M2 Internship Report:
Solving determinantal systems using homotopy techniques

Vu Thi Xuan
Symbolic Computation Group
David R. Cheriton School of Computer Science
University of Waterloo, Canada

Supervised by:

Éric Schost
David R. Cheriton School of Computer Science
University of Waterloo, Canada

and

Mohab Safey El Din
Sorbonne Universités, UPMC Univ. Paris 6
CNRS, INRIA Paris Center, LIP6, PolSys Team, France

February 1 – June 16, 2017

Abstract

Solving determinantal polynomial systems, that is systems whose equations are obtained as minors of polynomial matrices, is a recurrent question in areas such as optimization or real algebraic geometry. Results known as of now are not entirely satisfying; for instance, there is no known algorithm that would solve such systems with a complexity polynomial in the expected number of solutions.

Homotopy continuation techniques rely on following a deformation between the system one has to solve and another system, which is called start system, with a similar combinatorial structure, but whose solutions are easy to describe. In the context of determinantal systems, we define the start system by designing a *start matrix* in such a way that points at which the rank of the matrix decreases, are easy to identify.

In this report, we study how the symbolic homotopy techniques can be used in order to solve determinantal polynomial systems. We give an algorithm to find all isolated solutions for the determinantal system which is obtained from all maximal minors.

1 Introduction

1.1 Problem

In what follows, $\mathbb{K}$ is a field, $\mathbf{X} = (X_1, \ldots, X_n)$ is a set of n variables and $\mathbb{K}[\mathbf{X}]$ is the multivariate polynomial ring with coefficients in $\mathbb{K}$. Let $F \in \mathbb{K}[\mathbf{X}]^{p\times q}$ be a polynomial matrix, without loss of generality, we assume that $p \leqslant q$. For several reasons, one is interested in computing the set of points at which the evaluation of the matrix has rank at most $p-1$, called *maximal rank* problem. We restrict to the case $n = q - p + 1$. Hereafter, given a polynomial matrix $F \in \mathbb{K}[\mathbf{X}]^{p\times q}$ and a point $\mathbf{x} \in \overline{\mathbb{K}}^n$, the notation $F(\mathbf{x})$ means the evaluation of the matrix F at the point $\mathbf{x}$.

Problem 1 (Maximal rank problem)**.** *Given a field $\mathbb{K}$, a matrix $F \in \mathbb{K}[\mathbf{X}]^{p\times q}$ with $p \leqslant q$ and $n = q - p + 1$, compute the set of isolated points at which the evaluation of F has rank at most $p - 1$, that is compute the set*

$$S := \{\mathbf{x} \in \overline{\mathbb{K}}^n : \operatorname{rank}(F(\mathbf{x})) \leqslant p - 1\}.$$

A polynomial is called a $p \times p$ *minor* of F if it is the determinant of a $p \times p$ submatrix of F. To study Problem 1, we consider the system of all $p \times p$ minors of F, which is called the *determinantal system* of F. Indeed, these $p \times p$ minors simultaneously vanish at all the points which we are interested in, and then give rise to a study of the *determinantal ideal* which is generated by all $p \times p$ minors of F. Therefore, in order to find the set S, we give an algorithm to compute the isolated solutions of the determinantal system of F.

1.2 Contributions, related works, and outline

Henceforth, we use the notation below for the input matrix

$$F = \begin{pmatrix} f_{1,1} & \cdots & f_{1,q} \\ \vdots & \ddots & \vdots \\ f_{p,1} & \cdots & f_{p,q} \end{pmatrix}, \text{ where } f_{i,j} \in \mathbb{K}[\mathbf{X}] \text{ for } 1 \leqslant i \leqslant p, 1 \leqslant j \leqslant q.$$

We will present it by means of a *straight-line program*, that is, a sequence of elementary operations $+, -, \times$ that computes all of polynomials $f_{i,j}$ from the input variables $\mathbf{X}$. The *length* $\mathcal{E}$ of the input is the number of operations which we need to perform. Hereafter, we use the notations $\mathbf{f} = (f_1, \ldots, f_M) \in \mathbb{K}[\mathbf{X}]^M$ for the determinantal systems of input matrix F.

Contributions. In order to solve Problem 1, we study two cases of the input matrix. The first case, which is called *column degrees*, is when the entries in the column j have degrees at most D_j, that is, $\deg(f_{i,j}) \leqslant D_j$ for all $1 \leqslant i \leqslant p$; the second case (called *row degrees*) the entries in the row i have degrees at most D_i, that is, $\deg(f_{i,j}) \leqslant D_i$ for all $1 \leqslant j \leqslant q$. The elementary symmetric polynomials and the complete homogeneous symmetric polynomials (see Section 2 for more details) play a significant role in our algorithm. Let $E_{q-p+1}(D_1, \ldots, D_q)$ and $S_{q-p+1}(D_1, \ldots, D_p)$ be the elementary symmetric polynomial of degree $q - p + 1$ in q variables $D_1, \ldots, D_q$ and the complete homogeneous symmetric polynomial of degree $q - p + 1$ in p variables $D_1, \ldots, D_p$, respectively. Under genericity assumptions on the input, [**?**, Proposition A.6] and [**?**, Exercises 15.5 & 15.12] give us a bound for the the sum of the multiplicities of the isolated points of the corresponding determinantal ideal is either $E_{q-p+1}(D_1, \ldots, D_q)$ in column degrees case or $S_{q-p+1}(D_1, \ldots, D_p)$ in row degrees case. Meanwhile, we would like to give here a bound for that of any input matrix.

Theorem 1.1. *The sum of the multiplicities of the isolated points of the corresponding determinantal ideal is at most $\mathcal{T}$, where $\mathcal{T}$ is either $E_{q-p+1}(D_1,\ldots,D_q)$ in the column degrees case, or $S_{q-p+1}(D_1,\ldots,D_p)$ in the row degrees case.*

Concerning this bound for the case of row degrees, by using the similar argument as in [**?**, Section 3], under genericity assumptions, we can deduce the Hilbert series of $\mathbb{K}[\mathbf{X}]/\langle\mathbf{f}\rangle$ is

$$\mathrm{HS}_{\mathbb{K}[\mathbf{X}]/\langle\mathbf{f}\rangle}(t) = \frac{1-\left[\sum_{0\leqslant k\leqslant q-p}\left[(-1)^k\sum_{i_1+\cdots+i_p=k}\binom{q}{p+k}t^{\sum_{1\leqslant j\leqslant p}(i_j+1)D_j}\right]\right]}{(1-t)^{n+1}}.$$

In addition, if we can prove that there exists a function $N(t)$ such that

$$1-\left[\sum_{0\leqslant k\leqslant q-p}\left[(-1)^k\sum_{i_1+\cdots+i_p=k}\binom{q}{p+k}t^{\sum_{1\leqslant j\leqslant p}(i_j+1)D_j}\right]\right] = (1-t)^n N(t).$$

with $N(1) = S_{q-p+1}(D_1,\ldots,D_p)$, we can obtain a bound for the sum of the multiplicities of the isolated points of in the row degrees case as value of $N(1)$ under genericity assumptions on the input. However, it seems this equation is not easy to hold. We will prove Theorem 1.1 as a product of homotopy algorithm without any genericity assumptions on the input matrix.

For each case, we will construct an algorithm whose complexity is in the polynomial of $\mathcal{T},\mathcal{E}$ and the number of $p\times p$ minors of F, where $\mathcal{T}$ is either $E_n(D_1,\ldots,D_q)$ in column degrees case or $S_n(D_1,\ldots,D_p)$ in the row degrees case. The output of the algorithm in each case is a zero-dimensional parametrization for the isolated solutions of the determinantal system of the input matrix F. Given a field $\mathbb{K}$, a set in $\overline{\mathbb{K}}^n$ is a *zero-dimensional variety* if its cardinality is finite. Let $V\subset\overline{\mathbb{K}}^n$ be a zero-dimensional variety. A *zero-dimensional parametrization* $\mathscr{R} = ((q,v_1,\ldots,v_n),\lambda)$ of V consists in polynomials $(q,v_1,\ldots,v_n)$ such that $q\in\mathbb{K}[T]$ is monic and squarefree, all $v_i\in\mathbb{K}[T]$ and $\deg(v_i)<\deg(q)$, and λ is a $\mathbb{K}$-linear form in n variables, such that

- $\lambda(v_1,\ldots,v_n) = Tq' \bmod q$
- we have $V = \{(\frac{v_1(\tau)}{q'(\tau)},\ldots,\frac{v_n(\tau)}{q'(\tau)}) \mid q(\tau)=0\}$;

the constraint on λ says that the roots of q are the values taken by λ on V. The reasons for using the rational parametrization with q' as the denominator is well-known [**?**, **?**, **?**, **?**] : when $\mathbb{K}=\mathbb{Q}$, it leads to a precise theoretical control on the size of the coefficients.

The main idea behind our ingredient is to use the *homotopy*

$$H = (1-T)\cdot G + T\cdot F \in \mathbb{K}[T,\mathbf{X}]^{p\times q}$$

that connects a *start matrix* G to the target matrix F, where T is a new variable. However, we need some properties on the start matrix. If we know the solutions for the determinantal system of G, by applying Newton iteration to the determinantal system of H, we can find a zero-dimensional parametrization for the isolated solutions for that of F. Hereafter, we use the notations $\mathbf{g} = (g_1,\ldots,g_M)\in\mathbb{K}[\mathbf{X}]^M$ and $\mathbf{h} = (h_1,\ldots,h_M)\in\mathbb{K}[T,\mathbf{X}]^M$ for the determinantal systems start matrix G and homotopy matrix H, respectively. The initial points for Newton iterations are solutions of $\mathbf{g}$. In order to use the Newton iterations for those points, we need a square subsystem of $\mathbf{h}$ corresponds to each point such that the Jacobian matrix of this system has full rank at the initial point. The Newton iterations stop at a suitable moment, for which we can deduce a zero-dimensional parametrization for the isolated set of $\mathbf{f}$. Therefore, we need create a start matrix G such that

- the solutions of its determinantal system can be found effectively,
- we can extract a square subsystem with full-rank Jacobian,
- there is no solution of its determinantal system is at infinity.

The reasons why we need the third condition can be seen in the Section 4.

Theorem 1.2. *There is a randomized algorithm which solves Problem 1 in* $\left(\binom{q}{p}\mathcal{E}\mathcal{T}\right)^{\mathcal{O}(1)}$ *operations in* $\mathbb{K}$.

Related works. In [**?**], the authors work on the case where the input matrix F is a homogeneous polynomial matrix of degree D, that is $\deg(f_{i,j}) = D$ for all $1 \leqslant i \leqslant p, 1 \leqslant j \leqslant q$, under genericity assumptions on the input matrix. The authors use Gröbner bases algorithms when the input is the deterninantal system of F. By using this algorithm, when the input matrix F is homogeneous of degree D, Problem 1 can be solved in $\mathcal{O}(\binom{q}{p}\binom{Dm+1}{q-p+1}^{\omega})$ operations in $\mathbb{K}$, where ω is the exponent of matrix multiplication, with the best known bound being $\omega < 2.38$ [**?**, **?**]. Notice that in [**?**], the authors provide an algorithm for a more general problem: given a matrix F whose entries are polynomials of degree D in $\mathbb{K}[\mathbf{X}]$ and an integer $r < \min(p, q)$, compute the set of points at which the evaluation F has rank at most r. By contrast, we work on general input matrix F without generic assumptions when r equals p. We remark that when the input matrix is homogeneous, we can use our algorithm in the case of column degrees.

Numerical homotopy techniques have a lot of attention in systems of polynomials; for instance, in [**?**, **?**, **?**, **?**, **?**]. On symbolic side, in [**?**], the authors study the multi-homogeneous homotopy to compute a zero-dimensional parametrization of the algebraic set of a given system of polynomials.

In determinantal problems, it is mentioned in [**?**] that they can be solved by numerical homotopy methods. Meanwhile, we can not find any references, in our knowledge, for determinantal problems by using symbolic homotopy techniques. In this report, we study how symbolic homotopy techniques can be used to study the determinantal problems, in particular Problem 1.

Outline. The report is organized as follows. We begin in Section 2 with some notations as well as the definitions of affine varieties and ideals over multivariate polynomial rings. Then, in Section 3, we give the construction of a start matrix in the cases of column degrees and row degrees. A bound on the number of isolated solutions of determinantal systems is also provided in Section 4. After that, in Section 5, we provide details how to extract a square subsystem for Newton iteration. Algorithms which are used to solve our problem are given in Section 6. The report ends in Section 7 with conclusions and some perspectives for future research.

2 Notations and preliminaries

Given a polynomial matrix $F \in \mathbb{K}[\mathbf{X}]^{p\times q}$, we write $F_{l:k;e:f}$ for the submatrix of F containing rows $l, \ldots, k$ and columns $e, \ldots, f$. We also write $F_{l:k;*}$ for the submatrix of F containing the rows $l, \ldots, k$ and all q columns. The similar is applied for the matrix $F_{*;e:f}$.

We write M_{pq} for the vector space of matrices with p rows and q columns over the field $\mathbb{K}$. Given a multivariate polynomial $g \in \mathbb{K}[\mathbf{X}]$, if we do not give a specific mention, we will consider the degree of g is the total degree.

The elementary symmetric polynomial of degree r in m variables $t_1, \ldots, t_m$, written $E_r(t_1, \ldots, t_m)$, is defined as the coefficient of x^r in $(1 + t_1x)(1 + t_2x) \cdots (1 + t_mx)$. That is

$$E_r(t_1, \ldots, t_m) = \sum_{(i_1,\ldots,i_m)\subset\{1,\ldots,r\}^m} \prod_{j=1}^{m} t_{i_j}.$$

The complete homogeneous symmetric polynomial of degree r in m variables $t_1, \ldots, t_m$, written $S_r(t_1, \ldots, t_m)$, is defined as the coefficient of x^r in

$$\frac{1}{(1 - t_1x)(1 - t_2x) \cdots (1 - t_mx)} = (1 + t_1x + t_1^2x^2 + \cdots) \cdots (1 + t_mx + t_m^2x^2 + \cdots).$$

That is

$$S_r(t_1, \ldots, t_m) = \sum_{i_1+\cdots+i_m=r} t_1^{i_1} \ldots t_m^{i_m}.$$

There are some formulas which are obtained directly from the definition of the complete homogeneous symmetric polynomial, such as

$$S_r(t_1, \ldots, t_m) = \sum_{k=1}^{r} \sum_{(i_1,\ldots,i_k)\in\{1,\ldots,m\}^k} S_{r-k}(t_1, \ldots, t_k).$$

Ideals and varieties. Let $\mathbb{K}[\mathbf{X}]$ be a polynomial ring of n variables.

Definition 2.1. *Let $I \subset \mathbb{K}[\mathbf{X}]$ be an ideal. The* radical *of I, denoted by $\sqrt{I}$ is the set*

$$\{f \ : \ f^m \in I \text{ for some } m \in \mathbb{N}, \ m \geqslant 1\}.$$

An ideal $I \subset \mathbb{K}[\mathbf{X}]$ is *prime* if whenever $f, g \in \mathbb{K}[\mathbf{X}]$ and $fg \in I$, then either $f \in I$ or $g \in I$. An ideal $I \subset \mathbb{K}[\mathbf{X}]$ is called a *primary* ideal if $fg \in I$ implies $f \in I$ or $g^k \in I$ for some $k \in \mathbb{N}$. Remark that if I is primary in $\mathbb{K}[\mathbf{X}]$, then $\sqrt{I}$ is a prime ideal.

Definition 2.2. *Let I be an ideal in $\mathbb{K}[\mathbf{X}]$. A* primary decomposition *of I is an expression*

$$I = Q_1 \cap \cdots \cap Q_s,$$

where each Q_i is primary.

The decomposition is *irredundant* or *minimal* if $\sqrt{Q_i}$ are all distinct and $Q_i \not\supset \cap_{j\neq i} Q_j$ for all $1 \leqslant i \leqslant s$. After pruning redundant, we obtain $P_i = \sqrt{Q}_i$ for $1 \leqslant i \leqslant r$. The radical ideals P_i are then called the *associated primes* of I.

Theorem 2.1. *Let $I \subset \mathbb{K}[\mathbf{X}]$ be an ideal. Then, there exist unique $\mathcal{P}_1, \ldots, , \mathcal{P}_r$ prime ideal in $\mathbb{K}[\mathbf{X}]$ such that*

$$\sqrt{I} = \mathcal{P}_1 \cap \mathcal{P}_2 \cdots \cap \mathcal{P}_r$$

and $\mathcal{P}_1, \ldots, \mathcal{P}_r$ are called prime components of $\sqrt{I}$.

Example 2.1. Let $\mathbb{C}[X, Y]$ be the polynomial ring of two variables with complex coefficients. Let $I = \langle X^2 - Y \rangle \subset \mathbb{C}[X, Y]$ be the ideal generated by $X^2 - Y$; and $J = \langle X^2, Y^3 \rangle$ be the ideal generated by X^2 and Y^3. Then

- I is prime and J is not prime;

- the radical ideal of I is $\sqrt{I} = \langle X^2 - Y \rangle$ and the radical ideal of J is $\sqrt{J} = \langle X, Y \rangle$.

Example 2.2. Let $I = \langle X^2, XY \rangle \subset \mathbb{C}[X, Y]$. A primary decomposition of I is

$$I = \langle X^2, XY \rangle = \langle X \rangle \cap \langle X^2 Y \rangle,$$

where $P_1 = \langle X \rangle$ and $P_2 = \langle X, Y \rangle$ are the associated primes of I.

Definition 2.3. [Dimension of an ideal] *Let $\mathcal{P} \subset \mathbb{K}[\mathbf{X}]$ be a prime ideal. We say that d is the* Krull dimension *of $\mathcal{P}$ if and only if there exist prime ideals $\mathcal{P}_0, \mathcal{P}_1, \ldots, \mathcal{P}_d$ in $\mathbb{K}[\mathbf{X}]$ such that*

$$\mathcal{P}_0 \subsetneq \mathcal{P}_1 \subsetneq \cdots \subsetneq \mathcal{P}_d = \mathcal{P}.$$

The Krull dimension *of an ideal $I \subset \mathbb{K}[\mathbf{X}]$ is the maximum Krull dimension of the prime components of $\sqrt{I}$.*

Example 2.3. Let I be the ideal defined as in Example 2.1. Then, the dimension of I equals one.

The geometric objects corresponding to ideals of $\mathbb{K}[\mathbf{X}]$ are *affine varieties* (or *algebraic sets*) of $\overline{\mathbb{K}}^n$. An affine variety in $\overline{\mathbb{K}}^n$ is the set of all solutions of a system of equations. Hereafter, we will use variety for the short of affine variety. Given $\mathbf{f} = (f_1, \ldots, f_M)$ in $\mathbb{K}[\mathbf{X}]^M$, we write $V(\mathbf{f}) \in \overline{\mathbb{K}}^n$ for the variety defined by $\mathbf{f}$. That is

$$V(\mathbf{f}) = \{\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \overline{\mathbb{K}}^n \mid f_i(\boldsymbol{\alpha}) = 0 \text{ for all } 1 \leqslant i \leqslant M\}.$$

One of the important properties of varieties of $\overline{\mathbb{K}}^n$ is they define a topology on $\overline{\mathbb{K}}^n$, namely *Zariski topology*, where the closed sets of the topology are the varieties. The *Zariski closure* of a set S in $\overline{\mathbb{K}}^n$ is the smallest (for the inclusion ordering) Zariski closed set that contains S. A set V is *Zariski dense* in a set W if the Zariski closure of V contains in the Zariski closure of W. The Zariski topology will be useful for defining an algebraic notion of genericity for structured system.

Definition 2.4. *A property $\mathscr{P}$ of a family of systems $\mathfrak{F} \subset \overline{\mathbb{K}}[\mathbf{X}]$ which is a $\overline{\mathbb{K}}$-vector space of finite dimension is said to be* generic *if $\mathscr{P}$ is satisfied on a nonempty Zariski open subset of $V(\mathfrak{F})$.*

Example 2.4. Let us define systems $\mathfrak{F}$ as $A \cdot \mathbf{X} + b = 0$, where $A = [a_{i,j}]$ is the $n \times n$ matrix of variables and $b = [b_i]$ is the $n \times 1$ vector of variables. Let $\mathscr{P}$ be the property that a family of $A \cdot \mathbf{X} + b = 0$ has unique solution in $\overline{\mathbb{K}}^n$. Then, $\mathscr{P}$ is generic with a Zariski open set here is $\overline{\mathbb{K}}^{n^2} \backslash V(\det(A))$.

Definition 2.5. [Dimension of a variety] *Let V be a variety. The dimension of V is the largest d such that the image of V by $(X_1, \ldots, X_n) \to (X_{i_1}, \ldots, X_{i_d})$ is Zariski dense for some $(i_1, \ldots, i_d) \subset \{1, \ldots, n\}$.*

It is equivalent to define the dimension of a variety V as the Krull dimension of $\mathbb{K}[\mathbf{X}]/I(V)$, where

$$I(V) := \{f \in \mathbb{K}[\mathbf{X}] \mid f(\alpha) = 0 \ \forall\ \alpha \in V\},$$

which is called the ideal of V. A zero-dimensional variety is a finite set. A variety $V \subset \overline{\mathbb{K}}^n$ is *irreducible* if whenever V is written in the form $V = V_1 \cup V_2$, where V_1, V_2 are varieties, then either $V = V_1$ or $V = V_2$. The next result is given in [**?**, Theorem 4 – section 6 – chapter 4].

Theorem 2.2. *Let $V \subset \overline{\mathbb{K}}^n$ be a variety. Then V has a minimal decomposition*

$$V = V_1 \cup \cdots \cup V_m,$$

where each V_i is an irreducible variety and $V_i \not\subset V_j$ for $i \neq j$. Furthermore, this minimal decomposition is unique up to the order in which $V_1, \ldots, V_m$ are written; $V_1, \ldots, V_m$ are called the irreducible components *of V.*

Definition 2.6. *A variety is said to be* equidimensional *if and only if there exists $d \in \mathbb{N}$ such that all its irreducible components have dimension d.*

When $\mathbb{K}$ is algebraically closed, there is one-to-one correspondence between irreducible varieties in $\mathbb{K}^n$ and prime ideals in $\mathbb{K}[\mathbf{X}]$.

Example 2.5. Let $f = X^2 - Y \in \mathbb{C}[X, Y]$ and $g = X - Y$; then the variety $V(f) = \{(t^2, t) \mid t \in \mathbb{C}\}$ has dimension one while the variety $V(f, g) = \{(0, 0), (1, -1)\}$ zero-dimensional. Moreover, $V(f)$ is irreducible (since $\langle f \rangle$ is prime) while $V(f, g)$ is not an irreducible variety (since $\langle f, g \rangle$ is not a prime ideal).

Example 2.6. Let V be the variety which is defined by $X^2 - YZ = XZ - X = 0$ in $\mathbb{C}^3$, then $V = V_1 \cup V_2 \cup V_3$, where $V_1 = V(X, Y)$, $V_2 = V(X, Z)$ and $V_3 = V(Z - 1, X^2 - Y)$. In other words, V_1 is the Z-axis, V_2 is the Y-axis and V_3 is a parabola. Since $\langle X, Y \rangle$, $\langle X, Z \rangle$ and $\langle Z - 1, X^2 - Y \rangle$ are prime ideals in $\mathbb{C}[X, Y, Z]$ then V_1, V_2, V_3 are irreducible. Therefore, V_1, V_2, V_3 are irreducible components of V. Moreover, all of these components have dimension one, so V is equidimensional of dimension one.

A *hyperplane* H is the vanishing set of a linear polynomial in $\mathbb{K}[\mathbf{X}]$, that is $H = V\big(\sum a_i X_i + b\big)$.

Definition 2.7. [Degree of a variety] *Let V be an equidimensional variety of dimension d. The* degree *of V is the unique integer D such that $V \cap H_1 \cap \cdots \cap H_d$ consists of D points for generic hyperplanes $H_1, \ldots, H_p$.*

For any variety V, the degree of V is the sum of degrees of all irreducible components of V.

Given a set of polynomials $\mathbf{f} = (f_1, \ldots, f_M) \subset \mathbb{K}[\mathbf{X}]^M$, the *Jacobian matrix* of $\mathbf{f}$ is an $M \times n$ matrix defined as follows

$$\mathrm{Jac}(\mathbf{f}) = \begin{bmatrix} \frac{\partial f_1}{X_1} & \cdots & \frac{\partial f_1}{X_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_M}{X_1} & \cdots & \frac{\partial f_M}{X_n} \end{bmatrix}.$$

Solutions of polynomial systems. Given a polynomial system of N equations in n unknowns, $A(\mathbf{X}) = \mathbf{0}$. An isolated solution $\mathbf{x}^*$ of $A(\mathbf{X}) = \mathbf{0}$ is called a *singular* solution of $A(\mathbf{X}) = \mathbf{0}$ if and only if $\mathrm{rank}(\mathrm{Jac}(A)(\mathbf{x}^*)) < n$. Let us denote $\mathrm{mult}(\mathbf{x}^*)$ for the multiplicity of the solution $\mathbf{x}^*$ of $A(\mathbf{X}) = \mathbf{0}$. A solution $\mathbf{x}^*$ is called a *simple* root of $A(\mathbf{X}) = \mathbf{0}$ if $\mathrm{rank}(\mathrm{Jac}(A)(\mathbf{x}^*)) = n$.

3 Start matrix

We study two cases for the input matrix of Problem 1, those are column degrees and row degrees. We recall here that the notation $\mathcal{T}$ is either $E_{q-p+1}(D_1, \ldots, D_q)$ in the case of column degrees or $S_{q-p+1}(D_1, \ldots, D_p)$ in the row degrees case. Before going in the details of the start matrix, we need to define some genericity assumptions for the case of row degrees. Hereafter, give a polymomial matrix G, we use the notation $\mathbf{g} = (g_1, \ldots, g_M)$ for the determinantal system of G.

3.1 Genericity assumptions

Let $G = [g_{i,j}]_{1\leqslant i\leqslant p, 1\leqslant j\leqslant q}$ be a matrix where $g_{i,j}$ is a product of D_i linear forms, with each linear form has generic coefficients. We recall here that D_i is an integer that $\deg(f_{i,j}) \leqslant D_i$ for all $1 \leqslant j \leqslant q$. Notice that we use these genericity assumptions for only the row degrees case.

We say that the matrix G satisfies assumption $\mathcal{A}$ if

$\mathcal{A}(1)$. $\operatorname{rank}(G(\mathbf{x}^*)) = p - 1$ for all $\mathbf{x}^* \in V(\mathbf{g})$.

$\mathcal{A}(2)$. $\mathbf{g}$ has exactly $S_n(D_1, \ldots, D_p)$ distinct solutions.

$\mathcal{A}(3)$. $\mathbf{g}$ is a radical ideal (this genericity condition is equivalent to the property that $\operatorname{Jac}(\mathbf{g})(\mathbf{x}^*)$ has full rank for any $\mathbf{x}^* \in V(\mathbf{g})$).

Let us write $\mathcal{G} = \{\gamma_{i,j}^{(t,l_i)} \mid 1 \leqslant j \leqslant q, 0 \leqslant t \leqslant n \text{ and } i : 1 \leqslant i \leqslant p, 1 \leqslant l_i \leqslant D_i\}$ for the set of new indeterminantes for these generic coefficients. For $1 \leqslant i \leqslant p, 1 \leqslant j \leqslant q$ write $\mathfrak{g}_{i,j} = \prod_{l=1}^{D_i}(\gamma_{i,j}^{(n,l_i)}X_n + \cdots + \gamma_{i,j}^{(1,l_i)}X_1 + \gamma_{i,j}^{(0,l_i)}) \in \mathbb{K}[\mathcal{G}, \mathbf{X}]$. We will prove that assumption $\mathcal{A}$ is generic in the following sense.

Proposition 3.1. *For any $k \in \{1, 2, 3\}$, there exists a nonempty Zariski open set $\mathcal{O}_k$ such that $\mathbf{g}$ satisfies $\mathcal{A}(k)$ for $\mathfrak{g}_{i,j} \in \mathcal{O}_k$.*

Proof. Let us define the matrices G_1 and G_2 as follow

$$G_1 = \begin{pmatrix} \mathfrak{g}_{1,1} & \mathfrak{g}_{1,2} & \cdots & \mathfrak{g}_{1,q} \\ \mathfrak{g}_{2,1} & \mathfrak{g}_{2,2} & \cdots & \mathfrak{g}_{2,q} \\ \vdots & \vdots & \ddots & \vdots \\ \mathfrak{g}_{p,1} & \mathfrak{g}_{p,2} & \cdots & \mathfrak{g}_{p,q} \end{pmatrix} \text{ and } G_2 = \begin{pmatrix} \mathfrak{g}_{1,1} & 0 & \cdots & 0 & \mathfrak{g}_{1,p+1} & \cdots & \mathfrak{g}_{1,q} \\ 0 & \mathfrak{g}_{2,2} & \cdots & 0 & \mathfrak{g}_{2,p+1} & \cdots & \mathfrak{g}_{2,q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathfrak{g}_{p,p} & \mathfrak{g}_{p,p+1} & \cdots & \mathfrak{g}_{p,q} \end{pmatrix}.$$

The idea to prove $\mathcal{A}(k)$, for any $k \in \{1, 2, 3\}$, is by using induction on the number of variables n for the matrix of form G_1. Using the induction properties for smaller values of n, we show that property $\mathcal{A}(k)$ is true for the matrix G_2. Finally, by using this property of form G_2, we prove by a geometric argument that $\mathcal{A}(k)$ holds for any matrix of form G_1.

The complete proof is given in appendix A. □

3.2 Start matrix

In order to use the symbolic homotopy techniques, we need a start matrix G that connects to the target matrix F with some properties which we have mentioned in Section 1.

Column degrees

We first consider the case when $F = [f_{i,j}] \in \mathbb{K}[\mathbf{X}]^{p\times q}$ with $\deg(f_{i,j}) \leqslant D_j$ for all $1 \leqslant i \leqslant p$. We will construct a polynomial matrix $G \in \mathbb{K}[\mathbf{X}]^{p\times q}$ such that the determinantal system of G has $E_n(D_1, \ldots, D_q)$ solutions and we can find those solutions effectively.

In this subsection, we work over a field $\mathbb{K}$ of characteristic zero. For any $1 \leqslant i \leqslant p, 1 \leqslant j \leqslant q$, let us define $\lambda_{i,j}^{(k)} = (i + j)^k \in \mathbb{K}$ and $L_{i,j} = \sum_{k=1}^{n} \lambda_{i,j}^{(k)} X_k + \lambda_{i,j}^{(0)}$. Then, we define the matrix G as

$$G = \begin{pmatrix} g_1 & 2g_2 & \cdots & qg_q \\ g_1 & 2^2 g_2 & \cdots & q^2 g_q \\ \vdots & \vdots & \ddots & \vdots \\ g_1 & 2^p g_2 & \cdots & q^p g_q \end{pmatrix},$$

where g_i is the product of D_i linear forms $g_i = \prod_{j=1}^{D_i} L_{i,j}$.

Lemma 3.1. *Let G be the matrix as we define above and $\mathbf{g}$ be the ideal generated by $p \times p$ minors of G. Then, $\mathbf{g}$ has exactly $E_n(D_1, \ldots, D_q)$ solutions and there is an algorithm, namely Algorithm 1, to compute these solutions in $(nE_n(D_1, \ldots, D_q))^{\mathcal{O}(1)}$ operations in $\mathbb{K}$.*

Proof. Any $p \times p$ minor of G has the form

$$f_G = \lambda g_{i_1} \ldots g_{i_p}, \text{ where } (i_1, \ldots, i_p) \in \{1, \ldots, q\}^p \text{ and } \lambda \in \mathbb{K}, \lambda \neq 0.$$

Then, for any solution $\mathbf{x} \in V(\mathbf{g})$, $\mathbf{x}$ is a solution of n polynomials which are taken from $\{g_j\}_{1 \leqslant j \leqslant q}$. This implies

$$\begin{aligned} \#\{\text{solutions of } \mathbf{g}\} &= \sum_{(i_1,\ldots,i_n) \subset \{1,\ldots,q\}^n,\ i_j \neq i_k} \#\{\text{solutions of } g_{i_1} = \cdots = g_{i_n} = 0\} \\ &= \sum_{(i_1,\ldots,i_n) \subset \{1,\ldots,q\}^n,\ i_j \neq i_k} \prod_{j=1}^{n} D_{i_j} = E_n(D_1, \ldots, D_q). \end{aligned}$$

For the complexity, since each polynomial $L_{i,j}$ is linear, so the time to solve the system in the step 2.i is $n^{\mathcal{O}(1)}$; and there are $E_n(D_1, \ldots, D_p)$ systems which we need to solve. Therefore, the complexity of the Algorithm 1 is $(nE_n(D_1, \ldots, D_q))^{\mathcal{O}(1)}$.

□

Algorithm 1 StartMatrixColumnDegrees

Input: a matrix $G \in \mathbb{K}[\mathbf{X}]^{p \times q}$ which is defined as above.
Output: $E_n(D_1, \ldots, D_q)$ solutions of $\mathbf{g}$.

1. $S \leftarrow \emptyset$
2. for any $(i_1, \ldots, i_n) \in \{1, \ldots, q\}^n$:
   - for any $(j_1, \ldots, j_n) \in \{1, \ldots, D_{i_1}\} \times \cdots \times \{1, \ldots, D_{i_n}\}$:
     2.1. $\mathbf{x} \leftarrow$ solve the linear system $L_{i_1,j_1} = \cdots = L_{i_n,j_n} = 0$
     2.2. $S = S \cup \{\mathbf{x}\}$
3. return S

Row degrees

We here consider the case when $F = [f_{i,j}] \in \mathbb{K}[\mathbf{X}]^{p \times q}$ with $\deg(f_{i,j}) \leqslant D_i$ for all $1 \leqslant i \leqslant p$. We will construct a polynomial matrix $G \in \mathbb{K}[\mathbf{X}]^{p \times q}$ such that the determinantal system of G has $S_n(D_1, \ldots, D_p)$ solutions.

As in the proof of Proposition 3.1, we can use a matrix G as in the form of G_2 under some genericity assumptions. So, let us define a start matrix G as follows

$$G = \begin{pmatrix} g_1 & 0 & \cdots & 0 & g_{1,p+1} & \cdots & g_{1,q} \\ 0 & g_2 & \cdots & 0 & g_{2,p+1} & \cdots & g_{2,q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_p & g_{p,p+1} & \cdots & g_{p,q} \end{pmatrix},$$

where all $\{g_i\}$ and $\{g_{i,j}\}$ are products of D_i linear forms with generic coefficients. That is $g_i = \prod_{k=1}^{D_i} L_i^{(k)}$ and $g_{i,j} = \prod_{k=1}^{D_i} L_{i,j}^{(k)}$, where $L_i^{(k)}$ and $L_{i,j}^{(k)}$ are linear forms with generic coefficients.

The next property helps us reduce our problem to the problem with smaller dimension.

Proposition 3.2. *Let* $\mathbf{x}$ *be a solution of* $\mathbf{g}$ *and* k *be an integer such that* $k \leqslant \min(n,p)$. *If* $g_{i_1}(\mathbf{x}) = \cdots = g_{i_k}(\mathbf{x}) = 0$ *and* $g_j(\mathbf{x}) \neq 0$ *for* $j \in \{1,\ldots,p\}\backslash\{i_1,\ldots,i_k\}$, *then*

$$\operatorname{rank}(G_{i_1:i_k;p+1:q}(\mathbf{x})) \leqslant k-1,$$

where $G_{i_1:i_k;p+1:q}$ *is the submatrix of* G *that contains rows* $i_1,\ldots,i_k$ *and columns* $p+1,\ldots q$ *of* G.

Proof. Without of loss of generality, we prove this result for $(i_1,\ldots,i_k) = (1,\ldots,k)$. This means we have $g_1(\mathbf{x}) = \cdots = g_k(\mathbf{x}) = 0$ and $g_j(\mathbf{x}) \neq 0$ for any $j \in \{k+1,\ldots,p\}$. Let $G_{1:p;*} \in \mathbb{K}[\mathbf{X}]^{p\times p}$ be the submatrix of G consisting p rows and the columns $k+1,\ldots,p,j_1,\ldots,j_k$ of G, where $p+1 \leqslant j_i \leqslant q$. Let $f_{1:p;*}$ is the determinant of $G_{1:p;*}$. Then, for any solution $\mathbf{x}$ of $\mathbf{g}$, $f_{1:p;*}(\mathbf{x}) = 0$. Moreover, $f_{1:p;*} = \det(G_{1:p;*}) = g_{k+1,k+1}\ldots g_{p,p}\det(G_{1:k;j_1:j_k})$. Therefore, $\det(G_{1:k;j_1:j_k})(\mathbf{x}) = 0$. This holds for any $(j_1,\ldots,j_k) \in \{p+1,\ldots,q\}^k$. This implies that $\operatorname{rank}(G_{i_1:i_k;p+1:q}(\mathbf{x})) \leqslant k-1$. □

Therefore, in order to find the solutions for $\mathbf{g}$, we use the recursive algorithms for Problem 1 with the inputs are of smaller dimension. In each recursive call, we use either algorithm RowDeterminantalSystem or algorithm ColumnDeterminantalSystem which are given at the end of Section 6.

Lemma 3.2. *Let* G *be the matrix as we define above and* $\mathbf{g}$ *be the ideal generated by* $p\times p$ *minors of* G. *Then,* $\mathbf{g}$ *has exactly* $S_n(D_1,\ldots,D_p)$ *solutions. Moreover, there is an algorithm, namely Algorithm 2, to compute these solutions in* $(q\,d)^{\mathcal{O}(n)}$, *where* d *is either* $E_n(D_1+1,\ldots,D_q+1)$ *in the case of column degrees or* $S_n(D_1+1,\ldots,D_p+1)$ *in row degrees case.*

Proof. The number of solutions for $\mathbf{g}$ holds by using the genericity assumption $\mathcal{A}(2)$, so we need give here the complexity for this algorithm. Let us write $\mathbf{D}$ for $(D_1,\ldots,D_p)$ and $\mathbf{D}+1$ for $(D_1+1,\ldots,D_p+1)$. Let $\mathbf{x}$ be a solution of $\mathbf{g}=0$ with $g_i(\mathbf{x}) = 0$ for $i \in \mathcal{J}_k$ and $g_j(\mathbf{x}) \neq 0$ for $j \neq \mathcal{J}_k$. Let $G_{\mathcal{J}_k}$ be the submatrix of G that contains rows $i_1,\ldots,i_k$ and columns $p+1,\ldots,q$ of G. After rewriting $\{X_i\}_{i=1}^k$ in the form of $\{X_j\}_{j=k+1}^p$ and substituting them into the matrix $G_{\mathcal{J}_k}$, we obtain a matrix $G_{\mathcal{J}_k} = [g_{i,j}] \in \mathbb{K}[X_{k+1},\ldots,X_n]^{k\times(q-p)}$ for $i \in \mathcal{J}_k$ and $p+1 \leqslant j \leqslant q$. From Proposition 3.2, we can see that all of $k\times k$ minors of $G_{\mathcal{J}_k}$ should vanish at $\mathbf{x}$. Therefore, we need to solve Problem 1 in the case of row degrees with the input now is the matrix $G_{\mathcal{J}_k}$, for which we have an Algorithm name RowDeterminantalSystem (Section 6). The worst case for the Algorithm 2 is when we need to call the algorithm RowDeterminantalSystem in all recursive calls.

Let $T(p,q,\mathbf{D})$ be the complexity for the Algorithm 2 when $G \in \mathbb{K}[\mathbf{X}]^{p\times q}$ with $\deg(g_{i,j}) = D_i$ for all $1 \leqslant j \leqslant q$. Therefore,

$$T(p,q,\mathbf{D}) \leqslant \sum_{k=1}^{\min(n,p)} \sum_{\mathcal{J}_k\subset(1,\ldots,p\}^k} (\widetilde{T}(k,q-p,\mathbf{D}_{\mathcal{J}_k}+1) + d_{\mathcal{J}_k}), \tag{1}$$

where $\widetilde{T}(k,q-p,\mathbf{D}_{\mathcal{J}_k}+1)$ is the complexity of the Algorithm RowDeterminantalSystem when the input is a submatrix $G_{\mathcal{J}_k}$. The term $\mathbf{D}+1$ means $\widetilde{T}(k,q-p,\mathbf{D}_{\mathcal{J}_k}+1)$ is a fuction in $S_k(\mathbf{D}_{\mathcal{J}_k}+1) = S_k(D_{i_1}+1,\ldots,D_{i_k}+1)$, where $\mathcal{J}_k = (i_1,\ldots,i_k)$. The term $d_{\mathcal{J}_k}$ in eq. (1) is the runtime to recover $X_1,\ldots,X_k$ from $X_{k+1},\ldots,X_n$, which is $n^{\mathcal{O}(1)}$.

The inputs for Algorithm RowDeterminantalSystem now are $G_{\mathcal{J}_k}$ and a solutions set of a start matrix for $G_{\mathcal{J}_k}$. This means we need create a start matrix $G'_{\mathcal{J}_k}$ for $G_{\mathcal{J}_k}$, and find its solutions set. This solutions set $V(G_{\mathcal{J}_k})'$ can be found by calling Algorithm 2 for $G'_{\mathcal{J}_k}$. After that, by using $V(G'_{\mathcal{J}_k})$, we can find the isolated solutions for the determinantal system of $G_{\mathcal{J}_k}$ by using the DeterminantalSystem algorithm (Section 6) with the inputs are $V(G'_{\mathcal{J}_k})$ and $G_{\mathcal{J}_k}$. Therefore,

$$\widetilde{T}(k, q-p, \mathbf{D}_{\mathcal{J}_k}+1) \leqslant T(k, q-p, \mathbf{D}_{\mathcal{J}_k}) + S_k(\mathbf{D}_{\mathcal{J}_k}+1)q)^{\mathcal{O}(1)}, \tag{2}$$

where $(S_k(\mathbf{D}_{\mathcal{J}_k}+1)q)^{\mathcal{O}(1)}$ is the runtime for the Algorithm DeterminantalSystem with the inputs are $V(G'_{\mathcal{J}_k})$ and $G_{\mathcal{J}_k}$. From eq. (1) and eq. (2), we have

$$T(p, q, \mathbf{D}) \leqslant \sum_{k=1}^{\min(n,p)} \sum_{\mathcal{J}_k \subset (1,\ldots,p\}^k} (T(k, q-p, \mathbf{D}_{\mathcal{J}_k}) + (S_k(\mathbf{D}_{\mathcal{J}_k}+1)q)^{\mathcal{O}(1)}). \tag{3}$$

The recursive calls are now applied in order to obtain $T(k, q-p, \mathbf{D}_{\mathcal{J}_k})$. The depth of the recursion, in the worst case, is $\mathcal{O}(q)$ when the column dimension reaches one. At each level of the recursion, $T(i, j, \cdot) \leqslant (S_k(\mathbf{D}_{\mathcal{J}_k}+1)q)^{\mathcal{O}(1)})$. This implies

$$T(p, q, \mathbf{D}) \leqslant \sum_{k=1}^{\min(n,p)} \sum_{\mathcal{J}_k \subset (1,\ldots,p\}^k} (q \cdot S_k(\mathbf{D}_{\mathcal{J}_k}+1)q)^{\mathcal{O}(1)} \leqslant (S_n(\mathbf{D}+1)q)^{\mathcal{O}(1)}.$$

□

Algorithm 2 StartMatrixRowDegrees

Input: a matrix $G \in \mathbb{K}[\mathbf{X}]^{p\times q}$ which is defined as above.
Output: $S_n(D_1, \ldots, D_p)$ solutions of $\mathbf{g}$.

1. $m = \min\{n, p\}$
2. for $k = 1$ to m:
   2.1. for any $(i_1, \ldots, i_k) \subset \{1, \ldots, p\}^k$:
      i. from $g_{i_1} = \cdots = g_{i_k} = 0$, rewrite $\{X_i\}_{i=1}^k$ in the form of $\{X_i\}_{i=k+1}^n$
      ii. substitute $\{X_i\}_{i=1}^k$ into $G_{i_1:i_k;p+1:q}$
      iii. $p \leftarrow k; q \leftarrow q-p; n \leftarrow n-k$
         - if $p \leqslant q$:
           * $S' \leftarrow$ RowDeterminantalSystem$(G_{i_1:i_k;p+1:q}, G_{i_1:i_k;i_1:i_k \cup i_n:i_{n+k-1}})$
         - else:
           * $S' \leftarrow$ ColumnDeterminantalSystem$(G_{i_1:i_k;p+1:q}, \overline{G})$, where

             $\overline{G} \in \mathbb{K}[X_{k+1}, \ldots, X_n]^{p\times q}$ is a start matrix for $G_{i_1:i_k;p+1:q}$

         - deduce a zero-dimensional parametrization S for $V(\mathbf{g})$ from S'
      iv. $S \leftarrow S \cup \{\mathbf{x}\}$

4 A bound for the number isolated solutions of determinantal systems

Let $\mathbf{g} = (g_1, \ldots, g_M)$ in $\mathbb{K}[\mathbf{X}]^M$ be the determinantal system of G, and let $\mathcal{T}$ be the number of solutions of $\mathbf{g}$. That is $\mathcal{T} = E_n(D_1, \ldots, D_q)$ in the column degrees case, and $\mathcal{T} = S_n(D_1, \ldots, D_p)$ in the row degrees case. We also write $\mathbf{f} = (f_1, \ldots, f_M)$ in $\mathbb{K}[\mathbf{X}]^M$ for the determinantal system of F. In this section, we are going to prove that the number of the isolated solutions of $\mathbf{f}$ is at most $\mathcal{T}$.

4.1 Some properties of a parametric system of equations

Let $\mathbf{X} = (X_1, \ldots, X_N)$ be indeterminates over $\mathbb{K}$, as above, and let T be a new variable. We consider polynomials $\mathbf{h} = (h_1, \ldots, h_M)$ in $\mathbb{K}[T, \mathbf{X}]$, with $M \geqslant n$, and the ideal $J = \langle \mathbf{h} \rangle \subset \overline{\mathbb{K}}[\mathbf{X}]$; for τ in $\overline{K}$, we write $\mathbf{h}_\tau = (h_{\tau,1}, \ldots, h_{\tau,M}) = \mathbf{h}(\tau, \mathbf{X}) \subset \overline{\mathbb{K}}[\mathbf{X}]$. In this subsection, we give some general properties of the system $\mathbf{h}$, that hold under a few assumptions. First, consider the following properties related to the system $\mathbf{h}$ itself.

H_1. Any irreducible component of $V(J) \subset \overline{\mathbb{K}}^{n+1}$ has dimension at least one.

H_2. For any prime $P \subset \overline{\mathbb{K}}, \mathbf{X}]$, if the localization $J_P \subset \overline{\mathbb{K}}[T, \mathbf{X}]_P$ has height n, then it is unmixed (that is, all associated primes have height n).

An obvious example where such properties hold is when $M = n$. Then, H_1 is Krull's theorem, and H_2 is Macaulay's unmixedness theorem in the Cohen-Macaulay ring $\overline{\mathbb{K}}[T, \mathbf{X}]_P$ [**?**, Corollary 18.14]. More generally, these properties hold when $\mathbf{h}$ is the sequence of $p \times p$ minors of a $p \times q$ matrix with entries in $\mathbb{K}[T, \mathbf{X}]$, with $n = q - p + 1$ (the case $M = n$ corresponds to $p = 1$); see [**?**, Section 6].

Then, for τ in $\overline{K}$, we denote by $\mathsf{G}(\tau)$ the following three properties.

$\mathsf{G}_1(\tau)$. The ideal $\langle \mathbf{h}_\tau \rangle$ is radical in $\mathbb{K}[\mathbf{X}]$.

$\mathsf{G}_2(\tau)$. For $k = 1, \ldots, M$, $\deg_{\mathbf{X}}(h_k) = \deg_{\mathbf{X}}(h_{\tau,k})$.

$\mathsf{G}_3(\tau)$. The only common solution to $h^H_{\tau,1}(0, \mathbf{X}) = \cdots = h^H_{\tau,M}(0, \mathbf{X}) = 0$ is $(0, \ldots, 0) \in \overline{\mathbb{K}}^n$, where for $k = 1, \ldots, M$, $h^H_{\tau,k}$ is the polynomial in $\overline{\mathbb{K}}[X_0, \mathbf{X}]$ obtained by homogenizing $h_{\tau,k}$ using a new variable X_0. In particular, $V(\mathbf{h}\tau) \subset \mathbb{K}^n$ is finite.

The main result in this subsection is the following.

Proposition 4.1. *Suppose that* H_1 *and* H_2 *hold. Then, there exists an integer* c *such that for all* τ *in* $\overline{\mathbb{K}}$*, the sum of the multiplicities of the isolated solutions of* $\mathbf{h}_\tau$ *is at most* c*, and is equal to* c *if* $\mathsf{G}(\tau)$ *holds.*

Proof. The proof is given in appendix D. □

4.2 Number of isolated solutions of f

Given matrices M and N in $\mathbb{K}[\mathbf{X}]^{n \times n}$, we define a matrix Q in $\mathbb{K}[T, \mathbf{X}]^{n \times n}$ as $(1 - T) \cdot M + T \cdot N$. The next proposition tells us the relations between their determinants.

Proposition 4.2. *Let M, N and Q be the matrices we define above. Then,*

$$\det(Q) = (1-T)^n \det(M) + T \cdot f(T, \mathbf{X}) \text{ and } \det(Q) = (1-T) \cdot g(T, \mathbf{X}) + T^n \det(N),$$

where $h(T, \mathbf{X})$ and $g(T, \mathbf{X})$ are polynomials in $\mathbb{K}[T, \mathbf{X}]$.

Proof. Let us write $M = [g_{i,j}]_{1 \leqslant i,j \leqslant n}, N = [f_{i,j}]_{1 \leqslant i,j \leqslant n}$ and $Q = [h_{i,j}]_{1 \leqslant i,j \leqslant n}$; then for any i, j, $h_{i,j} = (1-T)g_{i,j} + Tf_{i,j}$. Then,

$$\begin{aligned}
\det(Q) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} h_{i,\sigma_i} \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} [(1-T)g_{i,\sigma_i} + Tf_{i,\sigma_i}] \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \left[(1-T)^n \prod_{i=1}^{n} g_{i,\sigma_i} + \overline{f}(T, \mathbf{X}) \right],
\end{aligned}$$

where $\overline{f}(T, \mathbf{X}) = \prod_{i=1}^{n} [(1-T)g_{i,\sigma_i} + Tf_{i,\sigma_i}] - (1-T)^n \prod_{i=1}^{n} g_{i,\sigma_i}$. Moreover, $\overline{f}(T, \mathbf{X})$ is a polynomial in $\mathbb{K}[T, \mathbf{X}]$ with all the terms are multiple of T. Therefore,

$$\begin{aligned}
\det(Q) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \left[(1-T)^n \prod_{i=1}^{n} g_{i,\sigma_i} \right] + \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \overline{f}(T, \mathbf{X}) \\
&= (1-T)^n \det(M) + T \cdot f(T, \mathbf{X})
\end{aligned}$$

Similarly, we obtain $\det(Q) = (1-T) \cdot g(T, \mathbf{X}) + T^n \det(N)$.

□

Let $\mathbf{f} = (f_1, \ldots, f_M), \mathbf{g} = (g_1, \ldots, g_M)$ and $\mathbf{h} = (h_1, \ldots, h_M)$ be the determinantal systems of F, G and H, respectively. From Proposition 4.2, for any h_i, there exist $\overline{f}_i$ and $\overline{g}_i$ in $\mathbb{K}[T, \mathbf{X}]$ such that

$$h_i = (1-T)^p g_i + T.\overline{f}_i \text{ and } h_i = (1-T)\overline{g}_i + T^p f_i, \tag{4}$$

which implies that $\mathbf{f} = \mathbf{h}_1 = (h_{1,i})_{1 \leqslant i \leqslant M}$ and $\mathbf{g} = \mathbf{h}_0 = (h_{0,i})_{1 \leqslant i \leqslant M}$.

Let $\mathbf{g}^H = (g_i^H)_{1 \leqslant i \leqslant M}$ be the polynomials in $\overline{\mathbb{K}}[X_0, \mathbf{X}]^M$ obtained by homozenizing $(g_i)_{1 \leqslant i \leqslant M}$ using a new variable X_0.

Proposition 4.3. *The only common solution to $g_1^H(0, \mathbf{X}) = \cdots = g_M^H(0, \mathbf{X})$ is $(0, \ldots, 0) \in \overline{\mathbb{K}}^n$.*

Proof. The proof is given in appendix B. □

Let $\mathbf{h} = (h_1, \ldots, h_M)$ be the determinantal system of the homotopy matrix H and let $\mathbf{h}_0^H = (h_{0,i}^H)_{1 \leqslant i \leqslant M}$ be the polynomials in $\overline{\mathbb{K}}[X_0, \mathbf{X}]^M$ obtained by homozenizing $(h_{0,i})_{1 \leqslant i \leqslant M}$ using a new variable X_0. Since $\mathbf{g} = \mathbf{h}_0$, then $\mathbf{g}^H = \mathbf{h}_0^H$; as a consequence of Proposition 4.3, we have the following result.

Corollary 4.1. *The only common solution to $\mathbf{h}_0^H(0, \mathbf{X}) = 0$ is $(0, \ldots, 0) \in \overline{\mathbb{K}}^n$.*

As we discuss in the previous subsection, the system $\mathbf{h}$ satisfies H_1 and H_2. Then from Proposition 4.1, there exists an integer c such that for all τ in $\overline{\mathbb{K}}$, the sum of the multiplicities of the isolated solutions of $\mathbf{h}_\tau$ is at most c. Moreover, since $\mathbf{g} = \mathbf{h}_0 = (h_i(0, \mathbf{X}))_{1 \leqslant i \leqslant M}$ and by using the

genericity assumption $\mathcal{A}(3)$ in Section 3.1, we have $\langle \mathbf{h}_0 \rangle = \langle \mathbf{g} \rangle$ is radical in $\overline{\mathbb{K}}[\mathbf{X}]$. The property $\mathsf{G}_2(0)$ can be verified from the construction of H; and $\mathsf{G}_3(0)$ is obtained from Corollary 4.1. In other words, the assumption $\mathsf{G}(0)$ hold when $\mathbf{h}$ is the determinantal system of H. Therefore, the number of isolated solutions of $\mathbf{h}_0$ is exactly c which equals $\mathcal{T}$. We apply again now Proposition 4.1 for $\tau = 1$ to obtain the following result.

Theorem 4.1. *Let $F \in \mathbb{K}[\mathbf{X}]^{p\times q}$ with $p \leqslant q$ and $\mathbf{f}$ be the ideal generated by the $p \times p$ minors of F. Then, the number of isolated solutions of $\mathbf{f}$ is at most $\mathcal{T}$.*

5 Excerpting square subsystem

Given $\mathbf{x}^*$ in $V(\mathbf{g})$, the aim of this section is extracting a square subsystem of determinantal system with full rank Jacobian for Newton iteration.

Let $\mathbf{x}^*$ be a solution of $\mathbf{g}$ and $\overline{G} \in \mathbb{K}[\mathbf{X}]^{(p-1)\times(p-1)}$ be a submatrix of G such that $\det(\overline{G})(\mathbf{x}^*) \neq 0$. Let $\overline{F}$ and $\overline{H}$ be the $(p-1) \times (p-1)$ submatrices of F and H, respectively with the column indices as the $\overline{G}$ column indices. Then, $\overline{H} = (1-T)\cdot\overline{G} + T\cdot\overline{F}$. By using Proposition 4.2, we have

$$\det(\overline{H}) = (1-T)^{p-1}\det(\overline{G}) + T\cdot h(T,\mathbf{X}),$$

where $h(T,\mathbf{X}) \in \mathbb{K}[T,\mathbf{X}]$. This implies

$$\det(\overline{H})(\mathbf{x}^*) = (1-T)^{p-1}\det(\overline{G})(\mathbf{x}^*) + T\cdot h(T,\mathbf{X})(\mathbf{x}^*).$$

From which and $\det(\overline{G})(\mathbf{x}^*) \neq 0$, we can deduce $\det(\overline{H})(\mathbf{x}^*)$ has zero-valuation. This means $\det(\overline{H})(\mathbf{x}^*) \neq 0$. We denote m for $\det(\overline{H})$, thanks to m we can construct the system of n equations (see Section 5.1).

The structure of this section as follows. In Section 5.1, we present how to obtain this system if we know m; after that, in Section 5.2 and Section 5.3, we will show how to find the matrix $\overline{G}$ such that $\overline{G}(\mathbf{x}^*) \neq 0$ for a fixer $\mathbf{x}^* \in V(\mathbf{g})$ in the case when we work on column degrees and row degrees respectively. As a consequence, we can build the matrix $\overline{H}$.

5.1 Local description

The main goal of this section is to give a local description of the variety associated to $\mathbf{h}$. We will show that it suffices to use n equations to describe the local variety $V(\mathbf{h})$. We follow the similar way as in [**?**, Section 2.2].

Let $H = [h_{i,j}]$ be a $p \times q$ polynomial matrix of $n+1$ variables with $p \leqslant q$. Let l and k be natural integers with $l \leqslant q$ and $k \leqslant \min\{p, l\}$. Let $I_k = (i_1, \ldots, i_k) \subset \{1, \ldots, l\}^k$ be an ordered sequence and $M(I_k)$ be the determinant of $H_{1:k;I_k}$. The Exchange Lemma below is an important tool in this section.

Lemma 5.1. [**?**] *Let H, l and k be given as above. Let $I_k = (i_1, \ldots, i_k)$ amd $I_{k-1} = (j_1, \ldots, j_{k-1})$ be two index sets such that $I_k \cap I_{k-1} \neq \emptyset$. Then,*

$$M(I_{k-1})M(I_k) = \sum_{j \in I_k \setminus I_{k-1}} \epsilon_j \; M(I_k \setminus \{j\}) \; M(I_{k-1} \cup \{j\}),$$

for suitable number $\epsilon_j \in \{1, -1\}$.

The following proposition is a similar version of [**?**, Proposition 5]. In [**?**], the authors use the matrix H as the Jacobian matrix of p polynomials $(f_1, \ldots, f_p) \in \mathbb{K}[\mathbf{X}]^p$ while here, we rewrite this proposition for the general polynomial matrix $H \in \mathbb{K}[T, \mathbf{X}]^{p\times q}$ where $p \leqslant q$. Noting that in [**?**], there is a condition that $p \leqslant n$.

Let $m \in \mathbb{K}[T, \mathbf{X}]$ be the $(p-1) \times (p-1)$ minor of H given by the first $(p-1)$ rows and $(p-1)$ columns, i.e., $m = \det(H_{1:p-1;1:p-1})$. Let us define $V(m) := \{\mathbf{x} \in \overline{\mathbb{K}[T]}^n : m(\mathbf{x}) = 0\}$ and $V(\mathbf{h})_m := V(\mathbf{h})\backslash V(m)$, where $V(\mathbf{h}) = \{\mathbf{x} \in \overline{\mathbb{K}}^n : f_H(\mathbf{x}) = 0 \text{ for all } f_H \in \langle \mathbf{h} \rangle\}$. Hereafter, for any $1 \leqslant i_1 < \cdots < i_p \leqslant n$, let us denote $M(i_1, \ldots, i_p) \in \mathbb{K}[T, \mathbf{X}]$ for the determinant of the submatrix of H which contains p rows and the columns $i_1, \ldots, i_p$.

Proposition 5.1. *Let $m, V(\mathbf{h}), V(\mathbf{h})_m$ and $V(m)$ be defined as above. Then,*

$$V(\mathbf{h})_m = \{\mathbf{x} \in \overline{\mathbb{K}[T]}^n \mid M(1, \ldots, p-1, s) = 0, m(\mathbf{x}) \neq 0 \text{ for } s \in \{p, \ldots, q\}\}.$$

In other words, the variety $V(\mathbf{h})$ is locally described by $q - p + 1$ polynomials (outside of $V(m)$), i.e., n polynomials

$$M(1, \ldots, p-1, p), M(1, \ldots, p-1, p+1), \ldots, M(1, \ldots, p-1, q).$$

Proof. $(\subseteq)$ It is obvious that for any $\mathbf{x} \in \overline{\mathbb{K}[T]}^n$ such that $\mathbf{x} \in V(\mathbf{h})_m$ we have

$$\mathbf{x} \in \{\mathbf{x} \in \overline{\mathbb{K}[T]}^n \mid M(1, \ldots, p-1, s) = 0, m(\mathbf{x}) \neq 0 \text{ for } s \in \{p, \ldots, q\}\}.$$

$(\supseteq)$ Let $\mathbf{x}$ be any point in $\overline{\mathbb{K}[T]}^n$ such that $m(\mathbf{x}) \neq 0$ and $M(1, \ldots, p-1, s)(\mathbf{x}) = 0$ for any $s \in \{p, \ldots, q\}$. We need to prove that $M(i_1, \ldots, i_p)(\mathbf{x}) = 0$ for any $(i_1, \ldots, i_p) \subset \{1, \ldots, q\}^p$. By using Lemma 5.1 for $M(1, \ldots, p-1) = m$, we have

$$m.M(i_1, \ldots, i_p) = \sum_{\{j \in \{i_1, \ldots, i_p\}\backslash\{1, \ldots, p-1\}} \epsilon_j \; M(\{i_1, \ldots, i_p\}\backslash\{j\}) \; M(1, \ldots, p-1, j),$$

for suitable $\epsilon_j \in \{1, -1\}$. Therefore,

$$m(\mathbf{x}).M(i_1, \ldots, i_p)(\mathbf{x}) = \sum_{j \in \{i_1, \ldots, i_p\}\backslash\{1, \ldots, p-1\}} \epsilon_j \; M(\{i_1, \ldots, i_p\}\backslash\{j\})(\mathbf{x}) \; M(1, \ldots, p-1, j)(\mathbf{x}).$$

Moreover, $M(1, \ldots, p-1, s)(\mathbf{x}) = 0$ for any $s \in \{p, \ldots, q\}$ and $m(\mathbf{x}) \neq 0$, so $M(i_1, \ldots, i_p)(\mathbf{x}) = 0$ for any $(i_1, \ldots, i_p) \subset \{1, \ldots, q\}^p$.

□

Remark 5.1. *The result in Proposition* 5.1 *remains true if we replace m by any $(p-1) \times (p-1)$ minor of H.*

5.2 Column degrees

In this section, we will find a $(p-1) \times (p-1)$ submatrix of H, namely $\overline{H}$, such that $m(\mathbf{x}^*) \neq 0$, where $m = \det(\overline{H})$ and $\mathbf{x}^*$ is a solution of $\mathbf{g}$ when we work on the case $\deg(f_{i,j}) \leqslant D_j$ for all $1 \leqslant i \leqslant p$. Let us recall that a start matrix G for this case is

$$G = \begin{pmatrix} g_1 & 2g_2 & \cdots & qg_q \\ g_1 & 2^2 g_2 & \cdots & q^2 g_q \\ \vdots & \vdots & \ddots & \vdots \\ g_1 & 2^p g_2 & \cdots & q^p g_q \end{pmatrix},$$

where g_i is the product of D_i linear forms, i.e., $g_i = \prod_{j=1}^{D_i} L_{i,j}$. Moreover, any $p \times p$ minor of G has the form $\lambda g_{i_1} \dots g_{i_p}$, where $(i_1, \dots, i_p) \in \{1, \dots, q\}^p$ and $\lambda \in \mathbb{K}$.

Without loss of generality, we choose $\mathbf{x}^*$ as a solution of the system of $q - p + 1 = n$ equations $g_1 = \cdots = g_{q-p+1} = 0$. Let $\overline{G} \in \mathbb{K}[\mathbf{X}]^{(p-1)\times(p-1)}$ be a submatrix of $G_{*;q-p+2:q}$, where $G_{*;q-p+2:q} \in \mathbb{K}[\mathbf{X}]^{p\times(p-1)}$ contains the columns $q-p+2, \dots, q$ of G. So, $\det(\overline{G}) = \lambda g_{q-p+2} \dots g_q$ for $\lambda \in \mathbb{K}^*$. By construction of $\{g_i\}_{i=1}^q$, we have $g_i(\mathbf{x}^*) \neq 0$ for all $q - p + 2 \leqslant i \leqslant q$. As a consequence, $\det(\overline{G})(\mathbf{x}^*) \neq 0$.

Furthermore, it can be verified that the Jacobian matrix of this system at $\mathbf{x}^*$ has full rank.

5.3 Row degrees

In this section, we will find a $(p-1) \times (p-1)$ submatrix of H, namely $\overline{H}$, such that $m(\mathbf{x}^*) \neq 0$, where $m = \det(\overline{H})$ and $\mathbf{x}^*$ is a solution of $\mathbf{g}$ when we work on the case $\deg(f_{i,j}) \leqslant D_i$ for all $1 \leqslant j \leqslant q$. Let us recall that a start matrix G in this case is

$$G = \begin{pmatrix} g_1 & 0 & \cdots & 0 & g_{1,p+1} & \cdots & g_{1,q} \\ 0 & g_2 & \cdots & 0 & g_{2,p+1} & \cdots & g_{2,q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_p & g_{p,p+1} & \cdots & g_{p,q} \end{pmatrix},$$

where all $\{g_i\}_{1\leqslant i\leqslant p}$ and $\{g_{k,j}\}_{1\leqslant k\leqslant p, p+1\leqslant j\leqslant q}$ have generic coefficients. We have seen that for any solution $\mathbf{x}^*$ of $\mathbf{g}$, there is at least one $i \in \{1, \dots, p\}$ such that $g_i(\mathbf{x}^*) = 0$.

If there is only one $i \in \{1, \dots, p\}$, without loss of generality we assume that $i = p$, such that $g_p(\mathbf{x}^*) = 0$ and $g_j(\mathbf{x}^*) \neq 0$ for $j \in \{1, \dots, p-1\}$; then we define $\overline{G} = \operatorname{diag}(g_1, \dots, g_{p-1})$. So, $\det(\overline{G})(\mathbf{x}^*) = \prod_{j=1}^{p-1} g_j(\mathbf{x}^*) \neq 0$.

If there are k polynomials $g_{i_1}, \dots, g_{i_k}$ for $(i_1, \dots, i_k) \subset \{1, \dots, p\}^k$ such that $g_{i_1}(\mathbf{x}^*) = \cdots = g_{i_k}(\mathbf{x}^*) = 0$ and $g_{i_j}(\mathbf{x}^*) \neq 0$ for $i_j \in \{1, \dots, p\} \setminus \{i_1, \dots, i_k\}$, we define $\overline{G} \in \mathbb{K}[\mathbf{X}]^{(p-1)\times(p-1)}$ as follows. Without loss of generality, let us work on $(i_1, \dots, i_k) = (p-k+1, \dots, p)$. For other tuples $(i_1, \dots, i_k)$, we can use the similar argument. The idea is using these g_{i_j} such that $g_{i_j}(\mathbf{x}^*) \neq 0$ to build the matrix $\overline{G}$. To sum up, we have $g_{p-k+1}(\mathbf{x}^*) = \cdots = g_p(\mathbf{x}^*) = 0$ and $g_j(\mathbf{x}^*) \neq 0$ for $1 \leqslant j \leqslant p-k$. Let us denote $A \in \mathbb{K}[\mathbf{X}]^{k\times(q-p)}$ for $G_{p-k+1:p;p+1:q}$. Then, by using the genericity assumption $\mathcal{A}(1)$, there exists a submatrix $G^* \in \mathbb{K}[\mathbf{X}]^{(k-1)\times(k-1)}$ of A such that $\det(G^*)(\mathbf{x}^*) \neq 0$. We have finished the existence of the matrix G^*, we are going to find where is G^* in A.

Since $G^* \in \mathbb{K}[\mathbf{X}]^{(k-1)\times(k-1)}$ is a submatrix of A such that $\det G^*(\mathbf{x}^*) \neq 0$, then $G^*(\mathbf{x}^*) \in \mathbb{K}^{(k-1)\times(k-1)}$ is a submatrix of $A(\mathbf{x}^*) \in \mathbb{K}^{k\times(q-p)}$ such that $G^*(\mathbf{x}^*)$ is full rank. Therefore, we can first, evaluate the matrix A at the point $\mathbf{x}^*$ to obtain the matrix $A(\mathbf{x}^*) \in \mathbb{K}^{k\times(q-p)}$; and after that, thanks to Gaussian eliminations we can find a submatrix $G^*(\mathbf{x}^*)$ of $A(\mathbf{x}^*)$ such that $\operatorname{rank}(G^*(\mathbf{x}^*)) = k-1$. We obtain the matrix $G^* \in \mathbb{K}[\mathbf{X}]^{(k-1)\times(k-1)}$ with the indices are the same as those of $G^*(\mathbf{x}^*)$. Finally, let us define $\overline{G}$ as

$$\overline{G} = \left[\begin{array}{c|c} \operatorname{diag}(g_1, \dots, g_{p-k}) & G_{1:p-k;\mathcal{J}} \\ \hline \mathbf{O}_{k-1,p-k} & G^* \end{array}\right] \in \mathbb{K}[\mathbf{X}]^{(p-1)\times(p-1)},$$

where $\mathcal{J}$ is the column indices set of G^*. Then, $\det(\overline{G}) = \prod_{j=1}^{p-k} g_j \cdot \det(G^*)$, for which we obtain $\det(\overline{G})(\mathbf{x}^*) \neq 0$.

For $\mathbf{x}^* \in V(\mathbf{g})$, the remaining problem in this subsection is to verify that this square subsystem has the Jacobian matrix of full rank at $\mathbf{x}^*$. Assume that $\ell_{p-k+1}(\mathbf{x}^*) = \cdots = \ell_p(\mathbf{x}^*) = 0$, where ℓ_i

is a linear form of g_i. Let $I_A \subset \mathbb{K}[X_{k+1}, \ldots, X_n]$ be the ideal generated by all $k \times k$ minors of A, where A is the matrix is defined as above. Let $\mathbf{g}_{\mathbf{x}^*}$ be the localization of $\mathbf{g}$ at $\mathbf{x}^*$. We claim that

$$\mathbf{g}_{\mathbf{x}^*} = \langle \ell_{p-k+1}, \ldots, \ell_p \rangle + I_A. \tag{5}$$

If eq. (5) holds, then $\mathbf{g}_{\mathbf{x}^*} = I_A + \langle X_1 + \ell_{p-k+1}, \ldots, X_k + \ell_p \rangle$. As a consequence,

$$\mathbb{K}[[\mathbf{X}]]/\mathbf{g}_{\mathbf{x}^*} \simeq \mathbb{K}[[\mathbf{X}]]/I_A + \langle X_1 + \ell_{p-k+1}, \ldots, X_k + \ell_p \rangle \simeq \mathbb{K}[[X_{k+1}, \ldots, X_n]]/I_A \simeq \mathbb{K},$$

which implies $\dim \mathbb{K}[[\mathbf{X}]]/\mathbf{g}_{\mathbf{x}^*} = 1$. In other words, the multiplicity of $\mathbf{x}^*$ is one [**?**, Appendix A].

In order to obtain eq. (5), we use the fact that any $(k-1) \times (q-p)$ submatrix of A has full rank at $\mathbf{x}^*$.

6 Homotopy techniques for determinantal systems

Given a multivariate polynomial matrix $F \in \mathbb{K}[\mathbf{X}]^{p \times q}$ with the number of variables is $q - p + 1$ and $p \leqslant q$; in this section, we build an algorithm by using the symbolic homotopy techniques to compute the isolated solutions of the determinantal system made by all $p \times p$ minors of F.

Let us denote $\mathbf{f} = (f_1, \ldots, f_M) \in \mathbb{K}[\mathbf{X}]^M$ be the system of $p \times p$ minors of the input matrix $F \in \mathbb{K}[\mathbf{X}]^{p \times q}$ with $M = \binom{q}{p}$. Let $G \in \mathbb{K}[\mathbf{X}]^{p \times q}$ be a start matrix and T be a new variable. Let us define the homotopy $H = (1-T)G + T.F \in \mathbb{K}[T, \mathbf{X}]^{p \times q}$. We denote $\mathbf{g} = (g_1, \ldots, g_M)$ in $\mathbb{K}[\mathbf{X}]^M$ and $\mathbf{h} = (h_1, \ldots, h_M)$ in $\mathbb{K}[T, \mathbf{X}]^M$ for the determiantal system of G and H, respectively.

6.1 Testing a point is isolated

Let $\mathbf{f} = (f_1, \ldots, f_M)$ be polynomials in $\mathbb{K}[\mathbf{X}]$, with $\mathbf{X} = (X_1, \ldots, X_n)$, for a field $\mathbb{K}$. Given a point $\mathbf{x}$ in $V(\mathbf{f})$, we discuss here how to decide whether $\mathbf{x}$ is an isolated point in $V(\mathbf{f})$. Without loss of generality, we assume that $M \geqslant n$; otherwise, $\mathbf{x}$ cannot be an isolated solution. In the determinantal system context, M equals $\binom{q}{p}$, the number of $p \times p$ minors of F and $M \geqslant n$. We make the following assumption (denoted by H below): we are given as input an integer μ such that

- either $\mathbf{x}$ belongs to a positive-dimensional component of $V(\mathbf{f})$,
- or $\mathbf{x}$ is isolated in $V(\mathbf{f})$, with multiplicity at most μ with respect to the ideal $\langle \mathbf{f} \rangle$.

Proposition 6.1. *Suppose that* $\mathbf{f}$ *is given by a straight-line program of length* $\mathcal{E}$*. If assumption* H *is satisfied, we can decide whether* $\mathbf{x}$ *is an isolated root of* $V(\mathbf{f})$ *using* $(\mu\, \mathcal{E}\, M)^{O(1)}$ *operations in* $\mathbb{K}$*.*

Proof. The proof is given in appendix C. □

6.2 Computing the isolated solutions for determinantal systems

Given polynomials $\mathbf{f} = (f_1, \ldots, f_M) \in \mathbb{K}[\mathbf{X}]^M$, we give an algorithm to compute a zero-dimensional parametrization of the isolated points of $V(\mathbf{f})$. All the notation of the previous subsection is still in use. In order to control the cost of the algorithm, we introduce the following assumptions:

A_1 Given $\mathbf{x} \in V(\mathbf{h}_0)$ having coordinates in a field extension $\mathbb{L}$ of $\mathbb{K}$, we can find in time $O\tilde{}(B\,[\mathbb{L} : \mathbb{K}])$ a sequence $\boldsymbol{i}_{\mathbf{x}} = (i_1, \ldots, i_n)$, with $1 \leqslant i_1 < \cdots < i_n \leqslant M$, such that the Jacobian matrix of $(h_{0,i_1}, \ldots, h_{0,i_n})$ has full rank n at $\mathbf{x}$, for some B independent of $\mathbf{x}$.

A_2 We know an integer d such that the curve $V(J')$ has degree at most d. Lemma D.1 implies that $c \leqslant d$.

A_3 For any $\boldsymbol{i} = (i_1, \ldots, i_n)$, with $1 \leqslant i_1 < \cdots < i_n \leqslant M$, we can compute $(h_{i_1}, \ldots, h_{i_n})$ using a straight-line program of length $\mathcal{E}$.

Proposition 6.2. *Using the previous assumptions, we can compute a zero-dimensional parametrization of the isolated points of of $V(\mathbf{f})$ using $(Bc + d\,\mathcal{E}\,M)^{\mathcal{O}(1)}$ operations in $\mathbb{K}$.*

In the determinantal systems context, for the assumption A_1, as we discuss in Section 5, given $\mathbf{x} \in V(\mathbf{h}_0)$, we can find $\boldsymbol{i}_{\mathbf{x}}$ in $\mathcal{O}(1)$ for the column degrees case; and for the row degrees case, B is in function of evaluating point $\mathbf{x}$ in $\overline{G}$ and the complexity of Gaussian eliminations. The homotopy matrix is constructed from the start matrix G and the target matrix F. Then, the degree of the curve $V(J')$ is at most either $E_n(D_1 + 1, \ldots, D_q + 1)$ in the case of column degree or $S_n(D_1 + 1, \ldots, D_p + 1)$ in the row degrees case; and for any $\boldsymbol{i} = (i_1, \ldots, i_n)$, with $1 \leqslant i_1 < \cdots < i_n \leqslant M$, we can compute $(h_{i_1}, \ldots, h_{i_n})$ using a straight-line program of length $(\mathcal{E})^{\mathcal{O}(1)}$, where $\mathcal{E}$ is the length of a straight-line program of the input matrix F.

Starting points. The algorithm starts by using the set of solution of the determiantal system of a start matrix which is defined as in Section 3.2. We can use either Algorithm 1 for column degrees case or Algorithm 2 for the case of row degrees. We denote this set as $V(\mathbf{g})$; and $|V(\mathbf{g})| = \mathcal{T}$ with $\mathcal{T} = E_n(D_1, \ldots, D_q)$ in column degrees case or $\mathcal{T} = S_n(D_1, \ldots, D_p)$ in row degrees case. For $j = 1, \ldots, \mathcal{T}$, from A_1, we can find $\boldsymbol{i}_{\mathbf{x}}$ such that $(h_{0,i})_{i \in \boldsymbol{i}_{\mathbf{x}}}$ has full rank n. By using the assumption A_1, the runtime in this step is $(B\,\mathcal{T})^{\mathcal{O}(1)}$.

Lifting power series and rational reconstruction. For $j = 1, \ldots, \mathcal{T}$, we apply the Newton iteration to the system $(h_{0,i})_{i \in \boldsymbol{i}_{\mathbf{x}}}$ to lift $\mathbf{x}$ into a zero-dimensional parametrization $\mathscr{R}_j = ((q_j, v_{j,1}, \ldots, v_{j,n}), \lambda)$ with coefficients in $\mathbb{K}[[T]]/\langle T^{2d}\rangle$, for d as in A_2.

As explained in [**?**, Section 2.2], using the algorithm of [**?**], this can be done using $(d\,\mathcal{E}\,n)^{\mathcal{O}(1)}$ operations in $\mathbb{K}$. Using the Chinese Remainder Theorem, we can combine all $\mathscr{R}_j$ into a single zero-dimensional parametrization $\mathscr{R}$ with coefficients in $\mathbb{K}[[T]]/\langle T^{2d}\rangle$; this can be done in $(dn)^{\mathcal{O}(1)}$.

Using the notation of the previous subsection and let $\Phi_1, \ldots, \Phi_c$ be the points of $V(\mathfrak{J}')$, with coordinates taken in $\overline{\mathbb{K}}\langle\langle T\rangle\rangle$, then the zeros of $\mathscr{R}$ in $\overline{\mathbb{K}}[[T]]/\langle T^{2d}\rangle$ are truncations of $\Phi_1, \ldots, \Phi_c$. Moreover, from A_2, J' is supposed to has degree at most d, knowing $\mathscr{R}$ at precision $2d$ allows us to reconstruct a zero-dimensional parametrization $\mathscr{S}$ with coefficients in $\mathbb{K}(T)$ such that the zeros of $\mathscr{S}$ is $V(\mathfrak{J}')$. This is done by applying rational function reconstruction to all coefficients of $\mathscr{R}$, as in [**?**], and takes time $(d\,n)^{\mathcal{O}(1)}$. Without loss of generality, by multiplying all denominators of $\mathscr{R}$ coefficients in $\mathbb{K}(T)$ by the least common multiple of theirs, we can deduce that all polynomials of $\mathscr{R}$, say $q, v_1, \ldots, v_n$, have coefficients in $\mathbb{K}[T]$. The degree bounds in [**?**] show that if we require that $q, v_1, \ldots, v_n$ are in $\mathbb{K}[T][U]$ and without a common factor in $\mathbb{K}[T]$, their total degrees are at most d, so this normalization can be computed using $(d\,n)^{\mathcal{O}(1)}$ operations in $\mathbb{K}$.

A finite set containing the isolated points of $V(\mathbf{f})$. Let us denote $J_1' = J + \langle T - 1\rangle$, then it can be seen in the proof of Lemma D.4 that $V(J_1')$ is finite. In addition, Lemma D.1 implies that for any isolated solution $\mathbf{x}$ of $\mathbf{f}$, $(1, \mathbf{x})$ is in $V(J_1')$. So, we first deduce from $\mathscr{S}$ a zero-dimensional parametrization $\mathscr{R}_1$ with coefficients in $\mathbb{K}$ of $V(J_1')$; and then by using the algorithm of Section 6.1, we discard from $V(J_1')$ those points that do not correspond to isolated points of $V(\mathbf{f})$. The complexity for testing isolated step is $(d\,\mathcal{E}\,M)^{\mathcal{O}(1)}$.

Let $\Phi'_1, \ldots, \Phi'_c$ be the roots of $\mathfrak{J}'$ in the field of Puiseux series $\overline{\mathbb{K}}\langle\langle T'\rangle\rangle$ at $T = 1$, where $T' = T-1$. Without loss of generality, we assume that $\Phi'_1, \ldots, \Phi'_\kappa$ are bounded, and $\Phi'_{\kappa+1}, \ldots, \Phi'_c$ are not, for some κ in $\{0, \ldots, c\}$, and we let $\varphi'_1, \ldots, \varphi'_\kappa$ by $\varphi'_i = \lim_0(\Phi'_i) \in \overline{\mathbb{K}}^n$ for $i = 1, \ldots, \kappa$, where $\lim_0(\Phi'_i)$ is the coefficient of T^0 in φ'_i. By Lemma D.5, $V(J' + \langle T-1\rangle) = \{\varphi'_i \mid i = 1, \ldots, k\}$. Lemma 4.4 in [**?**] then shows how to recover a zero-dimensional parametrization $\mathscr{R}_1 = ((q_1, v_{1,1}, \ldots, v_{1,n}), \lambda)$ with coefficients in $\mathbb{K}$ for the limit set $\{\varphi'_i \mid i = 1, \ldots, \kappa\}$ starting from $\mathscr{S}$, under some conditions on the linear form λ. Following [**?**] and [**?**], we ask that λ is a well-separating element,

1. λ is separating for $V(\mathfrak{J}') = \{\Phi'_1, \ldots, \Phi'_c\}$;
2. λ is separating for $V(J' + \langle T-1\rangle) = \{\varphi'_1, \ldots, \varphi'_{\kappa'}\}$.
3. $\nu(\lambda(\Phi_i)) = \mu_i$ for all $i = 1, \ldots, c$, where ν denotes the T'-adic valuation.

These conditions are satisfied for a generic choice of λ, as showed in [**?**]. When this is the case, Lemma 4.4 in [**?**] shows how to recover a zero-dimensional parametrization $\mathscr{R}_1$ with coefficients in $\mathbb{K}$ for the limit set $\{\varphi'_i \mid i = 1, \ldots, \kappa\}$ starting from $\mathscr{S}$, in time $(d\,n)^{\mathcal{O}(1)}$.

6.3 Algorithms.

We give an algorithm called Algorithm 3 to compute the isolated solutions set, S, for the determinanal system $\mathbf{f}$ when knowing the solution set $V(\mathbf{g})$ of the determinantal system of a start matrix. We denote $\mathscr{R}_1$ for a zero-dimensional parametrization with coefficients in $\mathbb{K}$ such that $S \subset \mathscr{R}_1$. Let $H \in \mathbb{K}[T, \mathbf{X}]^{p\times q}$ be defined as before, that is $H = (1-T)\cdot G + T \cdot F$. For each $\mathbf{x} \in V(\mathbf{g})$, let $\mathbf{h}^{(\mathbf{x})}$ in $\mathbb{K}[T, \mathbf{X}]^n$ a square subsystem such that $\mathbf{h}^{(\mathbf{x})}(0, \mathbf{x}) = 0$ and the Jacobian matrix of $\mathbf{h}^{(\mathbf{x})}$ has full rank n at $\mathbf{x}$. If we use Proposition 6.2 in determinantal system context when $M = \binom{q}{p}$ the number of $p \times p$ minors of the input matrix F, d is either $E_n(D_1+1, \ldots, D_q+1)$ or $S_n(D_1+1, \ldots, D_p+1)$, $c \leqslant d$, $\mathcal{E}$ is the length of a straight-line program of the input matrix F, $B = (\mathcal{E}q)^{\mathcal{O}(1)}$ and the fact that $d = \mathcal{T}^{\mathcal{O}(1)}$ where $\mathcal{T}$ is either $E_{q-p+1}(D_1, \ldots, D_q)$ in the column degrees case, or $S_{q-p+1}(D_1, \ldots, D_p)$ in the row degrees case, we obtain the following result.

Theorem 6.1. *The Algorithm 3 is correct and its complexity is* $\left(\binom{q}{p}\,\mathcal{E}\,\mathcal{T}\right)^{\mathcal{O}(1)}$ *operations in* $\mathbb{K}$.

In summary, if the input matrix is $F \in \mathbb{K}[\mathbf{X}]^{p\times q}$ such that $p \leqslant q$ and $\deg(f_{i,j}) \leqslant D_j$ for all $1 \leqslant i \leqslant p$, we will use the Algorithm 4; and if the input matrix is $F \in \mathbb{K}[\mathbf{X}]^{p\times q}$ such that $p \leqslant q$ and $\deg(f_{i,j}) \leqslant D_i$ for all $1 \leqslant i \leqslant q$, we can use the Algorithm 5 for the Problem 1.

7 Conclusions and future research

Given a field $\mathbb{K}$ and a matrix F in multivariate polymomial ring $\mathbb{K}[\mathbf{X}]$, in this report, we design an algorithm to compute the set of points with coordinates in algebraically closed field $\overline{\mathbb{K}}$ such that at those points the matrix does not have full rank. Our algorithm mainly uses the symbolic homopoty approach.

In the future, we would like to study how symbolic homotopy techniques could be applied in the more general question, that is given a field $\mathbb{K}$, a matrix $F \in \mathbb{K}[\mathbf{X}]^{p\times q}$ and an integer $r \leqslant \min(p, q)$, compute the points in $\overline{\mathbb{K}}^n$, at which the rank of the matrix is at most r. We also would like to study the polynomial systems solving with structures input systems, for instance, symetries, multi-homogeneity.

Algorithm 3 DeterminantalSystem

Input: a matrix $F \in \mathbb{K}[\mathbf{X}]^{p\times q}$ with $p \leqslant q$, the set $V(\mathbf{g})$.
Output: the isolated solutions set of $\mathbf{f}$.

1. for any $\mathbf{x} \in V(\mathbf{g})$:
   1.1. find a system $\mathbf{h}^{(\mathbf{x})}$ in $\mathbb{K}[T, \mathbf{X}]^n$
   1.2. compute $\mathscr{R}_{\mathbf{x}}$ zero-dimensional parametrization at precision $2d$.
   // $*$ use algorithm in [**?**]
2. combine $\{\mathscr{R}_{\mathbf{x}}\}_{\mathbf{x}\in V(\mathbf{g})}$ into $\mathscr{R}$
3. compute $\mathscr{S}$ with coefficients in $\mathbb{K}(T)$ from $\mathscr{R}$
   // $*$ apply RationalReconstruction algorithm in [**?**] to all coefficients of $\mathscr{R}$ at degree d
4. clean denominators of $\mathscr{S}$
5. deduce $\mathscr{R}_1$ from $\mathscr{S}$
6. $S \leftarrow$ removing from $\mathscr{R}_1$ non-isolated points of $V(\mathbf{f})$
   // $*$ apply algorithm in section 6.1
7. return S

Algorithm 4 ColumnDeterminantalSystem

Input: a matrix $F \in \mathbb{K}[\mathbf{X}]^{p\times q}$ with $p \leqslant q$ and $\deg(f_{i,j}) \leqslant D_j$ for all $1 \leqslant i \leqslant p$.
Output: the isolated solutions set of $\mathbf{f}$.

1. define a column start matrix $G \in \mathbb{K}[\mathbf{X}]^{p\times q}$ as in Section 3.2
2. $V(\mathbf{g}) \leftarrow$ StartMatrixColumnDegrees(G)
3. return DeterminantalSystem($F, V(\mathbf{g})$)

Algorithm 5 RowDeterminantalSystem

Input: a matrix $F \in \mathbb{K}[\mathbf{X}]^{p\times q}$ with $p \leqslant q$ and $\deg(f_{i,j}) \leqslant D_i$ for all $1 \leqslant j \leqslant q$.
Output: the isolated solutions set of $\mathbf{f}$.

1. define a row start matrix $G \in \mathbb{K}[\mathbf{X}]^{p\times q}$ as in Section 3.2
2. $V(\mathbf{g}) \leftarrow$ StartMatrixRowDegrees(G)
3. return DeterminantalSystem($F, V(\mathbf{g})$)

8 Acknowledgements

I would like to gratefully thank my two supervisors for giving me interesting research problems during my internship. They were fully available for answering all of my questions. I would also like to thank Labex Milyon for giving me a scholarship to come to ENS Lyon for studying. I acknowledge financial support provided by the scholarship *Explora Doc* from *Région Rhône-Alpes, France.*

A Proof of Propositon 3.1

Let $N = q(n+1)(\sum_{i=1}^{p} D_i)$ be the cardinality of the set $\mathcal{G}$. We notice that we are working on $n = q - p + 1$, where n is the number of variables. Let us define the matrices G_1 and G_2 as follow

$$G_1 = \begin{pmatrix} \mathfrak{g}_{1,1} & \mathfrak{g}_{1,2} & \cdots & \mathfrak{g}_{1,q} \\ \mathfrak{g}_{2,1} & \mathfrak{g}_{2,2} & \cdots & \mathfrak{g}_{2,q} \\ \vdots & \vdots & \ddots & \vdots \\ \mathfrak{g}_{p,1} & \mathfrak{g}_{p,2} & \cdots & \mathfrak{g}_{p,q} \end{pmatrix} \text{ and } G_2 = \begin{pmatrix} \mathfrak{g}_{1,1} & 0 & \cdots & 0 & \mathfrak{g}_{1,p+1} & \cdots & \mathfrak{g}_{1,q} \\ 0 & \mathfrak{g}_{2,2} & \cdots & 0 & \mathfrak{g}_{2,p+1} & \cdots & \mathfrak{g}_{2,q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathfrak{g}_{p,p} & \mathfrak{g}_{p,p+1} & \cdots & \mathfrak{g}_{p,q} \end{pmatrix}.$$

The idea to prove $\mathcal{A}(k)$, for any $k \in \{1,2,3\}$, is by using induction on the number of variables n for the matrix of form G_1. Using the induction properties for smaller values of n, we show that property $\mathcal{A}(k)$ is true for the matrix G_2. Finally, by using this property of form G_2, we prove by a geometric argument that $\mathcal{A}(k)$ holds for any matrix of form G_1. In this section, given a polynomial matrix G and an integer $k < p$, we denote I_G for the ideal generated by all $p \times p$ minors of G and $I_G^{(k)}$ for the ideal generated by all $k \times k$ minors of G.

A.1 Genericity of $\mathcal{A}(1)$

We use the fact that for any $\mathbf{x}^* \in V(I_G)$, the rank of the matrix $G(\mathbf{x}^*)$ is exactly $p-1$ if $\mathbf{x}^*$ does not belong to the variety of the ideal generated by $(p-1) \times (p-1)$ minors of G. Indeed, if $\mathbf{x}^* \in V(I_G^{(p-1)})$ where $I_G^{(p-1)} = \langle (p-1) \times (p-1) - \text{minors of } G \rangle$, then $\text{rank}(G(\mathbf{x}^*)) \leqslant p-2$.

Step 1 : First, we prove that there exists a non-empty Zariski open set $\mathcal{O}_1$ such that I_{G_1} satisfies $\mathcal{A}(1)$ for $g_{i,j} \in \mathcal{O}_1$, when G_1 is a square matrix as follows

$$G_1 = \begin{pmatrix} \mathfrak{g}_{1,1} & \cdots & \mathfrak{g}_{1,p} \\ \vdots & \ddots & \vdots \\ \mathfrak{g}_{p,1} & \cdots & \mathfrak{g}_{p,p} \end{pmatrix}.$$

We notice that in this case, the number of variables is $n = 1$ and the number of coefficients is $N = 2q.(\sum_{i=1}^{p} D_i)$. Let us define $I_{G_1}^{(p-1)} := \langle (p-1) \times (p-1) - \text{minors of } G_1 \rangle \subset \mathbb{K}[\mathcal{G}, \mathbf{X}]$ and $\Omega_1 = V(I_{G_1}^{(p-1)}) \subset \overline{\mathbb{K}}^N \times \mathbb{P}^1(\overline{\mathbb{K}})$. Then, Ω_1 is a Zariski closed in $\overline{\mathbb{K}}^N \times \mathbb{P}^1(\overline{\mathbb{K}})$. Let $\pi_{\mathcal{G}} : \overline{\mathbb{K}}^N \times \mathbb{P}^1(\overline{\mathbb{K}}) \to \overline{\mathbb{K}}^N$ be the projection on the $\mathcal{G}$ coordinates and $\Delta_1 = \pi_{\mathcal{G}}(\Omega_1)$. This implies Δ_1 is a Zariski closed in $\overline{\mathbb{K}}^N$. So, we define the Zariski open set $\mathcal{O}_1$ in $\overline{\mathbb{K}}^N$ as $\mathcal{O}_1 := \overline{\mathbb{K}}^N \setminus \Delta_1$. We claim that $\mathcal{O}_1$ is a non-empty set. Indeed, let $G_2 = \text{diag}(\mathfrak{g}_{1,1}, \ldots, \mathfrak{g}_{1,1})$ be a diagonal matrix and $I_{G_2}^{(p-1)} := \langle (p-1) \times (p-1) - \text{minors of } G_2 \rangle \subset \mathbb{K}[\mathcal{G}, \mathbf{X}]$. Therefore, for any $f_{G_2} \in I_{G_2}^{(p-1)}$, f_{G_2} has the form $\mathfrak{g}_{i_1,i_1} \ldots \mathfrak{g}_{i_{p-1},i_{p-1}}$ where $(i_1, \ldots, i_{p-1}) \in \{1, \ldots, p\}^{p-1}$. Moreover, for any $1 \leqslant i \leqslant p$, we have $\mathfrak{g}_{i,i} = (\gamma_{i,i}^{(1,1)} X_1 + \gamma_{i,i}^{(0,1)}) \times \cdots \times (\gamma_{i,i}^{(1,D_i)} X_1 + \gamma_{i,i}^{(0,D_i)})$. So, for any $(\mathfrak{g}^*, \mathbf{x}^*) \in V(I_{G_2}^{(p-1)})$, it

is the solution of $\gamma_{i,i}^{(1,t)}X_1 + \gamma_{i,i}^{(0,t)}X_0 = 0$ for $0 \leqslant t \leqslant D_i$. This equation always has solution in $\overline{\mathbb{K}}^2 \times \mathbb{P}^1(\overline{\mathbb{K}})$. This implies, if we define $\overline{\Omega}_1 := V(I_{G_2}^{(p-1)}) \in \overline{\mathbb{K}}^{N_2} \times \mathbb{P}^1(\overline{\mathbb{K}})$, $\overline{\Omega}_1$ will be a Zariski closed in $\overline{\mathbb{K}}^{N_2} \times \mathbb{P}^1(\overline{\mathbb{K}})$, where $N_2 = 2.(\sum_{i=1}^{p} D_i)$ is the number of generic coefficients for G_2. Finally, let us define $\overline{\Delta}_1$ as $\pi_{\overline{\mathcal{G}}}(\overline{\Omega}_1)$, where $\pi_{\overline{\mathcal{G}}} : \overline{\mathbb{K}}^{N_2} \times \mathbb{P}^1(\overline{\mathbb{K}}) \to \overline{\mathbb{K}}^{N_2}$; and $\overline{\mathcal{O}}_1 = \overline{\Delta}_1 \times 0^{N_1}$ which is non-empty set, where $N_1 = N - N_2$; and it can be seen that $\overline{\mathcal{O}}_1 \subset \mathcal{O}_1$. As a consequence, $\mathcal{O}_1$ is non-empty. We finished the first step of induction.

Step 2 : Let us now assume that $\mathcal{A}(1)$ holds for any $G_1 \in \mathbb{K}[\mathcal{G}, \mathbf{X}]^{p' \times q'}$ for any $n' \leqslant n$, where $n' = q' - p' + 1$; we prove $\mathcal{A}(1)$ is also true for $G_2 \in \mathbb{K}[\mathcal{G}, \mathbf{X}]^{p \times q}$ with $n = q - p + 1$. Note that $I_{G_2}^{(p-1)}$ contains $g_{i_1,i_1} \dots g_{i_{p-1},i_{p-1}}$ for any $(i_1, \dots, i_{p-1}) \in \{1, \dots, p\}^{p-1}$ and $i_j \neq i_t$. For any $(\mathfrak{g}^*, \mathbf{x}^*) \in (\overline{\mathbb{K}}^{N_2} \times \mathbb{P}^n(\overline{\mathbb{K}})) \cap V(I_{G_2}^{(p-1)})$, there are at least two $1 \leqslant j, t \leqslant p, j \neq t$ such that $\mathfrak{g}_{j,j}(\mathfrak{g}^*, \mathbf{x}^*) = \mathfrak{g}_{t,t}(\mathfrak{g}^*, \mathbf{x}^*) = 0$. If there are k numbers $i_1, \dots, i_k$, where $2 \leqslant k \leqslant \min(n, p)$, such that $g_{i_1,i_1}(\mathfrak{g}^*, \mathbf{x}^*) = \cdots = g_{i_k,i_k}(\mathfrak{g}^*, \mathbf{x}^*) = 0$, we define $\mathcal{J}_k = (i_1, \dots, i_k)$ and $G_{\mathcal{J}_k,p+1:q} \in \mathbb{K}[\mathcal{G}, \mathbf{X}]^{(n-k)\times(q-p)}$ is the submatrix of G_2 that contains the rows $\mathcal{J}_k$ and columns $p+1, \dots, q$. By using the similar argument as in Proposition 3.2, we have $\operatorname{rank}(G_{\mathcal{J}_k,p+1:q}(\mathfrak{g}^*, \mathbf{x}^*)) = k - 1$ for which the property $\mathcal{A}(1)$ holds as from induction hypothesis. Moreover,

$$V(I_{G_2}^{(p-1)}) = \bigcup_{\mathcal{J}_k \subset \{1,\dots,p\}^k,\ 2 \leqslant k \leqslant \min(n,p)} V(I_{\mathcal{J}_k}),$$

where $I_{\mathcal{J}_k}$ is the ideal generated by $\mathfrak{g}_{i,i}$ for $i \in \mathcal{J}_k$ and all $(k-2) \times (k-2)-$ minors of $G_{\mathcal{J}_k,p+1:q}$. Therefore, we can define a non-empty Zariski open, $\overline{\mathcal{O}}_1$, for G_2 as follows. For any $\mathcal{J}_k \subset \{1, \dots, p\}^k$, we rewrite $(X_1, \dots, X_k) \in \mathbb{K}[\mathcal{G}, X_{k+1}, \dots, X_n]^k$ and substitute into $G_{\mathcal{J}_k,p+1:q}$ to obtain $G_{\mathcal{J}_k,p+1:q} \in \mathbb{K}[\mathcal{G}, X_{k+1}, \dots, X_n]^{k\times(q-p)}$. By using the induction hypothesis, for any $\mathcal{J}_k$, there exists a Zariski closed set $\Delta_{\mathcal{J}_k} \subsetneq \overline{\mathbb{K}}^{N_{\mathcal{J}_k}}$, where $N_{\mathcal{J}_k} = n(q-p+1)(\sum_{i \in \mathcal{J}_k} D_i)$ is the number of coefficients of the matrix $[\operatorname{diag}(g_{i_1,i_1}, \dots, g_{i_k,i_k}) | G_{\mathcal{J}_k,p+1:q}]$. We finally, define

$$\overline{\mathcal{O}}_1 = \overline{\mathbb{K}}^{N_2} \setminus \Delta, \text{ where } N_2 = n(q-p+1)(\sum_{i=1}^{p} D_i) \text{ and } \Delta = \bigcup_{\mathcal{J}_k \subset \{1,\dots,p\}^k,\ 2 \leqslant k \leqslant \min(n,p)} \Delta_{\mathcal{J}_k}.$$

This is a nonempty Zariski open set in $\overline{\mathbb{K}}^{N_2}$ such that I_{G_2} satisfies $\mathcal{A}(1)$ when $g_{i,j} \in \overline{\mathcal{O}}_1$ which ends the second step of the proof.

Step 3 : Finally, let assume that $\mathcal{A}(1)$ holds for any $G_2 \in \mathbb{K}[\mathcal{G}, \mathbf{X}]^{p \times q}$, we prove $\mathcal{A}(1)$ is also true for any $G_1 \in \mathbb{K}[\mathcal{G}, \mathbf{X}]^{p \times q}$ as follows. Let us define $I_{G_1}^{(p-1)} = \langle (p-1) \times (p-1) - \text{minors of } G_1 \rangle$ and $\Omega_1 = V(I_{G_1}^{(p-1)}) \subset \overline{\mathbb{K}}^N \times \mathbb{P}^n(\overline{\mathbb{K}})$ is a Zariski closed. Similarly as in the first step, we define $\Delta_1 = \pi_{\mathcal{G}}(\Omega_1)$ is a Zariski closed in $\overline{\mathbb{K}}^N$, where $\pi_{\mathcal{G}} : \overline{\mathbb{K}}^N \times \mathbb{P}^n(\overline{\mathbb{K}}) \to \overline{\mathbb{K}}^N$ is a projection. So, we define the Zariski open set $\mathcal{O}_1$ in $\overline{\mathbb{K}}^N$ as $\mathcal{O}_1 := \overline{\mathbb{K}}^N \setminus \Delta_1$. By using the matrix G_1 of the form as in the second step and similar argument as the first step, we can deduce that $\mathcal{O}_1$ is non-empty.

We finished the proof for the property $\mathcal{A}(1)$.

A.2 Genericity of $\mathcal{A}(2)$

Step 1 : We show here that there exists a non-empty Zariski open set $\mathcal{O}_2$ such that I_{G_1} has $S_1(D_1, \dots, D_p)$ (that is $\sum_{i=1}^{p} D_i$) distinct solutions for $\mathfrak{g}_{i,j} \in \mathcal{O}_2$, when G_1 is a square matrix as follows

$$G_1 = \begin{pmatrix} \mathfrak{g}_{1,1} & \cdots & \mathfrak{g}_{1,p} \\ \vdots & \ddots & \vdots \\ \mathfrak{g}_{p,1} & \cdots & \mathfrak{g}_{p,p} \end{pmatrix}.$$

We notice that in this case, each $\mathfrak{g}_{i,j}$ has the form $\mathfrak{g}_{i,j} = (\gamma_{i,j}^{(1,1)}X_1+\gamma_{i,j}^{(0,1)})\times\cdots\times(\gamma_{i,j}^{(1,D_i)}X_1+\gamma_{i,j}^{(0,D_i)})$. Let us denote $m \in \mathbb{K}[\mathcal{G}, X_1]$ for the determinant of G_1, then m is homogeneous in $\mathcal{G}$ of degree p and $\deg_X(m) = \sum_{i=1}^{p} D_i$. Indeed, the coefficient of X_1^d, where $d = \sum_{i=1}^{p} D_i$, in m is $\det(A)$, where

$$A = \begin{pmatrix} \prod_{l=1}^{D_1}\gamma_{1,1}^{(1,l)} & \cdots & \prod_{l=1}^{D_1}\gamma_{1,p}^{(1,l)} \\ \vdots & \ddots & \vdots \\ \prod_{l=1}^{D_p}\gamma_{1,1}^{(1,l)} & \cdots & \prod_{l=1}^{D_p}\gamma_{1,p}^{(1,l)} \end{pmatrix} \in \mathbb{K}[\mathcal{G}]^{p\times p}.$$

which has non-zero determinant. Moreover, in order to obtain the condition that m has $\sum_{i=1}^{p} D_i$ distinct solutions we use $\mathrm{Res}_{X_1}(m, \frac{\partial m}{\partial X_1}) \neq 0$, where $\mathrm{Res}_{X_1}(m, \frac{\partial m}{\partial X_1})$ is the resultant between m and the derivative of m with respect to X_1. So, we can define $\mathcal{O}_2$ as follows.

Let $\Omega_2 = V(\mathrm{Res}_{X_1}(m, \frac{\partial m}{\partial X_1})) \subset \overline{\mathbb{K}}^N \times \mathbb{P}^1(\overline{\mathbb{K}})$ is a Zariski closed, where here $N = 2p(\sum_{i=1}^{p} D_i)$ is the number of coefficients for G_1. Then, we define $\Delta_2 = \pi_{\mathcal{G}}(\Omega_2) \subset \overline{\mathbb{K}}^N$ is a Zariski closed and take $\mathcal{O}_2$ as $\overline{\mathbb{K}}^N \setminus \Delta_2$ is a Zariski open. Therefore, for any $\mathfrak{g}_{i,j} \in \mathcal{O}_2$, we have m has $\sum_{i=1}^{p} D_i$ solutions. We need to check that $\mathcal{O}_2$ is non-empty. In order to finish this part, we use the matrix G_2 as a diagonal matrix $\mathrm{diag}(\mathfrak{g}_{1,1}, \ldots, \mathfrak{g}_{p,p})$ where $\mathfrak{g}_{i,i} = \prod_{l=1}^{D_i}(\gamma_{i,i}^{(1,l)}X_1 + \gamma_{i,i}^{(0,l)})$. Furthermore, the determinat of G_2 has the form $\prod_{i=1}^{p}\mathfrak{g}_{i,i}$, i.e., $\prod_{i=1}^{p}\prod_{l=1}^{D_i}(\gamma_{i,i}^{(1,l)}X_1 + \gamma_{i,i}^{(0,l)})$. Then, $\det(G_2)$ always has $\sum_{i=1}^{p} D_i$ distinct solutions. Therefore, $\overline{\mathbb{K}}^{N_2} \times 0^{N_1} \subset \mathcal{O}_2$ which implies that $\mathcal{O}_2$ is nonempty.

Step 2 : Let us now assume that $\mathcal{A}(2)$ holds for any $G_1 \in \mathbb{K}[\mathcal{G}, \mathbf{X}]^{p'\times q'}$ for any $n' \leqslant n$, where $n' = q' - p' + 1$; we prove $\mathcal{A}(2)$ is also true for $G_2 \in \mathbb{K}[\mathcal{G}, \mathbf{X}]^{p\times q}$ with $n = q - p + 1$. We follow the similar argument as in the second step of the proof for $\mathcal{A}(1)$. Here, instead of considering the ideal $I_{G_2}^{(p-1)}$, we consider the ideal I_{G_2} which is generated by $p \times p$ minors of G_2. We have that I_{G_2} contains $\mathfrak{g}_{1,1}\ldots\mathfrak{g}_{p,p}$. Then, for any solution, $(\mathfrak{g}^*, \mathbf{x}^*) \in \overline{\mathbb{K}}^{N_2} \times \mathbb{P}^n(\overline{\mathbb{K}})$ of I_{G_2}, there is at least one $i \in \{1, \ldots, p\}$ such that $\mathfrak{g}_{i,i}(\mathfrak{g}^*, \mathbf{x}^*) = 0$. If there are k numbers $i_1, \ldots, i_k$, where $1 \leqslant k \leqslant \min(n, p)$, such that $g_{i_1,i_1}(\mathfrak{g}^*, \mathbf{x}^*) = \cdots = g_{i_k,i_k}(\mathfrak{g}^*, \mathbf{x}^*) = 0$, we define $\mathcal{J}_k = (i_1, \ldots, i_k)$ and $G_{\mathcal{J}_k,p+1:q} \in \mathbb{K}[\mathcal{G}, \mathbf{X}]^{(n-k)\times(q-p)}$ is the submatrix of G_2 that contains the rows $\mathcal{J}_k$ and columns $p+1, \ldots, q$. From Proposition 3.2, we have $\mathrm{rank}(G_{\mathcal{J}_k,p+1:q}(\mathfrak{g}^*, \mathbf{x}^*)) \leqslant k-1$ for which the property $\mathcal{A}(2)$ holds as from induction hypothesis. Moreover,

$$V(I_{G_2}) = \bigcup_{\mathcal{J}_k\subset\{1,\ldots,p\}^k,\ 1\leqslant k\leqslant\min(n,p)} V(I_{\mathcal{J}_k}),$$

where $I_{\mathcal{J}_k}$ is the ideal generated by $\mathfrak{g}_{i,i}$ for $i \in \mathcal{J}_k$ and all $(k-1)\times(k-1)$ minors of $G_{\mathcal{J}_k,p+1:q}$. Therefore, we can define a non-empty Zariski open set, $\overline{\mathcal{O}}_2$, for G_2 as follows. For any $\mathcal{J}_k \subset \{1, \ldots, p\}^k$, we rewrite $(X_1, \ldots, X_k) \in \mathbb{K}[\mathcal{G}, X_{k+1}, \ldots, X_n]^k$ and substitute into $G_{\mathcal{J}_k,p+1:q}$ to obtain $G_{\mathcal{J}_k,p+1:q} \in \mathbb{K}[\mathcal{G}, X_{k+1}, \ldots, X_n]^{k\times(q-p)}$. By using the induction hypothesis, for any $\mathcal{J}_k$, there exists a Zariski closed set $\Delta_{\mathcal{J}_k} \subsetneq \overline{\mathbb{K}}^{N_{\mathcal{J}_k}}$ such that $I^{(p)}_{G_{\mathcal{J}_k,p+1:q}}$ has $S_{n-k}(D_{i_1}, \ldots, D_{i_k})$ distinct solutions, where $N_{\mathcal{J}_k} = n(q-p+1)(\sum_{i\in\mathcal{J}_k} D_i)$ is the number of coefficients of the matrix $[\mathrm{diag}(\mathfrak{g}_{i_1,i_1}, \ldots, \mathfrak{g}_{i_k,i_k})|G_{\mathcal{J}_k,p+1:q}]$. We finally, define

$$\overline{\mathcal{O}}_2 = \overline{\mathbb{K}}^{N_2} \setminus \Delta, \text{ where } N_2 = n(q-p+1)(\sum_{i=1}^{p} D_i) \text{ and } \Delta = \bigcup_{\mathcal{J}_k\subset\{1,\ldots,p\}^k,\ 1\leqslant k\leqslant\min(n,p)} \Delta_{\mathcal{J}_k}.$$

This is a nonempty Zariski open set in $\overline{\mathbb{K}}^{N_2}$ such that I_{G_2} satisfies $\mathcal{A}(2)$ when $g_{i,j} \in \overline{\mathcal{O}}_2$. Indeed, by this construction, the number of solutions of I_{G_2} equals

$$\sum_{k=1}^{\min(n,p)} \sum_{\mathcal{J}_k \subset \{1,\ldots,p\}^k} D_{i_1} \ldots D_{i_k}.\#\{\text{solutions of } I_{G_{\mathcal{J}_k,p+1:q}}\}$$

which is

$$\sum_{k=1}^{\min(n,p)} \sum_{\mathcal{J}_k \subset \{1,\ldots,p\}^k} D_{i_1} \ldots D_{i_k} S_{n-k}(D_{i_1},\ldots,D_{i_k}) = S_n(D_1,\ldots,D_p).$$

Step 3 : Finally, let assume that $\mathcal{A}(2)$ holds for any $G_2 \in \mathbb{K}[\mathcal{G},\mathbf{X}]^{p\times q}$, we will prove $\mathcal{A}(2)$ is also true for any $G_1 \in \mathbb{K}[\mathcal{G},\mathbf{X}]^{p\times q}$ as follows. We finish this step by using the result in Section 4. Indeed, we can use the fact that I_{G_1} satisfis G; and consider the matrices G_1 and G_2 here as the matrices F and G in Section 4, respectively. In other words, if G_2 has $S_n(D_1,\ldots,D_p)$ solutions, then so is G_1. Therefore, we can use the Zariski open set $\overline{\mathcal{O}}_2$ in the second step as $\mathcal{O}_2$ for G_1. This set is indeed non-empty from the second step above.

A.3 Genericity of $\mathcal{A}(3)$

Step 1 : We show here that there exists a nonempty Zariski open set $\mathcal{O}_3$ such that I_{G_1} is a radical ideal for $\mathfrak{g}_{i,j} \in \mathcal{O}_3$, where G_1 is as square matrix as follows

$$G_1 = \begin{pmatrix} \mathfrak{g}_{1,1} & \cdots & \mathfrak{g}_{1,p} \\ \vdots & \ddots & \vdots \\ \mathfrak{g}_{p,1} & \cdots & \mathfrak{g}_{p,p} \end{pmatrix}.$$

Let us denote by $m \in \mathbb{K}[\mathcal{G},X_1]$ the determinant of G_1, then $I_{G_1} = \langle m \rangle$. Notice that in this case, the number of variable is $n = 1$. We would like to have the property that

$$\frac{\partial m}{\partial X_1}(\mathbf{x}^*) \neq 0 \text{ for any } \mathbf{x}^* \in V(m).$$

Let us define $\mathcal{O}_3$ as follows. Let $\Omega_3 = V(\partial m/\partial X_1) \subset \overline{\mathbb{K}}^N \times \mathbb{P}^1(\overline{\mathbb{K}})$ is Zariski closed, where here $N = 2p(\sum_{i=1}^p D_i)$ is the number of coefficients for G_1. Then, we define $\Delta_3 = \pi_{\mathcal{G}}(\Omega_3) \subset \overline{\mathbb{K}}^N$ is Zariski closed and take $\mathcal{O}_3$ as $\overline{\mathbb{K}}^N \setminus \Delta_3$ is a Zariski open set. Therefore, for any $\mathfrak{g}_{i,j} \in \mathcal{O}_3$, we have $(\partial m/\partial X_1)(\mathbf{x}^*) \neq 0$. We need to check that $\mathcal{O}_3$ is non-empty. For this, we use the diagonal matrix G_2 as $\mathrm{diag}(\mathfrak{g}_{1,1},\ldots,\mathfrak{g}_{p,p})$. So, the determinant of G_2 is $\prod_{i=1}^p \mathfrak{g}_{i,i}$, where $\mathfrak{g}_{i,i} = \prod_{l=1}^{D_i}(\gamma_{i,i}^{(1,l)} X_1 + \gamma_{i,i}^{(0,l)})$. Let us denote u for $\det(G_2)$, then

$$\frac{\partial u}{\partial X_1} = \sum_{i=1}^{p} \frac{\partial \mathfrak{g}_{i,i}}{\partial X_1} \prod_{j\neq i} \mathfrak{g}_{j,j}.$$

For convenience, let us denote $f(X)$ for $\partial u/\partial X_1$ and rewrite $\det(G_2) = \prod_{i=1}^d (a_i X + b_i)$ for a_i and b_i are indeterminates and $d = \sum_{i=1}^p D_i$. Therefore,

$$f(X) = \sum_{i=1}^{d} a_i \prod_{j=1, j\neq i}^{d} (a_j X + b_j).$$

Moreover, for any $\mathbf{x}^* \in V(\det(G_2))$ and $\mathbf{x}^*$ is the solution of $a_iX + b_i = 0$, we have $a_j\mathbf{x}^* + b_j \neq 0$ for all $i \neq k$. Therefore,

$$f(\mathbf{x}^*) = a_i \prod_{j=1, j\neq i}^{d} (a_j\mathbf{x}^* + b_j) \neq 0.$$

This means that for any $\mathbf{x}^* \in V(\det(G_2))$, we always have $f(\mathbf{x}^*) \neq 0$. Thus, $\overline{\mathbb{K}}^{N_2} \times 0^{N_1} \subset \mathcal{O}_3$ which implies that $\mathcal{O}_3$ is non-empty.

Step 2 : Let us now assume that $\mathcal{A}(3)$ holds for any $G_1 \in \mathbb{K}[\mathcal{G}, \mathbf{X}]^{p'\times q'}$ for any $n' \leqslant n$, where $n' = q' - p' + 1$; we prove $\mathcal{A}(3)$ is also true for $G_2 \in \mathbb{K}[\mathcal{G}, \mathbf{X}]^{p\times q}$ with $n = q - p + 1$. As we noticed before, the assumption that I_{G_1} is radical is equivalent to the property that $\mathrm{Jac}(I_G)(\mathbf{x}^*)$ has full rank for any $\mathbf{x}^* \in V(I_G)$. In other words, $\mathbf{x}^* \in V(I_G)$ is a simple root in I_G.

Let us now consider any $\mathbf{x}^* \in V(I_{G_2})$, there exist k polynomials $\mathfrak{g}_{i_1,i_1}, \ldots, \mathfrak{g}_{i_k,i_k}$ such that $\mathfrak{g}_{i_1,i_1}(\mathbf{x}^*) = \cdots = \mathfrak{g}_{i_k,i_k}(\mathbf{x}^*) = 0$, where $1 \leqslant k \leqslant \min(n, p)$ and $\mathrm{rank}(G_{\mathcal{J}_k;p+1:q}(\mathbf{x}^*)) \leqslant k - 1$. That is $\mathbf{x}^*$ is solution of the system of $k \times k$ minors of $G_{\mathcal{J}_k;p+1:q}$, where $\mathcal{J}_k = (i_1, \ldots, i_k)$. Therefore, by considering any system of k polynomials $\mathfrak{g}_{i_1,i_1}(\mathbf{X}) = \cdots = \mathfrak{g}_{i_k,i_k}(\mathbf{X}) = 0$, we can rewrite the variables $X_1, \ldots, X_k$ in the linear forms of $X_{k+1}, \ldots, X_n$; then by substituting $\{X_i\}_{i=1}^k$ into $G_{\mathcal{J}_k:p+1:q}$ we obtain a matrix $\overline{G} \in \mathbb{K}[\mathcal{G}, X_k, \ldots, X_n]^{k\times(q-p)}$. Furthermore, this $\overline{G}$ matrix has property that any solution of its $k \times k$ minors system is simple by using induction hypothesis. Therefore, we can define the Zariski open set, $\overline{\mathcal{O}}_3$, for G_2 as follows.

For any $\mathcal{J}_k \subset \{1, \ldots, p\}^k$, we rewrite $(X_1, \ldots, X_k)$ in the forms of $X_{k+1}, \ldots, X_n$ and substitute into $G_{\mathcal{J}_k,p+1:q}$ to obtain $G_{\mathcal{J}_k,p+1:q} \in \mathbb{K}[\mathcal{G}, X_{k+1}, \ldots, X_n]^{k\times(q-p)}$. By using the induction hypothesis, for any $\mathcal{J}_k$, there exists a Zariski closed set $\Delta_{\mathcal{J}_k} \subsetneq \overline{\mathbb{K}}^{N_{\mathcal{J}_k}}$ such that any common solution to the $k\times k$ minors of $G_{\mathcal{J}_k,p+1:q}$ is simple, where $N_{\mathcal{J}_k} = n(q - p + 1)(\sum_{i\in\mathcal{J}_k} D_i)$ is the number of coefficients of the matrix $[\mathrm{diag}(\mathfrak{g}_{i_1,i_1}, \ldots, \mathfrak{g}_{i_k,i_k})|G_{\mathcal{J}_k,p+1:q}]$. We finally, define

$$\overline{\mathcal{O}}_3 = \overline{\mathbb{K}}^{N_2} \setminus \Delta, \text{ where } N_2 = n(q - p + 1)(\sum_{i=1}^{p} D_i) \text{ and } \Delta = \bigcup_{\mathcal{J}_k\subset\{1,\ldots,p\}^k,\ 1\leqslant k\leqslant\min(n,p)} \Delta_{\mathcal{J}_k}.$$

This is a non-empty Zariski open set in $\overline{\mathbb{K}}^{N_2}$ such that I_{G_2} satisfies $\mathcal{A}(3)$ when $g_{i,j} \in \overline{\mathcal{O}}_3$. Indeed, by this construction, from the linear of $X_1, \ldots, X_k$ in $X_{k+1}, \ldots, X_n$ and any solution of $k \times k$ minors of $G_{\mathcal{J}_k,p+1:q}$ is simple, we can deduce that any solution of $p \times p$ minors of G_2 is simple. It means that we finished the second step.

Step 3 : Let us consider the matrix $G_1 \in \mathbb{K}[\mathcal{G}, \mathbf{X}]^{p\times q}$, and $I_{G_1} := \langle p \times p - \text{ minors of } G_1\rangle$. Let $m_1, \ldots, m_d$ be the generators for I_{G_1}, where $d = \binom{q}{p}$ is the number of $p \times p$ minors of G_1. We would like to have the property that $\mathrm{Jac}(I_{G_1})(\mathbf{x}^*)$ has full rank for any $\mathbf{x}^* \in V(I_{G_1})$. We recall here that

$$\mathrm{Jac}(I_{G_1}) = \left[\frac{\partial m_j}{\partial X_i}\right]_{1\leqslant j\leqslant d, 1\leqslant i\leqslant n} \in \mathbb{K}[\mathcal{G}, \mathbf{X}]^{d\times n}.$$

We first notice that for since $n \leqslant d$, so for any $\mathbf{x}^* \in \overline{\mathbb{K}}^n$, the matrix $\mathrm{Jac}(I_{G_1})(\mathbf{x}^*)$ has rank at most n. Therefore, $\mathrm{Jac}(I_{G_1})(\mathbf{x}^*)$ should have rank n if we want the property that $\mathrm{Jac}(I_{G_1})$ has full rank at any point $\mathbf{x}^*$. For this argument, we consider the ideal which is generated by $n \times n$ minors of $\mathrm{Jac}(I_{G_1})$, that is $\mathcal{I}_m = \langle n \times n - \text{ minors of } \mathrm{Jac}(I_{G_1})\rangle$.

Let us define $\Omega_3 = V(\mathcal{I}_m) \subset \overline{\mathbb{K}}^N \times \mathbb{P}^n(\overline{\mathbb{K}})$ is a Zariski closed set. Let $\pi_{\mathcal{G}}$ be the projection on $\mathcal{G}$ coordinates, then we define $\Delta_3 = \pi_{\mathcal{G}}(\Omega_3)$ is a Zariski closed set in $\overline{\mathbb{K}}^N$. Finally, let us denote $\mathcal{O}_3$ for $\overline{\mathbb{K}}^N \setminus \Delta_3$ which is a Zariski open set in $\overline{\mathbb{K}}^N$. By using this construction, when $\mathfrak{g}_{i,j} \in \mathcal{O}_3$, we can see that $\mathrm{Jac}(I_{G_1})(\mathbf{x}^*)$ has full rank n for any $\mathbf{x}^* \in V(I_{G_1}))$. The remaining problem is to prove

that $\mathcal{O}_3$ is indeed a non-empty set. In order to finish this step, we use the matrix $G_2 \in \mathbb{K}[\mathcal{G}, \mathbf{X}]^{p\times q}$ which is defined as above and using the similar argument as in the first step, we can deduce that $\mathcal{O}_3$ is non-empty.

B Proof of Proposition 4.3

We prove this result for the case of column degrees and row degrees separately.

Column degree case. Any $p \times p$ minor f_G of G has the form $f_G = \lambda \cdot g_{i_1} \dots g_{i_p}$ where $(i_1, \dots, i_p) \subset \{1, \dots, q\}^p$ and $\lambda \in \mathbb{K}^*$, then

$$f_G^{\mathrm{H}}(X_0, \mathbf{X}) = \lambda \cdot g_{i_1}^{\mathrm{H}}(X_0, \mathbf{X}) \dots g_{i_p}^{\mathrm{H}}(X_0, \mathbf{X}).$$

Moreover, each entry $g_{i,j}$ of the matrix G is a product of D_j linear forms as defined in Section 3.2. Then, any common solution $\mathbf{x}$ to the system $\mathbf{g}^H(0, \mathbf{X})$ is a solution of the system $B\mathbf{X} = 0$, where $B = [\beta_{i,j}]_{1\leqslant i\leqslant n, 1\leqslant j\leqslant n}$ with $(\beta_{i,1}, \dots, \beta_{i,n}) \in \{(\lambda_{i,1}^{(1)}, \lambda_{i,1}^{(2)}, \dots, \lambda_{i,1}^{(n)}), \dots, (\lambda_{i,D_1}^{(1)}, \lambda_{i,D_1}^{(2)}, \dots, \lambda_{i,D_1}^{(n)})\}$ and $\lambda_{i,j}^{(k)} = (i+j)^k$. In other words, the matrix $B \in \mathbb{K}^{n\times n}$ is full rank, which implies $\mathbf{x} = (0, \dots, 0)$.

Row degree case. Let us recall here that the start matrix G has the form

$$G = \begin{pmatrix} \prod_{t=1}^{D_1} L_1^{(t)} & 0 & \cdots & 0 & g_{1,p+1} & \cdots & g_{1,q} \\ 0 & \prod_{t=1}^{D_2} L_2^{(t)} & \cdots & 0 & g_{2,p+1} & \cdots & g_{2,q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \prod_{t=1}^{D_p} L_p^{(t)} & g_{p,p+1} & \cdots & g_{p,q} \end{pmatrix},$$

where $g_{i,j} = \prod_{t=1}^{D_i} L_{i,j}^{(t)}$ with $L_i^{(t)}$ and $L_{i,j}^{(t)}$ are linear forms with generic coefficients.

Let $\mathbf{x}$ be a solution of the system $g_1^H(0, \mathbf{X}) = \cdots = g_M^H(0, \mathbf{X})$. We would like to prove $\mathbf{x} = (0, \dots, 0)$. Let us assume there exists one coordinate of $\mathbf{x} = (x_1, \dots, x_n)$ is non-zero. Without loss of generality, let us assume that $x_n \neq 0$ and $L_1^H(0, \mathbf{x}) = \cdots = L_k^H(0, \mathbf{x}) = 0$, where L_i is a linear form of $\prod_{t=1}^{D_i} L_i^{(t)}$ and $k \leqslant \min(n, p)$. Let us denote A for the submatrix of G that contains first k rows and columns $p+1, \dots, q$ of G, that is, $A = G_{1:k;p+1:q}$. Let $\mathbf{a} = (a_1, \dots, a_m)$ be the system of all $k \times k$ minors of A, then $\mathbf{a}^H(0, \mathbf{x}) = 0$. From $L_1^H(0, \mathbf{X}) = \cdots = L_k^H(\mathbf{X}) = 0$, we can rewrite $\{X_i\}_{i=1}^k$ in the form $\sum_{j=k+1}^n \ell_{i,j}(\cdot) X_j$, where $\ell_{i,j}(\cdot)$ are functions in generic coefficients; and then substitute $\{X_i\}_{i=1}^k$ into A. The matrix A now is in dimension $k \times (q-p)$ of $n-k$ variables $X_{k+1}, \dots, X_n$. Since $g_{i,j}$ is a product of D_i linear form, then all of $a_i^H(0, \mathbf{X})$ is a homogeneous polynomial of the form

$$a_i^H(0, \mathbf{X}) = \sum_{(j_1,\dots,j_{n-k}):\sum_{i=1}^{n-k} j_i = \sum_{i=1}^k D_i} f_{(j_1,\dots,j_{n-k})}(\cdot) \cdot X_{k+1}^{j_1} \cdots X_n^{j_{n-k}}, \tag{6}$$

where $f_{(j_1,\dots,j_{n-k})}(\cdot)$ are functions in generic coefficients. In other words, $a_i^H(0, \mathbf{X})$ contains all monomials of degree $\sum_{i=1}^k D_i$ in variables $X_{k+1}, \dots, X_n$. This implies

$$a_i^H(0, \mathbf{x}) = f_{(0,\dots,0,D)}(\cdot) x_n^D \neq 0,$$

which is a contradiction.

C Proof of Proposition 6.1

Reference [**?**] gives an algorithm to compute the dimension of $V(\mathbf{f})$ at $\mathbf{x}$, but its complexity is unclear to us, as it relies on linear algebra with matrices of potentially large size. Instead, we use an adaptation of a prior result by Mourrain [**?**], which allows us to control the size of the matrices we handle. We only give detailed proofs for new ingredients that are specific to our context, a key difference being the cost analysis in the straight-line program model: Mourrain's original result depends on the number of monomials appearing when we expand $\mathbf{f}$, which would be too high for the applications we will make of this result.

We assume that $\mathbf{x} = 0$; this is done by replacing $\mathbf{f}$ by the polynomials $\mathbf{f}(\mathbf{X} + \mathbf{x})$, which have complexity of evaluation $\mathcal{E}' = \mathcal{E} + n$. The basis of our algorithm is the following remark.

Lemma C.1. *Let I be the zero-dimensional ideal $\langle \mathbf{f} \rangle + \mathfrak{m}^{\mu+1}$, where $\mathfrak{m} = \langle X_1, \ldots, X_n \rangle$ is the maximal ideal at the origin. Then, if 0 is isolated in $V(\mathbf{f})$ if and only if it has multiplicity at most μ with respect to I.*

Proof. This follows from the following result [**?**, Theorem A.1]. For $k \geqslant 1$, let I_k be the zero-dimensional ideal $\langle \mathbf{f} \rangle + \mathfrak{m}^k$, and let ν_k be multiplicity of the origin with respect to this ideal. Then, the reference above proves that the sequence $(\nu_k)_{k \geqslant 1}$ is non-decreasing, and that 0 is isolated in $V(\mathbf{f})$ if and only if there exists $k \geqslant 1$ such that $\nu_k = \nu_{k+1}$.

- If 0 is isolated in $V(\mathbf{f})$, then by assumption H its multiplicity with respect to $\langle \mathbf{f} \rangle$ is at most μ, and its multiplicity with respect to I cannot be larger.
- Otherwise, by the result above, $\nu_{k+1} > \nu_k$ holds for all $k \geqslant 1$, so that $\nu_k \geqslant k$ holds for all such k (since $\nu_1 = 1$). In particular, the multiplicity of the origin with respect to I, which is $\nu_{\mu+1}$, is at least $\mu + 1$. □

Hence, we are left with deciding whether the multiplicity of the $\mathfrak{m}$-primary ideal I is at most μ. We do this by following and slightly modifying Mourrain's algorithm for the computation of the orthogonal $I^\perp$, that is, the set of $\mathbb{K}$-linear forms $\mathbb{K}[\mathbf{X}] \to \mathbb{K}$ that vanish on I; this is a $\mathbb{K}$-vector space naturally identified with the dual of $\mathbb{K}[\mathbf{X}]/I$, so it has dimension $m = \mathrm{mult}(0, I)$.

We do not need to give all details of the algorithm, let alone proof of correctness; we just mention the key ingredients for the cost analysis in our setting. A linear form $\beta : \mathbb{K}[\mathbf{X}] \to \mathbb{K}$ that vanishes on I must vanish on all monomials, except a finite number (since all monomials, except a finite number, belong to I); a natural way to represent such a linear form would then be as the finite generating series $\sum_{\alpha \in \mathbb{N}^n} \beta(X_1^{\alpha_1} \cdots X_n^{\alpha_n}) d_1^{\alpha_1} \cdots d_n^{\alpha_n}$, for some new variables $d_1, \ldots, d_n$; however the number of non-zero coefficients in such a sum cannot be bounded polynomially in n, μ.

Hence, the algorithm uses another way to represent the elements in $I^\perp$, by means of *multiplication matrices*. An important feature of $I^\perp$ is that it admits the structure of a $\mathbb{K}[\mathbf{X}]$-module: for k in $\{1, \ldots, n\}$ and β in $I^\perp$, the $\mathbb{K}$-linear form $X_k \cdot \beta : f \mapsto \beta(X_k f)$ is easily seen to still be in $I^\perp$. In particular, if $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_m)$ is a $\mathbb{K}$-basis of $I^\perp$, then for all k as above, and all i in $\{1, \ldots, m\}$, $Y_k \cdot \beta_i$ is a linear combination of $\beta_1, \ldots, \beta_m$. Mourrain's algorithm computes a basis $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_m)$ with the following features:

- for i in $\{1, \ldots, m\}$ and k in $\{1, \ldots, n\}$, we have $X_k \cdot \beta_i = \sum_{0 \leqslant j < i} \lambda_{i,j}^{(k)} \beta_j$ (hence $\lambda_{i,j}^{(k)}$ may be non-zero only for $j < i$)
- β_1 is the evaluation at 0, $f \mapsto f(0)$

- for i in $\{2,\dots,m\}$, $\beta_i(1)=0$.

The following lemma shows that the coefficients $(\lambda_{i,j}^{(k)})$ are sufficient to evaluate the linear forms β_i at f in $\mathbb{K}[\mathbf{X}]$. More precisely, knowing only their values for $j<i\leqslant s$, for any $s\leqslant m$, allows us to evaluate $\beta_1,\dots,\beta_s$ at such an f. The following lemma follows [**?**] in its description of the matrices $\mathbf{M}_{k,s}$; the (rather straightforward) complexity analysis in the straight-line program model is new.

Lemma C.2. *Let s be in $1,\dots,m$, and suppose that the coefficients $\lambda_{i,j}^{(k)}$ are known for $i=1,\dots,s$, $j=0,\dots,i-1$ and $k=1,\dots,n$. Given a straight-line program Γ of length L that computes $\mathbf{h}=(h_1,\dots,h_R)$, one can compute $\beta_i(h_r)$, for all $i=1,\dots,s$ and $r=1\dots,R$, using $(s\,L)^{O(1)}$ operations.*

Proof. By definition, for h in $\mathbb{K}[\mathbf{X}]$ and $k=1,\dots,n$, the following equality holds:

$$\begin{bmatrix}\beta_1(X_kh)\\ \vdots\\ \beta_s(X_kh)\end{bmatrix}=\mathbf{M}_{k,s}\begin{bmatrix}\beta_1(h)\\ \vdots\\ \beta_s(h)\end{bmatrix},\quad\text{with}\quad \mathbf{M}_{k,s}=\begin{bmatrix}\lambda_{1,1}^{(k)} & \cdots & \lambda_{s,1}^{(k)}\\ \vdots & & \vdots\\ \lambda_{1,s}^{(k)} & \cdots & \lambda_{s,s}^{(k)}\end{bmatrix}.$$

Remark that the matrices $\mathbf{M}_{k,s}$ all commute. Indeed, for any k,k' in $\{1,\dots,n\}$, and h as above, the relation above implies that

$$\Delta_{k,k',s}\begin{bmatrix}\beta_1(h)\\ \vdots\\ \beta_s(h)\end{bmatrix}=\begin{bmatrix}0\\ \vdots\\ 0\end{bmatrix},$$

where $\Delta_{k,k',s}=\mathbf{M}_{k,s}\mathbf{M}_{k',s}-\mathbf{M}_{k',s}\mathbf{M}_{k,s}$. Because the linear forms $\beta_1,\dots,\beta_s$ are linearly independent, this implies that all rows of $\Delta_{k,k',s}$ must be zero, as claimed. We then deduce that for any polynomial h in $\mathbb{K}[\mathbf{X}]$, we have the equality

$$\begin{bmatrix}\beta_1(h)\\ \vdots\\ \beta_s(h)\end{bmatrix}=h(\mathbf{M}_{1,s},\dots,\mathbf{M}_{N,s})\begin{bmatrix}\beta_1(1)\\ \vdots\\ \beta_s(1)\end{bmatrix}$$

On the other hand, our assumptions imply that the sequence $(\beta_1(1),\dots,\beta_s(1))$ is simply $(1,0,\dots,0)$. To prove the claim, note that the evaluations $h_1(\mathbf{M}_{1,s},\dots,\mathbf{M}_{n,s}),\dots,h_R(\mathbf{M}_{1,s},\dots,\mathbf{M}_{n,s})$ can be computed using the straight-line program Γ in $(s\,L)^{O(1)}$ operations. □

Mourrain's alorithm proceeds in an iterative manner, starting from $\boldsymbol{\beta}^{(1)}=(\beta_1)$ (and setting $e_1=1$), and computing successively $\boldsymbol{\beta}^{(2)}=(\beta_{e_1+1},\dots,\beta_{e_2})$, $\boldsymbol{\beta}^{(3)}=(\beta_{e_2+1},\dots,\beta_{e_3})$, …for some integers $e_1\leqslant e_2\leqslant e_3\dots$. Mourrain's algorithm stops when $e_{\ell+1}=e_\ell$, in which case $\beta_1,\dots,\beta_{e_\ell}$ is a $\mathbb{K}$-basis of $I^\perp$, and $e_\ell=\mathrm{mult}(0,I)$. In our case, we are not interested in computing this multiplicity, but only in deciding whether it is less than or equal to the parameter μ. We do it as follows: assume that we have computed $\boldsymbol{\beta}^{(1)},\boldsymbol{\beta}^{(2)},\dots,\boldsymbol{\beta}^{(\ell)}$, together with the corresponding integers $e_1,e_2,\dots,e_\ell$, with $e_1<\dots<e_\ell\leqslant\mu$. We compute $\boldsymbol{\beta}^{(\ell+1)}$ and $e_{\ell+1}$, and continue according to the following:

- if $e_{\ell+1}=e_\ell$, we conclude that the multiplicity $\mathrm{mult}(0,I)$ is $e_\ell\leqslant\mu$; we stop the algorithm;
- if $e_{\ell+1}>\mu$, we conclude that the multiplicity is greater than μ; we stop the algorithm;
- else, when $e_\ell<e_{\ell+1}\leqslant\mu$, we do another loop.

Because the e_ℓ's are an increasing sequence of integers, they satisfy $e_\ell \geqslant \ell$; hence, every time we enter the loop above we have $\ell \leqslant \mu$. To finish the analysis of the algorithm, it remains to explain how to compute $\boldsymbol{\beta}^{(\ell+1)}$ from $(\boldsymbol{\beta}^{(1)}, \boldsymbol{\beta}^{(2)}, \ldots, \boldsymbol{\beta}^{(\ell)}) = (\beta_1, \ldots, \beta_{e_\ell})$.

As per our description above, at any step of the algorithm, $\beta_1, \ldots, \beta_{e_\ell}$ are represented by means of the coefficients $\lambda_{i,j}^{(k)}$, for $0 \leqslant j < i \leqslant e_\ell$ and $1 \leqslant k \leqslant n$. At step ℓ, Mourrain's algorithm solves a homogeneous linear system S_ℓ with $n(n-1)e_\ell/2 + M'$ equations and $n.e_\ell$ unknowns, where M' is the number of generators of the ideal $I = \langle \mathbf{f} \rangle + \mathfrak{m}^{\mu+1}$. Remark that M' is not polynomial in μ and n, so the size of S_ℓ is *a priori* too large to fit our cost bound; we will explain below how to resolve this issue.

The nullspace dimension of this linear system gives us the cardinality $e_{\ell+1} - e_\ell$ of $\boldsymbol{\beta}^{(\ell+1)}$. Similarly, the coordinates of the $e_{\ell+1} - e_\ell$ vectors in a nullspace basis are precisely the coefficients $\lambda_{i,j}^{(k)}$ for $i = e_\ell+1, \ldots, e_{\ell+1}$, $j = 1, \ldots, e_\ell$ and $k = 1, \ldots, n$ (we have $\lambda_{i,j}^{(k)} = 0$ for $j = e_\ell+1, \ldots, i-1$). For all $\ell \geqslant 2$, all linear forms β in $\boldsymbol{\beta}^{(\ell)}$ are such that for all k in $\{1, \ldots, n\}$, $X_k \cdot \beta$ belongs to the span of $\boldsymbol{\beta}^{(1)}, \ldots, \boldsymbol{\beta}^{(\ell-1)}$; in particular, a quick induction shows that all linear forms in $\boldsymbol{\beta}^{(1)}, \ldots, \boldsymbol{\beta}^{(\ell)}$ vanish on all monomials of degree at least ℓ.

There remains the question of setting up the system S_ℓ. For k in $\{1, \ldots, n\}$ and a $\mathbb{K}$-linear form β, we denote by $X_k^{-1} \cdot \beta$ the $\mathbb{K}$-linear form defined as follows:

- $(X_k^{-1} \cdot \beta)(X_k f) = \beta(f)$ for all f in $\mathbb{K}[\mathbf{X}]$,
- $(X_k^{-1} \cdot \beta)(f) = 0$ if $f \in \mathbb{K}[\mathbf{X}]$ does not depend on X_k.

In other words, $(X_k^{-1} \cdot \beta)(f) = \beta(\delta_k(f))$ holds for all f, where $\delta_k : \mathbb{K}[\mathbf{X}] \to \mathbb{K}[\mathbf{X}]$ is the kth divided difference operator

$$f \mapsto \frac{f(X_1, \ldots, X_n) - f(X_1, \ldots, X_{k-1}, 0, X_{k+1}, \ldots, X_n)}{X_k}.$$

One verifies that, as the notation suggests, $X_k \cdot (X_k^{-1} \cdot \beta)$ is equal to β. This being said, we can then describe what the entries of S_ℓ are:

- the first $n(n-1)e_\ell/2$ equations involve only the coefficients $\lambda_{i,j}^{(k)}$ previously computed (we refer to [**?**, Section 4.4] for details of how exactly these entries are distributed in S_ℓ, as we do not need such details here).
- each of the other M' equations has coefficient vector

  $$c_f = \big((X_k^{-1} \cdot \beta_1)(f(X_1, \ldots, X_k, 0, \ldots, 0)), \ldots, (X_k^{-1} \cdot \beta_{e_\ell})(f(X_1, \ldots, X_k, 0, \ldots, 0)) \big)_{1 \leqslant k \leqslant n},$$

  where f is a generator of $I = \langle \mathbf{f} \rangle + \mathfrak{m}^{\mu+1}$.

We claim that only those equations corresponding to generators $f_1, \ldots, f_M$ of the input system $\mathbf{f}$ are useful, as all others are identically zero

We pointed out above that any linear form β_i in $\beta_1, \ldots, \beta_{e_\ell}$ vanishes on all monomials of degree at least ℓ. Since we saw that we must have $\ell \leqslant \mu$, all β_i as above vanish on monomials of degree μ; this implies that $X_k^{-1} \cdot \beta_i$ vanishes on all monomials of degree $\mu+1$. The generators f of $\mathfrak{m}^{\mu+1}$ have degree $\mu+1$, and for any such f, $f(X_1, \ldots, X_k, 0, \ldots, 0)$ is either zero, or of degree $\mu+1$ as well. Hence, for any k, β_i in $\beta_1, \ldots, \beta_{e_\ell}$ and f as above, $(X_k^{-1} \cdot \beta_i)(f(X_1, \ldots, X_k, 0, \ldots, 0))$ vanishes. This implies that the vector c_f is identically zero for such an f, and that the corresponding equation can be discarded.

Altogether, as claimed above, we see that we have to compute the values

$$(X_k^{-1} \cdot \beta_i)(f_j(X_1, \dots, X_k, 0, \dots, 0)),$$

for $k = 1, \dots, n$, $i = 1, \dots, e_\ell$ and $j = 1, \dots, M$. Fixing k, we let $\mathbf{f}_k = (f_{j,k})_{1 \leqslant j \leqslant M}$, where $f_{j,k}$ is the polynomial $f_j(X_1, \dots, X_k, 0, \dots, 0)$; note that the system $\mathbf{f}_k$ can be computed by a straight-line program of length $\mathcal{E}' = \mathcal{E} + n$. Then, applying the following lemma with $s = e_\ell \leqslant \mu$ and $\mathbf{h} = \mathbf{f}_k$, we deduce that the values $(X_k^{-1} \cdot \beta_i)(f_j(X_1, \dots, X_k, 0, \dots, 0))$, for k fixed, can be computed in time $(\mu\, \mathcal{E}\, n)^{\mathcal{O}(1)}$.

Lemma C.3. *Let s be in $1, \dots, m$, and suppose that the coefficients $\lambda_{i,j}^{(k)}$ are known for $i = 1, \dots, s$, $j = 0, \dots, i-1$ and $k = 1, \dots, n$. Given a straight-line program Γ of length L that computes $\mathbf{h} = (h_1, \dots, h_R)$ and given k in $\{1, \dots, n\}$, one can compute $(X_k^{-1} \cdot \beta_i)(h_r)$, for all $i = 1, \dots, s$ and $r = 1, \dots, R$, using $(s\, L\, N)^{O(1)}$ operations in $\mathbb{K}$.*

Proof. In view of the formula $(X_k^{-1} \cdot \beta)(f) = \beta(\delta_k(f))$, and of Lemma C.2, it is enough to prove the existence of a straight-line program of length $\mathcal{O}(L)$ that computes $(\delta_k(h_1), \dots, \delta_k(h_R))$.

To do this, we replace all polynomials $\gamma_{-n+1}, \dots, \gamma_L$ computed by Γ by terms $\lambda_{-n+1}, \dots, \lambda_L$ and $\mu_{-n+1}, \dots, \mu_L$, with $\lambda_\ell = \gamma_\ell(X_1, \dots, X_{k-1}, 0, X_{k+1}, \dots, X_N)$ and μ_ℓ in $\mathbb{K}[\mathbf{X}]$ such that $\gamma_\ell = \lambda_\ell + X_k \mu_\ell$ holds for all ℓ, so that in particular $\mu_\ell = \delta_k(\gamma_\ell)$. To compute λ_ℓ and μ_ℓ, assuming all previous $\lambda_{\ell'}$ and $\mu_{\ell'}$ are known, we proceed as follows:

- if $\gamma_\ell = X_k$, we set $\lambda_\ell = 0$ and $\mu_\ell = 1$;
- if $\gamma_\ell = X_{k'}$, with $k' \neq k$, we set $\lambda_\ell = X_{k'}$ and $\mu_\ell = 0$;
- if $\gamma_\ell = c_\ell$, with $c_\ell \in \mathbb{K}$, then we set $\lambda_\ell = c_\ell$ and $\mu_\ell = 0$;
- if $\gamma_\ell = \gamma_{a_\ell} \pm \gamma_{b_\ell}$, for some indices $a_\ell, b_\ell < \ell$, then we set $\lambda_\ell = \lambda_{a_\ell} \pm \lambda_{b_\ell}$ and $\mu_\ell = \mu_{a_\ell} \pm \mu_{b_\ell}$;
- if $\gamma_\ell = \gamma_{a_\ell} \gamma_{b_\ell}$, for some indices $a_\ell, b_\ell < \ell$, then we set $\lambda_\ell = \lambda_{a_\ell} \lambda_{b_\ell}$ and

$$\mu_\ell = \lambda_{a_\ell} \mu_{b_\ell} + \mu_{a_\ell} \lambda_{b_\ell} + X_k \mu_{a_\ell} \mu_{b_\ell}.$$

One verifies that in all cases, the relation $\gamma_\ell = \lambda_\ell + X_k \mu_\ell$ still holds. Since the previous construction allows us to compute λ_ℓ and μ_ℓ in $\mathcal{O}(1)$ operations from the knowledge of all previous $\lambda_{\ell'}$ and $\mu_{\ell'}$, we deduce that all λ_ℓ and μ_ℓ, for $\ell = -n+1, \dots, L$, can be computed by a straight-line program of length $\mathcal{O}(L + n)$. □

Taking all values of k into account, we see that we can compute all entries we need to set up the linear system S_ℓ using $(\mu\, \mathcal{E}\, n)^{\mathcal{O}(1)}$ operations in $\mathbb{K}$. After discarding the useless equations described above, the number of equations and unknowns in the system S_ℓ is polynomial in n, M and e_ℓ; since we saw that $n \leqslant M$ and $e_\ell \leqslant \mu$, this implies that we can find a nullspace basis of it in time $(\mu\, M)^{\mathcal{O}(1)}$.

Altogether, the time spend to find $\boldsymbol{\beta}^{(\ell+1)}$ from $(\boldsymbol{\beta}^{(1)}, \boldsymbol{\beta}^{(2)}, \dots, \boldsymbol{\beta}^{(\ell)}) = (\beta_1, \dots, \beta_{e_\ell})$ is polynomial in $\mu\, \mathcal{E}\, M$. Since we saw that we do at most μ such loops, the cumulated time remains polynomial in $\mu\, \mathcal{E}\, M$, and Proposition 6.1 is proved.

D Proof of Proposition 4.1

In this section, we work over a field $\mathbb{K}$ of characteristic zero. Let $J = Q_1 \cap \cdots \cap Q_r$ be an irredundant primary decomposition of J in $\overline{\mathbb{K}}[T, \mathbf{X}]$ and $P_1, \ldots, P_r$ are the associated primes. For some $s \leqslant r$, let $P_1, \ldots, P_s$ be the minimal primes so that $V(P_1), \ldots, V(P_s)$ are the irreducible components of $V(J)$ in $\overline{\mathbb{K}}^{n+1}$. As from H_1, these irreducible components all have dimension at least one. Let $t \leqslant s$ be such that $V(P_1), \ldots, V(P_t)$ are the irreducible components of $V(J)$ of dimension one whose image by $\pi_T : (\tau, x_1, \ldots, x_n) \mapsto \tau$ is dense in $\mathbb{K}$.

Lemma D.1. *Let τ be in $\overline{\mathbb{K}}$ and let $\mathbf{x} \in \overline{\mathbb{K}}^n$ be an isolated solution of the system $\mathbf{h}_\tau$. Then, $(\tau, \mathbf{x})$ belongs to $V(P_i)$ for at least one index i in $\{1, \ldots, t\}$, and does not belong to $V(P_i)$ for any index i in $\{t+1, \ldots, r\}$.*

Proof. Because $(\tau, \mathbf{x})$ cancels $\mathbf{h}$, it belongs at least to one of $V(P_1), \ldots, V(P_r)$. It remains to rule out the possibility that $(\tau, \mathbf{x})$ belongs to $V(P_i)$ for some index i in $\{t+1, \ldots, r\}$.

We first deal with indices i in $\{t+1, \ldots, s\}$. These are those primary components with minimal associated primes P_i that either have dimension at least two, or have dimension one but whose image by π is a single point. In both cases, all irreducible components of the intersection $V(P_i) \cap V(T - \tau)$ have dimension at least one. Since $\mathbf{x}$ is isolated in $V(\mathbf{h}_\tau)$, $(\tau, \mathbf{x})$ is isolated in $V(\mathbf{h}) \cap V(T - \tau)$, so it cannot belong to $V(P_i) \cap V(T - \tau)$ for any i in $\{t+1, \ldots, s\}$.

We conclude by proving that $(\tau, \mathbf{x})$ does not belong to $V(P_i)$, for any of the embedded primes $P_{s+1}, \ldots, P_r$. We proceed by contradiction, assuming for definiteness that $(\tau, \mathbf{x})$ belongs to $V(P_{s+1})$. Because P_{s+1} is an embedded prime, $V(P_{s+1})$ is contained in (at least) one of $V(P_1), \ldots, V(P_s)$. In view of the previous paragraph, it cannot be one of $V(P_{t+1}), \ldots, V(P_s)$. Now, all of $V(P_1), \ldots, V(P_t)$ have dimension one, so $V(P_{s+1})$ has dimension zero (so it is the point $\{(\tau, \mathbf{x})\}$). For the same reason, if $(\tau, \mathbf{x})$ belonged to another $V(P_i)$, for some $i > s+1$, $V(P_i)$ would also be zero-dimensional, and thus equal to $\{(\tau, \mathbf{x})\}$; as a result, $V(P_i)$ would be equal to $V(P_{s+1})$, and this would contradict the irredundancy of our decomposition.

To summarize, $(\tau, \mathbf{x})$ belongs to $V(P_{s+1})$, together with $V(P_i)$ for some indices P_i in $\{1, \ldots, t\}$ (say $P_1, \ldots, P_u$, up to reordering, for some $u \geqslant 1$), and avoids all other associated primes. Let us localize the decomposition $J = Q_1 \cap \cdots \cap Q_r$ at P_{s+1}. By [?, Proposition 4.9], $J_{P_{s+1}} = {Q_1}_{P_{s+1}} \cap \cdots \cap {Q_u}_{P_{s+1}} \cap {Q_{s+1}}_{P_{s+1}}$ is an irredundant primary decomposition of $J_{P_{s+1}}$ in $\overline{\mathbb{K}}, \mathbf{X}]_{P_{s+1}}$; the minimal primes are ${P_1}_{P_{s+1}}, \ldots, {P_u}_{P_{s+1}}$.

By Corollary 4 p.24 in [?], for any prime ${P_i}_{P_{s+1}}$, $i = 1, \ldots, u$ or $i = s+1$, the localization of $\overline{\mathbb{K}}[T, \mathbf{X}]_{P_{s+1}}$ at ${P_i}_{P_{s+1}}$ is equal to $\overline{\mathbb{K}}[T, \mathbf{X}]_{P_i}$. In particular, the height of ${P_i}_{P_{s+1}}$ in $\overline{\mathbb{K}}[T, \mathbf{X}]_{P_{s+1}}$ is equal to that of P_i in $\overline{\mathbb{K}}[T, \mathbf{X}]_{P_i}$, that is, n if $i = 1, \ldots, u$, since then $V(P_i)$ has dimension 1, or $n+1$ if $i = s+1$. Since $u \geqslant 1$, this proves that $J_{P_{s+1}}$ has height n. As a result, H_2 implies that $J_{P_{s+1}}$ is unmixed, a contradiction. □

Let us write $J = J' \cap J''$, with $J' = Q_1 \cap \cdots \cap Q_t$ and $J'' = Q_{t+1} \cap \cdots \cap Q_r$. For τ in $\overline{\mathbb{K}}$, we denote by $J_\tau \subset \overline{\mathbb{K}}[T, \mathbf{X}]$ the ideal $J + \langle T - \tau \rangle$, and similarly for J'_τ and J''_τ.

Lemma D.2. *Let τ and $\mathbf{x}$ be as in Lemma D.1. Then, the multiplicities of the ideals J_τ and J'_τ at $(\tau, \mathbf{x})$ are the same.*

Proof. Without loss of generality, assume that $\tau = 0 \in \overline{\mathbb{K}}$ and $\mathbf{x} = 0 \in \overline{\mathbb{K}}^N$. We start from the equality $J = J' \cap J''$, which holds in $\overline{\mathbb{K}}[T, \mathbf{X}]$, and we see it in $\overline{\mathbb{K}}[T, \mathbf{X}]$. The previous lemma implies that there exists a polynomial in J'' that does not vanish at $(\tau, \mathbf{x}) = 0 \in \overline{\mathbb{K}}^{n+1}$. This polynomial is a unit in $\overline{\mathbb{K}}[T, \mathbf{X}]$, which implies that the extension of J'' in $\overline{\mathbb{K}}[T, \mathbf{X}]$ is the trivial ideal $\langle 1 \rangle$, and

finally that the equality of extended ideals $J = J'$ holds in $\overline{\mathbb{K}}[T, \mathbf{X}]$. This implies the equality $J + \langle T \rangle = J' + \langle T \rangle$ in $\overline{\mathbb{K}}[T, \mathbf{X}]$, and the conclusion follows. □

Our goal is now to give a bound on the sum of the multiplicities of $\mathbf{h}_\tau$ at all its isolated roots, for any τ in $\overline{\mathbb{K}}$. To achieve this, we introduce $\mathfrak{J}$, the extension of J in $\overline{\mathbb{K}}(T)[\mathbf{X}]$, and similarly $\mathfrak{J}'$ and $\mathfrak{J}''$.

Lemma D.3. *The ideal $\mathfrak{J}'$ has dimension zero and $V(\mathfrak{J}') \subset \overline{\mathbb{K}(T)}^n$ is the set of isolated solutions of $V(\mathfrak{J}) \subset \overline{\mathbb{K}(T)}^n$.*

Proof. From the equality $J = J' \cap J''$ and Corollary 3.4 in [?], we deduce that $\mathfrak{J} = \mathfrak{J}' \cap \mathfrak{J}''$; the properties of J' (the irreducible components of $V(J')$ are precisely those irreducible components of $V(J)$ that have dimension one and with a dense image by π_T) imply our claim. □

Let us write $c = \dim_{\overline{\mathbb{K}}(T)}(\overline{\mathbb{K}}(T)[\mathbf{X}]/\mathfrak{J}')$. The following lemma relates this quantity to the multiplicities of the solutions in any fiber $\mathbf{h}_\tau$. This proves the first statement in Proposition 4.1.

Lemma D.4. *Let τ be in $\overline{\mathbb{K}}$. The sum of the multiplicities of the isolated solutions of $\mathbf{h}_\tau$ is at most equal to c.*

Proof. The sum in the lemma is also the sum of the multiplicities of the ideal J_τ at all $(\tau, \mathbf{x})$, for $\mathbf{x}$ an isolated solution of $\mathbf{h}_\tau$. By Lemma D.2, this is also the sum of the multiplicities of J'_τ at all $(\tau, \mathbf{x})$, for $\mathbf{x}$ an isolated solution of $\mathbf{h}_\tau$. We prove below that the sum of the multiplicities of J'_τ at all $(\tau, \mathbf{x})$, for $\mathbf{x}$ such that $(\tau, \mathbf{x})$ cancels J'_τ, is at most c; this will be enough to conclude (for any isolated solution $\mathbf{x}$ of $\mathbf{h}_\tau$, $(\tau, \mathbf{x})$ is a root of J'_τ, though the converse may not be true).

Let $m_1, \ldots, m_\mu$ be monomials that form a $\overline{\mathbb{K}}$-basis of $\overline{\mathbb{K}}[T, \mathbf{X}]/J'_\tau$; since $T - \tau$ is in J'_τ, these monomials can be assumed not to involve T. We will prove that they are still $\overline{\mathbb{K}}(T)$-linearly independent in $\overline{\mathbb{K}}(T)[\mathbf{X}]/\mathfrak{J}'$; this will imply that $\mu \leqslant c$, and finish the proof of the first statement.

Suppose that there exists a linear combination $A_1 m_1 + \cdots + A_\mu m_\mu$ in $\mathfrak{J}'$, with all A_i's in $\overline{\mathbb{K}}(T)$, not all of them zero. Thus, we have an equality $a_1/d_1\, m_1 + \cdots + a_\mu/d_\mu\, m_\mu = a/d$, with $a_1, \ldots, a_\mu$ and $d, d_1, \ldots, d_\mu$ in $\overline{\mathbb{K}}[T]$ and a in the ideal J'. Clearing denominators, we obtain a relation of the form $b_1 m_1 + \cdots + b_\mu m_\mu \in J'$, with not all b_i's zero. Let $(T - \tau)^e$ be the highest power of $T - \tau$ that divides all b_i's (this is well-defined, since not all b_i's vanish) so that we can rewrite the above as $(T - \tau)^e (c_1 m_1 + \cdots + c_\mu m_\mu) \in J'$, with $c_i = b_i/(T - \tau)^e \in \overline{\mathbb{K}}[T]$ for all i. In particular, our definition of e implies that the values $c_i(\tau)$ are not all zero.

Recall that the ideal J' has the form $J' = Q_1 \cap \cdots \cap Q_t$. For $i = 1, \ldots, t$, since Q_i is primary, the membership equality $(T - \tau)^e (c_1 m_1 + \cdots + c_\mu m_\mu) \in J'$ implies that either $c_1 m_1 + \cdots + c_\mu m_\mu$ or some power $(T - \tau)^{ef}$, for some $f > 0$, is in Q_i. Since Q_i does not contain non-zero polynomials in $\overline{\mathbb{K}}[T]$, $c_1 m_1 + \cdots + c_\mu m_\mu$ belongs to all Q_i's, that is, to J'. We can then evaluate this relation at $T = \tau$. We saw that the values $c_i(\tau)$ do not all vanish on the left, which is a contradiction with the independence of the monomials $m_1, \ldots, m_\mu$ modulo J'_τ. □

To conclude the proof of Proposition 4.1, we consider $\tau \in \overline{\mathbb{K}}$ such that $\mathsf{G}(\tau)$ holds. Without loss of generality, we assume that $\tau = 0$.

The field of Puiseux series $\overline{\mathbb{K}}\langle\langle T \rangle\rangle$ contains an algebraic closure of $\overline{\mathbb{K}}(T)$; we thus let $\Phi_1, \ldots, \Phi_{c'}$ be the points of $V(\mathfrak{J}')$, with coordinates taken in $\overline{\mathbb{K}}\langle\langle T \rangle\rangle$. In particular, we see that $c' \leqslant c$; we prove below that we actually have $c' = c$.

For a vector $\Phi = (\varphi_1, \ldots, \varphi_s)$ with entries in $\overline{\mathbb{K}}\langle\langle T \rangle\rangle$, the valuation $\nu(\Phi)$ is the minimum of the valuations of its exponents. We say that Φ is *bounded* if it has non-negative valuation; in this case, $\lim_0(\Phi)$ is defined as the vector $(\lim_0(\varphi_1), \ldots, \lim_0(\varphi_s))$, with $\lim_0(\varphi_i) = \mathrm{coeff}(\varphi_i, T^0)$ for all

i. Without loss of generality, we assume that $\Phi_1, \ldots, \Phi_\kappa$ are bounded, and $\Phi_{\kappa+1}, \ldots, \Phi_{c'}$ are not, for some κ in $\{0, \ldots, c'\}$, and we define $\varphi_1, \ldots, \varphi_\kappa$ by $\varphi_i = \lim_0(\Phi_i) \in \overline{\mathbb{K}}^n$ for $i = 1, \ldots, \kappa$.

Lemma D.5. *The equality* $V(J + \langle T \rangle) = \{\varphi_i \mid i = 1, \ldots, \kappa\}$ *holds.*

Proof. Let $B_1, \ldots, B_R$ be generators of the ideal J in $\mathbb{K}[T, \mathbf{X}]$, so that these polynomials also generate $\mathfrak{J}$ in $\mathbb{K}(T)[\mathbf{X}]$; then, the polynomials $b_i = B_i(0, \mathbf{X}) \in \mathbb{K}[\mathbf{X}]$, for $i = 1, \ldots, R$, are such that $J + \langle T \rangle = \langle T, h_1, \ldots, h_R \rangle$. Consider $i \leqslant \kappa$, and the corresponding vector of Puiseux series Φ_i. We know that for $j = 1, \ldots, R$, we have $B_j(\Phi_i) = 0$. Since all elements involved have non-negative valuation, we can take the coefficient of degree 0 in T in this equality and deduce $b_j(\varphi_i) = 0$, as claimed. Hence, each φ_i, for $i \leqslant \kappa$, is in $V(J + \langle T \rangle)$.

Conversely, take indeterminates $T_1, \ldots, T_n$, and let $\mathbb{L}$ be the algebraic closure of the field $\overline{\mathbb{K}}(T_1, \ldots, T_n)$; let $W \subset \mathbb{L}^{n+1}$ be the zero-set of the ideal $J \cdot \mathbb{L}[T, \mathbf{X}]$ and consider the projection $W \to \mathbb{L}^2$ defined by $(\tau, x_1, \ldots, x_n) \mapsto (\tau, T_1 x_1 + \cdots + T_n x_n)$. The Zariski closure S of the image of this mapping is a hypersurface. Since the ideal J is generated by polynomials with coefficients in $\mathbb{K}$, one deduces that S admits a squarefree defining equation in $\mathbb{K}(T_1, \ldots, T_n)[T, T_0]$.

Consider such a polynomial, say C, and assume without loss of generality that C belongs to $\mathbb{K}[T_1, \ldots, T_n][T, T_0]$. Because J admits no irreducible component lying above $T = \tau$, for any τ in $\overline{\mathbb{K}}$, C admits no factor in $\mathbb{K}[T]$; thus, $C(0, T_0)$ is non-zero.

Let $\ell \in \mathbb{K}[T_1, \ldots, T_n, T]$ be the leading coefficient of C with respect to T_0. Proposition 1 in [**?**] proves that C/ℓ, seen in $\mathbb{K}(T_1, \ldots, T_n, T)[T_0] \subset \mathbb{L}(T)[T_0]$, is the minimal polynomial of $T_1 X_1 + \cdots + T_n X_n$ in $\mathbb{L}(T)[\mathbf{X}]/J \cdot \mathbb{L}(T)[\mathbf{X}]$. The latter ideal is also the extension of $\mathfrak{J}$ to $\mathbb{L}(T)[\mathbf{X}]$, so C/ℓ factors as

$$\frac{C}{\ell} = \prod_{1 \leqslant i \leqslant c'} (T_0 - T_1 \Phi_{i,1} - \cdots - T_n \Phi_{i,n})$$

in $\mathbb{L}\langle\langle T \rangle\rangle[T_0]$. This gives the equality

$$C = \ell \prod_{1 \leqslant i \leqslant c'} (T_0 - T_1 \Phi_{i,1} - \cdots - T_n \Phi_{i,n})$$

over $\overline{\mathbb{K}}\langle\langle T \rangle\rangle[T_1, \ldots, T_n, T_0]$.

Let us extend the valuation ν on $\overline{\mathbb{K}}\langle\langle T \rangle\rangle$ to $\overline{\mathbb{K}}\langle\langle T \rangle\rangle[T_1, \ldots, T_n, T_0]$ in the direct manner, by setting $\nu(\sum_\alpha f_\alpha T_0^{\alpha_0} \cdots T_n^{\alpha_n}) = \min_\alpha \nu(f_\alpha)$. The fact that C has no factor in $\mathbb{K}[T]$ implies that $\nu(C) = 0$. Using Gauss' Lemma, we see that the valuation of the right-hand side is $\nu(\ell) + \sum_{\kappa < i \leqslant c} \mu_i$, with $\mu_i = \nu(\Phi_i)$ for all i; note that $\mu_i < 0$ for $i > \kappa$. Thus, we can rewrite

$$C = \left(T^{-\nu(\ell)} \ell\right) \prod_{1 \leqslant i \leqslant \kappa} (T_0 - T_1 \Phi_{i,1} - \cdots - T_N \Phi_{i,n}) \prod_{\kappa < i \leqslant c'} (T^{-\mu_i} T_0 - T^{-\mu_i} T_1 \Phi_{i,1} - \cdots - T^{-\mu_i} T_n \Phi_{i,n}),$$

where all terms appearing above have non-negative valuation. As a result, we can take the coefficient of T^0 term-wise, and obtain

$$C(0, T_0) = s \prod_{1 \leqslant i \leqslant \kappa} (T_0 - T_1 \varphi_{i,1} - \cdots - T_n \varphi_{i,n}),$$

where s is in $\overline{\mathbb{K}}[T_1, \ldots, T_n]$; note that $s \neq 0$, since $C(0, T_0)$ is non-zero. By construction of C, for any $\mathbf{x} = (x_1, \ldots, x_n)$ in $V(J + \langle T \rangle)$, $T_1 y_1 + \cdots + T_n y_n$ cancels $C(0, T_0)$, so $\mathbf{x}$ must be one of $\varphi_1, \ldots, \varphi_\kappa$.

□

Lemma D.6. *$\Phi_1, \ldots, \Phi_{c'}$ are bounded.*

Proof. For $i = 1, \ldots, c'$, write $\Phi_i = 1/T^{e_i}(\Psi_{i,1}, \ldots, \Psi_n)$, for a vector $(\Psi_{i,1}, \ldots, \Psi_{i,n})$ of Puiseux series of valuation zero, that is, such that all $\Psi_{i,j}$ are bounded and $(\psi_{i,1}, \ldots, \psi_{i,n}) = \lim_0(\Psi_{i,1}, \ldots, \Psi_{i,n})$ is nonzero. Hence, $e_i = -\nu(\Phi_i)$, and we have to prove that $e_i \leqslant 0$. By way of contradiction, we assume that $e_i > 0$.

The Puiseux series Φ_i cancels $h_1, \ldots, h_M$. For $k = 1, \ldots, M$, let $h_k^H \in \overline{\mathbb{K}}[T][X_0, \mathbf{X}]$ be the homogenization of h_k with respect to $\mathbf{X}$. From the equality $h_k^H(T^{e_i}, \Psi_{i,1}, \ldots, \Psi_{i,n}) = T^{e_i} h_k(\Phi_i)$, we deduce that $h_k^H(T^{e_i}, \Psi_{i,1}, \ldots, \Psi_{i,n}) = 0$ for all k. We can write $h_k = h_{0,k} + T\tilde{h}_k$, for some polynomial $\tilde{h}_k$ in $\overline{\mathbb{K}}[T, \mathbf{X}]$, and $\mathsf{G}_2(0)$ implies that $\deg_{\mathbf{X}}(\tilde{h}_k) \leqslant \deg_{\mathbf{X}}(h_{0,k})$. As a result, the homogenizations (with respect to $\mathbf{X}$) of $h_k, h_{0,k}$ and $\tilde{h}_k$ satisfy a relation of the form $h_k^H = h_{0,k}^H + X_0^{\delta_k} T\tilde{h}_k^H$, for some $\delta_k \geqslant 0$. This implies the equality

$$h_{0,k}^H(T^{e_i}, \Psi_{i,1}, \ldots, \Psi_{i,n}) + T^{\delta_k e_i + 1}\tilde{h}_k^H(T^{e_i}, \Psi_{i,1}, \ldots, \Psi_{i,n}) = 0.$$

The second term has positive valuation, so that $h_{0,k}^H(T^{e_i}, \Psi_{i,1}, \ldots, \Psi_{i,n})$ has positive valuation as well. Taking the coefficient of T^0, this means that $h_{0,k}^H(0, \psi_{i,1}, \ldots, \psi_{i,n}) = 0$ (since $e_i > 0$), which implies that $(\psi_{i,1}, \ldots, \psi_{i,n}) = (0, \ldots, 0)$, in view of $\mathsf{G}_3(0)$. This however contradicts the definition of $(\psi_{i,1}, \ldots, \psi_{i,n})$. □

For $i = 1, \ldots, c'$, we define $\varphi_i = (\varphi_{i,1}, \ldots, \varphi_{i,n})$ as $\varphi_i = \lim_0(\Phi_i) \in \overline{\mathbb{K}}^n$. In particular, all φ_i, $i = 1, \ldots, c'$, are roots of $\mathbf{h}_0$.

Lemma D.7. *The ideal $\mathfrak{J}'$ is radical; equivalently, $c' = c$.*

Proof. We know that $\mathfrak{J}'$ has dimension zero, so it is enough to prove that for $i = 1, \ldots, c'$, the localization of $\overline{\mathbb{K}}\langle\langle T\rangle\rangle[\mathbf{X}]/\mathfrak{J}'$ at the maximal ideal $\mathfrak{m}_{\Phi_i}$ is a field, or equivalently that the localization of $\overline{\mathbb{K}}\langle\langle T\rangle\rangle[\mathbf{X}]/\mathfrak{J}$ at $\mathfrak{m}_{\Phi_i}$ is a field. By the Jacobian criterion [**?**, Theorem 16.19.b], this is the case if and only if the Jacobian matrix of $\mathbf{h}$ with respect to $\mathbf{X}$ has full rank n at Φ_i. We know that $\varphi_i = \lim_0(\Phi_i)$ is a root of $\mathbf{h}_0$, and the Jacobian criterion conversely implies that since the ideal $\langle \mathbf{h}_0 \rangle$ is radical (by assumption $\mathsf{G}_1(0)$) and zero-dimensional (by assumption $\mathsf{G}_3(0)$), the Jacobian matrix of $\mathbf{h}_0(\mathbf{X}) = \mathbf{h}(0, \mathbf{X})$ has full rank n. Since this matrix is the limit at zero of the Jacobian matrix of $\mathbf{h}$ with respect to $\mathbf{X}$, taken at Φ_i, the latter must have full rank n, and our claim that $\mathfrak{J}'$ is radical is proved. □

To finish the proof of Proposition 4.1, we have to establish that $V(\mathbf{h}_0)$ consists of exactly c solutions. Let thus d be the number of points in $V(\mathbf{h}_0)$. Since $\langle \mathbf{h}_0 \rangle$ is radical (this is $\mathsf{G}_1(0)$), Lemma D.4 implies that $d \leqslant c$, so we only have to prove that $c \leqslant d$. To prove this, we prove that for i, i' in $\{1, \ldots, c\}$, with $i \neq i'$, we have $\varphi_i \neq \varphi_{i'}$.

Suppose to the contrary that $\varphi_i = \varphi_{i'}$. We know that the Jacobian matrix of $\mathbf{h}_0$ has full rank N at φ_i; up to reindexing, we assume that rows $1, \ldots, n$ correspond to a maximal nonzero minor. Let $\mathbf{h}' = (h_1, \ldots, h_n)$.

Let $m = \nu(\Phi_i - \Phi_{i'})$; since $\varphi_i = \varphi_{i'}$, we have $m > 0$. We can thus write $\Phi_i = f + T^m\delta_i$ and $\Phi_{i'} = f + T^m\delta_{i'}$, for some vectors of bounded Puiseux series $f, \delta_i, \delta_{i'}$ such that all terms in f have valuation less than m; in addition, $\lim_0(\delta_i) \neq \lim_0(\delta_{i'})$. Write the Taylor expansion of $\mathbf{h}'$ at f as

$$\mathbf{h}'(\Phi_i) = \mathbf{h}'(f) + \mathrm{jac}(\mathbf{h}', \mathbf{X})T^m\delta_i + T^{2m}r_i = 0$$

and

$$\mathbf{h}'(\Phi_{i'}) = \mathbf{h}'(f) + \mathrm{jac}_f(\mathbf{h}', \mathbf{X})T^m\delta_{i'} + T^{2m}r_{i'} = 0,$$

for some vectors of bounded Puiseux series $r_i, r_{i'}$. By subtraction and division by T^m, we obtain $\mathrm{jac}(\mathbf{h}', \mathbf{X})(\delta_i - \delta_{i'}) = T^m r$, for some vector of bounded Puiseux series r. Since $\mathrm{jac}(\mathbf{h}', \mathbf{X})$ is invertible, this further gives $\delta_i - \delta_{i'} = T^m r'$, where again r' is a vector of bounded Puiseux series. However, by construction the left-hand side has valuation zero, while the right-hand side has positive valuation (since $m > 0$). Hence, we derived a contradiction to our assumption that $\varphi_i = \varphi_{i'}$. The proof of Proposition 4.1 is complete.