Exact algorithms for linear matrix inequalities

Didier Henrion, Simone Naldi, Mohab Safey El Din

Exact algorithms for linear matrix inequalities

Didier Henrion[1,2,3] Simone Naldi[1,2] Mohab Safey El Din[4,5,6,7]

August 14, 2015

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 the size m of the pencil is fixed, such a bound, and hence the complexity, is polynomial in n, the number of variables. 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]CNRS, LAAS, 7 avenue du colonel Roche, F-31400 Toulouse; France.

[2]Université de Toulouse; LAAS, F-31400 Toulouse, France.

[3]Faculty of Electrical Engineering, Czech Technical University in Prague, Czech Republic.

[4]Sorbonne Universités, UPMC Univ Paris 06, Equipe PolSys, LIP6, F-75005, Paris, France.

[5]INRIA Paris-Rocquencourt, PolSys Project, France.

[6]CNRS, UMR 7606, LIP6, France.

[7]Institut Universitaire de France.

1 Introduction

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

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

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

Here $\succeq 0$ means "positive semidefinite" and the relation $A(x) \succeq 0$ is called a *linear matrix inequality* (LMI). The set $\mathscr{S}$ is closed and basic semi-algebraic, since it can be represented by sign conditions on the coefficients of the characteristic polynomial of the pencil. Indeed, if $\mathbb{I}_m$ is the identity matrix in $\mathbb{S}_m(\mathbb{Q})$, and $\det(A(x) + s\,\mathbb{I}_m) = f_m(x) + f_{m-1}(x)s + \cdots + f_1(x)s^{m-1} + s^m$ is the characteristic polynomial of $A(x)$, then

$$\mathscr{S} = \{x \in \mathbb{R}^n : f_1(x) \geq 0, \ldots, f_m(x) \geq 0\}$$

by Descartes' rule of signs. Moreover, it is a convex set, since for every $x, y \in \mathscr{S}$ it holds $A(tx + (1-t)y) = tA(x) + (1-t)A(y) \succeq 0$, for every $t \in [0, 1]$. This paper addresses the following decision problem for the spectrahedron $\mathscr{S}$:

Main Problem

Compute an exact algebraic representation of at least one point in $\mathscr{S}$, or decide that $\mathscr{S}$ is empty.

We present a probabilistic algorithm for solving this problem. If $\mathscr{S}$ is not empty, the expected output is a rational parametrization of a finite set $\mathscr{Z} \subset \mathbb{C}^n$ meeting $\mathscr{S}$ in at least one point x^* such that $A(x^*)$ has minimum rank among the matrices in $\{A(x) : x \in \mathscr{S}\}$. Indeed, as an outcome of designing our algorithm, we also compute the minimum rank attained by the pencil on the spectrahedron. This parametrization is represented by a vector $(q_0, q_1, \ldots, q_n, q_{n+1}) \subset \mathbb{Q}[t]$ of univariate polynomials with rational coefficients such that, for every $x = (x_1, \ldots, x_n) \in \mathscr{Z}$, there exists $t \in \mathbb{C}$ such that

$$q_{n+1}(t) = 0, \qquad \text{and} \qquad x_i = \frac{q_i(t)}{q_0(t)}, \ \ i = 1, \ldots, n,$$

(*cf.* [69]). Moreover, the points in $\mathscr{Z}$ are in one-to-one correspondence with the roots of q_{n+1}. Consequently, from this representation, the coordinates of the feasible point $x^* \in \mathscr{S}$ can be computed with arbitrary precision just 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 can model a large number of computational problems in practical applications [11, 83]. This includes one of the most important questions in computational algebraic geometry, that is the general polynomial optimization problem. Indeed, Lasserre [51] 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 [57]. 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

$$\begin{array}{ll} \min\limits_{x\in\mathbb{R}^n} & \sum\limits_{i=1}^{n} c_i x_i \\ \text{s.t.} & A(x) \succeq 0 \end{array} \tag{1}$$

is empty or not. The feasible set of the SDP (1) is defined by an LMI and hence it is a spectrahedron. Our Main Problem amounts to solving the feasibility problem for semidefinite programming, in exact arithmetic: given a $\mathbb{Q}-$definable semidefinite program as in (1) (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 (1) is attained or not, and for computing such a minimum in the affirmative case. While the number of iterations performed by the ellipsoid algorithm [32] to compute the approximation of a solution of (1) 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 (1) is related to its algebraic degree δ as computed in [58, 30], 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.

Moreover, the class of spectrahedra is of outstanding and independent interest in convex algebraic geometry. For example, it is currently conjectured, by Helton and Nie [40], that every convex closed semi-algebraic set $S \subset \mathbb{R}^p$ admits a *semidefinite representation*, that is it can be obtained as the projection of a spectrahedron $\mathscr{S} \subset \mathbb{R}^{p+d}$ over the first p variables, with the help of d lifting variables. This conjecture was proved by Scheiderer for $p = 2$ [76], however without an estimate of the number d of lifting variables. The conjecture remains unsolved for $p \geq 3$. Remark here that when a semidefinite representation of the set $S \subset \mathbb{R}^p$ is explicitely given, as

$$S = \{x \in \mathbb{R}^p : \exists\, y \in \mathbb{R}^d \,\text{such that}\, (x, y) \in \mathscr{S}\}$$

for some linear matrix $A(x,y) = A_0 + \sum_i x_i B_i + \sum_j y_j C_j$ defining a spectrahedron

$$\mathscr{S} = \{(x,y) \in \mathbb{R}^{p+d} : A(x,y) \succeq 0\},$$

then solving our Main Problem with input matrices $(A_0, B_1 \ldots, C_1 \ldots)$ straightforwardly yields a sample point lying in the semidefinite representable set S (obtained just discarding the last d variables). Thus we can also use our algorithm for deciding the emptiness of semidefinite representable sets. Moreover, from [80, Th. 1.1] we know that the irreducible components of the algebraic boundary of S are in one-to-one correspondence with the rank strata of $\mathscr{S}$.

Hence, any algorithmic approach to spectrahedra is desirable, mainly via exact computation, and solving our problem represents a first step towards more challenging decision or sampling problems involving these semi-algebraic sets or their linear projections. Among these, computing the affine dimension or a sample point in the relative interior of the input set seems to be particularly interesting. Indeed, checking full-dimensionality of a spectrahedron $\mathscr{S}$, or computing the linear equations of the minimal affine space containing $\mathscr{S}$, is important for the primal-dual formulation of the associated SDP problems.

We finally recall that solving LMIs is a basic subroutine of computer algorithms in systems control and optimization, especially in linear systems robust control [10, 44], but also for the analysis or synthesis of nonlinear dynamical systems [82], or in nonlinear optimal control with polynomial data [42, 14].

1.2 State of the art

As mentioned already, the set $\mathscr{S}$ is defined by sign conditions on the m coefficients of the characteristic polynomial of $A(x)$. These coefficients are polynomial functions of $x = (x_1, \ldots, x_n)$, and hence our Main Problem boils down to deciding the emptiness of a semi-algebraic set.

Deciding whether a semi-algebraic set is empty or not and, in the negative case, exhibiting a sample set of its elements, is a central question in computational real algebraic geometry [7]. A first algorithmic solution is given by Collins' Cylindrical Algebraic Decomposition algorithm [15], which solves the stronger problem of real quantifier elimination. The runtime of Collins' algorithm is doubly exponential in the number n of variables, while, by the Thom-Milnor bound, the number of connected components of a semi-algebraic subset of $\mathbb{R}^n$ is singly exponential in n. Thus, many efforts have been made to obtain optimal complexity bounds, that is also singly exponential in the number n of variables. The first singly exponential algorithm is due to Grigoriev and Vorobjov [29], and is based on the critical points method. Further works of Renegar [67], Heintz, Roy and Solernó [36], Basu, Pollack and Roy [6] also are based on the critical points method and have improved the previous algorithms. Moreover, the emptiness problem for semi-algebraic sets is related to that of computing finite sets meeting every connected component of a real algebraic set, the so-called real root finding problem (*cf.* [7, Prop. 13.1]). An efficient theoretical tool for the real root finding problem is the theory of polar varieties, developed in last decades towards an effective use in real algebraic geometry, see for example [3, 4, 71, 72]. The probabilistic algorithm in [31], which also relies on the construction of polar varieties,

can be used to decide the emptiness of $\mathscr{S}$, and its runtime applied to our problem is essentially cubic in m^{2n}, and linear in the complexity of evaluating the input.

For example, the algorithms in [7, Ch. 13] computes a description of the connected components of the input semi-algebraic set. Applied to $\mathscr{S}$, it would run within $m^{\mathcal{O}(n)}$ arithmetic operations. Such algorithms do not exploit the particular structure of spectrahedra understood as determinantal semi-algebraic sets. This structure has been recently exploited in [23, 24] for the fast computation of Gröbner bases of zero-dimensional determinantal ideals. In [48], the authors showed that deciding emptiness of $\mathscr{S}$ can be done in time $\mathcal{O}(m^{\min(n,m^2)})$, that is in polynomial time if either n or m is fixed. The main drawback of this algorithm is that it is based on Renegar's quantifier elimination, and hence it does not lead to efficient practical implementations. In [37, 38, 39] we designed a series of algorithms dedicated to the real root finding problem for positive-dimensional determinantal systems. Finally, the algorithm in [33], a version of [70] for spectrahedra, 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 5.2 we will apply our algorithm to one of these examples.

To get a purely algebraic certificate of emptiness for $\mathscr{S}$, one could use the classical approach by Positivstellensatz [53, 64, 78]. For example, Theorem 3.15 in [53] gives a Positivstellensatz certificate for the emptiness of any semi-algebraic set. As a snake biting his tail, this would lead to a family, or hierarchy, of semidefinite programs [51]. Indeed, by fixing an upper bound for the degrees of the sum-of-squares multipliers, the resulting problem is semidefinite in their unknown coefficients. Bounds for the degree of Positivstellensatz certificates are exponential in the number of variables and have been computed in [79] for Schmudgen's, and in [59] for Putinar's formulation. In the recent remarkable result of Lombardi, Perrucci and Roy described in [54], a uniform $5-$fold exponential bound for the degree of the Hilbert 17th problem, which asks for similar certificates for nonnegative polynomials as sums of squares of rational functions, has been provided. Klep and Schweighofer recently obtained an emptiness certificate dedicated to the spectrahedral case, by means of special quadratic modules associated to these sets [49]. It is shown there that deciding emptiness of $\mathscr{S}$ amounts to solving a sufficiently large SDP problem (whose size is exponential in either n or m), but for this latter task one has to use floating point implementations of interior-point algorithms.

1.3 Contribution and outline

The main contribution of this paper is the design of a computer algebra algorithm for solving the feasibility problem of semidefinite programming 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 [8, 56] can nowadays handle inputs with a high number of variables that are out of reach for our algorithms. Our goal here 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;

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 is full-dimensional, and hence it can also tackle instances with no interior point.

The main idea for solving our Main Problem is to exploit the relation between the geometry of spectrahedra and semidefinite programming, 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 Euclidean boundary of $\mathscr{S}$, denoted by $\partial\mathscr{S}$, 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 this first result, 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

$r \in \{0, \ldots, m-1\}$. This algorithm shares some features with those in [37, 39] and represents a generalization of the algorithm in [38] to the vector space of real symmetric matrices.

As in [37, 38, 39], 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 the Main Problem 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 for r satisfying $n < \binom{m-r+1}{2}$, the set $\mathcal{D}_r$ is empty. 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 $q = (q_0, q_1, \ldots, q_n, q_{n+1}) \in \mathbb{Q}[t]^{n+2}$ 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

$$O^{\sim}\left(n \sum_{r \leq m-1} \binom{m}{r} (n + p_r + r(m-r))^7 \binom{p_r + n}{n}^6\right) \quad \text{if } \mathscr{S} \text{ is empty, and}$$

$$O^{\sim}\left(n \sum_{r \leq r(A)} \binom{m}{r} (n + p_r + r(m-r))^7 \binom{p_r + n}{n}^6\right) \quad \text{if } \mathscr{S} \text{ is not empty,}$$

with $p_r = (m-r)(m+r+1)/2$. If $\mathscr{S}$ is not empty, the degree of q is in

$$\mathcal{O}\left(\binom{m}{r(A)} \binom{p_{r(A)} + n}{n}^3\right).$$

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 4. As highlighted by Theorem 3, the number of arithmetic operations and the degree of the output representation are bounded by explicit expressions involving the three parameters m, n and r. These bounds are computed by exploiting the multilinearity of intermediate polynomial systems generated during the procedure, and they are not sharp in general. By experiments on randomly generated symmetric pencils, reported in Section 5, we observe that the output degree coincides with the algebraic degree of generic semidefinite programs associated to $A(x)$, that is with data given in [58, Table 2]: this evidences the optimality of our approach. We did not succeed in proving exact formulas for such degrees. This is a work in progress, and we leave it as a conjecture (*cf.* Conjecture 13).

2 The smallest rank on a spectrahedron

In this section, 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, at all points of $\mathscr{S}$, the matrix A has rank at least $r = r(A)$ and there exists a point in $\mathscr{S}$ where the rank of A is exactly r. 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 $\mathcal{C} \subset \mathcal{D}_r \cap \mathbb{R}^n$ be the given connected component such that $\mathcal{C} \cap \mathscr{S} \neq \emptyset$, and let $x \in \mathcal{C} \cap \mathscr{S}$. One has $\operatorname{rank} A(x) = r$ and

$$e_1(x) = \ldots = e_{m-r}(x) = 0 < e_{m-r+1}(x) \leq \ldots \leq e_m(x).$$

Suppose that there exists $y \in \mathcal{C}$ such that $y \notin \mathscr{S}$; that is $\operatorname{rank} A(y) \leq r$ but $A(y)$ is not positive semidefinite. 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 $0 \in T$ (in fact, $g(0) = x \in \mathscr{S}$) 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, $\tilde{x}, \tilde{x}_p \in \mathcal{C} \subset \mathcal{D}_r \cap \mathbb{R}^n$ for all $p \geq N$, and since $\tilde{x} \in \mathscr{S}$, we get $\operatorname{rank} A(\tilde{x}) = r$ and

$\operatorname{rank} A(\tilde{x}_p) \leq r$ for all $p \geq N$. We also get that $\operatorname{rank} A(g(t)) = r$ 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

$$\varphi \colon \Big\{ p \in \mathbb{N} : p \geq N \Big\} \to \big\{ 0, 1, \ldots, r \big\}$$

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 $\operatorname{rank} A(\tilde{x}_p) \leq r$ for all p, then $0 \leq \varphi(p) \leq r$ for all p, and the map is well defined. In other words, the eigenvalues of $A(\tilde{x}_p)$ are

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

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 [1, Th. 3.4.8]. Since it is an integer-value sequence, this limit point is an integer number. Moreover, if $0 \leq \ell \leq r$ is a limit point, and $\{p_j\}_{j \in \mathbb{N}}$ a subsequence such that $\varphi(p_j) \to \ell$, then we claim that there exists an integer N' such that $\varphi(p_j) = \varphi(p_{j+1}) = \ell$ for all $j \geq N'$ (which means that $j \mapsto \varphi(p_j)$ is constant for $j \geq N'$): this holds since the map φ takes only integer values.

Suppose that there exists a limit point $\ell > 0$ (strictly positive), and let $\{p_j\}_{j \in \mathbb{N}}$ and N' be as above. One obtains that $\varphi(p_j) \to \ell$ and that this sequence is constant for $j \geq N'$. Thus, the zero eigenvalues of $A(\tilde{x}_{p_j})$ are

$$0 = \lambda_{\ell+1}(\tilde{x}_{p_j}) = \ldots = \lambda_{\ell+m-r}(\tilde{x}_{p_j}),$$

for all $j \geq N'$. Since $\tilde{x}_{p_j} \to \tilde{x}$ and $e_1, \ldots, e_m$ are continuous functions, we obtain that

$$\begin{aligned} e_1(\tilde{x}) \leq \ldots \leq e_\ell(\tilde{x}) \leq 0, \\ 0 = e_{\ell+1}(\tilde{x}) = \ldots = e_{\ell+m-r}(\tilde{x}), \\ 0 \leq e_{\ell+m-r+1}(\tilde{x}) \leq \ldots \leq e_m(\tilde{x}). \end{aligned}$$

Since $A(\tilde{x}) \succeq 0$, one gets $0 = e_1(\tilde{x}) = \ldots = e_{\ell+m-r}(\tilde{x})$, that is $A(\tilde{x})$ has at least $\ell + m - r > m - r$ zero eigenvalues. This implies that $\operatorname{rank} A(\tilde{x}) \leq r - 1$, which is a contradiction, since we assumed $\tilde{x} \in \mathscr{S}$ and that r is the minimum rank attained by A on $\mathscr{S}$.

We deduce that 0 is the unique limit point of φ, hence φ converges to 0. We already showed that in this case $\varphi(p) = 0$ for $p \geq N''$, for some $N'' \in \mathbb{N}$. This means in particular that for $p \geq N''$, the number of strictly negative eigenvalues of $A(\tilde{x}_p) = A(g(t_0 + \frac{1}{p}))$ is zero, that is the matrix A is positive semidefinite at any point in $\{\tilde{x}_p : p \geq N''\}$. So this set is included in $\mathscr{S}$, which contradicts our assumptions. We conclude that the set $\mathcal{C} \setminus \mathscr{S}$ is empty, that is $\mathcal{C} \subset \mathscr{S}$. By the minimality of the rank r in $\{\operatorname{rank} A(x) : x \in \mathscr{S}\}$, one deduces that $\mathcal{C} \subset (\mathcal{D}_r \setminus \mathcal{D}_{r-1}) \cap \mathbb{R}^n$. □

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

Basic notation

We refer to textbooks [7, 16, 35, 18] for the algebraic-geometric background of this paper. We recall below some basic definitions and notation.

We denote by $\mathbb{S}_m(\mathbb{Q})$ the vector space of symmetric matrices of size m with entries in $\mathbb{Q}$. Similarly, $\mathbb{M}_{p,q}(\mathbb{Q})$ denotes the space of $p \times q$ matrices with entries in $\mathbb{Q}$. We denote by $\mathrm{GL}_n(\mathbb{C})$ the set of $n \times n$ non-singular complex matrices. The tranpose of $M \in \mathbb{M}_{p,q}(\mathbb{Q})$ is M'. The cardinality of a finite set T or the number of entries of a vector v are denoted by $\#T$ and $\#v$.

A vector of polynomials $f = (f_1, \ldots, f_s) \subset \mathbb{Q}[x]$, with $x = (x_1, \ldots, x_n)$, is called a polynomial system. The ideal generated by its elements is denoted by $\langle f \rangle \subset \mathbb{Q}[x]$ and the associated algebraic set $\{x \in \mathbb{C}^n : f_i(x) = 0, i = 1, \ldots, s\}$ by $Z(\langle f \rangle)$. Algebraic sets 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 $\mathcal{Z} \subset \mathbb{C}^n$ algebraic set, we denote the set $\{x \in \mathbb{C}^n : M\,x \in \mathcal{Z}\}$ by $M^{-1}\mathcal{Z}$. The real trace $Z(\langle f \rangle) \cap \mathbb{R}^n$ is denoted by $Z_{\mathbb{R}}(\langle f \rangle)$ and is called a real algebraic set. Given a set $S \subset \mathbb{C}^n$, we denote by $I(S) \subset \mathbb{C}[x]$ the set of polynomials vanishing at every point of S. The set $I(S)$ is an ideal of $\mathbb{C}[x]$.

Let $f = (f_1, \ldots, f_s) \subset \mathbb{Q}[x]$. Its $s \times n$ 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 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. Otherwise, the union of its irreducible component of dimension p is called the equidimensional component of dimension p. 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 $\mathrm{sing}\,(\mathcal{Z})$, is the algebraic set defined by $f = (f_1, \ldots, f_s)$ and by all $c \times c$ minors of Df. If $\mathrm{sing}\,(\mathcal{Z}) = \emptyset$ we say that $\mathcal{Z}$ is smooth, otherwise singular. The points in $\mathrm{sing}\,(\mathcal{Z})$ are called singular, while points in $\mathrm{reg}\,(\mathcal{Z}) = \mathcal{Z} \setminus \mathrm{sing}\,(\mathcal{Z})$ 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 denoted by $\mathrm{crit}\,(g, \mathcal{Z})$ 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 $g(\mathrm{crit}\,(g,\mathcal{Z}))$ are called critical values, while points in $\mathbb{C}^m \setminus g(\mathrm{crit}\,(g,\mathcal{Z}))$ are called the regular values, of the restriction of g to $\mathcal{Z}$.

Expected dimension of low rank loci

We first revisit a known fact about the expected dimension of algebraic sets $\mathcal{D}_r$, for $r = 0, \ldots, m-1$ 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 : This proof is classical and is given in Appendix A. □

Incidence varieties

Let $A(x) = A_0 + x_1 A_1 + \cdots + x_n A_n$ be an $n-$variate $m \times m$ symmetric linear matrix, and let $0 \leq r \leq m-1$. We introduce lifting variables $y = (y_{i,j})_{1 \leq i \leq m, 1 \leq j \leq m-r}$ and we build an algebraic set whose projection on the $x-$space is contained in the algebraic set $\mathcal{D}_r$. Let

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

For $\iota = \{i_1, \ldots, i_{m-r}\} \subset \{1, \ldots, m\}$, with $\#\iota = m-r$, 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 sub-matrices. For any choice of indices $\iota = \{i_1, \ldots, i_{m-r}\}$ and for any matrix $S \in \mathrm{GL}_{m-r}(\mathbb{Q})$, we define the set

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

We denote by $f(A, \iota, S)$, or simply by f, when there is no ambiguity on ι and S, the polynomial system defining $\mathcal{V}_r(A, \iota, S)$. For $M \in \mathrm{GL}_n(\mathbb{C})$ we denote by $f(A \circ M, \iota, S)$ the entries of $A(M\,x)Y(y)$ and $Y_\iota - S$, and by $\mathcal{V}_r(A \circ M, \iota, S)$ its zero set. Since S has full rank, any relation $Y_\iota - S = 0$ implies that Y has full rank and that the projection of $\mathcal{V}_r$ over the $x-$space is by definition contained in $\mathcal{D}_r$. Often, we will have $S = \mathbb{I}_{m-r}$, the identity matrix, and in this case we simplify the notation by denoting $\mathcal{V}_r(A, \iota, \mathbb{I}_{m-r})$ by $\mathcal{V}_r(A, \iota)$, and $f(A, \iota, \mathbb{I}_{m-r})$ by $f(A, \iota)$. 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.

We finally remark the similarity between the polynomial system $A(x)Y(y) = 0$ and the so-called *complementarity conditions* for the solutions of a couple of primal-dual semidefinite program, see for example [58, Th. 3]. The difference is that, in our case, the special size of $Y(y)$ and the affine constraint $Y_\iota = S$ force a rank condition on $Y(y)$ and hence on $A(x)$.

Eliminating redundancies

The polynomial system defining $\mathcal{V}_r(A, \iota, S)$ contains redundancies induced by polynomial relations between its generators. These relations can be eliminated to obtain a minimal polynomial system defining the incidence variety, and allowing to compute the codimension of $\mathcal{V}_r$, as shown next.

Lemma 5 *Let $M \in \mathrm{GL}_n(\mathbb{C})$. Let $\iota \subset \{1, \ldots, m\}$, with $\#\iota = m - r$, and $S \in \mathrm{GL}_{m-r}(\mathbb{Q})$. 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 defining $\mathcal{V}_r$. 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 $M = \mathbb{I}_n$, $S = \mathbb{I}_{m-r}$ 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:

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

We claim that for $1 \leq i \neq j \leq m - r$, then

$$g_{i,j} \equiv g_{j,i} \mod \langle g_{k,\ell},\, k > m - r \rangle,$$

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 17 that, up to genericity assumptions, the ideal $\langle f_{red} \rangle$ is radical and that the cardinality $\#f_{red}$ matches exactly 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*

$$\begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \\ f_{31} & f_{32} \end{pmatrix} = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{12} & x_{22} & x_{23} \\ x_{13} & x_{23} & x_{33} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ y_{31} & y_{32} \end{pmatrix}.$$

We consider the classes of polynomials f_{12}, f_{21} *in the quotient ring* $\mathbb{Q}[x] \Big/ \langle f_{31}, f_{32} \rangle$*, deducing the following linear relation:*

$$f_{12} - f_{21} = y_{32}x_{13} - y_{31}x_{23} \equiv -y_{31}x_{33}y_{32} + y_{32}x_{33}y_{31} = 0.$$

Lagrange systems

Let $f(A, \iota, S)$ be the polynomial system defining $\mathcal{V}_r(A, \iota, S)$. We set

$$c = m(m-r) + \binom{m-r+1}{2} \qquad \text{and} \qquad e = \binom{m-r}{2},$$

so that $\mathcal{V}_r \subset \mathbb{C}^{c+e}$ and $c = \#f_{red}$ (*cf.* Lemma 5). We define, for a given $M \in \mathrm{GL}_n(\mathbb{C})$, the polynomial system $\ell = \ell(A \circ M, \iota, S)$, given by the coordinates of the map

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

where $e_1 \in \mathbb{Q}^n$ is the first element of the standard basis. We define also $\mathcal{Z}(A \circ M, \iota, S) = Z(\ell(A \circ M, \iota, S))$. When $S = \mathbb{I}_{m-r}$, we omit it in the previous notation.

Output representation

As already announced in the preamble of Section 1, the output of our algorithm is a finite set $\mathcal{Z} \subset \mathbb{C}^n$ represented by a rational univariate representation.

This is a vector $q = (q_0, q_1, \ldots, q_n, q_{n+1}) \subset \mathbb{Q}[t]$ of univariate polynomials with rational coefficients, such that the polynomials q_0 and q_{n+1} are coprime (that is, there exist $a, b \in \mathbb{C}[t]$ such that $aq_0 + bq_{n+1} = 1$, hence q_0 and q_{n+1} do not have common roots) and the set $\mathcal{Z}$ admits the description

$$\mathcal{Z} = \left\{ \left(\frac{q_1(t)}{q_0(t)}, \ldots, \frac{q_n(t)}{q_0(t)} \right) \ : q_{n+1}(t) = 0 \right\}.$$

Moreover, there is a bijective correspondance between the roots of q_{n+1}, counted with multiplicities, and the points in $\mathcal{Z}$. This correspondance remains bijective when restricted respectively to the real roots of q_{n+1} and to the points in $\mathcal{Z} \cap \mathbb{R}^n$.

Such a representation is exact since the coefficients of the output polynomials are rational numbers. We call the degree of q_{n+1}, the *degree of the rational parametrization* q. This integer corresponds to the cardinality of $\mathcal{Z}$, whenever q_{n+1} is square-free. Thus, we are interested in giving precise estimates of the degree of q.

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 [37, 38, 39]. It takes advantage of the particular properties of the incidence varieties over a symmetric low rank locus, as highlighted by Lemma 5.

Genericity properties

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

- Property P_1. We say that A satisfies P_1 if, for all $\iota \subset \{1, \ldots, m\}$, with $\#\iota = m - r$, and for all $S \in \mathrm{GL}_{m-r}(\mathbb{Q})$, the incidence variety $\mathcal{V}_r(A, \iota, S)$ is either empty or smooth and equidimensional. We will always suppose $S = \mathbb{I}_{m-r}$ without loss of generality.
- Property P_2. We say that A satisfies P_2 if, for all r such that $n < \binom{m-r+1}{2}$, the algebraic set $\mathcal{D}_r$ has the expected dimension. By Lemma 4, this means that $\mathcal{D}_r = \emptyset$. Property P_2 holds generically in $\mathbb{S}_m^{n+1}(\mathbb{Q})$, as shown by Lemma 4.

We also define the following properties 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. We suppose that A satisfies P_1 and P_2. In particular, since P_2 holds, if the input r satisfies $n < \binom{m-r+1}{2}$ then the algorithm returns the correct answer, that is the empty list.

LowRankSym(A, r)

Input: A symmetric $n-$variate linear matrix $A(x)$ of size m, encoded by the $m(m+1)(n+1)/2$ rational 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 $q = (q_0, q_1, \ldots, q_n, q_{n+1}) \in \mathbb{Q}[t]^{n+2}$, 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 $t^* \in Z_{\mathbb{R}}(q_{n+1})$ with $(q_1(t^*)/q_0(t^*), \ldots, q_n(t^*)/q_0(t^*)) \in \mathcal{C}$.

Procedure:

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

The previous algorithm uses this subroutine to check the genericity properties:

- 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.

The recursive call is described in the next box. We denote by $A \circ M$ the linear matrix $A(M\,x)$ for a given $M \in \mathrm{GL}_n(\mathbb{C})$.

LowRankSymRec(A, r)

Procedure:

1. choose $M \in \mathrm{GL}_n(\mathbb{Q})$;
2. $q \leftarrow [\,]$; for $\iota \in \{1, \ldots, m\}$ with $\#\iota = m - r$ do
   - $q_\iota \leftarrow$ Image(RatParProj$(\ell(A \circ M, \iota)), M^{-1})$;
   - $q \leftarrow$ 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:

- RatParProj. *Input:* The Lagrange system $\ell(A \circ M, \iota) \subset \mathbb{Q}[x, y, z]$; *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 $q \subset \mathbb{Q}[t]$ of this projection.
- 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 sets $\mathcal{Z}_1, \mathcal{Z}_2 \subset \mathbb{Q}[x_1, \ldots, x_N]$; *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 symmetric $n-$variate linear matrix $A(x)$ of size m, that is the $m(m+1)(n+1)/2$ entries of $A_0, A_1, \ldots, A_n$. The algorithm makes use of the routine LowRankSym described previously, to compute sample points in the algebraic sets $\mathcal{D}_r \cap \mathbb{R}^n$, for $r = 1, \ldots, m-1$. The expected output is one of the following four alternatives:

- an error message, when genericity assumptions are not satisfied;
- the empty list, when $\mathscr{S}$ is empty;
- a vector $x^* = (x_1^*, \ldots, x_n^*)$ such that $A(x^*) = 0$;
- a rational parametrization $q = (q_0, q_1, \ldots, q_n, q_{n+1}) \in \mathbb{Q}[t]^{n+2}$, such that there exists $t^* \in Z_{\mathbb{R}}(q_{n+1})$ with $A(q_1(t^*)/q_0(t^*), \ldots, q_n(t^*)/q_0(t^*)) \succeq 0$.

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 solutions, otherwise it returns x^* such that $A(x^*) = 0$;
- CheckLMI. *Input*: $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$ and a rational parametrization $q \subset \mathbb{Q}[t]$; *Output*: `true` if there exists $t^* \in Z_{\mathbb{R}}(q_{n+1})$ such that $A(q_1(t^*)/q_0(t^*), \ldots, q_n(t^*)/q_0(t^*)) \succeq 0$, and `false` otherwise.

The formal description is the following.

SolveLMI(A)

Input: A symmetric $n-$variate linear matrix $A(x)$ of size m, encoded by the $m(m+1)(n+1)/2$ rational entries of $A_0, A_1, \ldots, A_n$;

Output: The empty list [ ] if and only if $\{x \in \mathbb{R}^n : A(x) \succeq 0\}$ is empty; or an error message stating that 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 $q = (q_0, q_1, \ldots, q_n, q_{n+1}) \in \mathbb{Q}[t]^{n+2}$, such that there exists $t^* \in Z_{\mathbb{R}}(q_{n+1})$ with $A(q_1(t^*)/q_0(t^*), \ldots, q_n(t^*)/q_0(t^*)) \succeq 0$.

Procedure:

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").

3.4 Main algorithm: correctness

We prove that algorithm SolveLMI returns a correct output if genericity properties on input data and on random parameters chosen during its execution are satisfied. We write

down a correctness proof in Theorem 10, page 18; it relies on some preliminary results that are described before. The proofs of these intermediate results are given in Appendix B.

The first result is a regularity theorem for the incidence varieties. We focus on property P_1 for the input matrix A (*cf.* page 14).

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 $t \in \mathscr{T} \cap \mathbb{Q}$, the matrix $A_0 + tA_1 + x_2A_2 + \cdots + x_nA_n$ satisfies P_1.*

The second proposition computes the dimension of the set of critical points of the restriction of the map $\pi_1 \colon x \to x_1$ to $\mathcal{D}_r \setminus \mathcal{D}_{r-1}$. We show that the projection of $\mathcal{Z}(A \circ M, \iota, S) \cap \{(x, y, z) : \operatorname{rank} A(M\,x) = r\}$ 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 the incidence variety.

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 $\iota \subset \{1, \ldots, m\}$ of cardinality $m - r$ and $S \in \mathrm{GL}_{m-r}(\mathbb{Q})$, the following holds:*

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

Finally, we show, after a generic linear change of x variables, closure properties of the projection maps 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 $\mathcal{V}_r$.

We denote by $\pi_i \colon \mathbb{R}^n \to \mathbb{R}^i$ the map sending $x = (x_1, \ldots, x_n)$ to $(x_1, \ldots, x_i)$.

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 $x \in \pi_1^{-1}(t) \cap M^{-1}\mathcal{C}$, with* $\operatorname{rank} A(M\,x) = r$, *there exists $\iota \subset \{1, \ldots, m\}$ and $(x, y) \in \mathcal{V}_r(A \circ M, \iota)$ such that $\Pi_1(x, y) = t$.*

Propositions 7, 8 and 9 will be proved in Appendix B. We say that hypothesis H holds if:

- The matrix $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$ 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) *Let $A \in \mathbb{S}_{m,m}^{n+1}(\mathbb{Q})$ be the input of* SolveLMI. *Suppose that hypothesis* 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 $q = (q_0, q_1, \ldots, q_n, q_{n+1}) \in \mathbb{Q}[t]^{n+2}$ such that there exists $t^* \in Z_{\mathbb{R}}(q_{n+1})$ 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 that the linear system $A(x) = 0$ has at least one solution. Hence, the routine SolveLinear with input A returns a vector x^* such that $A(x^*) = 0$. Since the zero matrix is positive semidefinite, 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 that $A(x)$ has positive rank on $\mathscr{S}$. We claim that the subroutine LowRankSym is correct, in the following sense: with input the symmetric linear matrix A of size m and any $1 \leq r \leq m-1$, such that A satisfies P_1, the output of LowRankSym(A, r) is a rational parametrization whose solutions meet each connected component $\mathcal{C}$ of $\mathcal{D}_r$ 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. $\mathscr{S} \neq \emptyset$. Let $r \geq 1$ be the minimum rank attained by $A(x)$ on $\mathscr{S}$. Denote by $\mathcal{C} \subset \mathcal{D}_r \cap \mathbb{R}^n$ a connected component such that $\mathcal{C} \cap \mathscr{S} \neq \emptyset$. By Theorem 2, we deduce that $\mathcal{C} \subset \mathscr{S}$, and that $\mathcal{C} \cap \mathcal{D}_{r-1} = \emptyset$, by the minimality of r. Let q be the output of LowRankSym at Step 2 of SolveLMI. The correctness hypothesis on LowRankSym implies that q defines a finite set whose solutions meet $\mathcal{C}$, hence $\mathscr{S}$. Consequently, the subroutine 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 $\mathcal{D}_r$ is empty, and hence 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 $(n-1)-$variate symmetric linear matrix $\tilde{A}$ satisfying P_1, then LowRankSymRec with input $(\tilde{A}, r)$ returns a rational parametrization of a finite set meeting each connected component $\tilde{\mathcal{C}} \subset \tilde{\mathcal{D}}_r$ 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 $\mathcal{C} \subset \mathcal{D}_r$ 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. There are two possible scenarios.

First case. Suppose first that $\pi_1(M^{-1}\mathcal{C}) = \mathbb{R}$, let $t \in \mathbb{Q}$ be the rational number chosen at Step 3, 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 $\tilde{\mathcal{C}} \subset \tilde{\mathcal{D}}_r$ 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 $\pi_1^{-1}(t) \cap M^{-1}\mathcal{C} \neq \emptyset$ is finite, and for all x in this set, $\operatorname{rank} A(M\,x) = r$ (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 Complexity analysis

Our next step is to estimate the complexity of SolveLMI. This will be measured by counting the number of arithmetic operations performed over $\mathbb{Q}$, and will essentially rely on the complexities of state-of-the-art algorithms computing rational parametrizations. We start in Section 4.1 by computing bounds on the expected output degree.

4.1 Output degree estimates

We first provide a bound on the degree of the rational parametrizations, by computing Multilinear Bézout bounds (*cf.* [73, Ch. 11]).

Proposition 11 *Let $A \in \mathbb{S}_m^{n+1}$ be the input of* SolveLMI. *Let $p_r = (m-r)(m+r+1)/2$. If* H *holds, for all $\iota \subset \{1,\ldots,m\}$, the degree of the rational parametrization q_ι returned by* LowRankSymRec *at Step 2 is bounded above by*

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

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 polynomial system $f(A,\iota)$ defining the incidence variety $\mathcal{V}_r(A,\iota)$ 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, the incidence variety is defined by $Y_\iota - S = 0$ and by $m(m-r) - e = p_r$ entries of $A(x)Y(y)$, where $e = \binom{m-r}{2}$ is the number of redundancies. Hence we just eliminate equations $Y_\iota - S = 0$ and the variables corresponding to the entries of Y_ι. Consequently, the Lagrange system can be also simplified, by admitting only p_r Lagrange multipliers z (corresponding to the p_r equations defining the simplified system $A(x)Y(y) = 0$). 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 [73, Ch. 11], is the coefficient of the monomial $s_x^n s_y^{r(m-r)} s_z^{p_r-1}$ in the expansion of

$$(s_x+s_y)^{p_r}(s_y+s_z)^{n-1}(s_x+s_z)^{r(m-r)}.$$

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 $\theta(m,n,r) \leq \binom{p_r+n}{n}^3$ can be obtained by applying the following 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 $b = p_r$. □

We straightforwardly deduce the following global estimate on the degree of the output parametrization q.

Corollary 12 *Let $A \in \mathbb{S}_m^{n+1}$ be the input of* SolveLMI, *and suppose that $\mathscr{S}$ is not empty. Let $\theta(m,n,r)$ be the bound computed in Proposition 11. If* H *holds, 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 at most

$$\binom{m}{r(A)} \theta(m,n,r(A)) \in \mathcal{O}\left(\binom{m}{r(A)} \binom{p_{r(A)}+n}{n}^3 \right).$$

Proof : We recall that, by Proposition 11, for any $\iota \subset \{1, \ldots, m\}$ of cardinality $m-r$, the degree of the rational parametrization returned by LowRankSymRec at Step 2 is bounded above by $\theta(m, n, r)$. The proof follows since:

1. the number of subsets $\iota \subset \{1, \ldots, m\}$ of cardinality $m - r$ is $\binom{m}{m-r} = \binom{m}{r}$;
2. SolveLMI stops when r reaches $r(A)$.

□

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 11. 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 [17] or [60]. In [60, Table 1], the authors report on the EDdegree of determinantal hypersurfaces generated by linear matrices $A(x) = A_0 + x_1 A_1 + \cdots + x_n A_n$: 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. Analogous comparisons can be done with results in [60, Example 4] and [60, Corollary 3.5].

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 [58, 30] 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 [58, Table 2], we conclude this section with the following expected result, which is a work in progress.

Conjecture 13 *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 [58, 30]. If property* H *holds, then the sum of the degrees of the rational parametrizations computed during* SolveLMI *is given by the formula*

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

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

(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

4.2 The complexity of SolveLMI

Complexity of some subroutines

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

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

- The subroutine CheckLMI can be performed as follows. Let $q = (q_0, q_1, \ldots, q_n, q_{n+1}) \subset \mathbb{Q}[t]$ be the rational parametrization in the input of CheckLMI, and let $A(x)$ be the symmetric pencil. 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 [7, Ch. 13].

- Estimates for the complexities of Project, Lift, Image and Union are given in [73, Ch. 10]. In particular, if $\theta = \theta(m, n, r)$ is the bound computed in Proposition 11, and $\tilde{n} = n + r(m - r) + p_r$, then:
  - By [73, Lemma 10.1.5], Project is performed within $\tilde{n}^2\theta^2$ arithmetic operations;
  - By [73, Lemma 10.1.6], Lift is performed within $\tilde{n}\theta^2$ arithmetic operations;
  - By [73, Lemma 10.1.1], Image is performed within $\tilde{n}^2\theta + \tilde{n}^3$ arithmetic operations;
  - By [73, Lemma 10.1.3], Union is performed within $\tilde{n}\theta^2$ arithmetic operations.

Complexity of the main subroutine and of the whole algorithm

The complexity of LowRankSym can be estimated by computing the complexity of the recursive subroutine LowRankSymRec, which strictly depends on the computation of the rational parametrization. This computation can be performed via the symbolic-homotopy described in [47], and we base our complexity analysis on this reference. Indeed, we will be able to express the number of arithmetic operations as, essentially, a quadratic function of the bound $\theta(m, n, r)$ computed in Proposition 11.

We recall that for symmetric pencils, the simplified Lagrange system (*cf.* the proof of Proposition 11) 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.

We build the homotopy

$$t\ell + (1-t)\tilde{\ell} \subset \mathbb{Q}[x, y, z, t], \tag{2}$$

where t is a new variable. The system (2) defines a $1-$dimensional algebraic set, that is a curve. From [47, Proposition 6.1], if the solutions of $\tilde{\ell}$ are known, one can compute a rational parametrization of the solution set of system (2) 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; $N = p_r \# \Delta_{xy} + (n-1)\#\Delta_{yz} + r(m-r)\#\Delta_{xz}$; $Q = \max\{\|q\| : q \in \Delta_{xy} \cup \Delta_{yz} \cup \Delta_{xz}\}$; e is the number of isolated solutions of ℓ; is the degree of the curve $Z(t\ell + (1-t)\tilde{\ell})$; ω is the exponent of matrix multiplication.

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

Lemma 14 *Let $\mathcal{G}_{m,n,r}$ and $\theta(m,n,r)$ be respectively the set and the bound defined in Proposition 11, and suppose that $\mathcal{G}_{m,n,r}$ is not empty. 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 : The proof of this Lemma is technical and similar to that of [39, Lemma 10]. It is given in Appendix C. □

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

Proposition 15 *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 11. Let $p_r = (m-r)(m+r+1)/2$. Then Step 2 of* LowRankSymRec *returns a rational parametrization 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 11. We consider the bound on the degree of the homotopy curve given by Lemma 14. We deduce the claimed complexity result by applying [47, 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. Recall that $p_r = (m-r)(m+r+1)/2$.

Theorem 16 (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*

$$O^{\sim}\left(n \sum_{r \leq m-1} \binom{m}{r}(n + p_r + r(m-r))^7 \binom{p_r + n}{n}^6\right) \quad \text{if } \mathscr{S} \text{ is empty, and}$$

$$O^{\sim}\left(n \sum_{r \leq r(A)} \binom{m}{r}(n + p_r + r(m-r))^7 \binom{p_r + n}{n}^6\right) \quad \text{if } \mathscr{S} \text{ is not empty.}$$

Proof : The proof is immediate since:

- From Proposition 15, 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;
- $\theta(m,n,r) \leq \binom{n+p_r}{n}^3$ by Proposition 11;
- there are at most n recursive calls of LowRankSymRec in LowRankSym;
- SolveLMI stops when r reaches $r(A)$ if $\mathscr{S} \neq 0$, otherwise it stops when $r = m-1$;
- the cost of subroutines SolveLinear, CheckLMI, Project, Lift, Image and Union is negligible.

□

5 Experiments

Algorithm SolveLMI has been implemented in a MAPLE function, and it is part of a more general library called SPECTRA (Semidefinite Programming and Exact Computation Towards Real Algebra), to be 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 our computational experiments, all performed on a machine with the following characteristics: Intel(R) Xeon(R) CPU E7540@2.00GHz with 256 Gb of RAM. We use FGB [22] for fast computation of Gröbner bases. To compute the rational parametrizations we use the implementation in MAPLE of the change-of-ordering algorithm FGLM [26] and of its improved versions [27, 25].

5.1 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. Genericity of the data is ensured by fixing a natural number $N \in \mathbb{N}$ and by generating numerators and denominators uniformly in the interval $[-N, N]$. We report in Table 2 the timings and the degrees of output rational parametrizations.

In this table, 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 column LRS) with those of the function PointsPerComponents (column PPC) of the library RAGLIB developed by the third author [68]. 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 $\mathcal{D}_r \cap \mathbb{R}^n$. The symbol ∞ means that we did not succeed in computing the parametrizations after 48

(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

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 column totaldeg for $(m, n, r) = (4, 2, 5)$ is obtained as the sum $10 + 30 + 42$ of the integers in column deg for $m = 4, r = 2$ and $n = 3, 4, 5$. We remark that, as for Table 1, the value in column deg for a given triple m, n, r coincides with the algebraic degree of semidefinite programming, that is with $\delta(n, m, r)$ as defined in [58].

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 parameters m and 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 [25]: we believe that exploiting the special monomial structure of these systems could

lead to dedicated algorithms for computing their Gröbner bases.

5.2 Scheiderer's spectrahedron

We consider the following 6×6 symmetric pencil in 6 variables:

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

The matrix A is the Gram matrix of the trivariate polynomial

$$f(u_1, u_2, u_3) = u_1^4 + u_1u_2^3 + u_2^4 - 3u_1^2u_2u_3 - 4u_1u_2^2u_3 + 2u_1^2u_3^2 + u_1u_3^3 + u_2u_3^3 + u_3^4.$$

In other words, $f = v'A(x)v$ for all $x \in \mathbb{R}^6$, where $v = (u_1^2, u_1u_2, u_2^2, u_1u_3, u_2u_3, u_3^2)$ is the monomial basis of the vector space of homogeneous polynomials of degree 2 in u_1, u_2, u_3. The polynomial f is nonnegative over $\mathbb{R}^6$ and hence, since it is homogeneous of degree 4 in 3 variables, by Hilbert's theorem (*cf.* [45]) it is a sum of at most three squares of polynomials 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 (*cf.* [62, Sec. 6]).

Scheiderer proved in [75] 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 in the decomposition cannot be chosen to have rational coefficients, answering a question of Sturmfels. By Scheiderer's result, we can deduce that the spectrahedron $\mathscr{S}$ 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 $\mathscr{S}$ does not contain any point x with $\operatorname{rank} A(x) = 0$ and 1 (and precisely, that $\mathcal{D}_0 \cap \mathbb{R}^6 = \mathcal{D}_1 \cap \mathbb{R}^6 = \emptyset$) via the routine SolveLinear and LowRankSym with $r = 1$. Further, for $r = 2$, the algorithm returns the following rational parametrization of $\mathcal{D}_2 \cap \mathbb{R}^6$:

$$\begin{array}{ll} x_1 = \frac{3+16t}{-8+24t^2} & x_2 = \frac{8-24t^2}{-8+24t^2} \\ x_3 = \frac{8+6t+8t^2}{-8+24t^2} & x_4 = \frac{16+6t-16t^2}{-8+24t^2} \\ x_5 = \frac{-3-16t}{-8+24t^2} & x_6 = \frac{3+16t}{-8+24t^2} \end{array}$$

where t has to be chosen among the solutions of the univariate equation

$$8t^3 - 8t - 1 = 0.$$

The set $\mathcal{D}_2$ is, indeed, of dimension 0, degree 3, and it contains only real points. In particular, the technical assumption P_2 is not satisfied, 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 $A(x(t^*)) = V'V$ 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 $f = v'V'Vv = ||Vv||^2$. At the third point of $\mathcal{D}_2 \cap \mathbb{R}^6$:

$$\begin{pmatrix} 1.057453771 \\ -1.000000000 \\ 1.236416954 \\ 0.2364169545 \\ -1.057453771 \\ 1.057453771 \end{pmatrix}$$

the matrix $A(x)$ is indefinite, so it is not a valid Gram matrix.

To conclude, algorithm SolveLMI allows to design a computer-aided proof of Scheiderer's results about the polynomial f. In particular, we are able to compute a parametrization of the two possible decompositions of f as a sum of two squares in $\mathbb{R}[u_1, u_2, u_3]$, showing that the Gram spectrahedron $\mathscr{S}$ of f is not empty and that the minimum rank attained by A on $\mathscr{S}$ is two. 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 to approximate a feasible point.

6 Conclusion

In this paper, we have presented an exact algorithm that computes an algebraic representation of at least one feasible point of a linear matrix inequality $A(x) \succeq 0$, or that detects emptiness of the spectrahedron $\mathscr{S} = \{x \in \mathbb{R}^n : A(x) \succeq 0\}$. 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 sampling 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 5, 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, to be released in September 2015. It has to be understood as a starting point towards a systematic exact computer algebra approach to semidefinite programming and related questions.

A Proof of Proposition 4

Proof : Let $\tilde{x}$ denote the vector of $m(m+1)/2$ variables $x_{i,j}, 1 \leq i \leq j \leq m$, and let $X \in \mathbb{S}_m(\mathbb{Q}[\tilde{x}])$ be the symmetric matrix with entries $x_{i,j}$. Let minors $(r+1, X)$ be the list of $(r+1) \times (r+1)$ minors of X and let $\mathcal{Z} = Z(\text{minors}\,(r+1, X)) \subset \mathbb{C}^{m(m+1)/2}$. Let $\mathbb{G}(m-r, m)$ be the Grassmannian of $(m-r)-$planes in $\mathbb{C}^m$: it is an affine variety of dimension $r(m-r)$ (*cf.* [35, Lec. 6]). Let

$$\mathcal{I} = \{(X, \mathcal{H}) \in \mathbb{C}^{m(m+1)/2-1} \times \mathbb{G}(m-r, m) : \mathcal{H} \subset \ker(X)\}.$$

Let π_1 and π_2 be the projections of $\mathcal{I}$ respectively onto the first and the second factor. Then π_2 maps $\mathcal{I}$ surjectively onto $\mathbb{G}(m-r, m)$, and for $\mathcal{H} \in \mathbb{G}(m-r, m)$, then $\dim \pi_2^{-1}(\mathcal{H}) = r(r+1)/2$. To check this last dimension count, suppose without loss of generality that $\mathcal{H}$ is generated by the first $m-r$ vectors of the standard basis: then $\pi_2^{-1}(\mathcal{H})$ is the set of symmetric matrices such that the first $m-r$ columns and, hence, the first $m-r$ rows, are zero.

We deduce by the Theorem on the Dimension of Fibers [77, Sect. 6.3, Th. 7] that $\mathcal{I}$ is irreducible of dimension $r(m-r)+r(r+1)/2$. Thus $\mathcal{Z} = \pi_1(\mathcal{I})$ is irreducible, of dimension $r(m-r)+r(r+1)/2$ (and codimension $\binom{m-r+1}{2}$) since any fiber of π_1 is finite. We conclude that $\mathcal{D}_r$ has the claimed dimension by applying Bertini's theorem [77, Ch. 2,Sec. 6]. $\square$

B Proof of Propositions 7, 8 and 9

B.1 Proof of Proposition 7

Proof of Assertion 1: Suppose w.l.o.g. that $M = \mathbb{I}_n$ and $S = \mathbb{I}_{m-r}$. For $\iota \subset \{1, \ldots, m\}$ of cardinality $m-r$, let f_{red} be the polynomial system given by 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 the

length of f_{red}, that is $m(m-r)+\binom{m-r+1}{2}$. We conclude that, for $A \in \mathscr{A}_\iota$, A satisfies P_1. Then, 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, $Z(\varphi_A)$ equals $\mathcal{V}_r(A, \iota)$.

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 [73, 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.* [18, 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 $\# f_{red}$.

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 recall that A is a short-hand notation for the vector of symmetric matrices $(A_0, A_1, \ldots, A_n) \in \mathbb{S}_m^{n+1}(\mathbb{C})$; we denote by $a_{\ell,i,j}$ the variable encoding the $(i,j)-$th entry of the matrix A_ℓ. 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 reduction, 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 $m(m-r)+\binom{m-r+1}{2} = \# f_{red}$. Indeed, 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 $\#\iota = m-r$. 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 [73, 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 $t \in \mathscr{T} = \mathbb{C} \setminus \mathcal{H}$, the linear matrix $(A_0 + tA_1, A_2, \ldots, A_n)$ satisfies P_1. □

In the proof of Assertion 1 of Theorem 7, we have shown a stronger property of $\mathcal{V}_r(A,\iota)$, holding generically with respect to input parameters $A_0, A_1, \ldots, A_n$. This is highlighted by the next statement.

Corollary 17 *Let $\mathscr{A} \subset \mathbb{S}_m^{n+1}(\mathbb{Q})$ be the non-empty Zariski open set defined in Proposition 7, and let $A \in \mathscr{A}$. Then for every $\iota \subset \{1,\ldots,m\}$ with $\#\iota = m-r$, the ideal $\langle f_{red}\rangle = \langle f\rangle$ is radical, and $\mathcal{V}_r(A,\iota)$ is a complete intersection of codimension $\#f_{red}$.*

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 $\#f_{red} = m(m-r) + \binom{m-r+1}{2}$ at every point of $\mathcal{V}_r(A,\iota)$. By the Jacobian criterion [18, 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 $\#f_{red}$. Hence $I(\mathcal{V}_r(A,\iota))$ can be generated by a number of polynomials equal to the codimension of $\mathcal{V}_r(A,\iota)$, and we conclude. □

B.2 Proof of Proposition 8

We recall that for a given symmetric pencil $A \in \mathbb{S}_m^{n+1}(\mathbb{Q})$, $S \in \mathrm{GL}_{m-r}(\mathbb{C})$ and for $\iota \subset \{1,\ldots,m\}$ of cardinality $m-r$, we have denoted by $f = f(A,\iota,S)$ the polynomial system defining $\mathcal{V}_r(A,\iota,S)$. We set

$$c = m(m-r) + \binom{m-r+1}{2} \qquad \text{and} \qquad e = \binom{m-r}{2}.$$

Then f has length $c+e = m(m-r) + (m-r)^2$, and e is the number of redundancies that are eliminated by Lemma 5. By Lemma 5 and by Proposition 7, we deduce that:

- there exists $f_{red} \subset f$ of length c, such that $Z(f_{red}) = Z(f) = \mathcal{V}_r$;
- for $A \in \mathscr{A}$ (defined in Proposition 7), A satisfies P_1 and $\mathcal{V}_r = \mathcal{V}_r(A,\iota,S)$ is smooth and equidimensional of codimension c, for all $\iota \subset \{1,\ldots,m\}$.

In particular, the rank of Df is constantly equal to c if evaluated along a point in $\mathcal{V}_r$.

Let $A(x)$ be a symmetric linear matrix, and consider the locally closed set: $\mathcal{D}_r \setminus \mathcal{D}_{r-1} = \{x \in \mathbb{C}^n : \operatorname{rank} A(x) = r\}$. The set $\mathcal{D}_r \setminus \mathcal{D}_{r-1}$ 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 $S \in \mathrm{GL}_{m-r}(\mathbb{Q})$ and ι as above. Let N be the upper left $r \times r$ sub-matrix of $A(x)$, and consider the corresponding block division of A:

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

with $P, Q \in \mathbb{M}_{r,m-r}(\mathbb{Q})$ and $R \in \mathbb{M}_{m-r,m-r}(\mathbb{Q})$. Here $P = Q$ but we will not need to use this fact. 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:

$$Y^{(1)} + N^{-1}QY^{(2)} = 0, \qquad \Sigma(N)Y^{(2)} = 0, \qquad Y_\iota - S = 0, \tag{4}$$

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

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

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 and S as above, the critical points of the restriction of Π_w to $\mathcal{V}_r(A, \iota, S)$ are encoded by the polynomial system

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

where $z = (z_1, \ldots, z_{c+e}, 1)$ 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 18 *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 $w \in \mathscr{W}$, for all $\iota \subset \{1, \ldots, m\}$ of cardinality $m - r$ and $S \in \mathrm{GL}_{m-r}(\mathbb{Q})$, 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.

We prove below the following claim: given a $r \times r$ sub-matrix N of $A(x)$, there exists $\mathscr{W}_N \subset \mathbb{C}^n$ such that for $w \in \mathscr{W}_N$, (f, g, h) satisfies Q in $\{(x, y, z) : \det N \neq 0\}$. We straightforwardly 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 $U_\iota^{(2)} \in \mathbb{C}^{(m-r)\times(m-r)}$. We recall from (4) the local equations of $\mathcal{V}_r$:

$$Y^{(1)} + N^{-1}QY^{(2)} = 0, \qquad \Sigma(N)Y^{(2)} = 0, \qquad U_\iota Y(y) - S = 0.$$

We deduce the equality

$$S = U_\iota^{(1)} Y^{(1)} + U_\iota^{(2)} Y^{(2)} = (U_\iota^{(2)} - U_\iota^{(1)} N^{-1} P) Y^{(2)}$$

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

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

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

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

By hypothesis, the rank of $D\tilde{f}$ is constant and equal to c if evaluated at $(x,y) \in Z(\tilde{f}) = \mathcal{V}_r(A,\iota,S) \cap \{(x,y) : \det N \neq 0\}$. We similarly define

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

with $z = (z_1, \ldots, z_{c+e}, 1)$. The structure of $D\tilde{f}$ implies that polynomial $\tilde{h}_i$ reads $z_{(m-r)^2+i}$, for $i = 1, \ldots, m(m-r)$, and hence it can be eliminated, together with the corresponding variables $z_{(m-r)^2+i}$. 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

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

and, for $w \in \mathbb{C}^n$, its section map $\varphi_w \colon (x,y,z) \mapsto p(x,y,z,w)$. In the last part of this proof, we show that 0 is a regular value of the map p, and we conclude.

We first exclude the trivial situation $\varphi^{-1}(0) = \emptyset$, by defining in this case $\mathscr{W}_N = \mathbb{C}^n$.

Otherwise, let $(x,y,z,w) \in \varphi^{-1}(0)$. We first observe that polynomials in $\tilde{f}$ just depend on variables x and y, hence their contribution in the Jacobian matrix $D\varphi$ at (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,
- the derivatives with respect to $w_1, \ldots, w_n$, and
- the derivatives with respect 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 $D\varphi$ with 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

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

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 defined by

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

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 [77, Sect. 6.3, Theorem 7] we deduce that $\pi_x(\mathcal{E})$ has dimension 0. □

Proof of Assertion 3: Since the set $\mathcal{V}_r \cap \{(x, y) : \operatorname{rank} A(x) = r\}$ is smooth and equidimensional, by [73, 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 $z' D(f, \Pi_w) = 0$. 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. □

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 the set $\mathscr{W}$ defined in Lemma 18. The proof of all assertions follows from Lemma 18 since, for $M \in \mathscr{M}_1$, one gets the equality

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

where w' 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

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

is the image of the set of solutions of

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

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

$$f(A \circ M, \iota, S) = 0, \qquad z' \left(Df(A, \iota, S) \circ M\right) = (w', 0).$$

Hence the three assertions of Proposition 8 are straightforwardly deduced by those of Lemma 18. □

B.3 Proof of Proposition 9

For the proof of Assertion 1 of Proposition 9, we need to recall some notation introduced in [37, 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 denoted by $\Omega_p(\mathcal{Z})$. We define

$$\mathscr{S}(\mathcal{Z}) = \Omega_0(\mathcal{Z}) \cup \cdots \cup \Omega_{d-1}(\mathcal{Z}) \cup \operatorname{sing} \Omega_d \mathcal{Z}$$

where we recall that $\operatorname{sing} \mathcal{V}$ denotes the singular locus of an algebraic set $\mathcal{V}$, and

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

In the previous expression, $\operatorname{reg} \mathcal{V}$ denotes $\mathcal{V} \setminus \operatorname{sing} \mathcal{V}$, π_i the canonical projection map over the first i variables, and $\operatorname{crit}(g, \mathcal{V})$ 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 [37, Prop. 17] we proved that for any algebraic set $\mathcal{Z} \subset \mathbb{C}^n$ of dimension d, when M is chosen generically in $\mathrm{GL}_n(\mathbb{C})$ (that is, 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.* [77, 18] for a background in Noether position). Also, we used the previous fact in [37, Prop. 18] to prove closure properties of the restriction of projection maps π_i 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 [37, Prop. 17], for the algebraic set $\mathcal{D}_r$. Hence, for $M \in \mathscr{M}_2$, we deduce by [37, 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 [37, 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

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

Its projection $\Pi_x(\mathscr{O})$ on the $x-$space 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 in $A(M\,x)Y(y) = 0$ 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

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

where $\mathscr{O}_\iota = \{(x,y) : \det Y_\iota \neq 0\}$, and Y_ι is the square submatrix of Y obtained by isolating the rows indexed by ι.

Let $\mathcal{C} \subset \mathcal{D}_r \cap \mathbb{R}^n$ be a connected component. 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 $\operatorname{rank} A(Mx) = r$. 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 $\pi_1(x,y) = t$. □

C Proof of Lemma 14

Proof : Similarly to Proposition 11, we exploit the multilinear structure of the system defining the homotopy curve, that is $t\ell + (1-t)\tilde{\ell}$, to compute its degree e'. The system is bilinear with respect to the four groups x, y, z, t. We recall the cardinalities $\#x = n, \#y = r(m-r), \#z = p_r - 1, \#t = 1$, with $p_r = (m-r)(m+r+1)/2$. By [73, Ch. 11], e' is bounded by the sum of the coefficients of

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

modulo $I = \langle s_x^{n+1}, s_y^{r(m-r)+1}, s_z^{p_r}, s_t^2 \rangle \subset \mathbb{Z}[s_x, s_y, s_z, s_t]$. We see that $q = q_1 + s_t(q_2 + q_3 + q_4) + g$ with s_t^2 that divides g and

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

Hence $q \equiv q_1 + q_2 + q_3 + q_4 \mod I$, and the bound is given by the sum of the contributions of q_1, q_2, q_3 and q_4. The contribution of q_1 in the previous bound 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 11, and coincides with $\theta(m,n,r)$.

We compute the contribution of q_2. Let $q_2 = p_r s_t \tilde{q}_2$ with $\tilde{q}_2 \in \mathbb{Z}[s_x, s_y, s_z]$. 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 $s_x^n, s_y^{r(m-r)}, s_z^{p_r - 1}$, 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

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

where $\mathcal{G}_A = \{\max\{0, n - p_r\} \leq k \leq \min\{n - p_r + r(m-r), r(m-r)\}\}$;

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

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

where $\mathcal{G}_B = \{\max\{0, n - p_r + 1\} \leq k \leq \min\{n - p_r + r(m-r), r(m-r)\}\}$;

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

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

$$\text{where } \mathcal{G}_C = \{\max\{0, n-p_r+1\} \leq k \leq \min\{n-p_r+r(m-r)+1, r(m-r)\}\}.$$

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 $p_r(\Sigma_A + \Sigma_B + \Sigma_C) \in O\left(p_r \min\{n, p_r\}\,\theta(m,n,r)\right)$. We prove below this claim.

We define

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

so that $\theta(m,n,r)$ sums over $\chi_1 \leq k \leq \chi_2$ and 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

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

When k runs over all admissible indices, the rational function $\Psi(k)$ is non-decresing monotone, and its maximum is attained in $\Psi(\chi_2)$ and is bounded by $\min\{n, p_r\}$. By that 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 $\mathcal{O}\left(r(m-r) \min\{n, p_r\}\,\theta(m,n,r)\right)$. □

References

[1] R. G. Bartle, D. R. Sherbert. Introduction to real analysis. 3rd edition. John Wiley & Sons, New York, 1992.

[2] 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.

[3] B. Bank, M. Giusti, J. Heintz, M. Safey El Din, É. Schost. On the geometry of polar varieties. Applicable Algebra in Engineering, Communication and Computing. 21(1):33–83, 2010.

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

[5] A. Bhardwaj, P. Rostalski, R. Sanyal. Deciding polyhedrality of spectrahedra. `arXiv:1102.4367`, Feb. 2011.

[6] 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.

[7] S. Basu, R. Pollack, and M.-F. Roy. Algorithms in real algebraic geometry, volume 10 of Algorithms and Computation in Mathematics. 2nd edition. Springer Verlag, Berlin, 2006.

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

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

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

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

[12] W. Bruns, U. Vetter. Determinantal rings, Springer Verlag, Berlin Heidelberg, 1988.

[13] M.D. Choi, T.Y. Lam, B. Reznick. Sums of squares of real polynomials. Proceedings of Symposia in Pure mathematics 58:103–126, 1995.

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

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

[16] D. A. Cox, J. Little, D. O'Shea. Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra. 3rd edition, Springer, New York, 2007.

[17] J. Draisma, E. Horobet, G. Ottaviani, B. Sturmfels, R.R. Thomas. The Euclidean distance degree of an algebraic variety. to appear in Foundations of Computational Mathematics, 2015.

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

[19] D. Eisenbud. Linear sections of determinantal varieties. American Journal of Mathematics, 110(3):541–575, 1988.

[20] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra, 139(1–3):61–88, 1999.

[21] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reductions to zero (F5). Proceedings of ISSAC 2002, Lille, France, 2002.

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

[23] J.-C. Faugère, M. Safey El Din, P.-J. Spaenlehauer. On the complexity of the generalized MinRank problem. Journal of Symbolic Computation. 55:30–58, 2013.

[24] J.-C. Faugère, M. Safey El Din, P.-J. Spaenlehauer. Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology. Proceedings of ISSAC 2010, Munich, Germany, 2010.

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

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

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

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

[29] D. Grigoriev, N. Vorobjov. Solving systems of polynomial inequalities in subexponential time. Journal of Symbolic Computation, 5:37–64, 1988.

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

[31] 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.

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

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

[34] 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.

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

[36] J. Heintz, M.-F. Roy, P. Solerno. Description of the connected components of a semi-algebraic set in single exponential time. Discrete and Computational Geometry, 11:121–140, 1994.

[37] D. Henrion, S. Naldi, M. Safey El Din. Real root finding for determinants of linear matrices. to appear in Journal of Symbolic Computation, 2015.

[38] 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.

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

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

[41] B. Huber, B. Sturmfels. A polyhedral method for solving sparse polynomial systems. Math. Comput. 64(212):1541–1555, 1995.

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

[43] D. Henrion. Semidefinite geometry of the numerical range. Electronic Journal of Linear Algebra, 20:322–332, 2010.

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

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

[46] R. Hildebrand. Spectrahedral cones generated by rank 1 matrices. To appear in J. Global Optim., DOI:10.1007/s10898-015-0313-4, 2015.

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

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

[49] 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.

[50] J.B. Lasserre. Moments, positive polynomials and their applications. Imperial College Press, London, UK, 2010.

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

[52] J.B. Lasserre. A semidefinite programming approach to the generalized problem of moments. Mathematical Programming, 112:65-92, 2008.

[53] 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, pages 157–270, Springer, New York, 2009

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

[55] Y. Ma, L. Zhi. Computing real solutions of polynomial systems via low-rank moment matrix completion. Proceedings of ISSAC 2012, Grenoble, France, 249–256, 2012.

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

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

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

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

[60] G. Ottaviani, P.-J. Spaenlehauer, B. Sturmfels. Exact Solutions in Structured Low-Rank Approximation. SIAM J. Matrix Analysis Appl. 35(4):1521–1542, 2014.

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

[62] D. Plaumann, B. Sturmfels, C. Vinzant. Quartic curves and their bitangents. Journal of Symbolic Computation, 46:712–733, 2011.

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

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

[65] J.C. Ottem, K. Ranestad, B. Sturmfels, C. Vinzant. Quartic spectrahedra. Mathematical Programming, Ser. B, 151:585-612, 2015.

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

[67] J. Renegar. On the computational complexity and geometry of the first order theory of the reals. Journal of Symbolic Computation 13(3):255–352, 1992.

[68] M. Safey El Din. Raglib (real algebraic geometry library), Maple package. www-polsys.lip6.fr/~safey

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

[70] 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.

[71] 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, 224–231, 2003.

[72] 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.

[73] 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.

[74] R. Sanyal, F. Sottile, B. Sturmfels. Orbitopes. Mathematika 57:275–314, 2011.

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

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

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

[78] K. Schmüdgen. The K-moment problem for compact semi-algebraic sets. Mathematische Annalen, 289:203–206, 1991.

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

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

[81] M. Spivak. Calculus on manifolds. WA Benjamin New York. Vol 1 (1965).

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

[83] M.J. Todd. Semidefinite optimization. Acta Numerica, 10:515–560, 2001.

[84] A. Varvitsiotis. Combinatorial conditions for low rank solutions in semidefinite programming. PhD Thesis. Tilburg University, The Netherlands, 2013.

[85] C. Vinzant. Real algebraic geometry in convex optimization. PhD Thesis. University of California at Berkeley, 2011.