, hence one point in $\mathcal{C}$ by applying the subroutine Lift at Step 4. Correctness follows.

Second case. Otherwise, $\pi_1(M^{-1}\mathcal{C}) \neq \mathbb{R}$ and, since it is a closed set, its boundary is non-empty. Let t belong to the boundary of $\pi_1(M^{-1}\mathcal{C})$, and suppose w.l.o.g. that $\pi_1(M^{-1}\mathcal{C}) \subset [t, +\infty)$. Hence t is the minimum of the restriction of the map π_1 to $M^{-1}\mathcal{C}$. By Proposition 9, the set $\pi_1^{-1}(t) \cap M^{-1}\mathcal{C}$ is non-empty and finite, and for all $x \in \pi_1^{-1}(t) \cap M^{-1}\mathcal{C}$, $\operatorname{rank} A(M\,x) = r$ (indeed, for $x \in M^{-1}\mathcal{C}$, then $M\,x \in \mathcal{C}$ and hence $M\,x \notin \mathcal{D}_{r-1} \cap \mathbb{R}^n$). Fix $x \in \pi_1^{-1}(t) \cap M^{-1}\mathcal{C}$. By Proposition 9, there exists ι and $y \in \mathbb{C}^{m(m-r)}$ such that $(x, y) \in \mathcal{V}_r(A \circ M, \iota)$. Also, by Proposition 7, the set $\mathcal{V}_r(A \circ M, \iota)$ is smooth and equidimensional. One deduces that (x, y) is a critical point of the restriction of $\Pi_1 \colon (x, y) \to x_1$ to $\mathcal{V}_r(A \circ M, \iota)$ and that there exists z such that $(x, y, z) \in \mathcal{Z}(A \circ M, \iota)$. Hence, at Step 2, the routine LowRankSymRec outputs a rational parametrization q_ι, among whose solutions the vector x lies. □

4 Proof of intermediate results

4.1 Proof of Proposition 7

We prove Assertion 1 and 2 separately.

Proof of Assertion 1: Suppose w.l.o.g. that $M = \mathbb{I}_n$. For $\iota \subset \{1, \ldots, m\}$, with $\sharp\iota = m - r$, let $f_{red} \subset \mathbb{Q}[x, y]$ be the system defined in Lemma 5. We prove that there exists a non-empty Zariski open set $\mathscr{A}_\iota \subset \mathbb{S}_m^{n+1}(\mathbb{C})$ such that, if $A \in \mathscr{A}_\iota \cap \mathbb{S}_m^{n+1}(\mathbb{Q})$, f_{red} generates a radical ideal and $Z(f_{red})$ is empty or equidimensional, of codimension $\sharp f_{red} = m(m-r) + \binom{m-r+1}{2}$. We deduce that, for $A \in \mathscr{A}_\iota$, A satisfies P_1, and we conclude by defining $\mathscr{A} = \cap_\iota \mathscr{A}_\iota$ (non-empty and Zariski open).

Suppose w.l.o.g. that $\iota = \{1, \ldots, m-r\}$. We consider the map

$$\begin{array}{rccc} \varphi: & \mathbb{C}^{n+m(m-r)} \times \mathbb{S}_m^{n+1}(\mathbb{C}) & \longrightarrow & \mathbb{C}^{m(m-r)+\binom{m-r+1}{2}} \\ & (x, y, A) & \longmapsto & f_{red} \end{array}$$

and, for a fixed $A \in \mathbb{S}_m^{n+1}(\mathbb{C})$, its section map $\varphi_A \colon \mathbb{C}^{n+m(m-r)} \to \mathbb{C}^{m(m-r)+\binom{m-r+1}{2}}$ defined by $\varphi_A(x, y) = \varphi(x, y, A)$. Remark that, for any A, $Z(\varphi_A) = \mathcal{V}_r(A, \iota)$.

Suppose $\varphi^{-1}(0) = \emptyset$: this implies that, for all $A \in \mathbb{S}_m^{n+1}(\mathbb{C})$, $Z(f_{red}) = \mathcal{V}_r(A, \iota) = \emptyset$, that is A satisfies P_1 for $A \in \mathscr{A}_\iota = \mathbb{S}_m^{n+1}(\mathbb{C})$.

If $\varphi^{-1}(0) \neq \emptyset$, we prove below that 0 is a regular value of φ. We conclude that by Thom's Weak Transversality Theorem [60, Section 4.2] there exists a non-empty and Zariski open set $A_\iota \subset \mathbb{S}_m^{n+1}(\mathbb{C})$ such that if $A \in \mathscr{A}_\iota \cap \mathbb{S}_m^{n+1}(\mathbb{Q})$, 0 is a regular value of φ_A. Hence, by applying the Jacobian criterion (*cf.* [16, Theorem 16.19]) to the polynomial system f_{red}, we deduce that for $A \in \mathscr{A}_\iota \cap \mathbb{S}_m^{n+1}(\mathbb{Q})$, $\mathcal{V}_r(A, \iota)$ is smooth and equidimensional of codimension $\sharp f_{red}$.

Let $D\varphi$ be the Jacobian matrix of φ: it contains the derivatives of polynomials in f_{red} with respect to variables x, y, A. We denote by $a_{\ell,i,j}$ the variable encoding the $(i, j)-$th entry of the matrix $A_\ell, \ell = 0, \ldots, n$. We isolate the columns of $D\varphi$ corresponding to:

- the derivatives with respect to variables $\{a_{0,i,j} : i \leq m - r \text{ or } j \leq m - r\}$;
- the derivatives with respect to variables $y_{i,j}$ such that $i \in \iota$.

Let $(x, y, A) \in \varphi^{-1}(0)$, and consider the evaluation of $D\varphi$ at (x, y, A). The above columns contain the following non-singular blocks:

- the derivatives w.r.t. $\{a_{0,i,j} : i \leq m - r \text{ or } j \leq m - r\}$ of the entries of $A(x)Y(y)$ after the substitution $Y_\iota \leftarrow \mathbb{I}_{m-r}$, that is $\mathbb{I}_{(m-r)(m+r+1)/2}$;
- the derivatives w.r.t. $\{y_{i,j} : i \in \iota\}$ of polynomials in $Y_\iota - \mathbb{I}_{m-r}$, that is $\mathbb{I}_{(m-r)^2}$.

Hence, the above columns define a maximal non-singular sub-matrix of $D\varphi$ at (x, y, A), of size $m(m-r) + \binom{m-r+1}{2} = \sharp f_{red}$ (indeed, remark that the entries of $Y_\iota - \mathbb{I}_{m-r}$ do not

depend on variables $a_{0,i,j}$). Since $(x, y, A) \in \varphi^{-1}(0)$ is arbitrary, we deduce that 0 is a regular value of φ, and we conclude. □

Proof of Assertion 2: Fix $\iota \subset \{1, \ldots, m\}$ with $\sharp\iota = m - r$. Since A satisfies P_1, $\mathcal{V}_r(A, \iota)$ is either empty or smooth and equidimensional of codimension $m(m-r)+\binom{m-r+1}{2}$. Suppose first that $\mathcal{V}_r = \emptyset$. Hence for all $t \in \mathbb{C}$, $\mathcal{V}_r \cap \{x_1 - t = 0\} = \emptyset$, and we conclude by defining $\mathscr{T} = \mathbb{C}$. Otherwise, consider the restriction of the projection map $\Pi_1 : (x, y) \to x_1$ to $\mathcal{V}_r(A, \iota)$. By Sard's Lemma [60, Section 4.2], the set of critical values of the restriction of π_1 to $\mathcal{V}_r(A, \iota)$ is included in a finite subset $\mathcal{H} \subset \mathbb{C}$. We deduce that, for $t \in \mathscr{T} = \mathbb{C} \setminus \mathcal{H}$, then $(A_0 + tA_1, A_2, \ldots, A_n)$ satisfies P_1. □

Corollary 11 *Let $\mathscr{A} \subset \mathbb{S}_m^{n+1}(\mathbb{Q})$ be as in Proposition 7, and let $A \in \mathscr{A}$. Then for every $\iota \subset \{1, \ldots, m\}$ with $\sharp\iota = m-r$, the ideal $\langle f_{red}\rangle = \langle f\rangle$ is radical, and $\mathcal{V}_r(A, \iota)$ is a complete intersection of codimension $\sharp f_{red}$.*

Proof : We recall from the proof of Assertion 1 of Theorem 7 that, for $A \in \mathscr{A}$, the rank of the Jacobian matrix of f_{red} is $\sharp f_{red} = m(m - r) + \binom{m-r+1}{2}$ at every point of $\mathcal{V}_r(A, \iota)$. By the Jacobian criterion [16, Theorem 16.19], the ideal $\langle f_{red}\rangle$ is radical and the algebraic set $Z(f_{red}) = \mathcal{V}_r(A, \iota)$ is smooth and equidimensional of codimension $\sharp f_{red}$. Hence $I(\mathcal{V}_r(A, \iota)) = \langle f_{red}\rangle$ can be generated by a number of polynomials equal to the codimension of $\mathcal{V}_r(A, \iota)$, and we conclude. □

4.2 Proof of Proposition 8

Local equations of $\mathcal{V}_r(A, \iota)$

Suppose A is a (not necessarily symmetric) linear matrix. Let us give a local description of the algebraic sets $\mathcal{D}_r$ and $\mathcal{V}_r$ (*cf.* also [34, Section 5]). Consider first the locally closed set $\mathcal{D}_r \setminus \mathcal{D}_{r-1} = \{x \in \mathbb{C}^n : \operatorname{rank} A(x) = r\}$. This is given by the union of sets $\mathcal{D}_r \cap \{x \in \mathbb{C}^n : \det N(x) \neq 0\}$ where N runs over all $r \times r$ sub-matrices of $A(x)$. Fix $\iota \subset \{1, \ldots, m\}$ with $\sharp\iota = m - r$. Let N be the upper left $r \times r$ sub-matrix of $A(x)$, and consider the corresponding block division of A:

$$A = \begin{pmatrix} N & Q \\ P^T & R \end{pmatrix} \tag{3}$$

with $P, Q \in \mathbb{M}_{r,m-r}(\mathbb{Q})$ and $R \in \mathbb{M}_{m-r,m-r}(\mathbb{Q})$. Let $\mathbb{Q}[x, y]_{\det N}$ be the local ring obtained by localizing $\mathbb{Q}[x, y]$ at $\langle \det N\rangle$. Let $Y^{(1)}$ (resp. $Y^{(2)}$) be the matrix obtained by isolating the first r (resp. the last $m - r$) rows of $Y(y)$. Hence, the local equations of $\mathcal{V}_r$ in $\{(x, y) : \det N(x) \neq 0\}$ are given by:

$$Y^{(1)} + N^{-1}QY^{(2)} = 0, \qquad \Sigma(N)Y^{(2)} = 0, \qquad Y_\iota - \mathbb{I}_{m-r} = 0, \tag{4}$$

where $\Sigma(N) = R - P^T N^{-1} Q$ is the Schur complement of N in A. This follows from the following straightforward equivalence holding in the local ring $\mathbb{Q}[x, y]_{\det N}$ (*cf.* also [34, Lemma 13]):

$$A(x)Y(y) = 0 \qquad \text{iff} \qquad \begin{pmatrix} \mathbb{I}_r & 0 \\ -P^T & \mathbb{I}_{m-r} \end{pmatrix} \begin{pmatrix} N^{-1} & 0 \\ 0 & \mathbb{I}_{m-r} \end{pmatrix} \begin{pmatrix} N & Q \\ P^T & R \end{pmatrix} Y(y) = 0.$$

Intermediate lemma

Let $w \in \mathbb{C}^n$ be a non-zero vector, and consider the projection map induced by w: $\Pi_w \colon (x_1, \ldots, x_n, y) \mapsto w_1 x_1 + \cdots + w_n x_n$.

For $A \in \mathscr{A}$ (given by Proposition 7), for all ι as above, the critical points of the restriction of Π_w to $\mathcal{V}_r(A, \iota)$ are encoded by the polynomial system (f, g, h) where

$$f = f(A, \iota), \qquad (g, h) = z^T \begin{pmatrix} Df \\ D\Pi_w \end{pmatrix} = z^T \begin{pmatrix} D_x f & D_y f \\ w^T & 0 \end{pmatrix}, \tag{5}$$

and $z = (z_1, \ldots, z_{c+e}, 1)$ is a vector of Lagrange multipliers. Indeed, equations induced by (g, h) imply that the vector w is normal to the tangent space of $\mathcal{V}_r$ at (x, y).

We prove an intermediate lemma towards Proposition 8.

Lemma 12 *Let $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$ satisfy P_1. Then there exists a non-empty Zariski open set $\mathscr{W} \subset \mathbb{C}^n$ such that, if $w \in \mathscr{W} \cap \mathbb{Q}^n$, for all $\iota \subset \{1, \ldots, m\}$, with $\sharp\iota = m - r$, the following holds:*

1. *the system (f, g, h) in (5) satisfies Q in $\{(x, y, z) : \operatorname{rank} A(x) = r\}$;*
2. *the projection of $Z(f, g, h) \cap \{(x, y, z) : \operatorname{rank} A(x) = r\}$ on the $x-$space is empty or finite;*
3. *the projection of $Z(f, g, h) \cap \{(x, y, z) : \operatorname{rank} A(x) = r\}$ on (x, y) contains the set of critical points of the restriction of Π_w to $\mathcal{V}_r \cap \{(x, y) : \operatorname{rank} A(x) = r\}$.*

Proof of Assertion 1: The strategy relies on applying Thom Weak Transversality Theorem and the Jacobian criterion, as in the proof of Proposition 7. The similar passages will be only sketched.

We claim (and prove below) that, given a $r \times r$ sub-matrix N of A, there exists a non-empty Zariski open set $\mathscr{W}_N \subset \mathbb{C}^n$ such that, for $w \in \mathscr{W}_N$, (f, g, h) satisfies Q in $\{(x, y, z) : \det N \neq 0\}$. We deduce Assertion 1 by defining $\mathscr{W} = \bigcap_N \mathscr{W}_N$, where N runs over all $r \times r$ sub-matrices of $A(x)$.

Let $U_\iota \in \mathbb{C}^{(m-r)\times m}$ be the boolean matrix such that $U_\iota Y(y) = Y_\iota$, and let $U_\iota = (U_\iota^{(1)} \mid U_\iota^{(2)})$ be the subdivision with $U_\iota^{(1)} \in \mathbb{C}^{(m-r)\times r}$ and $U_\iota^{(2)} \in \mathbb{C}^{(m-r)\times(m-r)}$. The third equation in (4) equals $U_\iota Y(y) - \mathbb{I}_{m-r} = 0$. From (4) we deduce the equality

$$\mathbb{I}_{m-r} = U_\iota^{(1)} Y^{(1)} + U_\iota^{(2)} Y^{(2)} = (U_\iota^{(2)} - U_\iota^{(1)} N^{-1} Q) Y^{(2)}$$

and hence that both $Y^{(2)}$ and $U_\iota^{(2)} - U_\iota^{(1)} N^{-1} P$ are non-singular in $\mathbb{Q}[x, y]_{\det N}$. We deduce that the above local equations of $\mathcal{V}_r$ are equivalent to

$$Y^{(1)} + N^{-1} Q Y^{(2)} = 0, \qquad \Sigma(N) = 0, \qquad Y^{(2)} - (U_\iota^{(2)} - U_\iota^{(1)} N^{-1} P)^{-1} = 0$$

in $\mathbb{Q}[x, y]_{\det N}$. We collect the above equations in a system $\tilde{f}$, of length $c + e$. Hence, the Jacobian matrix of $\tilde{f}$ is

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

Since A satisfies P_1, the rank of $D\tilde{f}$ is constant and equal to c if evaluated at $(x,y) \in Z(\tilde{f}) = \mathcal{V}_r(A,\iota) \cap \{(x,y) : \det N \neq 0\}$. Similarly to (5), we define

$$(\tilde{g},\tilde{h}) = z^T \begin{pmatrix} D\tilde{f} \\ w^T \quad 0 \end{pmatrix}$$

with $z = (z_1,\ldots,z_{c+e},1)$. The polynomial relations $\tilde{h}_i = 0$ implies that $z_{(m-r)^2+i} = 0$, for $i = 1,\ldots,m(m-r)$, and hence they can be eliminated, together with the variables $z_{(m-r)^2+i}, i = 1,\ldots,m(m-r)$. Hence, one can consider the equivalent equations $(\tilde{f},\tilde{g},\tilde{h})$ where the last $m(m-r)$ variables z do not appear in $\tilde{g}$.

Let us define the map $\varphi\colon \mathbb{C}^{n+c+e+m(m-r)} \times \mathbb{C}^n \to \mathbb{C}^{n+c+e+m(m-r)}$, $\varphi(x,y,z,w) = (\tilde{f},\tilde{g},\tilde{h})$, and for $w \in \mathbb{C}^n$, its section map $\varphi_w\colon (x,y,z) \mapsto \varphi(x,y,z,w)$.

If $\varphi^{-1}(0) = \emptyset$, we define $\mathscr{W}_N = \mathbb{C}^n$ and conclude. Otherwise, let $(x,y,z,w) \in \varphi^{-1}(0)$. Remark that polynomials in $\tilde{f}$ just depend on (x,y), hence their contribution in $D\varphi(x,y,z,w)$ is the block $D\tilde{f}$, whose rank is c, since $(x,y) \in \mathcal{V}_r$. Hence, we deduce that the row-rank of $D\varphi$ at (x,y,z,w) is at most $n+c+m(m-r)$. Further, by isolating the columns corresponding to the derivatives with respect to x,y, to $w_1,\ldots,w_n$, and to $z_{(m-r)^2+i}, i = 1,\ldots,m(m-r)$, one obtains a $(n+c+e+m(m-r)) \times (2n+2m(m-r))$ sub-matrix of $D\varphi$ of rank $n+c+m(m-r)$. □

Proof of Assertion 2: From Assertion 1 we deduce that the locally closed set $\mathcal{E} = Z(f,g,h) \cap \{(x,y,z) : \operatorname{rank} A(x) = r\}$ is empty or $e-$equidimensional. If it is empty, we are done. Suppose that it is $e-$equidimensional. Consider the projection map $\pi_x(x,y,z) = x$, and its restriction to $\mathcal{E}$. Let $x^* \in \pi_x(\mathcal{E})$. Then $\operatorname{rank} A(x^*) = r$ and there exists a unique $y \in \mathbb{C}^{m(m-r)}$ such that $f(x^*,y) = 0$. Hence the fiber $\pi_x^{-1}(x^*)$ is isomorphic to the linear space $\{(z_1,\ldots,z_{c+e}) : (z_1,\ldots,z_{c+e})Df = (w^T,0)\}$. Since the rank of Df is c, one deduces that $\pi_x^{-1}(x^*)$ is a linear space of dimension e, and by the Theorem on the Dimension of Fibers [63, Sect. 6.3, Theorem 7] we deduce that $\pi_x(\mathcal{E})$ has dimension 0. □

Proof of Assertion 3: Since $\mathcal{V}_r \cap \{(x,y) : \operatorname{rank} A(x) = r\}$ is smooth and equidimensional, by [60, Lemma 3.2.1], for $w \neq 0$, the set crit $(\Pi_w, \mathcal{V}_r)$ coincides with the set of points $(x,y) \in \mathcal{V}_r$ such that the matrix

$$D(f,\Pi_w) = \begin{pmatrix} Df \\ D\Pi_w \end{pmatrix}$$

has a rank $\leq c$. In particular there exists $z = (z_1,\ldots,z_{c+e},z_{c+e+1}) \neq 0$, such that $z^T D(f,\Pi_w) = 0$. One can exclude that $z_{c+e+1} = 0$, since this implies that Df has a non-zero vector in the left kernel, which contradicts the fact that A satisfies P_1. Hence without loss of generality we deduce that $z_{c+e+1} = 1$, and we conclude. □

Proof of the proposition

We can finally deduce the proof of Proposition 8.

Proof of Proposition 8: Define $\mathscr{M}_1$ as the set of matrices $M \in \mathrm{GL}_n(\mathbb{C})$ such that the first row of M^{-1} is contained in $\mathscr{W}$ (defined in Lemma 12). The proof of all assertions

follows from Lemma 12 since, for $M \in \mathscr{M}_1$, one gets

$$\begin{pmatrix} Df(A \circ M, \iota) \\ e_1^T \quad 0 \cdots 0 \end{pmatrix} = \begin{pmatrix} Df(A, \iota) \circ M \\ w^T \quad 0 \cdots 0 \end{pmatrix} \begin{pmatrix} M & 0 \\ 0 & \mathbb{I}_{m(m-r)} \end{pmatrix}, \tag{6}$$

where w^T is the first row of M^{-1}. Indeed, for $z = (z_1, \ldots, z_{c+e})$, we deduce from the previous relation that the set of solutions to the equations

$$f(A, \iota) = 0, \qquad z^T Df(A, \iota) = (w^T, 0) \tag{7}$$

is the image of the set of solutions of

$$f(A \circ M, \iota) = 0, \qquad z^T Df(A \circ M, \iota) = (e_1^T, 0) \tag{8}$$

by the linear map

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} M^{-1} & 0 & 0 \\ 0 & \mathbb{I}_{m(m-r)} & 0 \\ 0 & 0 & \mathbb{I}_{c+e} \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

This last fact is straightforward since from (6) we deduce that system (8) is equivalent to $f(A \circ M, \iota) = 0, z^T (Df(A, \iota) \circ M) = (w^T, 0)$. Hence the three assertions of Proposition 8 are straightforwardly deduced by those of Lemma 12. □

4.3 Proof of Proposition 9

For the proof of Assertion 1 of Proposition 9, we need to recall some notation from [34, Sec. 5]. Let $\mathcal{Z} \subset \mathbb{C}^n$ be an algebraic set of dimension d. Its equidimensional component of dimension p, for $0 \leq p \leq d$, is $\Omega_p(\mathcal{Z})$. We define $\mathscr{S}(\mathcal{Z}) = \Omega_0(\mathcal{Z}) \cup \cdots \cup \Omega_{d-1}(\mathcal{Z}) \cup \mathrm{sing}\,\Omega_d\mathcal{Z}$, where we recall that $\mathrm{sing}\,\mathcal{V}$ denotes the singular locus of an algebraic set $\mathcal{V}$, and

$$\mathscr{C}(\pi_i, \mathcal{Z}) = \Omega_0(\mathcal{Z}) \cup \cdots \cup \Omega_{i-1}(\mathcal{Z}) \cup \bigcup_{r=i}^{d} \mathrm{crit}\,(\pi_i, \mathrm{reg}\,\Omega_r\mathcal{Z}),$$

Here $\mathrm{reg}\,\mathcal{V}$ denotes $\mathcal{V} \setminus \mathrm{sing}\,\mathcal{V}$, $\pi_i \colon x \mapsto (x_1, \ldots, x_i)$ and $\mathrm{crit}\,(g, \mathcal{V})$ the set of critical points of the restriction of a map g to $\mathcal{V}$. For $M \in \mathrm{GL}_n(\mathbb{C})$ we recursively define

- $\mathcal{O}_d(M^{-1}\mathcal{Z}) = M^{-1}\mathcal{Z}$;
- $\mathcal{O}_i(M^{-1}\mathcal{Z}) = \mathscr{S}(\mathcal{O}_{i+1}(M^{-1}\mathcal{Z})) \cup \mathscr{C}(\pi_{i+1}, \mathcal{O}_{i+1}(M^{-1}\mathcal{Z})) \cup \mathscr{C}(\pi_{i+1}, M^{-1}\mathcal{Z})$ for $i = 0, \ldots, d-1$.

In [34, Prop. 17] we proved that when M is generic in $\mathrm{GL}_n(\mathbb{C})$ (that is, it lies out of a proper algebraic set) the algebraic sets $\mathcal{O}_i(M^{-1}\mathcal{Z})$ have dimension at most i and are in Noether position with respect to $x_1, \ldots, x_i$ (*cf.* [63, 16] for a background in Noether position). We used this fact in [34, Prop. 18] to prove closure properties of the restriction of maps $\pi_i, i = 1, \ldots, d$, to the connected components of $\mathcal{Z} \cap \mathbb{R}^n$.

Proof of Assertion 1: We denote by $\mathscr{M}_2 \subset \mathrm{GL}_n(\mathbb{C})$ the non-empty Zariski open set defined in [34, Prop. 17], for the algebraic set $\mathcal{D}_r$. Hence, for $M \in \mathscr{M}_2$, we deduce by [34, Prop. 18] that for $i = 1, \ldots, d$, and for any connected component $\mathcal{C} \subset \mathcal{D}_r \cap \mathbb{R}^n$, the boundary of $\pi_i(M^{-1}\mathcal{C})$ is contained in $\pi_i(\mathcal{O}_{i-1}(M^{-1}\mathcal{D}_r) \cap M^{-1}\mathcal{C}) \subset \pi_i(M^{-1}\mathcal{C})$, and hence that $\pi_i(M^{-1}\mathcal{C})$ is closed. Moreover, let $\mathcal{C} \subset \mathcal{D}_r \cap \mathbb{R}^n$ be a connected component and let $t \in \mathbb{R}$ be in the boundary of $\pi_1(M^{-1}\mathcal{C})$. Then [34, Lemma 19] implies that $\pi_1^{-1}(t) \cap M^{-1}\mathcal{C}$ is finite. □

Proof of Assertion 2: Let $M \in \mathscr{M}_2$. Consider the open set

$$\mathscr{O} = \{(x, y) \in \mathbb{C}^{n+m(m-r)} : \operatorname{rank} A(M\,x) = r,\ \operatorname{rank} Y(y) = m - r\}.$$

Let $\Pi_x \colon \mathbb{C}^{n+m(m-r)} \to \mathbb{C}^n$, $\Pi_x(x, y) = x$. Then $\Pi_x(\mathscr{O})$ is the locally closed set $M^{-1}(\mathcal{D}_r \setminus \mathcal{D}_{r-1}) = \{x \in \mathbb{C}^n : \operatorname{rank} A(M\,x) = r\}$. We consider the restriction of polynomial equations $A(M\,x)Y(y) = 0$ to $\mathscr{O}$. By definition of $\mathscr{O}$, we can split the locally closed set $\mathscr{O} \cap Z(A(M\,x)Y(y))$ into the union

$$\mathscr{O} \cap Z(A(M\,x)Y(y)) = \bigcup_{\substack{\iota \subset \{1,\ldots,m\} \\ \sharp\iota = m-r}} \Big(\mathscr{O}_\iota \cap Z(A(M\,x)Y(y))\Big),$$

where $\mathscr{O}_\iota = \{(x, y) :\ \det Y_\iota \neq 0\}$.

Let $\mathcal{C}$ be a connected component of $\mathcal{D}_r \cap \mathbb{R}^n$. Let t lie in the frontier of $\pi_1(M^{-1}\mathcal{C})$, and $x \in \pi_1^{-1}(t) \cap M^{-1}\mathcal{C}$ with $\operatorname{rank} A(M\,x) = r$. Hence there exists $\iota \subset \{1, \ldots, m\}$ such that x lies in the projection of $\mathcal{V}_r(A \circ M, \iota)$ on the $x-$space. Hence there exists y such that $(x, y) \in \mathcal{V}_r(A \circ M, \iota)$ and such that $\pi_1(x, y) = t$. □

5 Complexity analysis

Our next goal is to estimate the arithmetic complexity of algorithm SolveLMI, that is the number of arithmetic operations performed over $\mathbb{Q}$. This will essentially rely on the complexities of state-of-the-art algorithms computing rational parametrizations.

5.1 Output degree estimates

We start by computing Multilinear Bézout bounds (*cf.* [60, Ch. 11]) on the output degree.

Proposition 13 *Let $A \in \mathbb{S}_m^{n+1}$ be the input of* SolveLMI*, and $0 \leq r \leq m-1$. Let $p_r = (m-r)(m+r+1)/2$. If* H *holds, for all $\iota \subset \{1, \ldots, m\}$, with $\sharp\iota = m - r$, the degree of the parametrization q_ι computed at Step 2 of* LowRankSymRec *is at most*

$$\theta(m, n, r) = \sum_{k \in \mathcal{G}_{m,n,r}} \binom{p_r}{n-k} \binom{n-1}{k + p_r - 1 - r(m-r)} \binom{r(m-r)}{k},$$

with $\mathcal{G}_{m,n,r} = \{k :\ \max\{0, n - p_r\} \leq k \leq \min\{n - \binom{m-r+1}{2}, r(m-r)\}\}$. Moreover, for all m, n, r, $\theta(m, n, r)$ is bounded above by $\binom{p_r+n}{n}^3$.

Proof : We can simplify the system $f = f(A, \iota)$ to a system of p_r bilinear equations with respect to variables $x = (x_1, \ldots, x_n)$ and $y = (y_{m-r+1,1}, \ldots, y_{m,m-r})$. Indeed, by Lemma 5, $\mathcal{V}_r(A, \iota)$ is defined by $Y_\iota - \mathbb{I}_{m-r} = 0$ and by $m(m-r) - e = p_r$ entries of $A(x)Y(y)$, where $e = \binom{m-r}{2}$. Hence we can eliminate equations $Y_\iota - \mathbb{I}_{m-r} = 0$ and the corresponding variables $y_{i,j}$. Consequently, the Lagrange system can be also simplified, by admitting only p_r Lagrange multipliers z. We can also eliminate the first Lagrange multiplier z_1 (since $z \neq 0$, one can assume $z_1 = 1$) and impose a rank defect on the truncated Jacobian matrix obtained by Df by eliminating the first column (that containing the derivatives with respect to x_1).

The bound $\theta(m, n, r)$, by [60, Ch. 11], equals the coefficient of $s_x^n s_y^{r(m-r)} s_z^{p_r-1}$ in $(s_x + s_y)^{p_r}(s_y + s_z)^{n-1}(s_x + s_z)^{r(m-r)}$. This can be easily obtained by writing down such an expansion and solving the associated linear system forcing the constraints on the exponents of the monomials. The result is exactly the claimed closed formula. The estimate $\theta(m, n, r) \leq \binom{p_r+n}{n}^3$ is obtained by applying the standard formula:

$$\binom{a+b}{a}^3 = \sum_{i_1,i_2,i_3=0}^{\min(a,b)} \binom{a}{i_1}\binom{b}{i_1}\binom{a}{i_2}\binom{b}{i_2}\binom{a}{i_3}\binom{b}{i_3}$$

with $a = n$ and $b = p_r$. □

Corollary 14 *With the hypotheses and notations of Proposition 13, the sum of the degrees of the rational parametrizations computed during* SolveLMI *is bounded above by* $\sum_{r \leq r(A)} \binom{m}{r} \theta(m, n, r)$. *The degree of the rational parametrization whose solutions intersect* $\mathscr{S}$ *is in*

$$\mathcal{O}\left(\binom{\frac{m^2+m}{2} + n}{n}^3\right).$$

Proof : Remark that the number of subsets $\iota \subset \{1, \ldots, m\}$, with $\sharp\iota = m - r$ is $\binom{m}{m-r} = \binom{m}{r}$, and that SolveLMI stops when r reaches $r(A)$. Hence the first part follows by applying Proposition 13. Finally, remark that $p_0 \geq p_1 \geq \cdots \geq p_r \geq \cdots$ for all m, and hence, by Proposition 13, the degree of the rational parametrization whose solutions intersect $\mathscr{S}$ is of the order of $\binom{p_r+n}{n}^3 \leq \binom{p_0+n}{n}^3 = \binom{\frac{m^2+m}{2}+n}{n}^3$. □

In the column deg of Table 1 we report the degrees of the rational parametrization q_ι returned by LowRankSymRec at Step 2, compared with its bound $\theta(m, n, r)$ computed in Proposition 13. For this table, the input are randomly generated symmetric pencils with rational coefficients. When the algorithm does not compute critical points (that is, when the Lagrange system generates the empty set) we put deg $= 0$.

We recall that the routine LowRankSymRec computes points in components of the real algebraic set $\mathcal{D}_r \cap \mathbb{R}^n$ not meeting the subset $\mathcal{D}_{r-1} \cap \mathbb{R}^n$, hence of the expected rank r. Moreover, we recall that LowRankSym calls recursively its subroutine LowRankSymRec, eliminating at each call the first variable. Hence, the total number of critical points computed by LowRankSym for a given expected rank r is obtained by summing up the integer in column deg for every admissible value of n. We remark here that both the degree

and the bound are constant and equal to 0 if n is large enough. Hence, the previous sum is constant for large values of n. Similar behaviors appear, for example, when computing the Euclidean Distance degree (EDdegree) of determinantal varieties, as in [15] or [50]. In [50, Table 1], the authors report on the EDdegree of determinantal hypersurfaces generated by linear matrices $A(x) = A_0 + x_1A_1 + \cdots + x_nA_n$: for generic weights in the distance function, and when the codimension of the vector space generated by $A_1, \ldots, A_n$ is small (for us, when n is big, since matrices A_i are randomly generated, hence independent for $n \leq \binom{m+1}{2} = \dim \mathbb{S}_m(\mathbb{Q})$) the EDdegree is constant. Similar comparisons can be done with data in [50, Example 4] and [50, Corollary 3.5].

(m,r,n)	deg	$\theta(m,n,r)$	(m,r,n)	deg	$\theta(m,n,r)$
$(3,2,2)$	6	9	$(4,3,9)$	0	0
$(3,2,3)$	4	16	$(5,2,5)$	0	0
$(3,2,4)$	0	15	$(5,2,6)$	35	924
$(3,2,5)$	0	6	$(5,2,7)$	140	10296
$(3,2,6)$	0	0	$(5,3,3)$	20	84
$(4,2,3)$	10	35	$(5,3,4)$	90	882
$(4,2,4)$	30	245	$(5,4,2)$	20	30
$(4,2,5)$	42	896	$(5,4,3)$	40	120
$(4,2,6)$	30	2100	$(5,4,4)$	40	325
$(4,2,7)$	10	3340	$(5,4,5)$	16	606
$(4,2,8)$	0	3619	$(6,3,3)$	0	0
$(4,2,9)$	0	2576	$(6,3,4)$	0	0
$(4,2,12)$	0	0	$(6,3,5)$	0	0
$(4,3,3)$	16	52	$(6,3,6)$	112	5005
$(4,3,4)$	8	95	$(6,4,2)$	0	0
$(4,3,7)$	0	20	$(6,4,3)$	35	165
$(4,3,8)$	0	0	$(6,5,3)$	80	230

Table 1: Degrees and bounds for rational parametrizations

The values in column deg of Table 1 must also be compared with the associated algebraic degree of semidefinite programming. Given integers k, m, r with $r \leq m-1$, Nie, Ranestad, Sturmfels and von Bothmer computed in [48, 24] formulas for the algebraic degree $\delta(k,m,r)$ of a generic semidefinite program associated to $m \times m$ $k-$variate linear matrices, with expected rank r. Since the values in column deg match exactly the corresponding values in [48, Table 2], we conclude this section with the following expected result, which is a work in progress.

Conjecture 15 *Let $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$ be the input of* SolveLMI*, and suppose that $\mathscr{S} = \{x \in \mathbb{R}^n : A(x) \succeq 0\}$ is not empty. Let $\delta(k,m,r)$ be the algebraic degree of a generic semidefinite program with parameters k, m, r as in [48, 24]. If* H *holds, then the sum of the degrees of the rational parametrizations computed during* SolveLMI *is*

$$\sum_{r=1}^{r(A)} \binom{m}{r} \sum_{k=p_r-r(m-r)}^{\min(n,p_r+r(m-r))} \delta(k,m,r),$$

where $p_r = (m-r)(m+r+1)/2$.

5.2 The complexity of SolveLMI

Complexity of some subroutines

We first provide complexity estimates for subroutines SolveLinear, CheckLMI, Project, Lift, Image and Union.

Complexity of SolveLinear. This subroutine computes, if it exists, a solution of the $A(x) = 0$. This can be essentially performed by Gaussian elimination. The complexity of solving $\binom{m+1}{2}$ linear equations in n variables is linear in $\binom{m+1}{2}$ and cubic in n.

Complexity of CheckLMI. This subroutine can be performed as follows. Let $q \subset \mathbb{Z}[t]$ be the rational parametrization in the input of CheckLMI. The spectrahedron $\mathscr{S} = \{x \in \mathbb{R}^n : A(x) \succeq 0\}$ is the semi-algebraic set defined, *e.g.*, by sign conditions on the coefficients of the characteristic polynomial

$$p(s,x) = \det(A(x) + s\,\mathbb{I}_m) = f_m(x) + f_{m-1}(x)s + \cdots + f_1(x)s^{m-1} + s^m.$$

That is, $\mathscr{S} = \{x \in \mathbb{R}^n : f_i(x) \geq 0, \forall\, i = 1, \ldots, m\}$. We make the substitution $x_i \leftarrow q_i(t)/q_0(t)$ in $A(x)$ and compute the coefficients of $p(s, x(t))$, that are rational functions of the variable t. Hence CheckLMI boils down to deciding on the sign of m univariate rational functions (that is, of $2m$ univariate polynomials) over the finite set defined by $q_{n+1}(t) = 0$. We deduce that the complexity of CheckLMI is polynomial in m and on the degree of q_{n+1} (that is, on the degree of q) see [6, Ch. 13].

Complexity of Project, Lift, Image *and* Union Estimates for the arithmetic complexities of these routines are given in [60, Ch. 10]. In particular, if $\theta = \theta(m, n, r)$ is the bound computed in Proposition 13, and $\tilde{n} = n + r(m-r) + p_r$, then:

- By [60, Lemma 10.1.5], Project is performed within $O^{\sim}(\tilde{n}^2\theta^2)$ operations;
- By [60, Lemma 10.1.6], Lift is performed within $O^{\sim}(\tilde{n}\theta^2)$ operations;
- By [60, Lemma 10.1.1], Image is performed within $O^{\sim}(\tilde{n}^2\theta + \tilde{n}^3)$ operations;
- By [60, Lemma 10.1.3], Union is performed within $O^{\sim}(\tilde{n}\theta^2)$ operations.

Complexity of LowRankSym and SolveLMI

The complexity of LowRankSym boils essentially down to the complexity of LowRankSymRec, that is the complexity of RatPar. This is performed with the symbolic homotopy algorithm [39]: we bound its complexity in this section. We just remark that computing the dimension of $\mathcal{D}_r$ at Step 1 of LowRankSym and performing the control routine IsReg can be done by combining the Jacobian criterion and Gröbner bases computations. Our complexity analysis omits this step.

We recall that the simplified Lagrange system defined in the proof of Proposition 13 contains: $p_r = (m-r)(m+r+1)/2$ polynomials of multidegree bounded by $(1,1,0)$; $n-1$ polynomials of multidegree bounded by $(0,1,1)$; $r(m-r)$ polynomials of multidegree bounded by $(1,0,1)$. Let us denote by ℓ this system. We denote by

$$\begin{aligned}
\Delta_{xy} &= \{1, x_i, y_j, x_i y_j : i = 1, \ldots, n, j = 1, \ldots, r(m-r)\} \\
\Delta_{yz} &= \{1, y_j, z_k, y_j z_k : j = 1, \ldots, r(m-r), k = 2 \ldots, p_r\} \\
\Delta_{xz} &= \{1, x_i, z_k, x_i z_k : i = 1, \ldots, n, k = 2, \ldots, p_r\}
\end{aligned}$$

the supports of the aforementioned three groups of polynomials. Let $\widetilde{\ell} \subset \mathbb{Q}[x,y,z]$ be a polynomial system such that:

- the length of $\tilde{\ell}$ equals that of ℓ;
- for $i = 1, \ldots, n-1+m^2-r^2$, the support of $\tilde{\ell}_i$ equals that of ℓ_i;
- the solutions of $\tilde{\ell}$ are known.

Remark that $\widetilde{\ell}$ can be easily built by considering suitable products of linear forms. We build the homotopy

$$\tau\ell + (1-\tau)\tilde{\ell} \subset \mathbb{Q}[x,y,z,\tau], \tag{9}$$

where τ is a new variable. The system (9) defines a curve. From [39, Proposition 6.1], if the solutions of $\tilde{\ell}$ are known, one can compute a rational parametrization of $Z(t\ell + (1-t)\tilde{\ell})$ within $\mathcal{O}((\tilde{n}^2 N \log Q + \tilde{n}^{\omega+1})ee')$ arithmetic operations over $\mathbb{Q}$, where: $\tilde{n}$ is the number of variables in ℓ; $N = p_r \sharp\Delta_{xy} + (n-1)\sharp\Delta_{yz} + r(m-r)\sharp\Delta_{xz}$; $Q = \max\{\|q\| : q \in \Delta_{xy} \cup \Delta_{yz} \cup \Delta_{xz}\}$; e is the number of isolated solutions of ℓ; e' is the degree of $Z(t\ell + (1-t)\tilde{\ell})$; ω is the exponent of matrix multiplication.

The technical lemma below gives a bound on the degree of $Z(t\ell + (1-t)\tilde{\ell})$.

Lemma 16 *Let $\mathcal{G}_{m,n,r}$ and $\theta(m,n,r)$ be the set and the bound defined in Proposition 13, and suppose that $\mathcal{G}_{m,n,r} \neq \emptyset$. Let e' be the degree of $Z(t\ell + (1-t)\tilde{\ell})$. Then $e' \in \mathcal{O}\left((n + p_r + r(m-r))\, \min\{n, p_r\}\, \theta(m,n,r)\right)$.*

Proof : Similarly to Proposition 13, we exploit the multilinear structure of $t\ell + (1-t)\tilde{\ell}$, to compute a bound on e'. The system is bilinear with respect to x, y, z, τ. We recall $\sharp x = n, \sharp y = r(m-r), \sharp z = p_r - 1, \sharp\tau = 1$, with $p_r = (m-r)(m+r+1)/2$. By [60, Ch. 11], e' is bounded by the sum of the coefficients of $q = (s_x + s_y + s_\tau)^{p_r}(s_y + s_z + s_\tau)^{n-1}(s_x + s_z + s_\tau)^{r(m-r)}$ modulo $I = \langle s_x^{n+1}, s_y^{r(m-r)+1}, s_z^{p_r}, s_\tau^2 \rangle \subset \mathbb{Z}[s_x, s_y, s_z, s_\tau]$. We see that $q = q_1 + s_\tau(q_2 + q_3 + q_4) + g$ with s_τ^2 that divides g and

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

Hence $q \equiv q_1 + s_\tau(q_2 + q_3 + q_4) \mod I$, and the bound is given by the sum of the contributions of q_1, q_2, q_3 and q_4 (multiplying q_2, q_3, q_4 by s_τ does not change the sum of the coefficients modulo I). The contribution of q_1 is the sum of the coefficients of its class modulo $I' = \langle s_x^{n+1}, s_y^{r(m-r)+1}, s_z^{p_r} \rangle$. This has been computed in Proposition 13, and coincides with $\theta(m,n,r)$. We compute the contribution of q_2. Let $q_2 = p_r \tilde{q}_2$. It is sufficient to compute the sum of the coefficients of $\tilde{q}_2$ modulo I' (defined above), multiplied by p_r. Since $\deg \tilde{q}_2 = n - 2 + p_r + r(m-r)$, and since the maximal powers admissible modulo I' are $s_x^n, s_y^{r(m-r)}$, and $s_z^{p_r-1}$, three configurations are possible.

(A) The coefficient of $s_x^{n-1} s_y^{r(m-r)} s_z^{p_r-1}$ in $\tilde{q}_2$, that is

$$\Sigma_A = \sum_k \binom{p_r - 1}{n-1-k} \binom{n-1}{k-1+p_r-r(m-r)} \binom{r(m-r)}{k};$$

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

$$\Sigma_B = \sum_k \binom{p_r - 1}{n-k} \binom{n-1}{k-1+p_r-r(m-r)} \binom{r(m-r)}{k};$$

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

$$\Sigma_C = \sum_k \binom{p_r - 1}{n-k} \binom{n-1}{k-2+p_r-r(m-r)} \binom{r(m-r)}{k}.$$

Hence we need to bound the expression $p_r(\Sigma_A + \Sigma_B + \Sigma_C)$. One can easily check that $\Sigma_A \leq \theta(m,n,r)$ and $\Sigma_B \leq \theta(m,n,r)$, while the same inequality is false for Σ_C. However, we claim that $\Sigma_C \leq (1 + \min\{n, p_r\})\, \theta(m,n,r)$ and hence that the contribution of q_2 is $p_r(\Sigma_A + \Sigma_B + \Sigma_C) \in \mathcal{O}\left(p_r \min\{n, p_r\}\, \theta(m,n,r)\right)$. We prove now this claim. Let

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

so that the sum in $\theta(m,n,r)$ runs over $\chi_1 \leq k \leq \chi_2$ and that in Σ_C over $\alpha_1 \leq k \leq \alpha_2$. Remark that $\chi_1 \leq \alpha_1$ and $\chi_2 \leq \alpha_2$. Denote by $\varphi(k)$ the $k-$th term in the sum defining Σ_C, and by $\gamma(k)$ the $k-$th term in the sum defining $\theta(m,n,r)$. Then for all indices k, admissible both for $\theta(m,n,r)$ and Σ_C, that is for $\alpha_1 \leq k \leq \chi_2$, one gets, by basic properties of binomial coefficients, that $\varphi(k) = \Psi(k)\, \gamma(k)$, with $\Psi(k) = \frac{k-1+p_r-r(m-r)}{n-k-p_r+r(m-r)-1}$. When k runs over all admissible indices, $\Psi(k)$ is non-decreasing monotone, and its maximum is $\Psi(\chi_2)$ and is bounded by $\min\{n, p_r\}$. We deduce the claimed inequality $\Sigma_C \leq (1 + \min\{n, p_r\})\, \theta(m,n,r)$, since if $\chi_2 < \alpha_2$ then $\chi_2 = \alpha_2 - 1$ and $\varphi(\alpha_2)$ is bounded above by $\theta(m,n,r)$.

Contributions of q_3 and q_4. As for q_2, we deduce that the contribution of q_3 is in $\mathcal{O}\left(n \min\{n, p_r\}\, \theta(m,n,r)\right)$ and that of q_4 is in $\mathcal{O}\left(r(m-r) \min\{n, p_r\}\, \theta(m,n,r)\right)$. □

We use this degree estimate to conclude our complexity analysis of LowRankSym.

Proposition 17 *Let $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$ be the input of* SolveLMI *and $0 \leq r \leq m-1$. Let $\theta(m,n,r)$ be the bound defined in Proposition 13. Let $p_r = (m-r)(m+r+1)/2$. Then* RatPar *returns a r.p. within $O^{\sim}\left(\binom{m}{r}(n+p_r+r(m-r))^7\,\theta(m,n,r)^2\right)$ arithmetic operations over $\mathbb{Q}$.*

Proof : Let ℓ be the simplified Lagrange system as in the proof of Proposition 13. We consider the bound on the degree of the homotopy curve given by Lemma 16. We deduce the claimed complexity result by applying [39, Proposition 6.1], and by recalling that there are $\binom{m}{r}$ many subsets of $\{1,\ldots,m\}$ of cardinality $m-r$. □

We straightforwardly deduce the following complexity estimate for SolveLMI.

Theorem 18 (Complexity of SolveLMI**)** *Let $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$ be the input symmetric pencil and suppose that* H *holds. Then the number of arithmetic operations performed by* SolveLMI *are in*

$$O^{\sim}\left(n\binom{\frac{m^2+m}{2}+n}{n}^6 \sum_{r\leq m-1}\binom{m}{r}(n+(m-r)(m+3r))^7\right).$$

Proof : From Proposition 17, we deduce that LowRankSymRec runs essentially within $O^{\sim}(\binom{m}{r}(n+p_r+r(m-r))^7\,\theta(m,n,r)^2)$ arithmetic operations. The inequality $\theta(m,n,r) \leq \binom{n+p_r}{n}^3$ is proved in Proposition 13. Moreover, there are at most n recursive calls of LowRankSymRec in LowRankSym, and SolveLMI stops at most when r reaches $m-1$. Finally, the cost of subroutines SolveLinear, CheckLMI, Project, Lift, Image and Union is negligible. We deduce that the complexity of SolveLMI is in $O^{\sim}\left(n\sum_{r\leq m-1}\binom{m}{r}(n+p_r+r(m-r))^7\binom{p_r+n}{n}^6\right)$ Since $p_r \leq p_0 = \frac{m^2+m}{2}$ and $p_r + r(m-r) \leq (m-r)(m+3r)$, we conclude. □

6 Experiments

SolveLMI is implemented in a MAPLE function, and it is part of a library called SPECTRA (Semidefinite Programming solved Exactly with Computational Tools of Real Algebra), released in September 2015. It collects efficient and exact algorithms solving a large class of problems in real algebraic geometry and semidefinite optimization.

We present in this section the results of our experiments. These have been performed on a machine with the following characteristics: Intel(R) Xeon(R) CPU E7540@2.00GHz with 256 Gb of RAM. We rely on the MAPLE implementation of the software FGB [17], for fast computation of Gröbner bases. To compute the rational parametrizations we use the implementation in MAPLE of the change-of-ordering algorithm FGLM [20] and of its improved versions [21, 19].

6.1 Generic symmetric pencils

We implemented the function LowRankSym and tested the running time of the implementation with input generic symmetric linear matrices. We recall that the algorithm

SolveLMI amounts to iterating LowRankSym by increasing the expected rank r. By generic data we mean that a natural number $N \in \mathbb{N}$ large enough is fixed, and numerators and denominators of the entries of $A_\ell, \ell = 0, \ldots, n$ are uniformly generated in the interval $[-N, N]$. We report in Table 2 the timings and the degrees of output rational parametrizations.

(m,r,n)	PPC	LRS	totaldeg	deg	(m,r,n)	PPC	LRS	totaldeg	deg
$(3,2,2)$	0.2	8	9	6	$(4,3,9)$	∞	28	40	0
$(3,2,3)$	0.3	11	13	4	$(4,3,10)$	∞	29	40	0
$(3,2,4)$	0.9	13	13	0	$(4,3,11)$	∞	30	40	0
$(3,2,5)$	5.1	14	13	0	$(5,2,2)$	0.6	0	0	0
$(3,2,6)$	15.5	15	13	0	$(5,2,3)$	0.9	0	0	0
$(3,2,7)$	31	16	13	0	$(5,2,4)$	1	1	0	0
$(3,2,8)$	109	17	13	0	$(5,2,5)$	1.6	1	0	0
$(3,2,9)$	230	18	13	0	$(5,2,7)$	∞	25856	175	140
$(4,2,2)$	0.2	0	0	0	$(5,3,2)$	0.4	1	0	0
$(4,2,3)$	0.3	2	10	10	$(5,3,3)$	0.5	3	20	20
$(4,2,4)$	2.2	9	40	30	$(5,3,4)$	∞	1592	110	90
$(4,2,5)$	12.2	29	82	42	$(5,3,5)$	∞	16809	317	207
$(4,2,6)$	∞	71	112	30	$(5,4,2)$	0.5	7	25	20
$(4,2,7)$	∞	103	122	10	$(5,4,3)$	10	42	65	40
$(4,2,8)$	∞	106	122	0	$(5,4,4)$	∞	42	105	40
$(4,2,9)$	∞	106	122	0	$(5,4,5)$	∞	858	121	16
$(4,3,3)$	1	10	32	16	$(6,3,3)$	4	0	0	0
$(4,3,4)$	590	21	40	8	$(6,3,4)$	140	1	0	0
$(4,3,5)$	∞	22	40	0	$(6,3,5)$	∞	2	0	0
$(4,3,6)$	∞	24	40	0	$(6,3,6)$	∞	704	112	112
$(4,3,7)$	∞	26	40	0	$(6,4,2)$	0.6	1	0	0
$(4,3,8)$	∞	27	40	0	$(6,5,3)$	∞	591	116	80

Table 2: Timings and degrees for dense symmetric linear matrices

We recall that m is the size of the input matrix, n is the number of variables and r is the expected maximum rank (that is, the index of the algebraic set $\mathcal{D}_r$). We compare our timings (reported in LRS) with those of the function PointsPerComponents (column PPC) of the library RAGLIB developed by the third author [56]. The input of PointsPerComponents are the $(r+1) \times (r+1)$ minors of the linear matrix, and the output is a rational parametrization of a finite set meeting each connected component of $\mathcal{D}_r \cap \mathbb{R}^n$. We do not consider the time needed to compute all the minors of $A(x)$ in PPC. The symbol ∞ means that we did not succeed in computing the parametrizations after 48 hours. Column deg contains the degree of the parametrization returned by LowRankSymRec at Step 2, or 0 if the empty list is returned. Column totaldeg contains the sum of the values in deg for k varying between 1 and n. For example, for $m = 4, r = 2$, for $n \leq 2$ and $n \geq 8$ the algorithm does not compute critical points, while it computes rational parametrizations of degree respectively $10, 30, 42, 30, 10$ for $n = 3, 4, 5, 6, 7$; the number 82 in totaldeg for $(m, n, r) = (4, 2, 5)$ is obtained as the sum $10 + 30 + 42$ of the integers in deg for $m = 4, r = 2$ and $n = 3, 4, 5$. We remark that, as for Table 1, the value in deg for a given triple m, n, r coincides with the algebraic degree of semidefinite programming, that is $\delta(n, m, r)$ as defined in [48].

Our algorithm allows to tackle examples that are out of reach for RAGLIB and that, most

of the time, the growth in terms of running time is controlled when m, r are fixed. This shows that our dedicated algorithm leads to practical remarkable improvements: indeed, for example, 4×4 linear matrices of expected rank 2 are treated in a few minutes, up to linear sections of dimension 9; we are also able to sample hypersurfaces in $\mathbb{R}^5$ defined by the determinant of 5×5 symmetric linear matrices; finally, symmetric linear matrices of size up to 6 with many rank defects are shown to be tractable by our approach. We observe that most of the time is spent to compute a Gröbner basis of the Lagrange systems, and for this we use new fast algorithms for the change of monomial orderings [19].

6.2 Scheiderer's spectrahedron

We consider the symmetric pencil

$$A(x) = \begin{pmatrix} 1 & 0 & x_1 & 0 & -3/2 - x_2 & x_3 \\ 0 & -2x_1 & 1/2 & x_2 & -2 - x_4 & -x_5 \\ x_1 & 1/2 & 1 & x_4 & 0 & x_6 \\ 0 & x_2 & x_4 & -2x_3 + 2 & x_5 & 1/2 \\ -3/2 - x_2 & -2 - x_4 & 0 & x_5 & -2x_6 & 1/2 \\ x_3 & -x_5 & x_6 & 1/2 & 1/2 & 1 \end{pmatrix}.$$

which is the *Gram matrix* of the trivariate polynomial

$$f(u_1, u_2, u_3) = u_1^4 + u_1 u_2^3 + u_2^4 - 3u_1^2 u_2 u_3 - 4u_1 u_2^2 u_3 + 2u_1^2 u_3^2 + u_1 u_3^3 + u_2 u_3^3 + u_3^4.$$

In other words, $f = v^T A(x) v$ for all $x \in \mathbb{R}^6$, where $v = (u_1^2, u_1 u_2, u_2^2, u_1 u_3, u_2 u_3, u_3^2)$ is the monomial basis of the vector space of homogeneous polynomials of degree 2 in u_1, u_2, u_3. Since f is globally nonnegative, by Hilbert's theorem [38] it is a sum of at most three squares in $\mathbb{R}[u_1, u_2, u_3]$, namely there exist $f_1, f_2, f_3 \in \mathbb{R}[u_1, u_2, u_3]$ such that $f = f_1^2 + f_2^2 + f_3^2$. Moreover, the spectrahedron $\mathscr{S} = \{x \in \mathbb{R}^6 : A(x) \succeq 0\}$ parametrizes all the sum-of-squares decompositions of f (and it is a particular example of a *Gram spectrahedron*). Hence $\mathscr{S}$ must contain a matrix of rank at most 3.

Scheiderer proved in [61] that f does not admit a sum-of-squares decomposition in the ring $\mathbb{Q}[u_1, u_2, u_3]$, that is, the summands f_1, f_2, f_3 cannot be chosen to have rational coefficients, answering a question of Sturmfels. We deduce that $\mathscr{S}$ does not contain points with rational coordinates. In particular, it is not full-dimensional (its affine hull has dimension ≤ 5) by straightforward density arguments.

We first easily check that $\mathcal{D}_0 \cap \mathbb{R}^6 = \mathcal{D}_1 \cap \mathbb{R}^6 = \emptyset$). Further, for $r = 2$, the algorithm returns the following rational parametrization of $\mathcal{D}_2 \cap \mathbb{R}^6$:

$$\left(\frac{3 + 16t}{-8 + 24t^2}, \frac{8 - 24t^2}{-8 + 24t^2}, \frac{8 + 6t + 8t^2}{-8 + 24t^2}, \frac{16 + 6t - 16t^2}{-8 + 24t^2}, \frac{-3 - 16t}{-8 + 24t^2}, \frac{3 + 16t}{-8 + 24t^2} \right).$$

where t satisfies $8t^3 - 8t - 1 = 0$. The set $\mathcal{D}_2$ is, indeed, of dimension 0, degree 3, and it contains only real points. Remark that the technical assumption P_2 is not satisfied here, since the expected dimension of $\mathcal{D}_2$ is -1. Conversely, the regularity assumptions on the incidence varieties are satisfied. By applying CheckLMI one gets that two of the three points lie on $\mathscr{S}$, that is those with the following floating point approximation up to 9

certified digits:

$$\begin{pmatrix} -0.930402926 \\ -1.000000000 \\ 0.731299211 \\ -0.268700788 \\ 0.930402926 \\ -0.930402926 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -0.127050844 \\ -1.000000000 \\ -0.967716166 \\ -1.967716166 \\ 0.127050844 \\ -0.127050844 \end{pmatrix}.$$

These correspond to the two distinct decompositions of f as a sum of 2 squares. An approximation of such representations can be computed by factorizing the matrix $A(x(t^*)) = V^T V$ where t^* is the corresponding root of $8t^3 - 8t - 1$ and $V \in \mathbb{M}_{2,6}(\mathbb{R})$ is full rank. The corresponding decomposition is $f = v^T V^T V v = ||Vv||^2$. At the third point of $\mathcal{D}_2 \cap \mathbb{R}^6$ the matrix $A(x)$ is indefinite, so it is not a valid Gram matrix.

To conclude, SolveLMI allows to design a computer-aided proof of Scheiderer's results. This example is interesting since the interior of $\mathscr{S}$ is empty and, typically, this can lead to numerical problems when using interior-point algorithms.

7 Conclusion

We have presented a probabilistic exact algorithm that computes an algebraic representation of at least one feasible point of a LMI $A(x) \succeq 0$, or that detects emptiness of $\mathscr{S} = \{x \in \mathbb{R}^n : A(x) \succeq 0\}$. The algorithm works under assumptions which are proved to be generically satisfied. When these assumptions are not satisfied, the algorithm may return a wrong answer or raises an error (when the dimension of some Lagrange system is not 0). The main strategy is to reduce the input problem to a sequence of real root finding problems for the loci of rank defects of $A(x)$: if $\mathscr{S}$ is not empty, we have shown that computing sample points on determinantal varieties is sufficient to sample $\mathscr{S}$, and that it can be done efficiently. Indeed, the arithmetic complexity is essentially quadratic on a multilinear Bézout bound on the output degree.

This is, to our knowledge, the first exact computer algebra algorithm tailored to linear matrix inequalities. We conjecture that our algorithm is optimal since the degree of the output parametrization matches the algebraic degree of a generic semidefinite program, with expected rank equal to the minimal achievable rank on $\mathscr{S}$. Since deciding the emptiness of $\mathscr{S}$ is a particular instance of computing the minimizer of a linear function over this set (namely, of a constant), our algorithm is able to compute minimal-rank solutions of special semidefinite programs, which is, in general, a hard computational task. Indeed, numerical interior-point algorithms typically return approximations of feasible matrices with maximal rank among the solutions (those lying in the relative interior of the optimal face). Moreover, the example of Scheiderer's spectrahedron shows that we can also tackle degenerate situations with no interior point which are typically numerically troublesome.

To conclude, as highlighted by the discussions in Section 6, our viewpoint includes an effective aspect, by which it is essential to translate into practice the complexity results that have been obtained. This is the objective of our MAPLE library SPECTRA. It must

be understood as a starting point towards a systematic exact computer algebra approach to semidefinite programming and related questions.

References

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

[2] B. Bank, M. Giusti, J. Heintz, M. Safey El Din, É. Schost. On the geometry of polar varieties. Appl. Alg. in Eng., Comm. and Comp. 21(1):33–83, 2010.

[3] B. Bank, M. Giusti, J. Heintz, G.-M. Mbakop. Polar varieties and efficient real elimination. Mathematische Zeitschrift, 238(1):115–144, 2001.

[4] R. G. Bartle, D. R. Sherbert. Introduction to real analysis. John Wiley & Sons, New York, 1992.

[5] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. Journal of the ACM, 43(6):1002-1046, 1996.

[6] S. Basu, R. Pollack, and M.-F. Roy. Algorithms in real algebraic geometry. Algorithms and Computation in Mathematics, Vol. 10. Springer Verlag, Berlin, 2006.

[7] A. Ben-Tal, A. Nemirovski. Lectures on modern convex optimization: analysis, algorithms, engineering applications. MPS-SIAM Series on Optimization, SIAM, Philadelphia, 2001.

[8] G. Blekherman, P. A. Parrilo, R. R. Thomas (Editors). Semidefinite optimization and convex algebraic geometry. SIAM, Philadelphia, 2013.

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

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

[11] M. Claeys. Mesures d'occupation et relaxations semi-définies pour la commande optimale. PhD thesis, LAAS CNRS, Univ. Toulouse, France, Oct. 2013.

[12] G. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decompostion. Automata Theory and Formal Languages, pages 134–183. Springer, Berlin, 1975.

[13] D. A. Cox, J. Little, D. O'Shea. Ideals, varieties, and algorithms. 3rd edition, Springer, New York, 2007.

[14] Dahan, X. and Schost, É.. Sharp estimates for triangular sets, Proceedings of the 2004 international symposium on Symbolic and algebraic computation, pp. 103–110, 2004.

[15] J. Draisma, E. Horobet, G. Ottaviani, B. Sturmfels, R.R. Thomas. The Euclidean distance degree of an algebraic variety. Found. of Comp. Math., 16(1):99–149, 2016.

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

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

[18] J.-C. Faugère, M. Safey El Din, P.-J. Spaenlehauer. On the complexity of the generalized MinRank problem. J. of Symb. Comp. 55:30–58, 2013.

[19] J.-C. Faugère, P. Gaudry, L. Huot, G. Renault. Polynomial systems solving by fast linear algebra. `arXiv:1304.6039`, Apr. 2013.

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

[21] J.-C. Faugère, C. Mou. Sparse FGLM algorithms. `arXiv:1304.1238`, Apr. 2013.

[22] J.-C. Faugère, M. Safey El Din and P.-J. Spaenlehauer. Critical points and Gröbner bases: the unmixed case. Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation, pp. 162–169, 2012.

[23] M. Giusti, G. Lecerf, B. Salvy. A Gröbner Free Alternative for Polynomial System Solving. Journal of Complexity, 17:154-211, 2011.

[24] H.-C. Graf v. Bothmer, K. Ranestad. A general formula for the algebraic degree in semidefinite programming. Bulletin of LMS, 41:193–197, 2009.

[25] 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.

[26] D. Grigoriev, N. Vorobjov. Solving systems of polynomial inequalities in subexponential time. J. of Symb. Comp., 5:37–64, 1988.

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

[28] Q. Guo, M. Safey El Din, L. Zhi. Computing rational solutions of linear matrix inequalities. Proceedings of ISSAC 2013, Boston, USA, 2013.

[29] F. Guo, E. Kaltofen, L. Zhi. Certificates of impossibility of Hilbert-Artin representations of a given degree for definite polynomials and functions. Proceedings of ISSAC 2012, Grenoble, France, 195–202, 2012.

[30] J. Harris. Algebraic geometry. A first course. Springer, New York, 1992.

[31] J. Heintz, M.-F. Roy, P. Solernó. Description of the connected components of a semi-algebraic set in single exponential time. Disc. and Comp. Geom. 11:121–140, 1994.

[32] J. W. Helton, J. Nie. Sufficient and necessary conditions for semidefinite representability of convex hulls and sets. SIAM J. Opt. 20, 759–791, 2009.

[33] D. Henrion. Optimization on linear matrix inequalities for polynomial systems control. Lecture notes of the International Summer School of Automatic Control, Grenoble, France, 2014.

[34] D. Henrion, S. Naldi, M. Safey El Din. Real root finding for determinants of linear matrices. J. of Symb. Comp. 74:205–238, 2016.

[35] 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.

[36] D. Henrion, S. Naldi, M. Safey El Din. Real root finding for low rank linear matrices. `arXiv:1506.05897`, May 2015.

[37] D. Henrion, J.B. Lasserre, C. Prieur, E. Trélat. Nonlinear optimal control via occupation measures and LMI relaxations. SIAM J. Control Opt. 47(4):1643–1666, 2008.

[38] D. Hilbert. Über die Dartstellung definiter Formen als Summe von Formenquadraten. Math. Ann. 32, 342–350, 1888.

[39] G. Jeronimo, G. Matera, P. Solernó, and A. Waissbein. Deformation techniques for sparse systems. Found. of Comp. Math., 9(1):1–50, 2009.

[40] L. Khachiyan and L. Porkolab. On the complexity of semidefinite programs. J. Global Optim., 10:351365, 1997.

[41] I. Klep, M. Schweighofer. An exact duality theory for semidefinite programming based on sums of squares. Mathematics of Operations Research, 38(3):569-590, 2013.

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

[43] M. Laurent. Sums of squares, moment matrices and optimization over polynomials. In M. Putinar and S. Sullivant (Editors). Emerging Applications of Algebraic Geometry, Vol. 149 of IMA, Volumes in Mathematics and its Applications, 157–270, Springer, New York, 2009

[44] H. Lombardi, D. Perrucci, M.-F. Roy. An elementary recursive bound for the effective Positivestellensatz and Hilbert 17th problem. `arXiv:1404.2338`, 2014.

[45] S. Melczer, B. Salvy. Symbolic-Numeric Tools for Analytic Combinatorics in Several Variables. Proceedings of ISSAC 2016, Waterloo, ACM, pp. 333–340, 2016.

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

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

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

[49] J. Nie, M. Schweighofer. On the complexity of Putinar Positivstellensatz. Journal of Complexity 23(1):135–150, 2007.

[50] G. Ottaviani, P.-J. Spaenlehauer, B. Sturmfels. Exact solutions in structured low-rank approximation. SIAM J. Matrix Analysis Appl. 35(4):1521–1542, 2014.

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

[52] M. Putinar. Positive polynomials on compact sets. Indiana University Mathematics Journal. 42(3):969–984, 1993.

[53] M. Ramana, A.J. Goldman. Some geometric results in semidefinite programming. J. Global Optim., 7:33–50, 1995.

[54] J. Renegar. On the computational complexity and geometry of the first order theory of the reals. J. of Symb. Comp. 13(3):255–352, 1992.

[55] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. Appl. Alg. in Eng., Comm. and Comp. 9(5):433–461, 1999.

[56] M. Safey El Din. Raglib, Maple package. `www-polsys.lip6.fr/~safey`

[57] M. Safey El Din, L. Zhi. Computing rational points in convex semi-algebraic sets and sums of squares decompositions. SIAM J. Opt., 20(6):2876–2889, 2010.

[58] M. Safey El Din, É. Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. Proceedings of ISSAC 2003, Philadelphia, 2003.

[59] M. Safey El Din, É. Schost. Properness defects of projections and computation of one point in each connected component of a real algebraic set. Discrete and Computational Geometry, 32(3):417–430, 2004.

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

[61] C. Scheiderer. Sums of squares of polynomials with rational coefficients. `arXiv:1209.2976`, Sep. 2012.

[62] C. Scheiderer. Semidefinite representation for convex hulls of real algebraic curves. `arXiv:1208.3865`, Aug. 2012.

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

[64] K. Schmüdgen. The K-moment problem for compact semi-algebraic sets. Math. Ann. 289:203–206, 1991.

[65] M. Schweighofer. On the complexity of Schmüdgen Positivstellensatz. J. of Complexity 20, 529–543, 2004.

[66] R. Sinn, B. Sturmfels. Generic spectrahedral shadows. SIAM J. Opt., 25(2):1209–1220, 2015.

[67] S. Tarbouriech, G. Garcia, J.M. Gomes da Silva, I. Queinnec. Stability and stabilization of linear systems with saturating actuators. Springer, London, 2011.