Real root finding for determinants of linear matrices

Didier Henrion, Simone Naldi, Mohab Safey El Din

Real root finding for determinants of linear matrices

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

October 27, 2014

Abstract

Let $A_0, A_1, \ldots, A_n$ be given square matrices of size m with rational coefficients. The paper focuses on the exact computation of one point in each connected component of the real determinantal variety $\{x \in \mathbb{R}^n : \det(A_0 + x_1A_1 + \cdots + x_nA_n) = 0\}$. Such a problem finds applications in many areas such as control theory, computational geometry, optimization, etc. Using standard complexity results this problem can be solved using $m^{O(n)}$ arithmetic operations. Under some genericity assumptions on the coefficients of the matrices, we provide an algorithm solving this problem whose runtime is essentially quadratic in $\binom{n+m}{n}^3$. We also report on experiments with a computer implementation of this algorithm. Its practical performance illustrates the complexity estimates. In particular, we emphasize that for subfamilies of this problem where m is fixed, the complexity is polynomial in n.

Keywords

Computer algebra, real algebraic geometry, determinantal varieties.

1 Introduction

1.1 Problem statement

Let $A_0, A_1, \ldots, A_n$ be given square matrices of size m with coefficients in the field of rationals $\mathbb{Q}$. Consider the affine map defined as

$$x = (x_1, \ldots, x_n) \mapsto A(x) = A_0 + x_1A_1 + \cdots + x_nA_n.$$

Consistently with the technical literature, we use the terminology *linear matrix* to refer to $A(x)$, even though the constant term A_0 is not necessarily zero. The determinant of

[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.

$A(x)$, denoted by $\det A(x)$, lies in the polynomial ring $\mathbb{Q}[x]$ and it has degree at most m. This polynomial defines the complex *determinantal variety*

$$\mathcal{D} := \big\{ x \in \mathbb{C}^n \ : \ \det A(x) = 0 \big\}.$$

In other words, $\mathcal{D} \subset \mathbb{C}^n$ is the set of complex vectors x at which $\mathrm{rank} A(x) \leq m-1$. The goal of this paper is to provide a *computer algebra algorithm* with explicit complexity estimates for computing at least one point in each connected component of the *real* determinantal variety $\mathcal{D} \cap \mathbb{R}^n$.

1.2 Motivations

First notice that when $n = 1$ our problem is called the real algebraic eigenvalue problem [44], and hence that the case $n > 1$ can be seen as a multivariate generalization.

Non-symmetric square matrices depending linearly on parameters arise in many problems of systems control and signal processing. For example, the Hurwitz matrix is used in stability criteria for systems described by linear ordinary differential equations, and vanishing of the determinant of the Hurwitz matrix corresponds to a bifurcation between stability and instability, see e.g. [6]. Alternatively, finding points on the real determinantal variety of the Hurwitz matrix amounts to finding parameters (e.g. corresponding to a feedback control law, or to structured uncertainty affecting the system) corresponding to a system configuration at the border of stability.

Another classical example of non-symmetric square linear matrix arising in signals and systems is the Sylvester matrix ruling controllability of a linear differential equation. In this context, vanishing of the determinant of the Sylvester matrix corresponds to a loss of controllability of the underlying system [31].

Linear matrices and optimization on determinantal varieties arise also in statistics [13, 29] and in computational algebraic geometry [14].

Under the assumption that the matrices $A_0, \ldots, A_n$ are symmetric, the matrix $A(x)$ is symmetric, and hence it has only real eigenvalues for all $x \in \mathbb{R}^n$. The condition $A(x) \succeq 0$, meaning that $A(x)$ is positive semidefinite, is called a *linear matrix inequality*, or LMI. It is a convex condition on the space of variables x which appears frequently in diverse problems of applied mathematics and especially in systems control theory, see e.g. [10]. A classical example is the Lyapunov stability condition for a linear ordinary differential equation which is an LMI in the parameters of a Lyapunov function (a certificate or proof of stability) depending quadratically on the system state.

When the matrix $A(x)$ is symmetric, the set

$$\mathcal{S} = \big\{ x \in \mathbb{R}^n \ \big| \ A(x) \succeq 0 \big\} \tag{1}$$

is called a *spectrahedron*. Spectrahedra are affine sections of the cone of positive semidefinite matrices and they represent closed convex basic semialgebraic sets, i.e. convex sets that can be defined by the common nonnegativity locus of a finite set of polynomials; they are the object of active studies mainly in optimization theory, real algebraic geometry and

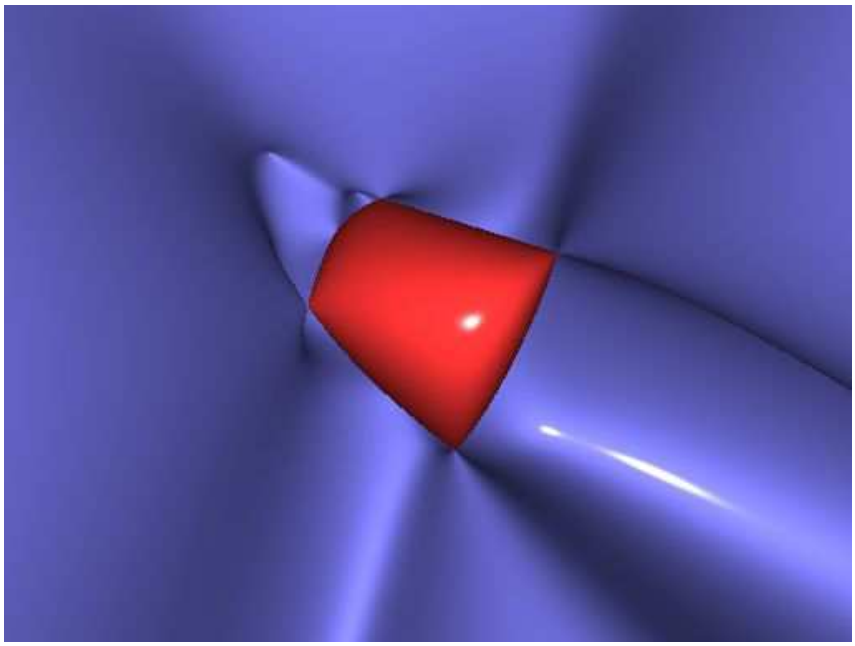

Figure 1: A spectrahedron (red) with its real determinantal variety.

control theory [33, 32, 9]. Following a question posed in [36, Section 4.3.1], the authors of [28] conjectured that every convex semialgebraic set is the projection of a spectrahedron. On Figure 1 is represented a spectrahedron (for $n = 3$ and $m = 5$) together with its real determinantal variety.

The minimization of a given function, for example a polynomial, over real convex sets is a central problem in optimization theory. If the function is linear and the set is a spectrahedron, this is exactly the aim of *semidefinite programming* (SDP), see [8]. If the input data of a semidefinite program are defined over $\mathbb{Q}$, the solutions are algebraic numbers, and the authors in [37] investigated their algebraic degree: giving explicit formulas or bounds for this value is a measure of the complexity of the given program.

Convex LMIs and SDP are also widely used for solving nonconvex polynomial optimization problems. Indeed, these optimization problems are linearized in the space of moments of nonnegative measures (which is infinite-dimensional) and a suitable sequence of LMI relaxations, or truncations (the so-called *Lasserre hierarchy*), that can be solved via SDP, provides the solution to the original problem. The feasible set of every truncated problem is a spectrahedron in the space of moments, for more details see [33, 32] and references therein.

So far, the problem of (deciding the existence and) computing such solutions has been addressed via several numerical methods, the most successful of which are primal-dual interior-point algorithms [8] implemented in *floating-point arithmetic* in different SDP solvers [35].

In this paper, the problem of computing points on spectrahedra is linked to polynomial systems solving over the reals. In fact, we are interested in the developement of an *exact computer algebra* algorithm to compute real points on hypersurfaces defined by the zero locus of determinants of affine matrix expressions. By exact algorithm we mean that

we do not content ourselves with approximate floating-point computations. Our main motivation starts from the geometrical aspects of SDP as explained above: boundaries of spectrahedra are subsets of determinantal hypersurfaces, and so solving this problem *efficiently* is a necessary step to address the associated positivity problem $A(x) \succeq 0$, since the rank of the matrix $A(x)$ at a point in the boundary of the spectrahedron $\mathcal{S}$ drops at least by one, while a point in the interior corresponds to a positive definite matrix. Finding such a point is a certificate of strict feasibility.

1.3 State of the art

Modern computer algebra algorithms for solving our problem require at most $m^{O(n)}$ arithmetic operations in $\mathbb{Q}$, see [7, Ch.11, Par.6] and references therein. The core idea is to reduce the input problem to a polynomial optimization problem whose set of optimizers is expected to be finite and to meet every connected component of the solution set under study. Such a reduction must be done carefully, especially for unbounded sets or singular situations. So far, it is an open problem to get a competitive implementation of the algorithms in [7]: unbounded and singular cases imply algebraic manipulations that have no impact on the complexity class but require to work over Puiseux series fields, and this increases the constant hidden by the big-O notation in the exponent.

During the past decade, tremendous efforts have been made to obtain algorithms that are essentially quadratic in m^n when dealing with one n-variate polynomial equation of degree m, see e.g. [2, 1, 4, 3, 41]. The goal is to get an implementation that reflects the theoretical complexity gains. Most of these algorithms are probabilistic: some random choices independent of the input are performed to ensure genericity properties. Our contribution shares these features and it is inspired by some geometric ideas in [41].

A main limitation is that the algorithms in [41] are dedicated to the smooth case. In our case, it turns out that $\mathcal{D}$ is in general a singular variety – see e.g. [11] and recall Figure 1 – which makes our problem more difficult from a geometric point of view.

Algorithms in [5] deal with singular situations but do not return sample points in the connected components that are contained in the singular locus of the variety. As a consequence, one cannot use them to decide the emptiness of $\mathcal{D} \cap \mathbb{R}^n$. The algorithm in [40] may be used but it suffers from an extra-cost, since it requires essentially m^{4n} arithmetic operations.

Moreover, in [21, 23, 24], the authors have developed algorithms and complexity estimates to isolate the real solutions of determinantal systems (see also [22] for related works on a bilinear setting). Beyond the interest of solving our problem for the aforementioned applications, it is of interest to extend these works to the real and positive dimensional case.

In practice, one can observe that, when a determinantal equation is given as input to software implementing singly exponential algorithms [39], its behaviour is significantly different and worse than the one observed on generic equations.

1.4 Basic definitions

Before describing the main results of this paper and the basic ideas on which they rely, we need to introduce some notations and basic definitions that are used further. We refer to [38, 43] for details.

We use the notations $\mathbb{Q}_* := \mathbb{Q} \setminus \{0\}$ and $\mathbb{C}_* := \mathbb{C} \setminus \{0\}$. We also denote $\mathbb{C}_*^m$ the set of non-zero complex vectors of length m.

A subset $\mathcal{V} \subset \mathbb{C}^n$ is said to be an *affine algebraic variety* defined over $\mathbb{Q}$ if there exists a system (i.e. a finite set) of polynomials $f = (f_1, \ldots, f_p) \in \mathbb{Q}[x]^p$ such that $\mathcal{V}$ is the locus of their common complex solutions, i.e. $\mathcal{V} = \{x \in \mathbb{C}^n \,:\, f(x) = 0\} = \{x \in \mathbb{C}^n \,:\, f_1(x) = \cdots = f_p(x) = 0\}$. In this case we write $\mathcal{V} = Z(f) = f^{-1}(0)$. Algebraic varieties are the closed sets in the Zariski topology, hence any set defined by a polynomial inequation $f \neq 0$ defines an open set for the Zariski topology. We also consider the closure $\overline{\mathcal{V}}$ of a set $\mathcal{V} \subset \mathbb{C}^n$ for the Zariski topology, that is the smallest algebraic subset of $\mathbb{C}^n$ containing $\mathcal{V}$.

The set of polynomials that vanish on an algebraic set $\mathcal{V}$ generates an ideal of $\mathbb{Q}[x]$ associated to $\mathcal{V}$, denoted by $I(\mathcal{V})$. This ideal is radical (i.e. $f^k \in I(\mathcal{V})$ for some integer k implies that $f \in I(\mathcal{V})$) and it is generated by a finite set of polynomials, say $f = (f_1, \ldots, f_p)$, and we write $I(\mathcal{V}) = \langle f_1, \ldots, f_p \rangle = \langle f \rangle$.

Let $\mathcal{V} \subset \mathbb{C}^n$ be an affine algebraic variety. Then the quotient ring $\mathbb{C}[\mathcal{V}] = \mathbb{C}[x]/I(\mathcal{V})$ is the *coordinate ring* of the variety $\mathcal{V}$: the elements of $\mathbb{C}[\mathcal{V}]$ are called *regular functions* on $\mathcal{V}$. A map $f\colon \mathcal{V} \to \mathcal{W} \subset \mathbb{C}^p$ defined over $\mathcal{V}$ with values in $\mathcal{W}$, such that $f \in \mathbb{C}[\mathcal{V}]^p$, is called a *regular map*, and if f is a bijection and its inverse is also a regular map, then f is an *isomorphism* of affine algebraic varieties.

Let $\mathrm{GL}_n(\mathbb{Q})$ denote the set of non-singular matrices of size n with coefficients in $\mathbb{Q}$. Its identity matrix is denoted by I_n. Given a matrix $M \in \mathrm{GL}_n(\mathbb{Q})$ and a polynomial system $x \in \mathbb{C}^n \mapsto f(x) \in \mathbb{C}^p$ we denote by $f \circ M$ the polynomial system $x \in \mathbb{C}^n \mapsto f(Mx) \in \mathbb{C}^p$. If $\mathcal{V} = Z(f)$, the image set $Z(f \circ M) = \{x \in \mathbb{C}^n : f(Mx) = 0\} = \{M^{-1}x \in \mathbb{C}^n : f(x) = 0\}$ is denoted by $M^{-1}\mathcal{V}$.

Let

$$\left(\frac{\partial f}{\partial x_k}\right) = \begin{pmatrix} \frac{\partial f_1}{\partial x_k} \\ \vdots \\ \frac{\partial f_p}{\partial x_k} \end{pmatrix}$$

denote the vector of $\mathbb{Q}[x]^p$ containing partial derivatives of f w.r.t. variable x_k, for some $k = 1, \ldots, n$. The co-dimension c of $\mathcal{V}$ is the maximum rank of the Jacobian matrix

$$Df := \left(\frac{\partial f}{\partial x_k}\right)_{k=1,\ldots,n} := \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & & \vdots \\ \frac{\partial f_p}{\partial x_1} & \cdots & \cdots & \frac{\partial f_p}{\partial x_n} \end{pmatrix}$$

evaluated at $x \in \mathcal{V}$. The dimension of $\mathcal{V} \subset \mathbb{C}^n$ is $n - c$.

Let $\mathcal{V} \subset \mathbb{C}^n$ be an algebraic set. We say that $\mathcal{V}$ is *irreducible* if it is not the union of two sets that are closed for the Zariski topology and strictly contained in $\mathcal{V}$. Otherwise $\mathcal{V}$ is the union of finitely many irreducible algebraic sets, its *irreducible components*.

Most of the time, we will consider *equidimensional* algebraic sets: these are algebraic sets whose irreducible components share the same dimension. An algebraic set $\mathcal{V}$ of dimension d is the union of equidimensional sets of dimensions $k = 0, 1, \ldots, d$: this is the so-called equidimensional decomposition of $\mathcal{V}$. Suppose that $\mathcal{V}$ is d-equidimensional, that is, equidimensional of dimension d. Given a polynomial system $f : \mathbb{C}^n \to \mathbb{C}^p$ and a point $x \in \mathcal{V} := Z(f)$, we say that x is *regular* if $Df(x)$ has rank $n - d$, and *singular* otherwise. An algebraic set whose points are all regular is called *smooth*, and *singular* otherwise. The set of singular points of an algebraic set $\mathcal{V}$ is denoted by $\operatorname{sing} \mathcal{V}$, while the set of its regular points is denoted by $\operatorname{reg} \mathcal{V}$.

Given a polynomial system $f : \mathbb{C}^n \to \mathbb{C}^p$, suppose that $\mathcal{V} = Z(f) \subset \mathbb{C}^n$ is a smooth d-equidimensional algebraic set, and let $g : \mathbb{C}^n \to \mathbb{C}^m$ be a polynomial system. Then the set of *critical points* of the restriction of g to $\mathcal{V}$ is defined by the zero set of f and the minors of size $n - d + m$ of the matrix

$$\begin{pmatrix} Df \\ Dg \end{pmatrix}$$

and we denote it by $\operatorname{crit}(g, f)$. In particular, the critical points of the restriction to $\mathcal{V}$ of the *projection map* $\pi_i \colon (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_i)$ is the zero set of f and the minors of size $n - d$ of the truncated Jacobian

$$\left(\frac{\partial f}{\partial x_k}\right)_{k=i+1,\ldots,n}$$

obtained by removing the first i columns in the Jacobian of f. The same definition applies to the equidimensional components of a generic algebraic set.

1.5 Data representation

1.5.1 Input

We assume that the linear matrix $A(x) = A_0 + x_1 A_1 + \cdots + x_n A_n$ is described via the square matrices $A_0, A_1, \ldots, A_n$ of size m with coefficients in $\mathbb{Q}$, which can also be understood as a point in $\mathbb{Q}^{(n+1)m^2}$. To refer to this input we use the short-hand notation A.

1.5.2 Output

Our goal is to compute exactly sample points in each connected component of the real variety $\mathcal{D} \cap \mathbb{R}^n$. Our algorithm consists of reducing the initial problem to isolating the real solutions of an algebraic set $\mathcal{Z} \subset \mathbb{C}^n$ of dimension at most 0. To this end, we compute a *rational parametrization* of $\mathcal{Z}$ that is given by a polynomial system $q = (q_0, q_1, \ldots, q_n, q_{n+1}) \in \mathbb{Q}[t]^{n+2}$ such that q_0, q_{n+1} are coprime (i.e. with constant greatest common divisor) and

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

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

Given a polynomial system defining a finite algebraic set $\mathcal{Z} \subset \mathbb{C}^n$, there exist many algorithms for computing such a parametrization of $\mathcal{Z}$. In the experiments reported in Section 6, we use implementations of algorithms based on Gröbner bases [16, 17] and the so-called change of ordering algorithms [20, 19] because they have the current best practical behavior. Nevertheless, our complexity analyses are based on the geometric resolution algorithm given in [27].

1.6 Main results and organization of the paper

The main result of the paper is sketched in the following. Its detailed statement is in Proposition 5 and it will be proved in Section 2.3.

There exists a probabilistic exact algorithm with input square matrices $A_0, A_1, \ldots, A_n$ of size m with coefficients in $\mathbb{Q}$, and output a rational parametrization encoding a finite set of points with non-empty intersection with each connected component of $\mathcal{D} \cap \mathbb{R}^n$. In case of success, the complexity of the algorithm is within

$$O^{\tilde{}}\left(n^2m^2(n+m)^5\binom{n+m}{n}^6\right)$$

arithmetic operations, where $O^{\tilde{}}(s) = O(s \log^k s)$ for some $k \in \mathbb{N}$.

Probabilistic aspects of this algorithm have been already mentioned and will be discussed in details in the next sections. In particular, the paper is organized as follows.

Section 2 contains a detailed description of the algorithm and of its subroutines. Moreover, its formal description is provided. Section 2.2 contains all regularity results, that is Propositions 1, 2 and 3, proved in the following sections. It also contains the proof of correctness of Theorem 4. As already mentioned, the proof of the main result is given in Section 2.3. *Section* 3 contains the proof of Proposition 1. *Section* 4 contains the proof of Proposition 2. *Section* 5 contains the proof of Proposition 3. Finally, *Section* 6 contains numerical data of experiments and some examples.

2 Algorithm: correctness and complexity

2.1 Description of the algorithm

Our algorithm is guaranteed to return an output under some genericity assumptions on the input. If the genericity assumptions are not satisfied, the algorithm raises an error. The algorithm consists of computing critical points of the restriction of linear projections to a given algebraic variety after a randomly chosen linear change of variables. These points are the solutions of a Lagrange system to be defined in this section.

2.1.1 Notations

Before giving an overview of the algorithm, we need to introduce some notations.

Change of variables. We denote by $A \circ M$ the affine map $x \mapsto A(Mx)$ obtained by applying a change of variables with matrix $M \in \mathrm{GL}_n(\mathbb{C})$. In particular $A = A \circ I_n$.

Incidence variety. Given a matrix $M \in \mathrm{GL}_n(\mathbb{C})$, define

$$\begin{array}{rccl} f(A \circ M): & \mathbb{C}^{n+m} & \to & \mathbb{C}^m \\ & (x, y) & \mapsto & A(Mx)y \end{array}$$

as a polynomial system of size m in the variables $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_m)$. Given $u = (u_1, \ldots, u_m) \in \mathbb{C}^m_*$, define

$$\begin{array}{rccl} f(A \circ M, u): & \mathbb{C}^{n+m} & \to & \mathbb{C}^{m+1} \\ & (x, y) & \mapsto & (A(Mx)y,\ u'y - 1) \end{array}$$

where $u'y := u_1y_1 + \cdots + u_my_m$ denotes the inner product of two vectors, and let $\mathcal{V}(A \circ M, u) := Z(f(A \circ M, u)) \subset \mathbb{C}^{n+m}$. We will see that under some *genericity assumptions*, algebraic variety $\mathcal{V}(A \circ M, u)$ is equidimensional and smooth.

Fiber. Given $w \in \mathbb{C}$, define

$$\begin{array}{rccl} f_w(A \circ M, u): & \mathbb{C}^{n+m} & \to & \mathbb{C}^{m+2} \\ & (x, y) & \mapsto & (A(Mx)y,\ u'y - 1,\ x_1 - w) \end{array}$$

and let $\mathcal{V}_w(A \circ M, u) := Z(f_w(A \circ M, u)) \subset \mathbb{C}^{n+m}$.

Lagrange system. Given $v \in \mathbb{C}$, let $J(x, y) := D_1 f(A \circ M, u)$ denote the matrix of size $m + 1$ by $n + m - 1$ obtained by removing the first column of the Jacobian matrix of $f(A \circ M, u)$, and define

$$\begin{array}{rccl} l(A \circ M, u, v): & \mathbb{C}^{n+2m+1} & \to & \mathbb{C}^{n+2m+1} \\ & (x, y, z) & \mapsto & (A(Mx)y,\ u'y - 1, J(x, y)'z,\ v \cdot z_{m+1} - 1) \end{array}$$

where variables $z = (z_1, \ldots, z_{m+1})$ stand for Lagrange multipliers, and let $\mathcal{Z}(A \circ M, u, v) := Z(l(A \circ M, u, v)) \subset \mathbb{C}^{n+2m+1}$.

Assumption G. We say that a polynomial system f of size p satisfies G if

- $\langle f \rangle$ is radical, and
- $Z(f)$ is either empty or smooth and equidimensional of co-dimension p.

We say that a linear map A satisfies G if the polynomial system $f(A, u)$ satisfies G for all $u \in \mathbb{C}^m_*$.

2.1.2 Formal description

The algorithm takes as input A which is assumed to satisfy G . Then, it chooses randomly $M \in \mathrm{GL}_n(\mathbb{Q})$, $u \in \mathbb{Q}^m$, $v \in \mathbb{Q}$ and $w \in \mathbb{Q}$ and computes a rational parametrization of $\mathcal{Z}(A \circ M, u, v) \subset \mathbb{C}^{n+2m+1}$. Its projection on the (x, y)-space is expected to be the set of critical points of the restriction to $\mathcal{V}(A \circ M, u)$ of the projection on the x_1-coordinate. Next, a recursive call is performed with input $A \circ M$ where the x_1-coordinate is instantiated to w. The new input should satisfy the same genericity properties as the one satisfied by A. Before giving a detailed description of the algorithm, we describe basic subroutines required by our algorithm.

Main subroutines. The algorithm uses the following subroutines:

- IsSing: it takes as input a polynomial system with coefficients in $\mathbb{Q}$ and it returns false if the system satisfies G, and true otherwise;
- RatPar: it takes as input a polynomial system with coefficients in $\mathbb{Q}$ defining a finite set and it returns a rational parametrization of the set, as defined in Section 1.5.2.

It also uses the following subroutines that perform basic operations on rational parametrizations of finite sets:

- Image: it takes as input a rational parametrization of a finite set $\mathcal{Z} \subset \mathbb{C}^N$ and a matrix $M \in \mathrm{GL}_N(\mathbb{C})$ and it returns a rational parametrization of the image set $M^{-1}\mathcal{Z}$ corresponding to a change of variables;
- Union: it takes as input two rational parametrizations of finite sets $\mathcal{Z}_1, \mathcal{Z}_2$ and returns a rational parametrization of $\mathcal{Z}_1 \cup \mathcal{Z}_2$;
- Project: it takes as input a rational parametrization of a finite set $\mathcal{Z}$ and a subset of variables, and it computes a rational parametrization of the projection of $\mathcal{Z}$ on the linear subspace generated by these variables;
- Lift: it takes as input a rational parametrization of a finite set $\mathcal{Z} \subset \mathbb{C}^N$ and a number $w \in \mathbb{C}$, and it returns a rational parametrization of $\mathcal{Z}' = \{(x, w) : x \in \mathcal{Z}\} \subset \mathbb{C}^{N+1}$.

We can now describe more precisely our algorithm RealDet. It uses a recursive subroutine RealDetRec that takes as input A satisfying G and returns a rational parametrization of a finite set which meets all connected components of $\mathcal{D} \cap \mathbb{R}^n$.

RealDetRec(A):

1. If $n = 1$ then return $(1, t, \det A(t))$;
2. Choose randomly
   - $M \in \mathrm{GL}_n(\mathbb{Q})$
   - $u = (u_1, \ldots, u_m) \in \mathbb{Q}^m$
   - $v \in \mathbb{Q}$

- $w \in \mathbb{Q}$;

3. $\mathsf{P} = \mathsf{Project}(\mathsf{RatPar}(l(A \circ M, u, v)), (x_1, \ldots, x_n))$;
4. $\mathsf{Q} = \mathsf{RealDetRec}(\mathsf{Substitute}(x_1 = w, A \circ M)))$;
5. $\mathsf{Q} = \mathsf{Lift}(\mathsf{Q}, w)$;
6. return $\mathsf{Image}(\mathsf{Union}(\mathsf{Q}, \mathsf{P}), M^{-1})$.

The main algorithm RealDet checks that the input satisfies G in which case it calls RealDetRec.

RealDet(A):

1. Choose randomly $u \in (\mathbb{Q}_*)^m$;
2. If IsSing($f(A, u)$) then output an error message saying that the genericity assumptions are not satisfied;
3. else return RealDetRec(A).

2.2 Proof of correctness

It is immediate that it is sufficient to prove the correctness of RealDetRec. This algorithm takes as input an affine map A satisfying G.

The result below shows that Assumption G is *generic* in the sense that there a exists a non-empty Zariski open set of $\mathbb{C}^{m^2(n+1)}$ contained in the set of linear matrices satisfying G. It is also useful to ensure that recursive calls are valid, i.e. the inputs in recursive calls satisfy the genericity assumption. The proof is given in Section 3.

Proposition 1 *Let $u = (u_1, \ldots, u_m) \in \mathbb{Q}_*^m$.*

1. *There exists a non-empty Zariski open set $\mathscr{A} \subset \mathbb{C}^{m^2(n+1)}$ such that for all $A \in \mathscr{A}$, $f(A, u)$ satisfies* G.
2. *If $A \in \mathscr{A}$ there exists a non-empty Zariski open set $\mathscr{W} \subset \mathbb{C}$ such that for any $w \in \mathscr{W}$ $f_w(A, u)$ satisfies* G.

Note that random choices are performed by algorithm RealDetRec at Step 2. These are needed to ensure some genericity properties. The first one ensures that set $\mathscr{Z}(A \circ M, u, v)$ is finite; it is proved in Section 4.

Proposition 2 *Let $u = (u_1, \ldots, u_m) \in \mathbb{Q}^m$, and assume that $A \in \mathscr{A}$. Then there exist two non-empty Zariski open sets $\mathscr{M}_1 \subset \mathrm{GL}_n(\mathbb{C})$ and $\mathscr{V} \subset \mathbb{C}$ such that for all $M \in \mathscr{M}_1 \cap \mathbb{Q}^{m \times m}$ and $v \in \mathscr{V} \cap \mathbb{Q}$, the following properties hold:*

1. *$\mathcal{Z}(A \circ M, u, v)$ is a finite set;*
2. *the Jacobian matrix $Dl(A \circ M, u, v)$ has maximal rank at any point of $\mathcal{Z}(A \circ M, u, v)$;*
3. *the projection of $\mathcal{Z}(A \circ M, u, v)$ on the (x, y)-space contains the set of critical points of the restriction to $\mathcal{V}(A \circ M, u)$ of the projection on the x_1-coordinate.*

The proposition below states that, for $M \in \mathrm{GL}_n(\mathbb{Q})$ generically chosen, and for any connected component $\mathcal{C}$ of $\mathcal{D} \cap \mathbb{R}^n$, $\pi_i(M^{-1}\mathcal{C})$ is closed for $i = 1, \ldots, n-1$. This is proved in Section 5.

Proposition 3 *Assume that $A \in \mathscr{A}$. Then there exist a non-empty Zariski open set $\mathscr{M}_2 \subset \mathrm{GL}_n(\mathbb{C})$ and a non-empty Zariski open set $\mathscr{U} \subset \mathbb{C}^m$ such that for any $M \in \mathscr{M}_2 \cap \mathbb{Q}^{n \times n}$, $u \in \mathscr{U} \cap \mathbb{Q}^m$ and any connected component $\mathcal{C}$ of $\mathcal{D} \cap \mathbb{R}^n$, the following holds:*

1. *for $i = 1, \ldots, n-1$, $\pi_i(M^{-1}\mathcal{C})$ is closed for the Euclidean topology;*
2. *for any $w \in \mathbb{R}$ lying on the boundary of $\pi_1(M^{-1}\mathcal{C})$, $\pi_1^{-1}(w) \cap M^{-1}\mathcal{C}$ is finite and there exists $(x, y) \in \mathbb{R}^n \times \mathbb{R}^m$ such that $(x, y) \in \mathcal{V}(A \circ M, u)$ and $\pi_1(x, y) = w$.*

Note that, starting with an n-variate affine map, there are n calls to RealDetRec, among which $n-1$ are recursive.

The random choices performed at Step 2 of every recursive call to RealDetRec can be organized in an array

$$\big((M^{(1)}, u^{(1)}, v^{(1)}, w^{(1)}), \ldots, (M^{(n-1)}, u^{(n-1)}, v^{(n-1)}, w^{(n-1)})\big) \tag{2}$$

where the upperscripts indicate the depth of the recursion. There are $n-1$ choices of these data because when $n = 1$ the recursive subroutine directly returns a rational parametrization without making such a choice. To ensure the correctness of RealDetRec, we need to assume that these choices are random enough so that data $(M^{(j)}, u^{(j)}, v^{(j)}, w^{(j)})$ lie in some prescribed non-empty Zariski open set $\mathscr{O}^{(j)}$ for $j = 1, \ldots, n-1$ as suggested by the previous propositions. Because of the recursive calls, *a priori* the set $\mathscr{O}^{(j)}$ depends on the previous choices. This is formalized by the following assumption.

Assumption H. We use the notations for sets introduced in Propositions 1, 2, 3, with the upperscript (j) to indicate the depth of recursion. We say that H holds if the array (2) satisfies the following conditions:

- $M^{(j)} \in \mathscr{M}_1^{(j)} \cap \mathscr{M}_2^{(j)} \cap \mathbb{Q}^{n \times n}$, for $j = 1, \ldots, n-1$;
- $u \in \mathscr{U}^{(j)} \cap (\mathbb{Q})^m$ for $j = 1, \ldots, n-1$;
- $v^{(j)} \in \mathscr{V}^{(j)} \cap \mathbb{Q}$, for $j = 1, \ldots, n-1$;
- $w^{(j)} \in \mathscr{W}^{(j)} \cap \mathbb{Q}$, for $j = 1, \ldots, n-1$.

We can now prove the following correctness statement.

Theorem 4 *Assume that $A \in \mathscr{A}$ and that* H *holds. Then,* RealDet(A) *returns a rational parametrization encoding a finite set of points with non-empty intersection with each connected component of $\mathcal{D} \cap \mathbb{R}^n$.*

Proof : Our reasoning is by induction on n, the number of variables. We start with the initialization. When $n = 1$, $\mathcal{D} \subset \mathbb{C}$ is finite. Then a rational parametrization of $\mathcal{D}$ is the triple $(1, t, \det A(t))$, which is the output result. Now, our induction assumption is that for any linear map $x \mapsto A(x) = A_0 + x_1 A_1 + \cdots + x_{n-1} A_{n-1}$ that satisfies G, the algorithm RealDetRec returns a correct answer provided that H holds.

Now, let A be a linear map and let $\mathcal{C}$ be a connected component of $\mathcal{D} \cap \mathbb{R}^n$. We let M, u, v and w be respectively the matrix, vectors and rational number chosen at Step 2 of RealDetRec, with input A.

First assume that the projection on the x_1-coordinate of $M^{-1}\mathcal{C}$ is the whole x_1-axis. Since A satisfies G, we deduce that $A \circ M$ satisfies G. Since H holds, we conclude by Proposition 1 that $f_w(A \circ M, u)$ generates a radical ideal and defines an algebraic variety which is either empty or smooth $(n-2)$-equidimensional.

Since, by assumption, $\pi_1(M^{-1}\mathcal{C})$ is the whole x_1-axis, there exists a connected component $\mathcal{C}'$ of the solution set of $f_w(A \circ M, u)$ such that $\{(w, x) \mid x \in \mathcal{C}'\}$ is contained in $M^{-1}\mathcal{C}$. In other words, the input of RealDetRec at Step 4 satisfies G and it is sufficient to compute sample points in each connected component of the solution set of $f_w(A \circ M, u)$ to obtain a sample point in $\mathcal{C}$. Correctness follows from the induction assumption which implies that RealDetRec computes at least one point in each connected component of the algebraic set defined by $f_w(A \circ M, u)$.

Now, assume that the projection π_1 on the x_1-coordinate of $M^{-1}\mathcal{C}$ is not the whole x_1-axis. Since H is satisfied, we deduce by Proposition 3 that $\pi_1(M^{-1}\mathcal{C})$ is closed for the Euclidean topology. Since $\pi_1(M^{-1}\mathcal{C}) \neq \mathbb{R}$ by assumption and since $\pi_1(M^{-1}\mathcal{C})$ is closed, there exists $x = (x_1, \ldots, x_n) \in M^{-1}\mathcal{C}$ such that $w = x_1$ lies in the boundary of $\pi_1(M^{-1}\mathcal{C})$. Without loss of generality, we assume below that $\pi_1(M^{-1}\mathcal{C})$ is contained in $[w, +\infty[$.

Recall that H holds. Then, by Proposition 3, $\pi_1^{-1}(w) \cap M^{-1}\mathcal{C}$ is finite and for all $x \in \pi_1^{-1}(w) \cap M^{-1}\mathcal{C}$ there exists $y \in \mathbb{R}^m$ such that $(x, y) \in \mathcal{V}(A \circ M, u)$.

Below, we reuse the notations of the algorithm and we prove that there exists $z \in \mathbb{C}^{m+1}$ such that (x, y, z) is a point lying in $\mathcal{Z}(A \circ M, u, v)$. Combined with Proposition 2, we also deduce that the above polynomial system defines a finite set which contains (x, y, z). Thus, the calls to RatPar and Project are valid and (x, y, z) lies in the finite set of points computed at Step 3 of RealDetRec. Correctness of the algorithm follows straightforwardly.

Thus, it remains to prove that there exists $z \in \mathbb{C}^{m+1}$ such that (x, y, z) lies in $\mathcal{Z}(A \circ M, u, v)$. Let $M^{-1}\mathcal{C}'$ be the connected component of $\mathcal{V}(A \circ M, u) \cap \mathbb{R}^{n+m}$ which contains (x, y). We claim that $w = \pi_1(x, y)$ lies on the boundary of $\pi_1(M^{-1}\mathcal{C}')$.

Indeed, assume by contradiction that this is not the case, i.e. $w \in \pi_1(M^{-1}\mathcal{C}')$ but does not lie in the boundary of $\pi_1(M^{-1}\mathcal{C}')$. This implies that there exists $\varepsilon > 0$ such that the interval $(w - \varepsilon, w + \varepsilon)$ lies in $\pi_1(M^{-1}\mathcal{C}')$. As a consequence, there exists $(x', y') \in M^{-1}\mathcal{C}'$ such that that $\pi_1(x', y') < w$. Moreover, since $(x', y') \in M^{-1}\mathcal{C}'$ and $M^{-1}\mathcal{C}'$ is connected, we deduce that there exists a continuous semi-algebraic function $\tau \colon [0, 1] \to M^{-1}\mathcal{C}'$ with

$\tau(0) = (x, y)$ and $\tau(1) = (x', y')$. Let π_x be the projection map $\pi_x(x, y) = x$. Since π_x and τ are continuous semi-algebraic functions, $\gamma = \pi_x \circ \tau$ is continuous and semi-algebraic (since it is the composition of semi-algebraic continuous functions). Finally, note that $\gamma(0) = x$ and $\gamma(1) = x'$; we deduce that $x' \in M^{-1}\mathcal{C}$ with $\pi_1(x') < w = \pi_1(x)$. This contradicts the fact that w lies in the boundary of $\pi_1(M^{-1}\mathcal{C})$ and that $\pi_1(M^{-1}\mathcal{C})$ lies in $[w, +\infty[$. We conclude that $w = \pi_1(x, y)$ lies on the boundary of $\pi_1(M^{-1}\mathcal{C}')$.

As a consequence of the implicit function theorem [7, Section 3.5], we deduce that (x, y) is a critical point of the restriction of the projection π_1 to $M^{-1}\mathcal{C}'$. Since $M^{-1}\mathcal{C}'$ is a connected component of $\mathcal{V}(A \circ M, u) \cap \mathbb{R}^n$ and since the input satisfies G, we deduce that the truncated Jacobian matrix $D_1 f(A \circ M, u)$ (defined jointly with the Lagrange system in paragraph 2.1.1) is rank defective at (x, y) (see [42, Sections 2.1.4 and 2.1.5]). Moreover, since H holds, we deduce by Proposition 2 that (x, y) lies in the projection of $\mathcal{Z}(A \circ M, u, v)$. Thus, there exists $z \in \mathbb{C}^{m+1}$ such that (x, y, z) lies in $\mathcal{Z}(A \circ M, u, v)$ as requested. □

2.3 Complexity analysis and degree bounds

In this section, we estimate the complexity of the algorithm RealDet and we give an explicit formula for a bound on the number of complex solutions computed by the algorithm.

We assume that G holds, so that we do not need to estimate the complexity of the subroutine IsSing and we focus on the complexity of the algorithm RealDetRec.

We assume in the sequel that H holds. On input A satisfying G, RealDetRec computes a rational parametrization of the solutions set of $l(A \circ M, u, v)$ (Step 3) and performs a recursive call with input Substitute$(x_1 = w, A \circ M)$ (Step 4). On input $l(A \circ M, u, v)$, our routine for computing rational parametrization of its solution set starts by building an equivalent system.

The complexity results stated below depend on degrees of geometric objects defined by systems which are equivalent to the Lagrange systems we consider. We need to introduce some notations.

The sequence of linear matrices that are considered during the recursive calls is denoted by $A^{(0)}, \ldots, A^{(n-1)}$, where $A^{(i)}$ is a linear matrix in $n - i$ variables; the systems $f(A^{(i)} \circ M^{(i)}, u^{(i)})$ for $0 \leq i \leq n - 1$ are respectively denoted by

$$f_i = (f_{i,1}, \ldots, f_{i,m+1})$$

where $f_{i,m+1} : y \mapsto y' u^{(i)} - 1$. Note that the f_i involve $n + m - i$ variables. The Lagrange systems $l(A^{(i)} \circ M^{(i)}, u^{(i)}, v^{(i)})$ are denoted by

$$l_i = (f_i, g_{i,1}, \ldots, g_{i,n+m-i})$$

where $g_{i,n+m-i} : z \mapsto v^{(i)} z_{n+m-i+1} - 1$.

Using $f_{i,m+1}$, one can eliminate one of the y-variables, say y_m, in f_i. We denote by

$$\tilde{f}_i = (\tilde{f}_{i,1}, \ldots, \tilde{f}_{i,m})$$

the polynomial system obtained this way. Recall that the polynomials $g_{i,1}, \ldots, g_{i,n+m-i}$ express that there is a nonzero vector in the left kernel of the truncated Jacobian matrix $D_1 f_i$. Hence, one can equivalently express the existence of a non-zero vector in the left kernel of the truncated Jacobian matrix $D_1 \tilde{f}_i$. This yields a new polynomial system

$$\tilde{l}_i := (\tilde{f}_{i,1}, \ldots, \tilde{f}_{i,m}, \tilde{g}_{i,m+1}, \ldots, \tilde{g}_{i,n-i-1}, \tilde{g}_{i,n-i}, \ldots, \tilde{g}_{i,n+2m-i-2}).$$

Note that since we have assumed that H holds, one can deduce using Proposition 2 that the Jacobian matrix $D\tilde{l}_i$ has maximal rank at any complex solution of $\tilde{l}_i$.

This new polynomial system contains:

- m polynomials which are bilinear in $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_{m-1})$;
- $m-1$ polynomials which are bilinear in $(x_1, \ldots, x_n)$ and $(z_1, \ldots, z_{m-1})$;
- $n-1$ polynomials which are bilinear in $(y_1, \ldots, y_{m-1})$ and $(z_1, \ldots, z_{m-1})$.

In the sequel, we denote by $\mathcal{V}_{i,j}$ the Zariski closure of the algebraic set defined by

$$\tilde{f}_{i,1}, \ldots, \tilde{f}_{i,j}, \qquad \text{when } 1 \leq j \leq m$$

and

$$\tilde{f}_{i,1}, \ldots, \tilde{f}_{i,m}, \tilde{g}_{i,m+1}, \ldots, \tilde{g}_{i,j} \qquad \text{when } m+1 \leq j \leq n+2m-i-2.$$

The algebraic set $\mathcal{W}_{i,j}$ is the subset of $\mathcal{V}_{i,j}$ at which the Jacobian matrix of its above defining system has maximal rank. For $0 \leq i \leq n-1$, we denote by

$$\delta_i = \max\{\deg \mathcal{W}_{i,j} \ : \ 1 \leq j \leq n+2m-i-2\}$$

and by δ the maximum of the δ_i. Remark that since H holds, Proposition 2 implies that $\mathcal{W}_{i,n+2m-i-2} = Z(\tilde{l}_i)$.

We start by estimating the complexity of the main subroutines called by RealDetRec. We prove the following result.

Proposition 5 *Assume that* H *holds. Then,* RealDetRec *outputs a rational parametrization whose real zero locus meets each connected component of* $\mathcal{D} \cap \mathbb{R}^n$ *within*

$$O^{\sim}\left(n^2 m^2 (n+m)^5 \delta^2\right)$$

arithmetic operations in $\mathbb{Q}$ *with* $\delta \leq \binom{n+m}{m}^3$ *and* $O^{\sim}(s) = O(s \cdot \log^k(s))$ *for some* $k \in \mathbb{N}$.

Assume that A satisfies G and that M, u and v lies in the non-empty Zariski open sets defined in Propositions 2 and 3.

Lemma 6 *Under the above notations and assumptions, there exists a probabilistic algorithm which, on input* l_i*, computes a rational parametrization of the complex solution set of it within*

$$O^{\sim}\left(n^2 m^2 (n+m)^5 \delta^2\right)$$

arithmetic operations in $\mathbb{Q}$ *with* $\delta \leq \binom{n+m}{m}^3$.

Proof of Proposition 5: Through its recursive calls, the algorithm RealDetRec computes rational parametrizations of the solution sets of the Lagrange systems $l_0, \ldots, l_{n-1}$.

Lemma 6 shows that these computations are done within

$$O^{\sim}\left((n+m)^2(nm^2+(n+m)^3)\delta^2\right)$$

arithmetic operations in $\mathbb{Q}$ with $\delta \leq \binom{n+m}{m}^3$. Since there are n Lagrange systems to solve, all these parametrizations are computed within

$$O^{\sim}\left(n^2m^2(n+m)^5\delta^2\right)$$

arithmetic operations in $\mathbb{Q}$. Note that in all systems $l_0, \ldots, l_{n-1}$ the number of variables is bounded by $n+2m+1$ and the cardinality of their solution set is bounded by δ.

Following [42, Lemma 10.1.3], the call to the routine Project at Step 3 requires at most $O^{\sim}((n+m)\delta^2)$ arithmetic operations in $\mathbb{Q}$.

Next, by [42, Lemma 10.1.1 and Lemma 10.1.3], the calls to the routines Image and Union and in Step 6 require respectively at most $O^{\sim}((n+m)^2\delta+(n+m)^3)$ and $O^{\sim}((n+m)\delta^2)$ arithmetic operations in $\mathbb{Q}$. Summing up all these complexity estimates yields to the announced complexity bounds. □

Proof of Lemma 6: It is sufficient to describe the proof for $l = l_0$ only. We use the geometric resolution algorithm given in [27] to compute a rational parametrization of the complex solution set of the system $\tilde{l}$ obtained following the construction in Paragraph 2.3. Note that since H holds by assumption, we deduce that $\tilde{l}$ is a reduced regular system, in the sense defined in the introduction of [27].

Note that all polynomials of $\tilde{l}$ have degree ≤ 2 and that evaluating $\tilde{l}$ requires $O^{\sim}(nm^2)$ arithmetic operations.

Thus, one can apply [27, Theorem 1]. When $\tilde{l}$ is a reduced regular sequence, it states that one can compute a rational parametrization of the complex solution set of $\tilde{l}$ in probabilistic time

$$O^{\sim}(\tilde{n}^2(\tilde{o}+\tilde{n}^3)\delta^2)$$

where

- $\tilde{n} = n+2m-2$ is the total number of variables involved in $\tilde{l}$,
- $\tilde{o}$ is the complexity of evaluating $\tilde{l}$,
- and δ is the quantity introduced in Paragraph 2.3.

We obtain that one can compute a rational parametrization of the complex solution set of $\tilde{l}$ in probabilistic time

$$O^{\sim}((n+m)^2(nm^2+(n+m)^3)\delta^2).$$

Our conclusion follows and the bound on δ is proved in the following lemma. □

Lemma 7 *Under the above notations and assumptions the following inequality holds:*

$$\delta \leq \binom{n+m}{m}^3.$$

Proof : To prove degree bounds on δ, we take into account the multi-linear structure in x, y, z of the intermediate systems

$$\tilde{f}_{i,1}, \ldots, \tilde{f}_{i,t}, \qquad \text{for } 1 \leq j \leq t$$

and

$$\tilde{f}_{i,1}, \ldots, \tilde{f}_{i,m}, \tilde{g}_{i,m+1}, \ldots, \tilde{g}_{i,m+t} \qquad \text{for } 1 \leq t \leq n+2m-i-2.$$

We define $\Delta(m,n;t)$ as follows:

- when $1 \leq t \leq m$, $\Delta(m,n;t)$ is the sum of the coefficients of the polynomial $(s_1+s_2)^t$ modulo the ideal generated by (s_1^{n+1}, s_2^m);
- when $m+1 \leq t \leq n+m-1$, $\Delta(m,n;t)$ is the sum of the coefficients of the polynomial $(s_1+s_2)^m(s_1+s_3)^{t-m}$ modulo the ideal generated by $(s_1^{n+1}, s_2^m, s_3^m)$;
- when $n+m \leq t \leq n+2m-2$, $\Delta(m,n;t)$ is the sum of the coefficients of the polynomial $(s_1+s_2)^m(s_1+s_3)^{n-1}(s_3+s_2)^{t-m-n+1}$ modulo the ideal generated by $(s_1^{n+1}, s_2^m, s_3^m)$.

By [42, Proposition 10.1.1], the degrees of *their components of highest dimension* is bounded by $\Delta(m,n;t)$. Immediate computations show that the following holds:

$$\Delta(m,n;t) = \begin{cases} \sum_{i=0}^{\min(n,t)} \binom{t}{i} & t \in \{1,\ldots,m\}, \\ \sum_{(i,j)\in\mathcal{F}_t} \binom{m}{i}\binom{t-m}{j} & t \in \{m+1,\ldots,n+m-1\}, \\ \sum_{(i,j,\ell)\in\mathcal{F}_t} \binom{m}{i}\binom{n-1}{j}\binom{t-m-n+1}{\ell} & t \in \{n+m,\ldots,n+2m-2\}. \end{cases}$$

for every m and n, where:

$$\mathcal{F}_t = \begin{cases} (i,j) \in \{1,\ldots,m\} \times \{0,\ldots,n-1\}, \\ 1 \leq i \leq \min(m,n), \\ \max(0,t-2m+1) \leq j \leq \min(t-m, i-1), \end{cases}$$

if $t \in \{m+1,\ldots,n+m-1\}$, and

$$\mathcal{F}_t = \begin{cases} (i,j,\ell) \in \{1,\ldots,m\} \times \{0,\ldots,n-1\} \times \{0,\ldots,t-m-n+1\}, \\ \max(0,t-2m+1) \leq j+\ell \leq n-1, \\ \max(1,t-2m+2) \leq i+\ell \leq \min(n,t-n+1). \end{cases}$$

if $t \in \{n+m,\ldots,n+2m-2\}$. Let us remark that relations defining $\mathcal{F}_{n+2m-2}$ become linear contraints, which yields the following equality for the case $t = n+2m-2$:

$$\Delta(m,n;n+2m-2) = \sum_{i=0}^{m-1} \binom{m}{n-i}\binom{n-1}{i}\binom{m-1}{i}. \tag{3}$$

One can easily check that for all $k \in \mathbb{N}$

$$\binom{n+m}{n}^k = \sum_{i_1,\ldots,i_k=0}^{n} \binom{m}{i_1}\binom{n}{i_1}\cdots\binom{m}{i_k}\binom{n}{i_k}.$$

Moreover, for all m, n and for $t \in \{1,\ldots,m\}$, $\Delta(m,n;t) \leq \Delta(m,n;t+1)$, and $\Delta(m,n;m)$ is bounded by $\binom{n+m}{n}$ because of the previous formula.

Let $t \in \{m+1,\ldots,n+m-1\}$. Then $\Delta(m,n;t) = \sum_{i=1}^{\min(m,n)} a_i \binom{m}{i}$ where

$$a_i = \sum_{j:(i,j)\in\mathcal{F}_t} \binom{t-m}{j} = \sum_{j=\max(0,t-2m+1)}^{\min(t-m,i-1)} \binom{t-m}{j} \leq \sum_{j=0}^{n} \binom{n}{i}\binom{m}{j}\binom{n}{j}.$$

and so $\Delta(m,n;t) \leq \binom{n+m}{n}^2$ for all $t \in \{m+1,\ldots,n+m-1\}$.

Finally, for $t \in \{n+m,\ldots,n+2m-2\}$, one gets

$$\Delta(m,n;t) \leq \sum_{i,j,\ell=0}^{n} \binom{m}{i}\binom{n-1}{j}\binom{t-m-n+1}{\ell} \leq \sum_{i,j,\ell=0}^{n} \binom{m}{i}\binom{n}{j}\binom{m}{\ell} \leq \binom{n+m}{n}^3.$$

□

2.3.1 Complexity of Project.

According to [42, Lemma 9.1.6], given a rational parametrization q defining a zero-dimensional set $\mathcal{Z} \subset \mathbb{C}^N$, there exists a probabilistic algorithm computing a rational parametrization q' of the projection $\pi_i(\mathcal{Z})$ whose complexity is within $\mathcal{O}^{\sim}(N \deg q^2)$ operations. We remark here that $\deg q$ is the cardinality of $\mathcal{Z}$ provided that q is square-free; if not, it is an upper bound. In the case of $\mathcal{Z}(A \circ M, u, v)$, we obtain from Lemma 7 that $\deg q \leq \binom{n+m}{n}^3$.

Lemma 8 *The complexity of* Project *in* RealDetRec *is*

$$\mathcal{O}^{\sim}\left((n+2m-2)\binom{n+m}{n}^6\right).$$

Proof : *It follows from the bound for δ of Lemma 7 and from [42, Lemma 9.1.6].* □

2.3.2 Complexity of Image, Union.

By [42, Lemma 9.1.1], given a rational parametrization q and a matrix $M \in \mathrm{GL}_N(\mathbb{Q})$, there exists an algorithm computing a rational parametrization q' such that $\mathcal{Z}(q') = M^{-1}\mathcal{Z}(q)$ using $\mathcal{O}^{\sim}(N^2\delta + N^3)$ operations. Moreover, by [42, Lemma 9.1.3] if q_1, q_2 are rational parametrizations with degree sum bounded by δ, a rational parametrization of $\mathcal{Z}(q_1) \cup \mathcal{Z}(q_2)$ can be computed in $\mathcal{O}^{\sim}(N\delta^2)$ operations.

Lemma 9 *The complexity of* Image *and* Union *in* RealDetRec *is*

$$\mathcal{O}^{\sim}\left((n+2m-2)^2\binom{n+m}{n}^3+(n+2m-2)^3+(n+2m-2)\binom{n+m}{n}^6\right).$$

Proof : *The proof of this fact follows straightforwardly from [42, Lemma 9.1.1], [42, Lemma 9.1.3] and Lemma 7.* □

2.3.3 A bound on the degree of the output

Let A be a $n-$variate linear matrix of size m and apply algorithm RealDet to A. Recall that the number $\Delta(m,n,n+2m-2)$ computed in (3) is a bound on the number of complex solutions computed by the first call of RealDetRec.

The following result, whose proof is straightforward, counts the maximum number of complex solutions computed by RealDet.

Lemma 10 *The number of complex solutions computed by* RealDet *with input a linear matrix A satisfying Assumption* G*, is upper-bounded by the number*

$$b(m,n)=\sum_{j=1}^{n}\Delta(m,j,j+2m-2)=\sum_{j=1}^{n}\sum_{i=0}^{m-1}\binom{m}{j-i}\binom{j-1}{i}\binom{m-1}{i}.$$

We remark the following facts:

- $\Delta(m,j,j+2m-2)=0$ if $j\geq 2m$;
- if $m=m_0$ is fixed, $n\mapsto b(m_0,n)$ is constant if $n\geq 2m_0$.

3 Regularity properties of the incidence variety

The aim of this section is to prove Proposition 1. To identify the linear map $x\mapsto A(x)=A_0+x_1A_1+\cdots+x_nA_n$ with a point in $\mathbb{C}^{m^2(n+1)}$, we denote by $a_{l,i,j}$ the entry of matrix A_l at row i and column j, for $l=0,1,\ldots,n$ and $i,j=1,\ldots,m$.

Proof of the first point of Proposition 1: Consider the polynomial map

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

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

$$\begin{array}{rccc} p_A: & \mathbb{C}^{n+m} & \longrightarrow & \mathbb{C}^{m+1} \\ & (x,y) & \longmapsto & p(x,y,A). \end{array}$$

Assume first that $Z(p)$ is empty. This is equivalent to saying that, for any $A\in\mathbb{C}^{m^2(n+1)}$, $\mathcal{V}(A,u):=Z(f(A,u))$ is empty. By the Nullstellensatz [12, Chap. 8], this implies that

for any $A \in \mathbb{C}^{m^2(n+1)}$, the ideal $I(\mathcal{V}(A,u)) = \langle f(A,u)\rangle = \langle 1\rangle$ is radical. We define $\mathscr{A} = \mathbb{C}^{(n+1)m^2}$ and conclude.

Assume that $Z(p)$ is non-empty. We prove below that there exists a non-empty Zariski open set $\mathscr{A} \subset \mathbb{C}^{m^2(n+1)}$ such that for any $A \in \mathscr{A}$, the Jacobian matrix $Df(A,u)$ has maximal rank at any point in $Z(p_A)$. This is sufficient to establish the requested property G since by the Jacobian criterion [15, Theorem 16.19] this implies that

- the ideal $\langle f(A,u)\rangle$ is radical;
- the algebraic set $\mathcal{V}(A,u)$ is either empty or smooth and equidimensional of codimension $m+1$ in $\mathbb{C}^{n+m}$.

To prove the existence of the aforementioned non-empty Zariski open set $\mathscr{A}$, we first need to prove that 0 is a regular value of p, i.e. at any point of the fiber $Z(p)$ the Jacobian matrix Dp with respect to variables x, y and $a_{\ell,i,j}$ has maximal rank. Take $(x,y,A) \in Z(p)$. It suffices to prove that there exists a maximal minor of $Df(A,u)$ which is not zero at (x,y,A).

Remark that, since y is a solution of the equation $u'y = 1$, there exists $1 \leq s \leq m$ such that $y_s \neq 0$. Moreover, since $u \neq 0$, there exists $1 \leq \ell \leq m$ such that $u_\ell \neq 0$. Now consider the submatrix of $Df(Au)$ obtained by selecting

- the partial derivatives with respect to y_ℓ where ℓ is as above;
- the partial derivatives with respect to $a_{0,r,s}$ for all $1 \leq r \leq m$ and for s as above.

Checking that this submatrix has maximal rank at (x,y,A) is straightforward since

- the partial derivatives of the entries of $A(x)y$ with respect to $a_{0,r,s}$ for $1 \leq r \leq m$ is the diagonal matrix with $y_s \neq 0$ on the diagonal;
- the partial derivative of the polynomial $u'y - 1$ with respect to y_ℓ is $u_\ell \neq 0$, while the partial derivatives of that polynomial with respect to $a_{0,r,s}$ are 0.

Thus, up to reordering the columns of this submatrix, it is triangular with non-zero entries on the diagonal. Finally, we conclude that 0 is a regular value of p. By Thom's Algebraic Weak Transversality theorem [42, Section 4.2] there exists a non-empty Zariski open set $\mathscr{A} \subset \mathbb{C}^{m^2(n+1)}$ such that, for every $A \in \mathscr{A}$, 0 is a regular value of the map p_A. This concludes the proof. □

Proof of the second point of Proposition 1: Let $A \in \mathscr{A}$ and consider the map

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

which is the restriction to $\mathcal{V}(A,u)$ of the projection on the first variable. Since $A \in \mathscr{A}$, the variety $\mathcal{V}(A,u)$ is either empty or smooth and equidimensional and by Sard's Lemma ([42, Section 4.2]) the image by π_1 of the set of critical points of π_1 is contained in an algebraic hypersurface of $\mathbb{C}$ (that is, a finite set). This implies that there exists a non-empty Zariski open set $\mathscr{W} \subset \mathbb{C}$ such that if $w \in \mathscr{W}$, at least one of the following fact holds:

- the set $\pi_1^{-1}(w) = \{(x, y) \in \mathcal{V}(A, u) \mid x_1 = w\}$ is empty: this fact implies that the system $f_w(A, u)$ defines the empty set, and that $\langle f_w(A, u)\rangle = \langle 1\rangle$, which is a radical ideal;
- for all $(x, y) \in \pi_1^{-1}(w)$, (x, y) is not a critical point of π_1; this fact implies that the Jacobian matrix of $f_w(A, u)$ has full rank at each point (x, y) in the zero set of $f_w(A, u)$, and so by the Jacobian criterion [15, Theorem 16.19] that $f_w(A, u)$ defines a radical ideal and its zero set is a smooth equidimensional algebraic set of codimension $m + 2$ in $\mathbb{C}^{n+m}$.

By this, we conclude that if $w \in \mathscr{W}$, the system $f_w(A, u)$ satisfies G. □

Example 11 *Consider the linear matrix*

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

whose real determinantal variety is the Cayley cubic surface with its four singular points $(x_1, x_2, x_3) \in \{(1, 1, 1), (1, -1, -1), (-1, 1, -1), (-1, -1, 1)\}$*, see Example 2 and Figure 3 in [37]. When evaluated at these points, A has rank one. The following* `Macaulay2` *code shows that the incidence variety is smooth.*

```
MyRand = () -> (((-1)^(random(ZZ)))*(random(QQ)))
R = QQ[x_1,x_2,x_3]
A = matrix{{1,x_1,x_2},{x_1,1,x_3},{x_2,x_3,1}}
D = ideal det A
dim D, degree D
SingD = ideal singularLocus D
dim SingD, degree SingD
S = QQ[x_1,x_2,x_3,y_1,y_2,y_3]
Y = matrix{{y_1},{y_2},{y_3}}
V = ideal(sub(A,S)*Y) + ideal(1-sum(3,i->MyRand()*(y_(i+1))))
dim V, degree V
SingV = ideal singularLocus V
dim SingV, degree SingV
```

The incidence variety in this example has dimension 2 *and degree* 7*.*

Example 12 *Consider the linear matrix*

$$A(x) = \begin{pmatrix} 1 + x_1 & x_2 & 0 & 0 \\ x_2 & 1 - x_1 & x_2 & 0 \\ 0 & x_2 & 2 + x_1 & x_2 \\ 0 & 0 & x_2 & 2 - x_1 \end{pmatrix}$$

whose real determinantal variety is a smooth quartic curve, the union of two nested ovals, see Figure 2. Here the incidence variety is a smooth variety of dimension 6 *and degree* 10*.*

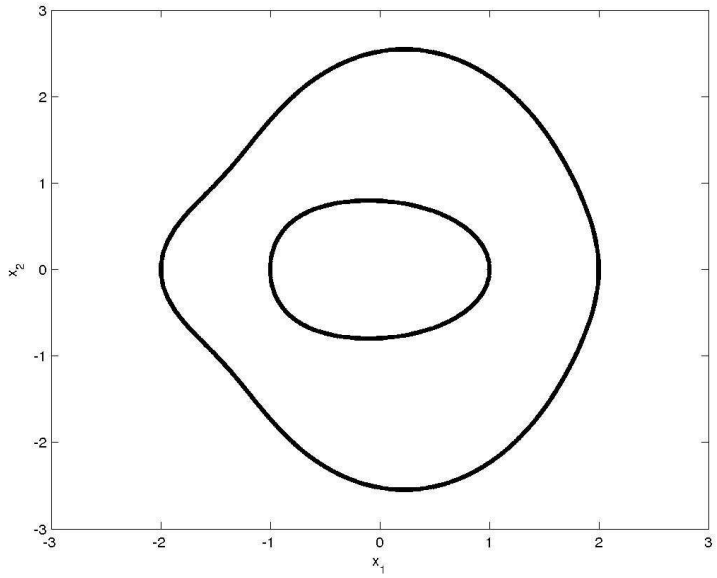

Figure 2: The smooth quartic curve of Example 12 with its two nested ovals.

4 Dimension properties of Lagrange systems

The aim of this Section is to prove Proposition 2.

There is some similarity between the statement of Proposition 2 and some properties of Lagrange systems given in [42, Chap. 8 and 9]. The main difference with [42] comes from the fact that here we ensure the finiteness of $\mathcal{Z}(A \circ M, u, v)$ with a change of variables that acts only on the x-coordinates. Consequently, this preserves the bilinear structure of the system $f(A \circ M, u)$.

Proof of Proposition 2: Since $A \in \mathscr{A}$, the polynomial system $f = f(A \circ M, u)$ satisfies G for all $M \in \mathrm{GL}_n(\mathbb{C})$ and $u \in \mathbb{C}_*^m$. We deduce that the $m+1$ by $n+m$ Jacobian matrix Df has maximal rank at all points $(x, y) \in \mathcal{V}(A \circ M, u)$.

In the sequel, we denote by $D_x f$ (resp. $D_y f$) the submatrix of Df obtained by removing all partial derivatives with respect to y (resp. x).

Let $z = (z_1, \ldots, z_{m+2})$ and $w = (w_1, \ldots, w_n)$, and denote by $g = (g_1, \ldots, g_n)$ (resp. $h = (h_1, \ldots, h_m)$) the first n (resp. last m) coordinates of the row vector

$$z' \begin{pmatrix} D_x f & D_y f \\ w_1, \ldots, w_n & 0 \cdots 0 \end{pmatrix}.$$

Remark that h does not depend on w or z_{m+2}. Remark also that since f satisfies G, the polynomial system f, g, h defines the critical points of the projection map

$$\pi_w \colon (x, y) \mapsto w_1 x_1 + \ldots + w_n x_n.$$

Now, consider the map

$$\begin{array}{rccc} p: & \mathbb{C}^n \times \mathbb{C}^m \times \mathbb{C}^{m+2} \times \mathbb{C} \times \mathbb{C}^n & \longrightarrow & \mathbb{C}^{m+1} \times \mathbb{C}^n \times \mathbb{C}^m \times \mathbb{C} \\ & (x, y, z, v, w) & \longmapsto & (f, g, h, v z_{m+1} - 1) \end{array}$$

and the map

$$q: \begin{array}{ccc} \mathbb{C}^n \times \mathbb{C}^m \times \mathbb{C}_*^{m+2} \times \mathbb{C}^n & \longrightarrow & \mathbb{C}^{m+1} \times \mathbb{C}^n \times \mathbb{C}^m \\ (x, y, z, w) & \longmapsto & (f, g, h) \end{array}$$

and, for a given $w \in \mathbb{C}_*^n$, the set $\mathcal{W}_w(A, u) = Z(q) \subset \mathbb{C}^n \times \mathbb{C}^m \times \mathbb{C}_*^{m+2}$. Finally, for given $v \in \mathbb{C}$ and $w \in \mathbb{C}_*^n$, consider the polynomial map

$$p_{v,w}: \begin{array}{ccc} \mathbb{C}^n \times \mathbb{C}^m \times \mathbb{C}^{m+2} & \longrightarrow & \mathbb{C}^{m+1} \times \mathbb{C}^n \times \mathbb{C}^m \times \mathbb{C} \\ (x, y, z) & \longmapsto & (f, g, h, vz_{m+1} - 1) \end{array}$$

and the corresponding algebraic variety $\mathcal{W}_{v,w}(A, u) := Z(p_{v,w})$.

Assume for the moment the following result whose proof is given later on.

Lemma 13 *Under the above notations and assumptions, there exist non-empty Zariski open sets $\mathscr{V} \subset \mathbb{C}$ and $\mathscr{W} \subset \mathbb{C}^n$ such that for all $v \in \mathscr{V}$ and $w \in \mathscr{W}$, the following properties hold:*

(a) $\mathcal{W}_{v,w}$ is a finite set;

(b) the Jacobian matrix associated to $p_{v,w}$ has maximal rank at any point of $\mathcal{W}_{v,w}$;

(b') the Jacobian matrix associated to q has maximal rank at any point of $\mathcal{W}_w$;

(c) the projection of $\mathcal{W}_{v,w}$ on the (x, y)-space contains the set of critical points of the restriction of the projection $\pi_w : (x_1, \ldots, x_n) \to w_1x_1 + \cdots + w_nx_n$ to $\mathcal{V}$.

Now, let $\mathscr{M}_1 \subset \mathrm{GL}_n(\mathbb{C})$ be the set of invertible matrices M such that the first row w' of M^{-1} lies in the set $\mathscr{W}$ given in Lemma 13. This is a non-empty Zariski open set of $\mathrm{GL}_n(\mathbb{C})$ since the entries of M^{-1} are rational functions of the entries of M. Let $\mathscr{V} \subset \mathbb{C}$ be the non-empty Zariski open set given by Lemma 13 and let $v \in \mathscr{V}$.

Let $e_1' = (1, 0, \ldots, 0) \in \mathbb{Q}^n$ and for all $M \in \mathrm{GL}_n(\mathbb{C})$, let

$$\tilde{M} := \begin{pmatrix} M & \mathbf{0} \\ \mathbf{0} & I_k \end{pmatrix}.$$

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

$$\begin{pmatrix} Df(A \circ M, u) \\ e_1' \quad 0 \cdots 0 \end{pmatrix} = \begin{pmatrix} Df(A, u) \\ w' \quad 0 \cdots 0 \end{pmatrix} \tilde{M}.$$

We conclude that the set of solutions of the system

$$\left(f(A, u), \quad z' \begin{pmatrix} D_x f & D_y f \\ w' & 0 \cdots 0 \end{pmatrix}, \quad vz_{m+1} - 1 \right) \tag{4}$$

is the image by the map $(x, y) \mapsto \tilde{M}^{-1}(x, y)$ of the set $\mathcal{S}$ of solutions of the system

$$\left(f(A \circ M, u), \quad z' \begin{pmatrix} Df(A \circ M, u) \\ e_1' \quad 0 \cdots 0 \end{pmatrix}, \quad vz_{m+1} - 1 \right). \tag{5}$$

Now, let π be the projection that forgets the coordinate z_{m+2}. Remark that $\pi(\mathcal{S}) = \mathcal{Z}(A \circ M, u, v)$ and that π is a bijection. Moreover, it is an isomorphism of affine algebraic varieties, since if $(x, y, z) \in \mathcal{S}$, then its z_{m+2}-coordinate is obtained by evaluating a polynomial at $(x, y, z_1 \dots z_{m+1})$.

Thus, Property (a) of Lemma 13 implies that $\mathcal{S}$ and $\pi(\mathcal{S}) = \mathcal{Z}(A \circ M, u, v)$ are finite which proves Assertion (1) of Proposition 2.

Property (b) of Lemma 13 implies that the Jacobian matrix associated to (5) has maximal rank at any point of $\mathcal{S}$. Since we already observed that $\pi(\mathcal{S}) = \mathcal{Z}(A \circ M, u, v)$ and that the map is an isomorphism, Assertion (2) follows.

Assertion (3) is a straightforward consequence of Property (c) of Lemma 13. □

To end this section, it remains to prove Lemma 13.

Proof of Lemma 13: Assume first that $Z(p) = \emptyset$. Then, for all $v \in \mathbb{C}$ and $w \in \mathbb{C}^n_*$ the algebraic set $\mathcal{W}_{v,w}$ is empty; this implies Assertion (a) and (b).

To prove (c), it is sufficient to prove that the set of critical points of the restriction of the projection π_w to $\mathcal{V}(A, u)$ is empty. Assume by contradiction that there exists such a critical point (x, y). By definition, we conclude that the matrix

$$\begin{pmatrix} D_x f & D_y f \\ w' & 0 \cdots 0 \end{pmatrix}$$

is rank defective. This implies that there is non-zero vector in its left kernel which contradicts emptyness of $Z(p)$ and proves that Assertion (c) holds.

Now, assume that $Z(p)$ is non-empty and take $(x, y, z, v, w) \in Z(p)$. We claim that zero is a regular value for p. Indeed, by Thom's Algebraic Weak Transversality theorem [42, Sect. 4.2] there exist two non-empty Zariski open sets $\mathscr{V} \subset \mathbb{C}$ and $\mathscr{W} \subset \mathbb{C}^n$ such that if $v \in \mathscr{V}$ and $w \in \mathscr{W}$, the zero vector is a regular value of the map $p_{v,w}$.

This implies that the Jacobian matrix associated to $p_{v,w}$ has maximal rank at any point of $\mathcal{W}_{v,w}(A, u)$; this is assertion (b). By the Jacobian criterion [15, Theorem 16.19], we also deduce assertion (a), i.e. that $\mathcal{W}_{v,w}(A, u)$ is finite since here the rank of the Jacobian matrix equals the dimension of the ambient space.

We prove now the announced claim: zero is a regular value for p. To do that it is sufficient to prove that there exists a maximal minor of the Jacobian matrix of p which is non-zero at (x, y, z, v, w). Note that the following properties hold:

- polynomials of $f(A, u)$ vanish at (x, y) and thus $(x, y) \in \mathcal{V}(A, u)$;
- since $A \in \mathscr{A}$, by Proposition 1 the Jacobian matrix $D(f)$ has maximal rank at (x, y);
- by the previous point, $z_{m+2} \neq 0$: in fact, if $z_{m+2} = 0$, we would obtain that $(x, y, z_1 \dots z_{m+1})$ is a solution of

$$(z_1, \dots, z_{m+1})\ Df(A \circ M, u)\ = 0,$$

  that is Df has a rank defect at (x, y), which is a contradiction.

- since $vz_{m+1} - 1 = 0$, one obtains $z_{m+1} \neq 0$.

We can isolate the submatrix of Dp built with the following matrices:

- the non-singular submatrix of Df given by Proposition 1;
- the partial derivatives with respect to $w_1, \ldots, w_n$;
- the partial derivatives with respect to $u_1, \ldots, u_m$;
- the partial derivative with respect to v.

This matrix is full rank because:

- the submatrix of Df has full rank;
- the partial derivatives of g with respect to $w_1, \ldots, w_n$ produce a diagonal matrix, with $z_{m+2} \neq 0$ on the diagonal;
- the partial derivatives of h with respect to $u_1, \ldots, u_m$ produce a diagonal matrix, with $z_{m+1} \neq 0$ on the diagonal;
- the partial derivative of $vz_{m+1} - 1$ with respect to v is $z_{m+1} \neq 0$.

Thus, up to reordering the columns of this submatrix, and to applying row-columns operations, it is triangular with non-zero entries on the diagonal. Finally, we conclude that zero is a regular value of p as claimed.

The proof of Assertion (b') follows the same argumentation as the one of (b), distinguishing the cases where $Z(q)$ is empty or not and, in the latter case, using mutatis mutandis the matricial constructions and tools based on the use of Thom's Algebraic Weak Transversality theorem.

It remains to prove Assertion (c) when $Z(p)$ is non-empty. Let $w \in \mathscr{W}$. We claim that the set of critical points of the restriction of π_w to $\mathcal{V}(A, u)$ is finite. Indeed, by [42, Sect. 3.2], this set is the projection on the (x, y)-space of the solution set $\mathcal{S}$ of the polynomial system

$$\left(f, \quad z' \begin{pmatrix} D_x f & D_y f \\ w' & 0 \cdots 0 \end{pmatrix} \right)$$

where $z \neq 0$. Let (x, y, z) be in $\mathcal{S}$ (note that this implies that (x, y) is a critical point of the restriction of π_w to $\mathcal{V}(A, u)$). Then, Assertion (b') implies that the Jacobian matrix associated to the above polynomial equations has maximal rank at (x, y, z). By the Jacobian criterion, we deduce that $\mathcal{S}$ has dimension 1. Now, remark that the homogeneity of the equations in the z-variables implies that for all $\lambda \neq 0$, $(x, y, \lambda z)$ lies in $\mathcal{S}$. Using the Theorem on the Dimension of Fibers [43, Sect. 6.3, Theorem 7] we deduce that the projection on the (x, y)-space of $\mathcal{S}$ is finite as claimed and that for any critical point (x, y) of the restriction of π_w to $\mathcal{V}(A, u)$, $\mathcal{E}_{x,y} := \{z \mid (x, y, z) \in \mathcal{S}\}$ has dimension 1.

Now, recall that, by assumption, f satisfies G which implies that the matrix $[D_x f \quad D_y f]$ has maximal rank at any point of $\mathcal{V}(A,u)$. This implies that the z_{m+2}-coordinates of the vectors z in $\mathcal{E}_{x,y}$ are non-zero.

Now, the set of $v \in \mathbb{C}$ such that the hyperplane defined by $vz_{m+1} = 1$ has a transversal intersection with $\mathcal{E}_{x,y}$ is non-empty and Zariski open. In fact, suppose to consider the set V of (x,y,z,w) defined by the polynomial equations

$$z'Df = [w, 0] \qquad z_{m+1} = 0 \qquad f = 0.$$

The image of the projection of V on x is the determinantal variety, and so it has dimension $n-1$. At a generic point $x \in \mathcal{D}$ the rank of $A(x)$ is $m-1$. We straightforwardly deduce that there exists a unique $y \in \mathbb{C}^m$ such that $f(x,y) = 0$. Similarly, using $\mathsf{rank}A(x) = m-1$, we deduce that there exists a unique z, w such that

$$z'Df(x,y) = [w, 0] \qquad z_{m+1} = 0 \qquad f(x,y) = 0.$$

Hence, the fiber has dimension 0 and the set V has dimension $n-1$. Projecting this set in the space $\mathbb{C}^n$ of w, one obtains a constructible set of dimension $\leq n-1$: this means that there exists a polynomial in $\mathbb{C}[w_1, \ldots, w_n]$ which vanishes on the image of the projection. This proves that for generic choices of $w \in \mathbb{C}^n$, the coordinate z_{m+1} is different from 0.

Now, define by $\mathscr{V}_{x,y} \subset \mathbb{C}$ the non-empty Zariski open set such that if $v \in \mathscr{V}_{x,y}$ then the hyperplane defined by $vz_{m+1} = 1$ has a transversal intersection with $\mathcal{E}_{x,y}$. Defining $\mathscr{V}$ as the finite intersection of all $\mathscr{V}_{x,y}$ when (x,y) runs over the set of critical point of the restriction of π_w to $\mathcal{V}(A,u)$ ends the proof. □

5 Closure properties of projection maps

The goal of this section is to prove Proposition 3. We start by introducing some notations.

Notations 14 *For an algebraic set $\mathcal{Z} \subset \mathbb{C}^n$ of dimension d, we denote by $\Omega_i(\mathcal{Z})$ the i-equidimensional component of $\mathcal{Z}$, for $i = 0, 1, \ldots, d$.*

We denote by $\mathscr{S}(\mathcal{Z})$ the union of the following sets:

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

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

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

Now, take $M \in \mathrm{GL}_n(\mathbb{C})$ *and fix* $\mathcal{Z} \subset \mathbb{C}^n$ *algebraic set of dimension* d*. We define the collection of algebraic sets* $\{\mathcal{O}_i(M^{-1}\mathcal{Z})\}_{0\leq i\leq d}$ *with*

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

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 $X_1, \ldots, X_i$.

Note that Point (2) of $\mathsf{P}(\mathcal{Z})$ implies Point (1) (this is an immediate consequence of [43, Chap. 1.5.3]). The following result shows that Property $\mathsf{P}(\mathcal{Z})$ holds for a generic choice of the matrix M and it will be proved later on.

Proposition 15 *Let* $\mathcal{Z} \subset \mathbb{C}^n$ *be an algebraic set of dimension* d*. There exists a non-empty Zariski open set* $\mathscr{M}_2 \subset \mathrm{GL}_n(\mathbb{C})$ *such that for all* $M \in \mathscr{M}_2$*,* M *satisfies* $\mathsf{P}(\mathcal{Z})$*.*

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 $\pi_i(\mathcal{O}_{i-1}(\mathcal{Z}) \cap \mathcal{C})$. When there is no ambiguity on $\mathcal{Z}$, we simply write that Q_i holds.

The following result describes properties of projections of the connected components of the real counterpart of an algebraic set when property $\mathsf{P}(\mathcal{Z})$ holds.

Proposition 16 *Let* $\mathcal{Z} \subset \mathbb{C}^n$ *be an algebraic set of dimension* d *and* $M \in \mathrm{GL}_n(\mathbb{C}) \cap \mathbb{Q}^{n\times n}$*. If* M *satisfies* $\mathsf{P}(\mathcal{Z})$*, then* $\mathsf{Q}_1(M^{-1}\mathcal{Z}), \ldots, \mathsf{Q}_d(M^{-1}\mathcal{Z})$ *hold.*

The relationship of Noether position with closedness properties of connected components of real counterparts in algebraic sets and critical points is already exhibited and exploited in [41]. Actually, Propositions 15 and 16 are already proved in [41] under the assumption that $\mathcal{Z}$ is smooth and equidimensional. We cannot make this assumption in our context to prove Proposition 3 since $\mathcal{D}$ is generically singular. Thus, this Section can be seen as a strict generalization of [41].

As in [41], we use the notion of proper map. A map $p : \mathcal{U} \subset \mathbb{C}^n \to \mathbb{C}^i$ is *proper at* $y \in \mathbb{C}^i$ if and only if there exists a neighbourhood $\mathcal{B}$ of y such that $p^{-1}(\overline{\mathcal{B}}) \cap \mathcal{U}$ is closed and bounded where $\overline{\mathcal{B}}$ is the closure of $\mathcal{B}$ for the strong topology. We simply say that p is proper when it is proper at any point of $\mathbb{C}^i$.

Proof of Proposition 16: To keep notations simple, we suppose that I_n satisfies $\mathsf{P}(\mathcal{Z})$. Our reasoning is by decreasing induction on the index i. In the whole proof we also define the following function on $\mathcal{Z}$: we associate to $y \in \mathcal{Z}$ the value

$$J(y) = \min\big\{j \mid y \in \mathcal{O}_j\big\}.$$

We start by establishing that Q_d holds. Let $x \in \mathbb{R}^d$ be on the boundary of $\pi_d(\mathcal{C})$. By [30, Lemma 3.10], Property $\mathsf{P}(\mathcal{Z})$ implies that the map π_d restricted to $\mathcal{O}_d(\mathcal{Z})$ is proper, and so closed. We deduce that the restriction of π_d to $\mathcal{O}_d(\mathcal{Z}) \cap \mathcal{C} \cap \mathcal{Z} = \mathcal{O}_d(\mathcal{Z}) \cap \mathcal{C}$ is closed and that $x \in \pi_d(\mathcal{O}_d(\mathcal{Z}) \cap \mathcal{C})$. Let $y \in \mathcal{O}_d(\mathcal{Z}) \cap \mathcal{C}$ such that $\pi_d(y) = x$. If $J(y) \leq d-1$ our conclusion follows immediately. Suppose now that $J(y) = d$. This implies that $y \in \operatorname{reg} \Omega_d(\mathcal{Z})$. By the Implicit Function Theorem we conclude that y is a critical point of π_d and that $y \in \operatorname{crit}(\pi_d, \operatorname{reg}(\Omega_d(\mathcal{Z}))) \subset \mathscr{C}(\pi_d, \mathcal{Z}) \subset \mathcal{O}_{d-1}(\mathcal{Z})$, which is a contradiction since we assumed $J(y) = d$.

Suppose now that Q_{i+1} holds. We proceed in two steps:

1. First, we prove that the boundary of $\pi_i(\mathcal{C})$ is included in $\pi_i(\mathcal{O}_i(\mathcal{Z}) \cap \mathcal{C})$. Indeed, let $x \in \mathbb{R}^i$ be on the boundary of $\pi_i(\mathcal{C})$. Let $p\colon \mathbb{R}^{i+1} \to \mathbb{R}^i$ be the map sending $(x_1, \dots x_{i+1})$ to $(x_1, \dots x_i)$, so that $\pi_i = p \circ \pi_{i+1}$. For $r > 0$, let $\mathcal{B}_r$ be the ball of center x and radius r in $\mathbb{R}^i$ and $\mathcal{B}'_r = p^{-1}(\mathcal{B}_r)$. We claim that $\mathcal{B}'_r$ meets both $\pi_{i+1}(\mathcal{C})$ and its complementary in $\mathbb{R}^{i+1}$.

   Indeed this is a consequence of the following immediate equalities

   $$\pi_i^{-1}(\mathcal{B}_r) \cap \mathcal{C} = \pi_{i+1}^{-1} \circ p^{-1}(\mathcal{B}_r) \cap \mathcal{C} = \pi_{i+1}^{-1}(\mathcal{B}'_r) \cap \mathcal{C}$$

   and $\pi_i^{-1}(\mathcal{B}_r) \cap \mathcal{C} \neq \emptyset$ and $\mathcal{B}_r \cap \{\mathbb{R}^i \setminus \pi_i(\mathcal{C})\} \neq \emptyset$. Since $\mathcal{B}'_r$ is connected, $\mathcal{B}'_r$ meets also the boundary of $\pi_{i+1}(\mathcal{C})$. Since Q_{i+1} holds, for every $r > 0$ there exists $y_r \in \mathcal{O}_i(\mathcal{Z}) \cap \mathcal{C}$ such that $\pi_{i+1}(y_r) \in \mathcal{B}'_r$, and so $\pi_i(y_r) \in \mathcal{B}_r$. Thus, x lies in the closure of the image by π_i of the set $\mathcal{O}_i(\mathcal{Z}) \cap \mathcal{C}$. This image is closed and our claim follows.

2. Second, we prove that Q_i holds. Let $x \in \mathbb{R}^i$ be on the boundary of $\pi_i(\mathcal{C})$. From (1), we deduce that there exists $y \in \mathcal{O}_i(\mathcal{Z}) \cap \mathcal{C}$ such that $\pi_i(y) = x$. Suppose by contradiction that for all y as above, $J(y) = i$. Fix $y \in \mathcal{O}_i(\mathcal{Z}) \setminus \mathcal{O}_{i-1}(\mathcal{Z})$ such that $\pi_i(y) = x$. In particular, $y \in \mathcal{O}_i(\mathcal{Z}) \setminus \mathscr{S}(\mathcal{O}_i(\mathcal{Z}))$, and thus, we deduce that $y \in \operatorname{reg}(\Omega_i(\mathcal{O}_i))$. Next, since $x \in \pi_i(\Omega_i(\mathcal{O}_i) \cap \mathcal{C})$ and lies on the boundary of $\pi_i(\mathcal{C})$, we deduce that x lies on the boundary of $\pi_i(\Omega_i(\mathcal{O}_i) \cap \mathcal{C})$. Finally, by the Implicit Function Theorem, we deduce that $y \in \operatorname{crit}(\pi_i, \operatorname{reg} \mathcal{O}_i) \subset \mathscr{C}(\pi_i, \mathcal{O}_i) \subset \mathcal{O}_{i-1}$, which is a contradiction since we assumed that $J(y) = i$.

We conclude that Q_i holds, and so all statements $\mathsf{Q}_1, \dots, \mathsf{Q}_d$ hold. □

Lemma 17 *Let $\mathcal{Z} \subset \mathbb{C}^n$ be an algebraic set. Let $M \in \mathrm{GL}_n(\mathbb{C})$ be such that M satisfies $\mathsf{P}(\mathcal{Z})$. Let $M^{-1}\mathcal{C}$ be a connected component of $M^{-1}\mathcal{Z} \cap \mathbb{R}^n$ and $w \in \mathbb{R}$ be on the boundary of $\pi_1(M^{-1}\mathcal{C})$. Then $\pi_1^{-1}(w) \cap M^{-1}\mathcal{C}$ is a non-empty finite set contained in $\mathcal{O}_0(M^{-1}\mathcal{Z}) \cap M^{-1}\mathcal{C}$.*

Proof of Lemma 17: By Proposition 16 we deduce that if $w \in \mathbb{R}$ belongs to the boundary of $\pi_1(\mathcal{C})$, there exists $x \in \mathcal{O}_0(M^{-1}\mathcal{Z}) \cap M^{-1}\mathcal{C}$ such that $\pi_1(x) = w$. So $(\mathcal{O}_0(M^{-1}\mathcal{Z}) \cap M^{-1}\mathcal{C}) \cap (\pi_1^{-1}(w) \cap M^{-1}\mathcal{C}) \neq \emptyset$. Now, we prove that $\pi_1^{-1}(w) \cap M^{-1}\mathcal{C} \subset \mathcal{O}_0(M^{-1}\mathcal{Z}) \cap M^{-1}\mathcal{C}$. Since M satisfies $\mathsf{P}(\mathcal{Z})$, $\mathcal{O}_0(M^{-1}\mathcal{Z})$ is finite and we also deduce that $\pi_1^{-1}(w) \cap M^{-1}\mathcal{C}$ is finite.

We use again the definition of the function $x \mapsto J(x)$ over $\mathcal{Z}$ used in the proof of Proposition 16. Suppose that there exists $x \in \pi_1^{-1}(w) \cap M^{-1}\mathcal{C}$ such that $J(x) = j > 0$; this implies that $x \in \mathcal{O}_j(\mathcal{Z}) \setminus \mathcal{O}_{j-1}(\mathcal{Z})$. In particular, we deduce that $x \in \operatorname{reg}(\Omega_j(\mathcal{O}_j(\mathcal{Z}))) \cap M^{-1}\mathcal{C}$. Since $w = \pi_1(x)$ is on the boundary of $\pi_1(M^{-1}\mathcal{C})$, we conclude that $\pi_j(x)$ is on the boundary of $\pi_j(\Omega_j(\mathcal{O}_j(M^{-1}\mathcal{Z})) \cap M^{-1}\mathcal{C})$. Moreover, since $x \in \operatorname{reg} \Omega_j(\mathcal{O}_j(M^{-1}\mathcal{Z})) \cap M^{-1}\mathcal{C}$, we conclude by the Implicit Function Theorem that x is a critical point of the restriction of π_j to $\mathcal{O}_j(M^{-1}\mathcal{Z})$. So $x \in \operatorname{crit}(\pi_j, \mathcal{O}_j(M^{-1}\mathcal{Z})) \subset \mathscr{C}(\pi_j, \mathcal{O}_j(M^{-1}\mathcal{Z})) \subset \mathcal{O}_{j-1}(M^{-1}\mathcal{Z})$. We conclude that contradiction $J(x) \leq j - 1$ which is a contradiction. □

We are now able to prove Proposition 3.

Proof of Proposition 3: Let $\mathscr{M}_2 \subset \mathrm{GL}_n(\mathbb{C})$ be the non-empty Zariski open set of matrices satisfying Property $\mathsf{P}(\mathcal{Z})$ defined in Proposition 15, and let $M \in \mathscr{M}_2$. Let $M^{-1}\mathcal{C}$ be a connected component of $M^{-1}\mathcal{D} \cap \mathbb{R}^n$, and let $1 \leq i \leq n-1$. Then, applying Proposition 16, we conclude that $\mathsf{Q}_i(M^{-1}\mathcal{D})$ holds. In particular the boundary of $\pi_i(M^{-1}\mathcal{C})$ is contained in $\pi_i(\mathcal{O}_{i-1}(\mathcal{D}^M) \cap M^{-1}\mathcal{C}) \subset \pi_i(M^{-1}\mathcal{C})$ which implies that $\pi_i(M^{-1}\mathcal{C})$ is closed. This proves Assertion (1).

We prove now Assertion (2). Take $w \in \mathbb{R}$ that lies in the frontier of $\pi_1(M^{-1}\mathcal{C})$. By Lemma 17, $\pi_1^{-1}(w) \cap M^{-1}\mathcal{C}$ is a finite set, and thus there exists $x \in M^{-1}\mathcal{D} \cap \mathbb{R}^n$ such that $x \in M^{-1}\mathcal{C}$ and $\pi_1(x) = w$. For all such x, the matrix $A(x)$ is rank defective. Fix $x \in \pi_1^{-1}(w) \cap M^{-1}\mathcal{C}$ and let $r \leq m-1$ be the rank of $A(x)$. Consider the linear system $y \mapsto f(A, u)$ parametrized by the vector u. This system has at least one solution y if and only if

$$\operatorname{rank} \begin{bmatrix} A(x) \\ u_1 \ \cdots \ u_m \end{bmatrix} = \operatorname{rank} \begin{bmatrix} A(x) & \mathbf{0} \\ u_1 \ \cdots \ u_m & 1 \end{bmatrix}.$$

Now, the second matrix has rank $r+1$, and the first matrix has rank $r+1$ if and only if u does not lie in the space generated by the rows of A. So there exists a non-empty Zariski open set $\mathscr{U}_x$ such that if $u \in \mathscr{U}_x$ the linear system has at least one solution.

We conclude the proof by taking

$$\mathscr{U} = \bigcap_{\mathcal{C} \subset \mathcal{D} \cap \mathbb{R}^n} \ \bigcap_{x \in \pi_1^{-1}(w) \cap M^{-1}\mathcal{C}} \mathscr{U}_x$$

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

The remainder of this Section is dedicated to the proof of Proposition 15. We start by introducing some notations.

Notations 18 *Let B be an n-by-n matrix of indeterminates. For $f \in \mathbb{Q}[x_1, \ldots, x_n]$, let $f \circ B \in \mathbb{Q}(B)[x_1, \ldots, x_n]$ denote the polynomial such that $(f \circ B)(x) = f(Bx)$, and if*

$\mathcal{V} \subset \mathbb{C}^n$ is defined by the ideal $I = \langle f_1, \ldots, f_s \rangle$, let $B^{-1}\mathcal{V}$ be the algebraic set defined by $I \circ B = \langle f_1 \circ B, \ldots, f_s \circ B \rangle \subset \mathbb{Q}(B)[x_1, \ldots, x_n]$.

For all $i = 0, 1, \ldots, d$, we denote by I_i, $I_i \circ M$ and $I_i \circ B$ the ideals associated to the algebraic sets $\mathcal{O}_i(\mathcal{Z}), \mathcal{O}_i(M^{-1}\mathcal{Z})$ and $\mathcal{O}_i(B^{-1}\mathcal{Z})$, see Notations 14.

Lemma 19 *Let $\mathcal{Z} \subset \mathbb{C}^n$ be an algebraic set of dimension d and $0 \leq i \leq d$. Let $\mathcal{P}$ be one of the components of the prime decomposition of $I \circ B_i$ and let $r = \dim \mathcal{P}$. Then $r \leq i$ and the ring extension $\mathbb{Q}(B)[x_1 \ldots x_r] \longrightarrow \mathbb{Q}(B)[x_1 \ldots x_n]/\mathcal{P}$ is integral.*

This Lemma is a generalization of [41, Prop.1] to the non-equidimensional case. Its proof shares similar techniques than those used for proving [41, Prop.1]. It exploits the properties of the geometric objects defined in Notations 14 to retrieve an equidimensional situation. We sketch below the main differences and will refer to the proof of [41, Prop. 1] for the steps that are identical.

Proof of Lemma 19: Our reasoning is by decreasing induction on the index i.

Suppose first that $i = d$, so that $I_d \circ B = I(B^{-1}\mathcal{Z})$ (recall that by definition $\mathcal{O}_d(B^{-1}\mathcal{Z}) = B^{-1}\mathcal{Z}$). Let $\mathcal{P}$ be a prime ideal of the prime decomposition of $I_d \circ B$, and let $r = \dim \mathcal{P}$. Thus, the algebraic set defined by $\mathcal{P}$ is an irreducible component of dimension $r \leq d$ and then $Z(\mathcal{P}) \subset \Omega_r(B^{-1}\mathcal{Z})$. By the Noether normalization lemma [34], the statement follows.

Suppose now that the statement is true for $i+1$. To simplify notations we write $\mathcal{O}_i$ instead of $\mathcal{O}_i(B^{-1}\mathcal{Z})$. In particular, we assume that $\mathcal{O}_{i+1}$ has dimension $\leq i+1$. Consider the ideal $I_i \circ B$; using the definitions of the geometric objects introduced in Notations 14 one obtains the following equalities:

$$I_i \circ B = I(\mathscr{S}(\mathcal{O}_{i+1})) \cap I(\mathscr{C}(\pi_{i+1}, \mathcal{O}_{i+1})) \cap I(\mathscr{C}(\pi_{i+1}, B^{-1}\mathcal{Z})).$$

Now, let $\mathcal{P}$ be a prime ideal associated to $I_i \circ B$. Then, $\mathcal{P}$ is a prime ideal associated to one of the three ideals in the above intersection. We investigate below the three possible cases:

1. $I(\mathscr{S}(\mathcal{O}_{i+1})) \subset \mathcal{P}$. Let $r = \dim \mathcal{P}$. In this case, we obtain

   $$\mathcal{P} \supset I(\Omega_0(\mathcal{O}_{i+1})) \cap \cdots \cap I(\Omega_i(\mathcal{O}_{i+1})) \cap I(\text{sing}\,(\Omega_{i+1}(\mathcal{O}_{i+1}))).$$

   Combined with the fact that $\mathcal{P}$ is prime, this implies that

   - either $I(\Omega_j(\mathcal{O}_{i+1})) \subset \mathcal{P}$, for some $0 \leq j \leq i$; then one gets $r \leq i$ and by the induction assumption that the extension $\mathbb{Q}(B)[x_1 \ldots x_r] \longrightarrow \mathbb{Q}(B)[x_1 \ldots x_n]/\mathcal{P}$ is integral ;
   - or $I(\text{sing}\,(\Omega_{i+1}(\mathcal{O}_{i+1}))) \subset \mathcal{P}$.

   Assume that $I(\text{sing}\,(\Omega_{i+1}(\mathcal{O}_{i+1}))) \subset \mathcal{P}$. We deduce that

   $$\dim(\mathcal{P}) \leq \dim(\text{sing}\,(\Omega_{i+1}(\mathcal{O}_{i+1}))).$$

Since $\dim(\Omega_{i+1}(\mathcal{O}_{i+1})) = i+1$ by definition, it follows that $\dim(\text{sing}\,(\Omega_{i+1}(\mathcal{O}_{i+1}))) \leq i$ and we deduce that $\dim(\mathcal{P}) \leq i$. Let $f \circ B = (f_1 \circ B, \ldots, f_s \circ B)$ be a set of generators of the ideal associated to $\Omega_{i+1}(\mathcal{O}_{i+1})$. Then

$$I(\text{sing}\,(\Omega_{i+1}(\mathcal{O}_{i+1}))) = \sqrt{\langle f \circ B, g_1, \ldots, g_N\rangle}$$

where $g_1, \ldots, g_N$ are the minors of size $(n-i-1) \times (n-i-1)$ of the Jacobian matrix $Df \circ B$. We prove below by induction on t that for any prime $\mathcal{Q}$ associated to $\langle f \circ B, g_1, \ldots, g_t\rangle$, the extension

$$\mathbb{Q}(B)[x_1 \ldots x_r] \longrightarrow \mathbb{Q}(B)[x_1 \ldots x_n]\,/\mathcal{Q}$$

is integral. Taking $t = N$ will conclude the proof.

For $t = 0$, the induction assumption implies that for any prime $\mathcal{Q}$ associated to $\langle f \circ B\rangle$, the extension $\mathbb{Q}(B)[x_1 \ldots x_r] \longrightarrow \mathbb{Q}(B)[x_1 \ldots x_n]\,/\mathcal{Q}$ is integral.

Assume now that for any prime $\mathcal{Q}'$ associated to $\langle f \circ B, g_1, \ldots, g_t\rangle$, the extension

$$\mathbb{Q}(B)[x_1 \ldots x_r] \longrightarrow \mathbb{Q}(B)[x_1 \ldots x_n]\,/\mathcal{Q}'$$

is integral.

We prove below that for any prime $\mathcal{Q}$ associated to $\langle f \circ B, g_1, \ldots, g_{t+1}\rangle$, the extension

$$\mathbb{Q}(B)[x_1 \ldots x_r] \longrightarrow \mathbb{Q}(B)[x_1 \ldots x_n]\,/\mathcal{Q}$$

is integral.

Remark that any prime $\mathcal{Q}$ associated to $\langle f \circ B, g_1, \ldots, g_{t+1}\rangle$ is a prime associated to $\mathcal{Q}' + \langle g_{t+1}\rangle$. Suppose that $g_{t+1} \notin \mathcal{Q}'$ (otherwise, the conclusion follows immediately) and let r' be the Krull dimension of $\mathcal{Q}'$.

By Krull's Principal Ideal Theorem, $\mathcal{Q}' + \langle g_{t+1}\rangle$ is equidimensional of dimension $r'-1$. Following *mutatis mutandis* the same argumentation as in the proof of [41, Prop. 1], the ideal $\mathcal{Q}' + \langle g_{t+1}\rangle$ contains a monic polynomial in $x_{r'}$, so that the extension

$$\mathbb{Q}(B)[x_1 \ldots x_{r'-1}] \longrightarrow \mathbb{Q}(B)[x_1 \ldots x_n]\,\Big/\,\mathcal{Q}' + \langle g_{t+1}\rangle$$

is integral. Our claim follows.

2. $I(\mathscr{C}(\pi_{i+1}, \mathcal{O}_{i+1}(B^{-1}\mathcal{Z}))) \subset \mathcal{P}$.

   Recall that $\mathscr{C}(\pi_{i+1}, \mathcal{O}_{i+1}(B^{-1}\mathcal{Z}))$ is the union of $\text{crit}\,(\pi_{i+1}, \text{reg}\,(\Omega_{i+1}(\mathcal{O}_{i+1})))$ and the sets $\Omega_j(B^{-1}\mathcal{Z})$ for $0 \leq j \leq i$. When $I(\Omega_j(B^{-1}\mathcal{Z})) \subset \mathcal{P}$, one can apply the induction assumption.

   Thus, we focus on the case where $I(\text{crit}\,(\pi_{i+1}, \text{reg}\,(\Omega_{i+1}(\mathcal{O}_{i+1})))) \subset \mathcal{P}$.

   The ideal $I(\text{crit}\,(\pi_{i+1}, \text{reg}\,(\Omega_{i+1}(\mathcal{O}_{i+1}))))$ is built as follows. Suppose that $f \circ B = (f_1 \circ B, \ldots, f_s \circ B)$ defines $I(\Omega_{i+1}(\mathcal{O}_{i+1}))$, that $g_1, \ldots, g_N$ are the square minors of size $n-i-1$ of the jacobian matrix of $f \circ B$ where the first i columns are eliminated, and that J is the ideal $I(\text{sing}\,(\Omega_{i+1}(\mathcal{O}_{i+1})))$. The following equality is immediate:

$$I(\text{crit}\,(\pi_{i+1}, \text{reg}\,(\Omega_{i+1}(\mathcal{O}_{i+1})))) = \sqrt{f \circ B + \langle g_1, \ldots, g_N\rangle} : J^{\infty},$$

where, if K, L are two ideals in the same ring R, then $K : L^\infty = \{p \in R \mid L^N p \subset K,\ \exists N \in \mathbb{N}\}$. We deduce that the ideal $\mathcal{P}$ is a prime component of $\sqrt{f \circ B + \langle g_1, \ldots, g_N \rangle}$ whose zero locus is not included in $\mathrm{sing}\,(\Omega_{i+1}(\mathcal{O}_{i+1}))$. The integral ring extension property is already proved (by induction) for every component of the ideal $\langle f \circ B \rangle$; so we proceed as in the first point.

3. $I(\mathscr{C}(\pi_{i+1}, B^{-1}\mathcal{Z})) \subset \mathcal{P}$.

   Again, recall that $\mathscr{C}(\pi_{i+1}, B^{-1}\mathcal{Z})$ is the union of $\Omega_j(B^{-1}\mathcal{Z})$ for $0 \leq j \leq i$ and the union for $r' \geq i$ of the sets $\mathrm{crit}\,(\pi_i, \mathrm{reg}\,(\Omega_{r'}(\mathcal{Z})))$ of critical points of the restriction of π_i to the regular locus of $\Omega_{r'}(B^1\mathcal{Z})$.

   Let $r' \geq i+1$, and $\Omega_{r'}(\mathcal{Z})$ be the equidimensional component of $\mathcal{Z}$ of dimension r'. So we can assume $I(\mathrm{crit}\,(\pi_{i+1}, \mathrm{reg}\,(\Omega_{r'}(B^{-1}\mathcal{Z})))) \subset \mathcal{P}$. The proof follows exactly the same argumentation as the one in the second point.

□

The following lemma plays the same role as the one in [41, Prop. 2]. It shows that there exists the integral extension property in Lemma 19 is maintained when specializing B to a generic matrix M of $\mathrm{GL}_n(\mathbb{C})$. The proof of the lemma below is exactly the same as the one of [41, Prop. 2].

Lemma 20 *Let $\mathcal{Z} \subset \mathbb{C}^n$ be an algebraic set of dimension d. There exists a non-empty Zariski open set $\mathscr{M}_2 \subset \mathrm{GL}_n(\mathbb{C})$ such that if $M \in \mathscr{M}_2 \cap \mathbb{Q}^{n\times n}$, the following holds. Let $i \in \{0, 1, \ldots, d\}$ and $\mathcal{P}$ be a prime component of $I_i \circ M$ and let $r = \dim(\mathcal{P})$. Then $r \leq i$ and the ring extension $\mathbb{C}[x_1 \ldots x_r] \longrightarrow \mathbb{C}[x_1 \ldots x_n]/_{\mathcal{P}}$ is integral.*

Now we can prove Proposition 15.

Proof of Proposition 15: Let $\mathscr{M}_2 \subset \mathrm{GL}_n(\mathbb{C})$ be the non-empty Zariski open set defined in Lemma 20. By Lemma 20, for $M \in \mathscr{M}_2$ and $0 \leq i \leq d$, any irreducible component of the algebraic set $O_i(M^{-1}Z)$ is in Noether position with respect to $x_1, \ldots, x_i$. This proves Point (2) of $\mathsf{P}(Z)$. Now, remark that [43, Chap. 1.5.3] implies that any irreducible component of $O_i(M^{-1}Z)$ has dimension $\leq i$. This proves Point (1) of $\mathsf{P}(Z)$. □

6 Practical experiments

In this section, we report on practical experiments done with a computer implementation of our algorithm.

We have implemented the algorithm RealDet under Maple. The computation of rational parametrizations is done using Gröbner bases, see [16, 17, 26, 25, 19]. We use the Gröbner basis library FGb [18] implemented in C by J.-C. Faugère and its interface with Maple.

We compare our implementation of RealDet with the Real Algebraic Geometry Library RAGLib [39] implemented by the second author. RAGLib is also a Maple library implementing algorithms based on the critical point method. It also uses Gröbner bases

and the library FGb for solving polynomial systems of dimension 0. We use its command `PointsPerComponents` to compute sample points in each connected component of the real counterpart of the hypersurface defined by the vanishing of the determinant of the matrix under consideration.

The computations that we report on have been performed on an Intel(R) Xeon(R) CPU E7540@2.00GHz 256 Gb of RAM. The symbol ∞ means that the computation did not end after 24 hours.

6.1 Simple example

We first illustrate the behavior of our algorithm on the simple planar determinantal quartic of Example 12. We would like to find at least one point $(x_1, x_2) \in \mathbb{R}^2$ in each connected component of the real variety defined by the equation

$$\det \begin{pmatrix} 1+x_1 & x_2 & 0 & 0 \\ x_2 & 1-x_1 & x_2 & 0 \\ 0 & x_2 & 2+x_1 & x_2 \\ 0 & 0 & x_2 & 2-x_1 \end{pmatrix} =$$

$$x_1^4 + 3x_1^2x_2^2 + x_2^4 - x_1x_2^2 - 5x_1^2 - 7x_2^2 + 4 = 0.$$

With input the previous linear matrix, the algorithm checks that the associated incidence variety $\mathcal{V}$ verifies the regularity properties. This is done by computing a Gröbner basis of the ideal generated by the polynomials defining $\mathcal{V}$ and by the maximal minors of the jacobian matrix, and verifying that this Gröbner basis is 1.

Then, the algorithm recursively computes rational parametrizations of the zero-dimensional Lagrange systems encoding critical points of the projection on the first variable, restricted to the incidence varieties (or its sections). To obtain this parametrization, we use the functions implemented in the Maple package `fgbrs` given in input a Gröbner basis of a zero-dimensional ideal, gives in output a rational parametrization of its solution set.

Once a rational parametrization of the desired output is given, we isolate the real roots which are given by isolating intervals, each of one guaranteed to contain a point on the curve. To give an idea of the output, we reproduce here one of these points, together with its approximation to 10 certified digits:

$$x_1 \in [\tfrac{12215640488392800048013279592433}{256536504662931063109335249846272}, \tfrac{3553640869340360235301844990525 19}{74628801356489036540897527228006 4}] \approx 0.4761755254$$
$$x_2 \in [-\tfrac{10810534239}{4294967296}, -\tfrac{345937095647}{137438953472}] \approx -2.517023645$$

The eight points are represented on the curve on Figure 3.

6.2 Timings

Table 1 reports on timings obtained with n-variate linear matrices of size m with rational coefficients chosen randomly. Thus, all matrices satisfy the genericity Assumption G.

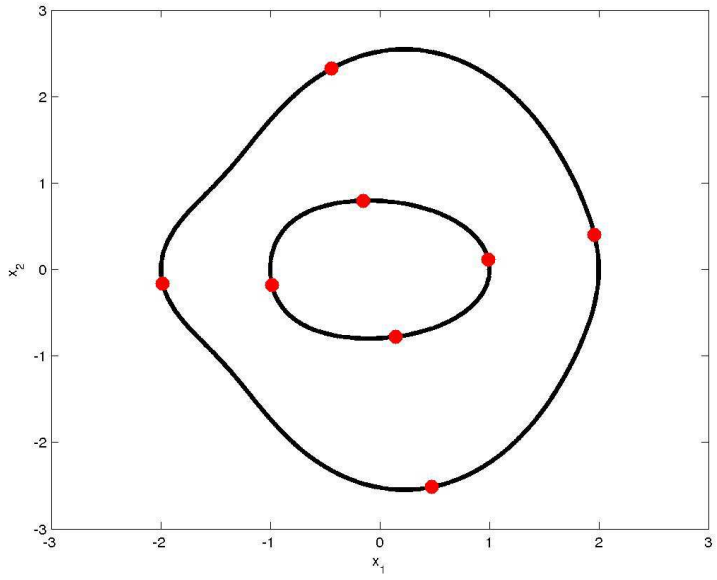

Figure 3: The determinantal quartic curve of Example 12 (black) and eight of its points (red) as returned by RealDet.

m	n	RealDet	RAGLIB	m	n	RealDet	RAGLIB
2	4	0.22 s	2.25 s	4	3	4.16 s	2.15 s
2	10	0.63 s	25.6 s	4	4	110 s	835 s
2	20	1.99 s	$\simeq$ 1 h	4	8	1824 s	∞
3	3	0.49 s	2.8 s	4	16	4736 s	∞
3	9	2.24 s	195 s	4	20	7420 s	∞
3	20	10.5 s	$\simeq$ 7 h	5	2	0.9 s	0.23 s
4	2	0.35 s	0.35 s	5	3	10.2 s	59 s

Table 1: Timings for RealDet applied to random linear matrices

We can observe that our implementation RealDet reflects the complexity gain since, for example, we are able to solve the problem for dense determinants of degree $m = 4$ and with $n = 16$ variables in less than one hour and a half; the same problem cannot be solved within a day by RAGLIB.

Also, when the size m of the matrix is fixed, we observe that the increase of time needed to perform the computation is well-controlled. Figures 4 and 5 illustrate this: the black (resp. red) curve represents how the computation time of our implementation (resp. RAGLIB) increases with respect to the number of variables when m is fixed to 3 and 4. Note that our implementation has the ability to solve problems with 20 variables which are unreachable by RAGLIB.

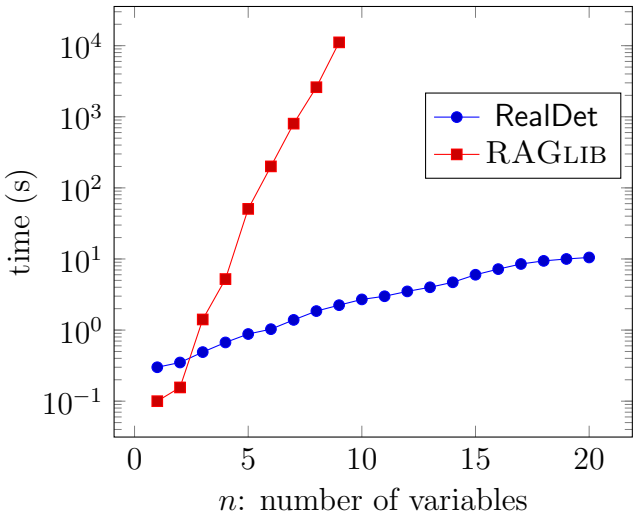

Figure 4: Timings for $m = 3$ and $n \leq 20$

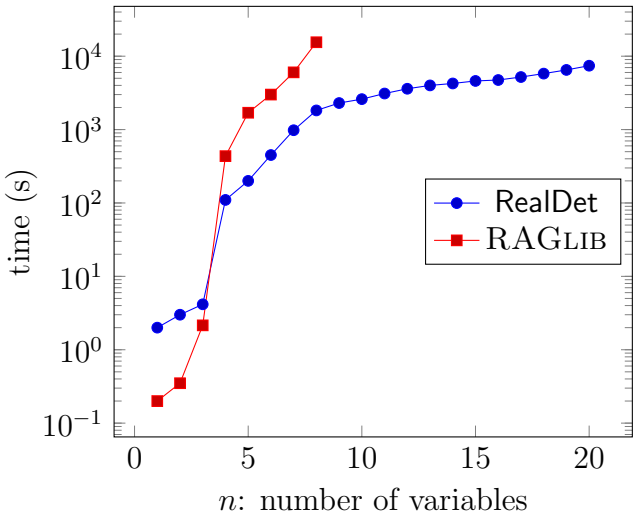

Figure 5: Timings for $m = 4$ and $n \leq 20$

6.3 Degree of the output

In Table 2, we report some data on the degrees of the rational parametrizations computed by RealDet. Recall that we have provided degree bounds in Section 2.3.

We conjectured that these bounds are not sharp; these experiments support this statement. In the column "degree" we report the sum of the degrees of the rational parametrizations computed by our algorithm for generic n-variate linear matrices of size m. We remark that if m is fixed, this value is constant when $n \geq 2m - 1$. The same property holds for the multi-linear bound for the degree of the output.

m	n	degree	bound	m	n	degree	bound	m	n	degree	bound
2	2	4	5	3	4	33	43	4	3	52	74
2	3	6	7	3	5	39	49	4	4	120	169
2	4	6	7	3	6	39	49	4	6	264	347
2	8	6	7	3	8	39	49	4	7	284	367
2	20	6	7	3	15	39	49	4	15	284	367
3	3	21	28	3	20	39	49	4	20	284	367

Table 2: Degree of the output for the generic case

Example 21 *Consider the matrix*

$$A(x) = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1m} \\ x_{21} & \ddots & & \vdots \\ \vdots & & & \\ x_{m1} & & & x_{mm} \end{pmatrix}.$$

We remark that, in the context of this paper, $A(x)$ is a linear matrix of size m, with m^2 variables, and it is expressed as a linear combination of m^2 matrices of rank 1. Allowing $x \in \mathbb{Q}^{m^2}$ to vary, the matrix $A(x)$ describes all matrices of size m with entries in $\mathbb{Q}$.

Let $b = (b_{11} \dots b_{mm}) \in \mathbb{Q}^{m^2}$ be a vector of rational numbers. We add the affine constraint $b'x = 1$, i.e. we solve the previous linear equation with respect to x_{11} and we substitute this value to x_{11} into $A(x)$.

b all ones	$m = 2$	$m = 3$	$m = 4$
degree	5	35	244

b generic	$m = 2$	$m = 3$	$m = 4$
degree	6	36	245

Table 3: Matrices with an affine constraint on the entries

In Table 3 we report on some numerical experiments. The two subtables contains the degree of the output of RealDet *and the computational times respectively when b is the vector of all ones, and when the coordinates of b are random values in $\mathbb{Q}$. We remark that the values of the degree are smaller than the corresponding values for the "dense" cases $(m, n) = (2, 3), (3, 8)$ and $(4, 15)$ that are respectively $6, 39$ and 284, as shown in Table 2.*

Example 22 *Consider the symmetric matrix*

$$A(x) = \begin{pmatrix} 2x_{11} & x_{12} & \dots & x_{1k} \\ x_{12} & \ddots & & \vdots \\ \vdots & & & \\ x_{1k} & & & 2x_{kk} \end{pmatrix}.$$

Matrix $A(x)$ has size m with $m(m+1)/2$ variables and it parametrizes all symmetric matrices. It is expressed as a linear combination of matrices of rank 1 or 2.

b all ones	$m=2$	$m=3$	$m=4$
degree	2	16	122

b generic	$m=2$	$m=3$	$m=4$
degree	3	21	136

Table 4: Symmetric matrices with an affine constraint on the entries

We add as above a linear relation $b'x = 1$ where $b \in \mathbb{Q}^{m(m+1)/2}$, and in Table 4 we report on experimental data. We observe the same behavior as in the previous example.

6.4 Complexity

In Figures 6 and 7, we consider two fundamental subclasses of the problem: when $n = m^2$ (non-symmetric case) and when $n = m(m+1)/2$ (symmetric case). We estimate in both cases the order of complexity

$$C(m,n) = n^2 m^2 (n+m)^5 \binom{m+n}{n}^6$$

of RealDet as computed in Proposition 5. We recall that standard complexity bounds for these classes of problems are in $m^{\mathcal{O}(n)}$.

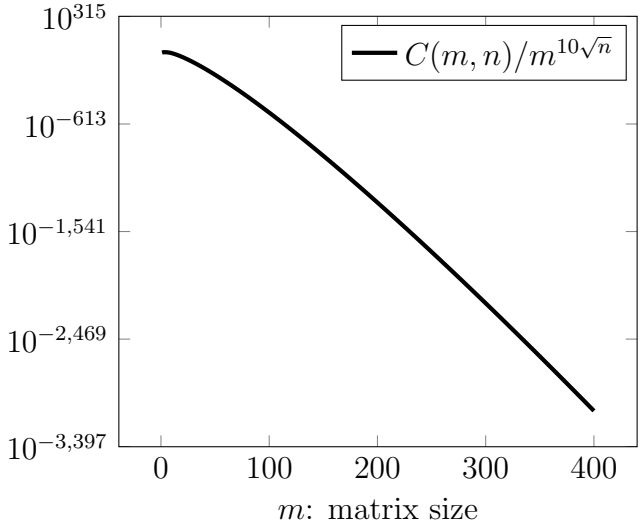

Figure 6: Complexity bound for $n = m^2$.

On Figure 6 we represent in logarithmic scale the ratio of $C(m,n)$ with $m^{10\sqrt{n}}$ (where the relation $n = m^2$ is fixed) as a function of the matrix size m. We remark that we obtain a bound which is strictly contained in $m^{\mathcal{O}(\sqrt{n})}$ since this ratio tends to zero. This numerical test shows that our complexity bound, significantly improves the previous one.

The same conclusion holds for the second case (Figure 7) where $n = (m^2+m)/2$, which includes the fundamental family of symmetric linear matrices), where our complexity is compared with m^{5n}. We also remark that similar results – not reported here for conciseness – have been obtained by imposing a linear relation between m and n, for example $n = 2m$ or $n = 3m$, and allowing m to vary.

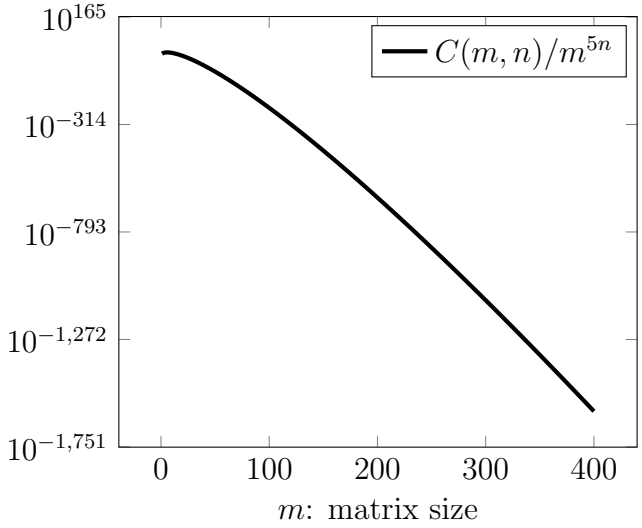

Figure 7: Complexity bound for $n = \frac{m^2+m}{2}$.

To summarize, the complexity of RealDet given by Proposition 5 is such that:

- when m is fixed, the complexity $n \mapsto C(m,n)$ is polynomial;
- when $n = m^2$ or $n = (m^2+m)/2$ or $n = \alpha m$, its asymptotic behavior when m grows is well-controlled and improves the state-of-the-art.

References

[1] 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.

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

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

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

[5] 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.

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

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

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

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

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

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

[12] 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.

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

[14] J. Draisma, E. Horobet, G. Ottaviani, B. Sturmfels, R. R. Thomas. The Euclidean distance degree of an algebraic variety. arXiv:1309.0049, 2013.

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

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

[17] 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), 2002.

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

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

[20] 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.

[21] 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), 2010.

[22] 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.

[23] 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 (ISAAC), 2012.

[24] 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.

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

[26] 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 (ISAAC), 2011.

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

[28] 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.

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

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

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

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

[33] 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.

[34] 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.

[35] 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.

[36] 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.

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

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

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

[40] 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.

[41] 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 (ISAAC), 2003.

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

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

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