Intersection theory and deformation algorithms: the multi-homogeneous case (Draft)

G. Jeronimo, J. Heintz, J. Sabia, P. Solernó

Contents

1 Homogeneous Bezout Theorem by deformation techniques

1.1 Notations

Let K be a field and let $\overline{K}$ be an algebraic closure of K, let n be a natural number, $x_0, \ldots, x_n$ a set of indeterminates over K and $d_1, \ldots, d_n$ positive integers.

For any non negative integer d we denote by Λ_d the set of non negative integer vectors $\alpha := (\alpha_0, \ldots, \alpha_n)$, such that $|\alpha| = d$, where $|\alpha|$ denotes the vector size $\alpha_0 + \cdots + \alpha_n$. We have $\#(\Lambda_d) = \binom{n+d}{n}$.
Let $A_\alpha^{(i)}$ be new indeterminates, where α runs on the set Λ_{d_i} and $1 \leq i \leq n$.

For the sake of simplicity we introduce the following notations:

- $X := (x_0, \ldots, x_n)$,
- $X^\alpha := x_0^{\alpha_0} x_1^{\alpha_1} \ldots x_n^{\alpha_n}$,
- $A^{(i)} := (A_\alpha^{(i)})_{\alpha \in \Lambda_{d_i}}$,
- $A := (A^{(i)})_{1 \leq i \leq n}$,
- $N := \sum_{i=1}^{n} \binom{n+d_i}{n}$,
- $\mathbb{A}^n := \mathbb{A}^n_{\overline{K}}$ (the affine space over $\overline{K}$) and $\mathbb{P}^n := \mathbb{P}^n_{\overline{K}}$ (the projective space over $\overline{K}$).

Let us consider generic homogeneous polynomial $F_1, \ldots, F_n \in K[A][X]$ of total degrees (in the variables X) respectively $d_1, \ldots, d_n$, defined as

$$F_i := \sum_{\alpha \in \Lambda_{d_i}} A_\alpha^{(i)} X^\alpha, \qquad \text{with } 1 \leq i \leq n.$$

1.2 Homogeneous generic Bezout Theorem

Interpreting the variables A in the polynomials F_i introduced above as coefficients lying in a ground field $K(A)$, the zeros of these polynomials define a 0-dimensional $K(A)$-variety $V \subset \mathbb{P}^n_{\overline{K(A)}}$.
The classical Bezout Theorem for generic homogeneous polynomials states that the cardinality (or degree) of the variety V is exactly the product $d_1 \ldots d_n$.
In this section we will show how this well known theorem may be obtained by means of a simple deformation procedure.

First let us observe that the genericity of the polynomials F_i implies that V does not contain points lying in the infinity-hyperplane $\{x_0 = 0\}$. Therefore, V may be considered as an affine variety contained in $\mathbb{A}^n_{\overline{K(A)}}$, defined by generic n-variate polynomials $f_1, \ldots, f_n \in K[A][x_1, \ldots, x_n]$, where $f_i := F_i(1, x_1, \ldots, x_n)$, for $i = 1, \ldots, n$.

On the other hand one may also consider the polynomials f_i as polynomials in all the variables A and $x_1, \ldots, x_n$, defining a N-dimensional K-variety $\mathcal{V} \subset \mathbb{A}^N \times \mathbb{A}^n$ (the so called "incidence variety").
Denote by $\pi : \mathcal{V} \to \mathbb{A}^N$ the canonical projection $\pi(a, x) := a$. This morphism is dominating (i.e. the Zariski closure of its image is $\mathbb{A}^N$) and induces the canonical ring inclusion $K[A] \hookrightarrow K[\mathcal{V}]$, where $K[\mathcal{V}] := K[A][x_1, \ldots, x_n]/(f_1, \ldots, f_n)$ is the ring of coordinates of the affine variety $\mathcal{V}$.
For any index i, $1 \leq i \leq n$, consider those variables $A_\alpha^{(i)}$ where α verifies that there exists an index $j \neq 0, i$ such that x_j divides X^α.
Running the index i between 1 and n, these variables generate a monomial prime ideal $\wp \subset K[A]$ which verifies:

$$F_i \equiv G_i(x_0, x_i) \qquad \mod \wp, \tag{1}$$

where $G_i \in K[A][x_0, x_1]$ is a generic homogeneous polynomial of degree d_i involving only the variables x_0 and x_i and its coefficients are independent variables which don't belong to the prime ideal $\wp$.

Let $Z \subset \mathbb{A}^N$ be the algebraic variety (in fact, a linear subspace) defined by the ideal $\wp$.

With these assumptions and notations the morphism π is generically finite in a Zariski neighbourhood of the fiber $\pi^{-1}(Z)$. This is a consequence of the following algebraic fact:

Lemma 1 *The canonical monomorphism $K[A]_\wp \hookrightarrow K[A]_\wp[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$ is an integral ring extension.*

Proof. Consider the "triangular" sequence of homogeneous polynomials $R_j^{(i)} \in K[A, X]$, with $0 \leq i \leq n-1$ and $i+1 \leq j \leq n$, recursively defined as follows:

- $R_j^{(0)} := F_j$, for $j = 1, \ldots, n$
- $R_j^{(1)} := \mathrm{Res}_{x_1}(R_1^{(0)}, R_j^{(0)})$, for $j = 2, \ldots, n$.
- $R_j^{(i)} := \mathrm{Res}_{x_i}(R_i^{(i-1)}, R_j^{(i-1)})$, for $2 \leq i \leq n-1$ and $j = i+1, \ldots, n$.

From elementary properties of the resultant we conclude that each $R_j^{(i)}$ is a homogeneous polynomial in $K[A][x_0, x_{i+1}, \ldots, x_n]$ which belongs to the ideal $(F_1, \ldots, F_n)$. In particular $R_n^{(n-1)}$ belongs to $(F_1, \ldots, F_n) \cap K[A][x_0, x_n]$.
Moreover, taking into account the matricial construction and the homogeneity of the resultant, from the modular relation (1), it follows by a straightforward recursive argument that the coefficient of the only monomial pure in x_j appearing in $R_j^{(j-1)}$ is an invertible element of the local ring $K[A]_\wp$, for $j = 1, \ldots, n$.
In particular, the polynomial $R_n^{(n-1)}(1, x_n)$ gives an integral dependence equation for the class of x_n in the ring $K[A]_\wp[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$ over the ring $K[A]_\wp$.
Clearly this procedure may be applied mutatis mutandis in order to provide integral dependence equations for the class of any variable x_i, $i = 1, \ldots, n$, modulo the ideal $(f_1, \ldots, f_n)K[A]_\wp[x_1, \ldots, x_n]$, and so the lemma follows. ■

Denote by $\mathbb{L}$ the fraction field of the integral domain $K[A]/\wp$ (or equivalently the residue field of the local ring $K[A]_\wp$) and set $g_i := G_i(1, x_i)$ (see formula (1) for the definition of the polynomials G_i).
Since each polynomials g_i is a generic polynomial of degree d_i, we conclude

$$\dim_{\mathbb{L}} \mathbb{L}[x_1, \ldots, x_n]/(g_1, \ldots, g_n) = d_1 \ldots d_n. \tag{2}$$

Corollary 2 *The ring $K[A]_\wp[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$ is a free $K[A]_\wp$-module with rank $d_1 \ldots d_n$.*

Proof. The freeness follows directly from [2, Corollary 18.17], as well as from the proof of [6, Prop.2] (in fact we may also show that the ring extension is monogenerated).
The computation of the rank is an immediate consequence of the preservation of the rank of free modules under tensorial product: if we denote $\mathcal{O}$ for the local ring $K[A]_\wp$, tensoring by $\mathcal{O}/\wp$ we have

$$\mathrm{rank}_{\mathcal{O}} \mathcal{O}[x_1, \ldots, x_n]/(f_1, \ldots, f_n) = \mathrm{rank}_{\mathcal{O}/\wp} \mathcal{O}[x_1, \ldots, x_n]/\wp + (f_1, \ldots, f_n).$$

The corollary follows from (2) since $\mathcal{O}/\wp = \mathbb{L}$ and $f_i \equiv g_i \mod \wp$. ■

With these notations we deduce:

Theorem 3 *(Generic homogeneous Bezout Theorem)*

$$\#(V) = d_1 \dots d_n.$$

Proof. Since the ideal $(f_1, \dots f_n) \subset K[A][x_1, \dots, x_n]$ is a radical ideal, in order to compute the number of points of V it suffices to calculate the dimension of $K(A)[x_1, \dots, x_n]/(f_1, \dots f_n)$ as a $K(A)$-vector space.
In fact this vector space is a localization of the algebra $K[A]_\wp[x_1, \dots, x_n]/(f_1, \dots, f_n)$ on the multiplicative set $K[A]_\wp \setminus \{0\}$ and then, from the previous corollary, we have:

$$\dim_{K(A)} K(A)[x_1, \dots, x_n]/(f_1, \dots, f_n) = \operatorname{rank}_{K[A]_\wp} K[A]_\wp[x_1, \dots, x_n]/(f_1, \dots, f_n) =$$

$$= d_1 \dots d_n.$$

■

The previous algebraic arguments may be easily translated to a more geometrical frame.
The closed subvariety $Z \subset \mathbb{A}^N$ defined by the ideal $\wp$ verifies that the projection $\pi : \mathcal{V} \to \mathbb{A}^N$ is a finite morphism locally in a Zariski neighbourhood of $\pi^{-1}(Z)$ (Lemma 1). Moreover, the fiber of a generic point of Z is 0-dimensional and its cardinality is equal to the cardinality of the fiber over a generic point of $\mathbb{A}^N$. In other words, the typical fiber of a point lying in the closed set Z has the same cardinality $d_1 \dots d_n$ than the typical fiber of the morphism π (Theorem 3).

The freeness stated in Corollary 2 may be interpreted as a flat deformation of the typical fiber over Z onto the typical fiber of a generic point of $\mathbb{A}^N$.

1.3 Algorithmic resolution of generic systems

In this section we show how the deformation introduced above is closely related with an algorithm for the resolution of generic polynomial equation systems by means of a Newton procedure (see also [14]).

We maintain the same notations introduced in the previous sections.

For every coefficient selection $a \in \mathbb{A}^N$, the fiber $\pi^{-1}(a)$ is geometrically described by the equations:

$$f_1(a, x) = 0, \dots, f_n(a, x) = 0. \tag{3}$$

Corollary 2 and Theorem 3 state that for a point a generically chosen in the proper closed set Z or in the whole ambient space $\mathbb{A}^N$, the equation system (3) has exactly $d_1 \dots d_n$ different solutions in $\mathbb{A}^n$.

Definition 4 *A point $a \in \mathbb{A}^N$ is called a lifting point for the generic system $\{f_1 = 0, \dots, f_n = 0\}$ if the following two conditions are fulfilled:*

1. *The fiber $\pi^{-1}(a)$ is finite and consists in $d_1 \dots d_n$ many points (in other words the fiber has maximal -or typical- cardinality).*
2. *The point a is not a ramification point of π, namely the Jacobian matrix $\left(\dfrac{\partial f_i}{\partial x_j}(a, x)\right)_{1 \le i,j \le n}$ is invertible for any point (a, x) lying in the fiber $\pi^{-1}(a)$.*

Example 5 *Let us observe that a point $a \in \mathbb{A}^N$ with maximal fiber is a lifting point if and only if the fiber $\pi^{-1}(a)$ is reduced (or equivalently non singular) in the scheme language. In particular, a generic point $a \in \mathbb{A}^N$ is a lifting point for π (see also [14]).*

Example 6 *A similar observation holds for a generic point of the closed proper irreducible subset $Z \subset \mathbb{A}^N$. Moreover, a point $a \in Z$ is a lifting point for π if and only if condition (1) of Definition 4 is satisfied. In order to prove this, consider a point $a \in Z$ such that $\#\pi^{-1}(a) = d_1 \ldots d_n$. Since $a \in Z$, this fiber consists in the zeros of the the univariate polynomials in separated variables $G_1(a, 1, x_1), \ldots, G_n(a, 1, x_n)$ (see formula (1) for the definition of the polynomials G_i). Since $\deg_{x_i} G_i(a, 1, x_i)$ is bounded by d_i for all $i = 1, \ldots, n$, we infer that each polynomial $G_i(a, 1, x_i)$ is square-free of degree exactly d_i. Then the Jacobian matrix is a diagonal invertible matrix for any point (a, x) in $\pi^{-1}(a)$.*

Example 7 *Suppose that the characteristic of the ground field K is 0. Let $a \in \mathbb{A}^N$ be the point associated to the coefficients of the homogeneous polynomials*

$$x_1^{d_1} - x_0^{d_1},\ x_2^{d_2} - x_0^{d_2}, \ldots, x_n^{d_n} - x_0^{d_n}. \tag{4}$$

Let us observe that the point a belongs to the subvariety Z.
If we denote $\mathbb{G}_m$ the group of the m-th roots of the unity we have $\pi^{-1}(a) = \mathbb{G}_{d_1} \times \cdots \times \mathbb{G}_{d_n}$. In particular $\#\pi^{-1}(a) = d_1 \ldots d_n$ and so Example 6 implies that the point a is a lifting point for π.

It is well known that the lifting points play a main role as start points in order to approximate solutions (in the numerical case) or to deformate continuously solutions (in the symbolic or seminumerical case) by means of suitable Newton procedures.
In fact the arguments to find generic resolutions of parametrized systems of [14] (see also [7] or [11]), slightly modified, allow to show that the solutions of any particular instance

$$f_1(b, x) = 0, \ldots, f_n(b, x) = 0 \tag{5}$$

having exactly $d_1 \ldots d_n$ many solutions can be obtained algorithmically by a homotopic deformation of the solutions of the system (3) defined by a lifting point a at start point.

In our case, we are able to show a more precise result: suppose that the particular instance (5) defines a positive dimensional set having exactly s many isolated solutions (the 0-dimensional components), with $s \geq 0$. The proof of [6, Prop.1] shows that s is bounded by the cardinal of the 0-dimensional typical fiber, $d_1 \ldots d_n$ in our situation.
We construct an algorithm which computes a solution set of the system (5) of certain cardinality t, with $s \leq t \leq d_1 \ldots d_n$, containing all the isolated solutions.

The construction of the algorithm may be sketched as follows:

- The first main step consists in compute a generic resolution following closely [14]. We take a "simple" fixed lifting point $a \in Z \subset \mathbb{A}^N$ (for instance the lifting point considered in Example 7) and a generic linear form $L \in K[x_1, \ldots, X_n]$. Applying a truncated Newton approximation operator and a probabilistic version of Padé approximants, we compute the minimal polynomial $P \in K(A)[T]$ (where T denotes a new indeterminate) of the class of L in $K(A)[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$ over the field $K(A)$.

- Let $b \in \mathbb{A}^N$ be the coefficient point associated to the particular instance (5). A carefull evaluation of the coefficients of P in the point b (using a L'Hopital-like argument to avoid eventual indeterminations), allows to compute a new non zero polynomial $P^{(b)} \in K[T]$ such that $P^{(b)}(L(z)) = 0$ for all isolated solution z of (5).

- Finally, since the constructions in the previous steps depend polynomially on the coefficients of the generic linear form L, a well-known argument based on the chain rule for the derivatives of a composition (see for instance [5]) gives a geometric description of a finite solution set of the system (5) containing all the isolated points z.

Since these arguments will be described carefully in a very similar context in Section 3 (for the bihomogeneous case), we omit here the details and the complexity estimations of this procedure. The precise result is summarized in the following:

Theorem 8 *Homogeneous resolution....*

2 Flat deformations and bihomogeneous Bezout Theorem

2.1 Some notations

Let K be a field and let $\overline{K}$ be an algebraic closure of K.
Let $n, m \in \mathbb{N}$ and denote by $K[x_0, \ldots, x_n, y_0, \ldots, y_m]$ the polynomial ring in the indeterminates $x_0, \ldots, x_n, y_0, \ldots, y_m$. For the sake of simplicity we write $X := (x_0, \ldots, x_n)$ and $Y := (y_0, \ldots, y_m)$. For each $e, d \in \mathbb{N}_0$ we denote by $\Lambda_{d,e} \subset \mathbb{N}_0^{n+1} \times \mathbb{N}_0^{m+1}$ the set defined as follows: $(\alpha, \beta) \in \Lambda_{d,e}$ if and only if $|\alpha| = d$ and $|\beta| = e$ (where $|\alpha| := \alpha_0 + \cdots + \alpha_n$ and $|\beta| := \beta_0 + \cdots + \beta_m$).

Let us consider a finite sequence $(d_1, e_1), \ldots, (d_{n+m}, e_{n+m})$ in $\mathbb{N}_0 \times \mathbb{N}_0$ and introduce $\sum_{i=1}^{n+m} \sharp(\Lambda_{d_i,e_i})$ many new indeterminates over $K[x_0, \ldots, x_n, y_0, \ldots, y_m]$ which will be denoted by $A_{\alpha\beta}^{(i)}$, where $1 \leq i \leq n+m$ and $(\alpha, \beta) \in \Lambda_{d_i,e_i}$. Finally denote by $A := \left(A_{\alpha\beta}^{(i)}\right)_{\substack{1 \leq i \leq n+m \\ (\alpha,\beta) \in \Lambda_{d_i,e_i}}}$.

In other words, if we consider the polynomials $F_1, \ldots, F_{n+m} \in K[A][x_0, \ldots, x_n, y_0, \ldots, y_m]$ defined as

$$F_i := \sum_{(\alpha,\beta) \in \Lambda_{d_i,e_i}} A_{\alpha\beta}^{(i)} X^\alpha Y^\beta, \qquad i = 1, \ldots, n+m$$

(X^α and Y^β are the standard notations for the monomials $x_0^{\alpha_0} \ldots x_n^{\alpha_n}$ and $y_0^{\beta_0} \ldots y_m^{\beta_m}$ respectively), they are K-generic bihomogeneous polynomials such that $\deg_X(F_i) = d_i$ and $\deg_Y(F_i) = e_i$.
In particular, the polynomials $F_1, \ldots, F_{n+m}$ are a regular sequence of $K[A][x_0, \ldots, x_n, y_0, \ldots, y_m]$ and define a reduced 0-dimensional subvariety V of the product space $\mathbb{P}^n_{\overline{K(A)}} \times \mathbb{P}^m_{\overline{K(A)}}$ where $\overline{K(A)}$ is an algebraic closure of the field $K(A)$.

The classical Multihomogeneous Bezout Theorem (which follows from the intersection theory for divisors) states that $\deg(V) = \sum d_{j_1} \ldots d_{j_n} e_{k_1} \ldots e_{k_m}$, where the sum is taken over all that indices satisfying the conditions

- $1 \leq j_1 < \cdots < j_n \leq n+m$
- $1 \leq k_1 < \cdots < k_m \leq n+m$
- $\{j_1, \ldots, j_n\} \cap \{k_1, \ldots, k_m\} = \emptyset$

The following sections are devoted to show how this result can be obtained by means of an elementary flat deformation.

2.2 The deformation

Following the notations introduced above, let us fix an index i, $1 \leq i \leq n+m$.
Denote by $A^{(i)}$ the set of the indeterminates $\left(A_{\alpha\beta}^{(i)}\right)_{(\alpha,\beta) \in \Lambda_{d_i,e_i}}$ (in other words the "coefficient indeterminates" occurring in the polynomial F_i).
Finally we call $N_i := \binom{n+d_i}{n}$ and $M_i = \binom{m+e_i}{m}$.

Consider the morphism $\mu : \mathbb{A}_K^{N_i} \times \mathbb{A}_K^{M_i} \to \mathbb{A}_K^{N_i M_i}$ defined as

$$\left((b_\alpha)_{|\alpha|=d_i}, (c_\beta)_{|\beta|=e_i} \right) \mapsto (b_\alpha c_\beta)_{\substack{|\alpha|=d_i \\ |\beta|=e_i}}.$$

Roughly speaking, the image of μ describe all the possible specialisations of the variables $A^{(i)}$ such that the corresponding generic polynomial F_i becomes a variable-separated reducible polynomial. More precisely:

Remark 9 A point $\left(a^{(i)}\right) \in \mathbb{A}_K^{N_i M_i}$ belongs to $\mathrm{Im}\,(\mu)$ if and only if

$$F_i\left(a^{(i)}, X, Y\right) = \Big(\sum_{|\alpha|=d_i} b_\alpha X^\alpha \Big) \Big(\sum_{|\beta|=e_i} c_\beta Y^\beta \Big)$$

for suitable $(b_\alpha) \in \mathbb{A}_K^{N_i}$ and $(c_\beta) \in \mathbb{A}_K^{M_i}$.

Moreover we have:

Proposition 10 *The image $\mu\left(\mathbb{A}_K^{N_i} \times \mathbb{A}_K^{M_i}\right)$ is a closed affine algebraic variety Z_i given by the (homogeneous) prime ideal $\wp_i \subset K[A^{(i)}]$ generated by the elements $A^{(i)}_{\alpha\beta} A^{(i)}_{\alpha'\beta'} - A^{(i)}_{\alpha'\beta} A^{(i)}_{\alpha\beta'}$ where (α, β) and (α', β') run over all the pairs in Λ_{d_i, e_i}.* ■

We write $\overline{A^{(i)}}$ for the class of the coordinate functions of the affine ring $K[A^{(i)}]$ modulo the ideal $\wp_i$. Then we have:

Proposition 11 *Fix a multi-index $\beta_0 \in \mathbb{N}_0^{m+1}$ such that $|\beta_0| = e_i$. Then the elements $\overline{A^{(i)}_{\alpha\beta_0}} \in K[\overline{A^{(i)}}]$ (where $\alpha \in \mathbb{N}_0^{n+1}$ runs over all the multi-indices with $|\alpha| = d_i$) are algebraically independent over K.*

Proof. Suppose that there exists a polynomial relation Q with coefficients in K such that $Q\left(\overline{A^{(i)}_{\alpha\beta_0}}\right) \in \wp_i$. Therefore we have a formula of the type

$$Q\left(A^{(i)}_{\alpha\beta_0}\right) = \sum_{\alpha_1, \beta_1, \alpha_2, \beta_2} P_{\alpha_1\beta_1\alpha_2\beta_2} \left(A^{(i)}_{\alpha_1\beta_1} A^{(i)}_{\alpha_2\beta_2} - A^{(i)}_{\alpha_2\beta_1} A^{(i)}_{\alpha_1\beta_2} \right)$$

with $P_{\alpha_1\beta_1\alpha_2\beta_2} \in K[A^{(i)}]$.
As the elements $A^{(i)}$ are algebraically independent over K, we can specialise $A^{(i)}_{\alpha\beta} \longmapsto 0$ for all $\beta \neq \beta_0$ and we conclude that

$$Q\left(A^{(i)}_{\alpha\beta_0}\right) = \sum_{\alpha_1, \alpha_2} \widetilde{P}_{\alpha_1\beta_0\alpha_2\beta_0} \left(A^{(i)}_{\alpha_1\beta_0} A^{(i)}_{\alpha_2\beta_0} - A^{(i)}_{\alpha_2\beta_0} A^{(i)}_{\alpha_1\beta_0} \right) = 0.$$

Since the elements $A^{(i)}_{\alpha\beta_0}$ are algebraically independent over K we deduce $Q = 0$. ■

We may also consider the point $\overline{A^{(i)}}$ as a point with $N_i M_i$ many coordinates.
From this point of view, $\overline{A^{(i)}}$ is the generic point of the irreducible variety Z_i (in the van der Waerden's sense) and verifies the equations defining $\wp_i$.

Let us observe that Proposition 11 implies that $\overline{A^{(i)}_{\alpha\beta}} \neq 0$ for all $(\alpha, \beta) \in \Lambda_{d_i, e_i}$. Therefore we have:

Remark 12 *Fix a pair $(\alpha_0, \beta_0) \in \Lambda_{d_i,e_i}$. Then the identity*

$$F_i\left(\overline{A^{(i)}}, X, Y\right) = \left(\sum_{|\alpha|=d_i} \overline{A^{(i)}_{\alpha\beta_0}} X^\alpha\right)\left(\sum_{|\beta|=e_i} \frac{\overline{A^{(i)}_{\alpha_0\beta}}}{\overline{A^{(i)}_{\alpha_0\beta_0}}} Y^\beta\right) \tag{6}$$

holds in $K(\overline{A^{(i)}})[X, Y]$.

Definition 13 *For any index i, $1 \le i \le n+m$, we fix a multi-index $(\alpha_0, \beta_0) \in \Lambda_{d_i,e_i}$. We define the following polynomials in $K[\overline{A^{(i)}}][X, Y]$:*

$$\Phi_i^{(X)} := \sum_{|\alpha|=d_i} \overline{A^{(i)}_{\alpha\beta_0}} X^\alpha \qquad \text{and} \qquad \Phi_i^{(Y)} := \sum_{|\beta|=e_i} \overline{A^{(i)}_{\alpha_0\beta}} Y^\beta.$$

From the formula (6) we observe that the identity

$$\overline{A^{(i)}_{\alpha_0\beta_0}} F_i\left(\overline{A^{(i)}}, X, Y\right) = \Phi_i^{(X)}\ \Phi_i^{(Y)} \tag{7}$$

holds in $K[\overline{A^{(i)}}][X, Y]$.

Notation 14 *Let $\wp$ be the ideal in $K[A]$ defined as $\wp := \wp_1 + \cdots + \wp_{n+m}$. Clearly the ideal $\wp$ is a prime ideal defining the irreducible variety $Z := Z_1 \times \cdots \times Z_{n+m} \subset \mathbb{A}^{N_1 M_1} \times \cdots \times \mathbb{A}^{N_{n+m} M_{n+m}}$. Denote by $\mathbb{F}$ an algebraic closure of the field $K(\overline{A})$, the quotient field of the coordinate ring of Z.*

Using this notation, from Proposition 11 we deduce:

Lemma 15 *The polynomials $\Phi_1^{(X)}, \ldots, \Phi_{n+m}^{(X)} \in K[\overline{A}][X]$ are generic (the same holds for the polynomials $\Phi_1^{(Y)}, \ldots, \Phi_{n+m}^{(Y)} \in K[\overline{A}][Y]$).*

Proof. From Proposition 11 the coefficients of the polynomials $\Phi_j^{(X)}$ are algebraically independent over K. Therefore all the coefficients of the polynomials $\Phi_1^{(X)}, \ldots, \Phi_{n+m}^{(X)}$ form an algebraically free family. ■

Corollary 16 *Let $1 \le j_1 < j_2 < \cdots < j_n \le n+m$, and $1 \le k_1 < k_2 < \cdots < k_m \le n+m$ be such that $\{j_1, j_2, \cdots, j_n\} \cap \{k_1, k_2, \cdots, k_m\} = \emptyset$. Then:*

1. *$\left\{\Phi_{j_1}^{(X)}, \ldots, \Phi_{j_n}^{(X)}, \Phi_{k_1}^{(Y)}, \ldots, \Phi_{k_m}^{(Y)}\right\}$ is a regular sequence in $\mathbb{F}[X, Y]$.*
2. *No point at the hyperplane of infinity is contained in the varieties defined by these polynomials. More precisely:*

$$\left\{\Phi_{j_1}^{(X)} = 0, \ldots, \Phi_{j_n}^{(X)} = 0\right\} \cap \{x_0 = 0\} = \emptyset$$
$$\left\{\Phi_{k_1}^{(Y)} = 0, \ldots, \Phi_{k_m}^{(Y)} = 0\right\} \cap \{y_0 = 0\} = \emptyset.$$

3. *The ideal $\left(\Phi_{j_1}^{(X)}, \ldots, \Phi_{j_n}^{(X)}, \Phi_{k_1}^{(Y)}, \ldots, \Phi_{k_m}^{(Y)}\right) \subset \mathbb{F}[X, Y]$ is a radical homogeneous ideal defining a 0-dimensional smooth projective variety of degree $d_{j_1} \cdots d_{j_n} e_{k_1} \cdots e_{k_m}$.*

Proof. Since the polynomials $\Phi_{j_1}^{(X)}, \ldots, \Phi_{j_n}^{(X)}$ (respectively the polynomials $\Phi_{k_1}^{(Y)}, \ldots, \Phi_{k_m}^{(Y)}$) involve only the variables X (respectively the variables Y) the three items follow directly from Lemma 15. ■

For each $1 \le i \le n+m$ we denote by $\varphi_i^{(X)}$ and $\varphi_i^{(Y)}$ the affinized of the homogeneous polynomials $\Phi_i^{(X)}$ and $\Phi_i^{(Y)}$ putting $x_0 = 1$ and $y_0 = 1$ respectively.

Corollary 17 *The ideal* $\left(\varphi_1^{(X)}\varphi_1^{(Y)},\ldots,\varphi_{n+m}^{(X)}\varphi_{n+m}^{(Y)}\right)\subset K(\overline{A})\left[x_1,\ldots,x_n,y_1,\ldots,y_m\right]$ *is a* 0*-dimensional smooth (radical) ideal.*

Proof. Let $\mathcal{M}\subset K(\overline{A})\left[x_1,\ldots,x_n,y_1,\ldots,y_m\right]$ be a prime ideal containing $\left(\varphi_1^{(X)}\varphi_1^{(Y)},\ldots,\varphi_{n+m}^{(X)}\varphi_{n+m}^{(Y)}\right)$. From Corollary 16 we conclude that $\mathcal{M}$ is a maximal ideal.
Denote by J the Jacobian determinant of the polynomials $\varphi_i^{(X)}\varphi_i^{(Y)}$ with respect to the variables $x_1,\ldots,x_n,y_1,\ldots,y_m$. From the Jacobian criterion (see for instance [10, Theorem 30.3]), it suffices to show that $J\notin\mathcal{M}$.
If $\overline{\mathcal{M}}$ denotes a maximal ideal in $\mathbb{F}[x,y]$ such that $\overline{\mathcal{M}}\cap K(\overline{A})[x,y]=\mathcal{M}$, there exists a point $p\in\mathbb{A}_{\mathbb{F}}^{n+m}$ such that $\overline{\mathcal{M}}$ is the maximal ideal associated to p.
In particular $\varphi_i^{(X)}(p)\varphi_i^{(Y)}(p)=0$ for all index $i=1,\ldots n+m$.
From Lemma 15 and Corollary 16 we infer that there exist well defined indices $j_1<\cdots<j_n$ and $k_1<\cdots<k_m$ verifying

- $\{j_1,\ldots,j_n\}\cap\{k_1,\ldots,k_m\}=\emptyset$.
- $\varphi_{j_l}^{(X)}(p)=0$ and $\varphi_{k_t}^{(Y)}(p)=0$ for all $1\leq l\leq n$, $1\leq t\leq m$.
- $\varphi_{k_t}^{(X)}(p)\neq 0$ and $\varphi_{j_l}^{(Y)}(p)\neq 0$ for all $1\leq l\leq n$, $1\leq t\leq m$.

Therefore, computing $J(p)$ we obtain that

$$J(p)=\pm\prod_{t=1}^{m}\varphi_{k_t}^{(X)}(p)\ \prod_{l=1}^{n}\varphi_{j_l}^{(Y)}(p)\ \ \det\left(\frac{\partial\varphi_{j_l}^{(X)}}{\partial x_s}\right)_{1\leq l,s\leq n}\det\left(\frac{\partial\varphi_{k_t}^{(Y)}}{\partial y_q}\right)_{1\leq t,q\leq m}$$

is different from zero, since the ideal $\left(\Phi_{j_1}^{(X)},\ldots,\Phi_{j_n}^{(X)},\Phi_{k_1}^{(Y)},\ldots,\Phi_{k_m}^{(Y)}\right)$ defines a smooth 0-dimensional variety containing p, and so $J\notin\mathcal{M}$. ■

2.3 The flatness of the deformation

2.3.1 Constructing some semimonical bihomogeneous equations

Lemma 18 *Let* $\wp\subset K[A]$ *be the prime ideal defined in Notation 14. There exist homogeneous polynomials* $R_1,\ldots,R_n\in K[A]_{\wp}[X]$ *such that the conditions*

1. $R_j\in K[A]_{\wp}[x_0,x_j]$,
2. $\deg(R_j)=\deg_{x_j}(R_j)$ *and* R_j *is monic in* x_j,
3. *for any* $q=0,\ldots,m$ *and for any* $t\in\mathbb{N}$ *sufficiently large, the polynomial* $y_q^tR_j$ *belongs to the ideal* $(F_1,\ldots,F_{n+m})\,K[A]_{\wp}[X,Y]$ *modulo* $\wp K[A]_{\wp}[X,Y]$,

hold for any $j=1,\ldots,n$.

Proof. From Lemma 15, we have that, for any choice of indices $1\leq j_1<j_2<\cdots<j_n\leq n+m$, the polynomials $\Phi_{j_1}^{(X)},\ldots,\Phi_{j_n}^{(X)}\in K[\overline{A}][X]$ define a 0-dimensional variety in $\mathbb{P}_{\mathbb{F}}^n$.
The Shape Lemma for finite projective varieties and the second assertion of Corollary 16 imply that, for any $j=1,\ldots,n$, there exists an homogeneous polynomial $\widetilde{R_j}\in K(\overline{A})[x_0,x_j]$ (depending on the choice of the indices $j_1,\ldots,j_n$) such that

- $\deg_{x_j}\left(\widetilde{R_j}\right)=\deg_X\left(\widetilde{R_j}\right)$ and $\widetilde{R_j}$ is monic in x_j.
- $\widetilde{R_j}$ belongs to the ideal generated by $\Phi_{j_1}^{(X)},\ldots,\Phi_{j_n}^{(X)}$ in $K(\overline{A})[X]$.

If we fix the index j, the product $\prod \widetilde{R_j}$ (where the product is taken over all possible choices of the indices j_i) is a homogeneous polynomial in $K(\overline{A})[x_0, x_j]$ which verifies:

- $\deg_{x_j}\left(\prod \widetilde{R_j}\right) = \deg_X\left(\prod \widetilde{R_j}\right)$ and $\prod \widetilde{R_j}$ is monic in x_j.
- $\prod \widetilde{R_j}$ belongs to the ideal $\bigcap\left(\Phi_{j_1}^{(X)}, \ldots, \Phi_{j_n}^{(X)}\right)$ in $K(\overline{A})[X]$, in particular

$$\prod \widetilde{R_j} \ \in \ \bigcap\left(\Phi_{j_1}^{(X)}, \ldots, \Phi_{j_n}^{(X)}, \Phi_{k_1}^{(Y)}, \ldots, \Phi_{k_m}^{(Y)}\right), \tag{8}$$

  where the intersection is taken over all those sequences $1 \leq j_1 < j_2 < \cdots < j_n \leq n+m$, $1 \leq k_1 < k_2 < \cdots < k_m \leq n+m$ such that $\{j_1, j_2, \cdots, j_n\} \cap \{k_1, k_2, \cdots, k_m\} = \emptyset$.

According to Formula (7) and Lemma 15, we have that the ideals

$$\bigcap\left(\Phi_{j_1}^{(X)}, \ldots, \Phi_{j_n}^{(X)}, \Phi_{k_1}^{(Y)}, \ldots, \Phi_{k_m}^{(Y)}\right) \quad \text{and} \quad (F_1, \ldots, F_{n+m})$$

define the same zeros in $\mathbb{P}^n_{\mathbb{F}} \times \mathbb{P}^m_{\mathbb{F}}$ and then the relation (8) implies, by means of Corollaries 16 and 17, that there exists $t_0 \in \mathbb{N}$ such that, for any $q = 0, \ldots, m$ the polynomial $y_q^{t_0} x_j^{t_0} \prod \widetilde{R_j}$ belongs to the ideal $(F_1, \ldots, F_{n+m})\, K(\overline{A})[X, Y]$.
We take the polynomial R_j as any lifting of $x_j^{t_0} \prod \widetilde{R_j}$ to the ring $K[A]_{\wp}[X, Y]$ (in fact one lifts only the coefficients). ■

Since the role of the variables X and Y may be interchanged we deduce also

Lemma 19 *There exist homogeneous polynomials $S_1, \ldots, S_m \in K[A]_{\wp}[Y]$ such that the conditions*

1. *$S_k \in K[A]_{\wp}[y_0, y_k]$,*
2. *$\deg(S_k) = \deg_{y_k}(S_k)$ and S_k is monic in y_k,*
3. *for any $\ell = 0, \ldots, n$ and for any $t \in \mathbb{N}$ sufficiently large, the polynomial $x_\ell^t S_k$ belongs to the ideal $(F_1, \ldots, F_{n+m})\, K[A]_{\wp}[X, Y]$ modulo $\wp K[A]_{\wp}[X, Y]$,*

hold for any $k = 1, \ldots, m$. ■

Let us observe that from the proof of Lemma 18 we may suppose without loss of generality that all the polynomials R_j have the same degree r and also that the polynomials S_k have the same degree s.
Fix now an exponent t, and indices q and j, $0 \leq q \leq m$, $1 \leq j \leq n$. The third condition of Lemma 18 may be rewritten as follows: there exists $P_{qj} \in \wp K[A]_{\wp}[X, Y]$ such that

$$y_q^t R_j + P_{qj} \in (F_1, \ldots, F_{n+m})\, K[A]_{\wp}[X, Y].$$

Since the ideal $(F_1, \ldots, F_{n+m})$ is bihomogeneous we can suppose that P_{qj} is also bihomogeneous with bidegree (r, t).
Analogously, for each ℓ, k, $0 \leq \ell \leq n$, $1 \leq k \leq m$, we have

$$x_\ell^t S_k + P'_{\ell k} \in (F_1, \ldots, F_{n+m})\, K[A]_{\wp}[X, Y]$$

with $P'_{\ell k} \in \wp K[A]_{\wp}[X, Y]$ bihomogeneous of bidegree (t, s).

Notation 20 *Fix an exponent t sufficiently large. For each choice of indices q, j, ℓ, k we denote*

$$\mathfrak{R}_{qj} := y_q^t R_j + P_{qj} \qquad \text{and} \qquad \mathfrak{S}_{\ell k} := x_\ell^t S_k + P'_{\ell k}$$

Observe that both bihomogeneous polynomials belong to the ideal $(F_1, \ldots, F_{n+m})\, K[A]_{\wp}[X, Y]$ and have bidegree (r, t) and (t, s) respectively.

2.3.2 Elimination of variables

The goal of this section is to show a recursive procedure which allows to eliminate variables of the polynomials $\mathfrak{R}_{qj}$ and $\mathfrak{S}_{\ell k}$, in order to find integral dependence equations.

Notation 21 *For any q, $q = 0, \ldots, m$, we define a family of polynomials $\mathfrak{R}_{qj}^{(\ell)}$ in $K[A]_{\wp}[X, Y]$ as follows:*

$$\begin{aligned} \mathfrak{R}_{qj}^{(0)} &:= \mathfrak{R}_{qj} \quad \text{for } j = 1, \ldots, n \\ \mathfrak{R}_{qj}^{(\ell)} &:= \mathrm{Res}_{x_\ell}\left(\mathfrak{R}_{q\ell}^{(\ell-1)}, \mathfrak{R}_{qj}^{(\ell-1)}\right) \quad \text{for } \ell = 1, \ldots, n-1 \text{ and } j = \ell+1, \ldots, n. \end{aligned}$$

Lemma 22 *Fix indices q, ℓ, j, such that $0 \leq q \leq m$, $0 \leq \ell \leq n-1$, $\ell+1 \leq j \leq n$. Then:*

1. $\mathfrak{R}_{qj}^{(\ell)} \in (F_1, \ldots, F_{n+m})\, K[A]_{\wp}[X, Y] \cap K[A]_{\wp}[x_0, x_{\ell+1}, \ldots, x_n, Y]$.
2. *There exist positive integers a, b (depending on q, ℓ, j) such that:*
   (a) $\mathfrak{R}_{qj}^{(\ell)}$ *is a bihomogeneous polynomial in $K[A]_{\wp}[x_0, x_{\ell+1}, \ldots, x_n, Y]$ of bidegree (ra, b).*
   (b) $\mathfrak{R}_{qj}^{(\ell)} \equiv y_q^b R_j^a\,(x_0, x_j) \mod \wp$ *and the leading coefficient of $\mathfrak{R}_{qj}^{(\ell)}$ (viewed as a polynomial in the variable x_j) is $y_q^b + w$ where $w \in \wp K[A]_{\wp}[Y]$.*

Proof. The proof is by recursion in ℓ.
For $\ell = 0$ the assertions follow from Lemma 18 and Notation 20.
Now suppose $\ell \geq 1$. Assertion 1. is a direct consequence of the inductive hypothesis and the fact that the resultant belongs to the ideal generated by the involved polynomials.
Since the resultant of bihomogeneous polynomials is also bihomogeneous (see for example [8, Ch.4, §4, pg.155] or [16, Ch. 1, Thm. 10.9]) we have Assertion 2.(a).
For the last statement, assume that $\mathfrak{R}_{q\ell}^{(\ell-1)} \equiv y_q^{b_1} R_\ell^{a_1}\,(x_0, x_\ell)$ and $\mathfrak{R}_{qj}^{(\ell-1)} \equiv y_q^{b_2} R_j^{a_2}\,(x_0, x_j)$ modulo $\wp$. Then $\mathfrak{R}_{qj}^{(\ell)} \equiv y_q^{b_1 D + b_2 a_1 r} R_j^{a_2 a_1 r}\,(x_0, x_j) \mod \wp$, where $D = \deg_{x_\ell}(\mathfrak{R}_{qj}^{(\ell-1)})$. Take $a := a_2 a_1 r$ and $b := b_1 D + b_2 a_1 r$. ■

After the $n-1$ recursive steps, we obtain a family of polynomials $\mathfrak{R}_{qn}^{(n-1)}$ for $q = 0, \ldots, m$ depending only on the variables x_0, x_n, Y.

The next reduction step consists in the elimination of the variables $x_1, \ldots, x_{n-1}$ in the polynomials $\mathfrak{S}_{\ell k}$.

Notation 23 *We define a family of polynomials $\mathfrak{S}_{0k}^{(\ell)}$ in $K[A]_{\wp}[X, Y]$ as follows:*

$$\begin{aligned} \mathfrak{S}_{0k}^{(0)} &:= \mathfrak{S}_{0k} \quad \text{for } k = 1, \ldots, m \\ \mathfrak{S}_{0k}^{(\ell)} &:= \mathrm{Res}_{x_\ell}\left(\mathfrak{R}_{k\ell}^{(\ell-1)}, \mathfrak{S}_{0k}^{(\ell-1)}\right) \quad \text{for } \ell = 1, \ldots, n \text{ and } k = 1, \ldots, n. \end{aligned}$$

With similar arguments as in the proof of Lemma 22 we obtain:

Lemma 24 *Fix indices ℓ, k, such that $0 \leq \ell \leq n$, $1 \leq k \leq m$. Then:*

1. $\mathfrak{S}_{0k}^{(\ell)} \in (F_1, \ldots, F_{n+m})\, K[A]_{\wp}[X, Y] \cap K[A]_{\wp}[x_0, x_{\ell+1}, \ldots, x_n, Y]$.
2. *There exist positive integers a, b, c (depending on ℓ, k) such that:*
   (a) $\mathfrak{S}_{0k}^{(\ell)}$ *is a bihomogeneous polynomial in $K[A]_{\wp}[x_0, x_{\ell+1}, \ldots, x_n, Y]$ of bidegree $(a, b+sc)$.*

(b) $\mathfrak{S}_{0k}^{(\ell)} \equiv x_0^a y_k^b S_k^c\,(y_0, y_k) \mod \wp$ *and the leading coefficient of* $\mathfrak{S}_{0k}^{(\ell)}$ *(viewed as a polynomial in the variable* y_k*) is* $x_0^a + w$ *where* $w \in \wp K[A]_\wp[x_0, x_{\ell+1}, \ldots, x_n]$.■

Finally we proceed to eliminate step-by-step the variables $y_1, \ldots, y_{m-1}$:

Notation 25 *We define a family of polynomials* $\mathfrak{Q}_k^{(\ell)}$ *with* $\ell = 0, \ldots, m-1$ *in* $K[A]_\wp[X, Y]$ *as follows:*

$$\begin{aligned} \mathfrak{Q}_k^{(0)} &:= \mathfrak{S}_{0k}^{(n)} \quad \text{for } k = 1, \ldots, m \\ \mathfrak{Q}_k^{(\ell)} &:= \mathrm{Res}_{y_\ell}\left(\mathfrak{Q}_\ell^{(\ell-1)}, \mathfrak{Q}_k^{(\ell-1)}\right) \quad \text{for } \ell = 1, \ldots, m-1 \text{ and } k = \ell+1, \ldots, m. \end{aligned}$$

After $(m-1)$ many steps we obtain a single polynomial $\mathfrak{Q}_m^{(m-1)} \in K[A]_\wp[x_0, y_0, y_m]$ with the following properties:

Proposition 26 *There exists* $a, b, c \in \mathbb{N}$ *such that*

1. $\mathfrak{Q}_m^{(m-1)}$ *is bihomogeneous of bi-degree* $(b, a+sc)$ *where* $s := \deg S_m$.
2. $\mathfrak{Q}_m^{(m-1)} \in (F_1, \ldots, F_{n+m})\, K[A]_\wp[X, Y] \cap K[A]_\wp[x_0, y_0, y_m]$.
3. $\mathfrak{Q}_m^{(m-1)} \equiv y_m^a x_0^b S_m^c\,(y_0, y_m) \mod \wp$ *and then the main coefficient of* $\mathfrak{Q}_m^{(m-1)}$ *(viewed as a polynomial in the variable* y_m*) is* $x_0^b + w$ *where* $w \in \wp K[A]_\wp[x_0]$ *is homogeneous of degree* b. ■

Notation 27 *For each* $i = 1, \ldots, n+m$ *denote by* f_i *the affinized with respect the variables* x_0, y_0 *of the bihomogeneous polynomial* F_i*; in other words:*

$$f_i := F_i\,(1, x_1, \ldots, x_n, 1, y_1, \ldots, y_m)\,.$$

Proposition 26 allows us to prove the main result of this Section which is the flatness of our deformation.

Theorem 28 *The standard morphism*

$$K[A]_\wp \hookrightarrow K[A]_\wp[x_1, \ldots, x_n, y_1, \ldots, y_m]/\,(f_1, \ldots, f_{n+m})$$

is an integral ring extension.

Proof. Since the role of y_m is equivalent to the role of any other variable y_k or x_j, $k = 1, \ldots, m$, $j = 1, \ldots, n$, it suffices to show that y_m is integral over $K[A]_\wp$.
After Proposition 26, consider the polynomial $P := \mathfrak{Q}_m^{(m-1)}(1, 1, T) \in K[A]_\wp[T]$. The leading coefficient of this polynomial is $1+w(1)$ (item 3 of Proposition 26), which is invertible in $K[A]_\wp$ because $w(1) \in \wp K[A]_\wp$. From item 2 of the same Proposition, we have that $P(y_m)$ belongs to the ideal $(f_1, \ldots, f_{n+m})\, K[A]_\wp[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and therefore, the polynomial P defines an integral dependence equation of the class of y_m in the affine ring $K[A]_\wp[x_1, \ldots, x_n, y_1, \ldots, y_m]/\,(f_1, \ldots, f_{n+m})$ over the local ring $K[A]_\wp$. ■

2.4 Bihomogeneous Bezout Theorem

2.4.1 The degree of a special fiber

We start recalling briefly some notations introduced in the previous sections.
Let $F_1, \ldots, F_{n+m} \in K[A][X, Y]$ be generic bihomogeneous polynomials with $\deg_X(F_i) = d_i$ and $\deg_Y(F_i) = e_i$ for $i = 1, \ldots, n+m$, and let $f_1, \ldots, f_{n+m}$ be the corresponding dehomogeneized polynomials putting $x_0 = 1$ and $y_0 = 1$.

Denote $N_i = \binom{n+d_i}{n}$, $M_i = \binom{m+e_i}{m}$ and $N := \sum_{i=1}^{n+m} N_i M_i$.
Consider the variety

$$\mathcal{V} := \left\{(a,x,y) \in \mathbb{A}^N \times \mathbb{A}^n \times \mathbb{A}^m / f_i\,(a,x,y) = 0,\ i = 1,\ldots,n+m\right\}$$

and the projection $\pi : \mathcal{V} \to \mathbb{A}^N$ defined as $\pi(a,x,y) = a$.
Let $Z \subset \mathbb{A}^N$ be the closed affine variety associated to the prime ideal $\wp \subset K[A]$ (see Notation 14).
The goal of this section is the computation of the degree of the fiber of Z under π.

Let us consider the integral ring extension of Theorem 28.
Tensoring this extension with the residual field $K[A]_\wp/\wp K[A]_\wp$ (in fact, the fraction field of $K[A]/\wp$ denoted as $K(\overline{A})$ in Subsection 2.2), we have the canonical inclusion

$$K\left(\overline{A}\right) \hookrightarrow K\left(\overline{A}\right)[x_1,\ldots,x_n,y_1,\ldots,y_m]/\left(f_1,\ldots,f_{n+m}\right).$$

Let $\mathbb{F}$ be an algebraic closure of $K(\overline{A})$ and let $\Phi_i^{(X)}$ and $\Phi_i^{(Y)} \in K[\overline{A}][X,Y]$ be the polynomials introduced in Definition 13.
Clearly we have:

$$\dim_{K(\overline{A})} K\left(\overline{A}\right)[x_1,\ldots,x_n,y_1,\ldots,y_m]/\left(f_1,\ldots,f_{n+m}\right) = \dim_{\mathbb{F}} \mathbb{F}[x_1,\ldots,x_n,y_1,\ldots,y_m]/\left(f_1,\ldots,f_{n+m}\right).$$

On the other hand, if $\varphi_i^{(X)}$ and $\varphi_i^{(Y)}$ denote the affinized of $\Phi_i^{(X)}$ and $\Phi_i^{(Y)}$ putting $x_0 = 1$ and $y_0 = 1$ respectively, from Formula (7) we deduce:

$$K(\overline{A})[x_1,\ldots,x_n,y_1,\ldots,y_m]/\left(f_1,\ldots,f_{n+m}\right) = K(\overline{A})[x_1,\ldots,x_n,y_1,\ldots,y_m]/(\varphi_1^{(X)}\varphi_1^{(Y)},\ldots,\varphi_{n+m}^{(X)}\varphi_{n+m}^{(Y)}).$$

From Corollaries 16 and 17 it follows that $(\varphi_1^{(X)}\varphi_1^{(Y)},\ldots,\varphi_{n+m}^{(X)}\varphi_{n+m}^{(Y)})$ is a radical 0-dimensional ideal and

$$\dim_{K(\overline{A})} K(\overline{A})[x_1,\ldots,x_n,y_1,\ldots,y_m]/(\varphi_1^{(X)}\varphi_1^{(Y)},\ldots,\varphi_{n+m}^{(X)}\varphi_{n+m}^{(Y)}) = \sum d_{j_1}\cdots d_{j_n} e_{k_1}\cdots e_{k_m},$$

where the sum is taken over all choices of indices satisfying $1 \le j_1 < \cdots < j_n \le n+m$, $1 \le k_1 < \cdots < k_m \le n+m$ and $\{j_1,\ldots,j_n\} \cap \{k_1,\ldots,k_m\} = \emptyset$.
Therefore we conclude that

$$\dim_{K(\overline{A})} K\left(\overline{A}\right)[x_1,\ldots,x_n,y_1,\ldots,y_m]/\left(f_1,\ldots,f_{n+m}\right) = \sum d_{j_1}\cdots d_{j_n} e_{k_1}\cdots e_{k_m}. \tag{9}$$

From the geometric point of view, Formula (9) says that the degree of $\pi^{-1}(Z)$ is $\sum d_{j_1}\cdots d_{j_n} e_{k_1}\cdots e_{k_m}$.

2.4.2 Passing from the fiber degree to the generic degree

Denote by $V := \{F_1 = 0,\ldots,F_{n+m} = 0\} \subset \mathbb{P}^n_{\overline{K(A)}} \times \mathbb{P}^m_{\overline{K(A)}}$.
In this section we compute the degree of the variety V from the degree of the fiber $\pi^{-1}(Z)$.

Let us consider again the integral extension:

$$K[A]_\wp \hookrightarrow K[A]_\wp[x_1,\ldots,x_n,y_1,\ldots,y_m]/\left(f_1,\ldots,f_{n+m}\right).$$

Theorem 29 *(Bihomogeneous Bezout Theorem) The ring*

$$K[A]_\wp[x_1,\ldots,x_n,y_1,\ldots,y_m]/\left(f_1,\ldots,f_{n+m}\right)$$

is a $K[A]_{\wp}$-finite free module of rank equal to $\sum d_{j_1}\cdots d_{j_n}e_{k_1}\cdots e_{k_m}$. In particular tensoring with the fraction field $K(A)$ we have

$$\dim_{K(A)} K(A)[x_1,\ldots,x_n,y_1,\ldots,y_m]/(f_1,\ldots,f_{n+m}) = \sum d_{j_1}\cdots d_{j_n}e_{k_1}\cdots e_{k_m}.$$

Therefore, since $(F_1,\ldots,F_{n+m}) \subset K[A][X,Y]$ is a prime ideal with no points at infinity, if $V := \{F_1=0,\ldots,F_{n+m}=0\} \subset \mathbb{P}^n_{K(A)} \times \mathbb{P}^m_{K(A)}$ we have that

$$\deg(V) = \sum d_{j_1}\cdots d_{j_n}e_{k_1}\cdots e_{k_m}.$$

Moreover, if $\sigma \in K[A]_{\wp}[x_1,\ldots,x_n,y_1,\ldots,y_m]/(f_1,\ldots,f_{n+m})$ verifies that $\left\{1,\overline{\sigma},\ldots,\overline{\sigma}^D\right\}$ is a $K(\overline{A})$-basis of $K(\overline{A})[x_1,\ldots,x_n,y_1,\ldots,y_m]/(f_1,\ldots,f_{n+m})$, then $\left\{1,\sigma,\ldots,\sigma^D\right\}$ is a $K[A]_{\wp}$-basis of $K[A]_{\wp}[x_1,\ldots,x_n,y_1,\ldots,y_m]/(f_1,\ldots,f_{n+m})$.

Proof. The proof follows closely [6, Proof of Prop. 2].
Set $\mathcal{O} := K[A]_{\wp}$ and $\mathfrak{M} := \wp K[A]_{\wp}$ its maximal ideal. Observe that $\mathcal{O}/\mathfrak{M} = K(\overline{A})$.
The ring $\mathcal{O}/\mathfrak{M}[x_1,\ldots,x_n,y_1,\ldots,y_m]/(f_1,\ldots,f_{n+m})$ is a semilocal reduced ring over a field (Corollary 17), and then from the shape lemma there exists an element (a "primitive element", which in fact may be taken as a K-linear combination of the variables) $\sigma \in \mathcal{O}[x_1,\ldots,x_n,y_1,\ldots,y_m]/(f_1,\ldots,f_{n+m})$ such that

$$\mathcal{O}/\mathfrak{M}[x_1,\ldots,x_n,y_1,\ldots,y_m]/(f_1,\ldots,f_{n+m}) = \mathcal{O}/\mathfrak{M}[\overline{\sigma}], \tag{10}$$

where $\overline{\sigma}$ denotes the class of σ modulo $\mathfrak{M}$.
Moreover, we have also that $\dim_{\mathcal{O}/\mathfrak{M}} \mathcal{O}/\mathfrak{M}[\overline{\sigma}]$ coincides with the degree of the minimal integral dependence equation of σ over $\mathcal{O}$ (recall that $\mathcal{O}$ is integrally closed) and also with the quantity $\sum d_{j_1}\cdots d_{j_n}e_{k_1}\cdots e_{k_m}$ in virtue of (9).
In particular we have that $\mathcal{O}[\sigma] \subset \mathcal{O}[x_1,\ldots,x_n,y_1,\ldots,y_m]/(f_1,\ldots,f_{n+m})$ is a free $\mathcal{O}$-module and

$$\operatorname{rank}_{\mathcal{O}}\mathcal{O}[\sigma] = \sum d_{j_1}\cdots d_{j_n}e_{k_1}\cdots e_{k_m}.$$

In order to conclude the proof it is enough to show that $\mathcal{O}[\sigma] = \mathcal{O}[x_1,\ldots,x_n,y_1,\ldots,y_m]/(f_1,\ldots,f_{n+m})$. This fact is an easy consequence of Nakayama's Lemma: Let us consider the exact sequence of finitely generated $\mathcal{O}$-modules

$$0 \to \mathcal{O}[\sigma] \xrightarrow{i} \mathcal{O}[x_1,\ldots,x_n,y_1,\ldots,y_m]/(f_1,\ldots,f_{n+m}) \to \operatorname{Coker}(i) \to 0. \tag{11}$$

Tensoring with the residual field $\mathcal{O}/\mathfrak{M}$ (which is right-exact) we obtain:

$$\mathcal{O}/\mathfrak{M}[\overline{\sigma}] \to \mathcal{O}/\mathfrak{M}[x_1,\ldots,x_n,y_1,\ldots,y_m]/(f_1,\ldots,f_{n+m}) \to \operatorname{Coker}(i)/\mathfrak{M}\operatorname{Coker}(i) \to 0.$$

Thus, from the identity (10), one infers that $\operatorname{Coker}(i)/\mathfrak{M}\operatorname{Coker}(i) = 0$ and then, by Nakayama's Lemma, $\operatorname{Coker}(i) = 0$ and so the exact sequence (11) says that

$$\mathcal{O}[\sigma] = \mathcal{O}[x_1,\ldots,x_n,y_1,\ldots,y_m]/(f_1,\ldots,f_{n+m})$$

and the Theorem is proved. ■

Corollary 30 *Let $\mathcal{V} \subset \mathbb{A}^N \times \mathbb{A}^n \times \mathbb{A}^m$ be the variety*

$$\mathcal{V} := \left\{(a,x,y) \in \mathbb{A}^N \times \mathbb{A}^n \times \mathbb{A}^m / f_i(a,x,y) = 0,\ i = 1,\ldots,n+m\right\}.$$

Then

$$\deg(\mathcal{V}) \leq \sum (d_{j_1}+1)\ldots(d_{j_n}+1)(e_{k_1}+1)\ldots(e_{k_m}+1),$$

where the sum runs over all choices of indices $j_1,\ldots,j_n,k_1,\ldots,k_m$ such that $1 \leq j_1 < \cdots < j_n \leq n+m$, $1 \leq k_1 < \cdots < k_m \leq n+m$ and $\{j_1,\ldots,j_n\} \cap \{k_1,\ldots,k_m\} = \emptyset$.

Proof. Let $L_1, \ldots, L_N$ be linear polynomials in $K[A, x, y]$ such that $\mathcal{W}_0 := \mathcal{V} \cap \{L_1 = 0, \ldots, L_N = 0\}$ is a finite algebraic set and

$$\#\mathcal{W}_0 = \deg(\mathcal{V}). \tag{12}$$

We may decompose each polynomial L_u, $u = 1, \ldots, N$, as a sum $L_u = L_u^{(A)} + L_u^{(x,y)}$, where $L_u^{(A)}$ is a linear form involving only the variables A, and $L_u^{(x,y)}$ is a linear polynomial involving only the variables x and y.

From the genericity on the choice of the polynomials L_u verifying (12), we may suppose without loss of generality that the square $N \times N$-matrix determined by the coefficients of the linear forms $L_u^{(A)}$ is a regular matrix; hence the relations $L_u = 0$, $u = 1, ..., N$, allow to replace the variables $A_{\alpha\beta}^{(i)}$ by linear polynomials in $K[x, y]$ in the equations $f_1, \ldots, f_{n+m}$, and so, the zero dimensional variety $\mathcal{W}_0$ can be defined by $n + m$ many polynomials that we call $h_1, \ldots, h_{n+m}$.

Observe that $\deg_x(h_i)$ and $\deg_y(h_i)$ are bounded by $d_i + 1$ and $e_i + 1$ respectively, for any index $i = 1, \ldots, n + m$.

Let us consider generic bihomogeneous polynomials $G_1, \ldots, G_{n+m} \in K[B, X, Y]$ of bi-degree $(d_i + 1, e_i + 1)$ for $i = 1, \ldots n + m$, where B denotes a new set of indeterminate coefficients. Denote by $g_1, \ldots, g_{n+m}$ the corresponding affinized polynomials (putting $x_0 = 1$ and $y_0 = 1$).

The polynomials $h_1, \ldots, h_{n+m}$ may be seen as specialisations of the polynomials g_i evaluating the coefficients B in adequate elements of K (depending on the coefficients of the linear polynomials $L_1, \ldots, L_N$).

If M denotes the number of all the new variables B, let $\mathcal{W} \subset \mathbb{A}^M \times \mathbb{A}^n \times \mathbb{A}^m$ be the algebraic set defined by the equations

$$g_1(b, x, y) = 0, \ldots, g_{n+m}(b, x, y) = 0$$

and let $\hat{\pi} : \mathcal{W} \to \mathbb{A}^M$ be the canonical projection on the M first coordinates (more precisely, $\hat{\pi}(b, x, y) := b$).

From Theorem 21, applied to the polynomial family $g_1, \ldots, g_{n+m}$, we have the equality:

$$\dim_{K(B)} K(B)[x, y]/(g_1, \ldots, g_{n+m}) = \sum (d_{j_1} + 1) \ldots (d_{j_n} + 1)(e_{k_1} + 1) \ldots (e_{k_m} + 1), \tag{13}$$

where the sum is taken over all choices of indices $j_1, \ldots, j_n, k_1, \ldots, k_m$ such that $1 \leq j_1 < \cdots < j_n \leq n + m$, $1 \leq k_1 < \cdots < k_m \leq n + m$ and $\{j_1, \ldots, j_n\} \cap \{k_1, \ldots, k_m\} = \emptyset$.

On the other hand, since $\mathcal{W}$ is a M-dimensional irreducible algebraic variety and $\hat{\pi}$ is a dominant morphism, Proposition 1 of [6] implies that for any $b \in \mathbb{A}^M$ such that $\hat{\pi}^{-1}(b)$ is finite, the relation

$$\sharp\hat{\pi}^{-1}(b) \leq [k(\mathcal{W}) : K(B)] = \dim_{K(B)} K(B)[x, y]/(g_1, \ldots, g_{n+m}) \tag{14}$$

holds.

Now, if we consider an element $b_0 \in \mathbb{A}^M$ such that $\hat{\pi}^{-1}(b_0) = \mathcal{W}_0$ (clearly such an element exists), from (12), (14) and (13) we conclude

$$\begin{aligned} \deg(\mathcal{V}) &= \sharp\mathcal{W}_0 = \sharp\hat{\pi}^{-1}(b_0) \leq \dim_{K(B)} K(B)[x, y]/(g_1, \ldots, g_{n+m}) = \\ &= \sum (d_{j_1} + 1) \ldots (d_{j_n} + 1)(e_{k_1} + 1) \ldots (e_{k_m} + 1) \end{aligned}$$

and the corollary follows. ■

2.5 Certain special fibers

Let $F_1, \ldots, F_{n+m} \in K[A][X, Y]$ be generic bihomogeneous polynomials with $\deg_X(F_i) = d_i$ and $\deg_Y(F_i) = e_i$ for $i = 1, \ldots, n + m$, and let $f_1, \ldots, f_{n+m}$ be the corresponding dehomogeneized polynomials putting $x_0 = 1$ and $y_0 = 1$. We denote $x := (x_1, \ldots, x_n)$ and $y := (y_1, \ldots, y_n)$.

Denote $N_i = \binom{n + d_i}{n}$, $M_i = \binom{m + e_i}{m}$ and $N := \sum_{i=1}^{n+m} N_i M_i$.

Consider the variety

$$\mathcal{V} := \left\{(a,x,y) \in \mathbb{A}^N \times \mathbb{A}^n \times \mathbb{A}^m / f_i\,(a,x,y) = 0,\ i = 1,\ldots,n+m\right\}$$

and the projection $\pi : \mathcal{V} \to \mathbb{A}^N$ defined as $\pi(a,x,y) = a$.
Let $Z \subset \mathbb{A}^N$ be the closed affine variety associated to the prime ideal $\wp \subset K[A]$ (see Notation 14).
For each $a \in \mathbb{A}^N$, we write $\mathcal{V}_a \subset \mathbb{A}^{n+m}$ for the algebraic variety

$$\mathcal{V}_a := \{(x,y) \in \mathbb{A}^{n+m} / f_1(a,x,y) = 0, \ldots, f_{n+m}(a,x,y) = 0\}$$

and $J(a,x,y)$ for the Jacobian of the polynomials $f_1(a,x,y),\ldots,f_{n+m}(a,x,y)$ with respect to the variables x and y.
The purpose of this section is to show the following theorem:

Theorem 31 *Let $a \in Z$ be a point such that $\pi^{-1}(a)$ is a 0-dimensional variety whose cardinal is $\sum d_{j_1} \ldots d_{j_n} e_{k_1} \ldots e_{k_m}$ (the existence of such points follows from Section 2.4). Then, for any $(p,q) \in \mathcal{V}_a$ we have $J(a,p,q) \neq 0$.*
In other words, the points $a \in Z$ with fiber of maximal cardinality are unramified for π.

Proof. Since $a \in Z$, for each index $i = 1,\ldots,n+m$, the polynomial $f_i(a,x,y)$ may be decomposed in the following way:

$$f_i(a,x,y) = \psi_i^{(x)} \psi_i^{(y)}, \tag{15}$$

where $\psi_i^{(x)} \in K[x]$, $\psi_i^{(y)} \in K[y]$ with $\deg \psi_i^{(x)} \leq d_i$ and $\deg \psi_i^{(y)} \leq e_i$ (see Remark 9, Proposition 10 and Notation 14).
For any choice of indices $j_1 < \cdots < j_n$, $k_1 < \cdots < k_m$ such that $\{j_1,\ldots,j_n\} \cap \{k_1,\ldots,k_m\} = \emptyset$ we denote

$$\mathcal{V}_{a,j_1,\ldots,j_n,k_1,\ldots,k_m} := \left\{(x,y) \in \mathbb{A}^{n+m} \ / \ \psi_{j_1}^{(x)}(x) = 0,\ldots,\psi_{j_n}^{(x)}(x) = 0, \psi_{k_1}^{(y)}(y) = 0,\ldots,\psi_{k_m}^{(y)}(y) = 0 \right\}.$$

We have the disjoint decomposition

$$\mathcal{V}_a = \bigcup_{\substack{j_1,\ldots,j_n \\ k_1,\ldots,k_m}} \mathcal{V}_{a,j_1,\ldots,j_n,k_1,\ldots,k_m}. \tag{16}$$

Moreover, as $\mathcal{V}_a$ is a 0-dimensional variety, for each $(p,q) \in \mathcal{V}_a$ there exist unique $j_1,\ldots,j_n,k_1,\ldots,k_m$ such that $\psi_{j_l}^{(x)}(p) = 0$ for $l = 1,\ldots,n$ and $\psi_{k_t}^{(y)}(q) = 0$ for $t = 1,\ldots,m$.
Thus we conclude

Claim 1. If $(j_1,\ldots,j_n,k_1,\ldots,k_m) \neq (j_1',\ldots,j_n',k_1',\ldots,k_m')$, $(p,q) \in \mathcal{V}_{a,j_1,\ldots,j_n,k_1,\ldots,k_m}$ and $(p',q') \in \mathcal{V}_{a,j_1',\ldots,j_n',k_1',\ldots,k_m'}$, then $p \neq p'$ and $q \neq q'$.
In particular, if $(p,q) \in \mathcal{V}_{a,j_1,\ldots,j_n,k_1,\ldots,k_m}$ then $\psi_{k_l}^{(x)}(p) \neq 0$ for every $l = 1,\ldots,m$ and analogously $\psi_{j_t}^{(y)}(q) \neq 0$ for every $t = 1,\ldots,n$.

From the affine Bezout inequality (cf. [6, Th. 1]), for each choice of indices $j_1 < \cdots < j_n$, $k_1 < \cdots < k_m$ such that $\{j_1,\ldots,j_n\} \cap \{k_1,\ldots,k_m\} = \emptyset$,

$$\begin{aligned} \deg\left(\mathcal{V}_{a,j_1,\ldots,j_n,k_1,\ldots,k_m}\right) &\leq \deg \psi_{j_1}^{(x)} \ldots \deg \psi_{j_n}^{(x)} \deg \psi_{k_1}^{(y)} \ldots \deg \psi_{k_m}^{(y)} \leq \\ &\leq d_{j_1} \cdots d_{j_n} e_{k_1} \cdots e_{k_m}. \end{aligned}$$

On the other hand, from the hypothesis on the cardinality of $\pi^{-1}(a)$ and the decomposition (16), we have

$$\sum_{\substack{j_1,\ldots,j_n \\ k_1,\ldots,k_m}} d_{j_1} \cdots d_{j_n} e_{k_1} \cdots e_{k_m} = \deg \pi^{-1}(a) = \sum_{\substack{j_1,\ldots,j_n \\ k_1,\ldots,k_m}} \deg\left(\mathcal{V}_{a,j_1,\ldots,j_n,k_1,\ldots,k_m}\right).$$

Combining both formulas, we deduce that

$$\deg\left(\mathcal{V}_{a,j_1,\ldots,j_n,k_1,\ldots,k_m}\right) = d_{j_1}\cdots d_{j_n}e_{k_1}\cdots e_{k_m}. \tag{17}$$

for each choice of indices $j_1,\ldots,j_n,k_1,\ldots,k_m$ such that $\{j_1,\ldots,j_n\}\cap\{k_1,\ldots,k_m\}=\emptyset$.

Now if we denote

$$H_{j_1,\ldots,j_n} := \left\{p\in\mathbb{A}^n / \psi_{j_l}^{(x)}(p)=0,\ l=1,\ldots,n\right\}$$

and

$$Z_{k_1,\ldots,k_m} := \left\{q\in\mathbb{A}^m / \psi_{k_t}^{(y)}(q)=0,\ t=1,\ldots,m\right\},$$

the previous remarks imply that

$$H_{j_1,\ldots,j_n}\times Z_{k_1,\ldots,k_m} = \mathcal{V}_{a,j_1,\ldots,j_n,k_1,\ldots,k_m}.$$

From (17) and Bezout inequality, the following relations hold:

$$\begin{aligned} d_{j_1}\cdots d_{j_n}e_{k_1}\cdots e_{k_m} &= \deg\left(\mathcal{V}_{a,j_1,\ldots,j_n,k_1,\ldots,k_m}\right) = \deg\left(H_{j_1,\ldots,j_n}\times Z_{k_1,\ldots,k_m}\right) = \\ &= \deg\left(H_{j_1,\ldots,j_n}\right)\deg\left(Z_{k_1,\ldots,k_m}\right) \leq \left(d_{j_1}\cdots d_{j_n}\right)\left(e_{k_1}\cdots e_{k_m}\right) \end{aligned}$$

and then

$$\deg H_{j_1,\ldots,j_n} = d_{j_1}\cdots d_{j_n} \qquad \text{and} \qquad \deg Z_{k_1,\ldots,k_m} = e_{k_1}\cdots e_{k_m}. \tag{18}$$

Claim 2. Let $(j_1,\ldots,j_n,k_1,\ldots,k_m)$ be a sequence of indices as above. Then, the ideals $(\psi_{j_1}^{(x)},\ldots,\psi_{j_n}^{(x)})\subset K[x]$ and $(\psi_{k_1}^{(y)},\ldots,\psi_{k_m}^{(y)})\subset K[y]$ are radical ideals.

Proof of the claim: By means of (18) we have

$$\dim_K K[x]/\sqrt{(\psi_{j_1}^{(x)},\ldots,\psi_{j_n}^{(x)})} = \deg H_{j_1,\ldots,j_n} = d_{j_1}\cdots d_{j_n} \tag{19}$$

On the other hand, from [1, Theorem 17],

$$\dim_K K\left[x\right]/(\psi_{j_1}^{(x)},\ldots,\psi_{j_n}^{(x)}) \leq d_{j_1}\cdots d_{j_n}. \tag{20}$$

Since $\dim_K K[x]/\sqrt{(\psi_{j_1}^{(x)},\ldots,\psi_{j_n}^{(x)})} \leq \dim_K K\left[x\right]/(\psi_{j_1}^{(x)},\ldots,\psi_{j_n}^{(x)})$, from (19) and (20) we obtain:

$$\dim_K K[x]/\sqrt{(\psi_{j_1}^{(x)},\ldots,\psi_{j_n}^{(x)})} = \dim_K K\left[x\right]/(\psi_{j_1}^{(x)},\ldots,\psi_{j_n}^{(x)}) = d_{j_1}\cdots d_{j_n}$$

and so $(\psi_{j_1}^{(x)},\ldots,\psi_{j_n}^{(x)}) = \sqrt{(\psi_{j_1}^{(x)},\ldots,\psi_{j_n}^{(x)})}$. This finishes the proof of Claim 2.

In order to conclude the proof of the theorem, let $(p,q)\in\mathcal{V}_a$. From the factorisation (15), it follows that the Jacobian matrix of the polynomials $f_i(a,x,y)$ in the point (p,q) has the following form:

$$\left(\begin{array}{c|c} \left(\psi_i^{(y)}(q)\,\dfrac{\partial\psi_i^{(x)}}{\partial x_j}(p)\right)_{\substack{1\leq i\leq n+m\\ 1\leq j\leq n}} & \left(\psi_i^{(x)}(p)\,\dfrac{\partial\psi_i^{(y)}}{\partial y_k}(q)\right)_{\substack{1\leq i\leq n+m\\ 1\leq k\leq m}} \end{array}\right).$$

The point (p,q) belongs to exactly one of the varieties $\mathcal{V}_{a,j_1,\ldots,j_n,k_1,\ldots,k_m}$ (see Claim 1). Without loss of generality we may suppose that $\{j_1,\ldots,j_n\}=\{1,\ldots,n\}$ and $\{k_1,\ldots,k_m\}=\{n+1,\ldots,n+m\}$.

Then

$$J(a,p,q) = \prod_{i=1}^{n} \psi_i^{(y)}(q) \prod_{i=n+1}^{n+m} \psi_i^{(x)}(p) \det \begin{pmatrix} \left(\frac{\partial \psi_i^{(x)}}{\partial x_j}(p)\right)_{1\le i,j\le n} & 0 \\ 0 & \left(\frac{\partial \psi_i^{(y)}}{\partial y_k}(q)\right)_{\substack{n+1\le i\le n+m \\ 1\le k\le m}} \end{pmatrix} =$$

$$= \prod_{i=1}^{n} \psi_i^{(y)}(q) \prod_{i=n+1}^{n+m} \psi_i^{(x)}(p) \det \left(\frac{\partial \psi_i^{(x)}}{\partial x_j}(p)\right)_{1\le i,j\le n} \det \left(\frac{\partial \psi_i^{(y)}}{\partial y_k}(q)\right)_{\substack{n+1\le i\le n+m \\ 1\le k\le m}}.$$

By Claim 1 the first two factors are different from zero and by Claim 2 the last two factors are also non-zero. This finishes the proof of the theorem. ■

3 Algorithmic resolution of bihomogeneous polynomial systems

3.1 On Padé approximants

Let $\mathbb{L}$ be an arbitrary field and let $Z_1, \ldots, Z_n$ be indeterminates over $\mathbb{L}$; let η be a point of $\mathbb{L}^n$. We denote by $\mathbb{L}[[Z-\eta]]$ the ring of multivariate formal power series in the variables $Z := (Z_1, \ldots, Z_n)$ developed around the point η with coefficients in $\mathbb{L}$.

Lemma 32 *Let $\Phi \in \mathbb{L}[[Z-\eta]]$ be a formal power series and δ be a positive integer. Suppose that there exist polynomials $P, Q \in \mathbb{L}[Z]$ verifying the following items:*

1. $\Phi = P/Q$
2. $\deg P, \deg Q \le \delta$
3. $Q(\eta) \neq 0$.

Suppose also that there exists a slp of length $\mathcal{L}$ which evaluates the first 3δ homogeneous components of Φ (homogeneous in $Z-\eta$).
Then there exists a probabilistic algorithm which computes a slp of length $O(\delta^3(\delta^4+\mathcal{L}))$ evaluating polynomials $P_0, Q_0 \in \mathbb{L}[Z]$ with degrees bounded by δ such that $\Phi = P_0/Q_0$ and $Q_0(\eta) \neq 0$ within complexity of order $O(\delta^3(\delta^4+\mathcal{L}))$.

Proof. Let $P, Q \in \mathbb{L}[Z]$ verifying the hypotheses of the Lemma; since $Q(\eta) \neq 0$, without loss of generality we may suppose that P and Q verifies

$$Q\,\Phi = P \qquad \text{and} \qquad Q(\eta) = 1. \tag{21}$$

We consider the $(Z-\eta)$-homogeneous decomposition of the polynomials P, Q and the series Φ

$$P := \sum_{i=0}^{\delta} p_i, \qquad Q := \sum_{i=0}^{\delta} q_i \qquad \text{and} \qquad \Phi := \sum_{i=0}^{\infty} \varphi_i,$$

where the p_i's, the q_i's and the φ_i's are polynomials $(Z-\eta)$-homogeneous of degree i. From the hypothesis $Q(\eta) = 1$, we have $q_0 = 1$.
Let T be a new variable and consider the new series in $\mathbb{L}[Z][[T]]$

$$\Psi := \sum_{i=0}^{\infty} \varphi_i\, T^i$$

and the polynomials in $\mathbb{L}[Z][T]$

$$p := \sum_{i=0}^{\delta} p_i\, T^i \qquad \text{and} \qquad q := \sum_{i=0}^{\delta} q_i\, T^i.$$

From the relation (21) we deduce the identity

$$q\Psi = p \qquad \text{and} \qquad q(0) = 1. \tag{22}$$

Let us observe that a polynomial $Q \in \mathbb{L}[Z]$ of minimal degree satisfying (21) induces a polynomial $q \in \mathbb{L}[Z][T]$ of minimal degree satisfying (22) and conversely.

Let $p^{\min}, q^{\min} \in \mathbb{L}[Z][T]$ be polynomials satisfying (22) such that $q^{\min}$ has minimal degree. Set $\delta_0 := \deg q^{\min}$, $\delta_1 := \deg p^{\min}$. The existence of a numerator $P \in \mathbb{L}[Z]$ and a denominator $Q \in \mathbb{L}[Z]$ for Φ with degrees bounded by δ implies $\delta_0, \delta_1 \leq \delta$. It is easy to see that $p^{\min}$ and $q^{\min}$ are uniquely determined and that they are also the polynomial pair (p, q) verifying (22) with q of minimal degree, even if polynomials in $\mathbb{L}(Z)[T]$ are considered.

Fix $k \geq \delta_0$, and assume that q and p are polynomials in $\mathbb{L}(Z)[T]$ satisfying equality (22) such that $\deg q = k$, $\deg p = \delta_1 + k - \delta_0 \leq \delta + k$ and $q(0) = 1$ (take for example, $p := (T+1)^{k-\delta_0} \cdot p^{\min}$, $q := (T+1)^{k-\delta_0} q^{\min}$).

Then, equality (22) induces the following relations involving the coefficients of p, q and Ψ (where $p_i := 0$ for $i > \deg p$)

$$\begin{array}{rcll}
p_0 & = & \varphi_0 & \\
p_1 & = & \varphi_1 + \varphi_0\, q_1 & \\
 & \vdots & & \\
p_{\delta+k} & = & \varphi_{\delta+k} + \varphi_{\delta+k-1}\, q_1 + \cdots + \varphi_{\delta}\, q_k & (*) \\
0 & = & \varphi_{\delta+k+1} + \varphi_{\delta+k}\, q_1 + \cdots + \varphi_{\delta+1}\, q_k & \\
 & \vdots & & \\
0 & = & \varphi_{\delta+2k} + \varphi_{\delta+2k-1}\, q_1 + \cdots + \varphi_{\delta+k}\, q_k &
\end{array}$$

The converse also holds, more precisely:

Claim 1: *Consider $(*)$ as a linear equation system in the unknowns $p_0, \ldots, p_{\delta+k}$, $q_1, \ldots, q_k$. Any solution of this system in the field $\mathbb{L}(Z)$ produces two polynomials $\widetilde{p}, \widetilde{q} \in \mathbb{L}(Z)[T]$ of degrees bounded by $\delta + k$ and k respectively, verifying $\widetilde{q}\,\Psi = \widetilde{p}$.*

Proof of the claim: Let

$$(\widetilde{p}_0, \ldots, \widetilde{p}_{\delta+k}, \widetilde{q}_1, \ldots, \widetilde{q}_k) \in \mathbb{L}(Z)^{\delta+2k+1}$$

be a solution of the system $(*)$ and let

$$\widetilde{p} := \sum_i \widetilde{p}_i T^i \qquad \text{and} \qquad \widetilde{q} := 1 + \sum_i \widetilde{q}_i T^i$$

be the associated polynomials in $\mathbb{L}(Z)[T]$.

Let $\Theta = \sum_i \theta_i T^i \in \mathbb{L}(Z)[[T]]$ be the formal power series whose coefficients are defined as

$$\theta_i := \begin{cases} \varphi_i & \text{for } i = 0, \ldots, \delta + 2k \\ -\sum_{j=1}^{k} \theta_{i-j}\, \widetilde{q}_j & \text{for } i > \delta + 2k \end{cases}$$

From the definition of the series Θ, it follows immediately that

$$\widetilde{q}\,\Theta = \widetilde{p}. \tag{23}$$

Then, it suffices to show that $\Psi = \Theta$.
As the first $\delta + 2k + 1$ coefficients of the series Ψ and Θ coincide, there exists a polynomial $H \in \mathbb{L}(Z)[T]$ of degree bounded by $\delta + 2k$ and series $\widetilde{\Psi}, \widetilde{\Theta} \in \mathbb{L}(Z)[[T]]$ of order at least $\delta + 2k + 1$ such that

$$\Psi \,=\, H + \widetilde{\Psi} \quad \text{ and } \quad \Theta \,=\, H + \widetilde{\Theta}.$$

Multiplying relations (22) and (23) by $\widetilde{q}$ and q respectively, we deduce the identities:

$$\widetilde{q}\,p = \widetilde{q}\,q\,H + \widetilde{q}\,q\,\widetilde{\Psi}$$
$$q\,\widetilde{p} = q\,\widetilde{q}\,H + q\,\widetilde{q}\,\widetilde{\Theta}$$

and hence

$$\widetilde{q}\,p - q\,\widetilde{p} = q\,\widetilde{q}\,(\widetilde{\Psi} - \widetilde{\Theta}).$$

Then (recall that the orders of $\widetilde{\Psi}$ and $\widetilde{\Theta}$ are at least $\delta + 2k + 1$) we conclude that $T^{\delta+2k+1}$ divides $\widetilde{q}\,p - q\,\widetilde{p}$. Since $\deg p, \deg \widetilde{p} \leq \delta + k$ and $\deg q, \deg \widetilde{q} \leq k$, we infer that $\widetilde{q}\,p = q\,\widetilde{p}$ and so, $\Psi = \Theta$. This finishes the proof of the claim.

Let us consider now the following linear system over the field $\mathbb{L}(Z)$:

$$\begin{pmatrix} \varphi_{\delta+k} & \varphi_{\delta+k-1} & \cdots & \varphi_{\delta+1} \\ \varphi_{\delta+k+1} & \varphi_{\delta+k} & \cdots & \varphi_{\delta+2} \\ \cdots & \cdots & \cdots & \cdots \\ \varphi_{\delta+2k-1} & \varphi_{\delta+2k-2} & \cdots & \varphi_{\delta+k} \end{pmatrix} \begin{pmatrix} q_1 \\ \vdots \\ q_k \end{pmatrix} = \begin{pmatrix} -\varphi_{\delta+k+1} \\ \vdots \\ -\varphi_{\delta+2k} \end{pmatrix}. \tag{24}$$

Note that this linear system consists in the last k equations of the system $(*)$.
Moreover, using the first $\delta + k$ equalities in $(*)$, we can obtain the vector $(p_0, \ldots, p_{\delta+k})$ from a solution $(q_1, \ldots, q_k)$ of (24).
Therefore, the existence of a solution for $(*)$ is equivalent to the existence of a solution for (24).

Summarizing:

Claim 2: *Let $p := \sum_{i=0}^{\delta+k} p_i T^i$ and $q := 1 + \sum_{i=1}^{k} q_i T^i$ be polynomials in $\mathbb{L}(Z)[T]$ of degrees bounded by $\delta + k$ and k respectively. The the following assertions are equivalent:*

- *(a) $q\,\Psi = p$.*
- *(b) $(q_1, \ldots, q_k)$ is a solution for the system (24) over the field $\mathbb{L}(Z)[T]$ and, for $i = 0, \ldots, \delta + k$, $p_i = \sum_{j=0}^{\min\{i,k\}} \varphi_{i-j}\, q_j$.*

By Claim 2, as δ_0 is the degree of the minimal denominator $q^{\min}$, the system (24) has a unique solution for $k := \delta_0$.
On the other hand, for $k > \delta_0$, there exists an infinite family of polynomials q, p such that $\deg q = k$, $\deg p \leq \delta + k$, $q(0) = 1$ and $q\,\Psi = p$ (namely, $q := h \cdot q^{\min}$ and $p := h \cdot p^{\min}$, where $h \in \mathbb{L}(Z)[T]$ is a polynomial of degree $k - \delta_0$ such that $h(0) = 1$)
Therefore Claim 2 implies that for $k > \delta_0$ the linear system (24) has an infinite solution set.
In particular, we have

$$\delta_0 = \max\{1 \leq k \leq \delta : \det(A_k) \neq 0\},$$

where A_k denotes the $k \times k$-matrix of the system (24).
Moreover, the coefficients of $q^{\min}$ can be obtained by solving (24) for $k = \delta_0$.
Finally, taking into account that $\deg p^{\min} \leq \delta$, it follows that the coefficients of $p^{\min}$ can be computed as $p_i := \sum_{j=0}^{i} \varphi_{i-j} q_j$ for $i = 0, \ldots, \delta$.

Now is quite simple to describe an algorithm computing the polynomials P_0 and Q_0 of the statement of the lemma.

1. The first task consists in determining $\delta_0 := \max\{1 \leq k \leq \delta : \det(A_k) \neq 0\}$, which is the degree of the minimal denominator q.

   Set $k := \delta$ and proceed as follows:

   (a) Compute a slp of length $O(k^4 + \mathcal{L})$ which evaluates $\det(A_k) \in \mathbb{L}[Z]$.

   (b) Choose randomly a point $a_0 \in \mathbb{L}^n$ and evaluate $\det(A_k)(a_0)$.

   (c) If $\det(A_k)(a_0) = 0$, set $k := k - 1$. Otherwise, $\delta_0 := k$.

   The complexity of this step is of order $O(\delta^5)$.

   Let us observe that $\det(A_{\delta_0})$ is a $(Z - \eta)$-homogeneous polynomial of degree $\delta_0(\delta + \delta_0)$.

2. Solve the linear system (24) for $k := \delta_0$.

   (a) Since $\det(A_{\delta_0}) \neq 0$ the solution may be obtained by Cramer's Rule :

$$\det(A_{\delta_0}) \begin{pmatrix} q_1 \\ \vdots \\ q_{\delta_0} \end{pmatrix} = \operatorname{adj}(A_{\delta_0}) \begin{pmatrix} -\varphi_{\delta+\delta_0+1} \\ \vdots \\ -\varphi_{\delta+2\delta_0} \end{pmatrix} =: \begin{pmatrix} \widetilde{q}_1 \\ \vdots \\ \widetilde{q}_{\delta_0} \end{pmatrix}.$$

   The complexity of this procedure is of order $O(\delta_0^4)$, the polynomials $\widetilde{q}_0 := \det(A_{\delta_0}), \widetilde{q}_1, \ldots, \widetilde{q}_{k_0}$ are given by slp's of length $O(\delta_0^4 + \mathcal{L})$ and their degrees are bounded by $\delta_0(\delta + \delta_0)$.

   (b) For each $1 \leq i \leq \delta_0$ compute the coefficient $q_i \in \mathbb{L}[Z]$ of q as the quotient of the exact division of $\widetilde{q}_i$ with $\widetilde{q}_0$.

   For this purpose we can apply the procedure of avoiding of divisions given in [15] (see also [9]), taking into account that a point $a_0 \in \mathbb{L}^n$ such that $\widetilde{q}_0(a_0) \neq 0$ is known.

   Since $\deg q_i \leq \delta$, this can be done in time $O(\delta^3(\delta^4 + \mathcal{L}))$.

3. A slp evaluating the coefficients of the polynomial p can be obtained by means of the equations $p_0 = \varphi_0$, $p_1 = \varphi_1 + \varphi_0\, q_1, \ldots, p_\delta = \varphi_\delta + \varphi_{\delta-1}\, q_1 + \cdots + \varphi_0\, q_\delta$, where $q_i = 0$ for $i > \delta_0$. The length of this slp is bounded by $O(\delta^3(\delta^4 + \mathcal{L}))$.

4. Take $P_0 := \sum_{i=0}^{\delta} p_i$ and $Q_0 := \sum_{i=0}^{\delta} q_i$.

   The polynomials P_0 and Q_0 are given by a slp of length $O(\delta^3(\delta^4 + \mathcal{L}))$.

Summarizing, the total complexity of the algorithm is bounded by $O(\delta^3(\delta^4 + \mathcal{L}))$ and the Lemma is proved. ■

3.2 Algorithmic resolution in the generic case

We recall the notations introduced in Section 2.1.
Let K be a field and let $\overline{K}$ be an algebraic closure of K.
Let $n, m \in \mathbb{N}$ and let $x_0, \ldots, x_n,\ y_0, \ldots, y_m$ indeterminates over K. We will denote $X := (x_0, \ldots, x_n)$, $Y := (y_0, \ldots, y_m)$, $x := (x_1, \ldots, x_n)$ and $y := (y_1, \ldots, y_m)$.
For each $d, e \in \mathbb{N}_0$ set

$$\Lambda_{d,e} = \{(\alpha, \beta) \in \mathbb{N}_0^{n+1} \times \mathbb{N}_0^{m+1} : |\alpha| = d,\ |\beta| = e\}.$$

Let $(d_1, e_1), \ldots, (d_{n+m}, e_{n+m}) \in \mathbb{N}_0 \times \mathbb{N}_0$. For each $1 \leq i \leq n + m$ we introduce a set of new indeterminates $A^{(i)} := (A^{(i)}_{\alpha\beta})_{(\alpha,\beta) \in \Lambda_{d_i,e_i}}$ associated to the monomials $X^\alpha Y^\beta$ of bidegree (d_i, e_i).
We will denote $A = (A^{(i)})_{1 \leq i \leq n+m}$.

Set

$$N_i := \binom{d_i + n}{n}, \quad M_i := \binom{e_i + m}{m} \quad \text{and} \quad N := \sum_{i=1}^{n+m} N_i M_i.$$

For each i, $1 \leq i \leq n+m$, let $F_i \in K[A][X,Y]$ be the bihomogeneous polynomial

$$F_i := \sum_{(\alpha,\beta)\in\Lambda_{d_i,e_i}} A_{\alpha\beta}^{(i)}\, X^\alpha Y^\beta.$$

From Theorem 29 the polynomials $F_1,\ldots,F_{n+m}$ define a zero-dimensional variety $V \subset \mathbb{P}^n_{\overline{K(A)}} \times \mathbb{P}^m_{\overline{K(A)}}$, with no points at infinity, of degree

$$D := \sum d_{j_1} \ldots d_{j_n} e_{k_1} \ldots e_{k_m},$$

where the sum runs over all choices of indices $1 \leq j_1 < \cdots < j_n \leq n+m$, $1 \leq k_1 < \cdots < k_m \leq n+m$, with $\{j_1,\ldots,j_n\} \cap \{k_1,\ldots,k_m\} = \emptyset$.
For each i, $1 \leq i \leq n+m$, we denote $f_i \in K[A][x,y]$ to the affinized polynomial

$$f_i := F_i(1, x_1, \ldots, x_n, 1, y_1, \ldots, y_m).$$

The polynomials $f_1,\ldots,f_{n+m}$ define the zero-dimensional variety $V \subset \mathbb{A}^{n+m}_{\overline{K(A)}}$ of degree D.
Let $\mathcal{V} \subset \mathbb{A}^N \times \mathbb{A}^n \times \mathbb{A}^m$ be the variety

$$\mathcal{V} := \left\{(a,x,y) \in \mathbb{A}^N \times \mathbb{A}^n \times \mathbb{A}^m / f_i\,(a,x,y) = 0,\ i = 1,\ldots,n+m\right\}.$$

Corollary 30 says that the degree of $\mathcal{V}$ is bounded by

$$\Delta := \sum (d_{j_1}+1)\ldots(d_{j_n}+1)(e_{k_1}+1)\ldots(e_{k_m}+1).$$

where the sum runs over all choices of indices $j_1,\ldots,j_n,k_1,\ldots,k_m$ such that $1 \leq j_1 < \cdots < j_n \leq n+m$, $1 \leq k_1 < \cdots < k_m \leq n+m$ and $\{j_1,\ldots,j_n\} \cap \{k_1,\ldots,k_m\} = \emptyset$.

The goal of this section is the computation of minimal polynomials for linear forms which separate the points of V.
More precisely:
Let $L \in K[x,y]$ be a linear form which separates the points of the variety V and let $P \in K(A)[T]$ be the monic minimal polynomial of the class of L with respect to the canonical extension $K(A) \hookrightarrow K(A)[x,y]/(f_1,\ldots,f_{n+m})$.

Remark 33 *It is well known that the degree of P as a polynomial in the variable T is exactly D (because L separates the points of the variety V) and that P can be written as $\sum_{i=0}^{D} \Phi_i T^i \in K(A)[T]$, where each of the coefficients Φ_i may be decomposed as a quotient P_i/Q_i with $\deg P_i \leq \Delta$ and $\deg Q_i \leq \Delta$ (see for instance [13, Prop. 1] or [14, Prop.1]).*

The main result of this section is the following:

Theorem 34 *Let $L \in K[x,y]$ be a linear form which separates the points of the variety V and let $P := \sum_{i=0}^{D} \Phi_i T^i \in K(A)[T]$ be the minimal polynomial of the class of L with respect to the canonical extension $K(A) \hookrightarrow K(A)[x,y]/(f_1,\ldots,f_{n+m})$.*
There exists a probabilistic algorithm which, for each i, $0 \leq i \leq D$, produces a straight-line program of length $O(\Delta^5(\Delta^2 + \log(\Delta)d^2(n+m)^7 N\, D^2))$ computing polynomials $P_i, Q_i \in K[A]$ such that $\Phi_i = P_i/Q_i$. The algorithm runs in time $O(D\,\Delta^5(\Delta^2 + \log(\Delta)d^2(n+m)^7 N\, D^2))$.

The following subsections are devoted to prove Theorem 34.

3.2.1 Choosing a lifting point

We will choose a lifting point $a \in K^N$ in such a way that the polynomials $f_i(a, x, y)$ have nice factorisation properties, namely all these polynomials can be decomposed as a product of independent linear factors.

Take a family of elements $\xi_{ir}^{(x)} \in K$ for $1 \leq i \leq n+m$ and $1 \leq r \leq d_i$, such that $\xi_{ir}^{(x)} \neq \xi_{i'r'}^{(x)}$ if $i \neq i'$ or $r \neq r'$.

For each $\xi_{ir}^{(x)}$ let us consider the associated linear form in the variables x:

$$L_{ir}^{(x)} := 1 + \xi_{ir}^{(x)} x_1 + (\xi_{ir}^{(x)})^2 x_2 + \cdots + (\xi_{ir}^{(x)})^n x_n.$$

The hypothesis on the choice of the elements $\xi_{ir}^{(x)}$ implies that every subset of n many linear forms $L_{ir}^{(x)}$ is a K-linearly independent set.

Analogously we define linear forms in the variables y as follows: let $\xi_{is}^{(y)} \in K$, for $1 \leq i \leq n+m$ and $1 \leq s \leq e_i$), be a family of elements such that $\xi_{is}^{(y)} \neq \xi_{i's'}^{(y)}$ if $i \neq i'$ or $s \neq s'$, and for any index i and any index s with $1 \leq s \leq e_i$ let $L_{is}^{(y)} \in K[y]$ be the linear form defined as

$$L_{is}^{(y)} = 1 + \xi_{is}^{(y)} y_1 + (\xi_{is}^{(y)})^2 y_2 + \cdots + (\xi_{is}^{(y)})^m y_m.$$

We also have that any subset of m linear forms $L_{is}^{(y)}$ is K-linearly independent.

For each index i, $1 \leq i \leq n+m$, denote by $a^{(i)} \in K^{N_i}$ the vector of coefficients of the polynomial

$$\prod_{1 \leq r \leq d_i} L_{ir}^{(x)} \prod_{1 \leq s \leq e_i} L_{is}^{(y)},$$

in a certain prefixed monomial order (for instance the lexicographic order).

Observe that this polynomial has bidegree (d_i, e_i) and then we have the identity:

$$f_i(a^{(i)}, x, y) = \prod_{1 \leq r \leq d_i} L_{ir}^{(x)} \prod_{1 \leq s \leq e_i} L_{is}^{(y)}.$$

We take as the *lifting point*, the point $a := (a^{(1)}, \ldots, a^{(n+m)}) \in K^N$.

Each vector $a^{(i)}$ may be computed from the elements $\xi_{ir}^{(x)}$ and $\xi_{is}^{(y)}$ in a straightforward way as follows:

First let us observe that the coefficients of a product of a n-variate polynomial of degree k with a n-variate polynomial of degree 1 (both given in dense form) can be computed in time bounded by $(2n+1)\binom{n+k+1}{n}$ in the obvious way (using $(n+1)\binom{n+k}{n}$ multiplications and $n\binom{n+k+1}{n}$ additions).

Therefore the computation of the coefficients of polynomial $\varphi_i^{(x)} := \prod_{1 \leq r \leq d_i} L_{ir}^{(x)}$ runs in time

$$(2n+1) \sum_{r=1}^{d_i - 1} \binom{n+r+1}{n}$$

which may be bounded by $(2n+1)d_i\binom{n+d_i}{n}$.

Similarly the coefficients of $\varphi_i^{(y)} := \prod_{1 \leq s \leq e_i} L_{is}^{(y)}$ can be obtained in time $(2m+1)e_i\binom{m+e_i}{m}$.

Then the computation of the vector $a^{(i)}$ (namely, the coefficients of the product $\varphi_i^{(x)}\varphi_i^{(y)}$) runs in time bounded by

$$(2n+1)d_i\binom{n+d_i}{n} + (2m+1)e_i\binom{m+e_i}{m} + \binom{n+d_i}{n}\binom{m+e_i}{m}.$$

Hence the lifting point $a \in K^N$ may be computed in time

$$\sum_{i=1}^{n+m} (2n+1)d_i \binom{n+d_i}{n} + (2m+1)e_i \binom{m+e_i}{m} + \binom{n+d_i}{n}\binom{m+e_i}{m}.$$

If we denote $d := \max_{1\leq i\leq n+m}\{d_i + e_i\}$, we may easily estimate this number by $O((n+m)dN)$.

Summarizing we have:

Remark 35 *The lifting point $a \in K^N$ can be computed in time $O((n+m)dN)$, where $N := \sum_{i=1}^{n+m} \binom{n+d_i}{n}\binom{m+e_i}{m}$ and $d := \max_{1\leq i\leq n+m}\{d_i + e_i\}$.*

3.2.2 Solving a split Vandermonde system

From the choice of the coefficient vector (or lifting point) $a \in K^N$ in the previous section, each polynomial $f_i(a^{(i)}, x, y)$ is a product of linear forms, and then the solutions of the system

$$f_1(a, x, y) = 0, \ldots, f_{n+m}(a, x, y) = 0 \tag{25}$$

are exactly the solutions of the linear systems

$$L_{1\,t_1} = 0, \ldots, L_{n+m\,t_{n+m}} = 0,$$

where, for each $1 \leq i \leq n+m$, we have $L_{it_i} = L^{(x)}_{ir_i}$ or $L_{it_i} = L^{(y)}_{is_i}$, for some $1 \leq r_i \leq d_i$ or $1 \leq s_i \leq e_i$.
Moreover, since these linear forms are of type

$$1 + \xi\, x_1 + \xi^2\, x_2 + \cdots + \xi^n\, x_n = 0 \quad \text{or} \quad 1 + \xi\, y_1 + \xi^2\, y_2 + \cdots + \xi^m\, y_m = 0$$

for different constants ξ, we conclude that the solutions of the system (25) are the solutions of the linear systems

$$L^{(x)}_{j_1\, r_{j_1}} = 0, \ldots, L^{(x)}_{j_n\, r_{j_n}} = 0,\ L^{(y)}_{k_1\, s_{k_1}} = 0, \ldots, L^{(y)}_{k_m\, s_{k_m}} = 0 \tag{26}$$

where $1 \leq j_1 < \cdots < j_n \leq n+m$, $1 \leq k_1 < \cdots < k_m \leq n+m$ and $\{j_1, \ldots, j_n\} \cap \{k_1, \ldots, k_m\} = \emptyset$, and also $1 \leq r_{j_i} \leq d_{j_i}$ for all $1 \leq i \leq n$ and $1 \leq s_{k_l} \leq e_{k_l}$ for all $1 \leq l \leq m$.

Let us observe that there are D many of these linear systems (where D is the Bezout number $\sum d_{j_1} \ldots d_{j_n} e_{k_1} \ldots e_{k_m}$) and each of them has a unique solution (the associated matrix is regular since it is a two-block Vandermonde and each block corresponds to a family of different elements of K).

Therefore in order to solve the system (25) it suffices to choose a sequence of indices as in formula (26) and find the solutions $\gamma^{(x)} \in K^n$ and $\gamma^{(y)} \in K^m$ of the linear systems

$$L^{(x)}_{j_1\, r_{j_1}} = 0, \ldots, L^{(x)}_{j_n\, r_{j_n}} = 0$$

and

$$L^{(y)}_{k_1\, s_{k_1}} = 0, \ldots, L^{(y)}_{k_m\, s_{k_m}} = 0$$

respectively.
The coordinates of $\gamma^{(x)}$ and $\gamma^{(y)}$ can be computed using Cramer's rule in time $O(n^4)$ and $O(m^4)$ respectively.

Summarizing:

Remark 36 *Let $a \in K^N$ be the lifting point constructed in the previous section. Then, the solutions of the system*

$$f_1(a, x, y) = 0, \ldots, f_{n+m}(a, x, y) = 0$$

may be obtained in time $O((n^4 + m^4)D)$.

3.2.3 Computing generic solutions by Newton algorithm

The goal of this section is to compute (starting from the solutions $(\gamma^{(x)}, \gamma^{(y)})$ computed above) suitable power series representing approximations of the generic solutions in $\overline{K(A)}^{n+m}$ of the system

$$f_1(A, x, y) = 0, \ldots, f_{n+m}(A, x, y) = 0. \tag{27}$$

Let $a \in K^N$ be the lifting point introduced in section 3.2.1, $V_a \subset K^{n+m}$ denotes the algebraic finite set defined by the system (25) and $\gamma_1, \ldots, \gamma_D$ the points of V_a computed in section 3.2.2.
For the sake of simplicity we denote by F the polynomial vector $(f_1, \ldots, f_{n+m}) \in K[A, x, y]^{n+m}$.
Let $DF \in K[A, x, y]^{(n+m)\times(n+m)}$ be the Jacobian matrix of the vector F with respect to the variables x and y:

$$DF := \left(\frac{\partial f_i}{\partial x_j} \mid \frac{\partial f_i}{\partial y_k} \right)_{\substack{1 \le i \le n+m \\ 1 \le j \le n,\, 1 \le k \le m}},$$

and let $J \in K[A, x, y]$ be the determinant of the matrix DF.
The choice of the lifting point $a \in K^N$ and Theorem 31 imply that for any γ_j, $1 \le j \le D$, we have

$$J(a, \gamma_j) \neq 0.$$

Therefore by [7, Lemma 3] one deduces that, for any index j, $1 \le j \le D$, there exists a well defined power series vector

$$\Gamma_j = (\Gamma_{j1}, \ldots, \Gamma_{j\,n+m}) \in K[[A - a]]^{n+m}$$

verifying:

- $f_1(\Gamma_j) = 0, \ldots, f_{n+m}(\Gamma_j) = 0$
- $\Gamma_j(a) := (\Gamma_{j1}(a), \ldots, \Gamma_{j\,n+m}(a)) = \gamma_j$

Moreover the quoted result also gives a way to approximate these power series vectors Γ_j:
Let us consider the Newton operator associated to the system F

$$N_F(x, y)^t := (x, y)^t - DF(x, y)^{-1} \cdot F(x, y)^t,$$

where ^{t} denotes transposition.
For each point $\gamma_j \in V_a$, we define a recursive sequence of $(n + m)$-tuples of rational functions $\Gamma_j^{(\kappa)} := (\Gamma_{j1}^{(\kappa)}, \ldots, \Gamma_{j\,n+m}^{(\kappa)})(\kappa \in \mathbb{N}_0)$ as follows:

$$\begin{array}{lcll} \Gamma_j^{(0)} & := & \gamma_j & \\ \Gamma_j^{(\kappa)} & := & N_F(\Gamma_j^{(\kappa-1)}) & \kappa \in \mathbb{N} \end{array}$$

Any coordinate function $\Gamma_{ji}^{(\kappa)}$ $(1 \le i \le n + m)$ of $\Gamma_j^{(\kappa)}$ can be interpreted as a formal power series in $K[[A - a]]$. In this way, for each index i, $1 \le i \le n + m$, the sequence of rational functions $(\Gamma_{ji}^{(\kappa)})_{\kappa \in \mathbb{N}_0}$ converges to a series $\Gamma_{ji} \in K[[A - a]]$ (in fact the i-th coordinate of Γ_j).
More precisely, for each $\kappa \in \mathbb{N}$, the series $\Gamma_{ji}^{(\kappa)}$ approximates Γ_{ji} with precision 2^κ, in other words, $\Gamma_{ji}^{(\kappa)} \equiv \Gamma_{ji} \mod (A - a)^{2^\kappa}$.
We will choose the number of iterations κ so that we get suitable approximations to each of the power series Γ_{ji}.

This approximation procedure can be performed algorithmically as follows:

1. Fix $\kappa \in \mathbb{N}$. Applying the algorithm of [4, Lemma 30], we obtain a straight-line program which encodes the numerators and a single denominator for the κ-th iteration of the Newton operator; more precisely, we obtain polynomials

$$g_1, \ldots, g_n, g_{n+1}, \ldots, g_{n+m}, h \in K[A, x, y]$$

such that

$$N_F^{(\kappa)}(x, y) = \left(\frac{g_1}{h}, \ldots, \frac{g_n}{h}, \frac{g_{n+1}}{h}, \ldots, \frac{g_{n+m}}{h}\right).$$

2. By simple evaluation of the polynomials g_i and h in the points γ_j $(1 \leq j \leq D)$, we obtain straight-line programs for the numerator and the denominator of each of the rational functions $\Gamma_{ji}^{(\kappa)}$ $(1 \leq j \leq D,\ 1 \leq i \leq n+m)$.

From the complexity bounds stated in [4, Lemma 30], and taking into account that the polynomials $f_1, \ldots, f_{n+m} \in K[A, x, y]$ can be evaluated in the obvious way by means of a slp of length $O(N)$, we obtain the following estimate for the complexity of the procedure described above:

Remark 37 *Denote by* $d := \max_{1 \leq i \leq n+m}\{d_i + e_i\}$. *Let* $\kappa \in \mathbb{N}$ *and, for every* $1 \leq j \leq D$, *let* $\Gamma_j^{(\kappa)}$ *be the* 2^κ*-approximation of the solution series vector* Γ_j *associated to the fiber solution* γ_j *as above. Then, for each* $1 \leq j \leq D$,

$$\Gamma_j^{(\kappa)} = \left(\frac{g_1(A, \gamma_j)}{h(A, \gamma_j)}, \ldots, \frac{g_n(A, \gamma_j)}{h(A, \gamma_j)}, \frac{g_{n+1}(A, \gamma_j)}{h(A, \gamma_j)}, \ldots, \frac{g_{n+m}(A, \gamma_j)}{h(A, \gamma_j)}\right) \in K(A)^{n+m},$$

where g_i $(1 \leq i \leq n+m)$ *and* h *are polynomials in* $K[A, x, y]$ *which can be obtained in time* $O(\kappa\, d^2 (n+m)^7 N)$ *as explained above and given by a slp of length of the same order.*

3.2.4 Approximating the minimal polynomial of L

Let $L := u_0 + u_1 x_1 + \cdots + u_n x_n + u_{n+1} y_1 + \cdots + u_{n+m} y_m \in K[x, y]$ be a linear form which separates the points of the 0-dimensional variety $V \subset \mathbb{A}^{n+m}_{\overline{K(A)}}$.

We will compute the coefficients (with respect to a new variable U) of a polynomial $\widetilde{P} \in K[A, U]$ which approximates the minimal polynomial P of the linear form L.

Since $V = \{\Gamma_1, \ldots, \Gamma_D\} \subset \mathbb{A}^{n+m}_{\overline{K(A)}}$ (see Section 3.2.3) and we assume that L separates these points, the minimal polynomial P of L is exactly the product $\prod_{j=1}^{D}(U - L(\Gamma_j))$.

We approximate the coefficients of P by means of the coefficients of another polynomial which is constructed in a similar way, but having as roots the elements $L(\Gamma_j^{(\kappa)})$ (which can be seen as approximations of the roots of P).

Let us consider the following polynomials in $K[A]$ (see Section 3.2.3 for the notations):

$$G_j(A) := u_0\, h(\gamma_j) + u_1\, g_1(\gamma_j) + \cdots + u_{n+m}\, g_{n+m}(\gamma_j) \qquad \text{for } j = 1, \ldots, D \tag{28}$$

$$H_j(A) := h(\gamma_j) \qquad \text{for } j = 1, \ldots, D \tag{29}$$

$$H(A) := \prod_{j=1}^{D} H_j(A) \tag{30}$$

Let $\widetilde{P} \in K[A, U]$ be the polynomial defined as:

$$\widetilde{P} := \prod_{j=1}^{D} U - L(\Gamma_j^{(\kappa)}) = \frac{1}{H(A)} \prod_{j=1}^{D} (H_j(A) U - G_j(A)) \tag{31}$$

Observe that, for each $0 \leq i \leq D$, the coefficient of the monomial U^i in the polynomial $\widetilde{P}$ is a rational function $\Psi_i/H \in K(A)$ (where $\Psi_i \in K[A]$).

Since for the lifting point $a \in K^N$ constructed in Section 3.2.1 we have that $H(a) = \prod_{j=1}^{D} h(a, \gamma_j) \neq 0$, these rational functions Ψ_i/H can be interpreted as elements of the power series ring $K[[A-a]]$ and, from the definition of the polynomial $\widetilde{P}$, it follows that, for each $0 \leq i \leq D$, Ψ_i/H approximates with precision 2^κ the corresponding coefficient $\Phi_i \in K[[A-a]]$ of the monomial U^i in the minimal polynomial P of the linear form L. In this sense, we will say that $\widetilde{P}$ approximates P with precision 2^κ.

The numerators $\Psi_0, \ldots, \Psi_D$ can be obtained as the coefficients of the polynomial $H(A)\widetilde{P}(A,U)$ with respect to the variable U by an interpolation procedure, while the denominator H can be obtained from its definition (30).

Now we estimate the complexity of these computations, assuming that the lifting point $a \in K^n$ and all the points γ_j $(1 \leq j \leq D)$ lying on its fiber are known:
First let us observe that, for each $1 \leq j \leq D$, from Remark 37, the polynomials $H_j(A)$ and $G_j(A)$ can be encoded by straight-line programs of length $O(\kappa\, d^2(n+m)^7 N)$ which are computed straightforward from the definitions (29) and (28).
Then, using these straight-line programs and the definitions (30) and (31), we obtain straight-line programs of length $O(\kappa\, d^2(n+m)^7 N\, D)$ encoding the polynomials $H(A)\widetilde{P}(A,U)$ and $H(A)$.
The complexity of these steps is of order $O(\kappa\, d^2(n+m)^7 N\, D)$.
Finally, the coefficients $\Psi_0, \ldots, \Psi_D$ of $H(A)\widetilde{P}(A,U)$ are computed by interpolation with respect to the variable U (see for instance [12, Prop. 3.1.1]), which involves the resolution of a linear system whose associated matrix is a Vandermonde square $(D+1)\times(D+1)$-matrix. Then, the complexity of this last step is of order $O(\kappa\, d^2(n+m)^7 N\, D^2 + D^4)$, which is also the complexity of the whole procedure, and the length of the slp representation obtained for the polynomials $\Psi_0, \ldots \Psi_D$ is bounded by $O(\kappa\, d^2(n+m)^7 N\, D^2)$.

Summarizing:

Remark 38 *Let $a \in K^N$ be the lifting point constructed in section 3.2.1 and let $\kappa \in \mathbb{N}$. Assume that the D solutions of the system (25) are given. Then, the procedure described above produces a straight-line program of length $O(\kappa\, d^2\,(n+m)^7 N D^2)$ which computes the numerators $\Psi_0, \ldots, \Psi_D \in K[A]$ and the denominator $H \in K[A]$ of the coefficients of a polynomial $\widetilde{P} \in K(A)[U]$ which approximates the minimal polynomial $P \in K(A)[U]$ with precision 2^κ. The sequential complexity of this procedure is of order $O(\kappa\, d^2\,(n+m)^7 N D^2 + D^4)$.*

3.2.5 Computing the minimal polynomial of L

In order to finish the proof of Theorem 34, in this Section we compute numerators and denominators which represent the coefficients of the minimal polynomial $P \in K(A)[U]$ of L with respect to the variable U, from the coefficients of a suitable approximation $\widetilde{P} \in K(A)[U]$ of this minimal polynomial.

For every $0 \leq i \leq D$, let $\Phi_i \in K[[A-a]]$ be the coefficient of the monomial U^i in the expansion of $P \in K(A)[U]$. By Remark 33, each of the series Φ_i $(0 \leq i \leq D)$ is a quotient of two polynomials belonging to the ring $K[A]$ whose total degrees are bounded by Δ. Therefore, Lemma 32 (Padé approximants) enables us to compute, from the homogeneous components of Φ_i of degrees bounded by 3Δ, polynomials $P_i, Q_i \in K[A]$ with $\deg P_i$ and $\deg Q_i$ bounded by Δ, such that $\Phi_i = P_i/Q_i$.
We obtain the required homogeneous components of the coefficients of P from the ones of the corresponding coefficients of a polynomial $\widetilde{P}$ which approximates P with precision 3Δ.

So, we fix $\kappa := \lceil \log(3\Delta) \rceil$ and we assume that a straight-line program which computes numerators $\Psi_0, \ldots, \Psi_D \in K[A]$ and a denominator $H \in K[A]$ of the coefficients of the polynomial $\widetilde{P}$ defined in (31) is given.

The procedure runs as follows:

For $i = 0, \ldots, D$:

1. Compute the homogeneous components of degrees bounded by 3Δ for the series $\Psi_i/H \in K[[A-a]]$. (Let us observe that these components coincide with the corresponding ones of the series Φ_i.)

2. Apply Lemma 32 in order to obtain polynomials $P_i, Q_i \in K[A]$ with $\deg P_i, \deg Q_i \leq \Delta$, $Q_i(a) = 1$ and $P_i/Q_i = \Phi_i$.

Now we estimate its complexity:
Denote by $\mathcal{L}$ the length of a slp which evaluates the input polynomials $\Psi_0, \ldots, \Psi_D$ and the polynomial H.
Fix i, $0 \leq i \leq D$.
Following the arguments given in [15] as well as the complexity estimate for the computation of homogeneous components of a polynomial given by a slp (see for instance [9]), we deduce that the first step of the procedure can be done in time $\mathcal{L}' := O(\Delta^2(\Delta + \mathcal{L}))$ and produces a slp of the same order for the homogeneous components it computes.
Then, by Lemma 32, the computation of the polynomials P_i and Q_i takes $O(\Delta^3(\Delta^4 + \mathcal{L}'))$ additional operations and each of these polynomials is encoded by a slp of length of the same order.

Therefore, we have:

Remark 39 *Let notations and assumptions be as before. Assume that a straight-line program of length $\mathcal{L}$ which evaluates the numerators $\Psi_0, \ldots, \Psi_D$ and the denominator H of the coefficients of the approximating polynomial $\widetilde{P} \in K(A)[U]$ is given. Then, the procedure above computes in time $O(D\Delta^5(\Delta^2 + \mathcal{L}))$, a numerator P_i and a denominator Q_i of degrees bounded by Δ for each coefficient Φ_i $(0 \leq i \leq D)$ of the minimal polynomial P. Each of the polynomials P_i, Q_i is encoded by means of a slp of length $O(\Delta^5(\Delta^2 + \mathcal{L}))$.*

We are now ready to prove Theorem 34:

Proof of Theorem 34. The probabilistic algorithm underlying the proof of the Theorem is obtained combining the procedures described from section 3.2.1 up to this section. Observe that we take $\kappa := \lceil \log(3\Delta) \rceil$ to obtained the desired approximation level.
In order to finish the proof, it suffices to consider the complexity estimations stated in Remarks 35, 36, 38 and 39, which imply that the algorithm runs in time:

$$O((n+m)d\,N) \;+\; O((n^4+m^4)D) \;+\; O(\log(\Delta)\,d^2(n+m)^7N) \;+$$
$$+\,O(\log(\Delta)\,d^2(n+m)^7N\,D^2 + D^4) \;+\; O(D\,\Delta^5(\Delta^2 + \log(\Delta)d^2(n+m)^7N\,D^2)).$$

Taking into account that $D^4 \leq D\Delta^7$ this sum may be estimated by

$$O(D\,\Delta^5(\Delta^2 + \log(\Delta)d^2(n+m)^7N\,D^2)) = O(D\,\Delta^7 + \Delta^5\log(\Delta)d^2(n+m)^7N\,D^3).$$

The length of the straight-line program encoding the polynomials P_i and Q_i $(0 \leq i \leq D)$ which represent the coefficients of the polynomial P follows in the same way from Remarks 38 and 39. ■

3.3 Description of the isolated points of a bihomogeneous polynomial system

We briefly recall the notations introduced in the previous sections.
Let $f_1, \ldots, f_{n+m} \in K[A, x, y]$ be the affinized polynomials which become from the generic bihomogeneous polynomials $F_1, \ldots, F_{n+m} \in K[A, X, Y]$, where A denotes the variable-coefficients.
Consider the parameters

$$\begin{aligned}
d_i &:= \deg_x(f_i), \qquad 1 \leq i \leq n+m,\\
e_i &:= \deg_y(f_i), \qquad 1 \leq i \leq n+m,\\
d &:= \max\{d_i + e_i \ / \ 1 \leq i \leq n+m\},\\
N_i &:= \binom{d_i+n}{n}\binom{e_i+m}{m}, \qquad 1 \leq i \leq n+m\\
N &:= \sum_{i=1}^{n+m} N_i,\\
D &:= \sum d_{j_1} \ldots d_{j_n} e_{k_1} \ldots e_{k_m},\\
\Delta &:= \sum (d_{j_1}+1)\ldots(d_{j_n}+1)(e_{k_1}+1)\ldots(e_{k_m}+1),
\end{aligned}$$

and the varieties

$$\begin{aligned}
\mathcal{V} : &= \{(a,x,y) \in \mathbb{A}^N \times \mathbb{A}^n \times \mathbb{A}^m \ / \ f_1(a,x,y) = 0, \ldots, f_{n+m}(a,x,y) = 0\}\\
V : &= \{(x,y) \in \mathbb{A}^{n+m}_{K(A)} \ / \ f_1(x,y) = 0, \ldots, f_{n+m}(x,y) = 0\}.
\end{aligned}$$

From Theorem 29 and [6], we know that D is the degree of V or equivalently, the degree of the generic fiber of the projection morphism $\pi : \mathcal{V} \to \mathbb{A}^N$ defined as $\pi(a,x,y) := a$.
From Corollary 30, Δ is an upper bound for $\deg(\mathcal{V})$.

3.3.1 Passing from the generic system to a specific system

For each $1 \leq i \leq n+m$ let $b_i \in K^{N_i}$, and set $b := (b_1, \ldots, b_{n+m}) \in K^N$.
The vector b induces a particular instance of our generic bihomogeneous polynomial system: the specific system obtained from the generic one

$$f_1(A,x,y) = 0, \ldots, f_{n+m}(A,x,y) = 0$$

by the evaluation

$$A^{(i)} \mapsto b_i, \qquad \text{for } i = 1, \ldots, n+m.$$

Denote by $V_b \subset \mathbb{A}^{n+m}$ the variety defined by this specific system, namely

$$V_b := \{(x,y) \in \mathbb{A}^n \times \mathbb{A}^m : f_1(b_1,x,y) = 0, \ldots, f_{n+m}(b_{n+m},x,y) = 0\}. \tag{32}$$

The goal of this section is to obtain, for each linear form $L \in K[x,y]$ which separates the points of the variety $V \subset \mathbb{A}^{n+m}_{K(A)}$, a univariate polynomial $P_L^{(b)}(U) \in K[U]$, depending on the point b, such that $P_L^{(b)}(L) \in K[x,y]$ is a non zero polynomial which vanishes in all the isolated points of V_b.

More precisely, with the notations introduced above, we will prove the following:

Theorem 40 *Let L be a linear form in $K[x,y]$ which separates the points of the generic variety $V \subset \mathbb{A}^{n+m}_{K(A)}$. Then, there exists a probabilistic algorithm which computes a non zero polynomial $P_L^{(b)} \in K[U]$ with $\deg_U(P_L^{(b)}) \leq D$ such that $P_L^{(b)}(L) \in K[x,y]$ vanishes in every isolated point of V_b. The algorithm runs in time $O(D^3\Delta^6(\Delta^2 + \log(\Delta)d^2(n+m)^7 N\, D^2))$.*

The polynomial $P_L^{(b)}$ will be obtained from the minimal polynomial of L computed by means of Theorem 34.
First, we show how to compute for any separating linear form L, a non zero polynomial $P_L \in K[A,U]$ such that $P_L(A,L)$ belongs to the ideal $(f_1,\ldots,f_{n+m}) \subset K[A,x,y]$.

Let L be a linear form in $K[x,y]$ and let $\Phi_L : \mathcal{V} \to \mathbb{A}^N \times \mathbb{A}$ be the morphism

$$\Phi_L(a,x,y) := (a, L(x,y)). \tag{33}$$

Since $\mathcal{V}$ is a N-dimensional irreducible variety and π is a dominant morphism, we observe that the Zariski closure of $\mathrm{Im}(\Phi_L) \subset \mathbb{A}^N \times \mathbb{A}$ is an algebraic irreducible variety of codimension 1, and then, it is defined by a square-free polynomial $Q_L \in K[A,U]$ (where U denotes a new variable).
Moreover, since $(f_1,\ldots,f_{n+m})$ is a prime ideal in $K[A][x,y]$ and $Q_L(a,L(x,y)) = 0$ for all $(a,x,y) \in \mathcal{V}$, we deduce:

$$\deg_U(Q_L) > 0 \qquad \text{and} \qquad Q_L(A,L(x,y)) \in (f_1,\ldots,f_{n+m})K[A][x,y]. \tag{34}$$

Now suppose that L separates the points of the variety $V \subset \mathbb{A}^{n+m}_{K(A)}$.

Let $P(A,U) \in K(A)[U]$ be the minimal polynomial of L in the algebraic extension

$$K(A) \hookrightarrow K(A)[x,y]/(f_1,\ldots,f_{n+m}).$$

Hence $P(A,L) \in K(A)[x,y]$ belongs to the ideal $(f_1,\ldots,f_{n+m})K(A)[x,y]$. If $h(A) \in K[A]$ is any polynomial such that $h(A)P(A,U)$ is a polynomial in $K[A,U]$, there exists a denominator $s(A) \in K[A] - \{0\}$ such that $s(A)h(A)P(A,L)$ belongs to the ideal $(f_1,\ldots,f_{n+m})K[A,x,y]$, which is a prime ideal. Since this ideal does not contain any non zero polynomial in $K[A]$, we deduce that $h(A)P(A,L)$ also belongs to the ideal $(f_1,\ldots,f_{n+m})K[A,x,y]$.
In particular $h(A)P(A,L)$ vanishes in every point in $\mathcal{V}$ and so, $h(A)P(A,U)$ vanishes over $\mathrm{Im}(\Phi_L)$. Then $h(A)P(A,U)$ is a multiple of Q_L in $K[A,U]$, and this fact holds for any $h \in K[A]$ such that $h(A)P(A,U) \in K[A,U]$.
On the other hand, from (34) we have that Q_L is a non zero polynomial in $K[A][U]$ such that the class of $Q_L(A,L(x,y))$ in $K(A)[x,y]/(f_1,\ldots,f_{n+m})$ is zero, so $Q_L(A,U)$ gives an algebraic equation for the class of L over $K(A)$ and therefore $P(A,U)$ divides $Q_L(A,U)$ in $K(A)[U]$.
From section 3.2.5 and the previous arguments we conclude that $D = \deg_U(P) = \deg_U(Q_L)$ and both polynomials differ in a multiple in $K(A)$.

Applying the algorithm underlying Theorem 34, we are able to compute polynomials $P_i, Q_i \in K[A]$, $i = 0,\ldots,D$, such that $\deg(P_i) \le \Delta$, $\deg(Q_i) \le \Delta$ and $P = \sum_{i=0}^{D} (\frac{P_i}{Q_i}) U^i$ (each quotient P_i/Q_i represents a power series $\Phi_i \in K[[A-a]]$ for the lifting point $a \in K^N$ chosen in section 3.2.1).

Let us consider the polynomial $P_L \in K[A,U]$ defined as

$$P_L := \sum_{i=0}^{D} \Big(P_i \prod_{\substack{0 \le j \le D \\ j \ne i}} Q_j \Big)\, U^i. \tag{35}$$

Observe that $P_L = P \prod_{i=0}^{D} Q_i$ and so, it is obtained from P by a trivial elimination of denominators. Then, the polynomials P_L and Q_L differ in a multiple in $K[A,U]$. Since $\deg_U(P_L) = \deg_U(Q_L)$, this multiple lies in $K[A]$ and therefore, as we have observed above for any $K[A]$-multiple of P belonging to $K[A,U]$,

$$P_L(A,L) \in (f_1,\ldots,f_{n+m}) \ \text{ in } \ K[A,x,y]. \tag{36}$$

For each $0 \leq i \leq D$ denote

$$P_{L\,i} := P_i \prod_{\substack{0 \leq j \leq D \\ j \neq i}} Q_j \tag{37}$$

the coefficients of P_L considered as a polynomial in the variable U. The coefficients $P_{L\,0}, P_{L\,1}, \ldots P_{L\,D}$ are polynomials in $K[A]$ whose degrees are bounded by ΔD.
Observe that the leading coefficient of P_L viewed as a polynomial in the variable U is

$$P_{L\,D} = \prod_{j=0}^{D-1} Q_j \tag{38}$$

as P is monic in U because it is a minimal polynomial, and then $P_{L\,D}(a) \neq 0$ for the lifting point $a \in K^N$ (recall that, by construction, $Q_j(a) \neq 0$ for every $0 \leq j \leq D$).
In particular, the polynomial $P_L(a, U)$ is not the zero polynomial in the ring $K[U]$.

We estimate the complexity for the computation of (the dense encoding of) P_L:

Denote $\mathcal{L}_0 := \Delta^5(\Delta^2 + \log(\Delta)\, d^2(n+m)^7 N\, D^2)$.
For every index i, $0 \leq i \leq D$, Theorem 34 states that the polynomials $P_i, Q_i \in K[A]$ can be evaluated by a slp of length $O(\mathcal{L}_0)$ and these slp's are constructed in time $O(D\mathcal{L}_0)$.
Hence formula (37) implies that each of the coefficients P_{Li} $(0 \leq i \leq D)$ can be encoded by a slp of length $O(D\,\mathcal{L}_0 + D)$, and all these slp's can be constructed within complexity $O(D\,\mathcal{L}_0 + D^2)$.
From the definition of $\mathcal{L}_0$, it follows that these quantities may also be written as $O(D\,\mathcal{L}_0)$ and then we have:

Remark 41 *For each index i, $0 \leq i \leq D$, the coefficient $P_{Li} \in K[A]$ of the polynomial $P_L = \sum_{i=0}^{D} P_{Li}\, U^i$ can be encoded by a slp of length $O(D\Delta^5(\Delta^2 + \log(\Delta)\, d^2(n+m)^7 N\, D^2))$.*
All these slp's can be constructed by means of an algorithm with similar running time order.

We are now ready to prove the main result of this section.

Proof. (Proof of Theorem 40.) Let notations and assumptions be as before.
From condition (36) we have that $P_L(A, L)$ belongs to the ideal $(f_1, \ldots, f_{n+m})K[A, x, y]$ and then (by simple evaluation)

$$P_L(b, L) \in (f_1(b, x, y), \ldots, f_{n+m}(b, x, y))K[x, y]. \tag{39}$$

If $P_L(b, U) \in K[U]$ is not the zero polynomial there is nothing to do: we take

$$P_L^{(b)} := P_L(b, U) \in K[U]$$

and, from (39), we have that $P_L(b, L) = 0$ over V_b; in particular, it vanishes over all the isolated points of V_b.

Now let us suppose that the polynomial $P_L(b, U)$ is identically zero.

Let t be a new variable and consider the polynomial

$$\widetilde{P} := P_L(b + t(a - b), U) = \widetilde{P}_D(t)\, U^D + \cdots + \widetilde{P}_1(t)\, U + \widetilde{P}_0(t) \in K[t, U],$$

where $a \in K^N$ denotes the lifting point chosen in section 3.2.1.
With these notations, the condition "$P_L(b, U)$ is identically zero" is equivalent to $\widetilde{P}_i(0) = 0$ for every $i = 0, \ldots, D$.
Set $r := \max\{k \in \mathbb{N} : t^k \text{ divides } \widetilde{P}_i \text{ for every } 0 \leq i \leq D\}$.

Observe that $r \geq 1$ because $P_L(b,U) \equiv 0$. On the other hand, the leading coefficient $\widetilde{P}_D(t)$ is exactly $P_{L\,D}(b+t(a-b)) = \prod_{0\leq j\leq D-1} Q_j(b+t(a-b))$ (see (38)) and then, it is not zero as a polynomial in t, that is $f<\infty$, as $\widetilde{P}_D(1) = \prod_{0\leq j\leq D-1} Q_j(a) \neq 0$.

Moreover, as $\deg_A P_L \leq D\,\Delta$, the inequality $1 \leq r \leq D\,\Delta$ holds.

We can write

$$\widetilde{P} = t^r\,(\widetilde{p}_D U^D + \widetilde{p}_{D-1}U^{D-1} + \cdots + \widetilde{p}_0)$$

for suitable $\widetilde{p}_j \in K[t]$, $0 \leq j \leq D$, such that there exists j verifying $\widetilde{p}_j(0) \neq 0$.

Claim: *Set $\widetilde{p} := \widetilde{p}_D U^D + \widetilde{p}_{D-1}U^{D-1} + \cdots + \widetilde{p}_0 \in K[t,U]$. The polynomial $\widetilde{p}(0,L) \in K[x,y]$ vanishes in all the isolated points of V_b.*

Proof of the claim: For each $1 \leq i \leq n+m$ let

$$\widetilde{f}_i := f_i(b+t(a-b),x,y) \in K[t,x,y]. \tag{40}$$

From the construction of the polynomials P_L and $\widetilde{P}$ it follows immediately from (36) that

$$\widetilde{P}(t,L) = t^r \widetilde{p}(t,L) \in (\widetilde{f}_1,\ldots,\widetilde{f}_{n+m}) \ \text{ in } K[t,x,y]. \tag{41}$$

Let $\Im := \sqrt{(\widetilde{f}_1,\ldots,\widetilde{f}_{n+m})} \subset K[t,x,y]$ be the nilradical of the ideal $(\widetilde{f}_1,\ldots,\widetilde{f}_{n+m})$ and let $\bigcap_{k=1}^{s} \wp_k$ be the primary irredundant decomposition of $\Im$. In particular, each $\wp_k$ is a prime ideal of $K[t,x,y]$ and $\wp_k \not\subset \wp_{k'}$ if $k \neq k'$.

From (41) we have that $t^r\widetilde{p}(t,L) \in \Im$, and $\widetilde{p}(t,L)$ belongs to the prime ideal $\wp_k$ for all those indices k such that $t \notin \wp_k$. In other words:

$$\widetilde{p}(t,L) \in \bigcap_{\substack{1\leq k\leq s\\ t\notin\wp_k}} \wp_k. \tag{42}$$

In order to prove that $\widetilde{p}(0,L)$ vanishes in the isolated points of V_b, we start observing the following identity which is a straightforward consequence of (32) and (40):

$$\{(t,x,y) \in \mathbb{A}^1 \times \mathbb{A}^{n+m} \,/\, \widetilde{f}_1 = 0,\ldots,\widetilde{f}_{n+m} = 0, t = 0\} = \{0\} \times V_b.$$

Let $\xi \in V_b$ be an isolated point. Then $(0,\xi)$ is an isolated point of $\{0\} \times V_b$.
For $k = 1,\ldots,s$, denote $V(\wp_k) \subset \mathbb{A}^1 \times \mathbb{A}^{n+m}$ the irreducible algebraic set defined by the zeros of the prime ideal $\wp_k$. Then, from the primary decomposition of $\Im$, it follows that $\{(t,x,y) \in \mathbb{A}^1 \times \mathbb{A}^{n+m} \,/\, \widetilde{f}_1 = 0,\ldots,\widetilde{f}_{n+m} = 0\} = \bigcup_{k=1}^{s} V(\wp_k)$ and, therefore,

$$\{(t,x,y) \in \mathbb{A}^1 \times \mathbb{A}^{n+m} \,/\, \widetilde{f}_1 = 0,\ldots,\widetilde{f}_{n+m} = 0, t = 0\} = \bigcup_{k=1}^{s} \Big(V(\wp_k) \cap \{t=0\}\Big).$$

In particular, for the considered isolated point ξ, there exists at least one index k_0, $1 \leq k_0 \leq s$, such that

$$(0,\xi) \in V(\wp_{k_0}) \cap \{t=0\}. \tag{43}$$

Since the algebraic varieties $V(\wp_k)$ $(1 \leq k \leq s)$ are the irreducible components of the algebraic set $\{(t,x,y) \in \mathbb{A}^1 \times \mathbb{A}^{n+m} \,/\, \widetilde{f}_1 = 0,\ldots,\widetilde{f}_{n+m} = 0\}$, which is defined by $(n+m)$-many equations in a $(n+m+1)$-dimensional ambient space, we conclude that $\dim(V(\wp_k)) \geq 1$ for all $k = 1,\ldots,s$.

Therefore, if $t \in \wp_k$ (or equivalently, if $V(\wp_k) \subset \{t = 0\}$), we infer that $V(\wp_k) \cap \{t = 0\} = V(\wp_k)$ is irreducible of dimension at least one and then it does not contain any isolated point. In particular, $t \in \wp_k$ implies $(0, \xi) \notin V(\wp_k)$.
Hence, condition (43) implies that $t \notin \wp_{k_0}$, and so, by (42), $\widetilde{p}(t, L) \in \wp_{k_0}$. Again by (43) we conclude that $\widetilde{p}(0, L(\xi)) = 0$.
This finishes the proof of the Claim.

We define

$$P_L^{(b)} := \widetilde{p}(0) = \widetilde{p}_D(0)U^D + \cdots + \widetilde{p}_1(0)U + \widetilde{p}_0(0).$$

From the construction of $\widetilde{p}$, it follows that $P_L^{(b)} \in K[U]$ is a non-zero polynomial and, by the previous Claim, this polynomial vanishes in all the isolated points of V_b.

The algorithm computing the polynomial $P_L^{(b)}$ runs in the following way:

1. Evaluate the indeterminate coefficients A in the vector b in the coefficients $P_{L\,0}, P_{L\,1}, \ldots, P_{L\,D}$ of the polynomial P_L.
2. If $P_{L\,j}(b) \neq 0$ for some $0 \leq j \leq D$, take $P_L^{(b)}(U) := P_L(b, U)$.
3. If $P_{L\,j}(b) = 0$ for every $0 \leq j \leq D$, consider the polynomial $\widetilde{P}(t, U) := P_L(b + t(a - b), U)$. Let $\widetilde{P}_0, \ldots, \widetilde{P}_D \in K[t]$ be the coefficients of $\widetilde{P}$ as a polynomial in the variable U (in other words, $\widetilde{P}_j = P_{Lj}(b + t(a - b))$.
4. Compute $r := \max\{k : t^k \text{ divides } \widetilde{P}_j \text{ for every } 0 \leq j \leq D\}$ as follows:
   For each $j = 0, \ldots, D$
   (a) Compute the coefficients of the polynomial $\widetilde{P}_j = \sum_{k=0}^{D\Delta} \widetilde{P}_{jk} t^k$.
   (b) Set $k_j := \min\{k : \widetilde{P}_{jk} \neq 0\}$.
   Take $r := \min\{k_j : j = 0, \ldots, D\}$.
5. Set $P_L^{(b)}(U) := \sum_{j=0}^{D} \widetilde{P}_{jr}\, U^j$.

In order to finish the proof of the theorem we estimate the complexity of the algorithm:

For the sake of simplicity denote by $\mathcal{L} := D\,\Delta^5(\Delta^2 + \log(\Delta) d^2 (n+m)^7 N\, D^2)$, namely the complexity time order required for the construction of the coefficients of the polynomial P and the length order of the slp's encoding each coefficient of the polynomial P_L (see Remark 41).

The computations in steps 1 and 2 can be done within complexity $O(D\mathcal{L})$, as they involve the specialisation of D polynomials given by slp's of length $O(\mathcal{L})$ each.
For every $0 \leq j \leq D$, a slp encoding of the coefficient $\widetilde{P}_j$ considered in step 3 is obtained from the slp encoding the corresponding coefficient P_{Lj} by evaluation in the vector $b + t(a - b)$, which does not modify the slp length order. This step does not increase the order of complexity.
To estimate the complexity of the last step, let us observe that for each index j, $\deg \widetilde{P}_j \leq \deg_A(P_L) \leq D\Delta$ (see (35)), and $\widetilde{P}_j$ is given by a slp of length $O(\mathcal{L})$. Then, we may obtain all the coefficients of the polynomials $\widetilde{P}_j$ $(0 \leq j \leq D)$ in time $O(D^2\Delta\,\mathcal{L} + (D\Delta)^4)$ by means of a standard interpolation procedure.
The comparisons needed to determine r do not change the complexity order.
Finally, step 5 does not modify the complexity either, as the polynomial defined can be constructed with $O(D)$ operations from the coefficients $\widetilde{P}_{jr}$ which have been computed in the previous step.

From the definition of $\mathcal{L}$ and the inequality $D \leq \Delta$, we have that the complexity of the whole algorithm may be estimated as $O(D^2\Delta\,\mathcal{L}) = O(D^3\Delta^6(\Delta^2 + \log(\Delta) d^2 (n+m)^7 N\, D^2))$.

This finishes the proof of the theorem. ■

Remark 42 *If V_b is a zero dimensional variety containing exactly D many points and the linear form L separates the points of V_b, then the roots of $P_L^{(b)}$ are exactly $L(\xi)$ with $\xi \in V_b$.*

3.3.2 Describing the isolated points of a specific system

Let $b \in \mathbb{A}^N$ as in the previous section and denote

$$V_b := \{(x,y) \in \mathbb{A}^{n+m} \ / \ f_1(b,x,y) = 0, \ldots, f_{n+m}(b,x,y) = 0\}$$

the solution of the particular instance of the generic bihomogeneous system obtained by the evaluation $A \mapsto b$.
This section is devoted to compute the geometric resolution of a 0-dimensional variety contained in V_b and containing the set of the isolated points of the variety V_b (see also [3] or [9]).
For this purpose we combine the construction of linear forms which separates isolated points of a given algebraic variety (following [9]) with the algorithm described in Theorem 40 in order to obtain an adequate generic family of linear forms L and in some sense their minimal polynomials over the isolated points of V_b.
Finally we apply the well-known trick based on the chain rule producing the geometric resolution (see for instance [5, Section 3.3]).

We start observing that there exist sufficiently many K-linear forms which separate the points of the generic 0-dimensional algebraic variety $V \subset \mathbb{A}^{n+m}_{\overline{K(A)}}$:

Remark 43 *The K-genericity of the coefficients of the equations defining V is preserved by any K-linear change of coordinates in K^n and/or in K^m. Then, if $(\lambda_1, \ldots, \lambda_n) \in K^n$, $(\lambda_{n+1}, \ldots, \lambda_{n+m}) \in K^m$ are arbitrary non-zero vectors, the linear form*

$$L := \sum_{i=1}^{n} \lambda_i x_i + \sum_{i=n+1}^{n+m} \lambda_i y_{i-n}$$

separates the points of V (if we suppose the contrary, none K-linear form involving at least one variable x_i and at least one variable y_j separates the points of V, but there exists a non-empty Zariski open subset of K^{n+m} of separating linear forms).

Consider the following linear forms:

$$z_k := x_k + y_1, \qquad k = 1, \ldots, n. \tag{44}$$

$$z_k := y_{k-n} - x_1 \qquad k = n+1, \ldots, n+m.$$

Clearly these new variables are linearly independent and then they define a system of coordinates in K^{n+m} or $\overline{K(A)}^{n+m}$.
¿From the previous Remark, all linear form z_k separates the points of the variety V.
Therefore we may apply Theorem 40 for $L := z_k$ an so we obtain an univariate polynomial non zero polynomial $P_{z_k}^{(b)} \in K[U]$ such that $P_{z_k}^{(b)}(z_k) \in K[x,y]$ vanishes in all isolated point of V_b. Moreover, without modify the complexity order of Theorem 40, we also may suppose that the univariate polynomial $P_{z_k}^{(b)}$ is square-free.

Let $T := (T_1, \ldots T_{n+m})$ be new indeterminates over $\overline{K}(A)$ (in particular also indeterminates over K).
For every $k = 1, \ldots n+m$, denote by $\hat{z}_k$ the following linear form in $K[T_1, \ldots, T_{n+m}][x,y]$:

$$\hat{z_k} := T_1 z_1 + \cdots + T_{k-1} z_{k-1} + T_{k+1} z_{k+1} + \cdots + T_{n+m} z_{n+m}.$$

Again Remark 43 implies that the linear forms $\hat{z}_k$ separate the points of V for any vector $(t_1, \ldots, t_{n+m})$ lying in a suitable Zariski non-empty open subset $\mathcal{U} = \{H(T_1, \ldots, T_{n+m}) \neq 0\} \subset K^{n+m}$.
Moreover, a polynomial H may be explicitly given:

- if $n, m > 1$ take $H := T_2 T_{n+2}(T_{n+1} + \cdots + T_{n+m} - T_1)(T_1 + \cdots + T_n + T_{n+1})$.
- if $n > 1,\ m = 1$ take $H := T_2(T_1 - T_{n+1}) \prod_{i=1}^{n+1}(T_1 + \cdots + T_{i-1} + T_{i+1} + \cdots + T_{n+1})$.
- if $n = 1,\ m > 1$ take $H := T_1(T_1 + T_2)(T_2 + \cdots + T_{m+1}) \prod_{i=2}^{m+1}(T_2 + \cdots + T_{i-1} + T_{i+1} + \cdots + T_{m+1} - T_1)$.
- if $n = m = 1$ take $H := T_1 T_2$.

Following the construction of the minimal polynomial P of Theorem 34, observe that if the separating linear form L is a linear combination of the variables x, y, then the polynomial P depends also polynomially on the coefficients of L, because P is the product $\prod_{j=1}^{D}(U - L(\Gamma_j))$, where Γ_j are the points of V (see Section 3.2.4).
In particular, since the variables z_k and the linear forms $\hat{z_k}$ are linear combinations of the variables x, y, for each index k we have that P depends polynomially in T (where P denotes the minimal polynomial of the linear forms z_k or $\hat{z_k}$ over V).
Therefore, if $\tau := (t_1, \ldots, t_{m+n}) \in \mathcal{U}$, the minimal polynomial associated to the linear form $\hat{z_k}(\tau)$ over V is well defined and it is obtained especializing the vector T in τ in the minimal polynomial of the generic form $\hat{z_k}$ over V.

Now, following the procedure described in Section 3.3.1, it is easy to construct in adequate running time a non-zero polynomial $H' \in K[T_1, \ldots, T_{m+n}]$ such that for any $\tau := (t_1, \ldots, t_{n+m}) \in K^{n+m} \setminus \{H' = 0\} \subset \mathcal{U}$, the polynomial $P^{(b)}_{\hat{z_k}(\tau)} \in K[U]$ constructed in Theorem 40, is square-free and depends polynomially in τ.

Following [9, Lemma 25 and Prop. 27], it is possible to construct in addmisible time from the generic linear forms z_k and $\hat{z_k}$, $k = 1, \ldots, n+m$ a new non zero polynomial $\widetilde{H} \in K[T_1, \ldots, T_{n+m}]$ such that for any $\tau = (t_1, \ldots, t_{n+m}) \in K^{n+m} \setminus \{\widetilde{H} = 0\}$ the following conditions are fullfiled:

- the linear form $L_\tau := \sum_{i=1}^{n} t_i x_i + \sum_{i=n+1}^{n+m} t_i y_{i-n}$ separates the isolated points of V_b.
- the polynomial $P^{(b)}_{L_\tau} \in K[U]$ depends polynomially on τ, it is square-free and vanishes in $L_\tau(q)$ for all isolated point $q \in V_b$ (in other word $P_{L_\tau}(\tau, L_\tau(q)) = 0$ for all isolated point $q \in V_b$).

Let us consider now the polynomial $P^{(b)}_{L_T} \in K[T][U]$, where $L_T := T_1 x_1 + \cdots + T_n x_n + T_{n+1} y_1 + \cdots + T_{n+m} y_m$. Denote by $I \subset K[x, y]$ the 0-dimensional ideal of the isolated points of V_b. Therefore the previous arguments implies that

$$P_{L_T}(L_T(x, y)) \in I K[T]_{\widetilde{H}}[x, y], \tag{45}$$

where $K[T]_{\widetilde{H}}$ denotes the ring of coordinates of the open $K^{n+m} \setminus \{\widetilde{H} = 0\}$.
Taking in (45) the derivative with respect to the variable T_i, $i = 1, \ldots, n+m$ (see for instance [5, Section 3.3]) and replacing the variables T in an arbitrary but fixed vector τ such that $\widetilde{H}(\tau) \neq 0$, we obtain a Kronecker parametric description of a finite set containing the isolated points of V_b (shape lemma):

$$\begin{cases} \rho(U)x_1 = v_1(\tau, U) \\ \vdots \quad \vdots \quad \vdots \\ \rho(U)x_n = v_n(\tau, U) \\ \rho(U)y_1 = v_{n+1}(\tau, U) \\ \vdots \quad \vdots \quad \vdots \\ \rho(U)y_m = v_{n+m}(\tau, U) \\ \\ P_{L_\tau}(U) = 0 \end{cases}, \tag{46}$$

where $\deg_U(v_i) < \deg_U(P_{L_\tau})$ and $\rho(U) := \dfrac{\partial P_{L_T}}{\partial U}(\tau, U)$. Observe that since $P_{L_T}(\tau, U)$ is square free we have $\rho(U)$ and $P_{L_T}(\tau, U)$ relatively prime in $K[U]$.

Finally, in order to avoid those points (x, y) verifying relations (46) but lying outside the algebraic set V_b, we replace the condition $P_{L_\tau}(U) = 0$ by a new polynomial equation $Q(U) = 0$, where $Q \in K[U]$ is constructed as follows:

1. Recall that for all i, $1 \leq i \leq n+m$, we denote $d_i := \deg_x(f_i)$, $e_i := \deg_y(f_i)$ and $d := \max\{d_i + e_i \ / \ 1 \leq i \leq n+m\}$. Therefore, for any index i, $\rho^d f_i(b, \dfrac{v_1}{\rho}, \ldots, \dfrac{v_{n+m}}{\rho})$ belongs to the polynomial ring $K[U]$.

2. Let Q be the GCD in $K[U]$ of the polynomials $\rho^d f_i(b, \dfrac{v_1}{\rho}, \ldots, \dfrac{v_{n+m}}{\rho})$, $1 \leq i \leq n+m$, and the polynomial P_{L_τ}.

Observe that Q and ρ are relatively prime polynomials in $K[U]$.

Hence

$$W_b := \left\{ \left(\frac{v_1(u)}{\rho(u)}, \ldots, \frac{v_{n+m}(u)}{\rho(u)} \right) \text{ with } Q(u) = 0 \right\}$$

is a 0-dimensional variety defined by a Kronecker (or uniparametric) parametrisation and satisfying :

- $W_b \subseteq V_b$.
- All the isolated points of V_b belong to W_b.

References

[1] L. Caniglia, A. Galligo, J. Heintz *Some new effectivity bounds in computational geometry,* Proc. 6th Int. Conf. Applied Algebra, Algebraic Algorithms and Error Correcting Codes AAECC–6, Roma 1988, Springer Lect. Notes Comput.Sci. **357** 131-151 (1989)

[2] D. Eisenbud, *Commutative Algebra with a view toward Algebraic Geometry (Grad. Texts Math. **150**) Springer 1994*

[3] M. Giusti, J. Heintz, *La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial,* Symposia Matematica, Vol XXXIV (1993) 216-256.

[4] M. Giusti, K. Hägele, J. Heintz, J. L. Montaña, L. M. Pardo, J. E. Morais, *Lower bounds for diophantine approximation,* J. Pure Appl. Algebra **117 & 118** (1997), pp. 277–317.

[5] M. Giusti, G. Lecerf, B. Salvy, *A Gröbner free alternative for polynomial system solving,* J. Complexity 17 (2001), No. 1, 154–211.

[6] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields,* Theoret. Comput. Sci. 24 (3) (1983) 239–277.

[7] J. Heintz, T. Krick, S. Puddu, J. Sabia, A. Waissbein, *Deformation techniques for efficient polynomial equation solving,* Journal of Complexity **16** (2000), pp. 70-109.

[8] W. Hodge, D. Pedoe: *Methods of Algebraic Geometry, Vol. 1, Cambridge Univ. Press 1968.*

[9] T. Krick, L. M. Pardo, *A computational method for diophantine aproximation,* Progress in Mathematics **143** (1996) 193-253.

[10] H. Matsumura: *Commutative Ring Theory. Cambridge Studies in Adv. Math.*

[11] A. Morgan, A. Sommese , C. Wampler, *A product-decomposition theorem for bounding Bézout numbers,* SIAM J. Numer. Anal. 32, 4, 1308-1325.

[12] S. Puddu, J. Sabia, *An effective algorithm for quantifier elimination over algebraically closed fields using straight line programs*, J. Pure Appl. Algebra **129** (1998) 173-200.

[13] J. Sabia, P. Solernó *Bounds for Traces in Complete Intersections and Degrees in the Nullstellensatz,* AAECC Journal **6**, No.6, Springer-Verlag (1995) 353-376.

[14] E. Schost: *Computing parametric geometric resolutions. Computing parametric geometric resolutions,* Appl. Algebra Engrg. Comm. Comput. 13 (2003), No. 5, 349–393.

[15] V. Strassen: *Vermeidung von Divisionen,* Journal für die Reine und Angewandte Mathematik **264** (1973) pp. 182–202.

[16] A. Walker, *Algebraic Curves. Princeton University Press, 1950.*