Solving determinantal systems using homotopy techniques

J.D. Hauenstein[1], M. Safey El Din[2], É. Schost[3], T. X. Vu[2,3]

December 13, 2017

Abstract

Let $\mathbf{K}$ be a field of characteristic 0 and $\overline{\mathbf{K}}$ be an algebraic closure of $\mathbf{K}$. Consider a sequence of polynomials $G = (g_1, \ldots, g_s)$ in $\mathbf{K}[X_1, \ldots, X_n]$, a polynomial matrix $F = [f_{i,j}] \in \mathbf{K}[X_1, \ldots, X_n]^{p \times q}$, with $p \leq q$ and the algebraic set $V_p(F, G)$ of points in $\overline{\mathbf{K}}$ at which all polynomials in G and all p-minors of F vanish. Such polynomial systems appear naturally in e.g. polynomial optimization, computational geometry.

We provide bounds on the number of isolated points in $V_p(F, G)$ depending on the maxima of the degrees in rows (resp. columns) of F. Next, we design homotopy algorithms for computing those points. These algorithms take advantage of the determinantal structure of the system defining $V_p(F, G)$. In particular, the algorithms run in time that is polynomial in the bound on the number of isolated points.

1 Introduction

Throughout, let $\mathbf{K}$ be a field of characteristic 0 with algebraic closure $\overline{\mathbf{K}}$, $(X_1, \ldots, X_n)$ is a set of n variables, and $\mathbf{K}[X_1, \ldots, X_n]$ is the multivariate polynomial ring in n variables with coefficients in $\mathbf{K}$. With this setup, let $F = [f_{i,j}] \in \mathbf{K}[X_1, \ldots, X_n]^{p \times q}$ be a polynomial matrix, with $p \leq q$. The first question which will interest us in this paper is to describe the set of points $\boldsymbol{x} \in \overline{\mathbf{K}}^n$ at which the evaluation of the matrix F has rank less than p. In the particular case $p = 1$, this simply means finding all common solutions of $f_{1,1}, \ldots, f_{1,q}$.

For any matrix F over a ring R, and for any integer r, $M_r(F)$ will denote the set of r-minors of F, and $I_r(F)$ will denote the ideal they generate in R. For any ideal I in $\mathbf{K}[X_1, \ldots, X_n]$, $V(I)$ will denote the zero-set of I in $\overline{\mathbf{K}}^n$, and for a matrix F with entries in $\mathbf{K}[X_1, \ldots, X_n]$, we will write $V_r(F) = V(I_r(F))$. In particular, for F of size $p \times q$, with $p \leq q$, the set of points introduced in the previous paragraph is

$$V_p(F) = \{\boldsymbol{x} \in \overline{\mathbf{K}}^n \mid \operatorname{rank}(F(\boldsymbol{x})) < p\}.$$

[1]Department of Applied and Computational Mathematics and Statistics, University of Notre Dame, USA
[2]Sorbonne Universités, UPMC Univ. Paris 06, CNRS, INRIA Paris Center, LIP6, PolSys Team, France
[3]David Cheriton School of Computer Science, University of Waterloo, ON, Canada

This is an algebraic set, since it is defined by the vanishing of all maximal minors of F.

We will discuss below dimension properties of $V_p(F)$. Recall that any algebraic set V is the finite union of its *irreducible components*: these are the maximal irreducible algebraic sets contained in it (an algebraic set is irreducible if it is not the union of two proper algebraic sets). The *dimension* of an algebraic set V is the largest integer d such that intersecting V with d generic hyperplanes yields finitely many points; those algebraic sets with all irreducible components of the same dimension are called *equidimensional*. We refer to e.g. [54, Chap. I and II] for these notions.

For the problem above, it is natural to consider the case where $n = q - p + 1$. Indeed, results due to Macaulay [40] and Eagon and Northcott [20] imply that all irreducible components of $V_p(F)$ have dimension at least $n-(q-p+1)$; furthermore, in the case $n = q-p+1$, $V_p(F)$ has dimension zero for a generic choice of the entries of F (this is proved for instance in [57]). Of course, even if we assume $n = q-p+1$, $V_p(F)$ may have components of positive dimension; in this case, we will be interested in describing only its *isolated points*, that is, the points in the irreducible components of $V_p(F)$ of dimension zero (this notion makes sense for any field $\mathbf{K}$; when $\mathbf{K} = \mathbb{R}$, these points are indeed isolated for the metric topology).

Studying the set $V_p(F)$ is a particular case of a slightly more general question. In addition to matrix F, we may indeed take into account further equations of the form $g_1 = \cdots = g_s = 0$, for some $G = (g_1, \ldots, g_s)$ in $\mathbf{K}[X_1, \ldots, X_n]$. In this setting, the natural relation between the number n of variables, the size of F and the number s of polynomials in G is now $n = q - p + s + 1$. Then, we define the algebraic set

$$V_p(F, G) = \{\boldsymbol{x} \in \overline{\mathbf{K}}^n \mid \operatorname{rank}(F(\boldsymbol{x})) < p \text{ and } g_1(\boldsymbol{x}) = \cdots = g_s(\boldsymbol{x}) = 0\};$$

this is thus the zero-set of the ideal $I_p(F) + \langle g_1, \ldots, g_s\rangle$. Our main problem is the following.

Problem 1. *For a field* $\mathbf{K}$*, a matrix* $F \in \mathbf{K}[X_1, \ldots, X_n]^{p\times q}$ *and polynomials* $G = (g_1, \ldots, g_s)$ *in* $\mathbf{K}[X_1, \ldots, X_n]$ *such that* $p \leq q$ *and* $n = q-p+s+1$*, compute the isolated points of* $V_p(F, G)$*.*

This problem appears in a variety of context; prominent examples are optimization problems [30, 38, 7, 29, 44], and related questions in real algebraic geometry [3, 5, 6, 8, 9, 10, 14, 16, 31, 48, 49, 51], where F consists of the Jacobian matrix of G, together with one extra row, corresponding to the gradient of a function g that we want to optimize on $V(G)$.

In several of these situations, we are only interested in the solutions of the system which consists of $G, M_p(F)$ at which its associated Jacobian matrix is full rank. This subset of solutions is finite and is always a subset of the set of isolated points of $V_p(F, G)$ [21, Theorem 16.19] ; we call these points *simple isolated points*.

The set of simple isolated points also coincides with $V_p(F, G)$ when the system $G, M_p(F)$ generates a radical ideal of dimension 0 – that case appears frequently in the context of algorithms in real algebraic geometry ; see e.g. [8]. Hence, it also makes sense to look at the following slight variant of Problem 1.

Problem 2. *For a field* $\mathbf{K}$*, a matrix* $F \in \mathbf{K}[X_1, \ldots, X_n]^{p\times q}$ *and polynomials* $G = (g_1, \ldots, g_s)$ *in* $\mathbf{K}[X_1, \ldots, X_n]$ *with* $p \leq q$ *and* $n = q - p + s + 1$*, compute the simple isolated points of* $V_p(F, G)$*.*

We will represent the output of our algorithm using univariate polynomials. Let $V \subset \overline{\mathbf{K}}^n$ be a zero-dimensional algebraic set defined over $\mathbf{K}$. A *zero-dimensional parametrization* $\mathscr{R} = ((w, v_1, \ldots, v_n), \lambda)$ of V consists of polynomials $(w, v_1, \ldots, v_n)$ such that $w \in \mathbf{K}[X]$ is monic and squarefree, all v_i's are in $\mathbf{K}[X]$ and satisfy $\deg(v_i) < \deg(w)$, and λ is a $\mathbf{K}$-linear form in n variables, such that

- $\lambda(v_1, \ldots, v_n) = Xw' \bmod w$ with $w' = \frac{\partial w}{\partial X}$;
- we have $V = Z(\mathscr{R})$, with

$$Z(\mathscr{R}) = \left\{ \left(\frac{v_1(\tau)}{w'(\tau)}, \ldots, \frac{v_n(\tau)}{w'(\tau)} \right) \mid w(\tau) = 0 \right\}.$$

The constraint on λ then says that the root of w are the values taken by λ on V. This representation was introduced in [39, 40], and has been used in a variety of algorithms, such as those in [25, 27, 1, 26, 46, 28]. The reason we use a rational parametrization, with w' as a denominator, goes back to [1, 46, 28]: when $\mathbf{K} = \mathbb{Q}$, this allows us to control precisely the bit-size of the coefficients, using bounds such as those in [53, 18]. (The same phenomenon holds with $\mathbf{K} = k(T)$ – k is field –, in which case we want to control degrees in T of the numerators and denominators of the coefficients of $\mathscr{R}$.)

Our first result gives a bound on the multiplicities of the solutions of $V_p(F, G)$. To state it, we need the following notation. Take $F = [f_{i,j}]_{1 \le i \le p, 1 \le j \le q}$ in $\mathbf{K}[X_1, \ldots, X_n]^{p \times q}$. We will consider two degree measures for matrix F (these have been used before for determinantal ideals, see for instance [45, 42]). For $i = 1, \ldots, p$, we will write $\operatorname{rdeg}(F, i)$ for the degree of the ith row of F, that is, $\operatorname{rdeg}(F, i) = \max(\deg(f_{i,j}))_{1 \le j \le q}$; similarly, for $j = 1, \ldots, q$, we write $\operatorname{cdeg}(F, j)$ for the degree of the jth column of F, that is, $\operatorname{cdeg}(F, j) = \max(\deg(f_{i,j}))_{1 \le i \le p}$. For $k \ge 0$, $E_k(\delta_1, \ldots, \delta_q)$ is the elementary symmetric polynomial of degree k in $(\delta_1, \ldots, \delta_q)$ and $S_k(\alpha_1, \ldots, \alpha_p)$ is the kth complete symmetric polynomial in $(\alpha_1, \ldots, \alpha_p)$.

Finally, recall the notion of multiplicity of a point $\boldsymbol{x}$ with respect to an ideal I in $\mathbf{K}[X_1, \ldots, X_n]$ (we refer to [21, Chap. 3] for more details on the following notions). The ideal I can be written as the intersection of finitely many primary components, that is, $I = Q_1 \cap \cdots \cap Q_r$ for some primary ideals $Q_1, \ldots, Q_r$; this decomposition is said to be minimal when $V(Q_i) \neq V(Q_j)$ for $i \neq j$. For $\boldsymbol{x} \in V(I)$, one says that $\boldsymbol{x}$ isolated in $V(I)$ when there exists a unique primary component Q_i (which has dimension zero) such that $\boldsymbol{x}$ is in $V(Q_i)$; although minimal primary decompositions are not unique, the fact that $\boldsymbol{x}$ is isolated implies that Q_i does not depend on the primary decomposition of I we consider; then, the *multiplicity* of $\boldsymbol{x}$ is defined as the dimension of $\mathbf{K}[X_1, \ldots, X_n]/Q_i$. The following is our first result.

Theorem 1. *Let F be in $\mathbf{K}[X_1, \ldots, X_n]^{p \times q}$ and let $G = (g_1, \ldots, g_s)$ be in $\mathbf{K}[X_1, \ldots, X_n]$, with $p \le q$ and $n = q - p + s + 1$. Then, the sum of the multiplicities of the isolated points of $I_p(F) + \langle g_1, \ldots, g_s \rangle$ is at most $\min(c, c')$ with*

$$c = \deg(g_1) \cdots \deg(g_s) E_{n-s}(\operatorname{cdeg}(F, 1), \ldots, \operatorname{cdeg}(F, q))$$

and

$$c' = \deg(g_1)\cdots\deg(g_s)S_{n-s}(\mathrm{rdeg}(F,1),\ldots,\mathrm{rdeg}(F,p)).$$

When $\mathrm{rdeg}(G,i) = \mathrm{cdeg}(F,j) = d$ for all i,j, the two bounds given above coincide, with common value $\deg(g_1)\cdots\deg(g_s)d^{n-s}\binom{q}{p-1}$; otherwise, either of the two expressions $E_{n-s}(\mathrm{cdeg}(F,1),\ldots,\mathrm{cdeg}(F,q))$ and $S_{n-s}(\mathrm{rdeg}(F,1),\ldots,\mathrm{rdeg}(F,p))$ can be the minimum.

Previous work by Miller and Sturmfels [42, Chapter 15] proved very general results on the multi-degrees of determinantal ideals built from matrices with indeterminate entries (in which case we have $s = 0$, but the assumption $n = q - p + 1$ does not hold); in particular, they obtain analogues (and generalizations) of the result in Theorem 1 in that context.

Nie and Ranestad proved in [45] that the bounds in Theorem 1 are equalities for two families of polynomials (in a similar context where the polynomials are homogeneous in $n+1$ variables):

- when entries of F are generic and homogeneous, and such that $\deg(f_{i,j}) = \mathrm{cdeg}(F,j)$ for all i,j, the ideal $I_p(F)$ has degree $E_n(\mathrm{cdeg}(F,1),\ldots,\mathrm{cdeg}(F,q))$;
- when entries of F are generic and homogeneous, and such that $\deg(f_{i,j}) = \mathrm{rdeg}(F,i)$ for all i,j, the ideal $I_p(F)$ has degree $S_n(\mathrm{rdeg}(F,1),\ldots,\mathrm{rdeg}(F,p))$.

From this, they deduce that the degree of the ideal $I_p(F) + \langle g_1,\ldots,g_s\rangle$ is at most $\deg(g_1)\cdots\deg(g_s)S_{n-s}(\mathrm{rdeg}(F,1),\ldots,\mathrm{rdeg}(F,p))$, for systems coming from optimization problems (the matrix F is the Jacobian matrix of $G = (g_1,\ldots,g_s)$, with one extra row of the form gradient(g) where g is a polynomial to be optimized under the constraints $g_1 = \cdots = g_s = 0$), and assuming that this ideal has dimension zero. For generic choices of such $G = (g_1,\ldots,g_s)$ and g, Spaenlehauer gave in [57] an explicit expression for the Hilbert function of the ideal $I_p(F) + \langle g_1,\ldots,g_s\rangle$.

Our second result gives bounds on the cost of computing a zero-dimensional parametrization of the isolated solutions of $V_p(F,G) = V(I_p(F) + \langle g_1,\ldots,g_s\rangle)$. Our algorithms take as input a *straight-line program* (that is, a sequence of elementary operations $+,-,\times$) that computes the entries of F and G from the input variables $X_1,\ldots,X_n$. The *length* σ of the input is the number of operations it performs. This assumption is not restrictive, since any matrix F and polynomials G can be computed by a straight-line program (a naive solution would consist in computing and adding all monomials in F and G).

Theorem 2. *Suppose that matrix* $F \in \mathbf{K}[X_1,\ldots,X_n]^{p\times q}$ *and polynomials* $G = (g_1,\ldots,g_s)$ *in* $\mathbf{K}[X_1,\ldots,X_n]$ *are given by a straight-line program of length* σ. *Assume that* $\deg(g_1),\ldots,\deg(g_s)$, *as well as* $\mathrm{cdeg}(F,1),\ldots,\mathrm{cdeg}(F,q)$ *and* $\mathrm{rdeg}(F,1),\ldots,\mathrm{rdeg}(F,p)$ *are all at least equal to* 1.

Then, there exists a probabilistic algorithm that solves Problem 1 in either

$$O^{\sim}\left(\binom{q}{p}n^3c(e+c^5)(\sigma+\chi)\right)$$

operations in $\mathbf{K}$*, with*

$$\begin{aligned} c &= \deg(g_1)\cdots\deg(g_s)E_{n-s}(\mathrm{cdeg}(F,1),\ldots,\mathrm{cdeg}(F,q)) \\ e &= (\deg(g_1)+1)\cdots(\deg(g_s)+1)E_{n-s}(\mathrm{cdeg}(F,1)+1,\ldots,\mathrm{cdeg}(F,q)+1) \\ \chi &= q\max(\mathrm{cdeg}(F,i), 1\le i\le q) + \max(\deg(g_i), 1\le i\le s) \end{aligned}$$

or

$$O^{\sim}\left(c'^2 n^5 \binom{q}{p}^2 (e' + c'^5 n)(\sigma + \chi')\right)$$

operations in $\mathbf{K}$*, with*

$$\begin{aligned} c' &= \deg(g_1)\cdots\deg(g_s)S_{n-s}(\mathrm{rdeg}(F,1),\ldots,\mathrm{rdeg}(F,p)) \\ e' &= (\deg(g_1)+1)\cdots(\deg(g_s)+1)S_{n-s}(\mathrm{rdeg}(F,1)+1,\ldots,\mathrm{rdeg}(F,p)+1) \\ \chi' &= \binom{q}{p} n + \max(\mathrm{rdeg}(F,i), \le i\le p) + \max(\deg(g_i), 1\le i\le s) + n^3. \end{aligned}$$

The assumption that all degrees be at least 1 is not a restriction. If $\deg(g_i) = 0$ for some i, g_i is a constant, so either the system is inconsistent (if $g_i \neq 0$) or g_i can be discarded. Similarly, if say $\mathrm{cdeg}(F,i) = 0$, the ith column of F consists of constants; after applying linear combinations with coefficients in $\mathbf{K}$ to the rows of F, we may assume that all entries in the ith column, except at most one, are non-zero without changing the column degrees. The ith column of F (and the row of the non-zero entry, if there is one) can then be discarded.

Remark further that in the common situation where all degrees involved in the formulas above are at least equal to 2, we have the inequalities $e \le c^2$ and $e' \le c'^2$; as a result, the runtimes become *polynomial* in respectively c, σ and c', σ. This is to be compared with Theorem 1, which shows that $\min(c, c')$ is a natural upper bound for the output size of such algorithms.

For solving Problem 2, one obtains slightly better complexity estimates.

Theorem 3. *Suppose that the matrix* $F \in \mathbf{K}[X_1,\ldots,X_n]^{p\times q}$ *and polynomials* $G = (g_1,\ldots,g_s)$ *in* $\mathbf{K}[X_1,\ldots,X_n]$ *are given by a straight-line program of length* σ*. Assume that* $\deg(g_1),\ldots,\deg(g_s)$*, as well as* $\mathrm{cdeg}(F,1),\ldots,\mathrm{cdeg}(F,q)$ *and* $\mathrm{rdeg}(F,1),\ldots,\mathrm{rdeg}(F,p)$ *are all at least equal to* 1*.*

Then, there exists a probabilistic algorithm that solves Problem 2 in either

$$O^{\sim}\left(\binom{q}{p}^2 n^3\, c(c + e(\sigma + \chi))\right)$$

operations in $\mathbf{K}$*, with*

$$\begin{aligned} c &= \deg(g_1)\cdots\deg(g_s)E_{n-s}(\mathrm{cdeg}(F,1),\ldots,\mathrm{cdeg}(F,q)) \\ e &= (\deg(g_1)+1)\cdots(\deg(g_s)+1)E_{n-s}(\mathrm{cdeg}(F,1)+1,\ldots,\mathrm{cdeg}(F,q)+1) \\ \chi &= q\max(\mathrm{cdeg}(F,i), 1\le i\le q) + \max(\deg(g_i), 1\le i\le s) \end{aligned}$$

or

$$O^{\sim}\left(c'^2 n^6 \binom{q}{p}^2 (c' + e'(\sigma + \chi'))\right)$$

operations in $\mathbf{K}$*, with*

$$\begin{aligned} c' &= \deg(g_1)\cdots\deg(g_s) S_{n-s}(\operatorname{rdeg}(F,1),\ldots,\operatorname{rdeg}(F,p)) \\ e' &= (\deg(g_1)+1)\cdots(\deg(g_s)+1) S_{n-s}(\operatorname{rdeg}(F,1)+1,\ldots,\operatorname{rdeg}(F,p)+1) \\ \chi' &= n\ q\ p \max(\operatorname{rdeg}(F,i), 1 \le i \le p) + \max(\deg(g_i), 1 \le i \le s) + n^3. \end{aligned}$$

The probabilistic aspects are as follows: at several steps, the algorithms on which Theorems 2 and 3 rely will draw elements from the base field at random. In all cases, there exists an algebraic hypersurface $\mathcal{H}$ of the parameter space such that success is guaranteed for all choices of parameters not in $\mathcal{H}$.

Our algorithm is based on a *symbolic homotopy continuation*. Homotopy continuation algorithms have become a foundational tools for numerical algorithms, either in continuation of Shub and Smale's early work [55], or along the lines of work by Morgan, Sommese, Wampler (as summarized, for instance, in [12, 56]), with an emphasis on the algebraic geometry underlying these techniques. By contrast, their usage in symbolic contexts is more recent. Early references are [33, 15], which deal with systems with no particular structure; further work extended this idea to sparse systems (in the polyhedral sense) [37, 34, 35, 36] and multihomogeneous systems [32, 50].

Most algorithms in the previous references have in common that they solve *square* systems, that is, systems with as many equations as unknowns. Extensions of these methods can deal with systems of positive dimension by essentially using variants of the algorithm for square systems.

In [50], these techniques are used to solve Problem 2 but the obtained complexity estimates depend on multi-homogeneous Bézout bounds involving the maxima of $\operatorname{rdeg}(F,1),\ldots,\operatorname{rdeg}(F,p)$ or $\operatorname{cdeg}(F,1),\ldots,\operatorname{cdeg}(F,q)$.

One of the novelties in this paper is to deal with determinantal systems of equations, which are in essence over-determined; this is made possible by the algebraic properties of determinantal ideals.

It is well-known that Gröbner bases behave rather well on over-determined systems. Starting from the determination of the Hilbert function of a determinantal ring due to Conca and Herzog [17], complexity estimates are given in [23, 22] for computing Gröbner basis of ideals generated by either $M_r(F)$ when $r \le p \le q$ or $G, M_p(F)$ where F is the Jacobian matrix associated to G with one extra row) but under some genericity assumptions on the entries of F or G. Besides, they are assumed to all have the same degree. This series of works culminates with the result obtained by Spaenlehauer in [57] where he removes this latter degree assumption and provides sharp complexity statements but still under genericity assumptions.

Overdetermined systems encoding rank defects in polynomial matrices have also been studied in the scope of the so-called geometric resolution algorithm in [4] with a slight generalization in [52] computing simple isolated solutions to the input system. As our algorithm

here, these algorithms take as input straight-line programs but instead of using deformation techniques to build a global homotopy, determinantal systems are solved incrementally in some chart. Hence, the complexity of these algorithms depends here on the maximum degrees of the varieties defined by the considered intermediate systems and, even without taking into account the dimension assumption, additional results would be needed to prove that these intermediate degrees are not larger than the quantities involved in our complexity estimates.

In the following paragraphs, we describe our results in more detail. As a preliminary, we will need an algorithm which takes as input polynomials $\boldsymbol{C} = (c_1, \ldots, c_m)$ and a point $\boldsymbol{x}$ in the zero-set of $\boldsymbol{C}$, and which decides whether $\boldsymbol{x}$ is an isolated points of $V(\boldsymbol{C})$. This one will be used to solve Problem (1).

Without any other information, this decision problem is difficult to solve in a good complexity. However, when a bound μ is known on the multiplicity of $\boldsymbol{x}$ as a root of $\boldsymbol{C}$, it becomes possible to solve this problem in time polynomial in the number of equations m, the number of variables n, the bound μ, and the complexity of evaluation σ of $\boldsymbol{C}$. This is explained in Section 2, where we explain how to modify an algorithm by Mourrain [43] and adapt it to our context.

In Section 3, we give an algorithm which takes as input a sequence of polynomials $\boldsymbol{C}$ and computes a zero-dimensional parametrization of the isolated points of $V(\boldsymbol{C})$, assuming the existence of a suitable homotopy deformation. Explicitly, we suppose that $\boldsymbol{C}$ involves variables $\boldsymbol{X} = (X_1, \ldots, X_n)$, we let T be a new variable, and we suppose that we know a family of polynomials $\boldsymbol{B}$ in $\mathbf{K}[T, \boldsymbol{X}]$ such that $\boldsymbol{B}(1, \boldsymbol{X}) = \boldsymbol{C}$. Let then $\boldsymbol{A}$ be the polynomials $\boldsymbol{B}(0, \boldsymbol{X})$, and suppose that $V(\boldsymbol{A})$ is finite, and that we are able to find a zero-dimensional parametrization of it efficiently. We will actually need a few further conditions (for instance, at all points in $V(\boldsymbol{A})$, the Jacobian matrix of these polynomials must have rank n).

We will see in Section 3 that when all these conditions hold, we can divise a homotopy algorithm that lifts the points of $V(\boldsymbol{A})$ (that correspond to $T = 0$) into a curve $\mathcal{C}$ parametrized by T. The isolated points of $V(\boldsymbol{C})$ all belong to the fiber of $\mathcal{C}$ above $T = 1$, but some points in this fiber can actually lie in positive dimensional components of $V(\boldsymbol{C})$; the algorithm of Section 2 will filter out such points. The complexity we obtain depends linearly on the complexity of evaluating $\boldsymbol{C}$ and polynomially on a bound on the sum of the multiplicites of the isolated points of $V(\boldsymbol{C})$ and the degree of the homotopy curve. When one only wants to compute simple solutions, a variant of the homotopy algorithm is given: this one is actually simpler since we substitute the algorithm of Section 2 with a simple criterion allowing to identify the simple solutions we aim at computing.

We will apply these results to our determinantal problems as follows. Given $F \in \mathbf{K}[\boldsymbol{X}]^{p \times q}$ and $G = (g_1, \ldots, g_s)$, we will build a matrix

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

that connects a *start matrix* L to the target matrix F, together with a homotopy of the form

$$V = (1 - T) \cdot K + T \cdot G,$$

that connects a start system $K = (k_1, \ldots, k_s)$ to the target system G. In Section 4, we prove that several assumptions of the algorithm of Section 3 are satisfied for such systems, independently of the choice of L and K.

The actual construction of the system K will be rather straightforward; the difficulty lies in the definition of a matrix L that will respect either the column-degree or the row-degree of F (while satisyfing all assumptions for the algorithm of Section 3). The column-degree case is treated in Section 5 in a rather straightforward way, whereas the row-degree case is more delicate, and is treated in Sections 6 and 7. In both cases, we bound the sum of the multiplicities of the isolated points in $V_p(F, G)$ (thereby establishing Theorem 1), as well as the degree of the homotopy curve.

2 A local dimension test

Let $\mathbf{L}$ be a field containing the field $\mathbf{K}$ and $\overline{\mathbf{L}}$ be an algebraic closure of $\mathbf{L}$. Let $\boldsymbol{C} = (c_1, \ldots, c_m)$ be polynomials in $\mathbf{K}[\boldsymbol{X}]$, with $\boldsymbol{X} = (X_1, \ldots, X_n)$. Given a point $\boldsymbol{x}$ with coordinates in $\mathbf{L}$ in the zero-set $V(\boldsymbol{C}) \subset \overline{\mathbf{L}}^n$, we discuss here how to decide whether $\boldsymbol{x}$ is an isolated point in $V(\boldsymbol{C})$. We make the following assumption in the rest of this section:

A. We are given as input an integer μ such that either $\boldsymbol{x}$ belongs to a positive-dimensional component of $V(\boldsymbol{C})$, or $\boldsymbol{x}$ is isolated in $V(\boldsymbol{C})$, with multiplicity at most μ with respect to the ideal $\langle \boldsymbol{C} \rangle$.

Without loss of generality, we also assume that $m \geq n$ (otherwise, $\boldsymbol{x}$ cannot be an isolated solution).

Proposition 4. *Suppose that $\boldsymbol{C}$ is given by a straight-line program of length σ. If assumption* A *is satisfied, we can decide whether $\boldsymbol{x}$ is an isolated root of $V(\boldsymbol{C})$ using*

$$O(n^4\mu^4 + n^2 m\mu^3 + n\sigma\mu^4) \subset (\mu\,\sigma\,m)^{O(1)}$$

operations in $\mathbf{L}$.

Reference [11] gives an algorithm to compute the dimension of $V(\boldsymbol{C})$ at $\boldsymbol{x}$, but its complexity is not known to us, as it relies on linear algebra with matrices of potentially large size (not necessarily polynomial in μ, σ, m). Instead, we use an adaptation of a prior result by Mourrain [43], 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 $\boldsymbol{C}$, which would be too high for the applications we will make of this result.

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

Lemma 5. *Let I be the zero-dimensional ideal $\langle \boldsymbol{C} \rangle + \mathfrak{m}^{\mu+1}$, where $\mathfrak{m} = \langle X_1, \ldots, X_n \rangle$ is the maximal ideal at the origin. Then, 0 is isolated in $V(\boldsymbol{C})$ if and only if the multiplicity d of I at the origin is at most μ.*

Proof. This follows from the following result [11, Theorem A.1]. For $k \geq 1$, let I_k be the zero-dimensional ideal $\langle \boldsymbol{C} \rangle + \mathfrak{m}^k$, and let ν_k be the multiplicity of the origin with respect to this ideal. Then, the reference above proves that the sequence $(\nu_k)_{k \geq 1}$ is non-decreasing, and that 0 is isolated in $V(\boldsymbol{C})$ if and only if there exists $k \geq 1$ such that $\nu_k = \nu_{k+i}$ for any $i \geq 0$.

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

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

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.

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

- for i in $\{1, \ldots, d\}$ and k in $\{1, \ldots, n\}$, we have $X_k \cdot \beta_i = \sum_{0 \leq j < i} \lambda_{i,j}^{(k)} \beta_j$ (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 $\{2, \ldots, d\}$, $\beta_i(1) = 0$.

The following lemma shows that the coefficients $(\lambda_{i,j}^{(k)})$ are sufficient to evaluate the linear forms β_i at any f in $\mathbf{L}[\boldsymbol{X}]$. More precisely, knowing only their values for $j < i \leq s$, for any $s \leq d$, allows us to evaluate $\beta_1, \ldots, \beta_s$ at such an f. The following lemma follows [43] in its description of the matrices $\boldsymbol{M}_{k,s}$; the (rather straightforward) complexity analysis in the straight-line program model is new.

Lemma 6. *Let s be in $1, \dots, d$, 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 σ that computes $\boldsymbol{h} = (h_1, \dots, h_R)$, one can compute $\beta_i(h_r)$, for all $i = 1, \dots, s$ and $r = 1, \dots, R$, using $O(s^3\,\sigma)$ operations in $\mathbf{L}$.*

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

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

Remark that the matrices $\boldsymbol{M}_{k,s}$ all commute with each other. 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 $\Delta_{k,k',s} = \boldsymbol{M}_{k,s}\boldsymbol{M}_{k',s} - \boldsymbol{M}_{k',s}\boldsymbol{M}_{k,s}$. 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 $\mathbf{L}[\boldsymbol{X}]$, we have the equality

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

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 lemma, it is then enough to note that the evaluations $h_1(\boldsymbol{M}_{1,s}, \dots, \boldsymbol{M}_{n,s}), \dots, h_R(\boldsymbol{M}_{1,s}, \dots, \boldsymbol{M}_{n,s})$ can be computed using the straight-line program doing $O(s^3\,\sigma)$ operations. □

Mourrain's algorithm 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 $e_1 \le e_2 \le e_3 \dots$ Mourrain's algorithm stops when $e_{\ell+1} = e_\ell$, in which case $\beta_1, \dots, \beta_{e_\ell}$ is an $\mathbf{L}$-basis of $I^\perp$, and $e_\ell = d$. 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 $e_1 < \cdots < e_\ell \le \mu$. 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 d of I at the origin is $e_\ell \le \mu$; we stop the algorithm;
- if $e_{\ell+1} > \mu$, we conclude that this multiplicity is greater than μ; we stop the algorithm;

- else, when $e_\ell < e_{\ell+1} \leq \mu$, we do another loop.

Because the e_ℓ's are an increasing sequence of integers, they satisfy $e_\ell \geq \ell$; hence, every time we enter the loop above we have $\ell \leq \mu$. 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 $0 \leq j < i \leq e_\ell$ and $1 \leq k \leq n$. At step ℓ, Mourrain's algorithm solves a homogeneous linear system T_ℓ with $n(n-1)e_\ell/2 + m'$ equations and ne_ℓ unknowns, where m' is the number of generators of the ideal $I = \langle \boldsymbol{C} \rangle + \mathfrak{m}^{\mu+1}$. Remark that m' is not polynomial in μ and n, so the size of T_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 $\ell \geq 2$, 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 T_ℓ. For k in $\{1, \ldots, n\}$ and an $\mathbf{L}$-linear form β, we denote by $X_k^{-1} \cdot \beta$ the $\mathbf{L}$-linear form defined by $\mathbf{L}$-linearity as follows:

- $(X_k^{-1} \cdot \beta)(X_k f) = \beta(f)$ for any monomial f in $\mathbf{L}[\boldsymbol{X}]$,
- $(X_k^{-1} \cdot \beta)(f) = 0$ if $f \in \mathbf{L}[\boldsymbol{X}]$ is a monomial which does not depend on X_k.

In other words, $(X_k^{-1} \cdot \beta)(f) = \beta(\delta_k(f))$ holds for all f, where $\delta_k : \mathbf{L}[\boldsymbol{X}] \to \mathbf{L}[\boldsymbol{X}]$ 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 T_ℓ are:

- the first $n(n-1)e_\ell/2$ equations involve only the coefficients $\lambda_{i,j}^{(k)}$ previously computed (we refer to [43, Section 4.4] for details of how exactly these entries are distributed in T_ℓ, as we do not need such details here).
- each of the other m' equations has coefficient vector

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

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

We claim that only those equations corresponding to generators $c_1, \ldots, c_m$ of the input system $\boldsymbol{C}$ 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 $\ell \leq \mu$, 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 v_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

$$(X_k^{-1} \cdot \beta_i)(c_j(X_1, \ldots, X_k, 0, \ldots, 0)),$$

for $k = 1, \ldots, n$, $i = 1, \ldots, e_\ell$ and $j = 1, \ldots, m$. Fixing k, we let $\boldsymbol{C}_k = (c_{j,k})_{1 \leq j \leq m}$, where $c_{j,k}$ is the polynomial $c_j(X_1, \ldots, X_k, 0, \ldots, 0)$; note that the system $\boldsymbol{C}_k$ can be computed by a straight-line program of length $\sigma' = \sigma + n$. Then, applying the following lemma with $s = e_\ell \leq \mu$ and $\boldsymbol{h} = \boldsymbol{C}_k$, we deduce that the values $(X_k^{-1} \cdot \beta_i)(c_j(X_1, \ldots, X_k, 0, \ldots, 0))$, for k fixed, can be computed in time $O(\mu^3(\sigma + n))$.

Lemma 7. *Let s be in $1, \ldots, d$, and suppose that the coefficients $\lambda_{i,j}^{(k)}$ are known for $i = 1, \ldots, s$, $j = 0, \ldots, i-1$ and $k = 1, \ldots, n$. Given a straight-line program Γ of length σ that computes $\boldsymbol{h} = (h_1, \ldots, h_R)$ and given k in $\{1, \ldots, n\}$, one can compute $(X_k^{-1} \cdot \beta_i)(h_r)$, for all $i = 1, \ldots, s$ and $r = 1, \ldots, R$, using $O(s^3(\sigma + n))$ operations in $\mathbf{L}$.*

Proof. In view of the formula $(X_k^{-1} \cdot \beta)(f) = \beta(\delta_k(f))$, and of Lemma 6, it is enough to prove the existence of a straight-line program of length $O(\sigma+n)$ that computes $(\delta_k(h_1), \ldots, \delta_k(h_R))$.

To do this, we replace all polynomials $\gamma_{-n+1}, \ldots, \gamma_\sigma$ computed by Γ by terms $\eta_{-n+1}, \ldots, \eta_\sigma$ and $\nu_{-n+1}, \ldots, \nu_\sigma$, with $\eta_\ell = \gamma_\ell(X_1, \ldots, X_{k-1}, 0, X_{k+1}, \ldots, X_n)$ and ν_ℓ in $\mathbf{L}[\boldsymbol{X}]$ such that $\gamma_\ell = \eta_\ell + X_k \nu_\ell$ holds for all ℓ, so that in particular $\nu_\ell = \delta_k(\gamma_\ell)$. To compute η_ℓ and ν_ℓ, assuming all previous $\eta_{\ell'}$ and $\nu_{\ell'}$ are known, we proceed as follows:

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

$$\nu_\ell = \eta_{a_\ell} \nu_{b_\ell} + \nu_{a_\ell} \eta_{b_\ell} + X_k \nu_{a_\ell} \nu_{b_\ell}.$$

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

Taking all values of k into account, we see that we can compute all entries we need to set up the linear system T_ℓ using $O(\mu^3 n(\sigma+n))$ operations in $\mathbf{L}$. After discarding the useless equations described above, the numbers of equations and unknowns in the system T_ℓ are respectively at most $n^2\mu+m$ and $n\mu$; this implies that we can find a nullspace basis of it in time $O(n^4\mu^3+n^2m\mu^2)$. Altogether, the time spent to find $\boldsymbol{\beta}^{(\ell+1)}$ from $(\boldsymbol{\beta}^{(1)},\boldsymbol{\beta}^{(2)},\ldots,\boldsymbol{\beta}^{(\ell)}) = (\beta_1,\ldots,\beta_{e_\ell})$ is $O(n^4\mu^3+n^2m\mu^2+n\sigma\mu^3)$.

Since we saw that we do at most μ such loops, the cumulated time is $O(n^4\mu^4+n^2m\mu^3+n\sigma\mu^4)$, and Proposition 4 is proved.

3 Symbolic homotopies

In this section, we work over a field $\mathbf{K}$, still using n variables $\boldsymbol{X}=(X_1,\ldots,X_n)$. Given polynomials $\boldsymbol{C}=(c_1,\ldots,c_m)$ in $\mathbf{K}[\boldsymbol{X}]^m$, we give an algorithm to compute a zero-dimensional parametrization of the isolated points of $V(\boldsymbol{C})$, assuming the existence of a suitable *homotopy deformation* of $\boldsymbol{C}$. We assume $m\geq n$, otherwise no isolated points exist in $V(\boldsymbol{C})$.

Let T be a new variable and consider polynomials $\boldsymbol{B}=(b_1,\ldots,b_m)$ in $\mathbf{K}[T,\boldsymbol{X}]$; for τ in $\overline{\mathbf{K}}$, we write $\boldsymbol{B}_\tau=(b_{\tau,1},\ldots,b_{\tau,m})=\boldsymbol{B}(\tau,\boldsymbol{X})\subset\overline{\mathbf{K}}[\boldsymbol{X}]$ and we assume that $\boldsymbol{B}$ is such that $\boldsymbol{B}_1=\boldsymbol{C}$. Define further the ideal $J=\langle\boldsymbol{B}\rangle\subset\overline{\mathbf{K}}[T,\boldsymbol{X}]$ and consider the folllowing assumptions.

B_1. Any irreducible component of $V(J)\subset\overline{\mathbf{K}}^{n+1}$ has dimension at least one.

B_2. For any maximal ideal $\mathfrak{m}\subset\overline{\mathbf{K}}[T,\boldsymbol{X}]$, if the localization $J_\mathfrak{m}\subset\overline{\mathbf{K}}[T,\boldsymbol{X}]_\mathfrak{m}$ 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, B_1 is Krull's theorem, and B_2 is Macaulay's unmixedness theorem in the Cohen-Macaulay ring $\overline{\mathbf{K}}[T,\boldsymbol{X}]_\mathfrak{m}$ [21, Corollary 18.14]. More generally, these properties hold when $\boldsymbol{B}$ is the sequence of p-minors of a $p\times q$ matrix with entries in $\mathbf{K}[T,\boldsymbol{X}]$, with $p\leq q$ and $n=q-p+1$; we discuss this, and a slightly more general situation, in Section 4.

For τ in $\overline{\mathbf{K}}$, we further denote by $\mathsf{C}(\tau)$ the following three properties.

$\mathsf{C}_1(\tau)$. For $k=1,\ldots,m$, $\deg_{\boldsymbol{X}}(b_k)=\deg_{\boldsymbol{X}}(b_{\tau,k})$ (where $\deg_{\boldsymbol{X}}$ denotes the degree in $\boldsymbol{X}$).

$\mathsf{C}_2(\tau)$. The only common solution to $b^H_{\tau,1}(\tau,\boldsymbol{X})=\cdots=b^H_{\tau,m}(\tau,\boldsymbol{X})=0$ is $(0,\ldots,0)\in\overline{\mathbf{K}}^n$, where for $k=1,\ldots,m$, $b^H_{\tau,k}$ is the polynomial in $\overline{\mathbf{K}}[X_0,\boldsymbol{X}]$ obtained by homogenizing $b_{\tau,k}$ using a new variable X_0. In particular, $V(\boldsymbol{B}_\tau)\subset\overline{\mathbf{K}}^n$ is finite.

$\mathsf{C}_3(\tau)$. The ideal $\langle\boldsymbol{B}_\tau\rangle$ is radical in $\overline{\mathbf{K}}[\boldsymbol{X}]$.

The first result in this section is the following.

Proposition 8. *Suppose that assumptions B_1 and B_2 hold. Then, there exists an integer c such that for all τ in $\overline{\mathbf{K}}$, the sum of the multiplicities of the isolated solutions of $\boldsymbol{B}_\tau$ is at most c, and is equal to c if $\mathsf{C}(\tau)$ holds.*

We next give our algorithms for

- computing the isolated solutions of the polynomial system $\boldsymbol{C} = (c_1, \ldots, c_m)$;
- computing the simple solutions of the polynomial system $\boldsymbol{C}$.

In order to control the cost of the algorithm, we introduce the following assumptions.

D_1. We are given τ in $\mathbf{K}$ such that $\mathsf{C}(\tau)$ holds; without loss of generality, we assume that $\tau = 0$. We also suppose that we know a description of $V(\boldsymbol{B}_0)$ by means of a zero-dimensional parametrization $\mathscr{R}_0 = ((w_0, v_{0,1}, \ldots, v_{0,n}), \lambda)$ with coefficients in $\mathbf{K}$. The linear form λ needs to satisfy some genericity requirements, that are described in Subsection 3.2.

D_2. We know an integer e such that the union of the one-dimensional components of $V(J)$ in $\overline{\mathbf{K}}^{n+1}$ has degree at most e (further, we prove that $e \geq c$ in Lemma 19).

D_3. We can compute $\boldsymbol{B}$ using a straight-line program of length σ.

Then, the second main result in this section is the following.

Proposition 9. *Assume that* $\mathsf{D}_1, \mathsf{D}_2$ *and* D_3 *hold. Letting* c *be as in Proposition 8. There exists a probabilistic algorithm which computes a zero-dimensional parametrization of the isolated points of* $V(\boldsymbol{C})$ *using*

$$O^{\sim}(c^5 m n^2 + c(e + c^5 n)(\sigma + n^3)) \subset (e\,\sigma\,m)^{O(1)}$$

operations in $\mathbf{K}$.

The variant below focuses on the computation of simple isolated points. We reuse the notations introduced above.

Proposition 10. *Under the assumptions of Proposition 9, there exists a probabilistic algorithm which computes a zero-dimensional parametrization of the simple isolated points of* $V(\boldsymbol{C})$ *using*

$$O^{\sim}(m\,n^2 c^2 + n\,(m\sigma + n^2)\,c\,e) \subset (e\,\sigma\,m)^{O(1)}$$

operations in $\mathbf{K}$.

Remark 11. *These algorithms rely on the choice of a* generic $\mathbf{K}$*-linear form. This form is used in the returned rational parametrization and must satisfy some properties which are described further (see Subsection 3.2). When the chosen form does not fulfill these requirements, either the algorithm fails or the output parametrization encodes a subset of the simple isolated* $V(\boldsymbol{C})$.

3.1 Proof of Proposition 8

This subsection is devoted to prove Proposition 8. In the course of the proof, we will give a precise characterization of the integer c mentioned in the proposition, although the statement given in the proposition will actually be enough for our further purposes. *In all the rest of this subsection, we assume that* B_1 *and* B_2 *hold.*

Consider an irredundant primary decomposition of the ideal $J = \langle \boldsymbol{B} \rangle$ in $\overline{\mathbf{K}}[T, \boldsymbol{X}]$, of the form $J = Q_1 \cap \cdots \cap Q_r$, and let $P_1, \ldots, P_r$ be the associated primes, that is, the respective radicals of $Q_1, \ldots, Q_r$. We assume that $P_1, \ldots, P_s$ are the minimal primes, for some $s \leq r$, so that $V(P_1), \ldots, V(P_s)$ are the (absolutely) irreducible components of $V(J) \subset \overline{\mathbf{K}}^{n+1}$. By B_1, these irreducible components all have dimension at least one. Refining further, we assume that $t \leq s$ is 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 Zariski dense in $\overline{\mathbf{K}}$.

Lemma 12. *Let* τ *be in* $\overline{\mathbf{K}}$ *and let* $\boldsymbol{x} \in \overline{\mathbf{K}}^n$ *be an isolated solution of the system* $\boldsymbol{B}_\tau$*. Then,* $(\tau, \boldsymbol{x})$ *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 $(\tau, \boldsymbol{x})$ cancels $\boldsymbol{B}$, it belongs at least to one of $V(P_1), \ldots, V(P_r)$. It remains to rule out the possibility that $(\tau, \boldsymbol{x})$ 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 $\boldsymbol{x}$ is isolated in $V(\boldsymbol{B}_\tau)$, $(\tau, \boldsymbol{x})$ is isolated in $V(\boldsymbol{B}) \cap V(T - \tau)$, 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 $(\tau, \boldsymbol{x})$ 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 $(\tau, \boldsymbol{x})$ 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 $\{(\tau, \boldsymbol{x})\}$). For the same reason, if $(\tau, \boldsymbol{x})$ belonged to another $V(P_i)$, for some $i > s+1$, $V(P_i)$ would also be zero-dimensional, and thus equal to $\{(\tau, \boldsymbol{x})\}$; 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, $(\tau, \boldsymbol{x})$ 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 $u \geq 1$), and avoids all other associated primes. Let us localize the decomposition $J = Q_1 \cap \cdots \cap Q_r$ at P_{s+1}. By [2, Proposition 4.9], $J_{P_{s+1}} = Q_{1P_{s+1}} \cap \cdots \cap Q_{uP_{s+1}} \cap Q_{s+1P_{s+1}}$ is an irredundant primary decomposition of $J_{P_{s+1}}$ in $\overline{\mathbf{K}}[T, \boldsymbol{X}]_{P_{s+1}}$; the minimal primes are $P_{1P_{s+1}}, \ldots, P_{uP_{s+1}}$.

By Corollary 4 p.24 in [41], for any prime $P_{iP_{s+1}}$, $i = 1, \ldots, u$ or $i = s+1$, the localization of $\overline{\mathbf{K}}[T, \boldsymbol{X}]_{P_{s+1}}$ at $P_{iP_{s+1}}$ is equal to $\overline{\mathbf{K}}[T, \boldsymbol{X}]_{P_i}$. In particular, the height of $P_{iP_{s+1}}$ in $\overline{\mathbf{K}}[T, \boldsymbol{X}]_{P_{s+1}}$ is equal to that of P_i in $\overline{\mathbf{K}}[T, \boldsymbol{X}]_{P_i}$, that is, n if $i = 1, \ldots, u$, since then $V(P_i)$

has dimension 1, or $n+1$ if $i = s+1$. Since $u \geq 1$, this proves that $J_{P_{s+1}}$ has height n. As a result, B_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 $\overline{\mathbf{K}}$, we denote by $J_\tau \subset \overline{\mathbf{K}}[T, \boldsymbol{X}]$ the ideal $J + \langle T - \tau \rangle$, and similarly for J'_τ and J''_τ.

Lemma 13. *Let τ and $\boldsymbol{x}$ be as in Lemma 12. Then, the multiplicities of the ideals J_τ and J'_τ at $(\tau, \boldsymbol{x})$ are the same.*

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

Our goal is now to give a bound on the sum of the multiplicites of $\boldsymbol{B}_\tau$ at all its isolated roots, for any τ in $\overline{\mathbf{K}}$.

To achieve this, we consider the Puiseux series field $\mathbf{S} = \overline{\mathbf{K}}\langle\langle T \rangle\rangle$ in T with coefficients in $\overline{\mathbf{K}}$. Since $\overline{\mathbf{K}}$ is algebraically closed and of characteristic 0, $\mathbf{S}$ is algebraically closed (actually, it is an algebraic closure of $\overline{\mathbf{K}}(T)$) and hence a perfect field.

Next, we consider the extension $\mathfrak{J}$ of J in $\mathbf{S}[\boldsymbol{X}]$, and similarly $\mathfrak{J}'$ and $\mathfrak{J}''$.

Lemma 14. *The ideal $\mathfrak{J}'$ has dimension zero and $V(\mathfrak{J}') \subset \mathbf{S}^n$ is the set of isolated solutions of $V(\mathfrak{J}) \subset \mathbf{S}^n$.*

Proof. From the equality $J = J' \cap J''$ and Corollary 3.4 in [2], 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 $c = \dim_{\mathbf{S}}(\mathbf{S}[\boldsymbol{X}]/\mathfrak{J}')$. Because $\mathbf{S}$ is an algebraic closure of $\overline{\mathbf{K}}(T)$, one has $\dim_{\overline{\mathbf{K}}(T)}(\overline{\mathbf{K}}(T)[\boldsymbol{X}]/\tilde{J}') = c$ where $\tilde{J}'$ is the extension of J' in $\overline{\mathbf{K}}(T)[\boldsymbol{X}]$.

The following lemma relates this quantity to the multiplicities of the solutions in any fiber $\boldsymbol{B}_\tau$. This proves the first statement in Proposition 8.

Lemma 15. *Let τ be in $\overline{\mathbf{K}}$. The sum of the multiplicities of the isolated solutions of $\boldsymbol{B}_\tau$ 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 $(\tau, \boldsymbol{x})$, for $\boldsymbol{x}$ an isolated solution of $\boldsymbol{B}_\tau$. By Lemma 13, this is also the sum of the multiplicities of J'_τ at all $(\tau, \boldsymbol{x})$, for $\boldsymbol{x}$ an isolated solution of $\boldsymbol{B}_\tau$. We prove below that the sum of the multiplicities of J'_τ at all $(\tau, \boldsymbol{x})$, for $\boldsymbol{x}$ such that $(\tau, \boldsymbol{x})$ cancels J'_τ, is at most c; this will be enough to conclude (for any isolated solution $\boldsymbol{x}$ of $\boldsymbol{B}_\tau$, $(\tau, \boldsymbol{x})$ is a root of J'_τ, though

the converse may not be true). Remark that the latter sum is simply the dimension of $\overline{\mathbf{K}}[T, \boldsymbol{X}]/J'_\tau$.

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

Suppose that there exists a linear combination $A_1 m_1 + \cdots + A_k m_k$ in $\mathfrak{J}'$, with all A_i's in $\overline{\mathbf{K}}(T)$, not all of them zero. Thus, we have an equality $a_1/d_1\, m_1 + \cdots + a_k/d_k\, m_k = a/d$, with $a_1, \ldots, a_k$ and $d, d_1, \ldots, d_k$ in $\overline{\mathbf{K}}[T]$ and a in the ideal J'. Clearing denominators, we obtain a relation of the form $e_1 m_1 + \cdots + e_k m_k \in J'$, with not all e_i's zero. Let $(T-\tau)^r$ be the highest power of $T - \tau$ that divides all e_i's (this is well-defined, since not all e_i's vanish) so that we can rewrite the above as $(T-\tau)^r(f_1 m_1 + \cdots + f_k m_k) \in J'$, with $f_i = e_i/(T-\tau)^r \in \overline{\mathbf{K}}[T]$ for all i. In particular, our definition of e_i implies that the values $f_i(\tau)$ 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 $(T-\tau)^r(f_1 m_1 + \cdots + f_k m_k) \in J'$ implies that either $f_1 m_1 + \cdots + f_k m_k$ or some power $(T-\tau)^{rs}$, for some $s > 0$, is in Q_i. Since Q_i does not contain non-zero polynomials in $\overline{\mathbf{K}}[T]$, $f_1 m_1 + \cdots + f_k m_k$ belongs to all Q_i's, that is, to J'. We can then evaluate this relation at $T = \tau$. We saw that the values $f_i(\tau)$ do not all vanish on the left, which is a contradiction with the independence of the monomials $m_1, \ldots, m_k$ modulo J'_τ. □

We now take τ in $\overline{\mathbf{K}}$ and we discuss the geometry of $V(J)$ near τ; without loss of generality, we suppose that $\tau = 0$. We already emphasized that the field $\mathbf{S}$ is an algebraic closure of $\overline{\mathbf{K}}(T)$; we thus let $\Phi_1, \ldots, \Phi_{c'}$ be the points of $V(\mathfrak{J}')$, with coordinates taken in $\mathbf{S}$. In particular, we see that $c' \leq c$; we prove below that if $\mathsf{C}(0)$ holds, we actually have $c' = c$ (that is, that $\mathfrak{J}'$ is radical).

Any series φ in $\mathbf{S}$ admits a well-defined *valuation* $\nu(\varphi)$, which is the smallest exponent that appears in its expansion support; the valuation $\nu(\Phi)$, for a vector $\Phi = (\varphi_1, \ldots, \varphi_s)$ with entries in $\mathbf{S}$, 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 $\varphi_i = \lim_0(\Phi_i) \in \overline{\mathbf{K}}^n$ for $i = 1, \ldots, \kappa$.

Lemma 16. *The equality $V(J' + \langle T \rangle) = \{\varphi_i \mid i = 1, \ldots, \kappa\}$ holds.*

Proof. Let $(s_1, \ldots, s_h)$ be generators of the ideal J' in $\overline{\mathbf{K}}[T, \boldsymbol{X}]$; they also generate $\mathfrak{J}'$ in $\overline{\mathbf{K}}(T)[\boldsymbol{X}]$. Then, the polynomials $s_{0,i} = s_i(0, \boldsymbol{X}) \in \overline{\mathbf{K}}[\boldsymbol{X}]$, for $i = 1, \ldots, h$, are such that $J' + \langle T \rangle = \langle T, s_{0,1}, \ldots, s_{0,h} \rangle$. Consider $i \leq \kappa$, and the corresponding vector of series Φ_i. We know that for $j = 1, \ldots, h$, we have $s_j(\Phi_i) = 0$. Since all elements involved have non-negative valuation, we can take the coefficient of degree 0 in T in this equality and deduce $s_{0,j}(\varphi_i) = 0$, as claimed. Hence, each φ_i, for $i \leq \kappa$, is in $V(J' + \langle T \rangle)$.

Conversely, take indeterminates $T_1, \ldots, T_n$, and let $\mathbf{L}$ be the algebraic closure of the field $\overline{\mathbf{K}}(T_1, \ldots, T_n)$; let $\mathcal{C} \subset \mathbf{L}^{n+1}$ be the zero-set of the ideal $J' \cdot \mathbf{L}[T, \boldsymbol{X}]$ and consider the

projection $\mathcal{C} \to \mathbf{L}^2$ defined by $(\tau, x_1, \ldots, x_n) \mapsto (\tau, T_1 x_1 + \cdots + T_n x_n)$. The Zariski closure $\mathcal{S}$ of the image of this mapping is a hypersurface, that is, a plane curve. Since the ideal J' is generated by polynomials with coefficients in $\overline{\mathbf{K}}$, one deduces that $\mathcal{S}$ admits a squarefree defining equation in $\overline{\mathbf{K}}(T_1, \ldots, T_n)[T, T_0]$.

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

Let $\ell \in \overline{\mathbf{K}}[T_1, \ldots, T_n, T]$ be the leading coefficient of C with respect to T_0. Proposition 1 in [53] proves that C/ℓ, seen in $\overline{\mathbf{K}}(T_1, \ldots, T_n, T)[T_0] \subset \mathbf{L}(T)[T_0]$, is the minimal polynomial of $T_1 X_1 + \cdots + T_n X_n$ in $\mathbf{L}(T)[\boldsymbol{X}]/\sqrt{J'} \cdot \mathbf{L}(T)[\boldsymbol{X}]$. The latter ideal is also the extension of $\sqrt{\mathfrak{J}'}$ to $\mathbf{L}(T)[\boldsymbol{X}]$, so C/ℓ factors as

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

in $\mathbf{L}'[T_0]$ where $\mathbf{L}'$ is the generalized Power series ring in T with coefficients in $\mathbf{L}$. This gives the equality

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

over $\mathbf{S}[T_1, \ldots, T_n, T_0]$.

Let us extend the valuation ν on $\mathbf{S}$ to $\mathbf{S}[T_1, \ldots, T_n, T_0]$ 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 $\overline{\mathbf{K}}[T]$ implies that $\nu(C) = 0$. Using Gauss' Lemma, we see that the valuation of the right-hand side is $\nu(\ell) + \sum_{\kappa < i \le c} \mu_i$, with $\mu_i = \nu(\Phi_i)$ for all i; note that $\mu_i < 0$ for $i > \kappa$. Thus, we can rewrite

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

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

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

where s is in $\overline{\mathbf{K}}[T_1, \ldots, T_n]$; note that $s \neq 0$, since $C(0, T_0)$ is non-zero. By construction of C, for any $\boldsymbol{x} = (x_1, \ldots, x_n)$ in $V(J' + \langle T \rangle)$, $T_1 x_1 + \cdots + T_n x_n$ cancels $C(0, T_0)$, so $\boldsymbol{x}$ must be one of $\varphi_1, \ldots, \varphi_\kappa$. □

To conclude the proof of Proposition 8, we now assume that property $\mathsf{C}(0)$ holds.

Lemma 17. *$\Phi_1, \ldots, \Phi_{c'}$ are bounded; equivalently, $\kappa = c'$.*

Proof. Since we want to prove that $\Phi_1, \ldots, \Phi_{c'}$ are bounded, one can assume that they are all non-zero.

For $i = 1, \ldots, c'$, write $\Phi_i = 1/T^{e_i}(\Psi_{i,1}, \ldots, \Psi_{i,n})$, for a vector $(\Psi_{i,1}, \ldots, \Psi_{i,n})$ of generalized power 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 non-zero. Hence, $e_i = -\nu(\Phi_i)$, and we have to prove that $e_i \leq 0$. By way of contradiction, we assume that $e_i > 0$.

The series Φ_i cancels $b_1, \ldots, b_m$. For $k = 1, \ldots, m$, let $b_k^H \in \overline{\mathbf{K}}[T][X_0, \boldsymbol{X}]$ be the homogenization of b_k with respect to $\boldsymbol{X}$. From the equality $b_k^H(T^{e_i}, \Psi_{i,1}, \ldots, \Psi_{i,n}) = T^{e_i} b_k(\Phi_i)$, we deduce that $b_k^H(T^{e_i}, \Psi_{i,1}, \ldots, \Psi_{i,n}) = 0$ for all k. We can write $b_k = b_{0,k} + T\tilde{b}_k$, for some polynomial $\tilde{b}_k$ in $\overline{\mathbf{K}}[T, \boldsymbol{X}]$, and $\mathsf{C}_1(0)$ implies that $\deg_{\boldsymbol{X}}(\tilde{b}_k) \leq \deg_{\boldsymbol{X}}(b_{0,k})$. As a result, the homogenizations (with respect to $\boldsymbol{X}$) of $b_k, b_{0,k}$ and $\tilde{b}_k$ satisfy a relation of the form $b_k^H = b_{0,k}^H + X_0^{\delta_k} T\tilde{b}_k^H$, for some $\delta_k \geq 0$. This implies the equality

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

The second term has positive valuation, so that $b_{0,k}^H(T^{e_i}, \Psi_{i,1}, \ldots, \Psi_{i,n})$ has positive valuation as well. Taking the coefficient of T^0, this means that $b_{0,k}^H(0, \psi_{i,1}, \ldots, \psi_{i,n}) = 0$ (since $e_i > 0$), which implies that $(\psi_{i,1}, \ldots, \psi_{i,n}) = (0, \ldots, 0)$, in view of $\mathsf{C}_2(0)$. This however contradicts the definition of $(\psi_{i,1}, \ldots, \psi_{i,n})$. □

Lemma 18. *The ideal $\mathfrak{J}'$ is radical; equivalently, $c' = c$.*

Proof. We know that $\mathfrak{J}'$ has dimension zero (Lemma 14), so it is enough to prove that for $i = 1, \ldots, c'$, the localization of $\mathbf{S}[\boldsymbol{X}]/\mathfrak{J}'$ at the maximal ideal $\mathfrak{m}_{\Phi_i}$ is a field, or equivalently that the localization of $\mathbf{S}[\boldsymbol{X}]/\mathfrak{J}$ at $\mathfrak{m}_{\Phi_i}$ is a field. Recall that $\mathbf{S}$ is algebraically closed, hence a perfect field. By the Jacobian criterion [21, Theorem 16.19.b], this is the case if and only if the Jacobian matrix of $\boldsymbol{B}$ with respect to $\boldsymbol{X}$ has full rank n at Φ_i. We know that $\varphi_i = \lim_0(\Phi_i)$ is a root of $\boldsymbol{B}_0$ (Lemma 16), and the Jacobian criterion conversely implies that since the ideal $\langle \boldsymbol{B}_0 \rangle$ is radical (by assumption $\mathsf{C}_3(0)$) and zero-dimensional (by assumption $\mathsf{C}_2(0)$), the Jacobian matrix of $\boldsymbol{B}_0(\boldsymbol{X}) = \boldsymbol{B}(0, \boldsymbol{X})$ has full rank n at φ_i. Since this matrix is the limit at zero of the Jacobian matrix of $\boldsymbol{B}$ with respect to $\boldsymbol{X}$, 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 8, we have to establish that $V(\boldsymbol{B}_0)$ consists of exactly c solutions. First, since $V(\boldsymbol{B}_0)$ is finite, Lemma 12 implies that $\boldsymbol{x}$ is in $V(\boldsymbol{B}_0)$ if and only if $(0, \boldsymbol{x})$ is in $V(J' + \langle T \rangle)$. Next, remark that the two previous lemma taken together imply that $c = \kappa$; thus, in view of Lemma 16, to conclude, it is enough to 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 $\boldsymbol{B}_0$ has full rank n at φ_i; up to reindexing, we assume that rows $1, \ldots, n$ correspond to a maximal non-zero minor. Let $\boldsymbol{B}' = (b_1, \ldots, b_n)$.

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

$$\boldsymbol{B}'(\Phi_i) = \boldsymbol{B}'(f) + \mathrm{jac}_f(\boldsymbol{B}', \boldsymbol{X})T^z\delta_i + T^{2z}r_i = 0$$

and

$$\boldsymbol{B}'(\Phi_{i'}) = \boldsymbol{B}'(f) + \mathrm{jac}_f(\boldsymbol{B}', \boldsymbol{X})T^z\delta_{i'} + T^{2z}r_{i'} = 0,$$

for some vectors of bounded series $r_i, r_{i'}$. By subtraction and division by T^z, we obtain $\mathrm{jac}_f(\boldsymbol{B}', \boldsymbol{X})(\delta_i - \delta_{i'}) = T^z r$, for some vector of bounded series r. Since $\mathrm{jac}_f(\boldsymbol{B}', \boldsymbol{X})$ is invertible, this further gives $\delta_i - \delta_{i'} = T^z r'$, where again r' is a vector of bounded series. However, by construction the left-hand side has valuation zero, while the right-hand side has positive valuation (since $z > 0$). Hence, we derived a contradiction to our assumption that $\varphi_i = \varphi_{i'}$. The proof of Proposition 8 is complete. (Although we do not need it now, the linearization used above also implies that all Φ_i are actually power series.)

We end this section with the proof that $e \geq c$.

Lemma 19. *Under the above notations and assumptions, the inequality $e \geq c$ holds.*

Proof. By definition of the integer e and the ideal J' previously defined, e is greater than or equal to the degree of $V(J')$ which is an algebraic curve.

The degree of this curve is greater than or equal to the cardinality of any fiber $V(J')_\tau$; in particular, we have

$$\sharp V(J')_0 \leq \deg(V(J')) \leq e.$$

Besides, Proposition 8 establishes that the number of isolated points of $V(\boldsymbol{B})_0$ equals c (because the ideal generated by $\langle \boldsymbol{B}, T\rangle$ is radical, multiplicities are equal to 1). By Lemma 12, all these points lie in $V(J')_0$ which allows us to deduce $c \leq e$. □

3.2 Proofs of Propositions 9 and 10

Let $\mathscr{R}_0 = ((w_0, v_{0,1}, \ldots, v_{0,n}), \lambda)$ be a zero-dimensional parametrization of $V(\boldsymbol{B}_0)$ obtained by means of assumption D_1, with q_0 and all $v_{0,j}$ in $\mathbf{K}[Y]$. Note that the degree of w_0 is the integer c.

Decomposing $\mathscr{R}_0$. We start by decomposing $\mathscr{R}_0$ into finitely many zero-dimensional parametrizations $\mathscr{R}_{0,j} = ((w_{0,j}, v_{0,j,1}, \ldots, v_{0,j,n}), \lambda)_{1\leq j\leq t}$, all with coefficients in $\mathbf{K}$, such that for j in $\{1, \ldots, t\}$, there exist $\boldsymbol{i}_j = (i_{j,1}, \ldots, i_{j,n})$ such that the Jacobian matrix of $(b_{0,i})_{i\in\boldsymbol{i}_j}$ has full rank n at $\boldsymbol{x}$, for all $\boldsymbol{x}$ in $Z(\mathscr{R}_{0,j})$.

If w_0 were irreducible, we would simply evaluate the Jacobian matrix of $\boldsymbol{B}_0$ at the point $(v_{0,1}/w_0', \ldots, v_{0,n}/w_0')$, which has coordinates in the field $\mathbf{L} = \mathbf{K}[Y]/\langle w_0\rangle$, and find a non-zero minor of size n in this matrix. It takes $O(n\sigma)$ oeprations in $\mathbf{L}$ to compute this Jacobian matrix, and $O(mn^2)$ operations in $\mathbf{L}$ to find an invertible minor, e.g. using Gaussian elimination. The total time, under the assumption that w_0 is irreducible, is thus $O(mn^2 + n\sigma)$ operations in $\mathbf{L}$, that is, $O\tilde{}((mn^2 + n\sigma)c)$ operations in $\mathbf{K}$.

When w_0 is not irreducible, $\mathbf{L} = \mathbf{K}[Y]/\langle w_0\rangle$ is a product of fields. We can still apply the same process as in the irreducible case; if the algorithm goes through, we have obtained our answer. In general, one workaround would be to factor w_0, but we do not want our runtime to depend on the cost of factoring polynomials (else our analysis would depend on the bit

size of the data when $\mathbf{K} = \mathbb{Q}$). Hence, we will use *dynamic evaluation techniques*, as in [19]. Indeed, the only issue that may arise is that we attempt to invert a zero-divisor. If this is the case, it means we have found a non-trivial factor r_0 of w_0: we can then replace $\mathscr{R}_0$ by two new zero-dimensional parametrizations, $\mathscr{R}'_0 = ((r_0, (v_{0,1}/s_0) \bmod r_0, \dots, (v_{0,n}/s_0) \bmod r_0), \lambda)$ and $\mathscr{R}''_0 = ((s_0, (v_{0,1}/r_0) \bmod s_0, \dots, (v_{0,n}/r_0) \bmod s_0), \lambda)$, with $s_0 = w_0/r_0$, that define a partition of $Z(\mathscr{R}_0)$ into the subsets $Z(\mathscr{R}'_0)$ and $Z(\mathscr{R}''_0)$ where r_0 vanishes, resp. is non-zero.

We can then start over again, from $\mathscr{R}'_0$ and $\mathscr{R}''_0$ independently. Overall, in the worst case, this splitting process induces a extra factor $O(c)$ in the runtime compared to the case where w_0 is irreducible, for a total of $O^{\sim}((mn^2 + n\sigma)c^2)$ operations in $\mathbf{K}$.

Lifting power series and rational reconstruction. For $j = 1, \dots, t$, we can then apply Newton iteration to the system $(b_i)_{i \in \boldsymbol{i}_j}$ to lift $\mathscr{R}_{0,j} = ((w_{0,j}, v_{0,j,1}, \dots, v_{0,j,n}), \lambda)$ into a zero-dimensional parametrization $\mathscr{R}_j = ((w_j, v_{j,1}, \dots, v_{j,n}), \lambda)$ with coefficients in $\mathbf{K}[[T]]/\langle T^{2e} \rangle$, for e as in D_2. Note that $c \leq e$: we saw in the last paragraphs of the previous subsection that c is the cardinality of $V(J' + \langle T \rangle)$, so that $c \leq \deg(V(J'))$, and the latter quantity is at most e.

As explained in [50, Section 2.2], using the algorithm of [28], this can be done using $O^{\sim}(c\,e(\sigma+n^2)n)$ operations in $\mathbf{K}$. Using the Chinese Remainder Theorem, we can combine all $\mathscr{R}_j$ into a single zero-dimensional parametrization $\mathscr{R}$ with coefficients in $\mathbf{K}[[T]]/\langle T^{2e} \rangle$, since for $j \neq j'$ $w_{0,j}$ and $w_{0,j'}$ generate the unit ideal in $\mathbf{K}[[T]]/\langle T^{2e} \rangle$; this takes time $O^{\sim}(c\,e\,n)$.

Using the notation of the previous subsection, the zeros of $\mathscr{R}$ in $\overline{\mathbf{K}}[[T]]/\langle T^{2e} \rangle$ are the truncations of the power series roots $\Phi_1, \dots, \Phi_c$ of $\mathfrak{J}'$. Since $V(J')$ has degree at most e, knowing $\mathscr{R}$ at precision $2e$ allows us to reconstruct a zero-dimensional parametrization $\mathscr{S}$ with coefficients in $\mathbf{K}(\tau)$ such that $Z(\mathscr{S}) = V(\mathfrak{J}')$, with all coefficients having numerator and denominator of degree at most e [53, Theorem 1]. This is done by applying rational function reconstruction to all coefficients of $\mathscr{R}$, as in [53], and takes time $O^{\sim}(c\,e\,n)$.

All in all, the total cost of this step is $O^{\sim}(c\,e(\sigma + n^2)n)$.

A finite set containing the isolated points of $V(\boldsymbol{C})$. As we did in the previous subsection for $T = 0$, we let $\Phi'_1, \dots, \Phi'_c$ be the roots of $\mathfrak{J}'$ in the field of generalized power series in T' with coefficients in $\overline{\mathbf{K}}$ at $T = 1$, with $T' = T - 1$. Without loss of generality, we assume that $\Phi'_1, \dots, \Phi'_{\kappa'}$ are bounded, and $\Phi'_{\kappa'+1}, \dots, \Phi'_c$ are not, for some κ' in $\{0, \dots, c\}$, and we define $\varphi'_1, \dots, \varphi'_{\kappa'}$ by $\varphi'_i = \lim_0(\Phi'_i) \in \overline{\mathbf{K}}^n$ for $i = 1, \dots, \kappa'$. By Lemma 16, $V(J' + \langle T - 1 \rangle) = \{\varphi'_i \mid i = 1, \dots, \kappa'\}$.

We can now specify our requirements on the linear form λ. Following [47] and [50], we ask that λ is a *well-separating element*, that is:

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

Applying Lemma 14 in [50, Section 3], these conditions are satisfied for a generic choice of λ. When this is the case, Lemma 4.4 in [47] shows how to recover a zero-dimensional parametrization $\mathscr{R}_1 = ((w_1, v_{1,1}, \ldots, v_{1,n}), \lambda)$ with coefficients in $\mathbf{K}$ for the limit set $V(J' + \langle T - 1 \rangle) = \{\varphi'_i \mid i = 1, \ldots, \kappa'\}$ starting from the previously computed rational parametrization $\mathscr{S}$, in time $O\tilde{}(c\,e\,n)$.

When the chosen form is not generic enough, the algorithm may fail or it will output a parametrization of a subset of the zero-dimensional set we aim to compute. We refer to [50, Remark 14] for a discussion on probabilistic aspects.

Cleaning. Finally, summing all the previous costs, one performs

$$O\tilde{}((mn^2 + n\sigma)c^2 + c\,e(\sigma + n^2)n)$$

operations in $\mathbf{K}$ for the first three steps (decomposition of $\mathscr{R}_0$, lifting and rational reconstruction and getting a finite set containing the isolated points of $V(\boldsymbol{C})$).

Lemma 12 implies that for any isolated solution $\boldsymbol{x}$ of $\boldsymbol{C}$, $(1, \boldsymbol{x})$ is in $V(J' + \langle T - 1 \rangle)$, so in a second time, we discard from $V(J' + \langle T - 1 \rangle)$ those points that do not correspond to isolated points of $V(\boldsymbol{C})$. All such points belong to a positive-dimensional component of $V(\boldsymbol{C})$. Hence, when $\mathbf{K}$ has characteristic 0, we can use the algorithm of Section 2. By Proposition 8, we can take c as an upper bound on the multiplicity of isolated solutions of $\boldsymbol{C}$.

Using the same dynamic evaluation techniques as in the first paragraph above, we can use the algorithm of Section 2 as if $Z(\mathscr{R}_1)$ were an irreducible variety, with an overhead $O(c)$. Since the number of splittings is bounded by c also, the total overhead is $O(c^2)$. The runtime deduced from Proposition 4 is

$$O(n^4c^6 + n^2mc^5 + n\sigma c^6)$$

operations in $\mathbf{K}$. Adding all costs seen so far, we prove Proposition 9 . The resulting algorithm, which we simply name Homotopy, is described hereafter.

The only difference to prove Proposition 10 is that we now need to discard from $V(J' + \langle T - 1 \rangle)$ those points at which the Jacobian matrix associated to $\boldsymbol{C}$ is not full rank. Doing that is easier than discarding those points which are not isolated. It suffices to construct a straight-line program evaluating that Jacobian matrix ; this can be done using Baur-Strassen's algorithm [13] which yields a straight-line program of length $\sigma' \in O(m\,\sigma)$ operations in $\mathbf{K}$. Next, one evaluates this matrix as done previously when we were decomposing $\mathscr{R}_0$ and use Gaussian elimination to identify divisors of w_1 that need to be removed. This Gaussian elimnation takes $O\tilde{}((mn^2 + n\sigma')c)$ operations in $\mathbf{K}$ which simplifies to $O\tilde{}(nm(n + \sigma)c)$. The final cleaning step is done using Algorithm Clean of [28] whose cost is dominated by the previous computations.

All in all, the total cost is

$$O\tilde{}((mn^2 + n\sigma)c^2 + c\,e(\sigma + n^2)n + nm(n + \sigma)c) \subset O\tilde{}(nm(n + \sigma)c^2 + c\,e(\sigma + n^2)n)$$

Algorithm 1 Homotopy$(\Gamma, \mathscr{R})$

Input: a straight-line program Γ of length σ that computes $\boldsymbol{B} \in \mathbf{K}[T, \boldsymbol{X}]^m$
a zero-dimensional parametrization $\mathscr{R}$ of the system $\boldsymbol{B}_0$
Output: a zero-dimensional parametrization of the isolated points of $V(\boldsymbol{C})$, with $\boldsymbol{C} = \boldsymbol{B}_1$

1. decompose $\mathscr{R}_0$ into $(\mathscr{R}_{0,j})_{1\le j\le t}$
   cost: $O^{\sim}((mn^2 + n\sigma)c^2)$
2. lift $(\mathscr{R}_{0,j})_{1\le j\le t}$ to $(\mathscr{R}_j)_{1\le j\le t}$ with coefficients in $\mathbf{K}[[T]]/\langle T^{2e}\rangle$
   cost: $O^{\sim}(c\,e(\sigma + n^2)n)$
3. combine $(\mathscr{R}_j)_{1\le j\le t}$ into $\mathscr{R}$ with coefficients in $\mathbf{K}[[T]]/\langle T^{2e}\rangle$
   cost: $O^{\sim}(c\,e\,n)$
4. compute a zero-dimensional parametrization $\mathscr{S}$ with coefficients in $\mathbf{K}(T)$ from $\mathscr{R}$
   cost: $O^{\sim}(c\,e\,n)$
5. deduce a zero-dimensional parametrization $\mathscr{R}_1$ with coefficients in $\mathbf{K}$ from $\mathscr{S}$
   cost: $O^{\sim}(c\,e\,n)$
6. remove from $Z(\mathscr{R}_1)$ points that are not isolated in $V(\boldsymbol{C})$
   cost: $O(n^4c^6 + n^2mc^5 + n\sigma c^6)$

operations in $\mathbf{K}$. Taking into account the inequality $e \ge c$ (Lemma 19) this simplifies to

$$O^{\sim}(mn^2c^2 + c\,e(m\sigma + n^2)n)$$

which ends to prove Proposition 10. In the sequel, the resulting algorithm is called Homotopy_simple. It differs from algorithm Homotopy at Step 6 where the cleaning step we just described replaces the one of Homotopy.

4 Properties of determinantal ideals

The following sections will show how to apply the algorithm of the previous section to Problems 1 (resp. 2), by applying Proposition 9 (resp. Proposition 10) to suitable deformations of our input systems. This proposition requires several assumptions to hold: some (noted B_1 and B_2; see Section 3) are related to the deformed system as a whole, while the others (C_1 to C_3) involve properties at the starting point of the homotopy ($T = 0$). In this section, we prove that a large variety of systems satisfy B_1 and B_2.

Let T and $\boldsymbol{X} = (X_1, \ldots, X_n)$ be variables, let J be an ideal in $\overline{\mathbf{K}}[T, \boldsymbol{X}]$, and let us recall properties B_1 and B_2:

B_1. Any irreducible component of $V(J) \subset \overline{\mathbf{K}}^{n+1}$ has dimension at least one.

B_2. For any maximal ideal $\mathfrak{m} \subset \overline{\mathbf{K}}[T, \boldsymbol{X}]$, if the localization $J_{\mathfrak{m}} \subset \overline{\mathbf{K}}[T, \boldsymbol{X}]_{\mathfrak{m}}$ has height n, then it is unmixed (that is, all associated primes have height n).

We pointed out in the previous section that when J is generated by n polynomials, the fact that these properties hold is well-known. To study the case of maximal minors of a polynomial matrix, we will use the following results, taken from [20, Section 6]. Let R be a Cohen-Macaulay ring and let I be the ideal generated by all p-minors of a $p \times q$ matrix $F \in R^{p\times q}$, with $p \leq q$. Then:

- if $I \neq R$, then the height of I is at most $q - p + 1$;
- if I has height $q-p+1$, then I is unmixed (all associated primes have height $q-p+1$).

Let then $G = (g_1, \ldots, g_s)$ be polynomials in $\mathbf{K}[T, \boldsymbol{X}]$, with $s \leq n$, and let F be a polynomial matrix in $\mathbf{K}[T, \boldsymbol{X}]^{p\times q}$, with $p \leq q$. We define $J = I_p(F) + \langle g_1, \ldots, g_s\rangle$, that is J is the ideal in $\overline{\mathbf{K}}[T, \boldsymbol{X}]$ generated by all p-minors of F, together with the polynomials G.

Proposition 20. *If $n = q - p + s + 1$, the ideal J satisfies B_1 and B_2.*

The proof occupies the rest of this section. Let $\boldsymbol{B} = M_p(F)$, the set of all p-minors of F, and let $V_1, \ldots, V_s$ be the $\overline{\mathbf{K}}$-irreducible components of $V(I) \subset \overline{\mathbf{K}}^n$. We prove in the next paragraph that $\dim(V_i) \geq (n+1) - (q-p+1)$ holds for all i. Of course, we can assume that $V(I) \neq \emptyset$, so that $I \neq \mathbf{K}[T, \boldsymbol{X}]$, otherwise the proposition itself would be vacuously true.

First, remark that for a point $\boldsymbol{x}$ in $V(I) \subset \overline{\mathbf{K}}^{n+1}$, and writing $\mathfrak{m} \subset \overline{\mathbf{K}}[T, \boldsymbol{X}]$ for the maximal ideal at $\boldsymbol{x}$, the height of $I_\mathfrak{m}$ in $\overline{\mathbf{K}}[T, \boldsymbol{X}]_\mathfrak{m}$ is equal to $(n + 1) - \max\{\dim(V_i) \mid 1 \leq i \leq s, \boldsymbol{x} \in V_i\}$. For $i = 1, \ldots, s$, let then $\boldsymbol{x}_i$ be a point in V_i that does not belong to any other $V_{i'}$, $i' \neq i$, and let $\mathfrak{m}_i$ be the corresponding maximal ideal; then, the previous equality becomes $\text{height}(I_{\mathfrak{m}_i}) = (n + 1) - \dim(V_i)$. Applying the first item mentioned above in $\overline{\mathbf{K}}[T, \boldsymbol{X}]_{\mathfrak{m}_i}$ (which is Cohen-Macaulay), we deduce that $(n+1) - \dim(V_i) \leq q-p+1$, that is, $\dim(V_i) \geq (n + 1) - (q - p + 1)$.

Notice that we can rewrite $(n+1)-(q-p+1)$ as $s+1$. Since G consists of s polynomials, all irreducible components of $V(J)$ must have dimension at least 1, by Krull's theorem; property B_1 follows.

We next prove B_2. Let $J_\mathfrak{m} = Q_1 \cap \cdots \cap Q_t$ be an irredundant primary decomposition of $J_\mathfrak{m}$ in $\overline{\mathbf{K}}[T, \boldsymbol{X}]_\mathfrak{m}$, and let $P_1, \ldots, P_t$ be the corresponding primes; we assume that the height of $J_\mathfrak{m}$ is n, and our goal is to prove that all P_i's have height n.

Of course, we can restrict to an ideal $\mathfrak{m}$ containing J; $\mathfrak{m}$ is then the maximal ideal at a point $\boldsymbol{x} \in \overline{\mathbf{K}}^{n+1}$ that belongs to $V(J)$. The height of the localization $J_\mathfrak{m} \subset \overline{\mathbf{K}}[T, \boldsymbol{X}]_\mathfrak{m}$ can be rewritten as $(n + 1) - \dim(V_{\boldsymbol{x}})$, where $V_{\boldsymbol{x}}$ is the union of the irreducible components of $V(J)$ passing through $\boldsymbol{x}$. Our assumption in B_2 is that the height of $J_\mathfrak{m}$ is n, that is, that $\dim(V_{\boldsymbol{x}}) = 1$. Thus, every irreducible component of $V(J)$ containing $\boldsymbol{x}$ has dimension 1.

Let W be an irreducible component of $V(\boldsymbol{B})$ containing $\boldsymbol{x}$. We claim that $\dim(W) = s+1$. Indeed, we mentioned in the first paragraph that $\dim(W) \geq s + 1$. If $\dim(W) > s + 1$, then by Krull's theorem, every irreducible component of $W \cap V(G)$ has dimension greater than 1; since $W \cap V(G)$ is a subset of $V(J)$ and contains $\boldsymbol{x}$, we have reached a contradiction. Now, the fact that $\dim(W) = s + 1$ for any irreducible component of $V(\boldsymbol{B})$ containing $\boldsymbol{x}$ means that $\langle \boldsymbol{B}\rangle_\mathfrak{m}$ has height $n - s = q - p + 1$. As a result, [21, Theorem 18.18] shows that $\overline{\mathbf{K}}[T, \boldsymbol{X}]_\mathfrak{m}/\langle \boldsymbol{B}\rangle_\mathfrak{m}$ is Cohen-Macaulay.

For an ideal $I \subset \overline{\mathbf{K}}[T, \boldsymbol{X}]_{\mathfrak{m}}$, we denote by $\bar{I}$ its image modulo $\langle \boldsymbol{B} \rangle_{\mathfrak{m}}$. By the remarks following [58, Theorem IV.5.9], $\bar{Q}_1 \cap \cdots \cap \bar{Q}_t$ is an irredundant primary decomposition of $\bar{J}_{\mathfrak{m}}$ in $\mathbf{K}[T, \boldsymbol{X}]_{\mathfrak{m}}/\langle \boldsymbol{B} \rangle_{\mathfrak{m}}$, with associated primes $\bar{P}_1, \ldots, \bar{P}_t$. In addition, if we let $P_1, \ldots, P_u$ be the minimal primes of $J_{\mathfrak{m}}$, for some $s \leq t$, $\bar{P}_1, \ldots, \bar{P}_u$ are the minimal primes of $\bar{J}_{\mathfrak{m}}$.

Our assumption says that $P_1, \ldots, P_u$ have height n. Because $\overline{\mathbf{K}}[T, \boldsymbol{X}]_{\mathfrak{m}}/\langle \boldsymbol{B} \rangle_{\mathfrak{m}}$ is local and Cohen-Macaulay, for any $i \leq t$, we have

$$\dim(\overline{\mathbf{K}}[T, \boldsymbol{X}]_{\mathfrak{m}}/\langle \boldsymbol{B} \rangle_{\mathfrak{m}}) = \dim((\overline{\mathbf{K}}[T, \boldsymbol{X}]_{\mathfrak{m}}/\langle \boldsymbol{B} \rangle_{\mathfrak{m}})/\bar{P}_i) + \text{height}(\bar{P}_i)$$

by [41, Theorem 17.4(i)]. The factor ring $(\overline{\mathbf{K}}[T, \boldsymbol{X}]_{\mathfrak{m}}/\langle \boldsymbol{B} \rangle_{\mathfrak{m}})/\bar{P}_i$ is simply $\overline{\mathbf{K}}[T, \boldsymbol{X}]_{\mathfrak{m}}/P_i$, so this can be rewritten as

$$s + 1 = \dim(\overline{\mathbf{K}}[T, \boldsymbol{X}]_{\mathfrak{m}}/P_i) + \text{height}(\bar{P}_i).$$

For $i \leq u$, we have $\dim(\overline{\mathbf{K}}[T, \boldsymbol{X}]_{\mathfrak{m}}/P_i) = 1$, so that $\text{height}(\bar{P}_i) = s$; for $i > u$, the height of $\bar{P}_i$ is necessarily $s + 1$. Because $\bar{P}_1, \ldots, \bar{P}_u$ are the minimal primes of $\bar{J}_{\mathfrak{m}}$, the height of $\bar{J}_{\mathfrak{m}}$ is thus s as well.

The ideal $\bar{J}_{\mathfrak{m}}$ is generated in $\overline{\mathbf{K}}[T, \boldsymbol{X}]_{\mathfrak{m}}/\langle \boldsymbol{B} \rangle_{\mathfrak{m}}$ by $G = (g_1, \ldots, g_s)$. Since $\overline{\mathbf{K}}[T, \boldsymbol{X}]_{\mathfrak{m}}/\langle \boldsymbol{B} \rangle_{\mathfrak{m}}$ is Cohen-Macaulay, $\bar{J}_{\mathfrak{m}}$ is unmixed, that is, $u = t$. As a result, $Q_1 \cap \cdots \cap Q_u$ is an irredundant primary decomposition of $J_{\mathfrak{m}}$, and $J_{\mathfrak{m}}$ is unmixed.

5 The column-degree homotopy

We are given a matrix $F = [f_{i,j}] \in \mathbf{K}[X_1, \ldots, X_n]^{p \times q}$ and polynomials $G = (g_1, \ldots, g_s)$ in $\mathbf{K}[X_1, \ldots, X_n]$, with $p \leq q$ and $n = q - p + s + 1$. We want to compute the isolated points (or the simple isolated points) of $V_p(F, G)$, with

$$V_p(F, G) = \{\boldsymbol{x} \in \overline{\mathbf{K}}^n \mid \text{rank}(F(\boldsymbol{x})) < p \text{ and } g_1(\boldsymbol{x}) = \cdots = g_s(\boldsymbol{x}) = 0\}.$$

In this section, we design an algorithm for these both tasks whose cost depends on the column degrees $\delta_1 = \text{cdeg}(F, 1), \ldots, \delta_q = \text{cdeg}(F, q)$; note in particular that with this notation, $\deg(f_{i,j}) \leq \delta_j$ holds for all i, j. We will also write $\gamma_1 = \deg(g_1), \ldots, \gamma_s = \deg(g_s)$.

We point out that (in the case where there are no polynomials G), the construction used in this section was already in the appendix of [45], where it was used to bound the number of solutions of determinantal systems (as we mentioned in the introduction).

Recall that for $k \geq 0$, $E_k(\delta_1, \ldots, \delta_q)$ denotes the elementary symmetric polynomial of degree k in $(\delta_1, \ldots, \delta_q)$.

Proposition 21. *Suppose that the matrix $F \in \mathbf{K}[X_1, \ldots, X_n]^{p \times q}$ and polynomials $G = (g_1, \ldots, g_s)$ in $\mathbf{K}[X_1, \ldots, X_n]$ are given by a straight-line program of length σ. Then, the sum of the multiplicities of the isolated points of $V_p(F, G)$ are at most $c = \gamma_1 \cdots \gamma_s E_{n-s}(\delta_1, \ldots, \delta_q)$.*

Assume that all γ_i's and δ_j's are at least equal to 1, and let $e = (\gamma_1+1) \cdots (\gamma_s+1) E_{n-s}(\delta_1 + 1, \ldots, \delta_q + 1)$, $\gamma = \max(\gamma_1, \ldots, \gamma_s)$ and $\delta = \max(\delta_1, \ldots, \delta_q)$.

There exists a randomized algorithm that computes these isolated points

$$O^{\sim}\left(\binom{q}{p} n^3 c(e+c^5)(\sigma+n^2\gamma+q\delta)\right)$$

operations in $\mathbf{K}$.

The next proposition states a better complexity estimate when one only computes isolated simple points of $V_p(F,G)$.

Proposition 22. *Reusing the notations introduced above, and letting* $\gamma = \max(\gamma_1,\ldots,\gamma_s)$ *and* $\delta = \max(\delta_1,\ldots,\delta_q)$*, there exists a randomized algorithm that computes the simple isolated points of* $V_p(F,G)$ *using*

$$O^{\sim}\left(\binom{q}{p}^2 n^3\, c(c+e(\sigma+\gamma+q\delta))\right)$$

operations in $\mathbf{K}$*,*

These propositions establish the first half of Theorems 1, 2 and 3.

We use the algorithms of Section 3. To match the notation of that section, we let $\boldsymbol{C} = (c_1,\ldots,c_s,\ldots,c_m)$ be polynomials defined as follows: $(c_1,\ldots,c_s) = (g_1,\ldots,g_s)$, and $(c_{s+1},\ldots,c_m)$ are the p-minors of F, so that $m = s + \binom{q}{p}$. Thus, $V_p(F,G)$ is the zero-set of $\boldsymbol{C}$.

Using the degrees $\gamma_1,\ldots,\gamma_s$ and $\delta_1,\ldots,\delta_q$, we construct a polynomial matrix $L \in \mathbf{K}[\boldsymbol{X}]^{p\times q}$, and polynomials $M = (m_1,\ldots,m_s)$ in $\mathbf{K}[\boldsymbol{X}]$, to use as a starting point for the homotopy algorithm. For any $1 \le j \le q$ and $1 \le k \le \delta_j$, let us define

$$\lambda_{j,k} = \lambda_{j,k,0} + \sum_{\ell=1}^{n} \lambda_{j,k,\ell} X_\ell,$$

where all $\lambda_{j,k,\ell}$ are random elements in $\mathbf{K}$. Then, for $j = 1,\ldots,q$, we define

$$\lambda_j = \prod_{k=1}^{\delta_j} \lambda_{j,k},$$

and we let L be the matrix

$$L = \begin{pmatrix} \lambda_1 & 2\lambda_2 & \cdots & q\lambda_q \\ \lambda_1 & 2^2\lambda_2 & \cdots & q^2\lambda_q \\ \vdots & \vdots & & \vdots \\ \lambda_1 & 2^p\lambda_2 & \cdots & q^p\lambda_q \end{pmatrix} \in \mathbf{K}[\boldsymbol{X}]^{p\times q}. \tag{1}$$

For $i = 1, \ldots, s$ and $k = 1, \ldots, \gamma_i$, let us further define

$$\mu_{i,k} = \mu_{i,k,0} + \sum_{\ell=1}^{n} \mu_{i,k,\ell} X_\ell,$$

where all $\mu_{i,k,\ell}$ are random elements in $\mathbf{K}$; then, we let

$$a_i = \prod_{k=1}^{\gamma_i} \mu_{i,k}.$$

We can thus define the system of equations $\boldsymbol{A} = (a_1, \ldots, a_s, \ldots, a_m)$, with a_i as above for $i = 1, \ldots, s$, and where $(a_{s+1}, \ldots, a_m)$ are the p-minors of L (taken in the same order as those in the system $\boldsymbol{C}$).

Let T be a new variable and define the matrix $U = (1 - T) \cdot L + T \cdot F \in \mathbf{K}[T, \boldsymbol{X}]^{p \times q}$. We let $\boldsymbol{B}$ be the polynomials in $\mathbf{K}[T, \boldsymbol{X}]$ given by $\boldsymbol{B} = (b_1, \ldots, b_s, \ldots, b_m)$, where

- $b_i = (1 - T)a_i + T g_i$ for $i = 1, \ldots, s$
- $(b_{s+1}, \ldots, b_m)$ are the p-minors of U, taken in the same order as those in $\boldsymbol{C}$.

We can then define J as the ideal generated by $\boldsymbol{B}$ in $\overline{\mathbf{K}}[T, \boldsymbol{X}]$. Using the notation of Section 3, we see that $\boldsymbol{B}_0 = \boldsymbol{A}$ and $\boldsymbol{B}_1 = \boldsymbol{C}$. Having in mind to apply Proposition 9 (resp. Proposition 10) to compute the isolated points (resp. simple isolated points) of $V(\boldsymbol{C}) = V_p(F, G)$, we now verify that all required assumptions are satisfied.

Properties B_1 and B_2. These follow from Proposition 20.

Property $\mathsf{C}_1(0)$. We have to prove that for $i = 1, \ldots, m$, $\deg_{\boldsymbol{X}}(b_i) = \deg_{\boldsymbol{X}}(a_i)$.

For $i = 1, \ldots, s$, this amounts to proving that $\deg_{\boldsymbol{X}}((1 - T)a_i + T g_i) = \deg_{\boldsymbol{X}}(a_i)$. The latter is by construction equal to γ_i. The former is at most γ_i (since b_i is the sum of two polynomials of degree γ_i in $\boldsymbol{X}$), but since evaluating T at 0 in b_i gives us g_i, its degree in $\boldsymbol{X}$ must be exactly γ_i.

To each index $i = s+1, \ldots, m$ corresponds a sequence $\boldsymbol{j}_i = (j_{i,1}, \ldots, j_{i,p})$ such that b_i and a_i are the minors built with columns indexed by $\boldsymbol{j}_i$ in respectively $U = (1 - T) \cdot L + T \cdot F$ and L. In view of the shape of L, the polynomial a_i is equal to $c_i \lambda_{j_{i,1}} \cdots \lambda_{j_{i,p}}$, with

$$c_i = \begin{vmatrix} j_{i,1} & j_{i,2} & \cdots & j_{i,p} \\ j_{i,1}^2 & j_{i,2}^2 & \cdots & j_{i,p}^2 \\ \vdots & \vdots & & \vdots \\ j_{i,1}^p & j_{i,2}^p & \cdots & j_{i,p}^p \end{vmatrix}.$$

Because $\mathbf{K}$ has characteristic zero, c_i is a non-zero constant, so that a_i has degree $\delta_{j_{i,1}} + \cdots + \delta_{j_{i,p}}$. Since the columns $(j_{i,1}, \ldots, j_{i,p})$ of U have respective degrees at most $(\delta_{j_{i,1}}, \ldots, \delta_{j_{i,p}})$, b_i has degree at most $\delta_{j_{i,1}} + \cdots + \delta_{j_{i,p}}$. However, evaluating T at 0 in b_i gives us back the polynomial a_i, so b_i must have degree exactly $\delta_{j_{i,1}} + \cdots + \delta_{j_{i,p}}$.

Property $\mathsf{C}_2(0)$. We have to prove that the homogenization of the system $\boldsymbol{A}$ has no root at infinity. Thus, let X_0 be a new variable, and let $\boldsymbol{A}^H = (a_1^H, \dots, a_m^H)$ be the homogenization of $\boldsymbol{A}$. For $i = 1, \dots, s$, we have

$$a_i^H = \prod_{k=1}^{\gamma_i} \mu_{i,k}^H \quad \text{with} \quad \mu_{i,k}^H = (\mu_{i,k,0} X_0 + \sum_{\ell=1}^{n} \mu_{i,k,\ell} X_\ell),$$

whereas for $i = s+1, \dots, m$,

$$a_i^H = c_i \lambda_{j_{i,1}}^H \dots \lambda_{j_{i,p}}^H, \qquad \text{for } \boldsymbol{j}_i = (j_{i,1}, \dots, j_{i,p}) \text{ as above,}$$

where for $j = 1, \dots, q$ we set $\lambda_j^H = \prod_{k=1}^{\delta_j} \lambda_{j,k}^H$, with

$$\lambda_{j,k}^H = \lambda_{j,k,0} X_0 + \sum_{\ell=1}^{n} \lambda_{j,k,\ell} X_\ell.$$

To prove $\mathsf{C}_2(0)$, we start by writing down all projective solutions of this system (this will be of use below), before adding the constraint $X_0 = 0$.

Since all a_i^H are products of linear forms, we find the solutions of $\boldsymbol{A}^H$ by setting some of these linear forms to zero. In order to cancel $a_1^H, \dots, a_s^H$, we choose indices $\boldsymbol{u} = (u_1, \dots, u_s)$, with $u_1 \in \{1, \dots, \gamma_1\}$, …, $u_s \in \{1, \dots, \gamma_s\}$, and we consider the equations

$$\mu_{i,u_i}^H = 0, \qquad \text{that is,} \qquad \mu_{i,u_i,0} X_0 + \sum_{\ell=1}^{n} \mu_{i,u_i,\ell} X_\ell = 0,$$

for $i = 1, \dots, s$. In what follows, we fix such an $\boldsymbol{u}$. Then, for a generic choice of coefficients $\mu_{i,k,\ell}$, these equations are equivalent to

$$X_{n-s+1} = \Phi_{n-s+1,\boldsymbol{u}}(X_0, \dots, X_{n-s}), \dots, X_n = \Phi_{n,\boldsymbol{u}}(X_0, \dots, X_{n-s}),$$

for some homogeneous linear forms $\Phi_{n-s+1,\boldsymbol{u}}, \dots, \Phi_{n,\boldsymbol{u}}$. After applying this substitution, for all $j = 1, \dots, q$, λ_j^H can be rewritten as

$$\lambda_{j,\boldsymbol{u}}^H = \prod_{k=1}^{\delta_j} \lambda_{j,k,\boldsymbol{u}}^H,$$

where

$$\lambda_{j,k,\boldsymbol{u}}^H = \lambda_{j,k,0} X_0 + \sum_{\ell=1}^{n-s} \lambda_{j,k,\ell} X_\ell + \sum_{\ell=n-s+1}^{n} \lambda_{j,k,\ell} \Phi_{\ell,\boldsymbol{u}}(X_0, \dots, X_{n-s}).$$

Then, $\boldsymbol{x} = (x_0, \dots, x_n)$ cancels $a_{s+1}^H, \dots, a_m^H$ if and only if $\boldsymbol{x}' = (x_0, \dots, x_{n-s})$ cancels the product $\lambda_{j_1,\boldsymbol{u}}^H \cdots \lambda_{j_p,\boldsymbol{u}}^H$, for any choice of p columns $\boldsymbol{j} = (j_1, \dots, j_p)$.

Lemma 23. *For $\boldsymbol{x}'$ in $\mathbb{P}^{n-s}(\overline{\mathbf{K}})$, the products $\lambda^H_{j_1,\boldsymbol{u}}(\boldsymbol{x}')\cdots\lambda^H_{j_p,\boldsymbol{u}}(\boldsymbol{x}')$ vanish for all choices of columns $\boldsymbol{j}=(j_1,\ldots,j_p)$ if and only if there exists $\{j_1,\ldots,j_{n-s}\}\subset\{1,\ldots,q\}$ such that $\lambda^H_{j_1,\boldsymbol{u}}(\boldsymbol{x}')=\cdots=\lambda^H_{j_{n-s},\boldsymbol{u}}(\boldsymbol{x}')=0$.*

Proof. Take an arbitrary representative $\boldsymbol{x}^*$ of $\boldsymbol{x}'$ in $\overline{\mathbf{K}}^{n+1}$, and consider the polynomial $(1+\lambda^H_{1,\boldsymbol{u}}(\boldsymbol{x}^*)Y_1)\cdots(1+\lambda^H_{q,\boldsymbol{u}}(\boldsymbol{x}^*)Y_q)$, for new variables $Y_1,\ldots,Y_q$. The products $\lambda^H_{j_1,\boldsymbol{u}}(\boldsymbol{x}^*)\cdots\lambda^H_{j_p,\boldsymbol{u}}(\boldsymbol{x}^*)$ are all zero if and only if this polynomial has degree less than p, that is, if and only if $q-p+1=n-s$ terms among $\lambda^H_{1,\boldsymbol{u}}(\boldsymbol{x}^*),\ldots,\lambda^H_{q,\boldsymbol{u}}(\boldsymbol{x}^*)$ vanish. □

For a given $\boldsymbol{u}$ and generic coefficients $\lambda_{j,k,\ell}$ and $\mu_{i,k,\ell}$, the linear forms $\lambda^H_{j,k,\boldsymbol{u}}$ are all pairwise distinct, so the condition of the lemma holds if and only if there exist $\boldsymbol{j}=\{j_1,\ldots,j_{n-s}\}\subset\{1,\ldots,q\}$ and $\boldsymbol{v}=(v_1,\ldots,v_{n-s})$, with v_k in $\{1,\ldots,\delta_k\}$ for all k, such that $\lambda^H_{j_k,v_k,\boldsymbol{u}}(\boldsymbol{x}')=0$ for $k=1,\ldots,n-s$.

This implies that for a fixed $\boldsymbol{u}$, the possible values of $\boldsymbol{x}'=(x_0,\ldots,x_{n-s})\in\mathbb{P}^{n-s}(\overline{\mathbf{K}})$ are determined as solutions of a linear system of size $n-s$. For a generic choice of the coefficients $\lambda_{j,k,\ell}$ and $\mu_{i,k,\ell}$, none of these points satisfies $X_0=0$, so that $\mathsf{C}_2(0)$ holds.

Property $\mathsf{C}_3(0)$. From $\mathsf{C}_2(0)$, we know that the projective variety defined by $\boldsymbol{A}^H$ has no point at infinity, so it is finite; as a result, the affine algebraic set defined by $\boldsymbol{A}$ is finite as well. In addition, all the affine solutions to $\boldsymbol{A}$ are obtained by setting $X_0=1$ in the projective solutions of $\boldsymbol{A}^H$. In other words, they are obtained by choosing indices $\boldsymbol{u}=(u_1,\ldots,u_s)$ with u_k in $\{1,\ldots,\gamma_k\}$ for all k, column indices $\boldsymbol{j}=(j_1,\ldots,j_{n-s})$, and $\boldsymbol{v}=(v_1,\ldots,v_{n-s})$, with v_k in $\{1,\ldots,\delta_k\}$ for all k, solving the affine linear system

$$\lambda_{j_1,v_1,\boldsymbol{u}}(X_1,\ldots,X_{n-s})=\cdots=\lambda_{j_{n-s},v_{n-s},\boldsymbol{u}}(X_1,\ldots,X_{n-s})=0$$

and using the expressions

$$X_{n-s+1}=\phi_{n-s+1,\boldsymbol{u}}(X_1,\ldots,X_{n-s}),\ldots,X_n=\phi_{n,\boldsymbol{u}}(X_1,\ldots,X_{n-s}),$$

where $\phi_{k,\boldsymbol{u}}(X_1,\ldots,X_{n-s})=\Phi_{n-s+1,\boldsymbol{u}}(1,X_1,\ldots,X_{n-s})$ for all k. To prove that the ideal generated by $\boldsymbol{A}$ is radical, we prove that at any point as described above, the Jacobian matrix of $\boldsymbol{A}$ with respect to $X_1,\ldots,X_n$ has full rank.

Let thus $\boldsymbol{u}$, $\boldsymbol{j}$ and $\boldsymbol{v}$ be as above, let $\boldsymbol{x}\in\overline{\mathbf{K}}^n$ be the corresponding point in $V(\boldsymbol{A})$, and consider equations $(a_1,\ldots,a_s)$ first. Each such equation is a product of linear forms such as $a_i=\prod_{k=1}^{\gamma_i}\mu_{i,k}$, with $\mu_{i,u_i}(\boldsymbol{x})=0$. Since the coefficients $\mu_{i,k,\ell}$ are chosen generically, for $i=1,\ldots,s$ and $k\neq u_i$, $\mu_{i,k}(\boldsymbol{x})$ is non-zero; as a result, in the local ring at $\boldsymbol{x}$, the polynomials $(a_1,\ldots,a_s)$ are equal (up to units) to the linear forms $(\mu_{1,u_1},\ldots,\mu_{s,u_s})$.

Next, we consider the p-minors of L; in what follows, we write $\boldsymbol{x}'=(x_1,\ldots,x_{n-s})$. Our starting point is that due to the genericity of the coefficients $\lambda_{j,k,\ell}$, since

$$\lambda_{j_1,v_1,\boldsymbol{u}}=\cdots=\lambda_{j_{n-s},v_{n-s},\boldsymbol{u}}=0$$

only admits $\boldsymbol{x}'$ as a solution, none of the other linear forms $\lambda_{j,k,\boldsymbol{u}}$ vanishes at $\boldsymbol{x}'$. Equivalently, none of the other linear forms $\lambda_{j,k}$ vanishes at $\boldsymbol{x}$.

Recall that $n = q - p + s + 1$, so that $n - s = q - (p-1)$. Hence, there are exactly $p-1$ columns of L not indexed by $\boldsymbol{j} = (j_1, \ldots, j_{n-s})$; call them $\boldsymbol{j'} = (j'_1, \ldots, j'_{p-1})$. We can then consider the products

$$\lambda_{j_1}\lambda_{j'_1}\cdots\lambda_{j'_{p-1}}, \ldots, \lambda_{j_{n-s}}\lambda_{j'_1}\cdots\lambda_{j'_{p-1}};$$

each of them (up to a non-zero constant) is a p-minor of L, so they appear as elements in the sequence $(a_{s+1}, \ldots, a_m)$, say as $(a_{e_1}, \ldots, a_{e_{n-s}})$. By the remark of the previous paragraph, in the local ring at $\boldsymbol{x}$, up to non-zero constants, these polynomials are respectively equal to the linear forms $\lambda_{j_1,v_1}, \ldots, \lambda_{j_{n-s},v_{n-s}}$.

To summarize, we have found that the linear equations $(\mu_{1,u_1}, \ldots, \mu_{s,u_s})$ and $(\lambda_{j_1,v_1}, \ldots, \lambda_{j_{n-s},v_{n-s}})$ belong to the ideal $\langle \boldsymbol{A} \rangle_{\mathfrak{m}}$, where $\mathfrak{m}$ is the maximal ideal at $\boldsymbol{x}$. As a result, the Jacobian matrix of $\boldsymbol{A}$ must be invertible at $\boldsymbol{x}$, and $\mathsf{C}_3(0)$ holds.

At this stage, we have established all assumptions necessary to apply Proposition 8. Since $\boldsymbol{B}$ satisfies $\mathsf{B}_1, \mathsf{B}_2$ and $\boldsymbol{A} = \boldsymbol{B}_0$ satisfies $\mathsf{C}_1, \mathsf{C}_2, \mathsf{C}_3$, we deduce that the sum of the multiplicities of the isolated solutions of $\boldsymbol{C} = \boldsymbol{B}_1$ is at most c, where c is the number of solutions of $\boldsymbol{A}$.

Lemma 24. *Under the above assumptions,* $c = \gamma_1 \cdots \gamma_s E_{n-s}(\delta_1, \ldots, \delta_q)$.

Proof. To estimate c, note first that there are $\gamma_1 \cdots \gamma_s$ choices of $\boldsymbol{u}$. For each choice of $\boldsymbol{u}$, there are $E_{n-s}(\delta_1, \ldots, \delta_q)$ ways to choose $\boldsymbol{j}$ and $\boldsymbol{v}$, where E_{n-s} denotes the elementary symmetric polynomials of degree $n - s$. □

This proves the first part of Proposition 21. We can now inspect assumptions $\mathsf{D}_1, \ldots, \mathsf{D}_4$, which are needed to apply the algorithm of Proposition 9. For the cost analysis below, as in Theorem 2, we assume that all γ_i's and δ_j's are at least equal to 1.

Property D_1. We know that $\mathsf{C}_1(0), \mathsf{C}_2(0), \mathsf{C}_3(0)$ hold, so we are going to compute a zero-dimensional parametrization of $V(\boldsymbol{A})$. We do this by following the description of the solutions of $\boldsymbol{A}$ given in the previous paragraph: for any choice of indices $\boldsymbol{u}$, $\boldsymbol{j}$ and $\boldsymbol{v}$ as above, the corresponding point $\boldsymbol{x} \in \overline{\mathbf{K}}^n$ in $V(\boldsymbol{A})$ can be found by solving the linear system of size n given by $(\mu_{1,u_1}, \ldots, \mu_{s,u_s})$ and $(\lambda_{j_1,v_1}, \ldots, \lambda_{j_{n-s},v_{n-s}})$, so in time $O(n^3)$. We repeat this procedure c times, using a total of $O(cn^3)$ operations in $\mathbf{K}$.

Knowing all the points in $V(\boldsymbol{A})$, we can construct a zero-dimensional parametrization $\mathscr{R}_0$ such that $Z(\mathscr{R}_0) = V(\boldsymbol{A})$ in time $O\tilde{}(cn)$ by means of fast interpolation [24, Chapter 10]. (Note that for practical purposes, we may modify the algorithm of Proposition 9 to take into account the fact that all points in $V(\boldsymbol{A})$ are in $\mathbf{K}^n$.)

Hence the total cost here is in $O(c\,n^3)$ operations in $\mathbf{K}$..

Property D_2. Next, we need to determine an upper bound e on the degree of the curve $V(J')$, where J' is the union of the one-dimensional irreducible components of $V(\boldsymbol{B}) \subset \overline{\mathbf{K}}^{n+1}$ whose projection on the T-axis is dense.

Lemma 25. *Under the above assumptions and notation, e is bounded above by* $(\gamma_1 + 1) \cdots (\gamma_s + 1) E_{n-s}(\delta_1 + 1, \ldots, \delta_q + 1)$.

Proof. Let us write $V(\boldsymbol{B}) = V(J') \cup V' \cup V''$, where V'' is the union of the other components of dimension one of $V(\boldsymbol{B})$ and V'' is the union of the components of higher dimension (by B_1, $V(\boldsymbol{B})$ has no isolated point), and let H be a generic hyperplane in coordinates $T, X_1, \ldots, X_n$. Then, $(V(J') \cup V') \cap V(H)$ is a finite set consisting of $\deg(V(J')) + \deg(V')$ points, whereas $V'' \cap V(H)$ consits only on components of positive dimension; these two sets are disjoint. Thus, we can take for e the number of isolated points of $V(\boldsymbol{B}) \cap V(H)$.

The hyperplane H is defined by an equation $h_0 + h_1 X_1 + \cdots + h_n X_n + h_{n+1} T = 0$. This equation allows us to rewrite T as $\eta(X_1, \ldots, X_n) = -(h_0 + h_1 X_1 + \cdots + h_n X_n)/h_{n+1}$; the points in $V(\boldsymbol{B}) \cap V(H)$ are thus in one-to-one correspondence with the solutions of the system $(\beta_1, \ldots, \beta_s, \beta_{s+1}, \ldots, \beta_m)$, where $\beta_i = (1-\eta)a_i + \eta g_i$, for $i = 1, \ldots, s$, and $\beta_{s+1}, \ldots, \beta_m$ are the p-minors of the matrix $\nu = (1-\eta)\, L + \eta\, F$. Now, the polynomials $(\beta_1, \ldots, \beta_s)$ have respective degrees at most $(\gamma_1 + 1), \ldots, (\gamma_s + 1)$, and the column degrees of ν are $\delta_1 + 1, \ldots, \delta_q + 1$.

We can then apply Proposition 8, which shows we can take for e the integer $(\gamma_1 + 1) \cdots (\gamma_s + 1) E_{n-s}(\delta_1 + 1, \ldots, \delta_q + 1)$. □

Property D_3. Finally, we need to give an estimate on the size of a straight-line program that computes the polynomials $\boldsymbol{B} = (b_1, \ldots, b_m)$, assuming that we are given a straight-line program Γ of size σ that computes polynomials $G = (g_1, \ldots, g_s)$ and the entries of F.

First, we estimate the complexity of computing the polynomials $(b_1, \ldots, b_s)$. For $i \leq s$, the ith polynomial b_i is equal to $(1 - T)a_i + T g_i$, where a_i is a product of γ_i linear forms in n variables. This polynomial can be computed in $O(n\gamma_i)$ operations in $\mathbf{K}$, hence for a total of $O(n(\gamma_1 + \cdots + \gamma_s))$ operations for $(a_1, \ldots, a_s)$, and $O(\sigma + n(\gamma_1 + \cdots + \gamma_s))$ for $(b_1, \ldots, b_s)$.

The polynomials $(b_{s+1}, \ldots, b_m)$ are the p-minors of $U = (1-T) \cdot L + T \cdot F$. The polynomials $\lambda_1, \ldots, \lambda_q$ can be computed in $O(n(\delta_1 + \cdots + \delta_q))$ operations, so that the entries of U can be computed in $O(\sigma + n(\delta_1 + \cdots + \delta_q))$ operations. From that, all p-minors of U can be deduced in $O(\binom{q}{p} n^3)$ further steps. To summarize, all polynomials in $\boldsymbol{B}$ can be computed by a straight-line program Γ' of size $\sigma' = O(\sigma + \binom{q}{p} n^3 + n(\gamma_1 + \cdots + \gamma_s + \delta_1 + \cdots + \delta_q))$.

Completing the cost analysis. We can then apply Proposition 9, whose runtime is $O^{\sim}(c^5 m n^2 + c(e + c^5 n)(\sigma' + n^3))$ operations in $\mathbf{K}$; since $m \leq n + \binom{q}{p}$, this can be simplified as

$$O^{\sim}\left(c(e + c^5 n)\left(\sigma + \binom{q}{p} n^3 + n(\gamma_1 + \cdots + \gamma_s + \delta_1 + \cdots + \delta_q)\right)\right).$$

Since $s \leq n$, $\gamma = \max(\gamma_1, \ldots, \gamma_s)$ and $\delta = \max(\delta_1, \ldots, \delta_q)$, our bound becomes $O^{\sim}\left(c(e + c^5 n)(\sigma + \binom{q}{p} n^3 + n^2 \gamma + q\delta)\right)$. This can also be rewritten as $O^{\sim}\left(c(e + c^5)(\sigma + \binom{q}{p} n^3 + n^2 \gamma + q\delta)\right)$, by means of a case discussion between e and $c^5 n$. If $c^5 n \leq e$, then $e + c^5 n$ is in $O(e)$. Else, we have $e \leq c^5 n$; since $e \geq 2^n$, this implies that $c \geq 2^n / n$, so that n is in $O(\log(c))$, and $e + c^5 n$ is in $O^{\sim}(c^5)$. At last, further simplification shows that the obtained bound can be simplified to

$$O^{\sim}\left(\binom{q}{p} n^3 c(e + c^5)(\sigma + n^2 \gamma + q\delta)\right)$$

which ends the proof of Proposition 21.

The resulting algorithm, called ColumnDegree is described below.

Algorithm 2 ColumnDegree(Γ)

Input: a straight-line program Γ of length σ that computes

- $F \in \mathbf{K}[X_1, \ldots, X_n]^{p \times q}$ with $\deg(f_{i,j}) \leq \delta_j$ for all j and $p \leq q$
- polynomials $G = (g_1, \ldots, g_s)$ in $\mathbf{K}[X_1, \ldots, X_n]$, with $n = q - p + s + 1$

Output: a zero-dimensional parametrization of the isolated points of $V_p(F, G)$

1. for any sequence $\boldsymbol{u} = (u_1, \ldots, u_s)$, with $u_j \in \{1, \ldots, \gamma_j\}$ for all j
   (a) for any subsequence $\boldsymbol{j} = (j_1, \ldots, j_{n-s})$ of $(1, \ldots, q)$
      i. for any sequence $\boldsymbol{v} = (v_1, \ldots, v_{n-s})$, with v_k in $\{1, \ldots, \delta_k\}$ for all k
         A. let $\mathscr{R}_{\boldsymbol{i},\boldsymbol{j},\boldsymbol{v}}$ a zero-dimensional parametrization of the solution of the system

$$\mu_{1,u_1} = \cdots = \mu_{s,u_s} = \lambda_{j_1,v_1} = \cdots = \lambda_{j_{n-s},v_{n-s}} = 0$$

cost: $O(cn^3)$, with $c = \gamma_1 \cdots \gamma_s E_{n-s}(\delta_1, \ldots, \delta_q)$

2. combine all $(\mathscr{R}_{\boldsymbol{u},\boldsymbol{j},\boldsymbol{v}})_{\boldsymbol{u},\boldsymbol{j},\boldsymbol{v}}$ into a zero-dimensional parametrization $\mathscr{R}$ cost: $O^{\sim}(cn)$
3. construct a straight-line program Γ' that computes all polynomials $\boldsymbol{B}$

length of Γ' is $\sigma' = O(\sigma + \binom{q}{p} n^3 + n(\alpha_1 + \cdots + \alpha_p) + n(\gamma_1 + \cdots + \gamma_s))$

4. return Homotopy($\Gamma', \mathscr{R}$)

cost: $O^{\sim}(c(e + c^5)(\sigma + cn^4))$, with $e = (\gamma_1 + 1) \cdots (\gamma_s + 1) E_{n-s}(\delta_1 + 1, \ldots, \delta_q + 1)$

Finally, to prove Proposition 22, we rely on the algorithm, called ColumnDegree_simple differs from ColumnDegree_simple only at the last step where Algorithm Homotopy_simple is called instead. Hence, one applies Proposition 10 yields a runtime $O^{\sim}(m\, n^2 c^2 + n\,(m\sigma' + n^2)\, c\, e)$ operations in $\mathbf{K}$. Using similar simplifications as above, we obtain as a bound

$$O^{\sim}\left(\binom{q}{p} n^3\, c^2 + n^2 \binom{q}{p}^2 n^2\, c\, e(\sigma + n + \gamma + q\delta)\right)$$

which we simplify as

$$O^{\sim}\left(\binom{q}{p}^2 n^3\, c(c + e(\sigma + \gamma + q\delta))\right)$$

This concludes the proof of Proposition 22.

6 Preliminaries for the row-degree homotopy

In this section, we work with two families of matrices of size $p \times q$, with $p \leq q$, and with entries that are polynomials in $n = q - p + 1$ variables; we prove several properties that will be used in our row-degree homotopy algorithm. Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ be positive integers. The matrices we consider are

$$M^H = \begin{pmatrix} \lambda^H_{1,1} & \lambda^H_{1,2} & \cdots & \lambda^H_{1,q} \\ \lambda^H_{2,1} & \lambda^H_{2,2} & \cdots & \lambda^H_{2,q} \\ \vdots & & & \vdots \\ \lambda^H_{p,1} & \lambda^H_{p,2} & \cdots & \lambda^H_{p,q} \end{pmatrix}, \tag{2}$$

and matrices of a more specialized kind of the form

$$N^H = \begin{pmatrix} \lambda^H_{1,1} & 0 & \cdots & 0 & \lambda^H_{1,p+1} & \cdots & \lambda^H_{1,q} \\ 0 & \lambda^H_{2,2} & \cdots & 0 & \lambda^H_{2,p+1} & \cdots & \lambda^H_{2,q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda^H_{p,p} & \lambda^H_{p,p+1} & \cdots & \lambda^H_{p,q} \end{pmatrix}, \tag{3}$$

where the ^{H} superscript indicates that all entries are homogenous. In both cases, for all i, j, the entry $\lambda^H_{i,j}$ is a product of α_i homogeneous linear forms in $n+1$ variables $X_0, \ldots, X_n$ with coefficients in $\mathbf{K}$ (except when $\lambda^H_{i,j}$ is explicitly set to zero in the second case), that is, $\lambda^H_{i,j} = \prod_{k=1}^{\alpha_i} \lambda^H_{i,j,k}$.

We are interested in describing the projective algebraic sets defined in $\mathbb{P}^n(\overline{\mathbf{K}})$ by the p-minors of N^H and M^H (note that these minors are all homogeous). In the rest of this section, if A^H is a matrix with polynomial entries that are homogeneous in $X_0, \ldots, X_n$, we use the notation $V_t(A^H)$ to denote the projective set defined by its t-minors in $\mathbb{P}^n(\overline{\mathbf{K}})$, for any $t \geq 1$ (we use the same notation for affine algebraic sets in those cases when the entries of our matrices are polynomials in $X_1, \ldots, X_n$; this should cause no confusion).

Proposition 26. *For generic choices of the coefficients of the linear forms $\lambda^H_{i,j,k}$, the following holds:*

- *the projective algebraic sets $V_p(M^H)$ and $V_p(N^H)$ have no solution at infinity (that is, with $X_0 = 0$);*
- *the Jacobian matrices of $I_p(M^H)$ and $I_p(N^H)$ with respect to $(X_0, \ldots, X_n)$ have rank n at every point of the above sets.*

The bulk of this section is devoted to prove this proposition. Our strategy is to work all along with linear forms with indeterminate coefficients, and establish the properties we want in this context. Explicitly, we prove below properties called $\mathsf{J}_2(\boldsymbol{\alpha}, q), \mathsf{K}_2(\boldsymbol{\alpha}, q)$ and $\mathsf{J}_4(\boldsymbol{\alpha}, q), \mathsf{K}_4(\boldsymbol{\alpha}, q)$, which establish the proposition. In what follows, for any ring R and any matrix $M \in R^{p \times q}$, if S is a subsequence of $(1, \ldots, p)$ and T a subsequence of $(1, \ldots, q)$, $M_{S,T}$

is the submatrix of M obtained by keeping rows indexed by S and columns indexed by T. We also call this the (S,T)-submatrix of M.

Let thus $\mathcal{A} = q(n+1)(\alpha_1 + \cdots + \alpha_p)$; this is the number of coefficients needed to define homogeneous linear forms $\lambda^H_{i,j,k}$ in $X_0, \ldots, X_n$, for $i = 1, \ldots, p$, $j = 1, \ldots, q$ and $k = 1, \ldots, \alpha_i$. If needed, we will write $\mathcal{A} = \mathcal{A}(\boldsymbol{\alpha}, q)$ to make the dependency in $\boldsymbol{\alpha}$ and q explicit. Let then $\mathfrak{L}$ be the sequence of $\mathcal{A}$ indeterminates $\mathfrak{L} = (\mathfrak{l}_{i,j,k,r})$, for i, j, k as above and $r = 0, \ldots, n$, and define

$$\mathfrak{l}^H_{i,j,k} = \mathfrak{l}_{i,j,k,0}X_0 + \mathfrak{l}_{i,j,k,1}X_1 + \cdots + \mathfrak{l}_{i,j,k,n}X_n,$$

as well as

$$\mathfrak{l}^H_{i,j} = \mathfrak{l}^H_{i,j,1} \cdots \mathfrak{l}^H_{i,j,\alpha_i} \in \mathbf{K}[\mathfrak{L}][\tilde{\boldsymbol{X}}],$$

with $\tilde{\boldsymbol{X}} = (X_0, X_1, \ldots, X_n)$. We can then define the matrix

$$\mathfrak{M}^H_{\boldsymbol{\alpha},q} = \begin{bmatrix} \mathfrak{l}^H_{1,1} & \cdots & \mathfrak{l}^H_{1,q} \\ \vdots & & \vdots \\ \mathfrak{l}^H_{p,1} & \cdots & \mathfrak{l}^H_{p,q} \end{bmatrix} \in \mathbf{K}[\mathfrak{L}][\tilde{\boldsymbol{X}}]^{p \times q}. \tag{4}$$

Remark that for all i, j, the (i,j)-th entry of $\mathfrak{M}^H_{\boldsymbol{\alpha},q}$ has degree α_i in $\tilde{\boldsymbol{X}}$; this matrix is thus the "generic" model of the matrix M^H seen previously.

Given $\Lambda = (\lambda_{i,j,k,r}) \in \overline{\mathbf{K}}^{\mathcal{A}}$, for any polynomial $\mathfrak{F}$ in $\mathbf{K}(\mathfrak{L})[\tilde{\boldsymbol{X}}]$, we write $\mathfrak{F}(\Lambda, \tilde{\boldsymbol{X}})$ for the polynomial obtained by evaluating $\mathfrak{l}_{i,j,k,r}$ at $\lambda_{i,j,k,r}$, for all indices i, j, k, r as above, as long as no denominator vanishes through this evaluation; the notation extends to polynomial matrices. More generally, for a field $\mathbf{L}$ containing $\mathbf{K}$, and Λ in $\mathbf{L}^{\mathcal{A}}$, the notation $\mathfrak{F}(\Lambda, \tilde{\boldsymbol{X}})$ is defined similarly.

Let next $\mathcal{A}' = n(n+1)(\alpha_1 + \cdots + \alpha_p)$; as above, we will write $\mathcal{A}' = \mathcal{A}'(\boldsymbol{\alpha}, q)$ when needed. Let $\mathfrak{L}' \subset \mathfrak{L}$ be the sequence of $\mathcal{A}'$ indeterminates $\mathfrak{L}' = (\mathfrak{l}_{i,j,k,r})$, for indices i, j, k, r as follows: i is in $\{1, \ldots, p\}$, j is in $\{i, p+1, \ldots, q\}$, and as previously, k is in $\{1, \ldots, \alpha_i\}$ and r is in $\{0, \ldots, n\}$. Remark that the polynomials $\mathfrak{l}^H_{i,j}$, for i, j as above, are in $\mathbf{K}[\mathfrak{L}'][\tilde{\boldsymbol{X}}] \subset \mathbf{K}[\mathfrak{L}][\tilde{\boldsymbol{X}}]$, and allow us to define

$$\mathfrak{N}^H_{\boldsymbol{\alpha},q} = \begin{bmatrix} \mathfrak{l}^H_{1,1} & 0 & 0 & \mathfrak{l}^H_{1,p+1} & \cdots & \mathfrak{l}^H_{1,q} \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \mathfrak{l}^H_{p,p} & \mathfrak{l}^H_{p,p+1} & \cdots & \mathfrak{l}^H_{p,q} \end{bmatrix} \in \mathbf{K}[\mathfrak{L}'][\tilde{\boldsymbol{X}}]^{p \times q}. \tag{5}$$

For $\Lambda' \in \overline{\mathbf{K}}^{\mathcal{A}'}$ and $\mathfrak{F}$ in $\mathbf{K}(\mathfrak{L}')[\tilde{\boldsymbol{X}}]$, the notation $\mathfrak{F}(\Lambda', \tilde{\boldsymbol{X}})$ is defined as in the case of polynomials over $\mathbf{K}(\mathfrak{L})$ described previously.

6.1 Setting up the recurrences

The basic idea behind the proofs below is the following: to prove that a property such as rank-deficiency holds for a matrix $\mathfrak{M}^H_{\boldsymbol{\alpha},q}$, we prove that it holds for a matrix of the form $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$, and use an openness property. To prove that property for the latter matrices, we proceed by

induction, relying on the presence of the left-hand diagonal block. Indeed, for a matrix such as $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ to be rank-deficient at $\tilde{\boldsymbol{x}} \in \mathbb{P}^n(\overline{\mathbf{K}(\mathfrak{L}')})$, at least one of $\mathfrak{l}^H_{1,1}, \dots, \mathfrak{l}^H_{p,p}$ must vanish at $\tilde{\boldsymbol{x}}$.

Suppose for instance that $\mathfrak{l}^H_{1,1}(\tilde{\boldsymbol{x}}) = \mathfrak{l}^H_{2,2}(\tilde{\boldsymbol{x}}) = 0$, while all other terms are non-zero. Then, the $((1,2),(p+1,\dots,q))$-submatrix of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}(\tilde{\boldsymbol{x}})$ itself must be rank-deficient. The constraints $\mathfrak{l}^H_{1,1}(\tilde{\boldsymbol{x}}) = \mathfrak{l}^H_{2,2}(\tilde{\boldsymbol{x}}) = 0$ give us two linear equations, which allow us to eliminate two coordinates of $\tilde{\boldsymbol{x}}$, say X_{n-1} and X_n. We can perform the corresponding substitution in the above submatrix, and we are left with a matrix of size $2 \times (n-1)$ that is of the form $\mathfrak{M}^H_{(\alpha_1,\alpha_2),n-1}(\mathfrak{H},(X_0,\dots,X_{n-2}))$, with entries depending on $X_0,\dots,X_{n-2}$, for some vector of coefficients $\mathfrak{H}$ obtained through the elimination of X_{n-1} and X_n. We can then invoke our induction assumption on the latter matrix.

To formalize this process, for a subsequence $\boldsymbol{i} = (i_1,\dots,i_\kappa)$ of $(1,\dots,p)$, we call the $(\boldsymbol{i},(p+1,\dots,q))$-submatrix of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ the submatrix of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ *associated* to $\boldsymbol{i}$; it consists of the rows of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ indexed by $\boldsymbol{i}$ and columns $p+1,\dots,q$. For such an $\boldsymbol{i}$, we let $R_{\boldsymbol{i}}$ be the set of all tuples $\boldsymbol{r} = (r_1,\dots,r_\kappa)$, with r_1 in $\{1,\dots,\alpha_{i_1}\}$, …, r_κ in $\{1,\dots,\alpha_{i_\kappa}\}$; for any k in $\{1,\dots,\kappa\}$, r_k will be the index of the factor $\mathfrak{l}^H_{i_k,i_k,r_k}$ of $\mathfrak{l}^H_{i_k,i_k}$ we cancel. For given $\boldsymbol{i}$ and $\boldsymbol{r}$, we will let $\mathfrak{L}'_{\boldsymbol{i},\boldsymbol{r}} \subset \mathfrak{L}'$ be the indeterminates corresponding to the coefficients of $\mathfrak{l}^H_{i_1,i_1,r_1},\dots,\mathfrak{l}^H_{i_\kappa,i_\kappa,r_\kappa}$, and of all entries $\mathfrak{l}^H_{i_1,p+1},\dots,\mathfrak{l}^H_{i_\kappa,q}$ of the submatrix associated to $\boldsymbol{i}$ in $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$.

By Gaussian elimination, we can rewrite the homogeneous linear equations $\mathfrak{l}^H_{i_1,i_1,r_1} = \dots = \mathfrak{l}^H_{i_\kappa,i_\kappa,r_\kappa} = 0$ as

$$X_{n-\kappa+1} = \mathfrak{f}_{n-\kappa+1,\boldsymbol{i},\boldsymbol{r}}(X_0,\dots,X_{n-\kappa}),\dots,X_n = \mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(X_0,\dots,X_{n-\kappa}), \tag{6}$$

for some homogeneous linear forms $\mathfrak{f}_{n-\kappa+1,\boldsymbol{i},\boldsymbol{r}},\dots,\mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}$ of $(X_0,\dots,X_{n-\kappa})$ with coefficients in $\mathbf{K}(\mathfrak{L}'_{\boldsymbol{i},\boldsymbol{r}})$. Applying this substitution in the entries of the submatrix of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ associated to $\boldsymbol{i}$ gives us the $\kappa \times (n-1)$ matrix $\mathfrak{M}^H_{\boldsymbol{\alpha}_{\boldsymbol{i}},n-1}(\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}},\tilde{\boldsymbol{X}}')$, with $\boldsymbol{\alpha}_{\boldsymbol{i}} = (\alpha_{i_1},\dots,\alpha_{i_\kappa})$, whose entries are products of homogeneous linear forms in $\tilde{\boldsymbol{X}}' = (X_0,\dots,X_{n-\kappa})$, and where $\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}$ is a vector of $\mathcal{A}(\boldsymbol{\alpha}_{\boldsymbol{i}},n-1)$ elements in $\mathbf{K}(\mathfrak{L}'_{\boldsymbol{i},\boldsymbol{r}})$.

The main result we will use in this section is the following lemma, which summarizes how the above process allows us to describe the projective zero-set of t-minors of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$, for any $t \le p$. This will be the basis of several recursions.

Lemma 27. *For t in $\{1,\dots,p\}$, $V_t(\mathfrak{N}^H_{\boldsymbol{\alpha},q}) \subset \mathbb{P}^n(\overline{\mathbf{K}(\mathfrak{L}')})$ is the union of the sets*

$$\left\{(\tilde{\boldsymbol{x}}',\mathfrak{f}_{n-\kappa+1,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{x}}'),\dots,\mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{x}}')) \mid \tilde{\boldsymbol{x}}' \in V_{\kappa-(p-t)}(\mathfrak{M}^H_{\boldsymbol{\alpha}_{\boldsymbol{i}},n-1}(\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}},\tilde{\boldsymbol{X}}')) \subset \mathbb{P}^{n-\kappa}(\overline{\mathbf{K}(\mathfrak{L}')})\right\}, \tag{7}$$

for $\boldsymbol{i} = (i_1,\dots,i_\kappa)$ of length $\kappa \in \{p-t+1,\dots,\min(p,n-1)\}$ and $\boldsymbol{r}$ in $R_{\boldsymbol{i}}$, and with $\tilde{\boldsymbol{X}}' = (X_0,\dots,X_{n-\kappa})$, together with

$$\{(1,\mathfrak{f}_{1,\boldsymbol{i},\boldsymbol{r}}(1),\dots,\mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(1))\}$$

if $t = p$ and $n \le p$, with $\boldsymbol{i} = (i_1,\dots,i_n)$ and $\boldsymbol{r}$ in $R_{\boldsymbol{i}}$.

We have to write a special case for $t = p$ and $n \le p$ in the last part of the lemma, since taking $\boldsymbol{i} = (i_1,\dots,i_n)$ of length $\kappa = n$ in (7) would lead to consider points in $\mathbb{P}^0(\overline{\mathbf{K}(\mathfrak{L}')})$.

Proof. A point $\tilde{\boldsymbol{x}} \in \mathbb{P}^n(\overline{\mathbf{K}(\mathfrak{L}')})$ belongs to $V_t(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$ if and only if some diagonal terms of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ vanish at $\tilde{\boldsymbol{x}}$, say $\mathfrak{l}^H_{i_k,i_k}(\tilde{\boldsymbol{x}}) = 0$ for $k = 1, \dots, \kappa$ (all other $\mathfrak{l}^H_{i,i}(\tilde{\boldsymbol{x}})$ being non-zero), and if the submatrix of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ associated to $\boldsymbol{i} = (i_1, \dots, i_\kappa)$ has rank less than $\kappa - (p-t)$ at $\tilde{\boldsymbol{x}}$. In particular, we must have $\kappa - (p-t) > 0$, that is, $\kappa \geq p - t + 1$.

For $k = 1, \dots, \kappa$, $\mathfrak{l}^H_{i_k,i_k}(\tilde{\boldsymbol{x}}) = 0$ if and only if there exists r_k in $\{1, \dots, \alpha_{i_k}\}$ such that $\mathfrak{l}^H_{i_k,i_k,r_k}(\tilde{\boldsymbol{x}}) = 0$. Thus, $\tilde{\boldsymbol{x}}$ is in $V_t(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$ if and only if there exists a subsequence $\boldsymbol{i} = (i_1, \dots, i_\kappa)$ of $(1, \dots, p)$, with $\kappa \geq p - t + 1$, and $\boldsymbol{r} = (r_1, \dots, r_\kappa)$ in $R_{\boldsymbol{i}}$ such that $\mathfrak{l}^H_{i_1,i_1,r_1}(\tilde{\boldsymbol{x}}) = \cdots = \mathfrak{l}^H_{i_\kappa,i_\kappa,r_\kappa}(\tilde{\boldsymbol{x}}) = 0$ and the submatrix of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ associated to $\boldsymbol{i}$ has rank less than $\kappa - (p-t)$ at $\tilde{\boldsymbol{x}}$.

Applying (6), we deduce that the coordinates $(x_0, \dots, x_n)$ of $\tilde{\boldsymbol{x}}$ satisfy

$$x_{n-\kappa+1} = \mathfrak{f}_{n-\kappa+1,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{x}}'), \dots, x_n = \mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{x}}'),$$

with $\tilde{\boldsymbol{x}}' = (x_0, \dots, x_{n-\kappa})$. In particular, $\kappa \leq n$, since otherwise this linear system would have no solution (recall that the coefficients are algebraically independent indeterminates). Remark also that $\tilde{\boldsymbol{x}}'$ is a well-defined element of $\mathbb{P}^{n-\kappa}(\overline{\mathbf{K}(\mathfrak{L}')})$, that is, it is not identically zero, since otherwise $\tilde{\boldsymbol{x}}$ would vanish as well.

For $\boldsymbol{i} = (i_1, \dots, i_\kappa)$ with $\kappa \leq n-1$, applying the above substitution in the submatrix of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ associated to $\boldsymbol{i}$ (which has size $\kappa \times (n-1)$), the rank condition above becomes that $\mathfrak{M}^H_{\boldsymbol{\alpha}_{\boldsymbol{i}},n-1}(\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}, \tilde{\boldsymbol{X}}')$ has rank less than $\kappa - (p-t)$ at $\tilde{\boldsymbol{x}}'$, that is, $\tilde{\boldsymbol{x}}'$ is in $V_{\kappa-(p-t)}(\mathfrak{M}^H_{\boldsymbol{\alpha}_{\boldsymbol{i}},n-1}(\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}, \tilde{\boldsymbol{X}}'))$. In this case, we are done.

When $\kappa = n$, that is, $\boldsymbol{i} = (i_1, \dots, i_n)$ (this can happen only if $n \leq p$), the linear equations above determine $\tilde{\boldsymbol{x}}$ entirely; setting $x_0 = 1$, we obtain $x_1 = \mathfrak{f}_{1,\boldsymbol{i},\boldsymbol{r}}(1), \dots, x_n = \mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(1)$. In this case, the submatrix of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ associated to $\boldsymbol{i}$ has size $n \times (n-1)$. Using the specialization of the coefficients that sets the off-diagonal entry to 0 and the ith diagonal entries to $X_0^{\alpha_i}$, $i = 1, \dots, n-1$, we see that its evaluation at $\tilde{\boldsymbol{x}}$ has rank $n-1$; as a result $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ has rank $p-1$ at $\tilde{\boldsymbol{x}}$. Thus, we need to take $\kappa = n$ into account only if $t = p$, that is, if we are interested in the maximal minors; in this case, we have to take into account the point $\{(1, \mathfrak{f}_{1,\boldsymbol{i},\boldsymbol{r}}(1), \dots, \mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(1))\}$. □

6.2 Solutions with higher rank defect

We discuss here the case $t = p-1$. We take parameters $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_p)$ and q, with $2 \leq p \leq q$, and we write $\mathcal{A} = \mathcal{A}(\boldsymbol{\alpha}, q)$ and $\mathcal{A}' = \mathcal{A}'(\boldsymbol{\alpha}, q)$; we will establish the following properties.

$\mathsf{J}_1(\boldsymbol{\alpha}, q)$. The projective algebraic set $V_{p-1}(\mathfrak{M}^H_{\boldsymbol{\alpha},q}) \subset \mathbb{P}^n(\overline{\mathbf{K}(\mathfrak{L})})$ is empty.

$\mathsf{K}_1(\boldsymbol{\alpha}, q)$. The projective algebraic set $V_{p-1}(\mathfrak{N}^H_{\boldsymbol{\alpha},q}) \subset \mathbb{P}^n(\overline{\mathbf{K}(\mathfrak{L}')})$ is empty.

The first step of the proof is to establish that for $\boldsymbol{\alpha}$ and q as above, $\mathsf{K}_1(\boldsymbol{\alpha}, q)$ implies $\mathsf{J}_1(\boldsymbol{\alpha}, q)$. Let us thus fix $\boldsymbol{\alpha}$ and q. Assumption $\mathsf{K}_1(\boldsymbol{\alpha}, q)$ implies that $V_{p-1}(\mathfrak{N}^H_{\boldsymbol{\alpha},q}(\Lambda', \tilde{\boldsymbol{X}}))$ is empty for a generic Λ' in $\overline{\mathbf{K}}^{\mathcal{A}'}$. We will prove that $V_{p-1}(\mathfrak{M}^H_{\boldsymbol{\alpha},q}(\Lambda, \tilde{\boldsymbol{X}}))$ is empty for a generic Λ in $\overline{\mathbf{K}}^{\mathcal{A}}$, which in turn establishes $\mathsf{J}_1(\boldsymbol{\alpha}, q)$.

Consider the ideal $I_{p-1}(\mathfrak{M}^H_{\boldsymbol{\alpha},q})$ in the polynomial ring $\mathbf{K}[\mathfrak{L}, \tilde{\boldsymbol{X}}]$ in $\mathcal{A}+n+1$ variables. This ideal defines an algebraic set $Z_{\boldsymbol{\alpha},q}$ in $\overline{\mathbf{K}}^{\mathcal{A}} \times \mathbb{P}^n(\overline{\mathbf{K}})$, and we let $\Delta_{\boldsymbol{\alpha},q} \subset \overline{\mathbf{K}}^{\mathcal{A}}$ be its projection on the first factor: this is the set of all Λ such that $V_{p-1}(\mathfrak{M}^H_{\boldsymbol{\alpha},q}(\Lambda, \tilde{\boldsymbol{X}}))$ is not empty. Because the source is a projective space, $\Delta_{\boldsymbol{\alpha},q}$ is closed (so its complement is open), and we just have to verify that it is not equal to the whole $\overline{\mathbf{K}}^{\mathcal{A}}$. This follows readily from property $\mathsf{K}_1(\boldsymbol{\alpha}, q)$, which proves that generic matrices of the form $\mathfrak{N}^H_{\boldsymbol{\alpha},q}(\Lambda', \tilde{\boldsymbol{X}})$ do not belong to $\Delta_{\boldsymbol{\alpha},q}$, so $\mathsf{J}_1(\boldsymbol{\alpha}, q)$ holds.

We finish the proof by induction. We first take $p = q$ and consider $\mathsf{K}_1(\boldsymbol{\alpha}, q)$. In this case, $n = 1$ and $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ is a diagonal matrix, whose diagonal entries are products of linear forms in (X_0, X_1) with indeterminate coefficients. Hence, no pair of entries $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ have any common solution in $\mathbb{P}^1(\overline{\mathbf{K}(\mathfrak{L}')})$, so the rank of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ is at least $p-1$ at any $\tilde{\boldsymbol{x}} \in \mathbb{P}^1(\overline{\mathbf{K}(\mathfrak{L}')})$. As a result, $\mathsf{K}_1(\boldsymbol{\alpha}, p)$ holds, and so does $\mathsf{J}_1(\boldsymbol{\alpha}, p)$, by the claim in the previous paragraph.

Consider next a pair $(\boldsymbol{\alpha}, q)$, with $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ and $2 \leq p < q$, and suppose that $\mathsf{J}_1(\boldsymbol{\alpha}', q')$ holds for all $(\boldsymbol{\alpha}', q')$ with $\boldsymbol{\alpha}' = (\alpha'_1, \ldots, \alpha'_{p'})$, $2 \leq p' \leq q'$, $p' \leq p$ and $q' < q$; we prove that $\mathsf{K}_1(\boldsymbol{\alpha}, q)$ holds (as above, this will also imply $\mathsf{J}_1(\boldsymbol{\alpha}, q)$).

Take $t = p - 1$ in Lemma 27. Then, the parameters $(\kappa - (p-t), \boldsymbol{\alpha_i}, n-1)$ used in each expression (7) are of the form $(\kappa - 1, \boldsymbol{\alpha_i}, n-1)$, with $2 \leq \kappa \leq \min(p, n-1)$. Since the $\mathcal{A}(\boldsymbol{\alpha_i}, n-1)$ entries of $\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}$ are algebraically independent over $\mathbf{K}$, $\mathbf{K}(\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}})$ is isomorphic to $\mathbf{K}(\lambda_{u,j,k,r})$, for $u = 1, \ldots, \kappa$, $j = 1, \ldots, n-1$, $k = 1, \ldots, \alpha_{i_u}$ and $r = 0, \ldots, n-\kappa$, so that $V_{\kappa-1}(\mathfrak{M}^H_{\boldsymbol{\alpha_i},n-1}(\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}, \tilde{\boldsymbol{X}}'))$ has the same cardinality as $V_{\kappa-1}(\mathfrak{M}^H_{\boldsymbol{\alpha_i},n-1})$. As a result, since $\boldsymbol{\alpha_i}$ has length $\kappa \geq 2$, and since we also have $\kappa \leq n-1$, $\kappa \leq p$ and $n-1 < q$, we can apply the induction hypothesis and deduce that all $V_{\kappa-1}(\mathfrak{M}^H_{\boldsymbol{\alpha_i},n-1}(\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}, \tilde{\boldsymbol{X}}'))$ appearing in Lemma 27 are empty. This in turn implies that $V_{p-1}(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$ is empty, as claimed.

6.3 Solutions at infinity

Next, we focus on the case $t = p$. We take parameters $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ and q, with $1 \leq p \leq q$, and we write $\mathcal{A} = \mathcal{A}(\boldsymbol{\alpha}, q)$ and $\mathcal{A}' = \mathcal{A}'(\boldsymbol{\alpha}, q)$; then, we prove the following properties.

$\mathsf{J}_2(\boldsymbol{\alpha}, q)$. The projective algebraic set $V_p(\mathfrak{M}^H_{\boldsymbol{\alpha},q}) \subset \mathbb{P}^n(\overline{\mathbf{K}(\mathfrak{L})})$ has no point satisfying $X_0 = 0$.

$\mathsf{K}_2(\boldsymbol{\alpha}, q)$. The projective algebraic set $V_p(\mathfrak{N}^H_{\boldsymbol{\alpha},q}) \subset \mathbb{P}^n(\overline{\mathbf{K}(\mathfrak{L}')})$ has no point satisfying $X_0 = 0$.

In particular, this implies that these sets are finite. We will prove these properties as we did in the previous paragraph; the first step is thus to establish that for $\boldsymbol{\alpha}$ and q as above, $\mathsf{K}_2(\boldsymbol{\alpha}, q)$ implies $\mathsf{J}_2(\boldsymbol{\alpha}, q)$.

Let us thus fix $\boldsymbol{\alpha}$ and q, and assume that $\mathsf{K}_2(\boldsymbol{\alpha}, q)$ holds. We prove that $V_p(\mathfrak{M}^H_{\boldsymbol{\alpha},q}(\Lambda, \tilde{\boldsymbol{X}}))$ has no point at infinity for a generic Λ in $\overline{\mathbf{K}}^{\mathcal{A}}$; this will imply $\mathsf{J}_2(\boldsymbol{\alpha}, q)$. Consider the ideal generated by $I_p(\mathfrak{M}^H_{\boldsymbol{\alpha},q})$ and X_0 in the polynomial ring $\mathbf{K}[\mathfrak{L}, \tilde{\boldsymbol{X}}]$ in $\mathcal{A}+n+1$ variables. This ideal defines an algebraic set $Z'_{\boldsymbol{\alpha},q}$ in $\overline{\mathbf{K}}^{\mathcal{A}} \times \mathbb{P}^n(\overline{\mathbf{K}})$, and we let $\Delta'_{\boldsymbol{\alpha},q} \subset \overline{\mathbf{K}}^{\mathcal{A}}$ be its projection on the first factor: this is thus the set of all Λ in $\overline{\mathbf{K}}^{\mathcal{A}}$ such that $V_p(\mathfrak{M}^H_{\boldsymbol{\alpha},q}(\Lambda, \tilde{\boldsymbol{X}}))$ has a point at infinity. Because the source is a projective space, $\Delta'_{\boldsymbol{\alpha},q}$ is closed (so its complement is open), and we just have to verify that it is not equal to the whole $\overline{\mathbf{K}}^{\mathcal{A}}$. This follows from property

$\mathsf{K}_2(\boldsymbol{\alpha}, q)$, which implies that matrices of the form $\mathfrak{N}^H_{\boldsymbol{\alpha},q}(\Lambda', \tilde{\boldsymbol{X}})$, for generic Λ' in $\overline{\mathbf{K}}^{\mathcal{A}'}$, do not belong to $\Delta'_{\boldsymbol{\alpha},q}$.

Again, we finish the proof by induction. We first take $p = q$, and we prove that $\mathsf{K}_2(\boldsymbol{\alpha}, q)$ holds ($\mathsf{J}_2(\boldsymbol{\alpha}, q)$ will follow, by the previous paragraph). In this case, $n = 1$ and $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ is a diagonal matrix, whose diagonal entries are products of homogeneous linear forms in (X_0, X_1) with indeterminate coefficients. Then, $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ has rank less than p at $\tilde{\boldsymbol{x}} \in \mathbb{P}^1(\overline{\mathbf{K}(\mathfrak{L}')})$ if and only if one of the linear factors of some diagonal term vanishes at $\tilde{\boldsymbol{x}}$. None of these linear forms has a projective root at infinity, so we are done.

Consider next a pair $(\boldsymbol{\alpha}, q)$, with $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ and $1 \le p \le q$ and suppose that $\mathsf{J}_2(\boldsymbol{\alpha}', q')$ holds for all $(\boldsymbol{\alpha}', q')$ with $\boldsymbol{\alpha}' = (\alpha'_1, \ldots, \alpha'_{p'})$, $1 \le p' \le q'$, $p' \le p$ and $q' < q$; we prove that $\mathsf{K}_2(\boldsymbol{\alpha}, q)$ holds; as above, this will imply $\mathsf{J}_2(\boldsymbol{\alpha}, q)$.

Take $t = p$ in Lemma 27. We first deal with the last contribution, corresponding to $\boldsymbol{i} = (i_1, \ldots, i_n)$, and thus $\kappa = n$: by design, the corresponding point is not at infinity. For the other contributions, the parameters $(\kappa - (p - t), \boldsymbol{\alpha_i}, n - 1)$ used in (7) are of the form $(\kappa, \boldsymbol{\alpha_i}, n-1)$, with $\boldsymbol{\alpha_i}$ of length $\kappa \in \{1, \ldots, \min(p, n-1)\}$; since all conditions $1 \le \kappa \le n-1$, $\kappa \le p$ and $n - 1 < q$ are satisfied, we can invoke the induction assumption. Since the coefficients $\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}$ are algebraically independent, we deduce that none of the projective sets $V_\kappa(\mathfrak{M}^H_{\boldsymbol{\alpha_i},n-1}(\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}, \tilde{\boldsymbol{X}}'))$ appearing in Lemma 27 has any point with $X_0 = 0$. As a consequence, $V_p(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$ has no point at infinity either, as claimed.

Refining J_1 The following is a strengthening of property J_1 above. That property asserts that for any $\tilde{\boldsymbol{x}}$ in $\mathbb{P}^n(\overline{\mathbf{K}(\mathfrak{L})})$, the $p \times q$ matrix $\mathfrak{M}^H_{\boldsymbol{\alpha},q}(\tilde{\boldsymbol{x}})$ has rank at least $p - 1$, so that there exists a non-zero $(p-1)$-minor in this matrix. We claim that actually, each $(p-1) \times q$ submatrix of $\mathfrak{M}^H_{\boldsymbol{\alpha},q}(\tilde{\boldsymbol{x}})$ has rank $p - 1$.

To rephrase this, consider $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ and q, with $1 \le p \le q$, together with a matrix $\mathfrak{m}^H_{\boldsymbol{\alpha},q}$, built as $\mathfrak{M}^H_{\boldsymbol{\alpha},q}$ before, but using products of homogeneous linear forms in $(n-1)+1 = q-p+1$ variables $X_0, \ldots, X_{n-1}$, instead of $n+1$ variables $X_0, \ldots, X_n$. Such a matrix takes the form

$$\mathfrak{m}^H_{\boldsymbol{\alpha},q} = \begin{bmatrix} \mathfrak{g}^H_{1,1} & \cdots & \mathfrak{g}^H_{1,q} \\ \vdots & & \vdots \\ \mathfrak{g}^H_{p,1} & \cdots & \mathfrak{g}^H_{p,q} \end{bmatrix} \in \mathbf{K}[\mathfrak{G}][X_0, \ldots, X_{n-1}]^{p \times q}, \tag{8}$$

with

$$\mathfrak{g}^H_{i,j,k} = \mathfrak{g}_{i,j,k,0} X_0 + \mathfrak{g}_{i,j,k,1} X_1 + \cdots + \mathfrak{g}_{i,j,k,n-1} X_{n-1},$$

and

$$\mathfrak{g}^H_{i,j} = \mathfrak{g}^H_{i,j,1} \cdots \mathfrak{g}^H_{i,j,\alpha_i} \in \mathbf{K}[\mathfrak{G}][X_0, \ldots, X_{n-1}],$$

where $\mathfrak{G} = (\mathfrak{g}_{i,j,k,\ell})$ are indeterminates, for $i = 1, \ldots, p$, $j = 1, \ldots, q$, $k = 1, \ldots, \alpha_i$ and $\ell = 0, \ldots, n-1$; we let $\mathcal{B} = qn(\alpha_1 + \cdots + \alpha_p)$ be the total number of coefficients $\mathfrak{g}_{i,j,k,\ell}$ involved. In this context, the following property could be proved by induction as in the other cases, but a direct proof is available.

$\mathsf{J}_3(\boldsymbol{\alpha}, q)$. The projective algebraic set $V_p(\mathfrak{m}^H_{\boldsymbol{\alpha},q}) \subset \mathbb{P}^{n-1}(\overline{\mathbf{K}(\mathfrak{G})})$ is empty.

To prove this property, take $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ and q as above. If $q = p$, we have $n = 1$, so the (i, j) entry of $\mathfrak{m}^h_{\boldsymbol{\alpha},q}$ has the form $\mathfrak{g}_{i,j,1,0} \cdots \mathfrak{g}_{i,j,\alpha_i,0} X_0^{\alpha_i}$; hence, the determinant of this matrix is non-zero, and the claim follows.

We can thus suppose $q > p$, so that $q - 1 \geq p$. Then, the $((1, \ldots, p), (1, \ldots, q-1))$-submatrix of $\mathfrak{m}^H_{\boldsymbol{\alpha},q}$ is of the form $\mathfrak{M}^H_{\boldsymbol{\alpha},q-1}$, with entries depending on $\mathcal{A}(\boldsymbol{\alpha}, q-1)$ parameters. Let $(c_i)_{i \in I}$ be the p-minors of $\mathfrak{m}^H_{\boldsymbol{\alpha},q}$ built by taking $p-1$ of the first $q-1$ columns of $\mathfrak{m}^H_{\boldsymbol{\alpha},q}$, together with its last column. Any such minor can be expanded along the last column as $c_i = \mathfrak{g}^H_{1,q} c_{i,1} + \cdots + \mathfrak{g}^H_{p,q} c_{i,p}$, where $\mathfrak{g}^H_{1,q}, \ldots, \mathfrak{g}^H_{p,q}$ are the entries of the last column, and $c_{i,1}, \ldots, c_{i,p}$ are $(p-1)$-minors from $\mathfrak{M}^H_{\boldsymbol{\alpha},q-1}$. Remark that $(c_{i,j})_{i \in I, 1 \leq j \leq p}$ are *all* $(p-1)$-minors of $\mathfrak{M}^H_{\boldsymbol{\alpha},q-1}$ (if $p = 1$, we have $I = \{1\}$ and $c_1 = \mathfrak{g}^H_{1,q}$, with $c_{1,1} = 1$).

By $\mathsf{J}_2(\boldsymbol{\alpha}, q-1)$, we deduce that $V_p(\mathfrak{M}^H_{\boldsymbol{\alpha},q-1}) \subset \mathbb{P}^{n-1}(\overline{\mathbf{K}(\mathfrak{G})})$ is finite. For all other points $\tilde{\boldsymbol{x}}$ in $\mathbb{P}^{n-1}(\overline{\mathbf{K}(\mathfrak{G})})$, $\mathfrak{M}^H_{\boldsymbol{\alpha},q-1}$ has full rank p at $\tilde{\boldsymbol{x}}$, and thus so does $\mathfrak{m}^H_{\boldsymbol{\alpha},q}$. Hence, we can focus on the points in $V_p(\mathfrak{M}^H_{\boldsymbol{\alpha},q-1})$. Consider a point $\tilde{\boldsymbol{x}}$ in this set; in particular, by $\mathsf{J}_2(\boldsymbol{\alpha}, q-1)$, we can take its first coordinate x_0 equal to 1. Using $\mathsf{J}_1(\boldsymbol{\alpha}, q-1)$, together with our remark on the $(p-1)$-minors of $\mathfrak{M}^H_{\boldsymbol{\alpha},q-1}$, we deduce that not all minors $(c_{i,j})_{i \in I, 1 \leq j \leq p}$ vanish at $\tilde{\boldsymbol{x}}$. Suppose thus that $c_{i_0,j_0}(\tilde{\boldsymbol{x}}) \neq 0$; we prove that $c_{i_0}(\tilde{\boldsymbol{x}}) \neq 0$, which is enough to conclude.

Let us split the $\mathcal{B}$ indeterminates $\mathfrak{G}$ into $\mathfrak{G}_1$ and $\mathfrak{G}_2$, where $\mathfrak{G}_1$ has cardinality $\mathcal{B}_1 = \mathcal{A}(\boldsymbol{\alpha}, q-1)$ and corresponds to the coefficients used in the entries $\mathfrak{g}^H_{1,1}, \ldots, \mathfrak{g}^H_{p,q-1}$ in $\mathfrak{M}^H_{\boldsymbol{\alpha},q}$, and $\mathfrak{G}_2$ of cardinality $\mathcal{B}_2 = \mathcal{B} - \mathcal{B}_1$ stands for the coefficients of the entries $\mathfrak{g}^H_{1,q}, \ldots, \mathfrak{g}^H_{p,q}$ in the last column of $\mathfrak{m}^H_{\boldsymbol{\alpha},q}$. Let us further write

$$c_{i_0}(\tilde{\boldsymbol{x}}) = \mathfrak{g}^H_{1,q}(\tilde{\boldsymbol{x}}) c_{i_0,1}(\tilde{\boldsymbol{x}}) + \cdots + \mathfrak{g}^H_{p,q}(\tilde{\boldsymbol{x}}) c_{i_0,p}(\tilde{\boldsymbol{x}}).$$

Since $V_p(\mathfrak{M}^H_{\boldsymbol{\alpha},q-1})$ is finite, the coordinates of $\tilde{\boldsymbol{x}}$ are algebraic over $\mathbf{K}(\mathfrak{G}_1)$. Thus, since $x_0 = 1$, the polynomial $\mathfrak{g}^H_{j_0,q}(\tilde{\boldsymbol{x}}) \in \overline{\mathbf{K}(\mathfrak{G}_1)}[\mathfrak{G}_2]$ admits $\mathfrak{g}_{j_0,q,1,0} \cdots \mathfrak{g}_{j_0,q,\alpha_{j_0},0}$ as a specialization, by setting to zero all coefficients $\mathfrak{g}_{j_0,q,k,\ell}$, for $k = 1, \ldots, \alpha_{j_0}$ and $\ell = 1, \ldots, n-1$ (remark that these coefficients belong to $\mathfrak{G}_2$). For $j \neq j_0$, $\mathfrak{g}^H_{j,q}(\tilde{\boldsymbol{x}}) \in \overline{\mathbf{K}(\mathfrak{G}_1)}[\mathfrak{G}_2]$ admits 0 as a specialization, by setting to zero all coefficients $\mathfrak{g}_{j,q,k,\ell}$, for $k = 1, \ldots, \alpha_j$ and $\ell = 0, \ldots, n-1$ (again, these coefficients belong to $\mathfrak{G}_2$).

The coefficients $c_{i_0,j}(\tilde{\boldsymbol{x}})$ are algebraic over $\mathbf{K}(\mathfrak{G}_1)$, so that $c_{i_0}(\tilde{\boldsymbol{x}})$ is in $\overline{\mathbf{K}(\mathfrak{G}_1)}[\mathfrak{G}_2]$. By the previous discussion, it admits

$$\mathfrak{g}_{j_0,q,1,0} \cdots \mathfrak{g}_{j_0,q,\alpha_{j_0},0} c_{i_0,j_0}(\tilde{\boldsymbol{x}})$$

as a specialization, which is non-zero. Thus, $c_{i_0}(\tilde{\boldsymbol{x}})$ is non-zero, as claimed.

6.4 Multiplicity of the solutions

The following is the last property we prove for matrices $\mathfrak{M}^H_{\boldsymbol{\alpha},q}$ and $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$. Again, we take parameters $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ and q, with $1 \leq p \leq q$, and we write $\mathcal{A} = \mathcal{A}(\boldsymbol{\alpha}, q)$ and $\mathcal{A}' = \mathcal{A}'(\boldsymbol{\alpha}, q)$; we will establish the following.

$\mathsf{J}_4(\boldsymbol{\alpha}, q)$. The Jacobian matrix of the p-minors of $\mathfrak{M}^H_{\boldsymbol{\alpha},q}$ with respect to $\tilde{\boldsymbol{X}} = (X_0, \ldots, X_n)$ has rank n at all points in $V_p(\mathfrak{M}^H_{\boldsymbol{\alpha},q})$.

$\mathsf{K}_4(\boldsymbol{\alpha}, q)$. The Jacobian matrix of the p-minors of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ with respect to $\tilde{\boldsymbol{X}} = (X_0, \dots, X_n)$ has rank n at all points in $V_p(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$.

As for other proofs involving both $\mathfrak{M}^H_{\boldsymbol{\alpha},q}$ and $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$, we first show that $\mathsf{K}_4(\boldsymbol{\alpha}, q)$ implies $\mathsf{J}_4(\boldsymbol{\alpha}, q)$.

We fix $\boldsymbol{\alpha}$ and q, and we assume that $\mathsf{K}_4(\boldsymbol{\alpha}, q)$ holds. Consider the ideal of the polynomial ring $\mathbf{K}[\mathfrak{L}, \tilde{\boldsymbol{X}}]$ in $\mathcal{A} + n + 1$ variables generated by the p-minors of $\mathfrak{M}^H_{\boldsymbol{\alpha},q}$, together with the n-minors of the Jacobian matrix of these equations with respect to $(X_0, \dots, X_n)$. This ideal defines an algebraic set $Z''_{\boldsymbol{\alpha},q}$ in $\overline{\mathbf{K}}^{\mathcal{A}} \times \mathbb{P}^n(\overline{\mathbf{K}})$, and we let $\Delta''_{\boldsymbol{\alpha},q} \subset \overline{\mathbf{K}}^{\mathcal{A}}$ be its projection on the first factor. By construction, for Λ in $\overline{\mathbf{K}}^{\mathcal{A}} - \Delta''_{\boldsymbol{\alpha},q}$, the Jacobian matrix of $M_p(\mathfrak{M}^H_{\boldsymbol{\alpha},q}(\Lambda, \tilde{\boldsymbol{X}}))$ has rank n at any $\tilde{\boldsymbol{x}}$ in $V_p(\mathfrak{M}^H_{\boldsymbol{\alpha},q}(\Lambda, \tilde{\boldsymbol{X}}))$. As before, because the source is a projective space, $\Delta''_{\boldsymbol{\alpha},q}$ is closed (so its complement is open), and we just have to verify that it is not equal to the whole $\overline{\mathbf{K}}^{\mathcal{A}}$. This follows from property $\mathsf{K}_4(\boldsymbol{\alpha}, q)$, which proves that generic matrices of the form $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ do not belong to $\Delta''_{\boldsymbol{\alpha},q}$.

Again, we finish the proof by induction. We first take $p = q$, and we prove that $\mathsf{K}_4(\boldsymbol{\alpha}, q)$ holds ($\mathsf{J}_4(\boldsymbol{\alpha}, q)$ will follow, by the previous paragraph). In this case, $n = 1$ and $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ is a diagonal matrix, whose diagonal entries are products of homogeneous linear forms $\mathfrak{l}^H_{i,i}$ depending on (X_0, X_1) and with indeterminate coefficients. The ideal $I_p(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$ is generated by the product of the terms $\mathfrak{l}^H_{i,i}$, which admits no repeated factors; the conclusion follows.

Consider next a pair $(\boldsymbol{\alpha}, q)$, with $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_p)$ and $1 \le p \le q$ and suppose that $\mathsf{J}_4(\boldsymbol{\alpha}', q')$ holds for all $(\boldsymbol{\alpha}', q')$ with $\boldsymbol{\alpha}' = (\alpha'_1, \dots, \alpha'_{p'})$, $1 \le p' \le q'$, $p' \le p$ and $q' < q$; we prove that $\mathsf{K}_4(\boldsymbol{\alpha}, q)$ holds; this will imply $\mathsf{J}_4(\boldsymbol{\alpha}, q)$.

We take $t = p$ in the formula of Lemma 27, and we first deal with the terms in (7). Thus, we choose a subsequence $\boldsymbol{i} = (i_1, \dots, i_\kappa)$ of $(1, \dots, p)$, with $1 \le \kappa \le \min(p, n-1)$, and indices $\boldsymbol{r} = (r_1, \dots, r_\kappa)$, with $1 \le r_k \le \alpha_{i_k}$ for all k. We prove that the Jacobian matrix of the p-minors of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ with respect to $\tilde{\boldsymbol{X}} = (X_0, \dots, X_n)$ has rank n at all points $\tilde{\boldsymbol{x}} = (x_0, \dots, x_n)$ of $V_p(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$ such that $\tilde{\boldsymbol{x}}' = (x_0, \dots, x_{n-\kappa})$ is in $V_\kappa(\mathfrak{M}^H_{\boldsymbol{\alpha}_{\boldsymbol{i}},n-1}(\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}, \tilde{\boldsymbol{X}}')) \subset \mathbb{P}^{n-\kappa}(\overline{\mathbf{K}(\mathfrak{L}')})$, and such that

$$x_{n-\kappa+1} = \mathfrak{f}_{n-\kappa+1,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{x}}'), \dots, x_n = \mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{x}}'). \tag{9}$$

By Lemma 27, taking all such $\tilde{\boldsymbol{x}}$ into account, for all $\boldsymbol{i}$ and $\boldsymbol{r}$, will cover all points in $V_p(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$, up to the exception of those points obtained from $\kappa = n$, which will admit a simpler treatment. For simplicity, we continue the proof with $\boldsymbol{i} = (1, \dots, \kappa)$, so that we have $\boldsymbol{\alpha}_{\boldsymbol{i}} = (\alpha_1, \dots, \alpha_\kappa)$.

We are going to exhibit some polynomials that belong to $I_p(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$, for which we can control the rank of the Jacobian at $\tilde{\boldsymbol{x}}$. First, we prove that for i in $\{1, \dots, \kappa\}$ and r in $\{1, \dots, \alpha_i\} - \{r_i\}$, as well as i in $\{\kappa + 1, \dots, p\}$ and r in $\{1, \dots, \alpha_i\}$, the value $\mathfrak{l}^H_{i,i,r}(\tilde{\boldsymbol{x}})$ is non-zero. We subdivide the indeterminates $\mathfrak{L}'$ into $\mathfrak{L}'_{\boldsymbol{i},\boldsymbol{r}}$ and $\mathfrak{L}''_{\boldsymbol{i},\boldsymbol{r}}$, where $\mathfrak{L}'_{\boldsymbol{i},\boldsymbol{r}}$ corresponds to the coefficients involved in $\mathfrak{l}^H_{i,i,r_i}$, for $i = 1, \dots, \kappa$, and in the submatrix of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ associated to $\boldsymbol{i}$, and $\mathfrak{L}''_{\boldsymbol{i},\boldsymbol{r}}$ are the other coordinates. By $\mathsf{J}_2(\boldsymbol{\alpha}_s, n-1)$, $V_\kappa(\mathfrak{M}^H_{\boldsymbol{\alpha}_{\boldsymbol{i}},n-1}(\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}, \tilde{\boldsymbol{X}}'))$ is finite; as a result, since all entries of $\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}$ are in $\mathbf{K}(\mathfrak{L}'_{\boldsymbol{i},\boldsymbol{r}})$, all coordinates of $\tilde{\boldsymbol{x}}$ are algebraic over $\mathbf{K}(\mathfrak{L}'_{\boldsymbol{i},\boldsymbol{r}})$. For i, r as above, the coefficients of the equation

$$\mathfrak{l}^H_{i,i,r} = \mathfrak{l}_{i,i,r,0} X_0 + \mathfrak{l}_{i,i,r,1} X_1 + \cdots + \mathfrak{l}_{i,i,r,n} X_n$$

are in $\mathbf{K}(\mathfrak{L}''_{\boldsymbol{i},\boldsymbol{r}})$, thus algebraically independent over the field of definition of $\tilde{\boldsymbol{x}}$, so that $\mathfrak{l}^H_{i,i,r}(\tilde{\boldsymbol{x}})$ is non-zero.

Remark 28. *This implies in particular that the union in Lemma 27 is disjoint.*

In the following two paragraphs, assume $\kappa \geq 2$ and take i in $\{1,\dots,\kappa\}$. We can then define $\boldsymbol{i}^* = (1,\dots,i-1,i+1,\dots,\kappa)$, $\boldsymbol{\alpha}^* = (\alpha_1,\dots,\alpha_{i-1},\alpha_{i+1},\dots,\alpha_\kappa)$, and we call $\mathfrak{N}^H_i$ the submatrix of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ associated to $\boldsymbol{i}^*$; this is a matrix with $\kappa-1$ rows (indexed by $\boldsymbol{i}^*$ in $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$) and $n-1$ columns (of indices $p+1,\dots,q$ in $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$).

We prove that there exists a $(\kappa-1)$-minor c_i of $\mathfrak{N}^H_i$ such that $c_i(\tilde{\boldsymbol{x}}) \neq 0$. Let indeed $\mathfrak{m}^H_i$ be the matrix obtained by applying the substitution (9) in $\mathfrak{N}^H_i$. This matrix has $\kappa-1$ rows and $n-1$ columns; its entries are products of linear forms in $(n-\kappa)+1$ variables $X_0,\dots,X_{n-\kappa}$, with coefficients that are algebraically independent over $\mathbf{K}$. We can thus apply $\mathsf{J}_3(\boldsymbol{\alpha}^*, n-1)$ to $\mathfrak{m}^H_i$, and deduce that this matrix has full rank $\kappa-1$ at $\tilde{\boldsymbol{x}}'$. Thus, $\mathfrak{N}^H_i$ has rank $\kappa-1$ at $\tilde{\boldsymbol{x}}$, from which the existence of the minor c_i follows. If $\kappa = 1$, we define $c_1 = 1$.

We next deduce that for i in $\{1,\dots,\kappa\}$, there exists a polynomial of the form $b_i\mathfrak{l}^H_{i,i,r_i}$ in the ideal $I_p(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$, with $b_i(\tilde{\boldsymbol{x}}) \neq 0$. Indeed, we consider the p-minor of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ obtained by taking the columns $i,\kappa+1,\dots,p$, and all $\kappa-1$ columns in the $(\kappa-1)$-minor c_i (if $\kappa = 1$, there is no need to consider such columns). Using the factorization

$$\mathfrak{l}^H_{i,i} = \beta_i \mathfrak{l}^H_{i,i,r_i}, \quad \text{with} \quad \beta_i = \mathfrak{l}^H_{i,i,1}\cdots\mathfrak{l}^H_{i,i,r_i-1}\mathfrak{l}^H_{i,i,r_i+1}\cdots\mathfrak{l}^H_{i,i,\alpha_i},$$

that minor evaluates to

$$b_i\mathfrak{l}^H_{i,i,r_i} \quad \text{with} \quad b_i = \beta_i\mathfrak{l}^H_{\kappa+1,\kappa+1}\cdots\mathfrak{l}^H_{p,p}c_i.$$

Hence, $b_i\,\mathfrak{l}^H_{i,i,r_i}$ belongs to $I_p(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$, and by the discussion of the three previous paragraphs, $b_i(\tilde{\boldsymbol{x}}) \neq 0$, as claimed. In what follows, we write $b = b_1\cdots b_\kappa$, so that $b(\tilde{\boldsymbol{x}}) \neq 0$ and $b\,\mathfrak{l}^H_{i,i,r_i}$ is in $I_p(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$. This in turn implies that all polynomials

$$b(X_{n-\kappa+1} - \mathfrak{f}_{n-\kappa+1,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{X}}')),\dots,b(X_n - \mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{X}}'))$$

are in $I_p(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$ as well.

Similarly, for every κ-minor η of the submatrix of $\mathfrak{N}^H_{\boldsymbol{\alpha},q}$ associated to $\boldsymbol{i}$, the polynomial $\mathfrak{l}^H_{\kappa+1,\kappa+1}\cdots\mathfrak{l}^H_{p,p}\,\eta$ belongs to $I_p(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$. Thus, $b\,\eta$ is in $I_p(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$ as well.

As a result, the polynomial $b\,\eta(\tilde{\boldsymbol{X}}', \mathfrak{f}_{n-\kappa+1,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{X}}'),\dots,\mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{X}}'))$ belongs to $I_p(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$. Now, $\gamma = \eta(\tilde{\boldsymbol{X}}', \mathfrak{f}_{n-\kappa+1,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{X}}'),\dots,\mathfrak{f}_{n,\boldsymbol{i},\boldsymbol{r}}(\tilde{\boldsymbol{X}}'))$ is one of the κ-minors of $\mathfrak{M}^H_{\boldsymbol{\alpha}_{\boldsymbol{i}},n-1}(\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}, \tilde{\boldsymbol{X}}')$, and all κ-minors of this matrix are obtained this way. To summarize, we have proved that

$$b\,\mathfrak{l}^H_{1,1,r_1},\dots,b\,\mathfrak{l}^H_{\kappa,\kappa,r_\kappa} \quad \text{and} \quad b\,\gamma, \text{ for all } \kappa\text{-minors } \gamma \text{ of } \mathfrak{M}^H_{\boldsymbol{\alpha}_{\boldsymbol{i}},n-1}(\mathfrak{H}_{\boldsymbol{i},\boldsymbol{r}}, \tilde{\boldsymbol{X}}')$$

are in $I_p(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$, with $b(\tilde{\boldsymbol{x}}) \neq 0$. The Jacobian matrix of these polynomials at $\tilde{\boldsymbol{x}}$ is, up to the non-zero constant $b(\tilde{\boldsymbol{x}})$, equal to that of $\mathfrak{l}^H_{1,1,r_1},\dots,\mathfrak{l}^H_{\kappa,\kappa,r_\kappa}$ (which is simply a matrix of constants), and of all κ-minors γ. Using our induction assumption, we know that the

Jacobian matrix of the ideal of κ-minors γ with respect to $\tilde{\boldsymbol{X}}'$ has rank $n-\kappa$ at $\tilde{\boldsymbol{x}}'$. As a result, the larger Jacobian matrix of all equations above has rank n at $\tilde{\boldsymbol{x}}$, as claimed.

It remains to deal with the case $\kappa = n$, for $n \leq p$; as above, we may simplify the discussion by assuming that $\boldsymbol{i} = (1, \ldots, n)$. In this case, the discussion is simpler: proceeding as above, but dealing only with the polynomials $\mathfrak{l}^H_{1,1}, \ldots, \mathfrak{l}^H_{n,n}$, we obtain the fact that equations of the form $b\,\mathfrak{l}^H_{1,1,r_1}, \ldots, b\,\mathfrak{l}^H_{n,n,r_n}$ belong to $I_p(\mathfrak{N}^H_{\boldsymbol{\alpha},q})$, with $b(\tilde{\boldsymbol{x}}) \neq 0$. The conclusion follows directly.

6.5 An algorithm

We conclude this section with an algorithm that applies the process in Lemma 27, in the case $t = p$, to non-homogeneous matrices. Indeed, while homogeneity is used at several steps in the proof (and will be needed again when we apply this result), our main algorithm deals with matrices without a homogeneous structure. Thus we will consider a matrix N as in (3), but with $X_0 = 1$. Explicitly, we have

$$N = \begin{pmatrix} \lambda_{1,1} & 0 & \cdots & 0 & \lambda_{1,p+1} & \cdots & \lambda_{1,q} \\ 0 & \lambda_{2,2} & \cdots & 0 & \lambda_{2,p+1} & \cdots & \lambda_{2,q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_{p,p} & \lambda_{p,p+1} & \cdots & \lambda_{p,q} \end{pmatrix}, \tag{10}$$

where for all i, j, $\lambda_{i,j}$ is the product of α_i linear forms $(\lambda_{i,j,k})_{1\leq k\leq \alpha_i}$ with coefficients in $\mathbf{K}$, in variables $X_1, \ldots, X_n$. By Proposition 26, we deduce that for a generic choice of the coefficients of these linear forms, $V_p(N) \subset \overline{\mathbf{K}}^n$ is a finite set, whose structure is given by Lemma 27. Besides, oberve that all points of $V_p(N)$ are simple and isolated (this is an immediate consequence of the second assertion of Proposition 26).

Algorithm RowDegreeDiagonal below takes as input the linear forms $(\lambda_{i,j,k})$ and computes a zero-dimensional parametrization of $V_p(N)$. In the algorithm, we assume the existence of a subroutine RowDegree_simple(Γ) which takes as input a straight-line program Γ that computes a polynomial matrix F and a system of equations G, and solves Problem 2 for this input using a row-degree homotopy. We give such an algorithm in the next section. We denote by $T_{\text{row}}(\sigma, \boldsymbol{\gamma}, \boldsymbol{\alpha}, q)$ the time spent by RowDegree_simple(Γ) on input a straight-line program of length σ that computes F with row degrees $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ and q columns, and $G = (g_1, \ldots, g_s)$ of degrees $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_s)$.

We will be use here the particular case of subroutine RowDegree_simple where the input matrix has the form

$$M = \begin{pmatrix} \lambda_{1,1} & \lambda_{1,2} & \cdots & \lambda_{1,q} \\ \lambda_{2,1} & \lambda_{2,2} & \cdots & \lambda_{2,q} \\ \vdots & & & \vdots \\ \lambda_{p,1} & \lambda_{p,2} & \cdots & \lambda_{p,q} \end{pmatrix}, \tag{11}$$

where for all i, j, $\lambda_{i,j}$ is the product of α_i (non necessarily homogeneous) linear forms $(\lambda_{i,j,k})_{1\leq k\leq \alpha_i}$ in n variables $X_1, \ldots, X_n$. In this case, each entry $\lambda_{i,j}$ can be computed in

Algorithm 3 RowDegreeDiagonal$((\lambda_{i,j,k})_{i,j,k})$

Input: linear forms $(\lambda_{i,j,k})_{i,j,k}$ making up the entries of $N \in \mathbf{K}[X_1, \ldots, X_n]^{p \times q}$ as in (10), with $p \leq q$ and $n = q - p + 1$
Output: a zero-dimensional parametrization $\mathscr{R}$ of $V_p(N)$

1. for any subsequence $\boldsymbol{i} = (i_1, \ldots, i_\kappa)$ of $(1, \ldots, p)$ with $1 \leq \kappa \leq \min(n-1, p)$
   (a) for any sequence $\boldsymbol{r} = (r_1, \ldots, r_\kappa)$, with r_k in $\{1, \ldots, \alpha_k\}$ for all k
      i. apply Gaussian elimination to the system $\lambda_{i_1,i_1,r_1} = \cdots = \lambda_{i_\kappa,i_\kappa,r_\kappa} = 0$ to rewrite $(X_{n-\kappa+1}, \ldots, X_n)$ as linear forms $(f_{j,\boldsymbol{i},\boldsymbol{r}})_{n-\kappa+1 \leq j \leq n}$ in $(X_1, \ldots, X_{n-\kappa})$.
      cost: $O(\sum_{\boldsymbol{i},\boldsymbol{r}} n^3)$
      ii. construct a straight-line program $\Gamma_{\boldsymbol{i},\boldsymbol{r}}$ that computes the matrix $M_{\boldsymbol{i},\boldsymbol{r}} \in \mathbf{K}[X_1, \ldots, X_{n-\kappa}]^{\kappa \times (n-1)}$ obtained by substituting $(f_{j,\boldsymbol{i},\boldsymbol{r}})_{n-\kappa+1 \leq j \leq n}$ into $N_{\boldsymbol{i},(p+1,\ldots,q)}$. The length of $\Gamma_{\boldsymbol{i},\boldsymbol{r}}$ is $O(\kappa n(\alpha_{i_1} + \cdots + \alpha_{i_\kappa}))$.
      cost: $O(\sum_{\boldsymbol{i},\boldsymbol{r}} (\alpha_{i_1} + \cdots + \alpha_{i_\kappa}) n^3)$
      iii. $\mathscr{R}'_{\boldsymbol{i},\boldsymbol{r}} \leftarrow$ RowDegree_simple$(\Gamma_{\boldsymbol{i},\boldsymbol{r}})$ (points have coordinates $(X_1, \ldots, X_{n-\kappa})$)
      cost: $\sum_{\boldsymbol{i},\boldsymbol{r}} T_{M,\mathrm{row}}((\alpha_{i_1}, \ldots, \alpha_{i_\kappa}), n-1)$
      iv. deduce $\mathscr{R}_{\boldsymbol{i},\boldsymbol{r}}$ from $\mathscr{R}'_{\boldsymbol{i},\boldsymbol{r}}$ by adding the expressions for $(X_{n-\kappa+1}, \ldots, X_n)$
      cost: $O(\sum_{\boldsymbol{i},\boldsymbol{r}} n^2 c'_{\boldsymbol{i},\boldsymbol{r}})$
2. if $n \leq p$, for any subsequence $\boldsymbol{i} = (i_1, \ldots, i_n)$ of $(1, \ldots, p)$
   (a) for any sequence $\boldsymbol{r} = (r_1, \ldots, r_n)$, with $r_k \in \{1, \ldots, \alpha_k\}$ for all k
      i. let $\boldsymbol{x}_{\boldsymbol{i},\boldsymbol{r}}$ be the solution of the system $\lambda_{i_1,i_1,r_1} = \cdots = \lambda_{i_n,i_n,r_n} = 0$
      cost: $O(\sum_{\boldsymbol{i},\boldsymbol{r}} n^3)$
      ii. create a zero-dimensional parametrization $\mathscr{R}_{\boldsymbol{i},\boldsymbol{r}}$ such that $Z(\mathscr{R}_{\boldsymbol{i},\boldsymbol{r}}) = \{\boldsymbol{x}_{\boldsymbol{i},\boldsymbol{r}}\}$
      cost: $O(\sum_{\boldsymbol{i},\boldsymbol{r}} n)$
3. combine all $(\mathscr{R}_{\boldsymbol{i},\boldsymbol{r}})_{\boldsymbol{i},\boldsymbol{r}}$ into the output $\mathscr{R}$
   cost: $\tilde{O}(\sum_{\boldsymbol{i},\boldsymbol{r}} n c'_{\boldsymbol{i},\boldsymbol{r}})$

$O(n\alpha_i)$ operations in $\mathbf{K}$, so that the whole matrix M can be computed by a straight-line program of length $O(nq(\alpha_1 + \cdots + \alpha_p))$. In this case there are no additional equations G, so we denote the cost of Algorithm RowDegree_simple for such input by

$$T_{M,\mathrm{row}}(\boldsymbol{\alpha}, q) = T_{\mathrm{row}}(nq(\alpha_1 + \cdots + \alpha_p), (), \boldsymbol{\alpha}, q). \tag{12}$$

We conclude this section with the cost analysis of Algorithm RowDegreeDiagonal.

Lemma 29. *Let $S_n(\alpha_1, \ldots, \alpha_p)$ be the degree n complete symmetric function of $(\alpha_1, \ldots, \alpha_p)$.*

The total cost of RowDegreeDiagonal$((\lambda_{i,j,k})_{i,j,k})$ *is*

$$\sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_\kappa)\\ \kappa\leq\min(n-1,p)}} \alpha_{i_1}\cdots\alpha_{i_\kappa} T_{M,\mathrm{row}}((\alpha_{i_1},\ldots,\alpha_{i_\kappa}),n-1) + O^{\sim}\left(n^3(c'+S_n(\alpha_1,\ldots,\alpha_p))\right),$$

where c' is the cardinality of $V_p(N)$.

Proof. The cost reported at each step in the algorithm is the total amount of time spent there, over all iterations (the sums in the first loop are for $\kappa \leq \min(n-1,p)$, the ones in the second loop for $\kappa = n$ if $n \leq p$). Several steps are straightforward to analyze; we briefly comment on a few others.

Step 1(a)ii uses the linear forms $(f_{j,\boldsymbol{i},\boldsymbol{r}})_{n-\kappa+1\leq j\leq n}$ to construct a straight-line program $\Gamma_{\boldsymbol{i},\boldsymbol{r}}$ that computes the entries of $M_{\boldsymbol{i},\boldsymbol{r}}$. This is done by computing the coefficients of the linear forms in $(X_1,\ldots,X_{n-\kappa})$ obtained after substitution. Each linear form requires a matrix-vector product with a matrix of size $(n-\kappa)\times n$, for $O(n^2)$ operations, whence a total of $O((\alpha_{i_1}+\cdots+\alpha_{i_\kappa})n^3)$ for all entries.

Step 1(a)iv consists in adding κ coordinates $(X_{n-\kappa+1},\ldots,X_n)$ to a zero-dimensional parametrization in variables $X_1,\ldots,X_{n-\kappa}$, where $(X_{n-\kappa+1},\ldots,X_n)$ are known as linear forms $(f_{j,\boldsymbol{i},\boldsymbol{r}})_{n-\kappa+1\leq j\leq n}$ in $(X_1,\ldots,X_{n-\kappa})$: this is done by means of a matrix product in size $(\kappa\times n-\kappa)$ by $(n-\kappa\times c'_{\boldsymbol{i},\boldsymbol{r}})$, where $c'_{\boldsymbol{i},\boldsymbol{r}}$ is the cardinality of $V_\kappa(M_{\boldsymbol{i},\boldsymbol{r}})$, for $\boldsymbol{i}=(i_1,\ldots,i_\kappa)$. The cost is thus $O(n^2c'_{\boldsymbol{i},\boldsymbol{r}})$; the sum of these costs is thus $O(n^2c')$, since the sum of all $c'_{\boldsymbol{i},\boldsymbol{r}}$ is equal to c' by Remark 28.

The combination in the last step is done by fast Chinese Remaindering, in quasi-linear time $O^{\sim}(\sum_{\boldsymbol{i},\boldsymbol{r}} nc'_{\boldsymbol{i},\boldsymbol{r}})$, which is $O^{\sim}(nc')$. Thus, the total runtime is

$$\sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_\kappa)\\ \boldsymbol{r}=(r_1,\ldots,r_\kappa)\\ \kappa\leq\min(n-1,p)}} T_{M,\mathrm{row}}((\alpha_{i_1},\ldots,\alpha_{i_\kappa}),n-1)$$
$$+ O^{\sim}\left(n^2c' + \sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_\kappa)\\ \boldsymbol{r}=(r_1,\ldots,r_\kappa)\\ \kappa\leq\min(n-1,p)}} (\alpha_{i_1}+\cdots+\alpha_{i_\kappa})n^3 + \sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_n)\\ \boldsymbol{r}=(r_1,\ldots,r_n)}} n^3\right).$$

The costs reported in the sums do not depend on $\boldsymbol{r}$, so that this can be rewritten as

$$\sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_\kappa)\\ \kappa\leq\min(n-1,p)}} \alpha_{i_1}\cdots\alpha_{i_\kappa} T_{M,\mathrm{row}}((\alpha_{i_1},\ldots,\alpha_{i_\kappa}),n-1)$$
$$+ O^{\sim}\left(n^2c' + \sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_\kappa)\\ \kappa\leq\min(n-1,p)}} \alpha_{i_1}\cdots\alpha_{i_\kappa}(\alpha_{i_1}+\cdots+\alpha_{i_\kappa})n^3 + \sum_{\boldsymbol{i}=(i_1,\ldots,i_n)} \alpha_{i_1}\cdots\alpha_{i_n}n^3\right).$$

The final simplification comes from noting that $\sum_{\boldsymbol{i}} \alpha_{i_1} \cdots \alpha_{i_\kappa}(\alpha_{i_1} + \cdots + \alpha_{i_\kappa})$, for $\boldsymbol{i}$ a subsequence of $(1, \ldots, p)$ of length $\kappa \leq \min(n-1, p)$, is bounded from above by $S_n(\alpha_1, \ldots, \alpha_p)$. The same holds for the second sum (which is empty if $n > p$). □

7 The row-degree homotopy

We now give algorithms to solve Problems 1 and 2 whose runtime will depend on the row-degrees of the input matrix F. These algorithms are more complex than the ones in Section 5, due to their recursive nature. This boils down to the fact that the start system we use for the homotopy must itself be solved by means of several homotopies of smaller size, along the lines of the discussion in the previous section.

Again, we are given a matrix $F = [f_{i,j}] \in \mathbf{K}[X_1, \ldots, X_n]^{p \times q}$ and polynomials $G = (g_1, \ldots, g_s)$ in $\mathbf{K}[X_1, \ldots, X_n]$, with $p \leq q$ and $n = q - p + s + 1$, and we want to compute the isolated points of $V_p(F, G)$, with

$$V_p(F, G) = \{\boldsymbol{x} \in \overline{\mathbf{K}}^n \mid \operatorname{rank}(F(\boldsymbol{x})) < p \text{ and } g_1(\boldsymbol{x}) = \cdots = g_s(\boldsymbol{x}) = 0\}.$$

We are now interested in designing an algorithm for computing the isolated points of $V_p(F, G)$ whose cost depends on the row degrees $\alpha_1 = \operatorname{rdeg}(F, 1), \ldots, \alpha_p = \operatorname{rdeg}(F, p)$; with this notation, $\deg(f_{i,j}) \leq \alpha_i$ holds for all i, j. As in Section 5, we write $\gamma_1 = \deg(g_1), \ldots, \gamma_s = \deg(g_s)$.

Proposition 30. *Suppose that matrix $F \in \mathbf{K}[X_1, \ldots, X_n]^{p \times q}$ and polynomials $G = (g_1, \ldots, g_s)$ in $\mathbf{K}[X_1, \ldots, X_n]$ are given by a straight-line program of length σ. Then, the multiplicities of the isolated points of $V_p(F, G)$ are at most $c' = \gamma_1 \cdots \gamma_s S_{n-s}(\delta_1, \ldots, \delta_q)$.*

If all γ_i's and α_j's are at least equal to 1, there exists a randomized algorithm that computes these isolated points using

$$O^{\sim}\left(c'^2 n^5 \binom{q}{p}^2 (e' + c'^5 n)(\sigma + \binom{q}{p} n + nqp\alpha + \gamma + n^3)\right)$$

operations in $\mathbf{K}$, with $c' = \gamma_1 \cdots \gamma_s S_{n-s}(\delta_1, \ldots, \delta_q)$ and $e' = (\gamma_1 + 1) \cdots (\gamma_s + 1) S_{n-s}(\delta_1 + 1, \ldots, \delta_q + 1)$, where $S_{n-s}(\cdots)$ is the complete homogeneous symmetric function of degree $n - s$.

The homotopy on which this algorithm relies makes use of Algorithm RowDegreeDiagonal given in the previous Section. This one itsself uses an algorithm called RowDegree_simple which, on input F and G, computes the simple isolated points of $V_p(F, G)$.

Proposition 31. *Reusing the notations introduced above and under the assumptions of Proposition 30, there exists a randomized algorithm that computes the simple isolated points of $V_p(F, G)$ using*

$$O^{\sim}\left(c'^2 n^6 \binom{q}{p}^2 (c' + e'(\sigma + nqp\alpha + \gamma + n^3))\right)$$

operations in $\mathbf{K}$.

These propositions complete the proof of Theorems 1, 2 and 3. We start by solving Problem 2 and hence give the algorithm Rowdegree_simple on which Proposition 31 relies.

7.1 Setting up the homotopy and sum of the multiplicities

To solve Problems 1 and 2, we are again going to rely on the algorithm of Section 3. As in Section 5, we let $\boldsymbol{C} = (c_1, \ldots, c_s, c_{s+1} \ldots, c_m)$ be such that $(c_1, \ldots, c_s) = (g_1, \ldots, g_s)$ and $(c_{s+1}, \ldots, c_m)$ are the p-minors of F. Our main concern is to design a sequence of polynomials $\boldsymbol{B} = (b_1, \ldots, b_s, \ldots, b_m)$ in $\mathbf{K}[T, \boldsymbol{X}]$ such that $\boldsymbol{C} = \boldsymbol{B}_1$, such that we can solve efficiently the system $\boldsymbol{A} = \boldsymbol{B}_0$, and such that $\boldsymbol{B}$ has the same degree profile as our target system $\boldsymbol{C}$.

The polynomials $(b_1, \ldots, b_s)$ are defined as in Section 5, letting a_i be a product of γ_i linear forms $\mu_{i,k}$ with randomly chosen coefficients, of the form

$$a_i = \prod_{k=1}^{\gamma_i} \mu_{i,k}, \quad \text{with} \quad \mu_{i,k} = \mu_{i,k,0} + \sum_{\ell=1}^{n} \mu_{i,k,\ell} X_\ell \tag{13}$$

and writing $b_i = (1-T)a_i + Tg_i$ for $i = 1, \ldots, s$. The difference will lie in the construction of the start matrix used in the homotopy. The construction presented in Section 5 does not carry over if we want to take row degrees into account. Instead, we use a deformation that cancels out many off-diagonal terms; following the construction in the previous section, we define N as in (10), that is

$$N = \begin{pmatrix} \lambda_{1,1} & 0 & \cdots & 0 & \lambda_{1,p+1} & \cdots & \lambda_{1,q} \\ 0 & \lambda_{2,2} & \cdots & 0 & \lambda_{2,p+1} & \cdots & \lambda_{2,q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_{p,p} & \lambda_{p,p+1} & \cdots & \lambda_{p,q} \end{pmatrix},$$

where for all i, j, $\lambda_{i,j}$ is a product of α_i linear forms with random coefficients in $\mathbf{K}$, of the form

$$\lambda_{i,j} = \prod_{k=1}^{\alpha_i} \lambda_{i,j,k}, \quad \text{with} \quad \lambda_{i,j,k} = \lambda_{i,j,k,0} + \sum_{\ell=1}^{n} \lambda_{i,j,k,\ell} X_\ell.$$

Then, we define $(b_{s+1}, \ldots, b_m)$ as the p-minors of $U = (1-T)\cdot N + T \cdot F$, and $\boldsymbol{B} = (b_1, \ldots, b_m)$. The polynomials $(a_{s+1}, \ldots, a_m)$ are defined as the p-minors of N, so that $\boldsymbol{A} = \boldsymbol{B}_0$; on the other hand, we also have $\boldsymbol{C} = \boldsymbol{B}_1$. Our next step is to prove that all assumptions of Propositions 8 and 9 are satisfied for $\boldsymbol{B}$ and $\boldsymbol{A} = \boldsymbol{B}_0$, as long as the coefficients of $a_1, \ldots, a_s$ and N are chosen generically.

Properties B_1 and B_2 These follow from Proposition 20.

Properties C_1, C_2 and C_3

Property $\mathsf{C}_1(0)$. We have to prove that for $i = 1, \dots, m$, $\deg_{\boldsymbol{X}}(b_i) = \deg_{\boldsymbol{X}}(a_i)$. We already established it in Section 5 for indices $i = 1, \dots, s$. For $i = s+1, \dots, m$, we can readily see that the degree of b_i in $\boldsymbol{X}$ is at most $\alpha_1 + \cdots + \alpha_p$, so it suffices to prove that the degree of all p-minors $(a_{s+1}, \dots, a_m)$ of N is $\alpha_1 + \cdots + \alpha_p$.

Indeed, any p-minor of N is of the form $\lambda_{i_1,i_1} \cdots \lambda_{i_\kappa,i_\kappa} \zeta$, for some sequence $\boldsymbol{i} = (i_1, \dots, i_\kappa) \subset (1, \dots, p)$ of length $\kappa \in \{0, \dots, p\}$ and some $(p-\kappa)$-minor ζ of $N_{\boldsymbol{i},(p+1,\dots,q)}$. Since the entries of $N_{\boldsymbol{i},(p+1,\dots,q)}$ are products of linear form with randomly chosen coefficients $(\lambda_{i,j,k,\ell})$, for a generic choice of these coefficients, the determinant ζ has degree $\sum_{i' \notin \boldsymbol{i}} \alpha_{i'}$. As a result, the corresponding p-minor of N has degree $\alpha_1 + \cdots + \alpha_p$, as claimed.

Property $\mathsf{C}_2(0)$. Next, we prove that the system $\boldsymbol{A} = \boldsymbol{B}_0$ has no solution at infinity. As in Section 5, we introduce a homogenization variable X_0, and we consider the system $\boldsymbol{A}^H = (a_1^H, \dots, a_s^H, \dots, a_m^H)$ obtained by homogenizing all equations in $\boldsymbol{A}$. Thus we have

$$a_i^H = \prod_{k=1}^{\gamma_i} \mu_{i,k}^H \quad \text{with} \quad \mu_{i,k}^H = \mu_{i,k,0} X_0 + \sum_{\ell=1}^{n} \mu_{i,k,\ell} X_\ell$$

for $i = 1, \dots, s$, whereas $a_{s+1}^H, \dots, a_m^H$ are the p-minors of the matrix

$$N^H = \begin{pmatrix} \lambda_{1,1}^H & 0 & \cdots & 0 & \lambda_{1,p+1}^H & \cdots & \lambda_{1,q}^H \\ 0 & \lambda_{2,2}^H & \cdots & 0 & \lambda_{2,p+1}^H & \cdots & \lambda_{2,q}^H \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_{p,p}^H & \lambda_{p,p+1}^H & \cdots & \lambda_{p,q}^H \end{pmatrix},$$

where $\lambda_{i,k}^H$ is the homogenization of $\lambda_{i,j}$. (This latter property requires genericity of the coefficients of the linear forms $\lambda_{i,k}^H$; it is enough that each p-minor of N have degree $\alpha_1 + \cdots + \alpha_p$.)

The solutions of $\boldsymbol{A}^H$ in $\mathbb{P}^n(\overline{\mathbf{K}})$ are found by first solving the equations $(a_1^H, \dots, a_s^H)$. As in Section 5, all a_i^H are products of linear forms, so any solution of $(a_1^H, \dots, a_s^H)$ is obtained by setting some of these linear forms to zero (at least one for each $i = 1, \dots, s$). We choose indices $\boldsymbol{u} = (u_1, \dots, u_s)$, with $u_1 \in \{1, \dots, \gamma_1\}$, $\dots$, $u_s \in \{1, \dots, \gamma_s\}$, and we solve

$$\mu_{i,u_i}^H = 0, \quad \text{that is,} \quad \mu_{i,u_i,0} X_0 + \sum_{\ell=1}^{n} \mu_{i,u_i,\ell} X_\ell = 0,$$

for $i = 1, \dots, s$. In what follows, we fix such an $\boldsymbol{u}$. Then, for a generic choice of coefficients $\mu_{i,k,\ell}$, these equations are equivalent to

$$X_{n-s+1} = \Phi_{n-s+1,\boldsymbol{u}}(X_0, \dots, X_{n-s}), \dots, X_n = \Phi_{n,\boldsymbol{u}}(X_0, \dots, X_{n-s}),$$

for some homogeneous linear forms $\Phi_{n-s+1,\boldsymbol{u}}, \dots, \Phi_{n,\boldsymbol{u}}$. After applying this substitution, for

all i, j, N^H can be rewritten as

$$N^H_{\boldsymbol{u}} = \begin{pmatrix} \lambda^H_{1,1,\boldsymbol{u}} & 0 & \cdots & 0 & \lambda^H_{1,p+1,\boldsymbol{u}} & \cdots & \lambda^H_{1,q,\boldsymbol{u}} \\ 0 & \lambda^H_{2,2,\boldsymbol{u}} & \cdots & 0 & \lambda^H_{2,p+1,\boldsymbol{u}} & \cdots & \lambda^H_{2,q,\boldsymbol{u}} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda^H_{p,p,\boldsymbol{u}} & \lambda^H_{p,p+1,\boldsymbol{u}} & \cdots & \lambda^H_{p,q,\boldsymbol{u}} \end{pmatrix},$$

with

$$\lambda^H_{i,j,\boldsymbol{u}} = \prod_{k=1}^{\alpha_i} \lambda^H_{i,j,k,\boldsymbol{u}}, \quad \text{and} \quad \lambda^H_{i,j,k,\boldsymbol{u}} = \sum_{\ell=0}^{n-s} \lambda_{i,j,k,\ell} X_\ell + \sum_{\ell=n-s+1}^{n} \lambda_{i,j,k,\ell} \Phi_{\ell,\boldsymbol{u}}(X_0, \ldots, X_{n-s}).$$

Remark that the entries of $N^H_{\boldsymbol{u}}$ are products of homogeneous linear forms in $(n-s)+1$ variables $(X_0, \ldots, X_{n-s})$, so that this matrix has the form seen in (3). As a result, for a generic choice of the coefficients $\mu_{i,k,\ell}$ and $\lambda_{i,j,k,\ell}$, the first item in Lemma 26 implies that there is no projective solution to $I_p(N^H_{\boldsymbol{u}})$ satisfying $X_0 = 0$. Taking into account all possible choices of $\boldsymbol{u}$, we deduce that there is no projective solution to $\boldsymbol{A}^H$ satisfying $X_0 = 0$, and $\mathsf{C}_2(0)$ is proved.

Property $\mathsf{C}_3(0)$. Finally, we have to prove that the Jacobian matrix of $\boldsymbol{A}$ has full rank n at any point in $V(\boldsymbol{A}) \subset \overline{\mathbf{K}}^n$. Let thus $\boldsymbol{x} = (x_1, \ldots, x_n)$ be in $V(\boldsymbol{A})$; in particular, $\tilde{\boldsymbol{x}} = (1, x_1, \ldots, x_n)$ is a projective solution of $\boldsymbol{A}^H$. Thus, there exists $\boldsymbol{u} = (u_1, \ldots, u_s)$ as above such that

$$x_{n-s+1} = \phi_{n-s+1,\boldsymbol{u}}(x_1 \ldots, x_{n-s}), \ldots, x_n = \phi_{n,\boldsymbol{u}}(x_1, \ldots, x_{n-s}),$$

where $\phi_{k,\boldsymbol{u}}(X_1, \ldots, X_{n-s}) = \Phi_{k,\boldsymbol{u}}(1, X_1, \ldots, X_{n-s})$ for all k, and such that and $N^H_{\boldsymbol{u}}$ has rank less than p at $\tilde{\boldsymbol{x}}' = (1, x_1, \ldots, x_{n-s})$. The second item of Lemma 26 shows that the Jacobian matrix of $M_p(N^H_{\boldsymbol{u}})$ with respect to $X_0, \ldots, X_{n-s}$ has rank $n-s$ at $\tilde{\boldsymbol{x}}'$. Since the first coordinate of $\tilde{\boldsymbol{x}}'$ is non-zero, and all generating polynomials of $I_p(N^H_{\boldsymbol{u}})$ are homogeneous, Euler's relation implies that the Jacobian matrix of $M_p(N_{\boldsymbol{u}})$ with respect to $X_1, \ldots, X_{n-s}$ has full rank $n-s$ at $\boldsymbol{x}' = (x_1, \ldots, x_{n-s})$, where

$$N_{\boldsymbol{u}} = \begin{pmatrix} \lambda_{1,1,\boldsymbol{u}} & 0 & \cdots & 0 & \lambda_{1,p+1,\boldsymbol{u}} & \cdots & \lambda_{1,q,\boldsymbol{u}} \\ 0 & \lambda_{2,2,\boldsymbol{u}} & \cdots & 0 & \lambda_{2,p+1,\boldsymbol{u}} & \cdots & \lambda_{2,q,\boldsymbol{u}} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_{p,p,\boldsymbol{u}} & \lambda_{p,p+1,\boldsymbol{u}} & \cdots & \lambda_{p,q,\boldsymbol{u}} \end{pmatrix}, \tag{14}$$

with

$$\lambda_{i,j,\boldsymbol{u}} = \prod_{k=1}^{\alpha_i} \lambda_{i,j,k,\boldsymbol{u}}, \quad \text{and} \quad \lambda_{i,j,k,\boldsymbol{u}} = \lambda_{i,j,k,0} + \sum_{\ell=1}^{n-s} \lambda_{i,j,k,\ell} X_\ell + \sum_{\ell=n-s+1}^{n} \lambda_{i,j,k,\ell} \phi_{\ell,\boldsymbol{u}}(X_1, \ldots, X_{n-s}).$$

We now prove that the Jacobian matrix of $\boldsymbol{A}$ with respect to $X_1, \ldots, X_n$ has full rank at $\boldsymbol{x}$.

The first step is similar to what we did in Section 5. For $i = 1, \ldots, s$, a_i is a product of linear forms of the form $a_i = \prod_{k=1}^{\gamma_i} \mu_{i,k}$, with $\mu_{i,u_i}(\boldsymbol{x}) = 0$. Since the coefficients $\mu_{i,k,\ell}$ are chosen generically, for $i = 1, \ldots, s$ and $k \neq u_i$, $\mu_{i,k}(\boldsymbol{x})$ is non-zero; as a result, in the local ring at $\boldsymbol{x}$, the polynomials $(a_1, \ldots, a_s)$ are equal (up to units) to the linear forms $(\mu_{1,u_1}, \ldots, \mu_{s,u_s})$. This further implies that

$$X_{n-s+1} - \phi_{n-s+1,\boldsymbol{u}}(X_1, \ldots, X_{n-s}), \ldots, X_n - \phi_{n,\boldsymbol{u}}(X_1, \ldots, X_{n-s}) \tag{15}$$

belong to the ideal generated by $(a_1, \ldots, a_s)$ in the local ring at $\boldsymbol{x}$.

Next, we consider the p-minors $(a_{s+1}, \ldots, a_m)$ of N. Let $\zeta \in \mathbf{K}[X_1, \ldots, X_n]$ be a p-minor of N, and let $\zeta_{\boldsymbol{u}} \in \mathbf{K}[X_1, \ldots, X_{n-s}]$ be the polynomial obtained after applying the substitution in (15) in N. Since ζ and all polynomials in (15) are in the ideal $\langle \boldsymbol{A} \rangle \cdot \mathcal{O}_{\boldsymbol{x}}$, the polynomial $\zeta_{\boldsymbol{u}}$ is in this ideal as well. Now, note that $\zeta_{\boldsymbol{u}}$ is a p-minor of $N_{\boldsymbol{u}}$ as defined in (14), and that all its p-minors are obtained this way. We pointed out above that the Jacobian matrix of these equations with respect to $X_1, \ldots, X_{n-s}$ has full rank $n - s$ at $\boldsymbol{x}'$. As a result, taking all $\zeta_{\boldsymbol{u}}$ into account, together with the equations in (15), we obtain a family of polynomials in $\langle \boldsymbol{A} \rangle \cdot \mathcal{O}_{\boldsymbol{x}}$ whose Jacobian matrix has rank n at $\boldsymbol{x}$, and $\mathsf{C}_3(0)$ is proved.

In view of the previous paragraphs, we can then apply Proposition 8. Since $\boldsymbol{B}$ satisfies $\mathsf{B}_1, \mathsf{B}_2$ and $\boldsymbol{A} = \boldsymbol{B}_0$ satisfies $\mathsf{C}_1, \mathsf{C}_2, \mathsf{C}_3$, we deduce that the sum of the multiplicities of the isolated solutions of $\boldsymbol{C} = \boldsymbol{B}_1$ is at most c', where c' is the number of solutions of $\boldsymbol{A}$. Our next step is to establish the value of c'. This is done in Corollary 33 below, which proves the first claim in Proposition 30.

Lemma 32. *Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_p)$ be positive integers. and let $S_t(\alpha_1, \ldots, \alpha_p)$ be the complete symmetric function of degree t in $\alpha_1, \ldots, \alpha_p$. For generic $p \times q$ matrices N as in (10) or M as in (11), with entries in $t = q - p + 1$ variables, $V_p(N)$ and $V_p(M)$ have cardinality $S_t(\alpha_1, \ldots, \alpha_p)$.*

Proof. First, let us show that if the claim holds for N in size $p \times q$, it holds for M as well. To this effect, we set up a homotopy between N and M, by considering the matrix $(1-T)\cdot N + T \cdot M$. The discussion in the previous paragraphs shows that (for generic choices of the coefficients) this matrix satisfies Properties B_1 and B_2, together with $\mathsf{C}_1(0), \mathsf{C}_2(0), \mathsf{C}_3(0)$. We claim that $\mathsf{C}_1(1), \mathsf{C}_2(1), \mathsf{C}_3(1)$ hold as well: the degree property in $\mathsf{C}_1(1)$ is proved as we did for $\mathsf{C}_1(0)$, and $\mathsf{C}_2(1), \mathsf{C}_3(1)$ are restatements of Lemma 26. As a result, we can apply Proposition 8 to the specializations of $(1-T)\cdot N + T \cdot M$ at $T = 0$ and $T = 1$, and conclude that $V_p(N)$ and $V_p(M)$ have the same cardinality, for generic choices of the coefficients of N and M.

We finish the proof by induction. If $p = q$, then $t = 1$, N is diagonal, and its determinant has degree $\alpha_1 + \cdots + \alpha_p = S_1(\alpha_1, \ldots, \alpha_p)$, so our claim holds for N (and thus for M). Suppose now that the claim is true for all $p' \leq p$ and all $q' < q$ with $p' \leq q'$ and for all choices of degrees $(\alpha_1, \ldots, \alpha_{p'})$. Following Algorithm RowDegreeDiagonal (which is essentially a restatement of Lemma 27) and Remark 28 (which states that the corresponding union is disjoint), we obtain

$$|V_p(N)| = \sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_\kappa) \\ \boldsymbol{r}=(r_1,\ldots,r_\kappa)}} |V_\kappa(M_{\boldsymbol{i},\boldsymbol{r}})|,$$

for all subsequences $\boldsymbol{i} = (i_1, \ldots, i_\kappa)$ of length $\kappa \in \{1, \ldots, \min(t-1, p)\}$ and $\boldsymbol{r} = (r_1, \ldots, r_\kappa)$, with $r_k \in \{1, \ldots, \alpha_k\}$ for all k, and where matrix $M_{\boldsymbol{i},\boldsymbol{r}}$ has $\kappa \leq p$ rows and $t-1 < q$ columns, with row degrees $(\alpha_{i_1}, \ldots, \alpha_{i_p})$; in particular, we can apply our induction assumption to such matrices. In addition, if $t \leq p$, we should take into account one extra point for each subsequence $(i_1, \ldots, i_t)$ of $(1, \ldots, p)$. Altogether, we obtain

$$|V_p(N)| = \sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_\kappa),\\ \boldsymbol{r}=(r_1,\ldots,r_\kappa)}} S_{t-\kappa}(\alpha_{i_1}, \ldots, \alpha_{i_\kappa}),$$

for $\kappa \in \{1, \ldots, \min(t, p)\}$, since $S_0 = 1$. For any given $\boldsymbol{i} = (i_1, \ldots, i_\kappa)$, there are $\alpha_{i_1} \cdots \alpha_{i_\kappa}$ choices of indices $\boldsymbol{r}$, so that we have

$$|V_p(N)| = \sum_{\boldsymbol{i}=(i_1,\ldots,i_\kappa)} \alpha_{i_1} \cdots \alpha_{i_\kappa} S_{t-\kappa}(\alpha_{i_1}, \ldots, \alpha_{i_\kappa}),$$

for $\boldsymbol{i} = (i_1, \ldots, i_\kappa)$ subsequence of $(1, \ldots, p)$ with $\kappa \in \{1, \ldots, \min(t, p)\}$. The latter sum is precisely $S_t(\alpha_1, \ldots, \alpha_p)$, so we are done. □

Corollary 33. *For a generic choice of coefficients $\mu_{i,k,\ell}$ and $\lambda_{i,j,k,\ell}$, the cardinality c' of the algebraic set $V(\boldsymbol{A})$ is $\gamma_1 \cdots \gamma_s S_{n-s}(\alpha_1, \ldots, \alpha_p)$.*

Proof. For a sequence $\boldsymbol{u} = (u_1, \ldots, u_s)$ as above, let $V_{\boldsymbol{u}}$ be the subset of $V(\boldsymbol{A})$ consisting of all those points $\boldsymbol{x}$ such that $\mu_{i,u_i}(\boldsymbol{x}) = 0$ for all i. Remark first that the sets $V_{\boldsymbol{u}}$ are (generically) pairwise disjoint: we pointed out above that for $\boldsymbol{x}$ in $V_{\boldsymbol{u}}$, any index i and any $k \neq u_i$, $\mu_{i,k}(\boldsymbol{x})$ is non-zero.

Let us thus fix $\boldsymbol{u} = (u_1, \ldots, u_s)$. The cardinality of $V_{\boldsymbol{u}}$ is equal to the number of points in $V_p(N_{\boldsymbol{u}})$; this is a polynomial matrix of size $p \times q$, with entries that are products of linear forms in $n-s = q-p+1$ variables and with row degrees $\alpha_1, \ldots, \alpha_p$. The previous lemma then shows that for any $\boldsymbol{u}$, for generic choices of the coefficients, $V_{\boldsymbol{u}}$ has cardinality $S_{n-s}(\alpha_1, \ldots, \alpha_p)$; the conclusion follows. □

7.2 Towards homotopy algorithms

Since B_1, B_2, $\mathsf{C}_1(0)$, $\mathsf{C}_2(0)$ and $\mathsf{C}_3(0)$ hold, we are going to apply Proposition 10 to compute the simple isolated points in $V_p(F, G)$. Recall that the resulting algorithm RowDegree_simple is used by the RowDegreeDiagonal of previous Section. Next, we will apply Proposition 9 In the following paragraphs, we discuss the required properties $\mathsf{D}_1, \mathsf{D}_2, \mathsf{D}_3$ in this context. In what follows, we assume that we are given a straight-line program Γ of length σ that computes the input matrix F and the input equations G. Besides, we also assume that all γ_i's and α_j's are at least equal to 1,

Property D_1. To perform the homotopy, we need a zero-dimensional parametrization of $V(\boldsymbol{A})$. We now describe how to obtain it; the process is based on Algorithm RowDegreeDiagonal given in the previous section, and makes up the first two steps in Algorithm RowDegree.

As a preliminary, we construct a straight-line program Δ that computes the entries of N: for all i, j, Δ computes and multiplies the values of the α_i linear forms involved in $\lambda_{i,j}$ using $O(n\alpha_i)$ step, so that its total length is $\sigma_N = O(n^2(\alpha_1 + \cdots + \alpha_p))$.

Then, for any sequence $\boldsymbol{u} = (u_1, \ldots, u_s)$, with u_j in $\{1, \ldots, \gamma_j\}$ for all j, we start by solving the equations $\mu_{1,u_1} = \cdots = \mu_{s,u_s} = 0$, to express $(X_{n-s+1}, \ldots, X_n)$ as linear forms $(\phi_{n-s+1,\boldsymbol{u}}, \ldots, \phi_{n,\boldsymbol{u}})$ in $(X_1, \ldots, X_{n-s})$; this takes a total of $O(\gamma_1 \cdots \gamma_s n^3)$ operations in $\mathbf{K}$.

From this, we deduce a straight-line program $\Delta_{\boldsymbol{u}}$ that computes the entries of matrix $N_{\boldsymbol{u}}$ from (14): it simply consists in Δ, to which we add $O(n^2)$ operations that evaluate $(\phi_{n-s+1,\boldsymbol{u}}, \ldots, \phi_{n,\boldsymbol{u}})$. Given $\Delta_{\boldsymbol{u}}$, we can then apply Algorithm RowDegreeDiagonal to compute a zero-dimensional parametrization $\mathscr{R}'_{\boldsymbol{u}}$ of $V_p(N_{\boldsymbol{u}})$. The number of points c' in the output is $S_{n-s}(\alpha_1, \ldots, \alpha_p)$ (Corollary 33), so by Lemma 29, Algorithm RowDegreeDiagonal takes time

$$T = \sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_\kappa) \\ \kappa \le \min(n-s-1,p)}} \alpha_{i_1} \cdots \alpha_{i_\kappa} T_{M,\mathrm{row}}((\alpha_{i_1}, \ldots, \alpha_{i_\kappa}), n-s-1) + O^{\sim}(n^3 S_{n-s}(\alpha_1, \ldots, \alpha_p)). \quad (16)$$

Since there are $\gamma_1 \cdots \gamma_s$ choices of $\boldsymbol{u}$, the total cost is $\gamma_1 \cdots \gamma_s T$.

The next stage consists in adding to each $\mathscr{R}'_{\boldsymbol{u}}$, which involves only variables $(X_1, \ldots, X_{n-s})$, the expressions of $(X_{n-s+1}, \ldots, X_n)$ obtained from $(\phi_{n-s+1,\boldsymbol{u}}, \ldots, \phi_{n,\boldsymbol{u}})$. As in the analysis of Algorithm RowDegreeDiagonal, the total runtime is $O(\gamma_1 \cdots \gamma_s n^2 S_{n-s}(\alpha_1, \ldots, \alpha_p)) = O(n^2 c')$. Finally, we combine the resulting parametrizations $(\mathscr{R}_{\boldsymbol{u}})_{\boldsymbol{u}}$ into a single parametrization $\mathscr{R}$ using Chinese Remaindering, in time $O^{\sim}(\gamma_1 \cdots \gamma_s n S_{n-s}(\alpha_1, \ldots, \alpha_p)) = O^{\sim}(nc')$.

Altogether, the overall time spent in computing the zero-dimensional parametrization $\mathscr{R}$ of $V(\boldsymbol{A})$ is $\gamma_1 \cdots \gamma_s \sum_{\boldsymbol{i}=(i_1,\ldots,i_\kappa),\kappa \le \min(n-s-1,p)} \alpha_{i_1} \cdots \alpha_{i_\kappa} T_{M,\mathrm{row}}((\alpha_{i_1}, \ldots, \alpha_{i_\kappa}), n-s-1)$ $+O^{\sim}(n^3 c')$.

Property D_2. Next, we need to determine an upper bound e' on the degree of the curve $V(J')$, where J' is the union of the one-dimensional irreducible components of $V(\boldsymbol{B}) \subset \overline{\mathbf{K}}^{n+1}$ whose projection on the T-axis is dense. Proceeding exactly as in Section 5, we can take for e' the integer $(\gamma_1 + 1) \cdots (\gamma_s + 1) S_{n-s}(\alpha_1 + 1, \cdots, \alpha_p + 1)$.

Property D_3. Finally, we need to give an estimate on the size of a straight-line program that computes the polynomials $\boldsymbol{B} = (b_1, \ldots, b_m)$, assuming that we are given a straight-line Γ program of size σ that computes polynomials $G = (g_1, \ldots, g_s)$ and the entries of F. We already defined a straight-line program Δ of size σ_N that computes all entries of N; for an extra $O(\binom{q}{p} n^3)$ operations, we can compute all entries of $U = (1-T) \cdot N + T \cdot F$ and all p-minors $(b_{s+1}, \ldots, b_m)$ of this matrix. Adding an extra $O(n(\gamma_1 + \cdots + \gamma_s))$ operations, we can also compute all polynomials $(a_1, \ldots, a_s)$, and thus $(b_1, \ldots, b_s)$.

Altogether, we have obtained a straight-line program Γ' that computes $\boldsymbol{B} = (b_1, \ldots, b_m)$ using $\sigma' = \sigma + \sigma_N + O(\binom{q}{p} n^3 + n(\gamma_1 + \cdots + \gamma_s)) = \sigma + O(\binom{q}{p} n^3 + n^2(\alpha_1 + \cdots + \alpha_p) + n(\gamma_1 + \cdots + \gamma_s))$ operations.

Algorithm 4 RowDegree_simple(Γ)

Input: a straight-line program Γ of length σ that computes $F \in \mathbf{K}[X_1, \ldots, X_n]^{p\times q}$ with $\deg(f_{i,j}) \leq \alpha_i$ and $G = (g_1, \ldots, g_s)$ in $\mathbf{K}[X_1, \ldots, X_n]$ with $p \leq q$, $n = q - p + s + 1$
Output: a zero-dimensional parametrization of the isolated points of $V_p(F, G)$

1. construct a straight-line program Δ that computes $N \in \mathbf{K}[X_1, \ldots, X_n]^{p\times q}$ as in (10)
   Length of Δ is $O(n^2(\alpha_1 + \cdots + \alpha_p))$
2. for any sequence $\boldsymbol{u} = (u_1, \ldots, u_s)$, with $u_j \in \{1, \ldots, \gamma_j\}$ for all j
   (a) apply Gaussian elimination to the system of linear forms $\mu_{1,u_1} = \cdots = \mu_{s,u_s} = 0$ given at (13) to rewrite $(X_{n-s+1}, \ldots, X_n)$ as linear forms $(\phi_{\boldsymbol{u},k})_{n-s+1\leq k\leq n}$ in $(X_1, \ldots, X_{n-s})$
   Cost: $O(\gamma_1 \cdots \gamma_s n^3)$
   (b) construct a straight-line program $\Delta_{\boldsymbol{u}}$ that computes the matrix $N_{\boldsymbol{u}} \in \mathbf{K}[X_1, \ldots, X_{n-s}]^{p\times q}$ obtained by substituting $(\phi_{\boldsymbol{u},k})_{n-s+1\leq k\leq n}$ into N
   Length of $\Delta_{\boldsymbol{u}}$ is $O(n^2(\alpha_1 + \cdots + \alpha_p))$
   (c) $\mathscr{R}'_{\boldsymbol{u}} \leftarrow$ RowDegreeDiagonal($\Gamma_{\boldsymbol{u}}$) (points have coordinates $(X_1, \ldots, X_{n-s})$
   Cost: $O^{\sim}(\gamma_1 \cdots \gamma_s T)$, for T as in (16)
   (d) deduce $\mathscr{R}_{\boldsymbol{u}}$ from $\mathscr{R}'_{\boldsymbol{u}}$ by adding the expressions for $(X_{n-s+1}, \ldots, X_n)$
   Cost: $O(n^2 c')$, with $c' = \gamma_1 \cdots \gamma_s S_{n-s}(\alpha_1, \ldots, \alpha_p)$
3. combine all $\mathscr{R}_{\boldsymbol{u}}$ into $\mathscr{R}$
   Cost: $O^{\sim}(nc')$
4. construct a straight-line program Γ' that computes all polynomials $\boldsymbol{B}$
   Length of Γ' is $\sigma' = O(\sigma + \binom{q}{p} n^3 + n^2(\alpha_1 + \cdots + \alpha_p) + n(\gamma_1 + \cdots + \gamma_s))$
5. return Homotopy_simple($\Gamma', \mathscr{R}$)
   Cost: $O^{\sim}(c'(e' + c'^5)(\sigma + c'n^4))$, with $e' = (\gamma_1 + 1) \cdots (\gamma_s + 1) S_{n-s}(\alpha_1 + 1, \ldots, \alpha_p + 1)$

7.3 Cost analysis for RowDegree_simple

The algorithm RowDegree_simple that we deduce from the above discussion is given hereafter. We indicate the arithmetic costs for intermediate steps.

To estimate its complexity, we finally apply Proposition 10, which gives a runtime of $O^{\sim}(c'^2 mn^2 + c'e'(\sigma' m + n^2))$ operations in $\mathbf{K}$ for the cost of calling the homotopy subroutine at the last step of Algorithm RowDegree_simple. This runtime is dominated by

$$O^{\sim}\left(c' mn^2 (c' + e'\sigma')\right). \tag{17}$$

Recall that $\sigma' = \sigma + O(\binom{q}{p} n^3 + n^2(\alpha_1 + \cdots + \alpha_p) + n(\gamma_1 + \cdots + \gamma_s))$ and $s \leq n$. Letting $\alpha = \max(\alpha_1, \ldots, \alpha_p)$ and $\gamma = \max(\gamma_1, \ldots, \gamma_s)$, we obtain after some extra simplifications

$$\sigma' \leq \sigma + n^3 O\left(\binom{q}{p} + p\alpha + \gamma\right).$$

Plugging the above right hand side in (17), this bound can be simplified as

$$O^{\sim}\left(c' m n^2 (c' + e'(\sigma + n^3 \binom{q}{p} + p\alpha + \gamma))\right).$$

Using $m \leq n + \binom{q}{p}$, the above can be bounded by

$$O^{\sim}\left(c' n^3 \binom{q}{p}^2 (c' + e'(\sigma + n^3 + p\alpha + \gamma))\right).$$

To conclude, the total cost of the algorithm is

$$T_{\text{row}}(\sigma, \boldsymbol{\gamma}, \boldsymbol{\alpha}, q) = \gamma_1 \cdots \gamma_s T + O^{\sim}\left(c' n^6 \binom{q}{p}^2 (c' + e'(\sigma + p\alpha + \gamma))\right), \tag{18}$$

with T as in (16). This will now allow us to give an estimate on $T_{M,\text{row}}$ by solving a simple recurrence relation.

Lemma 34. *One can take* $T_{M,\text{row}}((\alpha_1, \ldots, \alpha_p), q) = O^{\sim}(u^2 \mu^4 \binom{q}{p}^2 (u + v(\mu q p \alpha + \mu^3 + \gamma)))$, *with* $\mu = q - p + 1$, $u = S_\mu(\alpha_1, \ldots, \alpha_p)$ *and* $v = S_\mu(\alpha_1 + 1, \ldots, \alpha_p + 1)$.

Proof. We apply the previous formula in the case where $s = 0$, so that $\gamma_1 \cdots \gamma_s = 1$, and for a $p \times q$ input matrix M as in (11). In this case, we can take $\sigma = O(\mu q(\alpha_1 + \cdots + \alpha_p))$; following our convention in the previous section, the runtime $T_{\text{row}}(\sigma, (), (\alpha_1, \ldots, \alpha_p), q)$ is then written $T_{M,\text{row}}((\alpha_1, \ldots, \alpha_p), q)$. Equation (18), combined with the definition of T in (16), gives the recursion

$$\begin{aligned} T_{M,\text{row}}((\alpha_1, \ldots, \alpha_p), q) = & \sum_{\substack{\boldsymbol{i} = (i_1, \ldots, i_\kappa) \\ \kappa \leq \min(\mu - 1, p)}} \alpha_{i_1} \cdots \alpha_{i_\kappa} T_{M,\text{row}}((\alpha_{i_1}, \ldots, \alpha_{i_\kappa}), \mu - 1) \\ & + O^{\sim}\Big(u \mu^3 \binom{q}{p}^2 (u + v(\mu q p \alpha + \mu^3 + \gamma))\Big), \quad \mu = q - p + 1, \end{aligned} \tag{19}$$

with $u = S_\mu(\alpha_1, \ldots, \alpha_p)$ and $v = S_\mu(\alpha_1 + 1, \ldots, \alpha_p + 1)$. The right-hand term $O^{\sim}(u \mu^3 \binom{q}{p}^2 (u + v(\mu q p \alpha + \mu^3 + \gamma)))$ is at its maximum at the root of the recursion tree. Thus, we can find an upper bound on $T_{M,\text{row}}$ by finding a solution to the recurrence

$$T_{M,\text{row}}((\alpha_1, \ldots, \alpha_p), q) = \sum_{\substack{\boldsymbol{i} = (i_1, \ldots, i_\kappa) \\ \kappa \leq \min(\mu - 1, p)}} \alpha_{i_1} \cdots \alpha_{i_\kappa} T_{M,\text{row}}((\alpha_{i_1}, \ldots, \alpha_{i_\kappa}), \mu - 1) + C, \tag{20}$$

for some constant C, and substituting $C = O\tilde{}(u\mu^3\binom{q}{p}^2(u + v(\mu qp\alpha + \mu^3 + \gamma)))$. Now, a quick induction shows that $T_{M,\mathrm{row}} = C\mu S_\mu(\alpha_1, \ldots, \alpha_p)$ is a solution of (20). As a result, $T_{M,\mathrm{row}} = O\tilde{}(u^2\mu^4\binom{q}{p}^2(u + v(\mu qp\alpha + \mu^3 + \gamma)))$ is a solution of (19). □

We can then take the expression given in this lemma, and combine it with the definition of T in (16) and the runtime analysis (18); this shows that

$$T_{\mathrm{row}}(\sigma, \boldsymbol{\gamma}, \boldsymbol{\alpha}, q) = O\tilde{}\left(c'^2 n^5 \binom{q}{p}^2 (c' + e'(nqp\alpha + n^3 + \gamma)) + c' n^6 \binom{q}{p}^2 (c' + e'(\sigma + p\alpha + \gamma))\right).$$

This can be simplified to

$$O\tilde{}\left(c'^2 n^6 \binom{q}{p}^2 (c' + e'(\sigma + nqp\alpha + \gamma + n^3))\right)$$

which establishes Proposition 31

7.4 Cost analysis for RowDegree

Algorithm RowDegree is similar to RowDegree_simple: the only difference consists in calling algorithm Homotopy on which Proposition 9 at the last step (5) (instead of Homotopy_simple.

Hence, reusing the notation of the previous Subsection, as well as the runtime estimate given in Proposition 9, the total cost of algorithm RowDegree is

$$\gamma_1 \cdots \gamma_s T + O\tilde{}\left(c'^5 mn^2 + c'(e' + c'^5 n)(\sigma' + n^3)\right), \tag{21}$$

where

- T is as in (16);
- $m \leq n + \binom{q}{p}$ and $s \leq n$;
- $\sigma' == \sigma + O(\binom{q}{p} n^3 + n^2(\alpha_1 + \cdots + \alpha_p) + n(\gamma_1 + \cdots + \gamma_s))$.

Reusing Lemma 34 for bounding T in (21), we obtain that the total cost of algorithm RowDegree can be bounded by

$$O\tilde{}\left(c'^2 n^5 \binom{q}{p}^2 (c' + e'(nqp\alpha + n^3 + \gamma)) + c'^5 n^3 \binom{q}{p} + c' n^2 (e' + c'^5 n)(\sigma + \binom{q}{p} n + p\alpha + \gamma + n)\right)$$

which can be simplified to

$$O\tilde{}\left(c'^2 n^5 \binom{q}{p}^2 (e' + c'^5 n)(\sigma + \binom{q}{p} n + nqp\alpha + \gamma + n^3)\right).$$

This finishes to establish Proposition 30.

8 Example

Let us consider an input matrix $F \in \mathbb{F}_{9001}[X_1, X_2, X_3, X_4]^{2\times 5}$ with the row degrees are $\mathrm{rdeg}(F, 1) = 2$ and $\mathrm{rdeg}(F, 2) = 1$. So, we can take

$$M = \begin{pmatrix} \lambda_{1,1} & 0 & \lambda_{1,3} & \lambda_{1,4} & \lambda_{1,5} \\ 0 & \lambda_{2,2} & \lambda_{2,3} & \lambda_{2,4} & \lambda_{2,5} \end{pmatrix},$$

with

$$\begin{cases} \lambda_{1,1} = (2079X_1 + 2631X_2 - 1908X_3 + 4492X_4 + 241)(-103X_1 - 869X_2 - 485X_3 - 4006X_4 - 835), \\ \lambda_{1,3} = (3809X_1 - 3674X_2 + 3848X_3 - 397X_4 - 1663)(-264X_1 - 3694X_2 - 1764X_3 - 1111X_4 - 2645) \\ \lambda_{1,4} = (3750X_1 - 4147X_2 - 3384X_3 - 2178X_4 + 3092)(-2090X_1 - 1844X_2 + 2266X_3 + 4180X_4 - 172) \\ \lambda_{1,5} = (-3003X_1 + 3278X_2 - 1133X_3 + 3421X_4 + 2777)(-2870X_1 - 3369X_2 - 3864X_3 + 3912X_4 + 532) \end{cases}$$

and

$$\begin{cases} \lambda_{2,2} = -1839X_2 - 3560X_3 + 1141X_4 + 3690 \\ \lambda_{2,3} = -654X_1 - 2801X_2 + 72X_3 + 3252X_4 - 3363 \\ \lambda_{2,4} = 4029X_1 + 326X_2 - 514X_3 - 1787X_4 - 4162 \\ \lambda_{2,5} = 4495X_1 - 1666X_2 + 3990X_3 - 2909X_4 - 3666 \end{cases}$$

as a start matrix.

The first case is $\lambda_{1,1} = \lambda_{1,3} = \lambda_{1,4} = \lambda_{1,5} = 0$ and the zero-dimesional parametrization is $\cdots$

Need to finish the example

The second case is $\lambda_{2,2} = \lambda_{2,3} = \lambda_{2,4} = \lambda_{2,5} = 0$ and the zero-dimesional parametrization is $\cdots$

The last case is $\lambda_{1,1} = \lambda_{2,2} = 0$ and the matrix B has rank deficient, where

$$B = \begin{pmatrix} \lambda_{1,3} & \lambda_{1,4} & \lambda_{1,5} \\ \lambda_{2,3} & \lambda_{2,4} & \lambda_{2,5} \end{pmatrix}$$

- $\begin{cases} 2079X_1 + 2631X_2 - 1908X_3 + 4492X_4 + 241 = 0 \\ -1839X_2 - 3560X_3 + 1141X_4 + 3690 = 0 \end{cases}$ and $\mathrm{rank}(B) < 2$:

  By writing X_1 and X_2 in the forms of X_3, X_4, X_5 and substituting them in the matrix B we obtain $C \in \mathbb{F}_{9001}[X_2, X_3]$ with

$$\begin{cases} c_{1,1} = 2362X_3^2 + 352X_3X_4 + 4302X_4^2 + 203X_3 + 3798X_4 + 1170, \\ c_{1,2} = -3760X_3^2 - 4011X_3X_4 + 4139X_4^2 + 3442X_3 - 3363X_4 + 226, \\ c_{1,3} = -1719X_3^2 + 1378X_3X_4 + 1140X_4^2 + 2830X_3 + 3331X_4 + 4203, \end{cases}$$

  and

$$\begin{cases} c_{2,1} = -697X_3 - 3413X_4 - 2204, \\ c_{2,2} = -1401X_3 - 1381X_4 + 3311, \\ c_{2,3} = 3220X_3 + 1772X_4 + 1665. \end{cases}$$

The row degrees of the matrix C are $\mathrm{rdeg}(C,1) = 2$ and $\mathrm{rdeg}(C,2) = 1$. In order to find the points in $\overline{\mathbf{K}}$, where $\mathbf{K} = \mathbb{F}_{9001}$, at which the evaluation of the matrix C has rank less than 2, we construct a start matrix

$$M_C = \begin{pmatrix} m_{1,1} & 0 & m_{1,3} \\ 0 & m_{2,2} & m_{2,3} \end{pmatrix} \in \mathbf{K}[X_3, X_4]^{2\times 3}$$

as

$$\begin{cases} m_{1,1} = (4327X_3 + 682X_4 + 3685)(-489X_3 + 3874X_4 - 4373), \\ m_{1,3} = (3186X_3 + 3803X_4 - 2837)(-3934X_3 + 3860X_4 + 3147), \end{cases}$$

and $\begin{cases} m_{2,2} = 2299X_3 - 2004X_4 - 1225, \\ m_{2,3} = 3005X_3 - 923X_4 - 3389. \end{cases}$

A zero-dimensional parametrization for the solutions of $m_{1,1} = m_{1,3} = 0$ is $\mathscr{R}_{0,1} = (t^4 - 1894t^3 - 909t^2 - 3055t + 2116, t, 809t^3 + 2084t^2 - 3753t - 2346)$, a zero-dimensional parametrization for the solutions of $m_{2,2} = m_{2,3} = 0$ is $\mathscr{R}_{0,2} = (t + 1766, t, 6934)$, while that of $m_{1,1} = m_{2,2} = 0$ is $\mathscr{R}_{0,3} = (t^2 - 882t - 2349, t, -2833t - 589)$.

A homotopy matrix is $U = (1 - T) \cdot M_C + T \cdot C$. After the lifting step, we obtain the zero-dimensional parametrizations of $V(I_C)$ are $\mathscr{R}_{1,1} = \cdots$, $\mathscr{R}_{1,2} = \cdots$ and $\mathscr{R}_{1,3} = \cdots$

References

[1] M. E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeroes, multiplicities and idempotents for zerodimensional systems. In *Algorithms in algebraic geometry and applications. Proceedings of MEGA'94*, volume 142 of *Progress in Mathematics*, pages 1–15. Birkhaüser, 1996.

[2] M. Atiyah and I. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley Series in Mathematics. Addison-Wesley, 1969.

[3] P. Aubry, F. Rouillier, and M. Safey El Din. Real solving for positive dimensional systems. *Journal of Symbolic Computation*, 34(6):543–560, 2002.

[4] B. Bank, M. Giusti, J. Heintz, G. Lecerf, G. Matera, and P. Solernó. Degeneracy loci and polynomial equation solving. *Foundations of Computational Mathematics*, 15(1):159–184, 2015.

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

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

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

[8] B. Bank, M. Giusti, J. Heintz, M. Safey El Din, and É. Schost. On the geometry of polar varieties. *Applicable Algebra in Engineering, Communication and Computing*, pages 33–83, 2010.

[9] S. Basu, M.-F. Roy, M. Safey El Din, and É. Schost. A baby-step giant-step roadmap algorithm for general real algebraic sets. *Foundations of Computational Mathematics*, 14(6):1117–1172, 2014.

[10] D. J. Bates, D. A. Brake, J. D. Hauenstein, A. J. Sommese, and C. W. Wampler. On computing a cell decomposition of a real surface containing infinitely many singularities. In *Mathematical software—ICMS 2014*, volume 8592 of *Lecture Notes in Comput. Sci.*, pages 246–252. Springer, Heidelberg, 2014.

[11] D. J. Bates, J. D. Hauenstein, C. Peterson, and A. J. Sommese. A numerical local dimension test for points on the solution set of a system of polynomial equations. *SIAM Journal on Numerical Analysis*, 47(5):3608–3623, 2009.

[12] D. J. Bates, J. D. Hauenstein, A. J. Sommese, and C. W. Wampler. *Numerically solving polynomial systems with Bertini*, volume 25 of *Software, Environments, and Tools*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2013.

[13] W. Baur and V. Strassen. The complexity of partial derivatives. *Theoretical Computer Science*, 22:317–330, 1983.

[14] G. M. Besana, S. Di Rocco, J. D. Hauenstein, A. J. Sommese, and C. W. Wampler. Cell decomposition of almost smooth real algebraic surfaces. *Numer. Algorithms*, 63(4):645–678, 2013.

[15] A. Bompadre, G. Matera, R. Wachenchauzer, and A. Waissbein. Polynomial equation solving by lifting procedures for ramified fibers. *Theoretical Computer Science*, 315(2):335 – 369, 2004.

[16] D. A. Brake, D. J. Bates, W. Hao, J. D. Hauenstein, A. J. Sommese, and C. W. Wampler. Algorithm 976: `{B}ertini_real`: numerical decomposition of real algebraic curves and surfaces. *ACM Trans. Math. Software*, 44(1):Art. 10, 30, 2017.

[17] A. Conca and J. Herzog. On the hilbert function of determinantal rings and their canonical module. *Proceedings of the American Mathematical Society*, 122(3):677–681, 1994.

[18] X. Dahan and É. Schost. Sharp estimates for triangular sets. In *ISSAC*, pages 103–110. ACM, 2004.

[19] J. Della Dora, C. Discrescenzo, and D. Duval. About a new method for computing in algebraic number fields. In *EUROCAL'85*, volume 204 of *LNCS*, pages 289–290. Springer, 1985.

[20] J. Eagon and D. Northcott. Ideals defined by matrices and a certain complex associated with them. *Proceedings of the Royal Society of London. Series A. Mathematical and Physical Sciences*, 269(1337):188–204, 1962.

[21] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, 1995.

[22] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Critical points and grÖbner bases: The unmixed case. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, ISSAC '12, pages 162–169, New York, NY, USA, 2012. ACM.

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

[24] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 2003.

[25] P. Gianni and T. Mora. Algebraic solution of systems of polynomial equations using Groebner bases. In *AAECC*, volume 356 of *LNCS*, pages 247–257. Springer, 1989.

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

[27] M. Giusti, J. Heintz, J.-E. Morais, and L.-M. Pardo. When polynomial equation systems can be solved fast? In *AAECC-11*, volume 948 of *LNCS*, pages 205–231. Springer, 1995.

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

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

[30] F. Guo, M. Safey El Din, and L. Zhi. Global optimization of polynomials using generalized critical values and sums of squares. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, ISSAC '10, pages 107–114, New York, NY, USA, 2010. ACM.

[31] J. D. Hauenstein. Numerically computing real points on algebraic sets. *Acta Appl. Math.*, 125:105–119, 2013.

[32] J. Heintz, G. Jeronimo, J. Sabia, and P. Solerno. Intersection theory and deformation algorithms: the multi-homogeneous case, 2002.

[33] J. Heintz, T. Krick, S. Puddu, J. Sabia, and A. Waissbein. Deformation techniques for efficient polynomial equation solving. *Journal of Complexity*, 16(1):70–109, 2000.

[34] M. I. Herrero, G. Jeronimo, and J. Sabia. Computing isolated roots of sparse polynomial systems in affine space. *Theoretical Computer Science*, 411(44):3894 – 3904, 2010.

[35] M. I. Herrero, G. Jeronimo, and J. Sabia. Affine solution sets of sparse polynomial systems. *Journal of Symbolic Computation*, 51:34 – 54, 2013.

[36] M. I. Herrero, G. Jeronimo, and J. Sabia. Elimination for generic sparse polynomial systems. *Discrete & Computational Geometry*, 51(3):578–599, 2014.

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

[38] G. Jeronimo and D. Perrucci. A probabilistic symbolic algorithm to find the minimum of a polynomial function on a basic closed semialgebraic set. *Discrete & Computational Geometry*, 52(2):260–277, 2014.

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

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

[41] H. Matsumura. *Commutative Ring Theory*. Cambridge studies in advanced mathematics. Cambridge University Press, 1986.

[42] E. Miller and B. Sturmfels. *Combinatorial Commutative Algebra*. Springer Verlag, New York, 2005.

[43] B. Mourrain. Isolated points, duality and residues. *Journal of Pure and Applied Algebra*, 117/118:469–493, 1997. Algorithms for algebra (Eindhoven, 1996).

[44] J. Nie, J. Demmel, and B. Sturmfels. Minimizing polynomials via sum of squares over the gradient ideal. *Mathematical programming*, 106(3):587–606, 2006.

[45] J. Nie and K. Ranestad. Algebraic degree of polynomial optimization. *SIAM J. on Optimization*, 20(1):485–502, April 2009.

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

[47] F. Rouillier, M.-F. Roy, and M. Safey El Din. Finding at least one point in each connected component of a re al algebraic set defined by a single equation. *Journal of Complexity*, 16:716–750, 2000.

[48] M. Safey El Din and É. Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In *ISSAC'03*, pages 224–231. ACM, 2003.

[49] M. Safey El Din and É. Schost. A baby steps/giant steps probabilistic algorithm for computing roadmaps in smooth bounded real hypersurface. *Discrete and Computational Geometry*, 45(1):181–220, 2011.

[50] M. Safey El Din and É. Schost. Bit complexity for multi-homogeneous polynomial system solving application to polynomial minimization. *Journal of Symbolic Computation*, 2017.

[51] M. Safey El Din and É. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *J. ACM*, 63(6):48:1–48:37, January 2017.

[52] M. Safey El Din and P.-J. Spaenlehauer. Critical point computations on smooth varieties: Degree and complexity bounds. In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '16, pages 183–190, New York, NY, USA, 2016. ACM.

[53] É. Schost. Computing parametric geometric resolutions. *Appl. Algebra Engrg. Comm. Comput.*, 13(5):349–393, 2003.

[54] I. Shafarevich. *Basic Algebraic Geometry 1.* Springer Verlag, 1977.

[55] M. Shub and S. fSSmale. Complexity of bezout's theorem i: Geometric aspects. *Journal of the American Mathematical Society*, 6(2):459–501, 1993.

[56] A. J. Sommese and C. W. Wampler. *The numerical solution of systems of polynomials arising in engineering and science.* World Scientific, 2005.

[57] P.-J. Spaenlehauer. On the complexity of computing critical points with Gröbner bases. *SIAM Journal on Optimization*, 24(3):1382–1401, 2014.

[58] O. Zariski and P. Samuel. *Commutative Algebra.* Van Nostrand, 1958.