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]

October 25, 2017

Abstract

The problem of finding $m \times s$ matrices (with $m \geq s$) of rank r in a real affine subspace of dimension n has many applications in information and systems theory, where low rank is synonymous of structure and parsimony. We design computer algebra algorithms to solve this problem efficiently and exactly: 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 $\binom{n+m(s-r)}{n}$; 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 s, m, n, r be positive integers with $0 \leq r < s \leq m$ and let $A_0, \ldots, A_n$ be $m \times s$ 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.

By abuse of notation, we denote the vector $(A_0, A_1, \ldots, A_n) \in (\mathbb{Q}^{m\times s})^{n+1}$ by A. Given A as above, we consider the following complex 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 algorithm for deciding the emptiness of the real algebraic set $\mathcal{D}_r \cap \mathbb{R}^n$ and, if it is not empty, for computing at least one point in each connected component of $\mathcal{D}_r \cap \mathbb{R}^n$.

Our algorithm relies on a symbolic approach yielding exact output. By this, we mean that our output is an exact encoding of finitely many points whose coordinates are algebraic numbers, is exact since it provides a rational parametrization with coefficients in $\mathbb{Q}$ of those points. This is a vector of univariate polynomials $q = (q_0, q_1, \ldots, q_{n+1}) \in \mathbb{Q}[t]^{n+2}$ such that q_{n+1} is square-free, $q_0 = \frac{\partial q}{\partial t}$ and $\deg(q_i) < \deg(q_{n+1})$ for $1 \leq i \leq n$, and such that the following set

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

is contained in $\mathcal{D}_r$ and contains at least one point in each connected component of $\mathcal{D}_r \cap \mathbb{R}^n$. We give more details on this exact representation below in Section 2.3.

However, the nature of our algorithm is probabilistic, since we allow probabilistic subroutines performing operations on rational parametrizations. Moreover, we use random (i.e. generic) changes of variables to get geometric and algebraic properties of the algebraic sets that are built during the procedure.

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 [56], low rank moment matrices provide guarantees of global optimality of a convex relaxation of a non-convex optimization problem. 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. [62], [50] or [24] and the references therein. In these cases, the given affine subspace lies in the linear space of symmetric (or more structured) matrices, while in this paper we address the problem from a more general point of view.

Example 1 *In [53] the authors study distortion varieties, special algebraic varieties arising from computer vision. These have determinantal structure. For instance, equations for the distortion variety in [53, Ex. 1.1] are given by the* 2×2 *minors of the* 2×6 *matrix*

$$A(x_1, \ldots, x_{11}) = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 & x_{10} & x_6 & x_{11} \end{pmatrix}.$$

The matrix A defines a linear space of co-dimension 1 in the space of 2×6 matrices (indeed the $(1,6)-$entry equals the $(2,5)-$entry), and we are interested in the locus of rank-1 matrices of this form. The real points of this variety can be sampled with the algorithm developed in this paper, since regularity assumptions needed by the algorithm (and which are defined in Section 2.4) are satisfied by this example.

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. [20]. Finally, linear matrices and their loci of rank defects are the object of the so-called low rank approximation problem, see e.g. [66].

Also, note that grabbing real sample points in real algebraic sets defined by rank defects of matrices with polynomial entries finds also applications in control theory and medical imagery [16, 17].

In our paper, we are not after trying to solve approximately large-scale problem instances 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.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.

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 $\binom{n+m(s-r)}{n}^3$. Hence, for particular sub-classes of the problem, for example when the maximum dimension of the matrix is fixed, the multilinear bounds (and hence the complexity) are polynomial in the number of variables.

1.3 State of the art

We distinguish in the state-of-the-art three subproblems. The first one is on computing sample points in each connected component of real algebraic sets, hence without taking care of the determinantal structure we consider here. Next, we review on previous work taking care of the determinantal structure but in the context of zero-dimensional algebraic sets. Finally, we consider real algebraic sets defined by rank constraints on matrices with polynomial entries.

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

algebraic geometry. Since one typically deals with positive dimensional solution sets, one possible approach is to design algorithms computing a finite set intersecting each connected component of the real solution set under study. While the complexity of the first algorithm solving this problem [80] was not elementary recursive, Collins designed in [21] 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 [13, 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 [44] the critical point method which culminates with the algorithms in [13, Chap. 13] (see also references therein) running in time singly exponential in the number of variables n. It is based on the critical point method. The algorithms in [6, 7, 8, 9, 10, 73, 74] 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 [11, 43].

When one is only interested in computing generic points in algebraic varieties defined by rank constraints on matrices with polynomial entries by taking care of the determinantal structure, one can use dedicated algorithms in e.g. [5] based on variants of the geometric resolution algorithm [41] or Gröbner bases [31, 34]. Observe that, as it is, this is not sufficient to be applied to the problem of real root finding in positive dimensional real algebraic sets.

In the context of real algebraic sets defined by the vanishing of $(r+1, r+1)$ minors of $m \times s$ matrices with linear entries, which corresponds to the problem stated in Section 1.1, the following cases have been already treated:

- $m = s$ and $r = s - 1$: in [47], we designed a dedicated algorithm for computing sample points in each connected component of the studied real algebraic set under some genericity assumption on the input matrix pencil;
- $m = s$ and the considered matrix is *symmetric*: we designed in [49] a dedicated algorithm for this situation without any other constraint on r than $r \leq m-1$, again under some genericity assumption on the input matrix pencil. In [48], we also tackle the situation where the linear matrix is Hankel.

Observe that the cases $m \neq s$ and arbitrary r were pending. In the current paper, we deal with the case $m \neq s$ (assuming without loss of generality that $m \geq s$) and arbitrary $r \leq m - 1$. This paper builds on the previous work [47]: the spirit and the statement of our main result is rather close to this previous work but many of the techniques used in [47] cannot be applied *mutatis mutandis* to the more general setting we consider here and need to be adapted and generalized.

1.4 Paper outline and main results

The algorithm described in this paper, with input a $m \times s$ linear matrix $A(x) = A_0 + x_1 A_1 + \ldots + x_n A_n$, with $m \geq s$, $A_i \in \mathbb{Q}^{m \times s}$, $i = 0, 1, \ldots, n$, and an integer $r \leq s-1$, computes a rational parametrization of a finite set intersecting each connected component of $\mathcal{D}_r \cap \mathbb{R}^n$. The design of the algorithm is intended 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 the same problem in a more general setting.

Since algebraic sets defined by minors of fixed size of a polynomial matrix are generically singular, the input of our algorithm does not satisfy regularity properties. Hence, the first step is to generate a second algebraic set $\mathcal{V}_r$, defined by quadratic equations $A(x)Y(y) = 0$, where $Y(y)$ is a rectangular matrix whose columns generate the kernel of $A(x)$. The set we have obtained is a lifting of $\mathcal{D}_r$, which is traditionally called an *incidence variety*.

We investigate properties of this incidence variety, proving that unlike $\mathcal{D}_r$, the lifted set $\mathcal{V}_r$ is regular (smooth and equidimensional) when the input matrices $A = (A_0, A_1, \ldots, A_n)$ lie outside a given algebraic hypersurface in $(\mathbb{Q}^{m \times s})^{n+1}$. We show that our problem can be reduced to compute finitely many critical points of the restriction of a general linear projection to this lifted set. The system that defines these critical points has a special sparsity structure, namely it is bilinear in three groups of variables (the variables x describing $\mathcal{D}_r$, the variables y encoding the kernel, and Lagrange multipliers z). Using the symbolic homotopy algorithm in [76] (which builts upon the one in [52]), 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 [76], we show that the complexity is essentially quadratic on δ. This bound is dominated by $\binom{n+m(s-r)}{n}^3$. Note that this complexity estimate does not take into account the cost of checking that the genericity assumption on the input is satisfied, which we suppose to be true.

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 algorithm described here works under genericity assumptions on the input matrices $A_0, A_1, \ldots, A_n$: we prove that if these assumptions – which can be checked algorithmically – hold, then the output rational parametrization represents a finite set contained in $\mathcal{D}_r$ containing at least one point in each connected component of $\mathcal{D}_r \cap \mathbb{R}^n$. Finally, we prove that the genericity assumptions are satisfied in a dense open subset of the parameter space $(\mathbb{Q}^{m \times s})^{n+1}$ of all inputs. Moreover, we highlight that, contrarily to our previous contribution [47] concerning determinantal hypersurfaces, in this paper we explicitely describe the dependencies between the choice of parameters during the main algorithm. Indeed, often, the admissible parameters form a dense open set which depend on previous data.

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 describe the input/output data representation of our algo-

rithm.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 incidence variety, see Section 4, dimension of a variety built using so-called Lagrange multipliers, 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

2.1 Basic notions

We start by fixing some notation and recall basic notions ; more details about these notions can be found in [22, 25, 78].

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) defined over $\mathbb{Q}$ 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 $\mathbb{I}_n$. 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. The transpose of a matrix M is denoted by M^T.

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 codimension 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 $f\colon \mathbb{C}^n \to \mathbb{C}^q$ generate a radical ideal, and let $\mathcal{V} = \mathcal{Z}(f)$ be equidimensional of dimension d. Let $g\colon \mathbb{C}^n \to \mathbb{C}^p$. A point $x \in \operatorname{reg} \mathcal{V}$ is a critical point of the restriction of g to $\mathcal{V}$ if the minors of size $n-d+p$ of the extended Jacobian matrix $D(f,g)$ vanish at x. The Zariski-closure of the set of critical points is denoted by $\operatorname{crit}(g, \mathcal{V})$. 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 $\operatorname{crit}(\pi_1, \mathcal{V})$ is equivalently defined by the zero set of the polynomials in f and the maximal minors of $D_1 f$. The set $\operatorname{crit}(\pi_1, \mathcal{V})$ is also called a *polar variety* when $\mathcal{V}$ is smooth, see [9].

2.2 Incidence variety

Let $A = (A_0, A_1, \ldots, A_n)$ be $m \times s$ matrices ($m \geq s$) with entries in $\mathbb{Q}$, and $A(x) = A_0 + x_1 A_1 + \cdots + x_n A_n$ the associated linear matrix. If $x \in \mathcal{D}_r = \{x \in \mathbb{C}^n : \operatorname{rank} A(x) \leq r\}$, the right kernel of $A(x)$ is a subspace of dimension $\geq s-r$ in $\mathbb{C}^s$ by linear algebra.

We introduce $s(s-r)$ variables $y = (y_{1,1}, \ldots, y_{s,s-r})$, stored in a $s \times (s-r)$ linear matrix

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

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

$$\mathcal{V}_r(A,U) \coloneqq \big\{(x,y) \in \mathbb{C}^n \times \mathbb{C}^{s(s-r)} : A(x)Y(y) = 0, UY(y) - \mathbb{I}_{s-r} = 0\big\}. \tag{2}$$

Remark that the matrix $Y(y)$ has full rank $s-r$ if and only if there exists $U \in \mathbb{Q}^{(s-r)\times s}$ of full rank such that $UY(y) - \mathbb{I}_{s-r} = 0$. For $A \in (\mathbb{C}^{m\times s})^{n+1}$, $U = (u_{i,j})_{1\leq i\leq s-r, 1\leq j\leq s} \in \mathbb{Q}^{(s-r)\times s}$, and $c \coloneqq (m+s-r)(s-r)$, define

$$\begin{array}{rccc} f(A,U):\ \mathbb{C}^{n+s(s-r)} & \to & \mathbb{C}^c \\ (x,y) & \mapsto & (A(x)Y(y),\ UY(y) - \mathbb{I}_{s-r}) \end{array}.$$

Remark that $\mathcal{V}_r(A,U) = \mathcal{Z}(f(A,U))$ and that the projection of $\mathcal{V}_r(A,U)$ over the $x-$space is contained in the determinantal variety $\mathcal{D}_r$, by definition. We denote this projection map by

$$\begin{array}{rccc} \Pi_X:\ \mathbb{C}^{n+s(s-r)} & \to & \mathbb{C}^n \\ (x,y) & \mapsto & x \end{array}$$

We will prove that up to genericity assumptions on A and U, the algebraic variety $\mathcal{V}_r(A,U)$ is equidimensional and smooth. When the couple (A,U) is clear from the context, we will denote $f(A,U)$ by f.

2.3 Data representation

We briefly recall the representation of data in our algorithm.

The input is a $m \times s$ linear matrix $A(x) = A_0 + x_1 A_1 + \cdots + x_n A_n$, with $m \geq s$, encoded by the vector of defining matrices $A = (A_0, A_1, \ldots, A_n)$, with coefficients in $\mathbb{Q}$, and an integer r such that $r \leq s - 1$. The vector A is understood as a point in $(\mathbb{Q}^{m \times s})^{n+1}$.

The output is a finite set sampling the connected components 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, represented by a rational parametrization $q = (q_0, q_1, \ldots, q_n, q_{n+1}) \in \mathbb{Q}[t]^{n+2}$, that is with the representation as in (1). Here q_{n+1} is square-free ; moreover q_0, q_{n+1} are coprime (i.e. their greatest common divisor is constant) and the degrees of $q_0, \ldots, q_n$ are dominated by the one of q_{n+1}.

Observe that $\mathcal{Z}$ is in one-to-one correspondence with the roots of q_{n+1}. This encoding allows to reduce the original question to a univariate real root isolation problem.

Such an encoding for finite algebraic sets goes back to the work of Macaulay and Kronecker [54, 61] and extensively used and developed for computer algebra methods for solving polynomial systems (see e.g. [2, 37, 38, 40, 59, 71]). Also, for a better control of the size of the coefficients in the output it is often better to choose $q_0 = \frac{\partial q_{n+1}}{\partial t}$ (see e.g. [77]).

2.4 Genericity assumptions

Our algorithm works under some assumptions on the input A. We denote these assumptions with the letters G_1 and G_2. We will prove below in Section 3 that Assumptions G_1 and G_2 are generic. We recall that the parameter r is fixed and it holds $0 \leq r < s \leq m$.

Property G_1. A $m \times s$ linear matrix A satisfies G_1 if, for all $0 \leq p \leq r$, $\mathcal{D}_p \subset \mathbb{C}^n$ is either empty or $n - (m-p)(s-p)$-equidimensional, $\mathrm{sing}(\mathcal{D}_p) = \mathcal{D}_{p-1}$ and the ideal generated by the $(p+1, p+1)$ minors of $A(x)$ is radical.

Our algorithm takes as input a linear matrix $A(x)$ assuming that A satisfies G_1; we will prove that G_1 holds generically in the sequel. The second property, which we often refer to as a regularity property, is defined for any polynomial system.

Property G_2. A polynomial sequence $h = (h_1, \ldots, h_k) \in \mathbb{Q}[x_1, \ldots, x_n]^k$ satisfies G_2 if

- the ideal $\langle h \rangle$ is a radical ideal of co-dimension k, and
- the algebraic set $\mathcal{Z}(h) \subset \mathbb{C}^n$ is either empty or smooth and equidimensional.

3 Algorithm: description, correctness, complexity

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

3.1 Formal description

The input of LowRank is a couple (A, r), where A is a tuple of $n+1$ matrices $A_0, A_1, \ldots, A_n$, of size $m \times s$ ($m \geq s$), with entries in $\mathbb{Q}$, and $r \leq s-1$ 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 $\{x \in \mathbb{R}^n : \operatorname{rank} A(x) \leq r\}$ as described in Section 2.3.

3.1.1 Notation

Recall that given $A \in (\mathbb{C}^{m\times s})^{n+1}$ and $U \in \mathbb{C}^{(s-r)\times s}$, the polynomial system $f(A, U)$ (of cardinality $c = (m+s-r)(s-r)$) and its zero locus $\mathcal{V}_r(A, U)$ have been defined in Section 2.2.

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 $A = A \circ \mathbb{I}_n$. For $M \in \mathrm{GL}_n(\mathbb{C})$, and for all $A \in (\mathbb{C}^{m\times s})^{n+1}, U \in \mathbb{C}^{(s-r)\times s}$, we consequently denote by $f(A \circ M, U)$ the polynomial system $f(A, U)$ applied to $(M\,x, y)$, and by $\mathcal{V}_r(A \circ M, U) = \mathcal{Z}(f(A \circ M, U))$.

Fibers. Given $w \in \mathbb{C}^n$, we introduce the notation π_w for the map $\pi_w : \mathbb{C}^n \to \mathbb{C}$, $\pi_w(x) = w^T x$, and $\Pi_w : \mathbb{C}^{n+s(s-r)} \to \mathbb{C}$, $\Pi_w(x, y) = w^T x$, that is $\Pi_w = \pi_w \circ \Pi_X$. For $w \in \mathbb{C}^n$ and $t \in \mathbb{C}$, we define

$$\begin{array}{rccl} f_{w,t}: & \mathbb{C}^{n+s(s-r)} & \to & \mathbb{C}^{c+1} \\ & (x, y) & \mapsto & (f(A, U),\ \Pi_w(x, y) - t) \end{array}$$

and denote by $\mathcal{V}_{r,w,t}(A, U) = \mathcal{Z}(f_{w,t}) \subset \mathbb{C}^{n+s(s-r)}$ the section of $\mathcal{V}_r$ with the linear space defined by $\Pi_w(x, y) - t = 0$. When parameters are clear from the context, we use the shorter notation $\mathcal{V}_{r,w,t}$.

For $A \in (\mathbb{C}^{m\times s})^{n+1}$, and $w \in (\mathbb{C} \setminus \{0\})^n$ we denote by $A\big|_{w,t} \in (\mathbb{C}^{m\times s})^n$ the linear matrix obtained by eliminating one variable (up to renaming variable, x_1) from A using the affine equation $w^t\ x - t = 0$.

Lagrange systems. Given $w \in \mathbb{C}^n$, we define

$$\begin{array}{rccl} \ell(A, U, w): & \mathbb{C}^{n+s(s-r)+c} & \to & \mathbb{C}^{n+s(s-r)+c} \\ & (x, y, z) & \mapsto & (f(A, U), z^T Df - (w, 0)^T) \end{array}$$

where $z = (z_1, \ldots, z_c)$ is the column vector of Lagrange multipliers and $(w, 0) \in \mathbb{C}^{n+s(s-r)}$. Let $\mathcal{Z}(A, U, w) = \mathcal{Z}(\ell(A, U, w)) \subset \mathbb{C}^{n+s(s-r)+c}$.

3.1.2 Subroutines

The algorithm LowRank uses different subroutines, described as follows.

IsReg: inputs parameters A, U and outputs true if A satisfies G_1 and $f(A, U)$ satisfies G_2, `false` otherwise;

RatPar: inputs a polynomial system f; returns either the empty list if $\mathcal{Z}(f) = \emptyset$, or an error message if $\mathcal{Z}(f)$ is not zero-dimensional, otherwise a rational parametrization of $\mathcal{Z}(f)$;

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 $\{(t, x) : x \in \mathcal{Z}\}$;

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

This is the formal description of the algorithm. The main routine LowRank calls the recursive routine LowRankRec; the recursion is on the number of variables of the $m \times s$ linear matrix A (which is always denoted by n).

Algorithm LowRank(A, r)**:**

1. Choose $U \in \mathbb{Q}^{(s-r)\times s}$
2. If IsReg$(A, U) =$ `false` then return('error: input data not generic')
3. return LowRankRec(A, U, r)

Algorithm LowRankRec(A, U, r)**:**

4. If $n \leq (m-r)(s-r)$ then return(RatPar$(\mathcal{D}_r)$)
5. Choose $w \in \mathbb{Q}^n \setminus \{0\}$, P = Project(RatPar$(\ell(A, U, w)), x)$
6. Choose $t \in \mathbb{Q}$, Q = Lift(LowRankRec$(A\big|_{w,t}, U, r), t)$
7. return Union(Q, P).

3.2 Correctness

We start by stating intermediate results which will be used to prove the correctness of the algorithm. The proof of the first result below is given in Section 4.

Proposition 2 *Let $m, s, n, r \in \mathbb{N}$, with $0 \leq r < s \leq m$. The following holds.*

1. *There exists a non-empty Zariski open set $\mathscr{A} \subset (\mathbb{C}^{m\times s})^{n+1}$ such that for $A \in \mathscr{A}$, A satisfies Property G_1.*
2. *Let A satisfy G_1. There exists a non-empty Zariski open set $\mathscr{U}_A \subset \mathbb{C}^{(s-r)\times s}$ such that, for $U \in \mathscr{U}_A$, the following holds:*

(a) *$f(A,U)$ satisfies Property G_2;*

(b) *letting $\mathcal{N}_r(A,U)$ be the Zariski closure of $\mathcal{D}_r - \Pi_X(\mathcal{V}_r(A,U))$ and Z an irreducible component of $\mathcal{D}_p$ for $0 \leq p \leq r$, $Z \cap \mathcal{N}_r(A,U)$ has co-dimension at least 1 in Z.*

3. *Let $w \in \mathbb{Q}^n \setminus \{0\}$. There exists a non-empty Zariski open set $\mathscr{T}_A \subset \mathbb{C}$ such that if $t \in \mathscr{T}_A \cap \mathbb{Q}$, then $A\big|_{w,t}$ satisfies Property G_1.*

The second result is proved in Section 5.

Proposition 3 *Let A be in the non-empty Zariski open set $\mathscr{A} \subset (\mathbb{C}^{m\times s})^{n+1}$ and U in the non-empty Zariski open set $\mathscr{U}_A \subset \mathbb{C}^{(s-r)\times s}$ defined in Proposition 2. There exists a non-empty Zariski open set $\mathscr{W}_{A,U} \subset \mathbb{C}^n$ such that for $w \in \mathscr{W}_{A,U} \cap \mathbb{Q}^n$ the following holds.*

1. *$\mathcal{Z}(A,U,w)$ is finite and $\ell(A,U,w)$ satisfies Property G_2;*
2. *the projection of $\mathcal{Z}(A,U,w)$ on (x,y) contains the set of critical points of the restriction of $\Pi_w : (x,y) \to w^T x$ to $\mathcal{V}_r$.*

The following proposition will be proved in Section 6.

Proposition 4 *Let $\mathscr{A} \subset (\mathbb{C}^{m\times s})^{n+1}$ and $\mathscr{U}_A \subset \mathbb{C}^{(s-r)\times s}$ be the non-empty Zariski open sets, and let $\mathcal{N}_r(A,U) \subset \mathcal{D}_r$ be the Zariski closed set, defined in Proposition 2. Let $A \in \mathscr{A}$ and $U \in \mathscr{U}_A$. Let $\mathcal{C} \subset \mathbb{R}^n$ be a connected component of $\mathcal{D}_r \cap \mathbb{R}^n$.*

There exists a non-empty Zariski open set $\mathscr{W}'_{A,U} \subset \mathbb{C}^n$ such that, for $w \in \mathscr{W}'_{A,U} \cap \mathbb{Q}^n$, the following holds:

1. *$\pi_w(\mathcal{C})$ is closed*
2. *for $t \in \mathbb{R}$ in the boundary of $\pi_w(\mathcal{C})$, there exists (x,y,z) in $\mathcal{Z}(A,U,w)$ such that $\Pi_w(x,y) = t$ and $x \notin \mathcal{N}_r(A,U)$.*

Observe that in the above statements, the defined non-empty Zariski open sets (except for the set $\mathscr{A}$) have subscripts indicating which data they depend on. Hence, starting with A satisfying G_1, we highlight the following facts:

- the non-empty Zariski open set $\mathscr{U}_A$ (Proposition 2) depends on A;
- the non-empty Zariski open sets $\mathscr{W}_{A,U}$ (Proposition 3) and $\mathscr{W}'_{A,U}$ (Proposition 4) depend on A and U.

Hypothesis H_1. In the sequel, A (resp. U) is assumed to belong to the non-empty Zariski open set $\mathscr{A}$ (resp. $\mathscr{U}_A$) defined in Proposition 2.

One also has to ensure that the parameters $w \in \mathbb{Q}^n$ and $t \in \mathbb{Q}$ chosen, respectively, at steps 5 and 6 belong to the non-empty Zariski open sets defined in Proposition 3 and 4 at each call of LowRankRec. The choices of random parameters can be stored in an array

$$\left((w^{(n)}, t^{(n)}), \ldots, (w^{((m-r)(s-r))}, t^{((m-r)(s-r))})\right) \tag{3}$$

where the superscript represents the number of variables at the given recursion step (hence n here is the number of variables of A at the input of LowRank). We also denote by $\mathscr{T}^{(j)}$, $\mathscr{W}^{(j)}$ and $\mathscr{W}^{(j)'}$ the non-empty Zariski open sets defined by Propositions 2, 3 and 4, at the $(n-j+1)-$th recursion call (here we avoid the dependency on the Zariski open sets).

Hypothesis H_2. Given A and U satisfying H_1, the parameters (3) satisfy:

- $w^{(j)} \in \mathscr{W}^{(j)} \cap \mathscr{W}^{(j)'} \cap \mathbb{Q}^n \setminus \{0\}$ for $j = (m-r)(s-r), \ldots, n$;
- $t^{(j)} \in \mathscr{T}^{(j)} \cap \mathbb{Q}$ for $j = (m-r)(s-r), \ldots, n$.

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 $n \leq (m-r)(s-r)$. Since H_1 holds, then the variety $\mathcal{D}_r$ is empty or finite. Hence the algorithm returns the correct output, that is either the empty list or a rational parametrization of the finite set $\mathcal{V}_r$. Thereafter, we proceed by induction on n.

Let $n > (m-r)(s-r)$ and suppose that for any $(n-1)-$variate linear matrix, algorithm LowRank returns the expected output when H_1 and H_2 hold, namely one point per connected component of $\mathcal{D}_r \cap \mathbb{R}^n$. Let A be a $n-$variate $m \times s$ linear matrix, let r be an integer such that $0 \leq r \leq s-1$ and let $\mathcal{C}$ be a connected component of $\mathcal{D}_r \cap \mathbb{R}^n$. Let U be the matrix chosen at Step 1 of LowRank. Let $w \in \mathbb{Q}^n$ be the vector chosen at Step 5 of LowRankRec with input A, U, and r. Consider the projection $\pi_w \colon (x_1, \ldots, x_n) \to w^T x$ restricted to $\mathcal{V}_r(A, U)$. Since Property $\mathsf{H}_1, \mathsf{H}_2$ hold, by Proposition 4, $\pi_w(\mathcal{C})$ is closed, and so either $\pi_w(\mathcal{C}) = \mathbb{R}$ or $\pi_w(\mathcal{C}) \subsetneq \mathbb{R}$ 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 $\mathcal{C}$. This is proved next.

First case. Suppose first that $\pi_w(\mathcal{C}) = \mathbb{R}$. In particular, for $t \in \mathbb{Q}$ chosen at Step 6 of LowRankRec with input A, U, r, the set $\pi_w^{-1}(t)$ intersects $\mathcal{C}$, so $\pi_w^{-1}(t) \cap \mathcal{C} \neq \emptyset$. Let $A\big|_{w,t}$ be the $(n-1)-$variate $m \times s$ linear matrix obtained from A by substituting $x_1 = (1/w_1)(t - \sum_{j=2}^n w_j x_j)$ obtained from the linear constraint $w^T x = t$ (indeed, since $w \neq 0$, one can suppose $w_1 \neq 0$ up to permutation of indices). Remark that $\pi_w^{-1}(t) \cap \mathcal{C}$ is the union of some connected components of the determinantal variety $\mathcal{D}_r^{(n-1)} \cap \mathbb{R}^{n-1} = \{x \in \mathbb{R}^{n-1} : \operatorname{rank} A\big|_{w,t} \leq r\}$. Since H_1 holds, then $A\big|_{w,t}$ satisfies G_1; we deduce by the induction hypothesis (since $A\big|_{w,t}$ is $(n-1)-$variate) that 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 $\mathcal{C}$.

Second case. Suppose now that $\pi_w(\mathcal{C}) \neq \mathbb{R}$. By Proposition 4, $\pi_w(\mathcal{C})$ is closed. Since $\mathcal{C}$ is connected, $\pi_w(\mathcal{C})$ is a closed interval, and since $\pi_w(\mathcal{C}) \neq \mathbb{R}$ there exists t in the boundary of

$\pi_w(\mathcal{C})$ such that $\pi_w(\mathcal{C}) \subset [t, +\infty)$ or $\pi_w(\mathcal{C}) \subset (-\infty, t]$. Suppose without loss of generality that $\pi_w(\mathcal{C}) \subset [t, +\infty)$, so that t is the minimum value attained by π_w on $\mathcal{C}$.

By Proposition 4, there exist $x_2, \ldots, x_n$ in $\mathbb{R}$, $y \in \mathbb{C}^{s(s-r)}$ and $z \in \mathbb{C}^c$ such that, for $x = (t, x_2, \ldots, x_n)$, it holds that $(x, y, z) \in \mathcal{Z}(A, U, w)$, and $x \notin \mathcal{N}_r(A, U)$. Then, we conclude that the point $x \in \mathcal{C}$ appears among the solutions of the rational parametrization P obtained at Step 5 of LowRankRec. □

3.3 Complexity analysis

In this section we provide an analysis of the complexity of algorithm LowRank. We also give bounds for the maximum number of complex solutions computed by LowRank. We suppose that A satisfies Property G_1 and that $f(A, U)$ satisfies Property G_2. Recall that the complexity of checking these properties is not evaluated here.

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 rely on routines described in [76], 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 [69].

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 $n = (m-r)(s-r)$) or the Lagrange system $\ell(A \circ M, U, S, v)$ (if $n > (m-r)(s-r)$). 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 $m \times s$ linear matrix, $0 \leq r < s \leq m$ and let U and w be respectively the parameters chosen at step 1 of* LowRank *and at step 5 of* LowRankRec. *Suppose that H_1 and H_2 hold. Then:*

1. *if $n = (m-r)(s-r)$, the degree of the output of* RatPar *at step 4, is bounded from above by $\binom{m(s-r)}{(m-r)(s-r)}$;*
2. *if $n > (m-r)(s-r)$, the degree of the output of* RatPar *at step 5, with input $\ell(A, U, w)$, is bounded from above by*

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

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

Proof of Assertion 1: If $n = (m-r)(s-r)$, since H_1 holds, the dimension of $\mathcal{D}_r$ is zero. Consequently, the degree of the rational parametrization returned by RatPar is the degree of $\mathcal{D}_r$. We bound this degree by the degree of $\mathcal{V}_r$, which is a finite set by Proposition 2 (indeed, in the zero-dimensional case, the set $\mathcal{N}_r(A,U)$ is empty). Since the entries of $f(A,U)$ have a natural bilinear structure in x, y, one takes advantage in using the Multilinear Bézout bound (see [79] or [75, Chapter 11]) to bound the degree of the set it defines.

From $UY(y) - \mathbb{I}_{s-r}$ one can eliminate $(s-r)^2$ variables $y_{i,j}$. Indeed, recall that U has full rank $s-r$. Without loss of generality, we suppose that the last $s-r$ columns of U are linearly independent, and hence we eliminate the variables $y_{i,j}$ corresponding to the last $s-r$ rows of $Y(y)$. Abusing notation, we denote by the same symbol $f \subset \mathbb{Q}[x, y_{1,1}, \ldots, y_{r,s-r}]$ the polynomial system obtained after this elimination. It is constituted by $m(s-r)$ polynomials of multidegree bounded by $(1,1)$ with respect to $x = (x_1, \ldots, x_n)$ and $y = (y_{1,1}, \ldots, y_{r,s-r})$.

By the Multilinear Bézout theorem [75, Prop. I.1], $\deg \mathcal{Z}(f)$ is bounded by the sum of the coefficients of

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

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

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

- $m(s-r)$ polynomials of multidegree bounded by $(1,1,0)$;
- $n-1$ polynomials of multidegree bounded by $(0,1,1)$;
- $r(s-r)$ 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) satisfies G_2. As above, $\deg \mathcal{Z}(f,g,h)$ is bounded by the sum of the coefficients of

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

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 $s_x^n s_y^{r(s-r)} s_z^{m(s-r)-1}$ in the expansion

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

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

Proposition 6 implies straightforwardly the following estimate.

Corollary 7 *Suppose that the hypothesis of Proposition 6 are satisfied. Then* LowRank *returns a rational parametrization whose degree is less than or equal to*

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

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

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

Lemma 8 *For all m,s,n,r, with $r<s\leq m$, $\delta(m,s,n,r)\leq \binom{n+m(s-r)}{n}^3$.*

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

3.3.2 Complexity of RatPar

The computation of the rational parametrization by the subroutine RatPar is done via the symbolic homotopy algorithm [76]. In this section, we analyze the complexity of the algorithm in [76] for our special case.

We suppose that $n>(m-r)(s-r)$ and that the input of RatPar is the equivalent Lagrange system $\ell=\ell(A,U,w)\in\mathbb{Q}[x,y,z]^{n-1+(m+r)(s-r)}$ built in the proof of Assertion 2 of Proposition 6. First, the strategy consists in building a second polynomial system $\tilde{\ell}\subset\mathbb{Q}[x,y,z]$, such that:

- the length of $\tilde{\ell}$ equals that of ℓ, that is $=n-1+(m+r)(s-r)$;
- for $i=1,\ldots,n-1+(m+r)(s-r)$, the support of $\tilde{\ell}_i$ equals that of ℓ_i;
- the solutions of $\tilde{\ell}$ can be computed efficiently (see below).

Indeed, 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 $\Delta_1 = \{1, x_i, y_j, x_i y_j : 1 \leq i \leq n, 1 \leq j \leq r(s-r)\}$, 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, $1 \leq i \leq m(s-r)$. Hence we generate two linear forms $g_{i,1} \in \mathbb{Q}[x]$ and $g_{i,2} \in \mathbb{Q}[y]$ and we define $\tilde{\ell}_i(x,y) = g_{i,1}(x)g_{i,2}(y)$. We equivalently generate polynomials $\tilde{\ell}_j(y,z) = g_{j,1}(y)g_{j,2}(z)$, $m(s-r)+1 \leq j \leq m(s-r)+n-1$ and $\tilde{\ell}_k(x,z) = g_{k,1}(x)g_{k,2}(z)$, $m(s-r)+n \leq k \leq n-1+(m+r)(s-r)$.

We deduce straightforwardly that $\tilde{\ell}$ satisfies the above properties. Indeed, the set $\mathcal{Z}(\tilde{\ell})$ can be computed by solving systems of linear equations. When the affine polynomials $g_{i,1}, g_{i,2}, 1 \leq i \leq n-1+(m+r)(s-r)$, are chosen generically, the number of linear systems to be solved equals the multilinear Bézout bound $\delta(m,s,n,r)$, computed in Proposition 6. Hence the complexity of solving the starting system is in $\mathcal{O}((n+(m+r)(s-r))^{\omega}\delta(m,s,n,r))$, where ω is the exponent of linear algebra.

In [76], the authors build a homotopy path between ℓ and $\tilde{\ell}$, such as

$$t\ell + (1-t)\tilde{\ell} \subset \mathbb{Q}[x,y,z,t] \tag{4}$$

where t is a new variable. The system (4) defines a $1-$dimensional algebraic set, that is a curve. We deduce by [76, Theorem 1, Corollary 2 and Proposition 5] that, if the solutions of $\tilde{\ell}$ are known, one can compute a rational parametrization of the solution set of system (4) within $\mathcal{O}^{\sim}((\tilde{n}N\log Q + \tilde{n}^3)dd')$ arithmetic operations over $\mathbb{Q}$, where:

- $\tilde{n}$ is the number of variables in ℓ;
- $N = m(s-r)\#\Delta_1 + (n-1)\#\Delta_2 + r(s-r)\#\Delta_3$ (# 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 $\mathcal{Z}(t\ell + (1-t)\tilde{\ell})$;

Suppose the following preliminary lemma, whose proof is given in Appendix A.

Lemma 9 *Let $\mathcal{F}_{m,s,n,r}$ and $\delta(m,s,n,r)$ be the set and the bound defined in Proposition 6, and suppose $\mathcal{F}_{m,s,n,r} \neq \emptyset$. Then the degree of $\mathcal{Z}(t\ell + (1-t)\tilde{\ell})$ is in*

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

We can now state the main result of this paragraph.

Theorem 10 *Let $n > (m-r)(s-r)$. Let A be a $n-$variate $m \times s$ linear matrix, $0 \leq r < s \leq m$ and let U be the matrix chosen in step 1 of* LowRank*. Let $\delta = \delta(m,s,n,r)$ be the bound defined in Proposition 6. Then,* RatPar *returns a rational parametrization within*

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

arithmetic operations.

Proof : Following the notation introduced above, $\tilde{n} = n - 1 + (m + r)(s - r)$. the bound for d is δ and is given in Proposition 6 and a bound for d' is given in Lemma 9, and is in $\mathcal{O}^{\sim}(\tilde{n}^2\delta)$. Moreover, $N \in O(mnr(s-r)^2)$, and hence $N \in O(\tilde{n}^3)$. The proof follows from [76, Proposition 5], since the maximum diameter of $\Delta_1, \Delta_2, \Delta_3$ is bounded above by $\tilde{n}$, that is $Q \leq \tilde{n}$ in the notation above. □

3.3.3 Complexity of subroutines

For these complexity bounds, we refer to those given in [69, Lemma 3 and 4] (see [75, Lemma J.3, J.5 and J.6] for a unified treatment of these algorithms) from which they are obtained straightforwardly.

Proposition 11 *Let $\delta(m, s, n, r)$ be the bound defined in Proposition 6. At the first recursion step of* LowRankRec*, the following holds:*

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

4 Regularity of the incidence variety

The goal of this section is to prove Proposition 2. We introduce the notation $\mathfrak{B}$ representing a $m \times s$ matrix, with $m \geq s$, whose entries are indeterminates $\mathfrak{b} = (\mathfrak{b}_{i,j})$; similarly, the $(s - r) \times s$ matrix $\mathfrak{U}$ whose entries are indeterminates $\mathfrak{u} = (\mathfrak{u}_{i,j})$, and we use the notation $\mathfrak{a} = (\mathfrak{a}_{\ell,i,j})$ to denote generic entries of the linear matrix $A(x)$. All the projection maps will be denoted by π when source and target spaces are clear from the context.

Proof of Assertion 1 of Proposition 2: By [70, Prop 3.1], there exists a non-empty Zariski open set $\mathscr{A}_1' \subset (\mathbb{C}^{m\times s})^{n+1}$ such that for $A \in \mathscr{A}_1'$ and all $0 \leq p \leq r$, $\mathcal{D}_p \subset \mathbb{C}^n$ is either empty or $n - (m - p)(s - p)$-equidimensional, and $\mathrm{sing}(\mathcal{D}_p) = \mathcal{D}_{p-1}$. It remains to prove that there exists a non-empty Zariski open set $\mathscr{A}_1'' \subset (\mathbb{C}^{m\times s})^{n+1}$ such that, for $A \in \mathscr{A}_1''$ and all $0 \leq p \leq r$, the ideal generated by the $(p + 1, p + 1)$ minors of $A(x)$ is radical. Defining $\mathscr{A}_1$ as the intersection of $\mathscr{A}_1'$ and $\mathscr{A}_1''$ leads to the following conclusion: there exists a non-empty Zariski open set $\mathscr{A}_1 \subset (\mathbb{C}^{m\times s})^{n+1}$ such that for $A \in \mathscr{A}_1$, A satisfies G_1.

By [63, Chap. 16] and [82, Prop. 12.2], the ideal $I \subset \mathbb{C}[\mathfrak{b}]$ generated by the $(p + 1, p + 1)$ minors of $\mathfrak{B}$ is radical and $\mathcal{Z}(I)$ is prime, of co-dimension $(m - p)(s - p)$. We deduce that the Jacobian matrix of the set of generators of I has full rank $(m - p)(s - p)$ when instantiated at a smooth point (having rank exactly p) of $\mathcal{Z}(I)$. A simple dimension count shows that one can apply Bertini'stheorem [82, Theorem 17.16] when adding generic linear forms $\{L_{i,j} = \mathfrak{b}_{i,j} - \sum_\ell \mathfrak{a}_{\ell,i,j}x_\ell\}$ (where we put by convention $x_0 = 1$) to the ideal ideal $I' = I + \langle L_{i,j}\rangle$ to deduce that one obtains a prime ideal. Using the Jacobian crierion [25, Theorem 16.19], we deduce that the rank of the Jacobian matrix of I' equals the rank of

the Jacobian matrix of I (which is $(m-p)(s-p)$) plus $ms = \#\{L_{i,j}\}$, since an identity submatrix will appear in correspondence with the derivatives with respect to $\mathfrak{a}_{0,i,j}$. We consider now the restriction to $\mathcal{Z}(I')$ of the projection $\pi(\mathfrak{b}, \mathfrak{a}, x) = \mathfrak{a}$ eliminating variables $\mathfrak{b}, x$. By Sard's theorem the singular values of π lie in a Zariski-closed set of the image of π. We deduce that there exists a non-empty and Zariski-open set $\mathscr{A}_1'' \subset (\mathbb{C}^{m\times s})^{n+1}$ such that if $A \in \mathscr{A}_1''$, the ideal $I'' = I + \langle \mathfrak{b}_{i,j} - \sum_\ell a_{\ell,i,j} x_\ell \rangle \subset \mathbb{C}[\mathfrak{b}, x]$ is radical. Thus the intersection $I'' \cap \mathbb{C}[x]$ (that eliminates the variables $\mathfrak{b}$) still yields a radical ideal in $\mathbb{C}[x]$. Finally, note that this elimination ideal coincides with the ideal generated by the $(p+1, p+1)$ minors of $A(x)$ (indeed, the elimination is performed by substituting the generic entries of $\mathfrak{B}$ with the entries of A). We conclude that if $A \in \mathscr{A}_1''$, the ideal of $(p+1, p+1)$ minors of $A(x)$ is radical. □

Proof of Assertion 2 of Proposition 2: We prove now that there exists a non-empty Zariski open set $\mathscr{A}_2 \subset (\mathbb{C}^{m\times s})^{n+1}$ such that the following holds. For $A \in \mathscr{A}_2$, there exists a non-empty Zariski open set $\mathscr{U}_A \subset \mathbb{C}^{(s-r)\times s}$ such that for $U \in \mathscr{U}_A$, Assertions $(2a)$ and $(2b)$ of Proposition 2 are satisfied. Taking $\mathscr{A}$ as the intersection of $\mathscr{A}_1$ and $\mathscr{A}_2$ will end the proof.

Let $\mathfrak{F} \subset \mathbb{C}[\mathfrak{a}, \mathfrak{b}, \mathfrak{u}, y]$ denote the vector of polynomials consisting of: the generic linear forms $\{L_{i,j} = \mathfrak{b}_{i,j} - \sum_\ell \mathfrak{a}_{\ell,i,j} x_\ell\}$ as in the proof of Assertion 1, and the entries of $\mathfrak{B}Y$ and $\mathfrak{U}Y - \mathbb{I}_{s-r}$. First, remark that all solutions (A, B, U, y) of $\mathfrak{F} = 0$ satisfy $\operatorname{rank} U = \operatorname{rank} Y = s - r$ by the classical condition $\operatorname{rank} MN \leq \min\{\operatorname{rank} M, \operatorname{rank} N\}$. The Jacobian matrix $D\mathfrak{F}$ of $\mathfrak{F}$ has full rank when restricted to $\mathcal{Z}(F)$, since we can construct a non-singular block sub-matrix of $D\mathfrak{F}$ made by the following blocks:

- the derivatives of forms $L_{i,j}$ with respect to $\mathfrak{a}_{0,i,j}$, a $ms \times ms$ block equal to $\mathbb{I}_{ms}$;
- the derivatives of $\mathfrak{B}Y$ with respect to $\mathfrak{b}$, a $m(s-r) \times ms$ block-diagonal matrix with m blocks equal to Y^T;
- the derivatives of $\mathfrak{U}Y - \mathbb{I}_{s-r}$ with respect to $\mathfrak{u}$, a $(s-r)^2 \times s(s-r)$ block-diagonal matrix with $s-r$ blocks equal to Y^T.

By the Jacobian Criterion, $\mathfrak{F}$ satisfies G_2, hence $\mathcal{Z}(\mathfrak{F})$ is smooth and equidimensional. We consider the restriction of $\pi(\mathfrak{a}, \mathfrak{b}, \mathfrak{u}, x, y) = \mathfrak{a}$ to $\mathcal{Z}(\mathfrak{F})$. Applying Sard's theorem, we obtain a non-empty and Zariski-open set $\mathscr{A}_2$ such that, for $A \in \mathscr{A}_2$, the ideal generated by $\mathfrak{F}'$ (obtained from $\mathfrak{F}$ by instantiating $\mathfrak{a}$ to the entries of A) satisfies G_2.

Let us fix $A \in \mathscr{A}_2$. Considering the new projection $\pi : (\mathfrak{b}, \mathfrak{u}, x, y) \to \mathfrak{u}$ restricted to $\mathcal{Z}(\mathfrak{F}')$, and applying Sard's theorem implies that there exists $\mathscr{U}_A' \subset \mathbb{C}^{(s-r)\times s}$, non-empty and Zariski-open, such that if $U \in \mathscr{U}_A'$, instantiating $\mathfrak{u}$ to U yields a radical ideal $I \subset \mathbb{C}[\mathfrak{b}, x, y]$, with the Jacobian matrix of I full rank at every solution. Now, $f(A, U)$ with $A \in \mathscr{A}_2$ and $U \in \mathscr{U}_A'$ generates the elimination ideal $I \cap \mathbb{C}[x, y]$, hence it is still radical. Since $f(A, U)$ is obtained from I by instantiating $\mathfrak{b}$ to the entries of A, the Jacobian matrix $Df(A, U)$ is a submatrix of the Jacobian matrix of a set of generators of I, which has full rank. Since the polynomials in $f(A, U)$ do not depend on variables $\mathfrak{b}$, it is easily seen that $Df(A, U)$ has full rank too. Hence we deduce that, for $A \in \mathscr{A}_2$ and $U \in \mathscr{U}_A'$, $f(A, U)$ satisfies G_2, as claimed.

It remains to prove that there exists a non-empty Zariski open set $\mathscr{U}_A'' \subset \mathbb{C}^{(s-r)\times s}$ such that for $U \in \mathscr{U}_A''$, assertion (2b) holds. Finally taking the intersection of $\mathscr{U}_A'$ and $\mathscr{U}_A''$ to define $\mathscr{U}_A$ ends the proof. Let $A \in \mathscr{A}_2$, $p \leq r$ and let Z be one of the (finitely-many) irreducible components of $\mathcal{D}_p$, and let d be its dimension (all such components have the same dimension, since we proved that $\mathcal{D}_p$ is empty or equidimensional). Intersecting Z with d general hyperplanes, we get a finite number of smooth points in Z. For every such point $x \in Z$, we first build a Zariski-open set $\mathscr{U}''_{A,p,Z,x} \subset \mathbb{C}^{(s-r)\times s}$, as follows.

The rank of $A(x)$ is p since x is a smooth point of Z (because Z is an irreducible component of the Zariski closure of the set of points at which A has rank p). The polynomial system $y \mapsto f(A,U)$ is linear in y. Since rank$A(x) = p$, the condition $A(x)Y(y) = 0$ defines a linear space $V = \{Y(y) \in \mathbb{C}^{s\times(s-r)} : A(x)Y(y) = 0\}$ of dimension $(s-p)(s-r)$. Since $p \leq r$, remark that $(s-r)^2 \leq (s-p)(s-r)$. For a generic $U \in \mathbb{C}^{(s-r)\times s}$, the $(s-r)^2$ affine equations $UY(y) - \mathbb{I}_{s-r} = 0$ define a linear space intersecting V. Hence there exists a non-empty Zariski open set $\mathscr{U}''_{A,p,Z,x} \subset \mathbb{C}^{(s-r)\times s}$ such that, if $U \in \mathscr{U}''_{A,p,Z,x}$, the linear system $A(x)Y(y) = 0, UY(y) - \mathbb{I}_{s-r} = 0$ has at least one solution.

One concludes by defining

$$\mathscr{U}_A'' = \bigcap_{p\leq r} \bigcap_{Z\subset\mathcal{D}_p\cap\mathbb{R}^n} \bigcap_{x\in Z} \mathscr{U}''_{A,p,Z,x}$$

which is non-empty and Zariski open by the finiteness of the number of irreducible components of $\mathcal{D}_p \cap \mathbb{R}^n$ and of the set of points x in Z. □

Proof of Assertion 3 of Proposition 2: By Sard'sTheorem, the critical values of the projection $\pi_w(x) = w^T x$ are finitely many, hence the regular values of this map define a non-empty Zariski open set $\mathscr{T}_A \subset \mathbb{C}$. For w as in the hypothesis, and $t \in \mathscr{T}_A$, we denote by $\mathcal{D}'_p = \{x \in \mathbb{C}^{n-1} : \text{rank } A\big|_{w,t}(x) \leq p\}$. As in the proof of Assertion 1, since $A \in \mathscr{A}$, we deduce that if $t \in \mathscr{T}_A$, then the ideal $I = \langle\{(p+1)\times(p+1) \text{ minors of } A\}, \pi_w(x) - t\rangle$ is still radical and $\mathcal{Z}(I)$ has co-dimension $(m-p)(s-p)+1$. Remark that $I\cap\mathbb{R}[x_2,\ldots,x_n]$ is generated by the $(p+1)\times(p+1)$ minors of $A\big|_{w,t}$, it is still radical and $\mathcal{D}'_p = \mathcal{Z}(I \cap \mathbb{R}[x_2,\ldots,x_n])$ has co-dimension $(m-p)(s-p)$ in $\mathbb{C}^{n-1}$. Moreover, always for $t \in \mathscr{T}_A$, a point in $\mathcal{D}_p$ is regular if and only if it is regular in $\mathcal{D}_p \cap \mathcal{Z}(\pi_w(x) - t)$. Hence we deduce that for $t \in \mathscr{T}_A$, the matrix $A\big|_{w,t}$ satisfies Property G_1, as claimed. □

5 Dimension of Lagrange systems

The goal of this Section is to prove Proposition 3. We first need to give a local description of the incidence variety $\mathcal{V}_r$ and of the solution set $\mathcal{Z}(A,U,w)$ of the Lagrange system $\ell(A,U,w)$.

5.1 Local description of the incidence variety

As in our previous work [47], we need to compute equations for the incidence sets lifting the determinantal varieties. Here we generalize the equations in [47, Section 4] to the case of low-rank rectangular matrices.

Let $A = A_0 + x_1 A_1 + \ldots + x_n A_n$ be a $n-$variate $m \times s$ linear matrix with coefficients in $\mathbb{Q}$, and let $r \leq s-1$. From now on, for $g \in \mathbb{Q}[x]$, we denote by $\mathbb{Q}[x]_g$ the localization of the ring $\mathbb{Q}[x]$ at $\langle g \rangle$, see [25]. We recall that the polynomial system defining $\mathcal{V}_r$ is given by $f(A,U)$, which contains the entries of $A(x)Y(y)$ and $UY(y) - \mathbb{I}_{s-r}$. For $p \leq r$, let N be the upper-left $p \times p$ submatrix of A, so that

$$A = \begin{pmatrix} N & Q \\ P^T & R \end{pmatrix} \tag{5}$$

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

Lemma 12 *Let A, N, Q, P, R be as above, and U be any full-rank matrix. Then there exist $\{q_{i,j}\}_{1\leq i\leq p, 1\leq j\leq s-p}, \{q'_{i,j}\}_{1\leq i\leq m-p, 1\leq j\leq s-p} \subset \mathbb{Q}[x]_{\det N}$ such that the constructible set $\mathcal{V}_r \cap \{(x,y) : \det N(x) \neq 0\}$ is defined by the equations*

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

Proof : We denote by $Y^{(1)}$ and $Y^{(2)}$ the submatrices of $Y(y)$ containing respectively the first p rows and the last $s-p$ rows. We also use the block-division of A as in (5). We claim that in $\mathbb{Q}[x,y]_{\det N}$ the $m(s-r)$ equations $A(x)Y(y) = 0$ are equivalent to the $m(s-r)$ equations:

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

where $\Sigma(N) = R - P^T N^{-1} Q$ 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

$$\begin{pmatrix} \mathbb{I}_p & 0 \\ -P^T & \mathbb{I}_{m-p} \end{pmatrix} \begin{pmatrix} N^{-1} & 0 \\ 0 & \mathbb{I}_{m-p} \end{pmatrix} \begin{pmatrix} N & Q \\ P^T & R \end{pmatrix} Y(y) = 0.$$

□

5.2 The rank at a critical point

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

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

Lemma 12 implies that the equations of $\mathcal{V}_r$ in the open set $\{(x,y) : \det N \neq 0\}$ can be rewritten as $\widetilde{A}(x)Y(y) = 0$ and $UY(y) - \mathbb{I}_{s-r} = 0$: 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 $\{y_{i,j}\}_{1\le i\le p, 1\le j\le s-r}$, which can be expressed as polynomial functions of x and $\{y_{i,j}\}_{p+1\le i\le s, 1\le j\le s-r}$. That is, using the notations introduced in Lemma 12, we can express the entries of $Y^{(1)}$ as polynomials in x and in the entries of $Y^{(2)}$.

Now, consider the relations $UY(y) - \mathbb{I}_{s-r} = 0$ 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 $\mathbb{I}_{s-r}$ is full-rank, then U is full-rank and hence $UY(y) - \mathbb{I}_{s-r} = 0$ consists of $(s-r)^2$ independent relations. Finally one can eliminate $(s-r)^2$ among the $(s-p)(s-r)$ entries of $Y^{(2)}$ (suppose the first $(s-r)$ rows) and re-write $\Sigma(N)Y^{(2)} = 0$ as $(m-p)(s-r)$ relations in x and in the last $(r-p)(s-r)$ entries of $Y^{(2)}$.

Let us call F this polynomial system, and consider a vector of Lagrange multipliers $z = (z_1, \ldots, z_{(m-p)(s-r)})$ and the polynomial system

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

The solutions to the above polynomial system contain the critical points of the projection $\pi_w \colon \mathbb{C}^n \to \mathbb{C}$, $\pi_w(x) = w^T x \coloneqq w_1x_1 + \cdots + w_nx_n$, 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 rank exactly r (namely in $\mathcal{D}_r \setminus \mathcal{D}_{r-1}$).

The proof of the next Lemma follows *mutatis mutandis* that of [47, Lemma 14], hence its proof is given in Appendix B.

Lemma 13 *Let A, U be as above and suppose that A satisfies G_1. Let $p \le r-1$ and let $g = (g_1, \ldots, g_n)$ be the polynomial system defined above. Then there exists a non-empty Zariski open set $\widetilde{\mathscr{W}}_{A,U} \subset \mathbb{C}^n$ such that the following holds: if $w \in \widetilde{\mathscr{W}}_{A,U}$ then the system $g(x,y,z,w) = 0$ has no solutions in x, y, z.*

5.3 Local description of the Lagrange system

We consider the incidence variety $\mathcal{V}_r = \mathcal{V}_r(A,U)$ and the restriction of the projection $\Pi_w(x,y) = w^T x$ to $\mathcal{V}_r$, with $w \in \mathbb{C}^n$. Under the hypothesis that A satisfies G_1 and that $f(A,U)$ satisfies G_2, the set $\mathcal{V}_r$ is either empty or smooth and equidimensional of codimension $c \coloneqq (m+s-r)(s-r)$. 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 solutions of the Lagrange system $\ell(A,U,w)$:

$$f(A,U) = 0 \qquad (g,h) \coloneqq z^T \begin{pmatrix} D_x f & D_y f \\ w^T & 0 \end{pmatrix} = 0, \tag{6}$$

where $z = (z_1, \ldots, z_c, 1)$. The polynomial system (6) consists of $n + c + s(s-r)$ polynomials in $n + c + s(s-r)$ variables. We show that it can be re-written in a local form when we consider the local description of the incidence variety $\mathcal{V}_r$ as in Section 5.1.

We use the block-division of matrix A as in (5) 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 12 that the local equations of $\mathcal{V}_r$ are

$$Y^{(1)} = -N^{-1}QY^{(2)}, \qquad \Sigma(N)Y^{(2)} = 0, \qquad U^{(1)}Y^{(1)} + U^{(2)}Y^{(2)} = \mathbb{I}_{s-r},$$

where $Y^{(1)}, Y^{(2)}$ is the row-subdivision of the matrix $Y(y)$ as in Lemma 12 and $U^{(1)}, U^{(2)}$ is the corresponding column-subdivision of U. From the first and third groups of equations one obtains that $\mathbb{I}_{s-r} = U^{(1)}(-N^{-1}QY^{(2)}) + U^{(2)}Y^{(2)} = (-U^{(1)}N^{-1}Q + U^{(2)})Y^{(2)}$. Since $\mathbb{I}_{s-r}$ 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 $Y^{(2)} = (-U^{(1)}N^{-1}Q + U^{(2)})^{-1}$.

The entries of $\Sigma(N)$ in the local ring $\mathbb{Q}[x]_{\det N}$ are exactly the $(m-r)(s-r)$ 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 [75, Proposition 3.2.7]). Since A satisfies G_1, 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 $Y^{(2)} - (-U^{(1)}N^{-1}Q + U^{(2)})^{-1}$. The Jacobian matrix of f' has the form

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

We consider the polynomials

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

Polynomials in $h' = (h'_1, \ldots, h'_{s(s-r)})$ give the relations $z_i = 0$, for $i = (m-r)(s-r)+1, \ldots, c$, and can be eliminated together with variables $z_i, i = (m-r)(s-r)+1, \ldots, c$. So the local equations of the Lagrange system (6) are:

$$f' = 0, \qquad g' = 0 \tag{7}$$

This is a square system consisting of $n + c$ polynomials in $n + c$ variables.

5.4 Proof of Proposition 3

Proof of Assertion 1 of Proposition 3: Let $\widetilde{\mathscr{W}_{A,U}} \subset \mathbb{C}^n$ be the set defined by Lemma 13, and $w \in \widetilde{\mathscr{W}_{A,U}}$. Then one has that all solutions (x, y, z) to (6) (hence of the local version (7)) satisfy $\operatorname{rank} A(x) = r$. We deduce that there exists a $r \times r$ submatrix N of $A(x)$ such that $\det N \neq 0$. We prove below that there exists a non-empty Zariski open set $\mathscr{W}_{N,A,U} \subset \mathbb{C}^n$ such that, for $w \in \mathscr{W}_{N,A,U}$, the statement of Assertion 1 holds locally. Hence, to retrieve the global property, it is sufficient to define $\mathscr{W}_{A,U}$ as the (finite) intersection of sets $\widetilde{\mathscr{W}_{A,U}} \cap \mathscr{W}_{N,A,U}$, where N varies in the collection of $r \times r$ submatrices of A.

We suppose without loss of generality that N is the upper-left $r \times r$ submatrix of A. Let (f', g') be the local Lagrange system defined in (7). Consider the polynomial map

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

and, for a fixed $w \in \mathbb{C}^n$, its section map

$$\begin{array}{rccc} \varphi_w : & \mathbb{C}^{n+c} & \longrightarrow & \mathbb{C}^{n+c} \\ & (x,y,z) & \longmapsto & \varphi(x,y,z,w) \end{array}.$$

If $\varphi^{-1}(0) = \emptyset$, then for all $w \in \mathbb{C}^n$, $\varphi_w^{-1}(0) = \emptyset$, and the claim is proved by taking $\mathscr{W}_{N,A,U} = \widetilde{\mathscr{W}}_{A,U}$ (see Lemma 13).

Suppose now that $\varphi^{-1}(0) \neq \emptyset$ and let $(x,y,z,w) \in \varphi^{-1}(0)$. We claim that the Jacobian matrix of φ at (x,y,z,w) has maximal rank. Hence, 0 is a regular value for φ and by Thom's Weak Transversality Theorem [75, Proposition B.3] there exist a non-empty Zariski open set $\mathscr{W}_{N,A,U} \subset \mathbb{C}^n$ such that for $w \in \mathscr{W}_{N,A,U}$, 0 is a regular value of φ_w. This implies that, by the Jacobian criterion, the set $\mathcal{Z}(A,U,w) \cap \{(x,y,z) : \det N(x) \neq 0\}$ is empty or zero-dimensional. We prove below this claim by exhibiting a non-singular submatrix of $D\varphi$.

We remark that, since $f(A,U)$ satisfies G_2, the Jacobian matrix Df' has maximal rank at (x,y) and consider the submatrix of $D\varphi$ obtained by isolating:

- a non-singular maximal submatrix of Df';
- the derivatives of $g_1', \ldots, g_n'$ with respect to $w_1, \ldots, w_n$, giving the identity block $\mathbb{I}_n$.

The previous blocks define a submatrix of $D\varphi(x,y,z,w)$ of size $(n+c) \times (n+c)$ whose determinant does not vanish at (x,y,z,w). □

Proof of Assertion 2 of Proposition 3: Let $w \in \mathbb{C}^n$, and let $(x,y) \in \mathrm{crit}(\Pi_w, \mathcal{V}_r)$. Since $A \in \mathscr{A}$, $f(A,U)$ satisfies G_2 and $\mathcal{V}_r(A,U)$ is smooth and equidimensional. Hence $(x,y) \in \mathrm{reg}(\mathcal{V}_r(A,U)) = \mathcal{V}_r(A,U)$. In particular $Df(x,y)$ has full rank. Since $(x,y) \in \mathrm{crit}(\Pi_w, \mathcal{V}_r)$, the extended Jacobian matrix $D(f, \Pi_w)$ has a rank defect. Hence, there exists $z = (z_1, \ldots, z_{c+1}) \neq 0$ with $z^T D(f, \Pi_w)(x,y) = 0$. If $z_{c+1} = 0$, then $0 = z^T D(f, \Pi_w) = (z_1, \ldots, z_c) Df(x,y)$, which is a contradiction since $Df(x,y)$ has full rank. Then we can assume $z_{c+1} = 1$, and hence that $(x,y,z) \in \mathcal{Z}(A,U,w)$. We conclude that $\mathrm{crit}(\Pi_w, \mathcal{V}_r)$ is contained in the projection of $\mathcal{Z}(A,U,w)$ on (x,y), as claimed. □

6 Closure properties

The goal of this section is to prove Proposition 4. We use notation of [47, Section 5], which we recall below.

Notations. For $M \in \mathrm{GL}_n(\mathbb{C})$, and $\mathcal{Z} \subset \mathbb{C}^n$ any set, we define

$$M^{-1}\mathcal{Z} \coloneqq \{x \in \mathbb{C}^n : Mx \in \mathcal{Z}\} = \{M^{-1}x : x \in \mathcal{Z}\}.$$

Remark that, if $w \neq 0$ and if $M \in \mathrm{GL}_n(\mathbb{C})$ with $w = M_{(1)}^{-1}$ (the first row of M^{-1}), then

$$\pi_1(M^{-1}\mathcal{Z}) = M_{(1)}^{-1}\mathcal{Z} = \pi_{M_{(1)}^{-1}}(\mathcal{Z}) = \pi_w(\mathcal{Z}). \tag{8}$$

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 $k \geq i$ of the sets $\mathrm{crit}(\pi_i, \mathrm{reg}(\Omega_k(\mathcal{Z})))$ of critical points of the restriction of π_i to the regular locus of $\Omega_k(\mathcal{Z})$.

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 that an algebraic set $\mathcal{V} = \mathcal{Z}(I) \subset \mathbb{C}^n$ is in Noether position with respect to variables $x_1, \ldots, x_i$, if and only if the morphism $\varphi\colon \mathbb{C}[x_1, \ldots, x_i] \hookrightarrow \mathbb{C}[x_1, \ldots, x_n]/I$ is injective and integral. If this is the case, the induced morphism $\varphi^*\colon \mathcal{V} \to \mathbb{C}^i$ is the projection $\varphi^*(x) = (x_1, \ldots, x_i)$ and φ^* is one-to-one.

The following two properties have been defined in [47, 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 [47] 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 A and U be as in the hypothesis. Let $\mathscr{M}_{A,U} \subset \mathrm{GL}_n(\mathbb{C})$ be the non-empty Zariski open set defined in [47, Proposition 17] for $\mathcal{Z} = \mathcal{D}_r$. This set might depend on the choice of A and U, as explicited by the indices. One obtains that every $M \in \mathscr{M}_{A,U} \cap \mathrm{GL}_n(\mathbb{Q})$ satisfies $\mathsf{P}(\mathcal{D}_r)$. Remark that since $M \in \mathrm{GL}_n(\mathbb{Q})$, 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 $M \in \mathscr{M}_{A,U}$, by [47, 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 for all i. Let $\varphi\colon \mathbb{C}^{n\times n} \to \mathbb{C}^n$ be the map sending $M \in \mathbb{C}^{n\times n}$ to its first row $M_{(1)}$. The map φ is a projection, hence a morphism. Applying [45, 9.1, Ex.III], one gets that $\varphi(\mathscr{M}_{A,U}) \coloneqq \mathscr{W}^{(1)}_{A,U}$ is Zariski-open in $\mathbb{C}^n$. In particular, for $i = 1$ and applying (8), one gets that $\pi_w(\mathcal{C})$ is closed, for $w \in \mathscr{W}^{(1)}_{A,U}$. □

Proof of Assertion 2 of Proposition 4:

Let A and U be as in the hypothesis. Fix $0 \le p \le r$. Since $A \in \mathscr{A}$, by Proposition 2 the set $\mathcal{D}_p$ has the expected co-dimension, hence $c = (m-p)(s-p)$. Let $\eta_1, \ldots, \eta_c$ be local equations for $\mathcal{D}_p$.

We consider the following constructible set:

$$J = \left\{ (x, z, w) : x \in \mathcal{D}_p \cap \mathcal{N}_r(A, U), w_i = \sum_j z_j \frac{\partial \eta_j}{\partial x_i}, z \neq 0 \right\}$$

and the projection $\pi : \mathbb{C}^N \to \mathbb{C}^n$, $\pi(x, y, z, w) = w$, with $N = 2n + c$, where c is the co-dimension of $\mathcal{D}_p$. We claim that $\pi(J)$ is a constructible subset of $\mathbb{C}^n$ of positive co-dimension. Hence there exists a non-empty Zariski open set $\mathscr{W}^{(2)}_{A,U} \subset (\mathbb{C}^n \setminus \pi(J))$ such that Assertion 2 holds for $w \in \mathscr{W}^{(2)}_{A,U}$. We conclude the proof by defining $\mathscr{W}'_{A,U} = \mathscr{W}^{(1)}_{A,U} \cap \mathscr{W}^{(2)}_{A,U}$ (where $\mathscr{W}^{(1)}_{A,U}$ has been defined in the proof of Assertion 1).

We prove now our claim. By Assertion (2b) of Proposition 2, the set $\mathcal{D}_p \cap \mathcal{N}_r(A, U)$ has positive codimension in $\mathcal{D}_p$, hence it has codimension at least $c + 1$. Moreover, the equations $w_i = \sum_j z_j \frac{\partial \eta_j}{\partial x_i}$ define an algebraic set of co-dimension n (indeed, their Jacobian matrix has full rank, having a $n \times n$ identity matrix corresponding to the derivatives w.r.t. w_i). We deduce that J is a constructible set of dimension at most $N - (c+1+n) = n-1$ in $\mathbb{C}^N$. Hence its projection $\pi(J)$ has dimension at most $n-1$ in $\mathbb{C}^n$, as claimed. □

7 Experiments

This section reports on experiments made with a first implementation of our algorithm. Note that for computing rational parametrizations, we use Gröbner bases and change of ordering algorithms [30, 36]. Our experiments are done using the C library FGb, developed by J.-C. Faugère [28] and interfaced with Maple.

We start by comparing our implementation with implementations of general algorithms based on the critical point method in RAGLib [72]. 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 $m = s$ (for simplicity we perform computations on square matrices) 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 $m = s$, $2 \leq r \leq m-1$ 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	-	-
$(3,2,3)$	0.3	7.5	21	12	$(5,2,4)$	1	0.5	-	-
$(3,2,4)$	0.9	9.5	33	12	$(5,2,5)$	1.6	0.5	-	-
$(3,2,5)$	5.1	13.5	39	12	$(5,2,6)$	3	0.6	-	-
$(3,2,6)$	15.5	15	39	12	$(5,2,7)$	4.2	0.7	-	-
$(3,2,7)$	31	16.5	39	12	$(5,2,8)$	8	0.7	-	-
$(3,2,8)$	109	18	39	12	$(5,2,9)$	∞	903	175	175
$(3,2,9)$	230	20	39	12	$(5,3,2)$	0.4	0.5	-	-
$(4,2,2)$	0.2	0.5	-	-	$(5,3,3)$	0.5	0.5	-	-
$(4,2,3)$	0.3	0.5	-	-	$(5,3,4)$	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	-	-
$(4,3,3)$	1	8	52	36	$(6,3,4)$	140	1	-	-
$(4,3,4)$	590	18	120	68	$(6,3,5)$	∞	1	-	-
$(4,3,5)$	∞	56	204	84	$(6,3,6)$	∞	2	-	-
$(4,3,6)$	∞	114	264	84	$(6,3,7)$	∞	2	-	-
$(4,3,7)$	∞	124	284	84	$(6,3,8)$	∞	2	-	-
$(4,3,8)$	∞	124	284	84	$(6,4,2)$	0.6	40	-	-
$(4,3,9)$	∞	295	284	84	$(6,4,3)$	1	64	-	-
$(4,3,10)$	∞	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	-	-	$(6,5,4)$	∞	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 [72]. The symbol ∞ means that no result has been returned after 4 days of computation. In column deg we report the degree of the rational parametrization $q = (q_0, q_1, \ldots, q_n, q_{n+1})$ (we recall thet this is, by definition, the degree of q_{n+1}). Finally, in column maxdeg we report the maximum of the degrees of the partial rational

parametrizations (those corresponding to the different recursive steps of LowRank). When deg is "-", we mean that the empty list is returned.

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 corresponding 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 $n > (m+r)(s-r)$ and the input is generic, LowRank does not compute critical points at first calls. This fact is remarkable, since:
   - it is known (see [4, Ch. II]) that 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 the Thom-Porteous-Giambelli formula, *cf.* [4, Ch. II,§ 4]);
   - an algebraic invariant naturally associated to the output-size (the degree of q_{n+1}) is constant in n, coherently with the aforementioned 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. In the recent paper [75], an algorithm to address connectivity queries (for instance, deciding whether 2 points of a smooth compact real algebraic set lie on the same connected component) has been developed.

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 14 (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 $\mathcal{D}_2 = \{x \in \mathbb{C}^3 \mid \text{rank } A(x) \leq 2\}$ *is shown in Figure 1.*

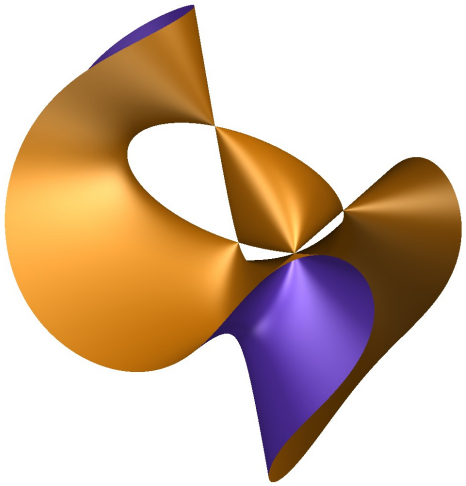

Figure 1: Cayley determinantal cubic surface with its four singular points on the boundary of its spectrahedron.

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 chooses a random matrix* U*, then 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 5, a rational parametrization of degree* 5 *is computed, 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:*

$$\begin{aligned} x_1 &\in [\tfrac{21081306277346124211}{1152921504606846976}, \tfrac{21081306277346754459}{1152921504606846976}] \approx 18.285118452 \\ x_2 &\in [\tfrac{5920353629066611305}{36028797018963968}, \tfrac{23681414516266799197}{144115188075855872}] \approx 164.322822823 \\ x_3 &\in [\tfrac{10496816461511385723}{2305843009213693952}, \tfrac{2624204115377866059}{576460752303423488}] \approx 4.552268485, \end{aligned}$$

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 computes 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 *returns 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 a few seconds (*< 5 *sec.).*

Example 15 *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 let (a_1, a_2, a_3, a_4) *vary randomly in* $\mathbb{Q}^4$*. For all random instances, 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 15 with generic parameters

Example 16 (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 $S = \{x \in \mathbb{R}^3 : A(x) \succeq 0\}$ *is known as the pillow, see also [15, 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.*

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* $x_2 + x_3 = 0$*.*

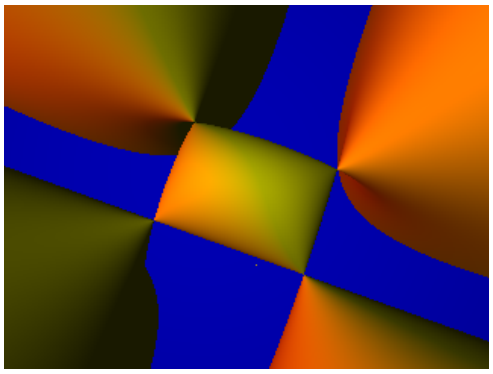

Figure 2: The pillow and its algebraic boundary

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 14, 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 14, 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 16 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] M.F. Anjos and J.B. Lasserre editors. Handbook of semidefinite, conic and polynomial optimization. International Series in Operational Research and Management Science. Volume 166, 2012.

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

[5] B. Bank, M. Giusti, J. Heintz, G. Lecerf, G. Matera, P. Solern, Degeneracy loci and polynomial equation solving. Foundations of Computational Mathematics, 15(1), 159-184, 2015.

[6] 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.

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

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

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

[10] 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.

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

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

[13] 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.

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

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

[16] B. Bonnard, J.-C. Faugère, A. Jacquemard, M. Safey El Din, T. Verron. Determinantal Sets, Singularities and Application to Optimal Control in Medical Imagery. Proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC 2016, Waterloo (Canada).

[17] B. Bonnard, O. Cots, J.-C. Faugère, A. Jacquemard, J. Rouot, M. Safey El Din and T. Verron. Algebraic-geometric techniques for the feedback classification and robustness of the optimal control of a pair of Bloch equations with application to Magnetic Resonance Imaging, submitted, 2017.

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

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

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

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

[22] 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.

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

[24] 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.

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

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

[27] 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.

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

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

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

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

[36] 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.

[37] P. Gianni and T. Mora. 1989. Algebraic solution of systems of polynomial equations using Groebner bases. In AAECC (LNCS), Vol. 356. Springer, 247–257.

[38] M. Giusti, J. Heintz, J.-E. Morais, and L.-M. Pardo. 1995. When polynomial equation systems can be solved fast?. In AAECC-11 (LNCS), Vol. 948. Springer, 205–231.

[39] M. Giusti, J. Heintz, J.-E. Morais, and L.-M. Pardo. 1997. Le rôle des structures de données dans les problèmes d'élimination. C. R. Acad. Paris 325 (1997), 1223–1228.

[40] M. Giusti, J. Heintz, J.-E. Morais, J. Morgenstern, and L.-M. Pardo. 1998. Straight-line programs in geometric elimination theory. Journal of Pure and Applied Algebra 124 (1998), 101–146.

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

[42] M. Golubitsky and V. Guillemin. Stable mappings and their singularities, Springer Science, 2012

[43] 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.

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

[45] R. Hartshorne. Algebraic Geometry. Graduate texts in mathematics 52 (1977).

[46] 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.

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

[48] D. Henrion, S. Naldi, M. Safey El Din. Real root finding for rank defects in linear Hankel matrices. Proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC 2015, Bath (UK).

[49] D. Henrion, S. Naldi, M. Safey El Din. Exact Algorithms for Linear Matrix Inequalities. SIAM J. Optim., 26(4), 25122539, 2016.

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

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

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

[53] J. Kileel, Z. Kukelova, B. Sturmfels, T. Pajdla. Distortion Varieties. To appear in Foundations of Computational Mathematics (2017).

[54] L. Kronecker. 1882. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. Journal für die reine und angewandte Mathematik 92 (1882), 1–122.

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

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

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

[58] 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.

[59] G. Lecerf. 2000. Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions. In ISSAC'00. ACM, 209–216.

[60] 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.

[61] F. S. Macaulay. 1916. The Algebraic Theory of Modular Systems. Cambridge University Press.

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

[63] E. Miller and B. Sturmfels. Combinatorial commutative algebra. Springer Science & Business Media, Vol. 227, 2004.

[64] 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.

[65] 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.

[66] 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.

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

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

[69] A. Poteaux and É. Schost. On the complexity of computing with zero-dimensional triangular sets. Journal of Symbolic Computation, 50(0):110-138, 2013.

[70] K. Ranestad. Algebraic degree in semidefinite and polynomial optimization. In Handbook on Semidefinite, Conic and Polynomial Optimization, pages 61–75. Springer, 2012.

[71] F. Rouillier. 1999. Solving zero-dimensional systems through the Rational Univariate Representation. Applicable Algebra in Engineering, Communication and Computing 9, 5 (1999), 433–461.

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

[73] 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.

[74] 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.

[75] M. Safey El Din, E. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. Journal of the ACM, Vol. 63, Iss. 6, February 2017, Article N. 48. ACM New York, NY, USA, 2017.

[76] M. Safey El Din, E. Schost. Bit complexity for multi-homogeneous polynomial system solvingApplication to polynomial minimization. Journal of Symbolic Computation, 2017.

[77] É. Schost. 2003. Computing parametric geometric resolutions. Applicable Algebra in Engineering, Communication and Computing 13, 5 (2003), 349–393.

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

[79] A.J. Sommese, C.W. Wampler. The numerical solution of systems of polynomials arising in engineering and science. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005.

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

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

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

A Appendix

Proof of Lemma 9: We exploit the multilinear structure of $t\ell + (1-t)\tilde{\ell}$. By the Multilinear Bézout theorem [79], $\deg \mathcal{Z}(t\ell + (1-t)\tilde{\ell})$ is bounded by the sum of the coefficients of

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

modulo $I = \langle s_x^{n+1}, s_y^{r(s-r)+1}, s_z^{m(s-r)}, s_t^2 \rangle \subset \mathbb{Z}[s_x, s_y, s_z, s_t]$. 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

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

and hence that $q \equiv q_1 + s_t(q_2 + q_3 + q_4) \mod I$. Below, we bound the contribution of $q_i, i = 1 \dots 4$. 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 $I' = \langle s_x^{n+1}, s_y^{r(s-r)+1}, s_z^{m(s-r)} \rangle$. This has been computed in Proposition 6, and coincides with $\delta(m,s,n,r)$.

The contribution of q_2. Write $q_2 = m(s-r)\tilde{q}_2$ 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 $m(s-r)$. Now, observe that $\deg \tilde{q}_2 = n-2+(m+r)(s-r)$ and that maxima powers admissible modulo I' are $s_x^n, s_y^{r(s-r)}, s_z^{m(s-r)-1}$. Hence, three configurations give a contribution.

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

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

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

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

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

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

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

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

Let us prove this claim. First, denote by

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

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

For all indices k admissible for both $\delta(m,s,n,r)$ and Σ_C, that is for $\alpha_1 \leq k \leq \chi_2$, one gets, by basic properties of binomial coefficients (we apply $\binom{a}{b-1} = \frac{b}{a-b-1}\binom{a}{b}$), that

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

When k runs over all admissible indices, the rational function $\Psi(k)$ is non-decreasing monotone, and its maximum is attained in $\Psi(\chi_2)$ and is bounded by $\min\{n, m(s-r)\}$. Three possible cases can hold:

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

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

3. $\chi_1 = 0$ and $\alpha_1 = n - m(s-r) + 1$. Hence, we deduce the chain of inequalities $0 \leq n - m(s-r) + 1 \leq 1$. Hence, either this case coincides with case 2 (if $n = m(s-r)$) or we deduce that $n = m(s-r) - 1$, and we fall into case 1.

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 $\mathcal{O}\left(n\,\min\{n, m(s-r)\}\,\delta(m,s,n,r)\right)$ and that of q_4 is in $\mathcal{O}\left(r(s-r)\,\min\{n, m(s-r)\}\,\delta(m,s,n,r)\right)$. □

B Appendix

Proof of Lemma 13: Let $C \subset \mathbb{C}^{2n+(r-p)(s-r)+(m-p)(s-r)}$ be the constructible set defined by $g = 0$ and by $\det N \neq 0$ and $\operatorname{rank} A(x) = p$, where the coordinates of w are variables. Let $\overline{C}$ be the Zariski closure of C. Let $\pi_x \colon (x,y,z,w) \to x$ be the restriction of the projection on the first n variables to C. The image $\pi_x(C)$ is dense in $\mathcal{D}_p$. Hence, since A satisfies G_1, it has dimension at most $n - (m-p)(s-p)$. The fiber of π_x over a generic point $x \in \mathcal{D}_p$ is the graph of the polynomial function $w = z^T D_x F$, and so it has codimension n and dimension $(r-p)(s-r) + (m-p)(s-r) = (m+r-2p)(s-r)$. By the Theorem of the Dimension of Fibers [78, Sect. 6.3, Th. 7] one deduces that the dimension of C (and of $\overline{C}$) is at most $n - (m-p)(s-p) + (m+r-2p)(s-r) = n - (r-p)(m-p+r-s) < n$. 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 $\widetilde{\mathscr{W}_{A,U}} = \mathbb{C}^n \setminus H$ ends the proof. □