Real root finding for low rank linear matrices

Didier Henrion, Simone Naldi, Mohab Safey El Din

Real root finding for low rank linear matrices

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

June 2, 2015

Abstract

The problem of finding low rank $m \times m$ matrices in a real affine subspace of dimension n has many applications in information and systems theory, where low rank is synonymous of structure and parcimony. We design a symbolic computation algorithm to solve this problem efficiently, exactly and rigorously: the input are the rational coefficients of the matrices spanning the affine subspace as well as the expected maximum rank, and the output is a rational parametrization encoding a finite set of points that intersects each connected component of the low rank real algebraic set. The complexity of our algorithm is studied thoroughly. It is essentially polynomial in $\binom{n+m(m-r)}{n}$ where r is the expected maximum rank; it improves on the state-of-the-art in the field. Moreover, computer experiments show the practical efficiency of our approach.

Keywords

symbolic computation; low rank matrices; real algebraic geometry.

1 Introduction

1.1 Problem statement

Let $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ be respectively the fields of rational, real and complex numbers. Let m, n, r be positive integers with $0 \leq r \leq m-1$ and let $A_0, \ldots, A_n$ be $m \times m$ matrices with entries in $\mathbb{Q}$. Let $x = (x_1, \ldots, x_n)$ be a set of n variables. We consider the *affine map (or linear matrix)* $A(x)$ defined by

$$(x_1, \ldots, x_n) \mapsto A(x) = A_0 + x_1 A_1 + \cdots + x_n A_n.$$

[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.

Given $A(x)$ as above, we consider the following algebraic set:

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

The goal of this paper is to design an efficient exact algorithm for solving the problem of computing at least one point in each connected component of the real algebraic set $\mathcal{D}_r \cap \mathbb{R}^n$.

By exact algorithm, we mean that we rely on multi-precision arithmetic; our output which encodes points whose coordinates are algebraic numbers is exact since it provides a rational parametrization with rational coefficients of those points. However, we allow probabilistic algorithms using on some random (i.e. generic) changes of variables.

By efficient algorithm, we mean that the theoretical worst-case complexity should be well understood and controlled, improving the state-of-the-art in the field. In particular, our algorithm should perform significantly better than general-purpose symbolic computation available algorithms, and this should be evidenced by explicit, reproducible experiments.

1.2 Motivations

The problem of finding low rank elements in a given affine subspace has many applications in systems, signal and information engineering, where low rank elements typically correspond to sparsity and structure requirements. For example, in the context of semidefinite programming (SDP) hierarchies for polynomial optimization [42], low rank moment matrices provide guarantees of global optimality of a convex relaxation of a nonconvex optimization problem.

Moreover, solving efficiently the real root finding problem for linear matrices is a first step towards obtaining complexity bounds for semidefinite programming. Indeed, let $A(x)$ be symmetric, and let $S = \{x \in \mathbb{R}^n \mid A(x) \succeq 0\}$ be the associated spectrahedron. One can prove that if r is the minimum rank attained by $A(x)$ over (the boundary of) S, then at least one of the connected components of $\mathcal{D}_r \cap \mathbb{R}^n$ is contained in S. This implies that one can decide the emptiness of S (and, hence, the feasibility of a semidefinite program) by deciding the emptiness of $\mathcal{D}_r \cap \mathbb{R}^n$.

Similarly, the geometry of low rank structured matrices (e.g. Hurwitz matrices, Hankel matrices, Toeplitz matrices, resultant matrices) is pervasive in algebraic approaches to information engineering (including systems control, signal processing, computer vision and computational geometry), see e.g. [46], [38] or [19] and the references therein. The specific geometry of low rank manifolds can be exploited to design efficient nonlinear local optimization algorithms [1]. Sparsity-promoting optimization methods are now commonly used in floating-point computational environments, and compressed sensing algorithms based on large-scale convex optimization methods are listed amongst the success stories of applied mathematics in engineering, see e.g. [15]. Finally, linear matrices and their loci of rank defects are the object of the so-called low rank approximation problem, see e.g. [49].

In our paper, we are not after large-scale problem instances solved approximately with floating point arithmetic. In contrast, our focus is on symbolic computation and rigorous

algorithms. This means that we are not concerned with numerical scaling and conditioning issues: all our computations are carried out with exact arithmetic on integers and rational numbers, and we provide mathematical guarantees of exactness of the output of our algorithm, under the assumption that the input is also exactly provided in rational arithmetic and satisfies some genericity assumptions that are specified below. Obviously, these guarantees come with a price, and our algorithm complexity is exponential in the number of variables or problem size, and hence limited to small dimensions. But this is not specific to our algorithm, this limitation is shared with all symbolic computation methods: our algorithm should be applied to small-size problems for which it is absolutely crucial to find exact solutions.

However, the main difference with the state-of-the-art is that the complexity achieved by our algorithm is essentially quadratic in a multilinear Bézout bound on the maximum number of complex solutions encoded by the output. This bound is itself dominated by $\binom{n+m(m-r)}{n}^3$. Hence, for particular sub-classes of the problem, for example when the size of the matrix is fixed, the multilinear bounds (and hence the complexity) are polynomial in the number of variables.

1.3 Example

Consider the Cayley determinantal cubic surface

$$\mathcal{D}_2 = \big\{x \in \mathbb{C}^3 \;\big|\; \text{rank } A(x) \leq 2\big\}.$$

with

$$A(x) = \begin{pmatrix} 1 & x_1 & x_2 \\ x_1 & 1 & x_3 \\ x_2 & x_3 & 1 \end{pmatrix}$$

whose real part delimits a convex open connected component whose closure is the well-known spectrahedron arising in the SDP relaxation of the MAXCUT combinatorial optimization problem, see e.g. [50, Example 2] and Figure 1. The Cayley surface has singularities captured by the set

$$\mathcal{D}_1 = \big\{x \in \mathbb{C}^3 \;\big|\; \text{rank } A(x) \leq 1\big\}.$$

whose real part consists of four points

$$\mathcal{D}_1 \cap \mathbb{R}^3 = \left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix} \right\}.$$

1.4 State of the art

Computing real solutions of systems of polynomial equations, and deciding the emptiness of real algebraic sets, is a central question in computational geometry. Since one typically

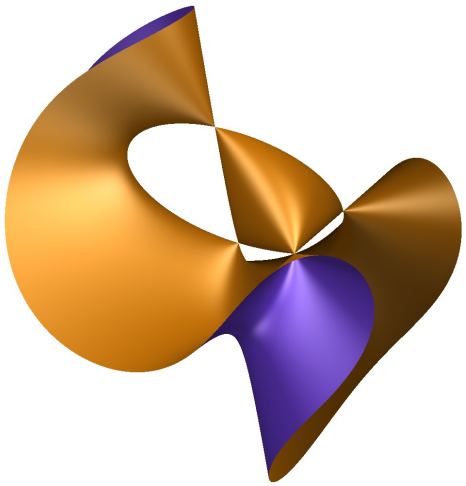

Figure 1: Cayley determinantal cubic surface with its four singular points on the boundary of its spectrahedron.

deals with positive dimensional solution sets, one possible approach is to design algorithms computing a finite set intersecting each connected component. While the complexity of the first algorithm solving this problem (Tarski, [57]) was not elementary recursive, Collins designed in [16] the Cylindrical Algebraic Decomposition algorithm, whose complexity is doubly exponential in the number of variables. Since Thom-Milnor bound for the maximum number of connected components of a real algebraic set (see [10, Theorem 7.23]) is singly exponential in the number of variables, tremendous efforts have been made to obtain optimal complexity bounds.

Grigoriev and Vorobjov introduced in [34] the first algorithm whose complexity is singly-exponential in the number of variables n. It is based on the critical point method. The algorithms in [5, 4, 7, 6, 8, 53, 54] also rely on the computation of critical points. On inputs of degree $\leq d$, they lead to almost optimal complexities which are essentially cubic in d^n for the general smooth case, quartic in d^n for the general singular one. These techniques have also been used in the context of polynomial optimization [33, 35].

In the context of algebraic varieties defined by the vanishing of the determinant of a linear matrix, which corresponds to the problem stated in Section 1.1 in the particular case $r = m - 1$, we designed in [37] an efficient algorithm based on the study of incidence varieties. In this previous work, the proof of correctness of the algorithm is based on regularity properties of the incidence varieties, and our theoretical analysis of worst-case complexity also strongly exploits the determinantal structure.

In the current paper, we build on our previous work [37] to allow the rank of the linear matrix to drop below the value $m - 1$, which means that the algebraic variety is defined not only by the vanishing of the determinant, but also that of lower order minors of the matrix. Consequently, the proof of correctness and the theoretical analysis of complexity of the algorithm should be adapted to this case. The basic ingredients of our algorithm remain essentially the same as those of [37]: we still consider critical points of some well chosen projections restricted to incidence varieties. However, the arguments used

in [37] cannot be applied *mutatis mutandis* to our context since we allow higher rank defects. Hence, our analysis of regularity properties of the indicence varietes as well as the bounds on the complexity are significantly revisited. In particular, for the computation of rational parametrizations we rely on homotopy-based techniques for obtaining geometric resolutions of finite sets, see [40].

1.5 Paper outline and main results

The algorithm described in this paper, with input a linear matrix $A(x) = A_0 + x_1A_1 + \ldots + x_nA_n$, with $A_i \in \mathbb{Q}^{m\times m}$, $i = 0, 1, \ldots, n$, and an integer $r \leq m-1$, computes a rational parametrization of a finite set intersecting each connected components of $\mathcal{D}_r \cap \mathbb{R}^n$. The design of the algorithm is intented to take advantage of the special structure of the input problem and hence to behave better than algorithms based on the critical point method that solve more general problems.

To do that, we investigate properties of an incidence variety and show that our problem can be reduced to compute finitely many critical points of the restriction of a well-chosen projection to this incidence variety. The system that defines these critical points has a special sparisty structure. Using routines in [40], one can compute a rational parametrization of these critical points by exploiting this sparsity structure. We establish a bound δ on the degree of the parametrization, and, using [40], we show that the complexity is essentially quadratic on δ. This bound is dominated by $\binom{n+m(m-r)}{n}^3$.

Moreover, we provide computer experiments that show that our strategy allows to tackle problems that are unreachable by implementations of other generic algorithms based on the critical point method.

The paper is structured as follows. In Section 2 we set up the general notation used throughout the paper and we recall the key notion of incidence variety. We also state formally the genericity properties under which our algorithm is guaranteed to provide a correct output. Finally, we decribe the input/output data representation of our algorithm, solely based on integer and rational arithmetic. In Section 3, we provide a formal description of our algorithm, we state its correctness, and we carry out a precise complexity analysis. The proof of correctness relies on the following technical ingredients: regularity of an indidence variety, see Section 4, dimension of a Lagrangian variety, see Section 5 and closure properties, see Section 6. The paper ends up with some computer experiments on an implementation of our algorithm, reported in Section 7.

2 Definitions and notation

We denote by $\mathbb{Q}^n$ (resp. $\mathbb{C}^n$) the set of vectors of length n with entries in $\mathbb{Q}$ (resp. $\mathbb{C}$).

A subset $\mathcal{V} \subset \mathbb{C}^n$ is an affine algebraic variety (equivalently affine algebraic set) if it is the common zero locus of a system of polynomials $f = (f_1, \ldots, f_q) \in \mathbb{Q}[x]^q$, with $x = (x_1, \ldots, x_n)$. We also write $\mathcal{V} = f^{-1}(0) = \mathcal{Z}(f)$. Algebraic varieties in $\mathbb{C}^n$ define the closed sets of the so-called Zariski topology. Zariski open subsets of $\mathbb{C}^n$ are sets whose

complement are Zariski closed; they are either empty or dense in $\mathbb{C}^n$.

The set of all polynomials vanishing on an algebraic set $\mathcal{V}$ is an ideal and it is denoted by $I(\mathcal{V}) \subset \mathbb{Q}[x]$. This ideal is radical (i.e. $g^k \in I(\mathcal{V})$ for some integer k implies that $g \in I(\mathcal{V})$) and it is generated by a finite set of polynomials, say $f = (f_1, \ldots, f_p)$. We also write $I(\mathcal{V}) = \langle f_1, \ldots, f_p \rangle = \langle f \rangle$ when a set of generators is known. We say that the length of the polynomial system $f = (f_1, \ldots, f_p)$ is p.

Let $\mathrm{GL}(n, \mathbb{C})$ (resp. $\mathrm{GL}(n, \mathbb{Q})$) be the set of non-singular $n \times n$ matrices with entries in $\mathbb{C}$ (resp. $\mathbb{Q}$). The identity matrix is denoted by I_n. Given a matrix $M \in \mathrm{GL}(n, \mathbb{Q})$ and a polynomial system $x \in \mathbb{C}^n \mapsto f(x) \in \mathbb{C}^p$ we denote by $f \circ M$ the polynomial system $x \in \mathbb{C}^n \mapsto f(M\,x) \in \mathbb{C}^p$. If $\mathcal{V} = \mathcal{Z}(f)$, the image set $\mathcal{Z}(f \circ M) = \{x \in \mathbb{C}^n : f(Mx) = 0\} = \{M^{-1}x \in \mathbb{C}^n : f(x) = 0\}$ is denoted by $M^{-1}\mathcal{V}$. Given $q \leq n$ and $M \in \mathbb{C}^{m \times m}$, we denote by $\mathrm{minors}(q, M)$ the set of determinants of $q \times q$ submatrices of M.

For $f \subset \mathbb{Q}[x]^q$, we denote by Df the Jacobian matrix of f, that is the $q \times n$ matrix $Df = (\frac{\partial f_i}{\partial x_j})_{i,j}$. When f generates a radical ideal, the co-dimension c of $\mathcal{Z}(f)$ is the maximum rank of Df evaluated at points in $\mathcal{Z}(f)$. Its dimension is $n-c$. The algebraic set $\mathcal{V} = \mathcal{Z}(f)$ is said irreducible, if it is not the union of two algebraic sets strictly contained in $\mathcal{Z}(f)$. If $\mathcal{V}$ is not irreducible, it is decomposable as the finite union of irreducible algebraic sets, called the irreducible components. If all the irreducible components have the same dimension, $\mathcal{V}$ is equidimensional. The dimension of $\mathcal{V}$ coincides with the maximum of the dimensions of its components.

Let $f\colon \mathbb{C}^n \to \mathbb{C}^q$ generate a radical ideal, and let $\mathcal{V} = \mathcal{Z}(f)$ be equidimensional of dimension d. A point $x \in \mathcal{V}$ such that the rank of Df is equal to $n - d$ is a regular point, otherwise is a singular point. We denote by $\mathrm{reg}\,\mathcal{V}$ and $\mathrm{sing}\,\mathcal{V}$ respectively the set of regular and singular points of $\mathcal{V}$.

Let $f\colon \mathbb{C}^n \to \mathbb{C}^q$ and let $\mathcal{V} = \mathcal{Z}(f)$ be equidimensional of dimension d. Let $g\colon \mathbb{C}^n \to \mathbb{C}^p$ and assume that f generates a radical ideal. The set of critical points of the restriction of g to $\mathcal{V}$ is defined as the set of points at which f and the minors of size $n - d + m$ of the extended Jacobian matrix $D(f, g)$ and at which $D(f)$ has rank $n - d$. It is denoted by $\mathrm{crit}(g, \mathcal{V})$. Let $\pi_1\colon \mathbb{C}^n \to \mathbb{C}$ be the projection $\pi_1(x) = x_1$ and let $D_1 f$ be the matrix obtained by deleting the first column of Df. Then $\mathrm{crit}(\pi_1, \mathcal{V})$ is equivalently defined by the zero set of f and by the maximal minors of $D_1 f$.

2.1 Incidence variety

Let $A = (A_0, A_1, \ldots, A_n)$ be $m \times m$ matrices with entries in $\mathbb{Q}$, and $A(x) = A_0 + x_1 A_1 + \cdots + x_n A_n$ the associated linear matrix. If $x \in \mathcal{D}_r = \{x \in \mathbb{C}^n : \mathrm{rank}\, A(x) \leq r\}$, the kernel of $A(x)$ has dimension $\geq m - r$. We introduce $m(m-r)$ variables $y = (y_{1,1}, \ldots, y_{m,m-r})$, stored in a $m \times (m-r)$ linear matrix

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

and, for $U \in \mathbb{Q}^{(m-r)\times m}$ and $S \in \mathbb{Q}^{(m-r)\times(m-r)}$, we define the *incidence variety* associated to (A, U, S) as

$$\mathcal{V}_r(A, U, S) := \big\{(x, y) : A(x)Y(y) = 0, UY(y) - S = 0\big\}. \tag{1}$$

Remark 1 *It is easy to check that the matrix $Y(y)$ has full rank $m - r$ if and only if there exists $U \in \mathbb{Q}^{(m-r)\times m}$ of full rank and $S \in \mathrm{GL}(m - r, \mathbb{Q})$ such that $UY(y) - S = 0$.*

For $A \in \mathbb{C}^{m^2(n+1)}$, $U = (u_{i,j})_{1\le i\le m-r, 1\le j\le m} \in \mathbb{Q}^{(m-r)\times m}$ and $S = (s_{i,j})_{1\le i,j\le m-r} \in \mathbb{Q}^{(m-r)\times(m-r)}$, define

$$\begin{array}{rccl} f(A,U,S): & \mathbb{C}^{n+m(m-r)} & \to & \mathbb{C}^{(2m-r)(m-r)} \\ & (x, y) & \mapsto & (A(x)Y(y),\ UY(y) - S) \end{array}$$

Remark that $\mathcal{V}_r(A, U, S) = \mathcal{Z}(f(A, U, S))$ and that the projection of $\mathcal{V}_r(A, U, S)$ over the $x-$space is contained in the determinantal variety $\mathcal{D}_r$, by definition. We will prove that up to genericity assumptions, the algebraic variety $\mathcal{V}_r(A, U, S)$ is equidimensional and smooth. When parameters are clear from the context, we will denote $f(A, U, S)$ by f.

2.2 Data representation

2.2.1 Input

The input of our algorithm is a $m \times m$ linear matrix $A(x) = A_0 + x_1A_1 + \cdots + x_nA_n$ encoded by the vector of defining matrices $(A_0, A_1, \ldots, A_n)$, with coefficients in $\mathbb{Q}$, and an integer r such that $0 \le r \le m - 1$. The vector $(A_0, A_1, \ldots, A_n)$ is understood as a point in $\mathbb{Q}^{(n+1)m^2}$. With abuse of notation, we refer to this input with the short-hand notation $A = (A_0, A_1, \ldots, A_n)$.

2.2.2 Output

The output of the algorithm encodes a finite set intersecting each connected component of $\mathcal{D}_r \cap \mathbb{R}^n$. Indeed, the initial problem is reduced to isolating the real solutions of an algebraic set $\mathcal{Z} \subset \mathbb{C}^n$ of dimension at most 0. To this end, we compute a rational parametrization of $\mathcal{Z}$ that is given by a polynomial system $q = (q_0, q_1, \ldots, q_n, q_{n+1}) \in \mathbb{Q}[t]^{n+2}$ such that q_0, q_{n+1} are coprime (i.e. their greatest common divisor is constant), $\mathcal{Z}$ is in one-to-one correspondence with the roots of q_{n+1}, and

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

This allows to reduce real root counting isolation to a univariate problem. Note that when q_{n+1} is square-free, the cardinality of $\mathcal{Z}$ is the degree of q_{n+1}; we denote it by $\deg q$. When $\mathcal{Z}$ is empty, we have $q = 1$.

One could remark that, since q_0 and q_{n+1} are coprime, one can obtain a rational parametrization with $q_0 = 1$. As observed in [2], choosing q_0 equal to the derivative of q_{n+1} leads, most of the time, to rational parametrizations with coefficients of smaller size in $q_1, \ldots, q_n$.

Given $f \subset \mathbb{Q}[x]$ defining a finite set $\mathcal{Z} \subset \mathbb{C}^n$, there exist many algorithms for computing a rational parametrization of $\mathcal{Z}$.

2.3 Genericity properties

Our algorithm works under some assumptions on the input A and r. We will prove below in Section 3 that these assumptions are generic.

2.3.1 Property G_1

We say that A satisfies G_1 if $\operatorname{sing} \mathcal{D}_r = \mathcal{D}_{r-1}$. In Proposition 2 below, we prove that this property is generic in the space of input matrices.

2.3.2 Property G_2

We say that a polynomial system $f = (f_1, \ldots, f_p) \in \mathbb{Q}[x_1, \ldots, x_n]^p$ satisfies G_2 if

- $\langle f \rangle$ is a radical ideal, and
- $\mathcal{Z}(f) \subset \mathbb{C}^n$ is either empty or smooth and equidimensional.

2.3.3 Property G

Finally, we say that (A, U, S) satisfies G if:

- A satisfies G_1, and
- $\mathcal{D}_p$ is empty or has co-dimension $(m-p)^2$, for $0 \leq p \leq r$, and
- $f(A, U, S)$ satisfies G_2.

3 Algorithm: description, correctness, complexity

In this section, we describe the algorithm LowRank, prove its correctness and estimate its complexity.

3.1 Formal description

The input of LowRank is a couple (A, r), where A is a tuple of $n+1$ square matrices $A_0, A_1, \ldots, A_n$ of size m, with entries in $\mathbb{Q}$, and $r \leq m-1$ is an integer. The algorithm is probabilistic and, upon success, its output is a rational parametrization encoding a finite set of points intersecting each connected component of the real algebraic set $\{x \in \mathbb{R}^n \mid \operatorname{rank} A(x) \leq r\}$, see section 2.2 for a comprehensive description of the input and output data.

3.1.1 Notation

Change of variables. Let $M \in \mathrm{GL}(n, \mathbb{C})$. As already explained in Section 2, we denote by $A \circ M$ the affine map $x \mapsto A(M\,x)$ obtained from A by applying a change of variables induced by the matrix M. In particular $A = A \circ I_n$. For $M \in \mathrm{GL}(n, \mathbb{C})$, and for all $A \in \mathbb{C}^{(n+1)m^2}, U \in \mathbb{C}^{(m-r)\times m}$ and $S \in \mathrm{GL}(m-r, \mathbb{C})$, we consequently denote by $f(A\circ M, U, S)$ the polynomial system $f(A, U, S)$ applied to $(M\,x, y)$, and by $\mathcal{V}_r(A\circ, U, S) = \mathcal{Z}(f(A \circ M, U, S))$.

Fibers. Recall that given $A \in \mathbb{C}^{m^2(n+1)}, M \in \mathrm{GL}(n, \mathbb{C}), U \in \mathbb{C}^{(m-r)\times m}$ and $S \in \mathrm{GL}(m-r, \mathbb{C})$, the polynomial system $f(A \circ M, U, S)$ and its zero locus $\mathcal{V}_r(A \circ M, U, S)$ have been defined in Section 2.1. Given $t \in \mathbb{C}$, define

$$\begin{array}{rccl} f_t: & \mathbb{C}^{n+m(m-r)} & \to & \mathbb{C}^{(2m-r)(m-r)+1} \\ & (x, y) & \mapsto & (f(A \circ M, U, S),\ x_1 - t) \end{array}$$

and denote by $\mathcal{V}_{r,t}(A \circ M, U, S) = \mathcal{Z}(f_t) \subset \mathbb{C}^{n+m(m-r)}$ the section of $\mathcal{V}_r$ with the linear space defined by $x_1 - t = 0$. When parameters are clear from the context, we use the shorter notation $\mathcal{V}_{r,t}$. We remark that, *e.g.* for $M = I_n$, $f_t = f(\tilde{A}, U, S)$ with $\tilde{A} = (A_0 + tA_1) + x_2A_2 + \ldots + x_nA_n$.

Lagrange systems. Given $v \in \mathbb{C}^{(2m-r)(m-r)}$, define

$$\begin{array}{rccl} \ell(A \circ M, U, S, v): & \mathbb{C}^{n+(3m-r)(m-r)} & \to & \mathbb{C}^{n+(3m-r)(m-r)} \\ & (x, y, z) & \mapsto & (f(A \circ M, U, S), z'D_1f,\ v'z - 1) \end{array}$$

where variables $z = (z_1, \ldots, z_{(2m-r)(m-r)})$ stand for Lagrange multipliers, and let $\mathcal{Z}(A \circ M, U, S, v) = \mathcal{Z}(\ell(A \circ M, U, S, v)) \subset \mathbb{C}^{n+m(m-r)+(2m-r)(m-r)}$.

3.1.2 Subroutines

The algorithm LowRank uses different subroutines, described as follows.

- IsReg: inputs parameters A, U, S and outputs true if (A, U, S) satisfies G and `false` otherwise;
- RatPar: inputs a zero-dimensional polynomial system f and returns a rational parametrization of its solutions;
- Project: inputs a rational parametrization of a finite set $\mathcal{Z} \subset \mathbb{C}^N$ and a subset of the variables $x_1, \ldots, x_N$, and outputs a rational parametrization of the projection of $\mathcal{Z}$ on the space generated by this subset;
- Lift: inputs a rational parametrization of a finite set $\mathcal{Z} \subset \mathbb{C}^N$ and a number $t \in \mathbb{C}$, and outputs a rational parametrization of $\{(t, x) : x \in \mathcal{Z}\}$;

- Image: inputs a rational parametrization of a finite set $\mathcal{Z} \subset \mathbb{C}^N$ and a matrix $M \in \mathrm{GL}(N, \mathbb{C})$; outputs a rational parametrization of $M^{-1}\mathcal{Z}$;
- Union: inputs rational parametrizations encoding finite sets $\mathcal{Z}_1, \mathcal{Z}_2$ and outputs a rational parametrization of $\mathcal{Z}_1 \cup \mathcal{Z}_2$.

3.1.3 The algorithm

With input (A, r), the algorithm draws randomly matrices U and S and checks whether A satisfies G. If this is the case, it calls a recursive subroutine called LowRankRec with the same input (A, r). Otherwise it returns an error message.

LowRank(A, r)

Input: A $n-$variate linear matrix $A(x)$ of size m, encoded by the $m^2(n+1)$ rational entries of $A_0, A_1, \ldots, A_n$, and an integer $0 \leq r \leq m-1$;

Output: Either an error message, or the output of LowRankRec.

Procedure:

1. Choose randomly $U \in \mathbb{Q}^{(m-r)\times m}$, $S \in \mathbb{Q}^{(m-r)\times(m-r)}$;
2. If IsReg(A, U, S) = `false` then return an error message saying that the input data A are not generic;
3. else return LowRankRec(A, r).

The subroutine LowRankRec is recursive. It takes as input the couple (A, r). Then:

- if $n < (m-r)^2$, it checks whether the algebraic set $\mathcal{D}_r$ is empty or not; if $\mathcal{D}_r = \emptyset$ it returns an empty list, otherwise it returns an error message;
- if $n = (m-r)^2$, it directly computes a rational parametrization of the projection of the finite set $\mathcal{V}_r$ on $(x_1, \ldots, x_n)$;
- if $n > (m-r)^2$, it computes a rational parametrization of the ideal $\langle \ell(A \circ M, U, S, v) \rangle$, where M, v are chosen randomly. Then it chooses a random value $t \in \mathbb{Q}$ and recall recursively LowRankRec with input (A', r) where A' is obtained by setting X_1 to t in $A \circ M$.

The output is a rational parametrization whose real solutions contain a point for each connected component of $\mathcal{D}_r$.

LowRankRec(A, r)

Input: A $n-$variate linear matrix $A(x)$ of size m, encoded by the $m^2(n+1)$ rational entries of $A_0, A_1, \ldots, A_n$, and an integer $0 \leq r \leq m-1$;

Output: Either an error message if 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 any connected component $\mathcal{C} \subset \mathcal{D}_r \cap \mathbb{R}^n$, there exists $t_0 \in \mathcal{Z}(q_{n+1})$ with $(q_1(t_0)/q_0(t_0), \ldots, q_n(t_0)/q_0(t_0)) \in \mathcal{C}$.

Procedure:

1. If $n < (m-r)^2$ then return an empty list;
2. If $n = (m-r)^2$ then return Project(RatPar(f), $(x_1, \ldots, x_n)$);
3. Choose randomly $M \in \mathrm{GL}(n, \mathbb{Q})$, $v \in \mathbb{Q}^{(2m-r)(m-r)}$;
4. P = Image(Project(RatPar($l(A \circ M, U, S, v)$), $(x_1, \ldots, x_n)$), M^{-1});
5. Choose randomly $t \in \mathbb{Q}$, and define $A = (A_0 + tA_1, A_2, \ldots, A_n)$;
6. Q = Lift(LowRankRec$(A, r), t)$;
7. return Union(Q, P).

3.2 Correctness

The correctness of the algorithm is proved in Theorem 5. It is supported by intermediate results that we discuss below.

The first result states that Property G holds when A is generic in $\mathbb{C}^{m^2(n+1)}$. Also, it states that Property G is inherited by generic sections f_t of the incidence variety. Its proof is contained in Section 4.

Proposition 2 *Let $S \in \mathrm{GL}(m-r, \mathbb{Q})$ and let $U \in \mathbb{Q}^{(m-r)\times m}$.*

1. *There exists a non-empty Zariski-open set $\mathscr{A} \subset \mathbb{C}^{m^2(n+1)}$ such that if $A \in \mathscr{A} \cap \mathbb{Q}^{m^2(n+1)}$, (A, U, S) satisfies Property* G*;*
2. *If (A, U, S) satisfies Property* G*, there exists a non-empty Zariski open set $\mathscr{T} \subset \mathbb{C}$ such that if $t \in \mathscr{T} \cap \mathbb{Q}$, and $\tilde{A} = (A_0 + tA_1) + x_2A_2 + \cdots + x_nA_n$, then $(\tilde{A}, U, S)$ satisfies* G*.*

The second result is about Lagrange system $\ell(A \circ M, U, S, v)$. We prove that its set of solutions is finite and that ℓ satisfies Property G_2. The proof of this result is contained in Section 5.

Proposition 3 *Let $S \in \mathrm{GL}(m-r, \mathbb{Q})$ and let $U \in \mathbb{Q}^{(m-r)\times m}$ be full-rank, and A such that (A, U, S) satisfies* G. *Let $c = (2m-r)(m-r)$. Then there exist non-empty Zariski open sets $\mathscr{V} \subset \mathbb{C}^c$ and $\mathscr{M}_1 \subset \mathrm{GL}(n, \mathbb{C})$ such that, if $v \in \mathscr{V} \cap \mathbb{Q}^c$ and $M \in \mathscr{M}_1 \cap \mathbb{Q}^{n\times n}$, the following holds:*

1. *$\mathcal{Z}(A \circ M, U, S, v)$ is empty or finite and $\ell(A \circ M, U, S, v)$ satisfies Property* G_2*;*
2. *the projection of $\mathcal{Z}(A \circ M, U, S, v)$ on (x, y) contains the set of critical points of the restriction of π_1 to $\mathcal{V}_r$.*

The following Proposition states that in generic coordinates the image of each connected component $\mathcal{C}$ of $\mathcal{D}_r \cap \mathbb{R}^n$ by each map $\pi_i(x) = (x_1, \ldots, x_i)$ is a closed subset of the real line $\mathbb{R}$ (for the Euclidean topology). In addition it states that the pre-images of values $t \in \mathbb{R}$ lying on the boundary of $\pi_1(\mathcal{C})$ can be computed as projections of critical points of π_1 restricted to $\mathcal{V}_r$.

Proposition 4 *Let $S \in \mathrm{GL}(m-r, \mathbb{Q})$. There exist non-empty Zariski open sets $\mathscr{U} \subset \mathbb{C}^{(m-r)\times m}$ and $\mathscr{M}_2 \subset \mathrm{GL}(n, \mathbb{C})$ such that if $U \in \mathscr{U} \cap \mathbb{Q}^{(m-r)\times m}$ and $M \in \mathscr{M}_2 \cap \mathbb{Q}^{n\times n}$, and if A is such that (A, U, S) satisfies* G*, and $d = \dim \mathcal{D}_r$, 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;*
2. *if $t \in \mathbb{R}$ lies on the boundary of $\pi_1(M^{-1}\mathcal{C})$ then $\pi_1^{-1}(t) \cap M^{-1}\mathcal{C}$ is finite and there exists $(x, y) \in \mathcal{V}_r(A \circ M, U, S)$ such that $\pi_1(x, y) = t$.*

Now, the previous results suggest that in order to prove correctness of the algorithm LowRank, both input data and parameters chosen internally must belong to pre-determined dense open subsets. We formalize this fact.

If the input of LowRank is a $(n+1)-$uple of matrices $A = (A_0, A_1, \ldots, A_n)$, the computation of the rational parametrization appearing in the procedure of LowRankRec is called exactly $n - (m-r)^2 + 1$ times. We recall that we denoted by $\mathscr{A}$ the non-empty Zariski open set computed in Proposition 2. Before the first call of LowRankRec, parameters U, S are chosen to define the algebraic set $\mathcal{V}_r(A, U, S)$ and no other choices of such matrices are done during the algorithm.

Hypothesis H_1. Input A and random parameters U, S satisfy:

- U is full-rank and $S \in \mathrm{GL}(m-r, \mathbb{Q})$;
- $A \in \mathscr{A} \cap \mathbb{Q}^{m^2(n+1)}$.

One also has to ensure that U, S belong to the non-empty Zariski open sets defined in Proposition 3 and 4 at each call of LowRankRec. Viceversa, parameter M strictly depends on the number of variables and so it is changed at each call. To summarize, the choices of random parameters done during LowRank can be stored in an array:

$$\left(U, S, (M^{(n)}, v^{(n)}, t^{(n)}), \ldots, (M^{((m-r)^2)}, v^{((m-r)^2)}, t^{((m-r)^2)})\right) \tag{2}$$

where the upperscript represents the number of variables. We also denote by $\mathscr{T}^{(j)}$, $\mathscr{U}^{(j)}$, $\mathscr{M}_1^{(j)}$, $\mathscr{M}_2^{(j)}$ and $\mathscr{V}^{(j)}$ the non-empty Zariski open sets defined by Propositions 2, 3 and 4, at the $(n-j+1)-$th recursion call.

Hypothesis H_2. Random parameters (2) satisfy:

- $U \in \bigcap_{j=(m-r)^2}^{n} \mathscr{U}^{(j)} \cap \mathbb{Q}^{(m-r)\times m}$;
- $S \in \mathrm{GL}(m-r, \mathbb{Q})$;
- $M^{(j)} \in \mathscr{M}_1^{(j)} \cap \mathscr{M}_2^{(j)} \cap \mathbb{Q}^{j\times j}$ for $j = (m-r)^2, \ldots, n$;
- $v^{(j)} \in \mathscr{V}^{(j)} \cap \mathbb{Q}^{(2m-r)(m-r)}$ for $j = (m-r)^2, \ldots, n$;
- $t^{(j)} \in \mathscr{T}^{(j)} \cap \mathbb{Q}$ for $j = (m-r)^2, \ldots, n$.

Theorem 5 *If* H_1 *and* H_2 *hold, algorithm* LowRank *returns a rational parametrization whose set of solutions intersects each connected component of* $\mathcal{D}_r \cap \mathbb{R}^n$.

Proof : Suppose first that $n < (m-r)^2$. Since H_1 holds, then the variety $\mathcal{D}_r$ is empty. Hence $\mathcal{D}_r \cap \mathbb{R}^n = \emptyset$ and the algorithm returns a correct output.

Thereafter, we proceed by induction on $n \geq (m-r)^2$.

If $n = (m-r)^2$, since H_1 holds, Proposition 2 implies that $\mathcal{V}_r$ is finite. We deduce that the routine RatPar returns a rational parametrization of $\mathcal{V}_r$ and the routine Project returns a parametrization of $\mathcal{D}_r$.

Let $n > (m-r)^2$ and suppose that for any $(n-1)-$variate linear matrix satisfying G, algorithm LowRank returns the expected output when H_1 and H_2 hold. Let A be a $n-$variate linear matrix of size m, let r be an integer such that $0 \leq r \leq m-1$ and let $\mathcal{C} \subset \mathcal{D}_r \cap \mathbb{R}^n$ be a connected component. Let U, S be the random matrices chosen at Step 1 of LowRank. Let $M \in \mathrm{GL}(n, \mathbb{C})$ be the matrix chosen at Step 3 of LowRankRec with input A and r, and consider the projection $\pi_1 \colon (x_1, \ldots, x_n) \to x_1$ restricted to $\mathcal{V}_r(A \circ M, U, S)$. Since Property $\mathsf{H}_1, \mathsf{H}_2$ hold, by Proposition 4, $\pi_1(M^{-1}\mathcal{C})$ is a closed subset of the image, and so either $\pi_1(M^{-1}\mathcal{C}) = \mathbb{R}$ or $\pi_1(M^{-1}\mathcal{C})$ is a closed set with non-empty boundary. We claim that, in both cases, LowRank with input (A, r) returns a point which lies in the connected component $M^{-1}\mathcal{C}$. This is proved next.

First case. Suppose first that $\pi_1(M^{-1}\mathcal{C}) = \mathbb{R}$. In particular, for $t \in \mathbb{Q}$ chosen at Step 5 of LowRankRec with input A, r, the set $\pi_1^{-1}(t)$ intersects $M^{-1}\mathcal{C}$, so $\pi_1^{-1}(t) \cap M^{-1}\mathcal{C} \neq \emptyset$. Let $A^{(n-1)}$ be the $(n-1)-$variate linear matrix obtained from $A \circ M$ by substituting $x_1 = t$. Remark that $\pi_1^{-1}(t) \cap M^{-1}\mathcal{C}$ is the union of some connected components of the determinantal variety $\mathcal{D}_r^{(n-1)} \cap \mathbb{R}^{n-1} = \{x \in \mathbb{R}^{n-1} : \operatorname{rank} A^{(n-1)} \leq r\}$. Since H_1 holds, $(A^{(n-1)}, U, S)$ satisfies G; we deduce that by the induction hypothesis the subroutine LowRankRec computes one point in each connected component of $\mathcal{D}_r^{(n-1)} \cap \mathbb{R}^{n-1}$, and so at least one point in $M^{-1}\mathcal{C}$.

Second case. Suppose now that $\pi_1(M^{-1}\mathcal{C}) \neq \mathbb{R}$. By Proposition 4, $\pi_1(M^{-1}\mathcal{C})$ is closed. Since $M^{-1}\mathcal{C}$ is connected, $\pi_1(M^{-1}\mathcal{C})$ is a closed interval, and since $\pi_1(M^{-1}\mathcal{C}) \neq \mathbb{R}$ there

exists t in the boundary of $\pi_1(M^{-1}\mathcal{C})$ such that $\pi_1(M^{-1}\mathcal{C}) \subset [t, +\infty)$ or $\pi_1(M^{-1}\mathcal{C}) \subset (-\infty, t]$. Suppose without loss of generality that $\pi_1(M^{-1}\mathcal{C}) \subset [t, +\infty)$, so that t is the minimum value attained by π_1 on $M^{-1}\mathcal{C}$.

Let $x = (t, x_2, \ldots, x_n) \in M^{-1}\mathcal{C}$. By Proposition 4, there exists $y \in \mathbb{C}^{m(m-r)}$ such that $(x, y) \in \mathcal{V}_r$. We claim that there exists $z \in \mathbb{C}^{(2m-r)(m-r)}$ such that (x, y, z) lies in $\mathcal{Z}(A \circ M, U, S, v)$. Then, we conclude that the point $x \in M^{-1}\mathcal{C}$ appears among the solutions of the rational parametrization P obtained at Step 4 of LowRankRec. Correction of the algorithm follows. Now we prove our claim.

Let $\mathcal{C}' \subset \mathcal{V}_r \cap \mathbb{R}^{n+m(m-r)}$ be the connected component such that $M^{-1}\mathcal{C}' \subset M^{-1}\mathcal{V}_r \cap \mathbb{R}^{n+m(m-r)}$ contains (x, y). We first prove that $t = \pi_1(x, y)$ lies on the boundary of $\pi_1(M^{-1}\mathcal{C}')$. Indeed, suppose that there exists $(\widetilde{x}, \widetilde{y}) \in M^{-1}\mathcal{C}'$ such that $\pi_1(\widetilde{x}, \widetilde{y}) < t$. Since $M^{-1}\mathcal{C}$ is connected, and since it is a connected component of a real algebraic variety, there exists a continuous semi-algebraic map $\tau\colon [0, 1] \to M^{-1}\mathcal{C}'$ with $\tau(0) = (x, y)$ and $\tau(1) = (\widetilde{x}, \widetilde{y})$. Let $\pi_x\colon \mathbb{R}^{n+m(m-r)} \to \mathbb{R}^n$ be the map $\pi_x(x, y) = x$. Then also $\pi_x \circ \tau$ is continuous and semi-algebraic (it is the composition of continuous semi-algebraic maps), and $(\pi_x \circ \tau)(0) = x$, $(\pi_x \circ \tau)(1) = \widetilde{x}$. Since $(\pi_x \circ \tau)(\theta) \in \mathcal{D}_r$ for all $\theta \in [0, 1]$, then $\widetilde{x} \in M^{-1}\mathcal{C}$. Since $\pi_1(\widetilde{x}) = \pi_1(\widetilde{x}, \widetilde{y}) < t$ we obtain a contradiction. So $\pi_1(x, y)$ lies on the boundary of $\pi_1(M^{-1}\mathcal{C}')$.

Since (A, U, S) satisfies G, hence $(A \circ M, U, S)$ satisfies G, and by the Implicity Function Theorem one deduces that (x, y) is a critical point of π_1 restricted to $\mathcal{V}_r$ and that, by Proposition 3, there exists $z \in \mathbb{C}^{(2m-r)(m-r)}$ such that $(x, y, z) \in \mathcal{Z}(A \circ M, U, S, v)$, as claimed. □

3.3 Complexity analysis

In this section we provide an analysis of the complexity of algorithm LowRank. We also give bounds for the number of complex solutions computed by LowRank.

We suppose that $f(A, U, S)$ satisfies Property G. We remark that this property can be checked, e.g. via Gröbner bases techniques. Indeed, the dimension of sets $\mathcal{D}_r$ can be computed with Gröbner bases. Further, using the Jacobian criterion [20, Theorem 16.19], the regularity of $\mathcal{V}_r$ is easily checked by verifying that the complex solution set to $f(A, U, S)$ and the maximal minors of its Jacobian matrix is empty.

In order to bound the complexity of LowRank, it is essentially sufficient to bound the complexity of LowRankRec. This latter quantity mainly depends on the subroutine RatPar computing the rational parametrization, whose complexity is computed in Section 3.3.2. We mainly rely on routines described in [40], which consists in a symbolic homotopy algorithm taking advantage of the sparsity structure of the input polynomial system.

Finally, complexity bounds for the subroutines Project, Lift, Image and Union are provided in Section 3.3.3 and refer to results of [55].

3.3.1 Bounds on the degree of the output of RatPar

We consider the subroutine RatPar at the first recursion step of LowRank. Its input consists in either the generators $f(A \circ M, U, S)$ of the incidence variety (if $n = (m-r)^2$) or the Lagrange system $\ell(A \circ M, U, S, v)$ (if $n > (m-r)^2$). In both cases, we provide below in Proposition 6 a bound on the degree of the rational parametrization returned by RatPar.

We recall that if $x^{(1)}, \ldots, x^{(p)}$ are p groups of variables, and $f \in \mathbb{Q}[x^{(1)}, \ldots, x^{(p)}]$, we say that the multidegree of f is $(d_1, \ldots, d_p)$ if its degree with respect to the group of variables $x^{(j)}$ is d_j for $j = 1, \ldots, p$.

Proposition 6 *Let A be a $n-$variate $m \times m$ linear matrix, $0 \leq r \leq m-1$ and let U, S and M, v be respectively the parameters chosen at step 1 of* LowRank *and at step 3 of* LowRankRec*. Suppose that* H_1 *and* H_2 *hold. Then:*

1. *if $n = (m-r)^2$, the degree of the output of* RatPar*, with input $f(A \circ M, U, S)$, is bounded from above by $\delta(m, n, r) = \delta(m, (m-r)^2, r) = \binom{m(m-r)}{(m-r)^2}$;*
2. *if $n > (m-r)^2$, the degree of the output of* RatPar*, with input $\ell(A \circ M, U, S)$, is bounded from above by*

$$\delta(m, n, r) = \sum_{k \in \mathcal{F}_{m,n,r}} \binom{m(m-r)}{n-k} \binom{n-1}{k + (m-r)^2 - 1} \binom{r(m-r)}{k},$$

with $\mathcal{F}_{m,n,r} = \{k : \max\{0, n - m(m-r)\} \leq k \leq \min\{n-(m-r)^2, r(m-r)\}\}$.

Proof of Assertion 1: If $n = (m-r)^2$, since H_1 holds, the dimension of the incidence variety $\mathcal{V}_r$ is zero. Consequently, the degree of the rational parametrization returned by RatPar is the degree of $\mathcal{V}_r$. Since the entries of $f(A \circ M, U, S)$ are bilinear polynomials in x, y, one can compute the Multilinear Bézout bound (see [55, Chapter 11]) on this degree.

From $UY(y) - S$ one can eliminate $(m-r)^2$ variables $y_{i,j}$ (for example, those corresponding to the last $m-r$ rows of $Y(y)$). Abusing notation, we denote by the same symbol $f \subset \mathbb{Q}[x, y_{1,1}, \ldots, y_{r,m-r}]$ the polynomial system obtained after this reduction. It is constituted by $m(m-r)$ polynomials of multidegree bounded by $(1,1)$ with respect to $x = (x_1, \ldots, x_n)$ and $y = (y_{1,1}, \ldots, y_{r,m-r})$.

By [55, Proposition 11.1.1], $\deg \mathcal{Z}(f)$ is bounded by the sum of the coefficients of

$$(s_x + s_y)^{m(m-r)} \mod \left\langle s_x^{n+1}, s_y^{r(m-r)+1} \right\rangle \subset \mathbb{Z}[s_x, s_y].$$

Since $n + r(m-r) = m(m-r)$, and since $(s_x + s_y)^{m(m-r)}$ is homogeneous of degree $m(m-r)$, the aforementioned bound equals the coefficient of $s_x^n s_y^{r(m-r)}$ in the expansion of $(s_x + s_y)^{m(m-r)}$, that is $\binom{m(m-r)}{(m-r)^2}$. □

Proof of Assertion 2: In this case, the input of RatPar is the Lagrange system $\ell(A \circ M, U, S, v)$. Let f be the reduced system defined in the proof of Assertion 1. We apply a similar reduction to $\ell(A \circ M, U, S, v)$. We introduce Lagrange multipliers $z = [1, z_2, \ldots, z_{m(m-r)}]$ (we put $z_1 = 1$ w.l.o.g., since $\ell(A \circ M, U, S, v)$ is defined over the Zariski open set $z \neq 0$) and we consider polynomials $(g, h) = z' D_1 f$. Hence the new reduced system $\ell = (f, g, h)$ is constituted by:

- $m(m-r)$ 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 $(1,0,1)$.

Moreover, by Proposition 3, $\mathcal{Z}(f,g,h)$ has dimension at most zero and (f,g,h) verifies G_2. By [55, Proposition 11.1.1], $\deg \mathcal{Z}(f,g,h)$ is bounded by the sum of the coefficients of

$$(s_x+s_y)^{m(m-r)}(s_y+s_z)^{n-1}(s_x+s_z)^{r(m-r)} \mod \left\langle s_x^{n+1}, s_y^{r(m-r)+1}, s_z^{m(m-r)} \right\rangle \subset \mathbb{Z}[s_x,s_y,s_z].$$

As in the proof of Assertion 1, by homogeneity of the polynomial and by counting the degrees, the previous sum is given by the coefficient of the monomial $s_x^n s_y^{r(m-r)} s_z^{m(m-r)-1}$ in the expansion

$$\sum_{i=0}^{m(m-r)} \sum_{j=0}^{n-1} \sum_{k=0}^{r(m-r)} \binom{m(m-r)}{i}\binom{n-1}{j}\binom{r(m-r)}{k} s_x^{i+k} s_y^{m(m-r)-i+j} s_z^{n-1-j+r(m-r)-k}.$$

The coefficient is obtained by setting the equalities $i+k=n$, $m(m-r)-i+j=r(m-r)$ and $n-1-j+r(m-r)-k = m(m-r)-1$. These equalities imply $i+k=n=j+k+(m-r)^2=j+k+i-j=i+k$ and consequently one deduces the claimed expression. □

Remark 7 *If $n=(m-r)^2$ and if the rank defect $d=m-r$ is fixed, we have $n=d^2$ is fixed and $\delta(m,n,r)=\delta(m,d^2,m-d)=\binom{md}{d^2} \in O(m^{d^2})$.*

Proposition 6 implies straightforwardly the following estimate.

Corollary 8 *Suppose that the hypothesis of Proposition 6 are satisfied. Then* LowRank *returns a rational parametrization whose degree is less than or equal to*

$$\binom{m(m-r)}{(m-r)^2} + \sum_{j=(m-r)^2+1}^{\min\{n,m^2-r^2\}} \delta(m,j,r).$$

Proof : Since H_1 holds, for $n<(m-r)^2$ the algorithm returns the empty list. For m,j,r let $\mathcal{F}_{m,j,r}$ be the set of indices defined in Proposition 6. Observe that $\mathcal{F}_{m,j,r}=\emptyset$ if and only if $j>m^2-r^2$. Hence, the thesis is deduced straightforward from bounds given in Proposition 6. □

One can also deduce the following bound on $\delta(m,n,r)$.

Lemma 9 *For all m,n,r, with $r \le m-1$, $\delta(m,n,r) \le \binom{n+m(m-r)}{n}^3$.*

Proof : This comes straightforwardly from the formula

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

applied with $a=n$ and $b=m(m-r)$, and from the expression of $\delta(m,n,r)$ computed in Proposition 6. □

3.3.2 Complexity of RatPar

As announced in the preamble of the Section, our complexity model for RatPar is the symbolic homotopy algorithm in [40].

We suppose that $n > (m-r)^2$ and that the input of RatPar is the reduced Lagrange system $\ell = \ell(A \circ M, U, S, v) \in \mathbb{Q}[x,y,z]^{n-1+m^2-r^2}$ built in the proof of Assertion 2 of Proposition 6. One can easily build a second polynomial system $\tilde{\ell} \subset \mathbb{Q}[x,y,z]$, 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.

In fact, we remind that by construction, ℓ contains three groups of quadratic polynomials in $\mathbb{Q}[x,y,z]$, of multidegree respectively bounded by $(1,1,0), (0,1,1)$ and $(1,0,1)$. We denote by $\Delta_1 \subset \mathbb{Q}[x,y], \Delta_2 \subset \mathbb{Q}[y,z]$ and $\Delta_3 \subset \mathbb{Q}[x,z]$ the supports of the three groups, so that for example $\Delta_1 = \{1, x_i, y_j, x_i y_j \mid 1 \leq i \leq n, 1 \leq i \leq r(m-r)\}$, or, equivalently, Δ_1 can be seen as the subset of $\mathbb{Z}^{n+r(m-r)}$ made by the exponents of its monomials. Let ℓ_i be with support in Δ_1, $1 \leq i \leq m(m-r)$. Hence we generate two linear forms $k_{i,1} \in \mathbb{Q}[x]$ and $k_{i,2} \in \mathbb{Q}[y]$ and we define $\tilde{\ell}_i(x,y) = k_{i,1}(x)k_{i,2}(y)$. We equivalently generate polynomials $\tilde{\ell}_i(y,z) = k_{i,1}(y)k_{i,2}(z)$, $m(m-r)+1 \leq i \leq m(m-r)+n-1$ and $\tilde{\ell}_i(x,z) = k_{i,1}(x)k_{i,2}(z)$, $m(m-r)+n \leq i \leq n-1+m^2-r^2$. We deduce straightforwardly that $\tilde{\ell}$ verifies the above properties, since its solutions can be computed by solving systems of linear equations.

In [40], the authors build a homotopy path between ℓ and $\tilde{\ell}$, such as

$$t\ell + (1-t)\tilde{\ell} \subset \mathbb{Q}[x,y,z,t] \tag{3}$$

where t is a new variable. The system (3) defines a $1-$dimensional algebraic set, that is a curve. We deduce by [40, Proposition 6.1] that, if the solutions of $\tilde{\ell}$ are known, one can compute a rational parametrization of the solution set of system (3) within $O((\tilde{n}^2 N \log Q + \tilde{n}^{\omega+1})dd')$ arithmetic operations over $\mathbb{Q}$, where:

- $\tilde{n}$ is the number of variables in ℓ;
- $N = m(m-r)\#\Delta_1 + (n-1)\#\Delta_2 + r(m-r)\#\Delta_3$ ($\#$ is the cardinality);
- $Q = \max_{i=1,2,3}\{\|q\| : q \in \Delta_i\}$;
- d is the number of isolated solutions of ℓ;
- d' is the degree of the curve $\mathcal{Z}(t\ell + (1-t)\tilde{\ell})$;
- ω is the exponent of matrix multiplication.

Suppose the following preliminary lemma, whose proof is given below.

Lemma 10 *Let $\mathcal{F}_{m,n,r}$ be the set defined in Proposition 6, and suppose $\mathcal{F}_{m,n,r} \neq \emptyset$. Let $\delta(m,n,r)$ be the bound defined in Proposition 6. Then the degree of $\mathcal{Z}(t\ell + (1-t)\tilde{\ell})$ is in*

$$O\left((n + m^2 - r^2)\, \min\{n, m(m-r)\}\, \delta(m,n,r)\right).$$

Theorem 11 *Let $n > (m-r)^2$. Let A be a $n-$variate $m \times m$ linear matrix, $0 \leq r \leq m-1$ and let M, U, S, v be the parameters chosen during the first recursive step of* LowRank*. Let $\delta = \delta(m,n,r)$ be the bound defined in Proposition 6. Then,* RatPar *returns a rational parametrization within*

$$O^{\sim}\left((n + m^2 - r^2)^7\, \delta^2\right)$$

arithmetic operations.

Proof : Following the notation introduced above, $\tilde{n} = n - 1 + m^2 - r^2$. the bound for d is δ and is given in Proposition 6 and a bound for d' is given in Lemma 10, and is in $O^{\sim}(\tilde{n}^2\delta)$. Moreover, $N \in O(nmr(m-r)^2)$, and hence $N \in O(\tilde{n}^3)$. The proof follows from [40, Proposition 6.1], since the maximum diameter of $\Delta_1, \Delta_2, \Delta_3$ is bounded above by $\tilde{n}$, that is $Q \leq \tilde{n}$. □

Proof of Lemma 10: We exploit the multilinear structure of $t\ell + (1-t)\tilde{\ell}$. By [55, Proposition 11.1.1], $\deg \mathcal{Z}(t\ell + (1-t)\tilde{\ell})$ is bounded by the sum of the coefficients of

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

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

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

and hence that $q \equiv q_1 + q_2 + q_3 + q_4 \mod I$. Below, we bound the contribution of $q_i, i = 1 \ldots 4$. The stated bound is given by the sum of the contributions and follows straightforwardly.

Contributions of q_1. The contribution of q_1 is the sum of its coefficients modulo the ideal $I' = \langle s_x^{n+1}, s_y^{r(m-r)+1}, s_z^{m(m-r)} \rangle$. This has been computed in Proposition 6, and coincides with $\delta(m,n,r)$.

The contribution of q_2. Write $q_2 = m(m-r)s_t\tilde{q}_2$ with $\tilde{q}_2 \in \mathbb{Z}[s_x, s_y, s_z]$. Consequently the contribution is given by the sum of the coefficients of $\tilde{q}_2$, modulo I', multiplied by $m(m-r)$. Now, observe that $\deg \tilde{q}_2 = n - 2 + m^2 - r^2$ and that maxima powers admissible modulo I' are $s_x^n, s_y^{r(m-r)}, s_z^{m(m-r)-1}$. Hence, three configurations give a contribution.

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

$$\Sigma_A = \sum_{k=0}^{r(m-r)} \binom{m(m-r)-1}{n-1-k} \binom{n-1}{k-1+(m-r)^2} \binom{r(m-r)}{k}.$$

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

$$\Sigma_B = \sum_{k=0}^{r(m-r)} \binom{m(m-r)-1}{n-k} \binom{n-1}{k-1+(m-r)^2} \binom{r(m-r)}{k}.$$

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

$$\Sigma_C = \sum_{k=0}^{r(m-r)} \binom{m(m-r)-1}{n-k} \binom{n-1}{k-2+(m-r)^2} \binom{r(m-r)}{k}.$$

So the contribution of q_2 equals $m(m-r)(\Sigma_A + \Sigma_B + \Sigma_C)$.

One easily deduces that $\Sigma_B \leq \delta(m,n,r)$ and $\Sigma_C \leq \delta(m,n,r)$. Remember that we suppose $\mathcal{F}_{m,n,r} \neq \emptyset$, that is $\delta(m,n,r) > 0$. We claim that $\Sigma_A \leq (1+\min\{n, m(m-r)\})\,\delta(m,n,r)$. Consequently, we conclude that the contribution of q_2 is $m(m-r)(\Sigma_A + \Sigma_B + \Sigma_C) \in O\left(m(m-r)\,\min\{n, m(m-r)\}\,\delta(m,n,r)\right)$.

Let us prove this claim. First, denote by

$$\begin{array}{ll} \chi_1 = \max\{0, n-m(m-r)\} & \chi_2 = \min\{r(m-r), n-(m-r)^2\} \\ \alpha_1 = \max\{0, n-1-m(m-r)\} & \alpha_2 = \min\{r(m-r), n-1-(m-r)^2\} \end{array}$$

the indices such that $\delta(m,n,r)$ sums over $\chi_1 \leq k \leq \chi_2$ and Σ_A over $\alpha_1 \leq k \leq \alpha_2$. Remark that $\alpha_1 \leq \chi_1$ and $\alpha_2 \leq \chi_2$. Finally, denote by $\varphi(k)$ the $k-$th term in the sum defining Σ_A, and by $\gamma(k)$ the $k-$th term in the sum defining $\delta(m,n,r)$.

For all indices k admissible for both $\delta(m,n,r)$ and Σ_A, that is for $\chi_1 \leq k \leq \alpha_2$, one gets, by basic properties of binomial coefficients, that

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

When k runs over all admissible indices, the rational function $\Psi(k)$ is non-increasing monotone, and its maximum is attained in $\Psi(\chi_1)$ and is bounded by $\min\{n, m(m-r)\}$. Three possible cases can hold:

1. $\chi_1 = 0$. Hence $\chi_2 = n-(m-r)^2$, $\alpha_1 = 0$ and $\alpha_2 = n-1-(m-r)^2 = \alpha_1 - 1$. We deduce straightforwardly from the above discussion that $\Sigma_A \leq \min\{n, m(m-r)\}\delta(m,n,r)$;

2. $\chi_1 = n-m(m-r)$ and $\alpha_1 = n-1-m(m-r)$. We deduce that $\chi_2 = \alpha_2 = r(m-r)$ and that $\Sigma_A = \sum_{k=\alpha_1}^{\chi_2} \varphi(k) \leq \varphi(\alpha_1) + \min\{n, m(m-r)\}\,\delta(m,n,r) \leq (1+\min\{n, m(m-r)\})\,\delta(m,n,r)$;

3. $\chi_1 = n-m(m-r)$ and $\alpha_1 = 0$. Actually, either this case coincides with case 1 (if $n = m(m-r)$) or we deduce that $n = 1+m(m-r)$, that is $\chi_1 = \chi_2 = 1$ and $\alpha_1 = \alpha_2 = 0$. By straightforward computations one deduces that $\Sigma_A \leq \delta(m,n,r)$.

The contribution of q_3 and q_4. Following exactly the same path as in the case of q_2, one respectively deduces that the contribution of q_3 is in $O\left(n\,\min\{n, m(m-r)\}\,\delta(m,n,r)\right)$ and that of q_4 is in $O\left(r(m-r)\,\min\{n, m(m-r)\}\,\delta(m,n,r)\right)$.

□

3.3.3 Complexity of other minor subroutines

For these complexity bounds, we refer to those given in [55, Lemma 10.1], [55, Lemma 10.3], [55, Lemma 10.5] and [55, Lemma 10.6], from which they are obtained straightforwardly.

Proposition 12 *Let $\delta(m,n,r)$ be the bound defined in Proposition 6. At the first recursion step of* LowRankRec*, the following holds:*

- *the complexity of* Project *is in* $O^{\sim}\left((n+m^2-r^2)^2\,(\delta(m,n,r))^2\right)$*;*
- *the complexity of* Lift *is in* $O^{\sim}\left((n+m^2-r^2)\,(\delta(m,n,r))^2\right)$*;*
- *the complexity of* Image *is in* $O^{\sim}\left((n+m^2-r^2)^2\,\delta(m,n,r)+(n+m^2-r^2)^3\right)$*;*
- *the complexity of* Union *is in* $O^{\sim}\left((n+m^2-r^2)\,(\delta(m,n,r))^2\right)$*.*

4 Regularity of the incidence variety

The goal of this section is to prove Proposition 2.

We start by proving Property G_1 in Assertion 1 and 2.

Proof of Property G_1 in Assertion 1: We denote by $\widehat{\sigma_r} \subset \mathbb{C}^{m\times m}$ the algebraic set of $m\times m$ matrices of rank $\leq r$. By [14, Proposition 1.1] its singular locus is $\widehat{\sigma}_{r-1}$. For all $A \in \mathbb{C}^{m^2(n+1)}$, the set $\mathcal{D}_r$ is the intersection of $\widehat{\sigma_r}$ with the linear space $\mathcal{L} = A_0 + \langle A_1, \ldots, A_n\rangle$. By Bertini's theorem (see [59, Theorem 17.16]), if $\mathcal{L}$ is generic, the following holds:

$$\operatorname{sing}\mathcal{D}_r = \operatorname{sing}(\mathcal{L}\cap\widehat{\sigma}_r) = \mathcal{L}\cap\operatorname{sing}\widehat{\sigma}_r = \mathcal{L}\cap\widehat{\sigma}_{r-1} = \mathcal{D}_{r-1}.$$

We conclude that there exists a non-empty Zariski open set $\mathscr{A}_1 \subset \mathbb{C}^{m^2(n+1)}$ such that if $A \in \mathscr{A}_1$ then A satisfies Property G_1. □

Proof of Property G_1 in Assertion 2: We suppose that (A,U,S) satisfies G. In particular A satisfies Property G_1. By Sard's Lemma [55, Section 4.2], there exists a non-empty Zariski open set $\mathscr{T}_1 \subset \mathbb{C}$ such that if $t \in \mathscr{T}_1$, then a point in $\mathcal{D}_r \cap \mathcal{Z}(x_1 - t)$ is regular if and only if it is regular in $\mathcal{D}_r$. Then, for $t \in \mathscr{T}_1$, the matrix obtained by instantiating x_1 to t in A satisfies Property G_1. □

We focus now on Property G_2. We denote by $a_{\ell,i,j}$ the entry of the matrix A_ℓ at row i and column j, for $\ell = 0,1,\ldots,n$, $i = 1,\ldots,m$ and $j = 1,\ldots,m$.

Our proof is essntially based on Thoms Algebraic Weak Transversality theorem [55, Section 4.2]. We deduce, applying this result to given algebraic maps, the existence of a non-empty Zariski open set with the requested properties.

Proof of Property G_2 in Assertion 1: Define

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

and, for a given $A \in \mathbb{C}^{m^2(n+1)}$, define the induced map

$$\begin{array}{rccc} f_A: & \mathbb{C}^n \times \mathbb{C}^{m(m-r)} & \longrightarrow & \mathbb{C}^{m(m-r)+(m-r)^2} \\ & (x,y) & \longmapsto & f(A,U,S). \end{array}$$

Suppose first that $f^{-1}(0) = \emptyset$. This is equivalent to saying that, for any $A \in \mathbb{C}^{m^2(n+1)}$, $\mathcal{V}_r(A,U,S) = \emptyset$. By the Nullstellensatz [17, Chap. 8], this implies that for any $A \in \mathbb{C}^{m^2(n+1)}$, $\langle f(A,U,S)\rangle = \langle 1\rangle$ which is a radical ideal, and so also $\langle f_t\rangle = \langle 1\rangle$ for all $t \in \mathbb{C}$. In this case we conclude by defining $\mathscr{A}_2 = \mathbb{C}^{m^2(n+1)}$ and $\mathscr{T}_2 = \mathbb{C}$.

Suppose now that $f^{-1}(0) \neq \emptyset$. We prove that there exists a non-empty Zariski open set $\mathscr{A}_2 \subset \mathbb{C}^{m^2(n+1)}$ such that if $A \in \mathscr{A}_2$, the Jacobian matrix of $f(A,U,S)$ has maximal rank at each point of $f_A^{-1}(0)$. This fact implies Property G_2 since we can apply the Jacobian Criterion [20, Theorem 16.19] to obtain that

- the ideal generated by $f(A,U,S)$ is radical;
- the algebraic set defined by $f(A,U,S)$ is either empty or smooth and equidimensional of co-dimension $(2m-r)(m-r)$.

We claim that 0 is a regular value of f, i.e. at any point of the fiber $f^{-1}(0)$ the Jacobian matrix J associated to $f(A,U,S)$ (with respect to variables $a_{\ell,i,j}$, $x = (x_1,\ldots,x_n)$ and $y = (y_{1,1},\ldots,y_{m,m-r})$) has maximal rank. By Thom's Algebraic Weak Transversality theorem [55, Section 4.2] we conclude that there exists a non-empty Zariski open set $\mathscr{A}_2 \subset \mathbb{C}^{m^2(n+1)}$ such that, for every $A \in \mathscr{A}_2$, 0 is a regular value of the induced map f_A, as claimed. We prove this claim in the sequel.

Let (x,y,A) be in the fiber $f^{-1}(0)$ and J be the Jacobian matrix of $f(A,U,S)$ evaluated at the point (x,y,A). We claim that there exists a maximal minor of J which is not zero at (x,y,A). In fact, we consider the submatrix of J obtained by:

- the $m(m-r) \times m^2$ block $\partial(A(x)Y(y))_{i,j}/\partial a_{0,k,\ell}$ of derivatives of polynomial entries of $A(x)Y(y)$ with respect to the variables $\{a_{0,k,\ell} \mid k,\ell = 1,\ldots,m\}$;
- the $(m-r)^2 \times m(m-r)$ block $\partial(UY(y)-S)/\partial y$ of derivatives of polynomial entries of $UY(y)-S$ with respect to variables y; remark also that these polynomials do not depend on a.

We remark that: the first block $\partial(A(x)y)_{i,j}/\partial a_{0,k,\ell}$, up to permuting rows and columns is a $m(m-r)\times m^2$ block-diagonal matrix, with m blocks of size $(m-r)\times m$ on the diagonal all equal to $Y(y)'$; the second block $\partial(UY(y)-s)/\partial y$, up to re-ordering polynomials and variables, is a $(m-r)^2 \times m(m-r)$ matrix with $m-r$ blocks of size $(m-r)\times m$ on the diagonal all equal to U.

Since $(x,y,A) \in f^{-1}(0)$, U and $Y(y)$ satisfy the matrix relation $UY(y) = S$ and S is full rank. So U and $Y(y)$ are full rank by the formula $\operatorname{rank}(UY(y)) \leq \min(\operatorname{rank} U, \operatorname{rank} Y(y))$. Moreover, polynomial entries of $UY(y) - S$ do not depend on parameters $a_{0,i,j}$. Hence we can extract a square non-singular submatrix of J of order $m(m-r)+(m-r)^2 = (2m-r)(m-r)$, proving that J has row-rank $(2m-r)(m-r)$. $\square$

Proof of Property G_2 in Assertion 2: Now, suppose that $A \in \mathbb{C}^{m^2(n+1)}$ is given such that $f(A,U,S)$ satisfies Property G_2. Let

$$\begin{array}{rccc} \pi_1: & \mathcal{V}_r(A,U,S) & \to & \mathbb{C} \\ & (x,y) & \mapsto & x_1 \end{array}$$

be the restriction to $\mathcal{V}_r$ of the projection on the first variable. Since f satisfies G_2, $\mathcal{V}_r(A,u,s)$ is smooth and equidimensional of co-dimension $(2m-r)(m-r)$. By Sard's Lemma ([55, Section 4.2]) the image of critical points of π_1 is included in a hypersurface of $\mathbb{C}$. Let $\mathscr{T}_2 \subset \mathbb{C}$ be the complement of this hypersurface. Then, if $t \in \mathscr{T}_2$, one of the following facts hold:

- $\pi_1^{-1}(t) = \emptyset$. In this case $\mathcal{Z}(f_t) = \emptyset$ and by the Nullstellensatz $I(\pi_1^{-1}(t)) = \langle f_t \rangle = \langle 1 \rangle$, which is a radical ideal;
- $\pi_1^{-1}(t) \neq \emptyset$ and for all $(x,y) \in \pi_1^{-1}(t)$, (x,y) is not a critical point of the map π_1. So the Jacobian matrix of f_t has full rank at each $(x,y) \in \mathcal{Z}(f_t)$, and by the Jacobian criterion f_t defines a radical ideal and $\mathcal{Z}(f_t)$ is smooth and equidimensional of co-dimension $(2m-r)(m-r)+1$.

□

We conclude by proving that $\mathcal{D}_p$ is either empty or has dimension $n-(m-p)^2$, and that this property is inherited after the recursive calls: this fact concludes Proposition 2.

Proof of dimension of $\mathcal{D}_p$ in Assertion 1: Let $0 \leq p \leq r$. Let $\tilde{x}$ denote the vector of m^2 independent variables $\tilde{x}_{i,j}, 1 \leq i,j \leq m$, and let $X \in \mathbb{C}^{m \times m}$ be the matrix $(\tilde{x}_{i,j})_{1 \leq i,j \leq m}$. By [14, Proposition 1.1], the set $\mathcal{Z}(\text{minors}(p+1,X)) \subset \mathbb{C}^{m^2}$ is irreducible of co-dimension $(m-p)^2$ and dimension $p(2m-p)$. Let $a_{\ell,i,j}$ be the entry of A_ℓ at row i and column j. Let $x = (x_1, \ldots, x_n)$ and let

$$I = \langle \text{minors}(p+1,X) \rangle + \langle \tilde{x}_{i,j} - a_{0,i,j} - a_{1,i,j}x_1 - \cdots - a_{n,i,j}x_n \rangle_{1 \leq i,j \leq m} \subset \mathbb{Q}[\tilde{x}, x].$$

The set $\mathcal{Z}(\text{minors}(p+1,X)) \subset \mathbb{C}^{m^2+n}$ is irreducible of co-dimension $(m-p)^2$ and dimension $m^2+n-(m-p)^2$ (in fact, variables $x_1, \ldots, x_n$ do not appear). If linear forms in $\langle \tilde{x}_{i,j} - a_{0,i,j} - a_{1,i,j}x_1 - \cdots - a_{n,i,j}x_n \rangle_{1 \leq i,j \leq m}$ are generic, then $\mathcal{Z}(I) \subset \mathbb{C}^{m^2+n}$ is empty or equidimensional of dimension $n-(m-p)^2$ (Bertini's theorem, see [59, Theorem 17.16]).

Let $\pi\colon \mathbb{C}^{m^2+n} \to \mathbb{C}^n$ be the projection $\pi(\tilde{x}, x) = x$. Let V be an irreducible component of $\mathcal{Z}(I)$. Then V has dimension $n-(m-p)^2$. For $x \in \pi(V)$, the fiber $\pi^{-1}(x)$ is finite. By the Theorem on the Dimension of Fibers [56, Sect. 6.3, Theorem 7], $\dim \pi(V) = \dim V = n-(m-p)^2$. We conclude that there exists a non-empty Zariski open set $\mathscr{A}^{(p)} \subset \mathbb{C}^{m^2(n+1)}$ such that if $A \in \mathscr{A}^{(p)}$, then $\mathcal{D}_p$ has dimension $n-(m-p)^2$. We conclude by defining $\mathscr{A}_3 = \bigcap_p \mathscr{A}^{(p)}$. □

Proof of dimension of $\mathcal{D}_p$ in Assertion 2: Now, suppose that $A \in \mathbb{C}^{m^2(n+1)}$ is such that $\mathcal{D}_p$ has co-dimension $(m-p)^2$ for some $0 \leq p \leq r$. Hence, by Bertini's theorem ([59, Theorem 17.16]) there exists $\mathscr{T}^{(p)} \subset \mathbb{C}$ such that if $t \in \mathscr{T} \cap \mathbb{Q}$, and $\tilde{A} = (A_0 + tA_1) + x_2A_2 + \cdots + x_nA_n$, hence $\tilde{\mathcal{D}}_p = \{x \in \mathbb{C}^{n-1} \mid \text{rank}\tilde{A}(x) \leq p\}$ has co-dimension $(m-p)^2$ or is empty. We conclude by defining $\mathscr{T}_3 = \bigcap_p \mathscr{T}^{(p)}$. □

The proof of Proposition 2 is now immediate by defining $\mathscr{A} = \mathscr{A}_1 \cap \mathscr{A}_2 \cap \mathscr{A}_3$ and $\mathscr{T} = \mathscr{T}_1 \cap \mathscr{T}_2 \cap \mathscr{T}_3$.

5 Dimension of Lagrange systems

The goal of this Section is to prove Proposition 3. This will be done in Section 5.4. Before that, we give a local description of the incidence variety and of the Lagrange system and we provide intermediate results.

5.1 Local description of the incidence variety

Let $A = A_0 + x_1 A_1 + \ldots + x_n A_n$ be a $n-$variate $m \times m$ linear matrix with coefficients in $\mathbb{Q}$, and let $r \leq m-1$. Here we give a local description of the incidence variety $\mathcal{V}_r(A, U, S)$. From now on, for $f \in \mathbb{Q}[x]$, we denote by $\mathbb{Q}[x]_f$ the local ring of $\mathbb{Q}[x]$ at f. We recall that the polynomial system defining $\mathcal{V}_r$ is given by $f(A, U, S)$, which contains the entries of $A(x)Y(y)$ and $UY(y) - S$. For $p \leq r$, let N be the upper-left $p \times p$ submatrix of A, so that

$$A = \begin{pmatrix} N & Q \\ P' & R \end{pmatrix} \tag{4}$$

with $Q \in \mathbb{Q}[x]^{p \times (m-p)}$, $P' \in \mathbb{Q}[x]^{(m-p) \times p}$ and $R \in \mathbb{Q}[x]^{(m-p) \times (m-p)}$. The next Lemma computes the equations of $\mathcal{V}_r$ in the local ring $\mathbb{Q}[x, y]_{\det N}$.

Lemma 13 *Let A, N, Q, P, R be as above, and U, S be any full-rank matrices. Then there exist $\{q_{i,j}\}_{1 \leq i \leq p, 1 \leq j \leq m-r} \subset \mathbb{Q}[x]_{\det N}$ and $\{q'_{i,j}\}_{1 \leq i,j \leq m-p} \subset \mathbb{Q}[x]_{\det N}$ such that the constructible set $\mathcal{V}_r \cap \{(x, y) : \det N(x) \neq 0\}$ is defined by the equations*

$$\begin{aligned} y_{i,j} - q_{i,1} y_{p+1,j} - \ldots - q_{i,m-p} y_{m,j} &= 0 \qquad 1 \leq i \leq p, 1 \leq j \leq m-r \\ q'_{i,1} y_{p+1,j} + \ldots + q'_{i,m-p} y_{m,j} &= 0 \qquad 1 \leq i \leq m-p, 1 \leq j \leq m-r \\ UY(y) - S &= 0. \end{aligned}$$

Proof : We denote by $Y^{(1)}$ and $Y^{(2)}$ the submatrices of $Y(y)$ containing respectively the first p rows and the last $m-p$ rows. We also use the block-division of A as in (4). We claim that in $\mathbb{Q}[x, y]_{\det N}$ the $m(m-r)$ equations $A(x)Y(y) = 0$ can be read as the $m(m-r)$ equations:

$$\begin{pmatrix} I_p Y^{(1)} + N^{-1} Q Y^{(2)} \\ \Sigma(N) Y^{(2)} \end{pmatrix} = 0$$

where $\Sigma(N) = R - P' N^{-1} Q$ is the Schur complement of N in A. Renaming the entries of $N^{-1}Q$ and $\Sigma(N)$ concludes the proof. To prove the claim, remark that since $\det N \neq 0$, $A(x)Y(y) = 0$ if and only if

$$\begin{pmatrix} I_p & 0 \\ -P' & I_{m-p} \end{pmatrix} \begin{pmatrix} N^{-1} & 0 \\ 0 & I_{m-p} \end{pmatrix} \begin{pmatrix} N & Q \\ P' & R \end{pmatrix} Y(y) = 0.$$

□

5.2 The rank at a critical point

Given $A, N, P, Q, R, \Sigma(N)$ as above, let

$$\widetilde{A} = \begin{pmatrix} I_p & N^{-1}Q \\ 0 & \Sigma(N) \end{pmatrix}.$$

Lemma 13 implies that the equations of $\mathcal{V}_r$ in the open set $\{(x, y) : \det N \neq 0\}$ can be rewritten as $\widetilde{A}Y(y) = 0$ and $UY(y) - S = 0$: the polynomial entries of the above expressions are elements of the local ring $\mathbb{Q}[x]_{\det N}$. Now, from the first group of relations $\widetilde{A}(x)Y(y) = 0$ one eliminates variables $\{y_{i,j}\}_{1\leq i\leq p, 1\leq j\leq m-r}$, which can be expressed as polynomial functions of x and $\{y_{i,j}\}_{p+1\leq i\leq m, 1\leq j\leq m-r}$. That is, using the notations introduced in Lemma 13, we can express the entries of $Y^{(1)}$ as polynomials in x and in the entries of $Y^{(2)}$.

Now, consider relations $UY(y) - S = 0$ where the entries of $Y^{(1)}$ have been eliminated. This is a linear system in the entries of $Y^{(2)}$ with coefficients in $\mathbb{Q}[x]_{\det N}$. Since S is full-rank, then U is full-rank and hence $UY(y) - S = 0$ consists of $(m-r)^2$ independent relations. Finally one can eliminate $(m-r)^2$ among the $(m-p)(m-r)$ entries of $Y^{(2)}$ (suppose the first $(m-r)$ rows) and re-write $\Sigma(N)Y^{(2)} = 0$ as $(m-p)(m-r)$ relations in x and in the last $(r-p)(m-r)$ entries of $Y^{(2)}$.

Call F this polynomial system, consider Lagrange multipliers $z = (z_1, \ldots, z_{(m-p)(m-r)})$ and the polynomial system

$$(g_1, \ldots, g_n) = z' D_x F - (w_1, \ldots, w_n).$$

The solutions to the above polynomial system contain the critical points of the projection π_w restricted to $\mathcal{V}_r \cap \{(x, y) : \det N \neq 0\}$. The next Lemma shows that, when w is generic in $\mathbb{C}^n$, the solutions to the Lagrange systems project on points of $\mathcal{D}_r$ with the expected maximal rank r.

Lemma 14 *Let A, U, S be as above and suppose that (A, r) satisfies G_3. Let $p \leq r-1$ and let $g = (g_1, \ldots, g_n)$ be the polynomial system defined above. Then there exists a non-empty Zariski open set $\widetilde{\mathscr{W}} \subset \mathbb{C}^n$ such that if $w \in \widetilde{\mathscr{W}}$ then $g = 0$ has no solution.*

Proof : Let $C \subset \mathbb{C}^{2n+(r-p)(m-r)+(m-p)(m-r)}$ be the constructible set defined by $g = 0$ and by $\det N \neq 0$ and $\operatorname{rank} A(x) = p$, and let $\overline{C}$ be its Zariski closure. Let $\pi_x \colon (x, y, z, w) \to x$ be the projection on the first n variables. The image $\pi_x(C)$ is included in $\mathcal{D}_p \subset \mathcal{D}_r$ and hence, since (A, r) satisfies G_3, it has dimension at most $n - (m-p)^2$. Moreover this projection is dense in $\mathcal{D}_p$. The fiber of π_x over a generic point $x \in \mathcal{D}_p$ is the graph of the polynomial function $w = z' D_x F$, and so it has co-dimension n and dimension $(r-p)(m-r) + (m-p)(m-r) = (m-r)(m+r-2p)$. By the Theorem of the Dimension of Fibers [56, Sect. 6.3, Theorem 7] one deduces that the dimension of C (and hence of $\overline{C}$) is at most $n - (m-p)^2 + (m-r)(m+r-2p) = n - (r-p)^2$. Since $p \leq r-1$ then $\overline{C}$ has dimension at most $n-1$. We deduce that the projection of $\overline{C}$ onto the space $\mathbb{C}^n$ of w is a constructible set of dimension at most $n-1$, and it is included in a hypersurface $H \subset \mathbb{C}^n$. Defining $\widetilde{\mathscr{W}} = \mathbb{C}^n \setminus H$ ends the proof. □

5.3 An intermediate lemma

We consider the incidence variety $\mathcal{V}_r = \mathcal{V}_r(A, U, S)$ and the restriction of the projection $\pi_w \colon (x, y) \to w'x$ to $\mathcal{V}_r$, with $w \in \mathbb{C}^n$. Under the hypothesis that (A, U, S) satisfies G, the set $\mathcal{V}_r$ is either empty or smooth and equidimensional of co-dimension $c := (2m-r)(m-r)$. Hence the set of critical points of the restriction of π_w to $\mathcal{V}_r$ is the projection on the (x, y)-space of the solution set of the system

$$f(A, U, S), \qquad (g, h) = z' \begin{pmatrix} D_x f & D_y f \\ w' & 0 \end{pmatrix},$$

where $z = (z_1, \ldots, z_c, z_{c+1}) \neq 0$. Now, for $A \in \mathscr{A}$, at any solution (x, y, z) of this polynomial system, $z_{c+1} \neq 0$. Moreover, with the hypothesis $w \neq 0$, also $(z_1, \ldots, z_c) \neq 0$. So one introduces a linear combination $\sum_{i=1}^{c} v_i z_i - 1$ with $v \in \mathbb{Q}^c$, and we consider the system

$$f = 0, \qquad g = 0, \qquad h = 0, \qquad \sum_{i=1}^{c} v_i z_i - 1 = 0. \tag{5}$$

The polynomial system (5) has $n+c+m(m-r)+1$ polynomials and $n+c+m(m-r)+1$ variables. We denote by $\mathcal{W}_w(A, U, S, v) \subset \mathbb{C}^{n+c+(m-r)^2+1}$ its zero set. We prove in next Lemma that when w is generic, the set $\mathcal{W}_w(A, U, S, v)$ is finite and regular, and that it encodes the critical points of π_w restricted to $\mathcal{V}_r$. The proof exploits the local description of $\mathcal{V}_r$ given in Section 5.1.

Lemma 15 *Let (A, U, S) satisfy G. There exist non-empty Zariski open sets $\mathscr{V} \subset \mathbb{C}^c$ and $\mathscr{W} \subset \mathbb{C}^n$ such that if $v \in \mathscr{V}$ and $w \in \mathscr{W}$, the following holds:*

1. *the set $\mathcal{W}_w(A, U, S, v)$ is finite and the Jacobian matrix of (5) has maximal rank at each point of $\mathcal{W}_w(A, U, S, v)$;*
2. *the projection of $\mathcal{W}_w(A, U, S, v)$ on the (x, y)-space contains the critical points of $\pi_w \colon (x, y) \to w'x$ restricted to $\mathcal{V}_r(A, U, S)$.*

Proof of Assertion 1 of Lemma 15: We first show that the Lagrange system (5) can be re-written in a local form when we consider the local description of the incidence variety $\mathcal{V}_r$ as above. Let $\widetilde{\mathscr{W}} \subset \mathbb{C}^n$ be the set defined by Lemma 14, and $w \in \widetilde{\mathscr{W}}$. Then one has that all solutions (x, y, z) to the system (5) are such that rank $A(x) = r$. Hence, there exists a $r \times r$ submatrix N of $A(x)$ such that $\det N \neq 0$. We prove below that there exist non-empty Zariski open sets $\mathscr{V}'_N \subset \mathbb{C}^c$ and $\mathscr{W}_N \subset \mathbb{C}^n$ such that for $v \in \mathscr{V}'_N$ and $w \in \mathscr{W}_N$, the statement of Assertion (1) holds locally. Hence, to retrieve the global property, it is sufficient to define $\mathscr{V}'$ (resp. $\mathscr{W}$) as the finite intersection of sets $\mathscr{V}'_N$ (resp. $\mathscr{W}_N$), where N varies in the collection of $r \times r$ submatrices of A.

We use the block-division of matrix A as in (4) with $p = r$ and without loss of generality one can assume to work in the open set $\det N \neq 0$, with N the upper-left $r \times r$ submatrix of A. We deduce by Lemma 13 that the local equations of $\mathcal{V}_r$ are

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

where $Y^{(1)}, Y^{(2)}$ is the row-subdivision of the matrix $Y(y)$ as in Lemma 13 and $U^{(1)}, U^{(2)}$ is the correspondent column-subdivision of U. From the first and third groups of equations one obtains that $S = U^{(1)}(-N^{-1}QY^{(2)}) + U^{(2)}Y^{(2)} = (-U^{(1)}N^{-1}Q + U^{(2)})Y^{(2)}$. Since S is full-rank, then $Y^{(2)}$ and $-U^{(1)}N^{-1}Q + U^{(2)}$ are non-singular, and so:

- the second group of equations can be re-written as $\Sigma(N) = 0$;
- the third group of equations can be re-written as $Y^{(2)} = (-U^{(1)}N^{-1}Q + U^{(2)})^{-1}S$.

The entries of $\Sigma(N)$ in the local ring $\mathbb{Q}[x]_{\det N}$ are exactly the $(m-r)^2$ minors of $A(x)$ obtained as determinants of the $(r+1) \times (r+1)$ submatrices of $A(x)$ containing N (see for example the proof of [55, Proposition 3.2.7]). Since (A, U, S) satisfies G, A satisfies G_1, and the jacobian $D_x[\Sigma(N)]_{i,j}$ of the vector of entries of $\Sigma(N)$ has full-rank at each point x such that $\operatorname{rank} A(x) = r$.

We call $f' = (f'_1, \ldots, f'_c)$ the local equations represented by the entries of $Y^{(1)} + N^{-1}QY^{(2)}$, $\Sigma(N)$ and $Y^{(2)} - (-U^{(1)}N^{-1}Q + U^{(2)})^{-1}S$. The Jacobian matrix of f' has the form

$$Df' = (D_x f' \;\; D_y f') = \begin{pmatrix} D_x[\Sigma(N)]_{i,j} & 0_{(m-r)^2 \times m(m-r)} \\ \star & I_{r(m-r)} \quad \star \\ & 0 \quad I_{(m-r)^2} \end{pmatrix}$$

We consider the polynomials

$$(g'_1, \ldots, g'_n, h'_1, \ldots, h'_{m(m-r)}) = (z_1, \ldots, z_c, z_{c+1}) \begin{pmatrix} D_x f' & D_y f' \\ w_1 \; \ldots \; w_n & 0 \end{pmatrix}.$$

Polynomials in $h' = (h'_1, \ldots, h'_{m(m-r)})$ give the relations $z_i = 0$, for $i = (m-r)^2 + 1, \ldots, c$, and can be eliminated together with variables $z_i, i = (m-r)^2 + 1, \ldots, c$. So the local equations of the Lagrange system (5) are:

$$f' = 0, \qquad g' = 0, \qquad \sum_{i=1}^{(m-r)^2} v_i z_i - 1 = 0,$$

for a given $v \in \mathbb{Q}^{(m-r)^2}$. This is a square system with $n + c + 1$ polynomials and $n + c + 1$ variables. Now, consider the map

$$\begin{array}{rccc} p: & \mathbb{C}^{n+c+1} \times \mathbb{C}^n \times \mathbb{C}^{(m-r)^2} & \longrightarrow & \mathbb{C}^{n+c+1} \\ & (x, y, z, w, v) & \longmapsto & (f', g', \sum_{i=1}^{(m-r)^2} v_i z_i - 1) \end{array}$$

and its section map

$$\begin{array}{rccc} p_{v,w}: & \mathbb{C}^{n+c+1} & \longrightarrow & \mathbb{C}^{n+c+1} \\ & (x, y, z) & \longmapsto & (f', g', \sum_{i=1}^{(m-r)^2} v_i z_i - 1), \end{array}$$

for given $v \in \mathbb{C}^{(m-r)^2}$ and $w \in \mathbb{C}^n$. If $p^{-1}(0) = \emptyset$, then for all v, w, $p_{v,w}^{-1}(0) = \emptyset$, and the claim is proved by taking $\mathscr{V}' = \mathscr{V}'_N = \mathbb{C}^c$ and $\mathscr{W} = \mathscr{W}_N = \widetilde{\mathscr{W}}$ (see Lemma 14).

Suppose now $p^{-1}(0) \neq \emptyset$ and let $(x, y, z, w, v) \in p^{-1}(0)$. We claim that the Jacobian matrix of p at (x, y, z, w, v) has maximal rank. Hence, 0 is a regular value for p and by Thom's Weak Transversality Theorem [55, Section 4.2] there exist $\mathscr{V}_N'' \subset \mathbb{C}^{(m-r)^2}$ and $\mathscr{W}_N \subset \mathbb{C}^n$ non-empty Zariski open sets, such that if $v \in \mathscr{V}_N''$ and $w \in \mathscr{W}_N$, then 0 is a regular value for $p_{v,w}$. This implies that, by the Jacobian criterion, the set $\mathcal{W}_w(A, U, S, v) \cap \{(x, y, z) \mid \det N(x) \neq 0\}$ is empty or zero-dimensional, and that the claim is true with $\mathscr{V}_N' = \mathscr{V}_N'' \times \mathbb{C}^{c-(m-r)^2}$, which is also non-empty and Zariski open. We prove below this claim by exhibiting a non-singular submatrix of Dp.

We remark that, since (A, U, S) satisfies G, the Jacobian matrix Df' has maximal rank at (x, y). Moreover, $z_{c+1} \neq 0$ and by the relation $\sum v_i z_i - 1 = 0$ there exists $1 \leq \ell \leq (m-r)^2$ such that $z_\ell \neq 0$. Then we consider the submatrix of Dp obtained by isolating:

- the non-singular submatrix of Df';
- the derivatives of $g_1, \ldots, g_n$ with respect to $w_1, \ldots, w_n$, giving the identity block Id_n;
- the derivative of $\sum v_i z_i - 1$ with respect to v_ℓ.

The previous blocks isolate a matrix of size $(n + c + 1) \times (n + c + 1)$ whose determinant does not vanish at (x, y, z, w, v). □

Proof of Assertion 2 of Lemma 15: This proof is similar to that of [37, Lemma 15].

Suppose first that $\mathcal{W}_w(A, U, S, v) = \emptyset$ for all $w \in \mathbb{C}^n$ and $v \in \mathbb{C}^c$. Fix $w \in \mathbb{C}^n$, $(x, y) \in \mathcal{V}_r(A, U, S)$ and suppose that (x, y) is a critical point of π_w restricted to $\mathcal{V}_r$. Then, since $\mathcal{V}_r$ is equidimensional, there exists $z \neq 0$ such that (x, y, z) verifies the equations $z'Df = [w, 0]$. Since $z \neq 0$, there exists $v \in \mathbb{C}^c$ such that $v'z = 1$. So we conclude that $(x, y, [z, 1]) \in \mathcal{W}_w(A, U, S, v)$, which is a contradiction. Hence $\mathrm{crit}(\pi_w, \mathcal{V}_r) = \emptyset$ and Assertion 2 is proved.

Suppose now that (A, U, S) satisfy G and that $\mathcal{Z}(p)$ is non-empty. Suppose that $w \in \mathscr{W}$ (the set defined in the proof of Assertion 1). By [55, Sect. 3.2], $\mathrm{crit}(\pi_w, \mathcal{V}_r)$ is the image of the projection $\pi_{x,y}$ on x, y of the constructible set:

$$\mathcal{S} = \{(x, y, z) : f = g = h = 0,\ z \neq 0\}$$

where f, g, h have been defined in (5). One can easily prove, by means of Thom's Weak Transversality theorem, that $\mathcal{S}$ has dimension at most 1. Moreover, for each (x, y) in $\pi_{x,y}(\mathcal{S})$, the fiber $\pi_{x,y}^{-1}(x, y)$ has dimension 1, since if $(x, y, z) \in \pi_{x,y}^{-1}(x, y)$, then $(x, y, \lambda z) \in \pi_{x,y}^{-1}(x, y)$ for all $\lambda \neq 0$. By the Theorem on the Dimension of Fibers [56, Sect. 6.3, Theorem 7], we deduce that $\pi_{x,y}(\mathcal{S})$ is finite. Fix now $(x, y) \in \pi_{x,y}(\mathcal{S})$ and let $\mathscr{V}_{(x,y)} \subset \mathbb{C}^c$ be the non-empty Zariski open set such that if $v \in \mathscr{V}_{(x,y)}$, the hyperplane $\sum v_i z_i - 1 = 0$ intersects transversely $\pi_{x,y}^{-1}(x, y)$. Let $\mathscr{V}' \subset \mathbb{C}^c$ be the set defined in the proof of Assertion 1. By defining

$$\mathscr{V} = \mathscr{V}' \bigcap_{(x,y) \in \pi_{x,y}(\mathcal{S})} \mathscr{V}_{(x,y)}$$

one concludes the proof. Indeed, $\mathscr{V}$ is a finite intersection of non-empty Zariski open sets. □

5.4 Proof of Proposition 3

We finally use Lemma 15 to show that, up to a generic change of variables, the set of critical points is finite.

Proof of Proposition 3: Let $\mathscr{M}_1 \subset \mathrm{GL}(n,\mathbb{C})$ be the set of $M \in \mathrm{GL}(n,\mathbb{C})$ such that the first row w' of M^{-1} lies in the set $\mathscr{W}$ given in Lemma 15: this set is non-empty and Zariski open since the entries of M^{-1} are rational functions of the entries of M. Let $\mathscr{V} \subset \mathbb{C}^c$ be the non-empty Zariski open set given by Lemma 15 and let $v \in \mathscr{V}$. We denote by $e'_1 = (1,0,\ldots,0) \in \mathbb{Q}^n$.

Remark that for any $M \in \mathscr{M}_1$ the following identity holds:

$$\begin{pmatrix} Df(A\circ M,U,S) \\ e'_1 \quad 0\cdots 0 \end{pmatrix} = \begin{pmatrix} Df(A,U,S)\circ M \\ w' \quad 0\cdots 0 \end{pmatrix} \begin{pmatrix} M & 0 \\ 0 & I_{m(m-r)} \end{pmatrix}$$

where $Df(A,U,S)\circ M$ means that at all entries of $Df(A,U,S)$ we substitute $x \mapsto M\,x$.

We conclude that the set of solutions of the system

$$f(A,U,S)=0, \quad (z_1,\ldots,z_c)Df(A,U,S) + z_{c+1}(w',0) = 0, \quad v'z - 1 = 0 \tag{6}$$

is the image by the map

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

of the set $\mathcal{S}$ of solutions of the system

$$f(A\circ M,U,S)=0, \quad (z_1,\ldots,z_c)Df(A\circ M,U,S) + z_{c+1}(e'_1,0) = 0, \quad v'z-1=0. \tag{7}$$

Now, let π be the projection that forgets the last coordinate z_{c+1}. Remark that $\pi(\mathcal{S}) = \mathcal{Z}(A\circ M,U,S,v)$ and that π is a bijection. Moreover, it is an isomorphism of affine algebraic varieties, since if $(x,y,z)\in\mathcal{S}$, then its z_{c+1}-coordinate is obtained by evaluating a polynomial at $(x,y,z_1\ldots z_c)$.

Thus, Assertion 1 of Lemma 15 implies that:

- $\mathcal{S}$ and $\pi(\mathcal{S}) = \mathcal{Z}(A\circ M,U,S,v)$ are finite;
- the Jacobian matrix associated to (7) has maximal rank at any point of $\mathcal{S}$.

Since $\pi(\mathcal{S}) = \mathcal{Z}(A\circ M,U,S,v)$ and that π is an isomorphism, Assertion 1 of Proposition 3 follows.

Assertion (2) is a straightforward consequence of Assertion 2 of Lemma 15. □

6 Closure properties

The goal of this section is to prove Proposition 4. We use notation of [37, Section 5], which we recall below.

Notations Let $\mathcal{Z} \subset \mathbb{C}^n$ be an algebraic variety of dimension d. The $i-$equidimensional component of $\mathcal{Z}$ is denoted by $\Omega_i(\mathcal{Z})$, $i = 0, \ldots, d$. We denote by $\mathscr{S}(\mathcal{Z})$ the union of the following sets:

- $\Omega_0(\mathcal{Z}) \cup \cdots \cup \Omega_{d-1}(\mathcal{Z})$
- the set $\mathrm{sing}(\Omega_d(\mathcal{Z}))$ of singular points of $\Omega_d(\mathcal{Z})$

and by $\mathscr{C}(\pi_i, \mathcal{Z})$ the Zariski closure of the union of the following sets:

- $\Omega_0(\mathcal{Z}) \cup \cdots \cup \Omega_{i-1}(\mathcal{Z})$;
- the union for $r \geq i$ of the sets $\mathrm{crit}(\pi_i, \mathrm{reg}(\Omega_r(\mathcal{Z})))$ of critical points of the restriction of π_i to the regular locus of $\Omega_r(\mathcal{Z})$.

For $M \in \mathrm{GL}(n, \mathbb{C})$ we recursively define the collection of algebraic sets $\{\mathcal{O}_i(M^{-1}\mathcal{Z})\}_{0 \leq i \leq d}$ as follows:

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

We recall the two following properties defined in [37, Section 5].

Property $\mathsf{P}(\mathcal{Z})$. Let $\mathcal{Z} \subset \mathbb{C}^n$ be an algebraic set of dimension d. We say that $M \in \mathrm{GL}_n(\mathbb{C})$ satisfies $\mathsf{P}(\mathcal{Z})$ when for all $i = 0, 1, \ldots, d$

1. $\mathcal{O}_i(M^{-1}\mathcal{Z})$ has dimension $\leq i$;
2. $\mathcal{O}_i(M^{-1}\mathcal{Z})$ is in Noether position with respect to $x_1, \ldots, x_i$.

Property $\mathsf{Q}(\mathcal{Z})$. Let $\mathcal{Z}$ be an algebraic set of dimension d and $1 \leq i \leq d$. We say that $\mathsf{Q}_i(\mathcal{Z})$ holds if for any connected component $\mathcal{C}$ of $\mathcal{Z} \cap \mathbb{R}^n$ the boundary of $\pi_i(\mathcal{C})$ is contained in $\pi_i(\mathcal{O}_{i-1}(\mathcal{Z}) \cap \mathcal{C})$. We say that $\mathsf{Q}(\mathcal{Z})$ holds if $\mathsf{Q}_i(\mathcal{Z})$ holds for all $1 \leq i \leq d$.

In [37] the authors proved that given any algebraic variety $\mathcal{Z}$ of dimension d, Property $\mathsf{P}(\mathcal{Z})$ holds generically in $\mathrm{GL}(n, \mathbb{C})$ (Proposition 17) and that if $M \in \mathrm{GL}(n, \mathbb{C})$ satisfies $\mathsf{P}(\mathcal{Z})$, then $\mathsf{Q}(M^{-1}\mathcal{Z})$ holds (Proposition 18). We use these results in the following proof of Proposition 4.

Proof of Assertion 1 of Proposition 4: Let $\mathscr{M}_2 \subset \mathrm{GL}(n, \mathbb{C})$ be the non-empty Zariski open set computed by [37, Proposition 17] for $\mathcal{Z} = \mathcal{D}_r$. One obtains that any $M \in \mathscr{M}_2$ verifies $\mathsf{P}(\mathcal{D}_r)$. Remark that since $M \in \mathrm{GL}(n, \mathbb{C})$ there is a natural bijective correspondence between the set of connected components of $\mathcal{D}_r \cap \mathbb{R}^n$ and the ones of $M^{-1}\mathcal{D}_r \cap \mathbb{R}^n$ given by $\mathcal{C} \leftrightarrow M^{-1}\mathcal{C}$. Fix a connected component $M^{-1}\mathcal{C} \subset M^{-1}\mathcal{D}_r \cap \mathbb{R}^n$ and consider the projection π_i restricted to $M^{-1}\mathcal{D}_r \cap \mathbb{R}^n$. Since $M \in \mathscr{M}_2$, by [37, Proposition

18] the boundary of $\pi_i(M^{-1}\mathcal{C})$ is contained in $\pi_i(\mathcal{O}_{i-1}(M^{-1}\mathcal{D}_r)\cap M^{-1}\mathcal{C})$ and in particular in $\pi_i(M^{-1}\mathcal{C})$. This implies that $\pi_i(M^{-1}\mathcal{C})$ is closed and so Assertion 1. □

Proof of Assertion 2 of Proposition 4: Let us prove Assertion 2. Let $M \in \mathscr{M}_2$ and let $t \in \mathbb{R}$ lie in the boundary of $\pi_1(M^{-1}\mathcal{C})$. By [37, Lemma 19] the set $\pi_1^{-1}(t) \cap M^{-1}\mathcal{C}$ is finite. Fix $x \in \pi_1^{-1}(t) \cap M^{-1}\mathcal{C}$, and let $p \leq r$ be the rank of $A(x)$. Since x is fixed, the polynomial system $y \mapsto f(A, U, S)$ parametrized by U, S is linear in y and can be written in the form

$$\begin{pmatrix} A(x) \\ U \end{pmatrix} Y(y) = \begin{pmatrix} 0_{m\times(m-r)} \\ S \end{pmatrix} \tag{8}$$

Let B be the matrix on the right side of (8). This system is equivalent to $m - r$ linear systems of equations whose unknowns are the columns of $Y(y)$ and whose constant terms are the columns of B. Now, each of these systems has a solution if and only if, by Rouché-Capelli Theorem [43], each column of B lies in the space spanned by the columns of $A(x)$, that is if and only if the following equality holds:

$$\operatorname{rank}\begin{pmatrix} A(x) \\ U \end{pmatrix} = \operatorname{rank}\begin{pmatrix} A(x) & 0_{m\times(m-r)} \\ U & S \end{pmatrix}.$$

Denote by $r_{x,U}$ the number of rows of U that do not lie in the space spanned by the rows of $A(x)$ and by $r_{x,U,S}$ the number of rows of $[U \mid S]$ that do not lie in the space spanned by the rows of $[A(x) \mid 0]$. Since S is full-rank, one necessarily deduces that for all U, $r_{x,U} \leq r_{x,U,S} = m - r$ (in fact, no line of S is the zero vector). Moreover, since x is fixed, then there exists a non-empty Zariski open set $\mathscr{U}_{\mathcal{C},x}$ such that if $U \in \mathscr{U}_{\mathcal{C},x}$ then $r_{x,U} = m - r$ and

$$\operatorname{rank}\begin{pmatrix} A(x) \\ U \end{pmatrix} = p + r_{x,U} = p + m - r$$

and

$$\operatorname{rank}\begin{pmatrix} A(x) & 0_{m\times(m-r)} \\ U & S \end{pmatrix} = p + r_{x,U,S} = p + m - r,$$

so that the system has at least one solution. One concludes by defining

$$\mathscr{U} = \bigcap_{\mathcal{C}\subset\mathcal{D}_r\cap\mathbb{R}^n} \bigcap_{x\in\pi_1^{-1}(t)\cap\mathcal{C}} \mathscr{U}_{\mathcal{C},x}$$

which is non-empty and Zariski open by the finiteness of the number of connected components of $\mathcal{D}_r \cap \mathbb{R}^n$ and of the set $\pi_1^{-1}(t) \cap \mathcal{C}$. □

7 Practical Experiments

This section reports on practical experiments made with a first implementation of our algorithm. Note that for computing rational parametrizations, we use Gröbner bases and change of ordering algorithms [25, 31]. Our experiments are done using the C library FGb, developed by J.-C. Faugère [23] and interfaced with Maple. The implementation will be freely released as a Maple library and made available at

`http://homepages.laas.fr/henrion/software`

We start by comparing our implementation with implementations of general algorithms based on the critical point method in RAGLIB [52]. Next, we comment the behaviour of our algorithm on special examples that are well-known by the research community working on linear matrices.

7.1 Comparison with RAGLIB

We have generated randomly linear matrices for various values of m and n and run our implementation for different values of r. By randomness of rational numbers we mean that we generate couples of integers chosen with uniform distribution in a fixed interval. Clearly, this would imply that the set of inputs is finite (hence, it is not a Zariski dense set). On the other hand, this does not affect genericity and also the correctness of the algorithm since the requested properties can be checked before its execution.

Our implementation is written in MAPLE. As said above, we use the Gröbner engine FGB for computing in practice rational parametrizations. All computations have been done on an Intel(R) Xeon(R) CPU $E7540@2.00$GHz 256 Gb of RAM. We report in Table 1 numerical data of our tests. For any choice of m, $2 \leq r \leq m-1$ and n, we generate a random dense linear matrix A and we let LowRank run with input (A, r).

(m,r,n)	PPC	LowRank	deg	maxdeg	(m,r,n)	PPC	LowRank	deg	maxdeg
$(3,2,2)$	0.2	6	9	6	$(5,2,3)$	0.9	0.5	0	0
$(3,2,3)$	0.3	7.5	21	12	$(5,2,4)$	1	0.5	0	0
$(3,2,4)$	0.9	9.5	33	12	$(5,2,5)$	1.6	0.5	0	0
$(3,2,5)$	5.1	13.5	39	12	$(5,2,6)$	3	0.6	0	0
$(3,2,6)$	15.5	15	39	12	$(5,2,7)$	4.2	0.7	0	0
$(3,2,7)$	31	16.5	39	12	$(5,2,8)$	8	0.7	0	0
$(3,2,8)$	109	18	39	12	$(5,2,9)$	∞	903	175	175
$(3,2,9)$	230	20	39	12	$(5,3,2)$	0.4	0.5	0	0
$(4,2,2)$	0.2	0.5	0	0	$(5,3,3)$	0.5	0.5	0	0
$(4,2,3)$	0.3	0.5	0	0	$(5,3,4)$	43	22	50	50
$(4,2,4)$	2.2	2.5	20	20	$(5,3,5)$	∞	5963	350	300
$(4,2,5)$	12.2	26	100	80	$(5,4,2)$	0.5	125	25	20
$(4,2,6)$	∞	593	276	176	$(5,4,3)$	10	167	105	80
$(4,2,7)$	∞	6684	532	256	$(5,4,4)$	∞	561	325	220
$(4,2,8)$	∞	42868	818	286	$(5,4,5)$	∞	5574	755	430
$(4,2,9)$	∞	120801	1074	286	$(6,3,3)$	4	1	0	0
$(4,3,3)$	1	8	52	36	$(6,3,4)$	140	1	0	0
$(4,3,4)$	590	18	120	68	$(6,3,5)$	∞	1	0	0
$(4,3,5)$	∞	56	204	84	$(6,3,6)$	∞	2	0	0
$(4,3,6)$	∞	114	264	84	$(6,3,7)$	∞	2	0	0
$(4,3,7)$	∞	124	284	84	$(6,3,8)$	∞	2	0	0
$(4,3,8)$	∞	124	284	84	$(6,4,2)$	0.6	40	0	0
$(4,3,9)$	∞	295	284	84	$(6,4,3)$	1	64	0	0
$(4,3,10)$	∞	303	284	84	$(6,4,4)$	341	300	105	105
$(4,3,11)$	∞	377	284	84	$(6,5,3)$	95	276	186	150
$(5,2,2)$	0.6	0.5	0	0	$(6,5,4)$	∞	8643	726	540

Table 1: Timings and degrees for dense linear matrices

We compare our timings (reported in column "LowRank") with the function PointsPerComponents (column "PPC") of the real algebraic geometry library RAGlib, implemented by the third author [52]. The symbol ∞ means that the no result has been returned after 4 days of computation.

We make the following remarks about Table 1.

1. We first observe that our algorithm is most of the time faster than RAGlib and it allows to tackle examples that are out of reach of RAGlib.

2. The growth in terms of timings with respect to n seems to respect the correspondent growth in terms of degrees of output parametrizations ; in particular note that we have established that for r and m fixed, the sum of the degrees of parametrizations we need to compute stabilizes when n grows. This is observed in practice of course and is reflected in our timings compared to those of RAGlib.

3. Accordingly to the related Multilinear Bézout Bounds computed in section 3.3.1, the degrees of rational parametrizations stabilize when n grows, since when $n > m^2 - r^2$ and the input is generic, LowRank does not compute critical points at first calls. This fact is remarkable, since:

   - a natural geometric invariant associated to $\mathcal{D}_r$, its degree as complex algebraic set, does not depend on the dimension n of the affine section (one can prove easily that generically this degree is given by Thom-Porteous-Giambelli formula, *cf.* [3, Ch. II,§ 4]);
   - an algebraic invariant naturally associated to the output-size (the degree) is constant in n, coherently with the abovementioned geometric invariant.

Finally, we give a final remark on potential *a posteriori* verification of the correctness of the output of LowRank. Deciding whether a finite set, encoded by a rational parametrization, meets every connected component of a given real algebraic set, is a hard problem, far from being solved, both from a theoretical and computational viewpoint. As far as the authors know, there are no symbolic or numerical algorithms able to perform this task. Also, producing such a certificate seems to be hard to imagine, but this was not among the goals of this paper. Anyway LowRank is able to produce a certified correct output when regularity assumptions (that can be checked *a priori*) holds.

7.2 Examples

In this last section, we consider some examples of linear matrices coming from the literature, and we test the behavior of LowRank. We consider examples of symmetric linear matrices since, as observed in Section 1.2, the main motivation for solving the real root finding problem is to obtain dedicated algorithms for spectrahedra and semidefinite programming.

Example 16 (The Cayley cubic) *We consider the* 3×3 *linear matrix*

$$A(x) = \begin{pmatrix} 1 & x_1 & x_2 \\ x_1 & 1 & x_3 \\ x_2 & x_3 & 1 \end{pmatrix}.$$

The real trace of the complex determinantal variety $\mathcal{D}_2 = \left\{x \in \mathbb{C}^3 \;\middle|\; \text{rank } A(x) \leq 2\right\}$ *is shown in Figure 1. The convex region* $\{x \in \mathbb{R}^3 \mid A(x) \succeq 0\}$ *is the Cayley spectrahedron. We run* LowRank *with input* (A, r) *with* $r = 2$ *and* $r = 1$ *(the case* $r = 0$ *is trivial since* $A(x)$ *is always non-zero and hence* $\mathcal{D}_0$ *is empty). In both cases, the algorithm first verifies that the genericity assumptions are satisfied.*

Let us first analyze the case $r = 2$. LowRank *runs* 3 *recursive steps. Its output is a rational parametrization of degree* 14 *with* 12 *real solutions and* 2 *complex solutions. We give below details of each recursive call of* LowRankRec. *At the first, at step 4, a rational parametrization of degree* 5 *is returned, with the following* 5 *real solutions:*

$$\left\{\begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\-1\\-1\end{pmatrix}, \begin{pmatrix}-1\\1\\-1\end{pmatrix}, \begin{pmatrix}-1\\-1\\1\end{pmatrix}, \begin{pmatrix}18.285118452\\164.322822823\\4.552268485\end{pmatrix}\right\}.$$

The coordinates of the fifth point are approximated to 9 *certified digits and such approximation can be computed by isolating the coordinates in intervals of rational numbers as:*

$$\begin{aligned}
x_1 &\in [\tfrac{21081306277346124211}{1152921504606846976}, \tfrac{21081306277346754459}{1152921504606846976}] \approx 18.285118452\\
x_2 &\in [\tfrac{5920353629066611305}{36028797018963968}, \tfrac{23681414516266799197}{144115188075855872}] \approx 164.322822823\\
x_3 &\in [\tfrac{10496816461511385723}{2305843009213693952}, \tfrac{26242041153778660 59}{576460752303423488}] \approx 4.552268485,
\end{aligned}$$

Remark that it also computes the 4 *singular points of* $\mathcal{D}_2$*, where the rank of* A *is* 1. *At the second (resp. third) recursive call, it returns a rational parametrization of degree* 6 *(resp. of degree* 3*) with* 4 *(resp.* 3*) real solutions.*

In the case $r = 1$*, step 4 of* LowRankRec *returns a rational parametrization of degree* 4 *which encodes the* 4 *singular points of* $\mathcal{D}_2 \cap \mathbb{R}^3$*, that is* $\mathcal{D}_1 \cap \mathbb{R}^3$*. At the second and third recursions,* LowRankRec *return empty lists.*

We finally remark that the above results are typical, in the sense that the 4 *singular points contained in* $\mathcal{D}_1 \cap \mathbb{R}^3$ *are always computed at the first recursion step, both in case* $r = 2$ *and* $r = 1$*. Conversely, the coordinates of the other real solutions depend on the choice of random parameters (while their number is constant). Moreover, all computations end after few seconds (*< 5 *sec.).*

Example 17 *Let*

$$A(x) = \begin{pmatrix} a_1 & x_1 & x_2 & x_3\\ x_1 & a_2 & x_3 & x_4\\ x_2 & x_3 & a_3 & x_5\\ x_3 & x_4 & x_5 & a_4 \end{pmatrix},$$

where $x = (x_1, x_2, x_3, x_4, x_5)$ *are variables and* (a_1, a_2, a_3, a_4) *are parameters. We first instantiate* (a_1, a_2, a_3, a_4) *to* $(1, 1, 1, 1)$ *and in this case we obtain that with input* $(A, 2)$ *and* $(A, 3)$*, the genericity assumptions requested by* LowRank *are not satisfied. For* $r = 1$*, these assumptions are satisfied and the algorithm returns a degree* 4 *parametrization, with* 4 *real solutions encoding* $\mathcal{D}_1 \cap \mathbb{R}^5$.

Subsequently, we let (a_1, a_2, a_3, a_4) *vary randomly in* $\mathbb{Q}^4$*. For all random instantiations, we observe that the inputs* $(A, 3), (A, 2)$ *and* $(A, 1)$ *verify the genericity assumptions, and that*

the degrees of the rational parametrizations returned at each recursion step are constant, while the number of real solutions changes with parameters. We summarize our results in Table 2.

	$r = 3$	$r = 2$	$r = 1$
partial degrees	[12 24 24 12 4]	[12 20 8 0 0]	[0 0 0 0 0]
total degree	76	40	0
time (s)	768	21.5	4.6

Table 2: Degrees and timings for Example 17 with generic parameters

Example 18 (The pillow) *Let*

$$A(x) = \begin{pmatrix} 1 & x_1 & 0 & x_1 \\ x_1 & 1 & x_2 & 0 \\ 0 & x_2 & 1 & x_3 \\ x_1 & 0 & x_3 & 1 \end{pmatrix}.$$

The spectrahedron $S = \{x \in \mathbb{R}^3 \mid A(x) \succeq 0\}$ is known as the pillow, see also [12, Section 5.1.1]. It is pictured in Figure 2 with the help of the software POVRAY *(**http://www.povray.org**) implementing the raytracing algorithm.*

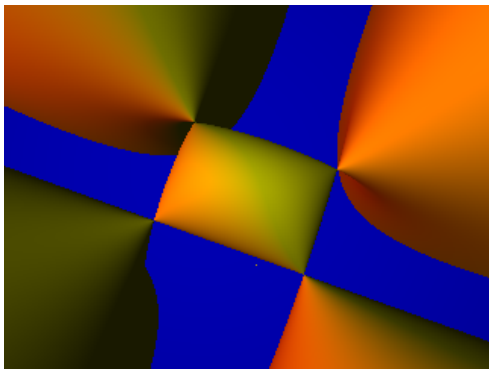

Figure 2: The pillow and its algebraic boundary

The Zariski closure of its boundary is the real trace of the complex hypersurface defined by the vanishing of

$$\det A(x) = 1 - x_3^2 - x_2^2 - 2x_1^2 + x_1^2x_3^2 - 2x_1^2x_2x_3 + x_1^2x_2^2.$$

As clear from Figure 2, the determinantal hypersurface consists in four branches arising from the convex set S.

The boundary of S contains 4 singular points of the determinantal hypersurface, where $A(x)$ has rank 2. Their coordinates can be found by computing a Gröbner basis of the ideal generated by the 3×3 minors of A, which is $\{2x_1^2 - 1, 2x_3^2 - 1, x_2 + x_3\}$. In particular, these four points are contained in the hyperplane $x_2 = -x_3$.

We tested LowRank *with input* $(A, 2)$. *We obtain that at the first recursion, at step 4 a rational parametrization* $q = (q_0, q_1, q_2, q_3, q_4)$ *of degree* 4 *(with only real roots) is computed. By isolating the* 4 *real roots of* q_4 *as in Example 16, one gets the following rational approximations of the singular points:*

$$x_1 \in [-\tfrac{6521908912666475339}{9223372036854775808}, -\tfrac{13043817825332644843}{18446744073709551616}] \approx -\sqrt{2}/2$$
$$x_2 \in [\tfrac{26087635650665343561}{36893488147419103232}, \tfrac{6521908912666428733}{9223372036854775808}] \approx \sqrt{2}/2$$
$$x_3 \in [-\tfrac{6521908912666412349}{9223372036854775808}, -\tfrac{13043817825332731855}{18446744073709551616}] \approx -\sqrt{2}/2.$$

As for Example 16, we observe a typical output in terms of the degree of the rational parametrizations and the number of real solutions. Details are given in Table 3.

	$r = 3$	$r = 2$	$r = 1$
partial degrees	[6 8 4]	[4 0 0]	[0 0 0]
total degree	18	4	0
real solutions	14	4	0
time (s)	< 5	< 5	< 5

Table 3: Degrees and timings for Example 18 for the pillow

References

[1] P.-A. Absil, R. Mahony, R. Sepulchre. Optimization algorithms on matrix manifolds. Princeton University Press, 2008.

[2] M.E. Alonso, E. Becker, M.F. Roy, T. Wörmann. Zeros, multiplicities, and idempotents for zero-dimensional systems. Algorithms in algebraic geometry and applications, pp. 1-15. Birkhäuser, Basel, 1996.

[3] E. Arbarello, J. Harris, M. Cornalba, P. Griffiths. Geometry of Algebraic Curves. Volume I. Grundlehren der Mathematischen Wissenschaften, vol. 267, Springer-Verlag, New York, 1985.

[4] B. Bank, M. Giusti, J. Heintz, G.-M. Mbakop. Polar varieties and efficient real equation solving: the hypersurface case. Journal of Complexity, 13(1):5–27, 1997.

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

[6] B. Bank, M. Giusti, J. Heintz, L.-M. Pardo. Generalized polar varieties and efficient real elimination procedure. Kybernetika, 40(5):519–550, 2004.

[7] B. Bank, M. Giusti, J. Heintz, L.-M. Pardo. Generalized polar varieties: geometry and algorithms. Journal of Complexity, 21(4):377-412, 2005.

[8] B. Bank, M. Giusti, J. Heintz, L. Pardo. Bipolar varieties and real solving of a singular polynomial equation. Jaen Journal of Approximation, 2(1):65–77, 2010.

[9] B. R. Barmish. New tools for robustness of linear systems. Macmillan Publishing Company, New York, 1994.

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

[11] A. Ben-Tal, A. Nemirovski. Lectures on modern convex optimization. SIAM, Philadelphia, 2001.

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

[13] S. P. Boyd, L. El Ghaoui, E. Feron, V. Balakrishnan. Linear matrix inequalities in system and control theory. SIAM, Philadelphia, 1994.

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

[15] E. J. Candès. Mathematics of sparsity (and a few other things). Proceedings of the International Congress of Mathematicians, Seoul, South Korea, 2014.

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

[17] 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.

[18] J. Draisma, J. Rodriguez. Maximum likelihood duality for determinantal varieties. International Mathematics Research Notices, Oxford University Press, 2013.

[19] J. Draisma, E. Horobet, G. Ottaviani, B. Sturmfels, R. R. Thomas. The Euclidean distance degree of an algebraic variety. Foundations of Computational Mathematics, published online January 2015.

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

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

[22] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reductions to zero (F5). In Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC), Lille, France, 2002.

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

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

[25] 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.

[26] 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. In Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC), Munich, Germany, 2010.

[27] J.-C. Faugère, M. Safey El Din, P.-J. Spaenlehauer. Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1): algorithms and complexity. Journal of Symbolic Computation, 46(4):406–437, 2011.

[28] J.-C. Faugère, M. Safey El Din, P.-J. Spaenlehauer. Critical points and Gröbner bases: the unmixed case. In Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC), Grenoble, France, 2012.

[29] 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.

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

[31] J.-C. Faugère, C. Mou. Fast algorithm for change of ordering of zero-dimensional Gröbner bases with sparse multiplication matrices. In Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC), San Jose, USA, 2011.

[32] M. Giusti, G. Lecerf, B. Salvy. A Gröbner-free alternative for polynomial system solving. Journal of Complexity, 17(1):154–211, 2001.

[33] A. Greuet and M. Safey El Din. Probabilistic algorithm for polynomial optimization over a real algebraic set. SIAM Journal on Optimization, 24(3):1313–1343, 2014.

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

[35] B. Bank, M. Giusti, J. Heintz, M. Safey El Din. Intrinsic complexity estimates in polynomial optimization. Journal of Complexity, 30(4), 430-443, 2014.

[36] J. W. Helton, J. Nie. Sufficient and necessary conditions for semidefinite representability of convex hulls and sets. SIAM Journal on Optimization, 20(2):759–791, 2009.

[37] D. Henrion, S. Naldi, M. Safey El Din. Real root finding for determinants of linear matrices. LAAS-CNRS Report 14514, hal-01077888, 2014.

[38] J. Hauenstein, J. Rodriguez, B. Sturmfels. Maximum likelihood for matrices with rank constraints. Journal of Algebraic Statistics, 5(1):18–38, 2014.

[39] Z. Jelonek. Testing sets for properness of polynomial mappings. Mathematische Annalen, 315(1):1–35, 1999.

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

[41] V. Kučera. Discrete linear control: the polynomial approach. John Wiley and Sons, Chichester, UK, 1979.

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

[43] S. Lang. Linear Algebra. Springer-Verlag, New York, 1987

[44] M. Laurent. Sums of squares, moment matrices and optimization over polynomials. Pages 157-270 in M. Putinar, S. Sullivant (Editors). Emerging applications of algebraic geometry, Vol. 149 of IMA Volumes in Mathematics and its Applications, Springer-Verlag, New York, 2009.

[45] A. Logar. A computational proof of the Noether normalization lemma. In Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, pages 259–273, Lecture Notes in Computer Science, 357, Springer, Berlin, 1989.

[46] I. Markovsky. Low rank approximation: algorithms, implementation, applications. Communications and Control Engineering. Springer, 2012.

[47] H. D. Mittelmann. The state-of-the-art in conic optimization software. In Handbook of Semidefinite, Cone and Polynomial Optimization (M. Anjos and J. Lasserre eds), International Series in Operations Research and Management Science, 166, Springer, New York, 2012.

[48] A. Nemirovski. Advances in convex optimization: conic programming. Pages 413-444 in M. Sanz-Sol, J. Soria, J. L. Varona, J. Verdera (Editors). Proceedings of International Congress of Mathematicians, Madrid, Spain, August 2006. Vol. 1, EMS Publishing House, 2007.

[49] G. Ottaviani, P.-J. Spaenlehauer, B. Sturmfels Exact solutions in Structured Low-Rank Approximation. SIAM Journal on Matrix Analysis and Applications, 35(4):1521–1542, 2014.

[50] J. Nie, K. Ranestad, B. Sturmfels. The algebraic degree of semidefinite programming. Mathematical Programming, 122(2):379–405, 2010.

[51] D. Perrin. Algebraic geometry: an introduction. Springer, Berlin, 2008.

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

[53] M. Safey El Din. Finding sampling points on real hypersurfaces is easier in singular situations. In Electronic proceedings of MEGA (Effective Methods in Algebraic Geometry), 2005.

[54] M. Safey El Din, E. Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC), Philadelphia, USA, 2003.

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

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

[57] A. Tarski. A decision method for elementary algebra and geometry. University of California Press, 1951.

[58] J. H. Wilkinson. The algebraic eigenvalue problem. Oxford University Press, UK, 1965.

[59] J. Harris. Algebraic geometry. A first course. Springer, 1992.