INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Some applications of Bezoutians in Effective Algebraic Geometry

Mohamed Elkadi — Bernard Mourrain

N° 3572

Décembre 1998

THÈME 2

Rapport de recherche

ISSN 0249-6399

Some applications of Bezoutians in Effective Algebraic Geometry

Mohamed Elkadi* , Bernard Mourrain†

Thème 2 — Génie logiciel
et calcul symbolique
Projet SAGA

Rapport de recherche n° 3572 — Décembre 1998 — 38 pages

Abstract: In this report, we investigate some problems of effectivity, related to algebraic residue theory. We show how matrix techniques based on Bezoutian formulations, enable us to derive new algorithms for these problems, as well as new bounds for the polynomials involved in these computations. More precisely, we focus on the computation of relations of algebraic dependencies between $n+1$ polynomials in n variables and show how to deduce the residue of n polynomials in n variables. Applications for testing the properness of a polynomial map, for computing its Lojasiewicz exponent, and for inverting polynomial maps are also considered. We also show how Bezoutian matrices, enable us to compute a non-trivial multiple of the resultant on any irreducible algebraic variety and decompose an algebraic variety into irreducible components.

Key-words: Bezoutian matrix, algebraic residue, Lojasiewicz exponent, polynomial equations, resultant.

* UNSA, UMR 6621, Parc Valrose, B.P. 71, 06108 Nice Cedex02, elkadi@hera.unice.fr
† INRIA, SAGA, 2004 route des Lucioles, B.P. 93, 06902 Sophia Antipolis, mourrain@sophia.inria.fr,
(partially supported by European ESPRIT project FRISCO, LTR 21.024)

Quelques applications des Bézoutiens en Géométrie Algébrique Effective

Résumé : Dans ce rapport, nous étudions quelques problèmes de géométrie algébrique effective, liés à la théorie des résidus algébriques. Nous montrons comment une approche matricielle basée sur les Bézoutiens, nous permet de proposer de nouveaux algorithmes et de nouvelles bornes sur les polynômes intervenants dans ces problèmes. Plus précisément, nous nous penchons sur le calcul de relations de dépendance algébrique entre $n+1$ polynômes en n variables et montrons comment en déduire le calcul du résidu de n polynômes en n variables. Nous considérons ensuite des applications de cette méthode au test de propreté d'une application polynomiale, au calcul de son exposant de Lojasiewicz et à l'inversion explicite d'application polynomiale. Nous montrons également comment les matrices de Bézoutiens nous permettent de calculer un multiple non-trivial du résultant sur une variété algébrique irréductible quelconque (quand celui-ci existe), et de décomposer toute variété algébrique en composantes irréductibles.

Mots-clés : matrice Bézoutienne, résidu algébrique, exposant de Lojasiewicz, équations polynomiales, résultant.

Contents

1 Introduction

In this report, we study some classical problems occurring in effective algebraic geometry, like finding algebraic relations between $n+1$ polynomials in n variables, computing the residue of a zero-dimensional affine complete intersection, testing the properness of a polynomial map, and inverting a polynomial map. These questions can be handled, at least in theory, by elimination methods through Gröbner computations, but sometimes with an unpredictable explosion in the complexity of the computation. Our approach emphasizes on the structure of these computations. It is based on matrix formulations and, more specifically on Bezoutian matrices. This tool has many applications in several areas such as commutative algebra, complex analysis, or complexity theory (see [38], [27], [5], [7], [26], [20]). Here, we exploit a basic but fundamental property, which yields the multiplication map by the polynomial f_0, modulo the n elements $f_1, \dots, f_n$, from the Bezoutian matrix of $f_0, \dots, f_n$. We show how this is sufficient to handle the preceding list of problems and we derive new algorithms for solving them effectively. In particular, we compute the residue τ_f, which describes completely the structure of the quotient ring $\mathcal{A} = R/(f_1, \dots, f_n)$ (see [38], [27], [4], [16]). Thus, in the case of zero-dimensional affine complete intersections, this approach yields a new algorithm for constructing the quotient $\mathcal{A}$, and consequently for solving polynomial systems. Examples (computed in `maple`) illustrate the different techniques. An advantage of our approach is to provide explicit formulations for the objects that we are computing. Therefore, their computational structure can be handled more carefully in order to devise more efficient algorithms, and enable us, for instance, to deduce new bounds on the degree and height of the polynomials involved in these computations.

Let us now describe the connections between the different sections of this paper. After stating the first basic properties of Bezoutians in section 2, we use them in section 3 to compute algebraic relations between $n+1$ polynomials $f_0, \ldots, f_n$ in n variables. The relations obtained for $f_0 = z_i$ are used in section 4 through the generalized transformation law [7], to compute the residue τ_f of the polynomial map $f = (f_1, \ldots, f_n)$. In section 5, we investigate the problem of testing the properness of a polynomial map f and give an algorithm for computing its Lojasiewicz exponent, by analyzing the algebraic relations between z_i and $f_1, \ldots, f_n$ (for $i = 1, \ldots, n$). We propose an algorithm for testing the invertibility of a polynomial map and for computing its inverse, also based on Bezoutian computations. In the next section, we relate Bezoutians and resultants over an irreducible variety. Finally, we show how a maximal minor of the Bezoutian matrix gives us a rational representation of the isolated points of a variety and use it to obtain a geometric decomposition of this variety. This new algorithm is illustrated by examples.

Here are some general notations that will be used hereafter. Let $\mathbb{K}$ be a field, not necessarily of characteristic 0. In some sections we will need to work over $\mathbb{C}$. This will be made more precise. Let $R = \mathbb{K}[z] = \mathbb{K}[z_1, \ldots, z_n]$ be the ring of polynomials in the variables $z_1, \ldots, z_n$, with coefficients in $\mathbb{K}$, $\widehat{R}$ its dual (the set of linear maps from R to $\mathbb{K}$).

The height of $a = \frac{p}{q} \in \mathbb{Q}$ (p and q are relatively prime) is $h(a) = \max(|p|, |q|)$. The height of a polynomial $P = \sum a_\alpha z^\alpha \in \mathbb{Q}[z]$ is $h(P) = \max_\alpha h(a_\alpha)$.

Let $f_1, \ldots, f_n$ be polynomials in R. The ideal generated by these n elements will be denoted by I, the quotient R/I by $\mathcal{A}$ and the class in $\mathcal{A}$ of an element $p \in R$ by $\overline{p}$. We assume in the following that $\mathcal{A}$ *is a finite vector space, of dimension* D, which means that $f_1, \ldots, f_n$ is a complete intersection. We will denote by $\widehat{\mathcal{A}}$ the dual space of $\mathcal{A}$, which we will identify with the vector space $I^\perp = \{\Lambda \in \widehat{R} : \Lambda(g) = 0, \forall g \in I\}$. This dual space $\widehat{\mathcal{A}}$ has an R-module structure: for any $a, b \in R$ and any $\Lambda \in \widehat{\mathcal{A}}$, we have $(a \cdot \Lambda)(b) = \Lambda(ab)$.

2 Basic properties of Bezoutians

In this section, we recall the construction of Bezoutian matrices, that we will use hereafter. We will also give some bounds on the size of these matrices and on the height of their coefficients.

Definition 2.1 *The Bezoutian $\Theta_{f_0,\ldots,f_n}$ of $f_0, \ldots, f_n$ in R (or simply Θ_{f_0} if $f_1, \ldots, f_n$ are fixed) is the polynomial in $\mathbb{K}[z_1, \ldots, z_n, \xi_1, \ldots, \xi_n] = \mathbb{K}[z, \xi]$ defined by*

$$\Theta_{f_0,\ldots,f_n}(z_1, \ldots, z_n, \xi_1, \ldots, \xi_n) := \begin{vmatrix} f_0(z) & \theta_1(f_0)(z,\xi) & \cdots & \theta_n(f_0)(z,\xi) \\ \vdots & \vdots & \vdots & \vdots \\ f_n(z) & \theta_1(f_n)(z,\xi) & \cdots & \theta_n(f_n)(z,\xi) \end{vmatrix},$$

where

$$\theta_i(f_j)(z,\xi) := \frac{f_j(\xi_1, \ldots, \xi_{i-1}, z_i, \ldots, z_n) - f_j(\xi_1, \ldots, \xi_i, z_{i+1}, \ldots, z_n)}{z_i - \xi_i}.$$

Let

$$\Theta_{f_0}(z,\xi) = \sum_{\alpha,\beta} \lambda_{\alpha,\beta}\, z^{\alpha}\xi^{\beta}, \quad \lambda_{\alpha,\beta} \in \mathbb{K} ,$$

be the decomposition of the Bezoutian in $\mathbb{K}[z,\xi]$*. We order the monomials that appear in* Θ_{f_0}*. The matrix* $B_{f_0,\ldots,f_n} = (\lambda_{\alpha,\beta})_{\alpha,\beta}$ *(or simply* B_{f_0}*) is the Bezoutian matrix of* $f_0,\ldots,f_n$*.*

Remark 2.2 —E. Bézout proposed a construction of the resultant of two polynomials f_0, f_1 in one variable based on Θ_{f_0,f_1} (see [6]). This explains the terminology used here.

Remark 2.3 — The determinant in definition 2.1 is invariant if we substitute, in the first column ξ for z.

Definition 2.4 *Let* $\mathbf{v} = (v_i)_{i\in\mathbb{N}}, \mathbf{w} = (w_j)_{j\in\mathbb{N}}$ *be two bases of the* $\mathbb{K}$*-vector space* R*, and let*

$$\Theta_{f_0}(z,\xi) = \sum_{i,j} \nu_{ij}\, v_i(z)\, w_j(\xi) \ , \quad \nu_{ij} \in \mathbb{K} ,$$

be the decomposition of the Bezoutian in these bases. We denote by $[\Theta_{f_0}]_{\mathbf{v},\mathbf{w}} = (\nu_{ij})_{i\in\mathbb{N},j\in\mathbb{N}}$ *the coefficient matrix of* Θ_{f_0} *in the bases* $\mathbf{v}$ *and* $\mathbf{w}$*.*

Remark 2.5 —The matrix $[\Theta_{f_0}]_{\mathbf{v},\mathbf{w}}$ is exactly the matrix of the $\mathbb{K}$-linear map

$$\begin{array}{rcl} \Theta^{\triangleright}_{f_0} : \widehat{R} & \to & R \\ \Lambda & \mapsto & \Theta^{\triangleright}_{f_0}(\Lambda) := \sum_{i,j} \nu_{ij}\Lambda(w_j)v_i(z) \end{array}$$

in the dual basis $(\widehat{w_j})_{j\in\mathbb{N}}$ of $\widehat{R}$ and the basis $(v_i)_{i\in\mathbb{N}}$ of R.

Similarly, we define the map $\Theta^{\triangleleft}_{f_0} : \Lambda \mapsto \Theta^{\triangleleft}_{f_0}(\Lambda) := \sum_{i,j} \nu_{ij}\, \Lambda(v_i)w_j(z)$. The matrix of this map in the bases $(\widehat{v_j})_{j\in\mathbb{N}}$ and $(w_i)_{i\in\mathbb{N}}$ is the transposed of $[\Theta_{f_0}]_{\mathbf{v},\mathbf{w}}$.

The matrix $[\Theta_{f_0}]_{\mathbf{v},\mathbf{w}}$ has only a finite number of non-vanishing entries. Hereafter, $[\Theta_{f_0}]_{\mathbf{v},\mathbf{w}}$ will denote this finite matrix.

The following lemma shows that the Bezoutian matrices B_{f_0}, for all $f_0 \in R$, admit a diagonal decomposition in a common basis. It will be used extensively in the following sections.

Let $I = (f_1,\ldots,f_n)$ and I_0 be the intersection of primary components of I corresponding to isolated points of the variety $\mathcal{V}(I)$ defined by I. We have $I = I_0 \cap J$ and $\mathcal{A}_0 = R/I_0$ of finite dimension D.

Lemma 2.6 *Let* $\mathcal{A}_0 = R/I_0$ *be the quotient algebra associated with the isolated points of* $\mathcal{V}(f_1,\ldots,f_n)$*, and let* D *be its dimension over* $\mathbb{K}$*. There exists two bases* $\mathbf{v} = (v_i)_{i\in\mathbb{N}}$ *and*

$\mathbf{w} = (w_i)_{i\in\mathbb{N}}$ of R such that $(\overline{v}_1,\ldots,\overline{v}_D), (\overline{w}_1,\ldots,\overline{w}_D)$ are bases of $\mathcal{A}_0$, $v_i, w_i \in I_0$ for $i > D$, and for any f_0 in R the matrix $[\Theta_{f_0}]_{\mathbf{v},\mathbf{w}}$ is of the form

$$\begin{array}{cc} \begin{array}{cc} v_1 \ \ldots \ v_D & v_{D+1} \ldots \end{array} & \\ \left(\begin{array}{c|c} M_{f_0} & \mathbf{0} \\ \hline \mathbf{0} & L_{f_0} \end{array}\right) & \begin{array}{l} w_1 \\ \vdots \\ w_D \\ w_{D+1} \\ \vdots \end{array} \end{array} \tag{1}$$

where M_{f_0} is the matrix of multiplication by $\overline{f}_0$ in the basis $(\overline{v}_1,\ldots,\overline{v}_D)$ of $\mathcal{A}_0$.

Proof. Let us assume that $\mathbb{K}$ is algebraically closed and let $\mathcal{V}_0(I) = \{\zeta_1,\ldots,\zeta_d\}$ be the set of isolated roots of $f_1 = \cdots = f_n = 0$. According to the structure theorem of artinian rings (see eg. [41][chap. 4], [32]), we have $\mathcal{A}_0 = \mathcal{A}_{\zeta_1} \oplus \cdots \oplus \mathcal{A}_{\zeta_d}$ where $\mathcal{A}_{\zeta_i} = R_{\mathbf{m}_{\zeta_i}}/I\, R_{\mathbf{m}_{\zeta_i}}$, $\mathbf{m}_{\zeta_i}$ is the maximal ideal defining ζ_i and $R_{\mathbf{m}_{\zeta_i}}$ is the localization at $\mathbf{m}_{\zeta_i}$.

We identify the dual $\widehat{\mathcal{A}}_0$ of $\mathcal{A}_0$ with $I_0^{\perp}$.

Let us consider the two vector subspaces $E = \Theta_1^{\triangleright}(\widehat{\mathcal{A}}_0)$ and $F = \Theta_1^{\triangleleft}(\widehat{\mathcal{A}}_0)$ of R. From $\dim_{\mathbb{K}}(\widehat{\mathcal{A}}_0) = D$, we deduce that E and F are of dimension $\leq D$. According to [27], [38], as $\mathcal{A}_{\zeta_i}$ are local complete intersections defined by $f_1,\ldots,f_n$, $\overline{\Theta}_1^{\triangleright}$ and $\overline{\Theta}_1^{\triangleleft}$ are isomorphisms between $\widehat{\mathcal{A}}_{\zeta_i}$ and $\mathcal{A}_{\zeta_i}$, and thus between $\widehat{\mathcal{A}}_0 = \oplus_{i=1}^d \widehat{\mathcal{A}}_{\zeta_i}$ and $\mathcal{A}_0 = \oplus_{i=1}^d \mathcal{A}_{\zeta_i}$.

Therefore, the image of $\widehat{\mathcal{A}}_0$ by $\Theta_1^{\triangleright}$ and $\Theta_1^{\triangleleft}$ are at least of dimension D. Consequently, $\dim E = \dim F = D$ and E is isomorphic as a vector space to $\mathcal{A}_0$, so that we have $R = E \oplus I_0$ and by symmetry $R = F \oplus I_0$.

From this, we deduce that Θ_1 is in $E\otimes F \oplus I_0 \otimes I_0$, for it is in $E\otimes F\oplus E\otimes I_0\oplus I_0\otimes F\oplus I_0\otimes I_0$ and $\Theta_1^{\triangleright}(I_0^{\perp}) = E$, $\Theta_1^{\triangleleft}(I_0^{\perp}) = F$.

Let us fix now f_0 in R. It is clear from the definition 2.1 and the remark 2.3 that $\Theta_{f_0}(z,\xi) - f_0(\xi)\Theta_1(z,\xi)$ is in the ideal of $\mathbb{K}[z,\xi]$ generated by $f_1(\xi),\ldots,f_n(\xi)$. Consequently,

$$\Theta_{f_0}^{\triangleright}(\widehat{\mathcal{A}}_0) = (f_0(\xi)\Theta_1)^{\triangleright}(\widehat{\mathcal{A}}_0) = \Theta_1^{\triangleright}(f_0 \cdot \widehat{\mathcal{A}}_0) \subset \Theta_1^{\triangleright}(\widehat{\mathcal{A}}_0) = E.$$

The same argument shows that $\Theta_{f_0}^{\triangleleft}(\widehat{\mathcal{A}}_0) \subset F$, and therefore that $\Theta_{f_0} \in E \otimes F \oplus I_0 \otimes I_0$.

Let $\mathbf{v} = (v_i)_{i\in\mathbb{N}}$ and $\mathbf{w} = (w_i)_{i\in\mathbb{N}}$ be two bases of R such that $(v_1,\ldots,v_D)$ is a basis of E, $(w_1,\ldots,w_D)$ a basis of F and $v_i \in I_0$, $w_i \in I_0$ for $i > D$. As we have the decomposition $\Theta_{f_0} \in E \otimes F \oplus I_0 \otimes I_0$, $[\Theta_{f_0}]_{\mathbf{v},\mathbf{w}}$ has a block-diagonal form.

Let us denote by $C_{f_0} = (c_{ij}(f_0))_{1\leq i,j\leq D}$ the upper-left block in this decomposition and by $M_{f_0} = (m_{ij})_{1\leq i,j\leq D}$ the matrix of multiplication by f_0 in the basis $(\overline{v}_1,\ldots,\overline{v}_D)$ of $\mathcal{A}_0$. We deduce from decomposition (1) that, modulo the ideal $(f_1(z),\ldots,f_n(z))$, we have

$$\sum_{i,j=1}^{D} c_{ij}(f_0)\, v_i \otimes w_j \quad \equiv \quad \Theta_{f_0} \quad \equiv \quad f_0(z)\Theta_1 \quad \equiv \quad f_0(z) \sum_{i,j=1}^{D} c_{ij}(1)\, v_i \otimes w_j$$

$$\equiv \sum_{i,j=1}^{D} c_{ij}(1)\, f_0(z)\; v_i \otimes w_j \;\equiv \sum_{k,j=1}^{D} \left(\sum_{i=1}^{D} m_{ki} c_{ij}(1)\right) v_k \otimes w_j \;,$$

which implies that $C_{f_0} = M_{f_0}\, C_1$.

Notice that the matrix C_1 is invertible, for it is the matrix of $\overrightarrow{\Theta_1}$ in the bases $(\overline{v}_1, \ldots, \overline{v}_D)$ of $\mathcal{A}_0$ and its dual basis in $\widehat{\mathcal{A}}_0$. Indeed, as $f_1, \ldots, f_n$ is a complete intersection, this map is an isomorphism between $\widehat{\mathcal{A}}_0$ and $\mathcal{A}_0$ (see [4], [27], [38], [16]). By a change of bases, we may assume that $C_1 = \mathbb{I}_D$, so that the matrix of $[\Theta_{f_0}]_{\mathbf{v},\mathbf{w}}$ is of the form (1). □

Let $d_i = \deg(f_i)$ and $d = \max_{i=0,\ldots,n} d_i$. For $\alpha, \beta \in \mathbb{N}^n$, we denote by $l_{\alpha,\beta}$ the number of tuples $(m_0, \ldots, m_n)$ such that m_i is a monomial of f_i and $z^{\alpha}\, \xi^{\beta}$ appears in $\Theta_{m_0,\ldots,m_n}$. Let $l = \max l_{\alpha,\beta}$.

Lemma 2.7 *Let $f_0, \ldots, f_n \in \mathbb{Q}[z]$ and let $h = \max_{0 \le i \le n} h(f_i)$. Then, the size of $B_{f_0,\ldots,f_n}$ is bounded by $(e\, d)^n$ (where $\log(e) = 1$) and the height of the coefficients of the Bezoutian matrix is bounded by $(n+1)\left(h + n \log(d+1) + \frac{1}{2}\log(n+1)\right)$.*

Proof. The size of $B_{f_0,\ldots,f_n}$ is bounded by $\left(\begin{array}{c} (n+1)\, d \\ n \end{array} \right)$, that is by the number of monomials in $z_1, \ldots, z_n$ of degree at most $\sum_{i=0}^{n} d_i - n \le (n+1)\, d$. According to Stirling formula, $n! \ge \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$, we have

$$\left(\begin{array}{c} (n+1)\, d \\ n \end{array} \right) \le \frac{1}{n!}(n+1)^n d^n \le \frac{1}{\sqrt{2\pi n}} \left(\frac{n+1}{n}\right)^n (e\, d)^n \le \frac{e}{\sqrt{2\pi n}} (e\, d)^n \le (e\, d)^n$$

for $n \ge 2$ and we check easily that the inequality holds with $n = 1$.

As $\Theta_{f_0,\ldots,f_n}$ is an alternate multilinear function of $f_0, \ldots, f_n$, any coefficient of $B_{f_0,\ldots,f_n}$ is a sum of at most l (where l is defined above) $(n+1)\times(n+1)$ determinants of the coefficients of the input polynomials $f_0, \ldots, f_n$. Notice that l is roughly bounded by the number of tuples of monomials $(m_0, \ldots, m_n)$ of degree $\le d$, that is by $(d+1)^{(n+1)\, n}$. According to Hadamard formula, the height of these coefficients is bounded by

$$(n+1)\big(h + \frac{1}{2}\log(n+1)\big) + \log(l) \le (n+1)\big(h + n \log(d+1) + \frac{1}{2}\log(n+1)\big)$$

□

Remark 2.8 — According to [9], the rank of $B_{1,f_1,\ldots,f_n}$ is bounded by

$$G_{n,d} = \sum_{0 \le k \le n(d-1)} \min(g_k, g_{n(d-1)-k})$$

where $d = \max\{\deg(f_i), i = 1, \ldots, n\}$ and g_k is the number of n-tuples $a_1, \ldots, a_n$ such that $a_1 \le d-1, a_1+a_2 \le 2\,(d-1), \ldots, a_1+\cdots+a_n \le n(d-1)$ and $a_1+\cdots+a_n = k$. Combinatorial arguments, related to enumeration of Dick Paths and due to L. Habsieger [24], show that $G_{n,d}$ is bounded above by $n^{-\frac{1}{2}} \left(\frac{e}{2}\right)^n d^n$ and below by $n^{\frac{1}{2}} \left(\frac{e}{2}\right)^{\frac{n}{2}} d^n$. In other words, we may replace e by $\frac{e}{2}$ in the bound on the rank of the Bezoutian matrix.

3 Relations of algebraic dependency

Let $f_0, \ldots, f_n$ be $n+1$ elements of R such that the n polynomials $f_1, \ldots, f_n$ are algebraically independent over $\mathbb{K}$. Then, for algebraic dimension reasons, there is a non-zero polynomial P such that $P(f_0, \ldots, f_n) = 0$. Our goal in this section is to show how to find such a polynomial P, using elementary algebra, and the properties of the Bezoutians.

Theorem 3.1 — *Let $u = (u_0, \ldots, u_n)$ be new parameters and assume that $\mathcal{A} = R/(f_1, \ldots, f_n)$ is a vector space of finite dimension D. Then, every non-identically zero maximal minor $P(u_0, \ldots, u_n)$ of the Bezoutian matrix of the polynomials $f_0 - u_0, \ldots, f_n - u_n$ in $\mathbb{K}[u][z_1, \ldots, z_n]$ satisfies the identity $P(f_0, \ldots, f_n) = 0$.*

Proof. For each $i \in \{1, \ldots, n\}$, the functions $z_i, f_1, \ldots, f_n$ are algebraically dependent over $\mathbb{K}$. Thus, $\mathbb{K}(z)$ is a finite field extension of $\mathbb{K}(f)$ (where $\mathbb{K}(z) = \mathbb{K}(z_1, \ldots, z_n)$, and $\mathbb{K}(f) = \mathbb{K}(f_1, \ldots, f_n)$). Its degree will be denoted by d. By introducing the parameters $\tilde{u} = (u_1, \ldots, u_n)$, we have $\dim_{\mathbb{K}(f)} \mathbb{K}(z) = \dim_{\mathbb{K}(\tilde{u})} \mathbb{K}(\tilde{u})[z]/(f_1 - u_1, \ldots, f_n - u_n) = d$. Indeed, if $(v_1, \ldots, v_d)$ is a $\mathbb{K}(f)$-basis of $\mathbb{K}(z)$, with $v_i \in \mathbb{K}[z], 1 \leq i \leq d$, then $(\overline{v}_1, \ldots, \overline{v}_d)$ is a $\mathbb{K}(\tilde{u})$-basis of $\mathbb{K}(\tilde{u})[z]/(f - \tilde{u})$.

From now on, we work in the field $\mathbb{K}(\tilde{u}) = \mathbb{K}(u_1, \ldots, u_n)$. We check that $\Theta_1^{\tilde{u}} := \Theta_{1, f_1 - u_1, \ldots, f_n - u_n} = \Theta_{1, f_1, \ldots, f_n} = \Theta_1$ and that the Bezoutian of $f_0 - u_0, \ldots, f_n - u_n$ is

$$\Theta_{f_0 - u_0, f_1 - u_1, \ldots, f_n - u_n} := \Theta_{f_0, f_1 - u_1, \ldots, f_n - u_n} - u_0\, \Theta_{1, f_1 - u_1, \ldots, f_n - u_n} = \Theta_{f_0}^{\tilde{u}} - u_0\, \Theta_1^{\tilde{u}}.$$

By lemma 2.6, there exists two bases $\mathbf{v}$ and $\mathbf{w}$ of $\mathbb{K}(\tilde{u})[z]$ such that the Bezoutian matrices of $f_0, f_1 - u_1, \ldots, f_n - u_n$ in these bases, is of the form

$$[\Theta_g^{\tilde{u}}]_{\mathbf{v},\mathbf{w}} = \begin{array}{cc} \begin{array}{cc} v_1 \ \ldots \ v_d & v_{d+1} \ldots \end{array} & \\ \left(\begin{array}{c|c} M_g & \mathbf{0} \\ \hline \mathbf{0} & L_g \end{array}\right) & \begin{array}{c} w_1 \\ \vdots \\ w_d \\ w_{d+1} \\ \vdots \end{array} \end{array}$$

for $g = f_0$ and $g = 1$. Let $\mathbf{v}' = (z^\alpha)_{\alpha \in \mathbb{N}^n}, \mathbf{w}' = (\xi^\beta)_{\beta \in \mathbb{N}^n}$ be the monomial bases of $\mathbb{K}[z]$ and $\mathbb{K}[\xi]$. Then the matrices $[\Theta_{f_0}^{\tilde{u}}]_{\mathbf{v}',\mathbf{w}'}, [\Theta_{f_0}^{\tilde{u}}]_{\mathbf{v},\mathbf{w}}$ and $[\Theta_1]_{\mathbf{v}',\mathbf{w}'}, [\Theta_1]_{\mathbf{v},\mathbf{w}}$ can be deduced from each other (by change of bases) by left and right multiplication by invertible matrices $R(\tilde{u})$ and $Q(\tilde{u})$ with coefficients in $\mathbb{K}(\tilde{u})$. So

$$\begin{array}{rcl} B(u) := [\Theta^{\tilde{u}}_{f_0-u_0}]_{\mathbf{v}',\mathbf{w}'} & = & [\Theta^{\tilde{u}}_{f_0}]_{\mathbf{v}',\mathbf{w}'} - u_0\,[\Theta^{\tilde{u}}_{1}]_{\mathbf{v}',\mathbf{w}'} \\ & = & R(\tilde{u})N(u)Q(\tilde{u}) \end{array}$$

where

$$N(u) = \left(\begin{array}{c|c} (M_{f_0} - u_0\mathbb{I}_d) & \mathbf{0} \\ \hline \mathbf{0} & L_{f_0} - u_0 L_1 \end{array}\right)$$

and $\mathbb{I}_d$ is the identity matrix of size d. Consequently, a non-zero maximal minor $P(u_0,\ldots,u_n)$ of $B(u)$ is a linear combination, with coefficients in $\mathbb{K}(\tilde{u})$, of the non-zero maximal minors of the matrix $N(u)$. These minors are all multiples of $\det(M_{f_0} - u_0\mathbb{I}_D)$. Therefore $P(u_0,\ldots,u_n)$ is a multiple of the characteristic polynomial of the multiplication by $\overline{f}_0$ in the quotient $\mathbb{K}(\tilde{u})[z]/(f_1-u_1,\ldots,f_n-u_n)$. Using Cayley-Hamilton's theorem and substituting f_i for u_i, $1 \le i \le n$, we deduce that $P(f_0,\ldots,f_n) = 0$. □

In practice, we use Gaussian elimination (Bareiss Method) in order to find a non-zero maximal minor of the Bezoutian matrix.

Example 3.2 *We illustrate the above method by this example in* `maple`.

```
> f0:= x;  f1 := x^2+y^2+z^2; f2 := x^3+y^3+z^3; f3 := x^4+y^4+z^4;
> mbezout([f0-u[0],f1-u[1],f2-u[2],f3-u[3]],[x,y,z]):
> last(ffgausselim("));
```

$$\begin{aligned} &-\big(12\,{u_0}^{12} - 24\,{u_0}^{10}u_1 - 16\,{u_0}^{9}u_2 + \big(24\,{u_1}^{2} - 12\,u_3\big)\,{u_0}^{8} + 48\,{u_0}^{7}u_2u_1 \\ &\quad + \big(-8\,{u_2}^{2} - 24\,{u_1}^{3}\big)\,{u_0}^{6} + \big(-24\,{u_1}^{2}u_2 + 24\,u_3u_2\big)\,{u_0}^{5} \\ &\quad + \big(-24\,{u_2}^{2}u_1 + 6\,u_3{u_1}^{2} + 3\,{u_3}^{2} + 15\,{u_1}^{4}\big)\,{u_0}^{4} + \big(8\,{u_1}^{3}u_2 - 24\,u_1u_3u_2 + 16\,{u_2}^{3}\big)\,{u_0}^{3} \\ &\quad + \big(-6\,{u_1}^{5} - 12\,u_3{u_2}^{2} + 6\,{u_3}^{2}u_1 + 12\,{u_1}^{2}{u_2}^{2}\big)\,{u_0}^{2} \\ &\quad + {u_1}^{6} - 3\,{u_1}^{2}{u_3}^{2} + 12\,u_1u_3{u_2}^{2} - 2\ ,{u_3}^{3} - 4\,{u_2}^{4} - 4\,{u_1}^{3}{u_2}^{2}\big)^{2} \end{aligned}$$

The Bezoutian matrix is of size 50×50 *and of rank* 24 *and its non-zero maximal minor is of degree* 24 *in* (u_0, u_1, u_2, u_3).

Proposition 3.3 — *Under the notations of lemma 2.7, the polynomials P given by theorem 3.1 are at most of degree $(e\,d)^n$ and its height is bounded by*

$$(n+1)\,(e\,d)^n\ \left(h + (n+1)\,\log(d+1) + \log(n+1) + 2\right).$$

Proof. Let N be the size of the Bezoutian matrix $B_{f-u} := B_{f_0-u_0,\ldots,f_n-u_n}$. According to lemma 2.7, $N \leq (e\,d)^n$. The matrix B_{f-u} is linear in the variables $u_0, u_1, \ldots, u_n$ and can be decomposed as $B_{f-u} = B_f + u_0 B_0 + \cdots + u_n B_n$, where B_f, and the B_i are Bezoutian matrices. Let $T = (n+1)(h+n\,\log(d+1)+\frac{1}{2}\log(n+1))$ be the bound on the heights of the coefficients of these matrices, given in lemma 2.7. Let $\Delta(u)$ be a maximal minor of B_{f-u}, which is at most of degree N in u.

The coefficient of $u_0^{a_0}\cdots u_n^{a_n}$ in $\Delta(u)$ is the sum of the determinants obtained by choosing a_0 columns of B_0, a_1 columns of $B_1, \ldots, a_n$ columns of B_n and at most $N-(a_0+\cdots+a_n)$ columns of B_f. The number of possible choices is bounded by the number of applications from the N columns to the set $\{1,\ldots,n+2\}$, that is by $(n+2)^N$. By Hadamard inequality, the height of each of these determinants is bounded by $N\left(T+\frac{1}{2}\log(N)\right)$. Thus, the height of the coefficient of the monomial $u_0^{a_0}\cdots u_n^{a_n}$ in $\Delta(u)$ is bounded by

$$\begin{aligned} & N\,(T+\frac{1}{2}\log(N)) + \log((n+2)^N) \\ \leq\ & (e\,d)^n\left((n+1)\left(h+n\,\log(d+1)+\frac{1}{2}\log(n+1)\right)+n\,(\log(d)+1)+\log(n+2)\right) \\ \leq\ & (n+1)\,(e\,d)^n\,\left(h+(n+1)\,\log(d+1)+\log(n+1)+2\right). \end{aligned}$$

□

The following proposition describes the uniqueness of the irreducible polynomial P such that $P(f_0,\ldots,f_n)=0$. It will be used in section 5.

Proposition 3.4 — *Let $f_0,\ldots,f_n$ be $n+1$ polynomials of R such that $f_1,\ldots,f_n$ are $\mathbb{K}$-algebraically independent. Then there is a unique irreducible $P\in\mathbb{K}[u_0,\ldots,u_n]$ (up to constant) satisfying $P(f_0,\ldots,f_n)=0$. If $\mathbb{K}$ is infinite and* $\deg f_0 \leq \min_{1\leq i\leq n}\deg f_i$, *the degree of P is at most*

$$\delta = \frac{\deg f_1\cdots\deg f_n}{[\mathbb{K}(z):\mathbb{K}(f_0,\ldots,f_n)]}.$$

Moreover, if $f_1,\ldots,f_n$ have no zero at infinity, then the degree of P is exactly δ.

The proof of the proposition 3.4 uses the following lemma, which is easy to set up (see [28]).

Lemma 3.5 *Let K be a finite field extension of $\mathbb{K}$, $\theta\in K$, C_θ and P_θ are respectively the characteristic and minimal polynomial of the multiplication by θ in K. Then $C_\theta = P_\theta^{[K:\mathbb{K}(\theta)]}$.*

Proof. The existence of P comes from the fact that the algebraic dimension of the field extension $\mathbb{K}-\mathbb{K}(f)$ ($\mathbb{K}(f)=\mathbb{K}(f_1,\ldots,f_n)$) is equal to n and the factoriality of $\mathbb{K}[u_0,\ldots,u_n]$.

For the unicity of P, suppose that there exists two irreducible polynomials P_1, P_2 such that $P_i(f_0,\ldots,f_n)=0, i=1,2$. The resultant $R\in\mathbb{K}[u_1,\ldots,u_n]$ of P_1,P_2 as polynomials in $\mathbb{K}[u_1,\ldots,u_n][u_0]$ satisfies $R(f_1,\ldots,f_n)=0$. As $f_1,\ldots,f_n$ are $\mathbb{K}$-algebraically independent $R=0$. Thus P_1, P_2 have a non-constant common divisor in $\mathbb{K}(u_1,\ldots,u_n)[u_0]$, and in $\mathbb{K}[u_0,\ldots,u_n]$ too. Therefore, $P_1 = cP_2$ with $c\in\mathbb{K}$.

Consider the finite extension $\mathbb{K}(z)$ of $\mathbb{K}(f)$. Let $\tilde{C}$ and $\tilde{P}$ be respectively the characteristic and minimal polynomial of the multiplication by f_0 in the $\mathbb{K}(f)$-vector space $\mathbb{K}(z)$. Let $C, P \in \mathbb{K}[u_0, \ldots, u_n]$ be the polynomials obtained respectively from $\tilde{C}, \tilde{P}$ by substituting u_i for f_i ($i = 1, \ldots, n$) and by taking the numerator. The polynomial P is the unique irreducible element of $\mathbb{K}[u_0, \ldots, u_n]$ satisfying $P(f_0, \ldots, f_n) = 0$. By lemma 3.5, $\tilde{C} = \tilde{P}^{[\mathbb{K}(z):\mathbb{K}(f_0,\ldots,f_n)]}$, and $C = P^{[\mathbb{K}(z):\mathbb{K}(f_0,\ldots,f_n)]}$. Changing the variables u_i to $u_i - s_i u_0, 1 \le i \le n, s_i \in \mathbb{K}$; then $\deg P = \deg_{u_0} P$. Since $\deg(C) = \deg_{u_0}(C) = \deg_{u_0}(\tilde{C}) \le \deg(f_1 + s_1 f_0) \cdots \deg(f_n + s_n f_0)$. Moreover, the equality holds if $f_1 + s_1 f_0, \ldots, f_n + s_n f_0$ have no zero at infinity. We deduce that

$$\deg P \le \frac{\deg(f_1 + s_1 f_0) \cdots \deg(f_n + s_n f_0)}{[\mathbb{K}(z) : \mathbb{K}(f_0, \ldots, f_n)]}.$$

The equality holds if $f_1, \ldots, f_n$ have no zero at infinity. $\square$

Another proof of this proposition is given in [34].

4 Residue calculus

The residue is a special linear form on $\mathcal{A}$, associated to the map $f = (f_1, \ldots, f_n)$ defining the quotient $\mathcal{A}$. In some way, the structure of this quotient is condensed in this linear form. We can, for instance, recover directly from it, the dimension of $\mathcal{A}$ or the multiplication table. Its construction is direct in some case like the so-called Pham maps (see [1], [11]) where the polynomials f_i are of the form $z_i^{d_i} + R_i(z)$ with $\deg(R_i) < d_i$. Residues for equations defining zero-dimensional projective varieties are also direct to handle (see eg. [16]) and recently generalization of this situation to projective toric varieties has also been studied (see [10]).

The goal of this section is to show how to compute effectively the residue τ_f associated to a *general* polynomial map f, using the algebraic relations of dependency and a result from [7], and to give some direct applications of this residue computation.

Let

$$\begin{array}{rcl} f : \mathbb{K}^n & \to & \mathbb{K}^n \\ z & \mapsto & f(z) = (f_1(z), \ldots, f_n(z)) \end{array}$$

be a polynomial map, such that the set of zeroes $\mathcal{Z}$ is finite over the algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$. Let $I = (f_1, \ldots, f_n)$ be the ideal generated by the components of f.

Definition 4.1 *(see [38], [27], [16], [4]) The residue τ_f is the unique linear form on R such that*

1. $\tau_f(I) = 0$,
2. $\Theta^{\triangleright}_{1,f_1,\ldots,f_n}(\tau_f) - 1 \in I$.

We recall also the analytic definition over $\mathbb{C}$ (see [22]):

$$\text{For } \ h \in R \ , \quad \tau_f(h) = \sum_{\alpha \in \mathcal{Z}} \frac{1}{(2i\pi)^n} \int_{\{z \in V_\alpha : |f_i(z)| = \epsilon_i, 1 \le i \le n\}} \frac{h(z)}{f_1(z) \ldots f_n(z)} dz \ ,$$

where V_α is a small neighborhood of α, $\varepsilon_1, \ldots, \varepsilon_n$ are positive and $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n)$ is outside a negligible set defined by Sard's theorem.

For each $i \in \{1, \ldots, n\}$, let $h_i(f; z_i) := a_{i,0}(f) z_i^{m_i} + \cdots + a_{i,m_i}(f) = 0$ $(i = 1, \ldots, n)$, be algebraic relations between the functions $z_i, f_1, \ldots, f_n$ given by the Bezoutian (see section 3).

Proposition 4.2 — *Let $u = (u_1, \ldots, u_n) \in \mathbb{K}^n$. If for each $i \in \{1, \ldots, n\}$, there is $j_i \in \{0, \ldots, m_i - 1\}$, with $a_{i,j_i}(u) \neq 0$, then for any $h \in R$, the computation of the multivariate residue $\tau_{f-u}(h)$ reduces to univariate residue computation.*

Proof. According to the hypotheses, we have

$$g_i(z_i) := a_{i,j_i}(u) z_i^{m_i - j_i} + \cdots + a_{i,m_i}(u) = \sum_{j=1}^{n} A_{i,j}(f_j - u_j) \quad , \quad 1 \le i \le n \ ,$$

where $A_{i,j} \in \mathbb{K}[z]$. We put $g(z) = \big(g_1(z_1), \ldots, g_n(z_n)\big)$. Using the transformation law (see [27], [38], [16] and [4]), we have

$$\begin{aligned} \tau_{f-u}(h) &= \tau_g\left(h \det(A_{i,j})\right) \\ &= \sum_{\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n} c_\alpha \prod_{i=1}^{n} \big(\tau_{g_i}(z_i^{\alpha_i})\big) , \quad c_\alpha \in \mathbb{K} \ , \\ &= \sum_{\alpha \in \mathbb{N}^n} c_\alpha \prod_{i=1}^{n} \left(\frac{c_{i,\alpha_i}}{a_{i,j_i}(u)^{\max(0, \ \alpha_i - m_i + j_i + 1)}} \right) , \quad c_{i,\alpha_i} \in \mathbb{K}. \end{aligned}$$

□

If we apply this proposition with the fraction field $\mathbb{K}(u)$ (where $u_1, \ldots, u_n$ are formal parameters) instead of $\mathbb{K}$, we obtain the residue τ_{f-u} over $\mathbb{K}(u)[z]$. For any $h \in \mathbb{K}[z]$, $\tau_{f-u}(h)$ is a rational fraction in u, whose denominator is the product of powers of the $a_{i,j_i}(u)$.

This proposition yields (in the case where $(a_{i,j}(0))_{1 \le i \le n, 0 \le j \le m_i - 1}$ are not all zero) a direct algorithm for computing the residue by means of the n algebraic relations between $z_i, f_1, \ldots, f_n, 1 \le i \le n$, given by the Bezoutian, and by reduction to univariate residues.

In the general case, the computation of the residue, can be done using a result from [7], as follows.

For $(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n$, we define s_i, R_i and S_i as follows:

$$h_i(\alpha_1 t, \ldots, \alpha_n t; z_i) = \sum_{j=1}^{n} A_{i,j}(f_j - \alpha_j t) = t^{s_i} \big(R_i(z_i) - t S_i(z_i, t)\big). \tag{2}$$

Proposition 4.3 —*[7] If $R_i(z_i) \neq 0$, then for any $g \in R$,*

$$\begin{aligned}\tau_f(g) &= \tau_{t^{|s|+1}, R_1 - tS_1, \ldots, R_n - t\, S_n}(g\,\Delta) \\ &= \sum_{k=(k_1,\ldots,k_n)\in\mathbb{N}^n, |k|\leq |s|} \tau_{(t^{|s|+1-|k|}, R_1^{k_1+1}, \ldots, R_n^{k_n+1})}(g S_1^{k_1} \ldots S_n^{k_n}\,\Delta)\end{aligned}$$

and $\Delta = \det\big(A_{i,j}\big)$.

The proof of this result is based on a generalization of the transformation law.

Notice that this sum can be computed as follows. For any polynomial $a \in \mathbb{K}[z]$, let us define $\rho_i(a) = q_i\, tS_i + r_i$ for $i = 1, \ldots, n$ where q_i and r_i are respectively the quotient and remainder in the Euclidean division of a by R_i and $\rho_0(a) = r_0$ where r_0 is the remainder in the Euclidean division of a by $t^{|s|+1}$. By construction, we have $\rho_i(a) \equiv a$ modulo $(t^{|s|+1}, R_1 - t\,S_1, \ldots, R_n - t\,S_n)$.

Applying iteratively $\rho_0, \rho_1, \ldots, \rho_n$ to the polynomial $\Delta\, g$ will eventually end with a polynomial g^* of degree $\leq |s|$ in t and $\leq \deg(R_i)$ in z_i. Then the residue $\tau_f(g)$ is the coefficient of $t^{|s|}\, z_1^{d_1-1} \cdots z_n^{d_n-1}$ in g^*, for $\Delta\, g - g^* \in (t^{|s|+1}, R_1 - t\,S_1, \ldots, R_n - t\,S_n)$.

By combination of proposition 4.3 and of the computations of the algebraic relations from section 3, we obtain an algorithm for the computation of the multivariate residue for any complete intersection.

Algorithm 4.4 — The residue of $f_1, \ldots, f_n$.
Let $f_1, \ldots, f_n$ be a complete intersection in R and let $g \in R$.

1. For every $i \in \{1, \ldots, n\}$, compute the algebraic relations $h_i(u; z_i)$ between z_i and $f_1, \ldots, f_n$ (using the Bezoutian computation of the previous section).
2. Choose a generic vector $(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n$ and compute the exponents s_i and the polynomials $R_i(z_i), S_i(z_i, t)$ and the coefficients $(A_{i,j})_{i,j=1,\ldots,n}$ defined in (2). Let d_i be the degree of R_i in z_i.
3. Compute $\Delta = \det(A_{i,j})$ and apply $\rho_0, \ldots, \rho_n$ (defined above) to $\Delta\, g$ until a fixed point g^* is reached. Take the coefficient c of $t^{|s|}\, z_1^{d_1-1} \cdots z_n^{d_n-1}$ in g^*.

The coefficient c is the residue $\tau_f(g)$.

Remark 4.5 — The number of Euclidean divisions in this process is bounded by $n \times (|s|+1)$.

If d is a bound on the degrees of the input polynomials $f_1, \ldots, f_n$, then according to lemma 3.3, R_i, S_j and $A_{i,j}$ are of degree $\leq (ed)^n$ and the degree of Δ is bounded by $(ed)^{2\,n}$.

Let h be a bound on the height of $f_1, \ldots, f_n$ and α and let $g = z^\beta$, $\beta \in \mathbb{N}^n$. Then according to lemma 3.3 (substituting u_i by $\alpha_i\, t$ in the maximal minor), the heights of $R_i, S_i, A_{i,j}$ is bounded by $H = \mathcal{O}\left(n\,(n + h + \log(d))(e\,d)^n\right)$. The height of Δ (obtained by substituting z by ζ in $\Theta_{1,f}$) is bounded by $T = \mathcal{O}\left(n(h + n\log(d))\right)$. The Euclidean division of $g\Delta$ by R_i increases its height by $\deg(g\Delta)\, H$. The number of Euclidean divisions is bounded by $n \times (|s| + 1) \leq n(e\,d)^n$. Therefore, the heights of $\tau_f(z^\beta)$ is bounded by

$$\mathcal{O}\left(n^2(n + h + \log(d))(|\beta| + (ed)^{2n})(ed)^n\right).$$

Applications

Let us give some direct applications of this residue computation. See also [16], [4], for other applications.

The dimension of $\mathcal{A}$. If the characteristic of $\mathbb{K}$ is zero, it is possible to compute the dimension of the vector space $\mathcal{A}$. According to the following formula (see [27], [38], [9], [16]):

$$\dim_{\mathbb{K}}(\mathcal{A}) = \tau_f(J_f),$$

where J_f is the Jacobian determinant of $(f_1, \ldots, f_n)$.

Matrices of multiplication. Let $(b_i)_{i=1,\ldots,D}$ be a basis of $\mathcal{A}$ and let $a \in \mathcal{A}$. The transpose of the matrix of multiplication by a in the dual basis of $(b_i)_{i=1,\ldots,D}$ can be computed using following idea. As τ_f is a basis of the $\mathcal{A}$-module $\widehat{\mathcal{A}}$, the set of linear forms $(b_i \cdot \tau)$ is a basis of $\widehat{\mathcal{A}}$. Thus for $i = 1, \ldots, D$, there exist $m_{i,j} \in \mathbb{K}$ such that

$$a \cdot (b_i \cdot \tau) = \sum_{j=1}^{D} m_{i,j}\, (b_j \cdot \tau).$$

The matrix $\mathtt{M} = (m_{i,j})_{i,j=1,\ldots,D}$ is the matrix of multiplication by a in the basis $(b_i \cdot \tau)$ of $\widehat{\mathcal{A}}$. This coefficients $m_{i,j}$ can be computed by solving the linear systems

$$[\tau(a\, b_i\, b_j)]_{i,j=1,\ldots,D} = \mathtt{M}\ [\tau(b_i\, b_j)]_{i,j=1,\ldots,D}.$$

According to [32], such a matrix can then be used to deduce the roots of the system $f_1 = \cdots = f_n = 0$, by eigenvector computations.

Solving polynomial systems. Let $f_1, \ldots, f_n$ be n equations of $\mathbb{K}[x_1, \ldots, x_n]$ defining a zero-dimensional variety $V(f_1 = \cdots = f_n = 0) = \{\zeta_1, \ldots, \zeta_d\}$, where $\zeta_i = (\zeta_{i,1}, \ldots, \zeta_{i,n}) \in \overline{\mathbb{K}}^n$.

We can compute the coefficients of the univariate polynomial

$$P_j(T) = (T - \zeta_{1,j}) \cdots (T - \zeta_{d,j}) = T^m - \sigma_1 T^{d-1} + \cdots + (-1)^m \sigma_d$$

which determines the j^{th} coordinates of the roots, in terms of the residues. Indeed the coefficients σ_l are related to the Newton sums $S_{i,l} := \sum_{j=1}^{d} \zeta_{j,i}^l$ by the classical relations between the symmetric functions of roots of a polynomial. These Newton sums are given by the formula

$$S_{i,l} = \tau_f(x_i^l J) = Tr(x_i^l)$$

where J is the Jacobian of the $f_1, \ldots, f_n$. Thus, by computing these values, thanks to algorithm 4.4, we can deduce the polynomial $P_j(T)$ and compute the j^{th} coordinates of the roots. It can also be used to express all the coordinates of the roots as rational fractions of the the root of a univariate polynomial (see [1], [21], [37]).

The membership problem. It is also possible to test if an element f_0 belongs to the ideal $(f_1, \ldots, f_n)$, by linear algebra on polynomials of "small degree". In general, the complexity of this problem is doubly exponential (see [30]). For complete intersection, the bounds on the degree are simply exponential ([5], [14], [15], [26]). Using the residue, it is possible to transform such a problem into a linear one of even smaller size.

Proposition 4.6 — *There exists a polynomial g of degree at most $\sum_{i=1}^n \deg f_i - n$ which is a non-zero divisor in $\mathcal{A}$ such that, f_0 is in the ideal generated by $f_1, \ldots, f_n$, if and only if,*

$$g f_0 = g_1 f_1 + \cdots + g_n f_n \quad , \quad g_i \in \mathbb{K}[z] \quad , \tag{3}$$

with

$$\deg(g_j\, f_j) \leq \sum_{i=0}^{n} \deg f_i - n \ , \quad 1 \leq j \leq n.$$

Proof. From the definition 2.1 and the remark 2.3,

$$\begin{aligned} \Theta_{f_0} &= f_0(z)\Theta_1(z,\xi) + f_1(z)\Delta_1(z,\xi) + \cdots + f_n(z)\Delta_n(z,\xi) \\ &= f_0(\xi)\Theta_1(z,\xi) + f_1(\xi)\tilde{\Delta}_1(z,\xi) + \cdots + f_n(\xi)\tilde{\Delta}_n(z,\xi), \end{aligned}$$

with $\Delta_i, \tilde{\Delta}_i \in \mathbb{K}[z,\xi], 1 \leq i \leq n$.

If $f_0 \in (f_1, \ldots, f_n)$, then

$$\Theta_{f_0}{}^{\triangleright}(\tau_f) = f_0(z)\,(\Theta_1{}^{\triangleright}\tau_f)) - g_1 f_1 - \cdots - g_n f_n = 0.$$

We put $g = \Theta_1{}^{\triangleright}(\tau_f)$. As $g - 1 \in (f_1, \ldots, f_n)$ (definition 4.1), g is a non-zero divisor in $\mathcal{A}$. □

The identity (3) can viewed as a linear system, where the unknowns are the coefficients of $g_1, \ldots, g_n$. Thus, if we want to test whether a polynomial f_0 is in the ideal $(f_1, \ldots, f_n)$; first we compute $g = \Theta_1{}^{\triangleright}\tau_f$ (section 4), and test whether $g f_0$ is in the vector space generated by the multiples of the initial polynomials of degree $\leq \sum_{i=0}^n \deg(f_i) - n$.

5 Properness and Lojasiewicz exponent

Our goal in this section is to give an effective method to test whether a polynomial map $f : \mathbb{C}^n \to \mathbb{C}^n$ is proper or not. The interest of the properness comes from the Jacobian conjecture and the study of the automorphisms of $\mathbb{C}^n$ [3]. It also plays a crucial role in the effective Hilbert's Nullstellensatz (see [5], [15]).

Definition 5.1 *A polynomial map $f : \mathbb{K}^n \to \mathbb{K}^n$ is dominating if $\mathbb{K}(z)$ is a finite field extension of $\mathbb{K}(f)$. The geometric degree of f is the degree of this extension.*

Proposition 5.2 — *[23] For a polynomial map $f = (f_1, \ldots, f_n) : \mathbb{K}^n \to \mathbb{K}^n$, these conditions are equivalent*

1. *f is a dominant map.*
2. *The functions $f_1, \ldots, f_n$ are algebraically independent over $\mathbb{K}$.*
3. *The Jacobian $J_f = \det\left(\frac{\partial f_i}{\partial z_j}\right)_{i,j}$ of f is not identically zero.*

In this case, the geometric degree of f is also equal to $\dim_{\mathbb{K}(u)} \mathbb{K}(u)[z]/(f-u)$. Thus generically the cardinality of the fibers of f is exactly the geometric degree.

Definition 5.3 *A polynomial map $f : \mathbb{C}^n \to \mathbb{C}^n$ is proper if the inverse image of a compact subset of $\mathbb{C}^n$ is compact (i.e. $\lim_{||z|| \to \infty} ||f(z)|| = \infty$).*

Proposition 5.4 — *For a dominating map $f : \mathbb{C}^n \to \mathbb{C}^n$, the following conditions are equivalent*

1. *f is proper.*
2. *For every $h \in \mathbb{C}[z]$, the characteristic polynomial of the $\mathbb{C}(u)$-endomorphism*

$$\begin{array}{rcl} \overline{h} : \mathbb{C}(u)[z]/(f-u) & \to & \mathbb{C}(u)[z]/(f-u) \\ a & \mapsto & \overline{h}a \end{array}$$

   has coefficients in $\mathbb{C}[u]$.

3. *The ring $\mathbb{C}[z]$ is an integral extension of $\mathbb{C}[f]$ (i.e. $\forall i \in \{1, \ldots, n\}, \exists m_i \in \mathbb{N}^*$:*

$$z_i^{m_i} + a_{i,1}(f) z_i^{m_i - 1} + \cdots + a_{i,m_i}(f) = 0 \quad , \quad \text{with} \quad a_{i,j} \in \mathbb{C}[z]).$$

4. *There are $R, C, d > 0$ such that, $\forall z \in \mathbb{C}^n$, $||z|| \geq R \implies ||f(z)|| \geq C||z||^d$.*
5. *$\forall h \in \mathbb{C}[z], \tau_{f-u}(h) \in \mathbb{C}[u]$.*
6. *$\forall i \in \{1, \ldots, n\}, \forall j \in \{1, \ldots, d\}$ (d is the geometric degree of f), $\tau_{f-u}(z_i^j J_f) \in \mathbb{C}[u]$.*

Proof. We denote by $\mathcal{Z}(f-u) = \{\alpha_1(u), \ldots, \alpha_d(u)\}$ the set of zeroes over the algebraic closure of $\overline{\mathbb{C}(u)}$.

1 $\Rightarrow$ *2*. Following [33], let

$$P(u; X) = X^d + a_1(u) X^{d-1} + \cdots + a_d(u) = \prod_{i=1}^{d} \Big(X - h(\alpha_i(u)) \Big) \in \mathbb{C}(u)[X]$$

be the characteristic polynomial of the endomorphism $\overline{h}$. The coefficients $a_i(u), 1 \leq i \leq d$, of P satisfy

$$\begin{aligned} |a_i(u)| &= \left| \sum_{1\leq j_1<\ldots<j_i\leq d} h(\alpha_{j_1})\ldots h(\alpha_{j_i}) \right| \\ &\leq \sum_{1\leq j_1<\ldots<j_i\leq d} C_h(1+||\alpha_{j_1}(u)||)^{\deg h}\ldots(1+||\alpha_{j_i}(u)||)^{\deg h} \quad , \end{aligned}$$

with $C_h \in \mathbb{C}$. The assumption that f is proper implies that

$$\forall A>0 \quad , \quad \exists B>0 \quad : \quad \forall z\in\mathbb{C}^n, ||z||\geq B \Longrightarrow ||f(z)||\geq A.$$

Let $u \in \mathbb{C}^n$ be generic such that $||u|| \leq A$. We have $|a_i(u)| \leq C$, $C>0$, so $a_i \in \mathbb{C}[u], 1 \leq i \leq d$.

2 $\Rightarrow$ *3*. The relations of integral dependency are given by the characteristic polynomials of the multiplications by $\overline{z}_i, 1 \leq i \leq n$, in $\mathbb{C}(u)[z]/(f-u)$.

3 $\Rightarrow$ *4*. It is easy to see that if x is a root of a polynomial $X^m + a_1X^{m-1} + \cdots + a_m$ of one variable, then $|x| \leq m \max_{j\in\{1,\ldots,m\}}(|a_j|^{1/j})$. From this observation and the algebraic relations $z_i^{m_i} + a_{i,1}(f)z_i^{m_i-1} + \cdots + a_{i,m_i}(f) = 0, 1 \leq i \leq n$, we deduce that

$$|z_i| \leq C_i \max_{j=1,\ldots,m_i} |a_{i,j}(f)|^{1/j} \quad , \quad C_i>0.$$

Then there is $C>0$ such that for sufficiently large $z\in\mathbb{C}^n$,

$$||z|| \leq C\ ||f(z)||^{\max_{i\in\{1,\ldots,n\}}\max_{j\in\{1,\ldots,m_i\}}\left(\frac{\deg a_{i,j}}{j}\right)} \quad .$$

4 $\Rightarrow$ *1*. It is evident.

3 $\Rightarrow$ *5*. Let $g=(g_1,\ldots,g_n)$, with

$$g_i(u;z_i) = z_i^{m_i} + a_{i,1}(u)z_i^{m_i-1} + \cdots + a_{i,m_i}(u) = \sum_{j=1}^n A_{i,j}(u;z)(f_j-u_j) \ , \quad A_{i,j}\in\mathbb{C}[u,z].$$

By the transformation law of residues

$$\tau_{f-u}(h) = \tau_g\left(h\det(A_{i,j})\right) = \sum_\alpha c_\alpha(u)\prod_{i=1}^n \tau_{g_{(u;z_i)}}(z_i^{\alpha_i}) \ , \quad c_\alpha\in\mathbb{C}[u].$$

As g_i is a monic polynomial, $\tau_{f-u}(h)\in\mathbb{C}[u]$.

5 $\Rightarrow$ *6*. It is evident.

6 $\Rightarrow$ *3*. For a polynomial g, we consider the endomorphism of multiplication by $\overline{g}$ in the $\mathbb{C}(u)$-vector space $\mathbb{C}(u)[z]/(f-u)$. The characteristic polynomial of this endomorphism

$$P(u;X) = X^d - \sigma_1(u)X^{d-1} + \cdots + (-1)^d\sigma_d(u) \quad ,$$

where $\sigma_i, 1 \leq i \leq d$, are the elementary symmetric functions of $g(\alpha_1(u)), \ldots, g(\alpha_d(u))$. We know that σ_i is a function of the Newton's sums $S_j(u) = \tau_{f-u}(g^j J_f)$. We fix $i \in \{1, \ldots, n\}$ and $g(z) = z_i$. By hypothesis $S_j(u) = \tau_{f-u}(z_i^j J_f) \in \mathbb{C}[u]$, so $P(u; X) \in \mathbb{C}[u][X]$, and

$$z_i^d - \sigma_1(f) z_i^{d-1} + \cdots + (-1)^d \sigma_d(f) = 0.$$

□

Remark 5.5 — If for every $i \in \{1, \ldots, n\}$, we have a relation of algebraic dependency

$$a_{i,0}(f_1, \ldots, f_n) z_i^{m_i} + \cdots + a_{i,m_i}(f_1, \ldots, f_n) = 0\ ,$$

given by means of the Bezoutian (section 3), which is a relation of integral dependency (i.e. $a_{i,0}$ is a non-zero constant), then the map $f = (f_1, \ldots, f_n)$ is proper (proposition 5.4). If there exists $i \in \{1, \ldots, n\}$ such that $a_{i,0}$ is a non-constant polynomial, we decompose $a_{i,0}(u_1, \ldots, u_n) u_0^{m_i} + \cdots + a_{i,m_i}(u_1, \ldots, u_n)$ into irreducible polynomials and look at the unique irreducible polynomial

$$Q_i(u_0, \ldots, u_n) = q_{i,0}(u_1, \ldots, u_n) u_0^{n_i} + \cdots + q_{i,n_i}(u_1, \ldots, u_n) \in \mathbb{C}[u_0, \ldots, u_n]$$

which satisfies $Q_i(z_i, f_1, \ldots, f_n) = 0$ (see proposition 3.4). Thus f is proper, if and only if, the polynomials $q_{i,0}$ are non-zero constants. This requires to factorise polynomials.

We may also test properness, with no factorization, as follows:

Algorithm 5.6 — TESTING THE PROPERNESS OF f.

1. Compute the geometric degree of f: $d = \dim_{\mathbb{C}(u)} \mathbb{C}(u)[z]/(f-u) = \tau_{f-u}(J_f)$, using proposition 4.2,
2. Compute the rational functions $\tau_{f-u}(z_i^j J_f), 1 \leq i \leq n, 1 \leq j \leq d$, using proposition 4.2.

The map f is proper, if and only if, these fractions are polynomials.

Remark 5.7 — As the polynomials a_i in the decomposition of

$$\Theta_{1,f_1,\ldots,f_n}(z, \xi) = \sum_{i=1}^{s} a_i(z) b_i(\xi)$$

in $\mathbb{C}[z, \xi]$ generate the vector space $\mathcal{A}$ (see [38], [27], [4], [16]), it is enough to show in the proposition 5.4.5, that for all $i \in \{1, \ldots, s\}, \tau_{f-u}(a_i) \in \mathbb{C}[u]$ as above.

If K is any field of characteristic 0, and the polynomial map $f : \mathbb{K}^n \to \mathbb{K}^n$ is a dominating map, the algorithm 5.6 tells us whether the ring extension $\mathbb{K}[z]$ of $\mathbb{K}[f]$ is an integral extension or not.

A polynomial map $f : \mathbb{C}^n \to \mathbb{C}^n$ which defines a discrete variety, satisfies the following relation:

$$\exists\ R, C > 0, d \in \mathbb{R}\ :\ \forall z \in \mathbb{C}^n\ ,\ ||z|| \geq R \implies ||f(z)|| \geq C||z||^d.$$

Definition 5.1 *The Lojasiewicz exponent of f is*

$$\mathcal{L}(f) = \sup\{d \in \mathbb{R} : \exists\ R, C > 0,\ \forall z \in \mathbb{C}^n, ||z|| \geq R \implies ||f(z)|| \geq C||z||^d\}.$$

This number characterizes properness: f is proper, if and only if, $\mathcal{L}(f) > 0$. We have the following bounds for a proper polynomial map f:

$$\frac{\min_{1\leq i\leq n} \deg f_i}{\prod_{i=1}^n \deg f_i} \leq \mathcal{L}(f) \leq \min_{1\leq i\leq n} \deg f_i.$$

See [33], where a more precise lower bound was given. The properness and the Lojasiewicz exponent were studied extensively by Chadzynski-Krasinski (for $n = 2$) and by Ploski (see [12], [33]).

When we have n relations of integral dependency

$$z_i^{m_i} + a_{i,1}(f) z_i^{m_i - 1} + \cdots + a_{i,m_i}(f) = 0\ \ ,\ \ m_i \in \mathbb{N}^*\ \ ,\ \ a_{i,j} \in \mathbb{C}[z]\ ,$$

we deduce from the proof of *3* $\Rightarrow$ *4* of the proposition 5.4, that

$$\mathcal{L}(f) \geq \frac{1}{\max_{i\in\{1,\ldots,n\}} \max_{j\in\{1,\ldots,m_i\}} \left(\frac{\deg a_{i,j}}{j}\right)}.$$

Ploski has shown, that equality holds if we take the relations of integral dependency given by the characteristic polynomials of the n endomorphisms of multiplication by $\overline{z}_i, 1 \leq i \leq n$, in the $\mathbb{C}(u)$-vector space $\mathbb{C}(u)[z]/(f-u)$.

Using the methods developed above and Ploski's formula, we can compute $\mathcal{L}(f)$ as follows:

Algorithm 5.8 — THE LOJASIEWICZ EXPONENT $\mathcal{L}(f)$.

1. For every $i \in \{1, \ldots, n\}$, compute the unique irreducible polynomial h_i such that $h_i(z_i, f_1, \ldots, f_n) = 0$, from the algebraic relations given in 3.1.
2. From lemma 3.5, we know that the characteristic polynomial P_i of the multiplication by z_i is a power of h_i and that its degree is equal to $D = \tau_{f-u}(J_f)$. Compute $P_i = h_i^{\frac{D}{\deg(h_i)}}$.
3. Deduce from the degrees of the coefficients $a_{i,j}$ of the characteristic polynomials P_i, the Lojasiewicz exponent

$$\frac{1}{\mathcal{L}(f)} = \max_{i\in\{1,\ldots,n\}} \max_{j\in\{1,\ldots,m_i\}} \left(\frac{\deg a_{i,j}}{j}\right).$$

Notice that this algorithm requires to factorise the algebraic relations, that we deduce from the Bezoutian (section 2). However, we can deduce directly from the residue τ_{f-u}, the characteristic polynomial P_i of the multiplication by z_i, modulo $f-u$, by computing an linear recurrence relation of degree D between the coefficients $\tau_{f-u}(z_i^k)$, $k=0,\ldots,2D$.

Example 5.9 We compute here the Lojasiewicz exponent for a proper polynomial map having zeroes at infinity.

```
> f1:=x^2+y^2+z^2-x ; f2:=x^2+y^2+z^2-y ; f3:=x^2+y^2+z^2-z;
> mbezout([x-u[0],f1-u[1],f2-u[2],f3-u[3]],[x,y,z]):
> last(ffgausselim("));
```

$$3u_0^2+(4u_1-2u_2-2u_3-1)u_0+u_3^2-2u_2u_1+2u_1^2+u_2^2-2u_3u_1-u_1$$

```
> mbezout([y-u[0],f1-u[1],f2-u[2],f3-u[3]],[x,y,z]):
> last(ffgausselim("));
```

$$-3u_0^2+(2u_1-4u_2+2u_3+1)u_0-u_3^2+2u_3u_2-u_1^2-2u_2^2+2u_2u_1+u_2$$

```
> mbezout([z-u[0],f1-u[1],f2-u[2],f3-u[3]],[x,y,z]):
> last(ffgausselim("));
```

$$3u_0^2+(4u_3-2u_2-2u_1-1)u_0-2u_3u_1-2u_3u_2+2u_3^2+u_1^2+u_2^2-u_3\ .$$

According to Ploski's formula $\mathcal{L}(f)=1$.

6 Invertible polynomial maps

A special case of interest of proper maps, concerns bijective polynomial maps. In this section, we focus on this subclass, showing how the Bezoutian can be used advantageously to compute the inverse of such a map.

Proposition 6.1 — *Let $f:\mathbb{C}^n\to\mathbb{C}^n$ be a bijective polynomial map. Then, its inverse $f^{-1}=(g_1,\ldots,g_n)$ is also polynomial. More precisely,*

$$\forall i\in\{1,\ldots,n\}\ ,\quad \forall w\in\mathbb{C}^n\ ,\quad g_i(w)\ =\ J_f\tau_{f-w}(z_i)\ =\ J_f\sum_{|\alpha|\le 1/\mathcal{L}(f)}\tau_{f^{\alpha+1}}(z_i)w^{\alpha}.$$

Proof. For $h\in R$,

$$\tau_f(h)=\frac{1}{2i\pi}\int_{\{z\in\mathbb{C}^n:|f_i(z)|=\varepsilon_i\}}\frac{h(z)}{f_1(z)\ldots f_n(z)}dz\ .$$

By the local inverse theorem, the Jacobian J_f of f does not vanish. So J_f is a non-zero scalar and f is a global biholomorphism. Therefore

$$\forall w\in\mathbb{C}^n\quad,\quad g_i(w)=\sum_{\alpha\in\mathbb{N}^n}a_{i,\alpha}w^{\alpha}\quad,\quad\text{with}\quad a_{i,\alpha}=\frac{1}{\alpha!}\frac{\partial^{\alpha}g_i}{\partial w^{\alpha}}(0)\ .$$

Using Cauchy's formula and the change of variables $\xi = f(z)$

$$a_{i,\alpha} = \frac{1}{(2i\pi)^n} \int_{\{\xi=(\xi_1,\ldots,\xi_n)\in\mathbb{C}^n : |\xi_i|=\varepsilon_i\}} \frac{g_i(\xi)}{\xi^{\alpha+1}} d\xi = J_f \tau_{f^{\alpha+1}}(z_i).$$

If $w = (w_1, \ldots, w_n) \in \mathbb{C}^n, |w_i| < \varepsilon_i, 1 \le i \le n,$

$$\begin{aligned} \tau_{f-w}(z_i) &= \frac{1}{(2i\pi)^n} \int_{\{z\in\mathbb{C}^n : |f_i(z)|=\varepsilon_i\}} \frac{z_i}{(f_1(z)-w_1)\ldots(f_n(z)-w_n)} dz \\ &= \sum_{\alpha\in\mathbb{N}^n} \tau_{f^{\alpha+1}}(z_i) w^\alpha. \end{aligned}$$

As the map f is a biholomorphism, it is proper. Then $\tau_{f-w}(z_i)$ is polynomial in w (proposition 5.4), so for sufficiently large α

$$\tau_{f^{\alpha+1}}(z_i) = \frac{a_{i,\alpha}}{J_f} = 0 \quad ,$$

and g_i is polynomial.

Since there exists $c > 0$ such that for large $z \in \mathbb{C}^n$,

$$||f^{-1}(z)||^{\mathcal{L}(f)} \le c\ ||f(f^{-1}(z))|| = c\ ||z|| \quad , \quad \text{and} \quad ||z|| \le ||f^{-1}(f(z))|| \le c\ ||f(z)||^{\deg f^{-1}} \ ,$$

we deduce that $\deg f^{-1} = \frac{1}{\mathcal{L}(f)}$. □

The above result is known (see [33]). The interesting fact here is that f^{-1} is given explicitly in terms of residue, and can be computed using the methods developed above. This yields an algorithm based, on Bezoutians and residue computations, for deciding whether a polynomial map $f : \mathbb{C}^n \to \mathbb{C}^n$ is an automorphism and for computing its inverse:

Algorithm 6.2 — Invertible polynomial maps.

Let $f : \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map and J_f its Jacobian.

1. If $J_f \notin \mathbb{C}\backslash\{0\}$, then f is not invertible.
2. Test whether f is a proper map (using algorithm 5.6):
   - If f is not proper, then f is not invertible.
   - If $J_f \in \mathbb{C}\backslash\{0\}$ and f is a proper map, then it is invertible. Compute its inverse $f^{-1} = (g_1, \ldots, g_n)$ where $g_i(u) = \tau_{f-u}(z_i)$ (proposition 4.2).

If we allow factorization of the algebraic relation given in 3.1, then the inverse of f can be computed directly by the following proposition:

Proposition 6.3 — *Let $v_0, \ldots, v_n$ be new parameters and $f_0 = v_0 + v_1 z_1 + \cdots + v_n z_n$ be a generic linear form. If $f : \mathbb{C}^n \to \mathbb{C}^n$ is invertible, then any maximal minor of the Bezoutian matrix $B_{f_0, f_1-u_1, \ldots, f_n-u_n}$ is divisible by an element of the form*

$$v_0 + v_1 g_1(u) + \cdots + v_n g_n(u) \ , \quad g_i \in \mathbb{C}[u_1, \ldots, u_n] \ ,$$

and $g = (g_1, \ldots, g_n)$ is the inverse of f.

Proof. As f is invertible, for any $u \in \mathbb{C}^n$, the variety $\mathcal{Z}(f-u)$ is reduced to the unique (simple) point $\zeta^u = f^{-1}(u)$ and the quotient $\mathcal{A} = \mathbb{C}[z_1,\ldots,z_n]/(f-u)$ is of dimension 1. This implies that the matrix of multiplication M_{z_i} by z_i in $\mathcal{A}$ is the 1×1 matrix $[\zeta_i^u], 1 \le i \le n$, where ζ_i^u is the i^{th} coordinate of ζ^u. By the proposition 5.4, ζ_i^u is also equal to $g_i(u)$, with $g_i \in \mathbb{C}[u_1,\ldots,u_n]$. In other words $(g_1(u),\ldots,g_n(u))$ is the inverse of f. According to proposition 3.1, any maximal minor of $B_{f_0,f_1-u_1,\ldots,f_n-u_n}$ is divisible by

$$\det(v_0\,\mathbb{I}_1 + v_1 M_{z_1} + \cdots + v_n M_{z_n}) = v_0 + v_1\, g_1(u) + \cdots + v_n g_n(u),$$

which proves the proposition. □

Example 6.4 — We consider a "generic" map $f=(f_1,f_2)$ over $\mathbb{C}^2$ of degree ≤ 3:

$$\begin{array}{l} f_1 = x + a_1x^2 + a_2xy + a_3y^2 + a_4x^3 + a_5x^2y + a_6xy^2 + a_7y^3 \\ f_2 = y + b_1x^2 + b_2xy + b_3y^2 + b_4x^3 + b_5x^2y + b_6xy^2 + b_7y^3 \end{array}$$

The Jacobian variety

$$\begin{vmatrix} \frac{\partial f_1}{\partial x} & \frac{\partial f_1}{\partial y} \\ \frac{\partial f_2}{\partial x} & \frac{\partial f_2}{\partial y} \end{vmatrix} = 1$$

is defined by the 14 equations:

$$\begin{array}{l} -3\,a_6b_5 + 9\,a_4b_7 + 3\,a_5b_6 - 9\,a_7b_4, 6\,a_4b_6 - 6\,a_6b_4, -3\,a_7b_6 + 3\,a_6b_7, 3\,a_4b_5 - 3\,a_5b_4, \\ \quad 2\,a_5 - 4\,a_3b_1 + 2\,b_6 + 4\,a_1b_3, -a_2b_5 + a_5b_2 - 4\,a_6b_1 + 6\,a_4b_3 + 4\,a_1b_6 - 6\,a_3b_4, \\ \quad a_2b_6 - a_6b_2 + 6\,a_1b_7 - 6\,a_7b_1 + 4\,a_5b_3 - 4\,a_3b_5, -6\,a_7b_5 + 6\,a_5b_7, 2\,b_3 + a_2, \\ \quad 2\,a_1 + b_2, 3\,a_2b_7 + 2\,a_6b_3 - 3\,a_7b_2 - 2\,a_3b_6, 2\,a_1b_2 - 2\,a_2b_1 + 3\,a_4 + b_5, \\ \quad -2\,a_3b_2 + 2\,a_2b_3 + 3\,b_7 + a_6, 3\,a_4b_2 - 2\,a_5b_1 + 2\,a_1b_5 - 3\,a_2b_4. \end{array}$$

The Bezoutian matrix is a 10×10 matrix of rank 9 (after simplification by the above equations for $a_4 \neq 0, a_5 \neq 0$). A maximal minor of this matrix is:

$$\begin{array}{l} \frac{4}{729{a_4}^4{a_5}^2}\left(3\,v_2a_4 - v_1a_5\right)^8 \Big(v_0 \\ \quad +(u_1 - \frac{3a_4a_2}{2a_5}\,{u_1}^2 - a_2\,u_1u_2 - \frac{a_5a_2}{6a_4}\,{u_2}^2 - a_4\,{u_1}^3 - a_5\,{u_1}^2u_2 - \frac{{a_5}^2}{3\,a_4}\,u_1{u_2}^2 - \frac{{a_5}^3}{27{a_4}^2}\,{u_2}^3)v_1 \\ \quad +(u_2 + \frac{9\,{a_4}^2a_2}{2\,{a_5}^2}\,{u_1}^2 + 3\,\frac{a_4a_2}{a_5}\,u_1u_2 + \frac{a_2}{2}\,{u_2}^2 + 3\,\frac{{a_4}^2}{a_5}\,{u_1}^3 + 3\,a_4\,{u_1}^2u_2 + a_5\,u_1{u_2}^2 + \frac{{a_5}^2}{9\,a_4}\,{u_2}^3)v_2\Big). \end{array}$$

So that the inverse of f is

$$\begin{array}{l} g_1(u) = u_1 - \frac{3a_4a_2}{2a_5}\,{u_1}^2 - a_2\,u_1u_2 - \frac{a_5a_2}{6a_4}\,{u_2}^2 - a_4\,{u_1}^3 - a_5\,{u_1}^2u_2 - \frac{{a_5}^2}{3\,a_4}\,u_1{u_2}^2 - \frac{{a_5}^3}{27{a_4}^2}\,{u_2}^3 \\ g_2(u) = u_2 + \frac{9\,{a_4}^2a_2}{2\,{a_5}^2}\,{u_1}^2 + 3\,\frac{a_4a_2}{a_5}\,u_1u_2 + \frac{a_2}{2}\,{u_2}^2 + 3\,\frac{{a_4}^2}{a_5}\,{u_1}^3 + 3\,a_4\,{u_1}^2u_2 + a_5\,u_1{u_2}^2 + \frac{{a_5}^2}{9\,a_4}\,{u_2}^3. \end{array}$$

This enables us to check the Jacobian conjecture for polynomials in two variables, of degree ≤ 3. It is already known in this case that it is true (see [3]), but without computing explicitly the inverse.

7 Bezoutians and resultants

In this section, we relate Bezoutians and Resultants. We recall the definition of Resultants over an irreducible projective variety X and show that in the case (of practical importance) where an open subset of X is parameterized by a polynomial map, this resultant is a factor of any maximal minor of the Bezoutian matrix. We illustrate this approach, by constructing the resultant of 3 equations on a quadric surface.

Elimination theory deals with the problem of finding conditions on parameters of a polynomial system, so that these equations have a common solution in a fixed algebraic set X. A typical situation is the case of $n+1$ "polynomials"

$$\left\{ \begin{array}{rcl} f_0(x) & = & \sum_{j=0}^{k_0} c_{0,j}\, \psi_{0,j}(x) \\ & \vdots & \\ f_n(x) & = & \sum_{j=0}^{k_n} c_{n,j}\, \psi_{n,j}(x) \end{array} \right.$$

where $\mathbf{c} = (c_{i,j})$ are parameters, x is a point of the variety X of dimension n, and the vector functions $\mathcal{L}_i(x) = (\psi_{i,j}(x))_{j=0,\ldots,k_i}$ are regular functions on X (see [25]) independent of the parameters $\mathbf{c}$. Let us denote by $f_0(x) = \cdots = f_n(x) = 0$ the global system of equations on X. In the language of modern algebraic geometry, the $\mathcal{L}_i$ would correspond to line bundles and the $f_i(x)$ to sections (see [18]).

The elimination problem consists, in this case, in finding necessary (and sufficient) conditions on the parameters $\mathbf{c} = (c_{i,j})_{i,j}$ such that the equations $f_0 = 0, \ldots, f_n = 0$ have a common root in X.

In the classical case, $\mathcal{L}_i(x)$ is the vector of all monomials of degree d_i and X is the projective space $\mathbb{P}^n$ of dimension n. The functions f_i are generic homogeneous polynomials of degree d_i. The necessary and sufficient condition on the parameters $\mathbf{c} = (c_{i,j})_{i,j}$ such that the homogeneous polynomials $f_0, \ldots, f_n$ have a common root in $X = \mathbb{P}^n$ is $\mathrm{Res}_{\mathbb{P}^n}(f_0, \ldots, f_n) = 0$ where $\mathrm{Res}_{\mathbb{P}^n}$ is the *classical projective resultant.*

Considering a geometric point of view, we are looking for the set of parameters $\mathbf{c} = (c_{i,j})$ such that there exists $x \in X$ with $\sum_{j=0}^{k_i} c_{i,j}\psi_{i,j}(x) = 0$ for $i = 0, \ldots, n$. In other words, the parameter vector $\mathbf{c}$ is the projection of the point $(\mathbf{c}, x)$ of the *incidence variety*

$$W_X = \{(\mathbf{c}, x) \in \mathbb{P}^{k_0} \times \cdots \times \mathbb{P}^{k_n} \times X;\ \sum_{j=0}^{k_i} c_{i,j}\psi_{i,j}(x) = 0\ ;\ i = 0, \ldots, n\}.$$

We denote by

$$\begin{array}{rcl} \pi_1 : W_X & \rightarrow & \mathbb{P}^{k_0} \times \cdots \times \mathbb{P}^{k_n}, \\ \pi_2 : W_X & \rightarrow & X, \end{array}$$

the two natural projections. The image of W_X by π_1 is precisely the set of parameters $\mathbf{c}$ for which the system has a root. The image by π_2 of a point of W_X is a solution in X of the associated system. Any polynomial in $\mathbf{c} = (c_{i,j})_{i,j}$ which vanishes on the projection $\pi_2(W_X)$ is called an *inertia form* (see [40]). The inertia forms are homogeneous polynomials in each subset $(c_{i,j})_{j=0,\ldots,k_i}$ of parameters.

Definition 7.1 — *If $\pi_1(W_X)$ is an hypersurface, then its equation (unique up to a scalar) will be called the* resultant *of $f_0, \ldots, f_n$. It will be denoted by* $\mathrm{Res}_X(f_0, \ldots, f_n)$.

In order to be in this case, we impose the following conditions:

Conditions 7.2

1. *X is a projective irreducible variety.*
2. *The regular functions $\mathcal{L}_i$ do not vanish identically on X (for $i = 0, \ldots, n$).*
3. *For generic values of* $\mathbf{c}$*, the system $f_0, \ldots, f_n$ has no solution in X, and n of these equations (say $f_1, \ldots, f_n$) have a finite number of common solutions.*

The point 1 is required, because affine algebraic varieties do not behave correctly by projection, but projective algebraic sets do.

Consider a point $x \in X$ and its fiber $\pi_2^{-1}(x)$ which is a linear space of $\mathbb{P}^{k_0} \times \cdots \times \mathbb{P}^{k_n} \times \{x\}$. As $\mathcal{L}_i(x) \neq 0$, for $i = 0, \ldots, n$ (condition 6.2.2), this space is of dimension $\sum_{i=0}^{n} k_i - n - 1$. By the fiber theorem (see [39][p. 60, 61], [25][p. 139]), we deduce that W_X is irreducible and of dimension $\sum_{i=0}^{n} k_i - 1$.

Thus, its projection by π_1 is an irreducible variety of dimension $\leq \sum_{i=0}^{n} k_i - 1$ or of codimension ≥ 1. Let us call Z this projection.

Let U be the dense subset of $\mathbb{P}^{k_0} \times \cdots \times \mathbb{P}^{k_n}$ such that the system $f_1 = \cdots = f_n = 0$ has a finite number of solutions (in X). Then $W_X \cap (U \times X)$ is a dense subset of W_X and projects by π_1 onto $Z \cap U$. As $\mathcal{Z}(f_1 = \cdots = f_n = 0)$ is finite, for any $\mathbf{c} \in Z \cap U$, $\pi_1^{-1}(\mathbf{c}) = \{(\mathbf{c}, \zeta) \,; \zeta \in \mathcal{Z}(f_1 = \cdots = f_n = 0) \cap \mathcal{Z}(f_0 = 0)\}$ is finite. Therefore, W_X and Z are of the same dimension and Z is an hypersurface of $\mathbb{P}^{k_0} \times \cdots \times \mathbb{P}^{k_n}$, defined by a unique equation $\mathrm{Res}_X(f_0, \ldots, f_n)$ (up to a scalar), called the *resultant* of $f_0, \ldots, f_n$ over X.

Assume that $\phi : \mathbb{A}^n \to X$ is a polynomial map such that $\phi(\mathbb{A}^n) = X_0$ is dense in X. Then $\tilde{f}_i = f_i \circ \phi$ is a polynomial in the variables $z = (z_1, \ldots, z_n)$ and the Bezoutian $\Theta_{\tilde{f}_0, \ldots, \tilde{f}_n}$ is well defined. The next theorem shows that the resultant $\mathrm{Res}_X(f_0, \ldots, f_n)$ can be recovered from the Bezoutian matrix $B_{\tilde{f}_0, \ldots, \tilde{f}_n}$.

Theorem 7.3 — *Assume that the conditions 7.2 are satisfied and that $\phi : \mathbb{A}^n \to X$ is a polynomial map such that its image is dense in X. Then any maximal minor of the Bezoutian matrix $B_{\tilde{f}_0, \ldots, \tilde{f}_n}$ is divisible by the resultant* $\mathrm{Res}_X(f_0, \ldots, f_n)$.

Proof. According to the conditions 7.2, the set of coefficients $(c_{i,j})$ of $f_1, \ldots, f_n$ such that $\mathcal{Z}(f_1 = \cdots = f_n = 0)$ is finite is a dense subset of $\mathbb{P}^{k_1} \times \cdots \times \mathbb{P}^{k_n}$. As $X_0 = \phi(\mathbb{A}^n)$ is a dense subset of X, the set of coefficients $c_{i,j}$ such that $\mathcal{Z}(f_1 = \cdots = f_n = 0)$ is finite and in X_0 is also a dense subset. Let us choose "generic" coefficients in this dense subset, for $f_1, \ldots, f_n$.

Then, the $\mathbb{K}$-vector space $\mathbb{K}[z_1,\ldots,z_n]/(\tilde{f}_1,\ldots,\tilde{f}_n)$ is of finite dimension. Let us denote by D_g the generic dimension of this quotient. For any $\tilde{f}_0 \in R$, we denote by $r_g(f_0)$ the generic rank of the Bezoutian matrix $B_{\tilde{f}_0,\ldots,\tilde{f}_n}$. The minors of size $r_g(f_0)$ of $B_{\tilde{f}_0}$ are polynomials in $\mathbf{c}$, which are not all identically zero and any minor of size $r_g(f_0)+1$ is identically zero.

According to lemma 2.6, for generic values of $\mathbf{c}$, the matrix $B_{\tilde{f}_0}$ can be decomposed as in (1), so that the rank of this matrix is

$$rank(M_{\tilde{f}_0}) + rank(L_{f_0}).$$

As for generic values of $\mathbf{c}$, the variety $\mathcal{Z}(\tilde{f}_0 = \cdots = \tilde{f}_n = 0)$ is empty, the multiplication matrix $M_{\tilde{f}_0}$ is generically invertible (the eigenvalues of $M_{\tilde{f}_0}$ are the values of f_0 at the roots of $\tilde{f}_1,\ldots,\tilde{f}_n$), that is of rank $D_g = \dim_{\mathbb{K}}\left(R/(\tilde{f}_1,\ldots,\tilde{f}_n)\right)$.

Let us choose now $f_1,\ldots,f_n$ such that their roots are in X_0 and f_0 has a common root with $f_1,\ldots,f_n$. In this case, $Res_X(f_0,\ldots,f_n)=0$. Moreover, we have $rank(M_{\tilde{f}_0}) < D_g$ (for $\tilde{f}_0$ vanishes at one of the roots of $\tilde{f}_1,\ldots,\tilde{f}_n$), and by specialization the rank of L_{f_0} cannot exceed the generic rank. Thus, the matrix $B_{\tilde{f}_0}$ is of rank $< r_g(f_0)$ and all the $r_g(f_0)\times r_g(f_0)$ minors vanish.

As the set of systems $(f_0,\ldots,f_n)$ such that $\mathcal{Z}(f_1=\cdots=f_n=0)\subset X_0$ and f_0 vanishes at one of these points, is a dense subset of the resultant variety $\mathcal{Z}(Res_X(f_0,\ldots,f_n)=0)$, it implies that any maximal minor of the Bezoutian matrix vanishes on this resultant variety. Consequently, any maximal minor (of size $r_g(f_0)$) is divisible by the resultant, which proves the theorem. $\square$

Example 7.4 — We want to compute the "resultant" (in some sense) of

$$\left\{\begin{array}{l} f_0 = c_{0,0} + c_{0,1}x + c_{0,2}y \\ f_1 = c_{1,0} + c_{1,1}x + c_{1,2}y + c_{1,3}(x^2+y^2) + c_{1,4}(x^2+y^2)^2 \\ f_2 = c_{2,0} + c_{2,1}x + c_{2,2}y + c_{2,3}(x^2+y^2) + c_{2,4}(x^2+y^2)^2. \end{array}\right.$$

Computing the Bezoutian matrix of these polynomials in (x,y), which is a 12×12 matrix of rank 10, and factoring a maximum non-zero minor of this matrix yields

$$c_{0,1}\left(-c_{1,4}c_{2,3}+c_{1,3}c_{2,4}\right)^3\left(c_{0,1}c_{1,4}c_{2,2}-c_{0,1}c_{1,2}c_{2,4}-c_{2,1}c_{0,2}c_{1,4}+c_{1,1}c_{0,2}c_{2,4}\right)\left({c_{0,2}}^2+{c_{0,1}}^2\right)^2$$
$$\left({c_{0,1}}^4{c_{1,0}}^4{c_{2,4}}^4+2\,{c_{0,1}}^2{c_{0,2}}^2{c_{1,0}}^4{c_{2,4}}^4+{c_{0,2}}^4{c_{1,0}}^4{c_{2,4}}^4-4\,c_{0,0}{c_{0,1}}^3{c_{1,0}}^3c_{1,1}{c_{2,4}}^4+\cdots\right).$$

In order to describe one of these factors as a resultant over a variety X, we consider first the following map

$$\begin{array}{rcl} \gamma:\mathbb{A}^2 & \to & \mathbb{A}^3 \\ (x,y) & \mapsto & (x,y,x^2+y^2). \end{array}$$

The closure of its image in $\mathbb{P}^3$ is a quadric of equation $z_0z_3-(z_1^2+z_2^2)=0$. Let us consider now the toric variety $\mathcal{T}$ associated to the polytopes A_0, A_1, A_1 where $A_0=(1,t_1,t_2)$,

$A_1 = (1, t_1, t_2, t_3, t_3^2)$, and the associated map ρ from $(\mathbb{C}^*)^3$ to $\mathcal{T}$ (see [18][chap. 8]). By construction, the image of ρ is dense in $\mathcal{T}$. Let $U = \gamma^{-1}((\mathbb{C}^*)^3)$ be the open subset of $\mathbb{A}^2$, so that $\rho \circ \gamma$ defines a map from U to $\mathcal{T}$. Let $\mathcal{Q}$ denotes the closure of its image in $\mathcal{T}$. In this case, the vectors $\mathcal{L}_i$ are just "coordinate" vectors on the toric variety $\mathcal{T}$. We check that the conditions 7.2 are satisfied. Thus, by theorem 7.3, $\mathrm{Res}_{\mathcal{Q}}(f_0, f_1, f_2)$ divides a maximal minor of the Bezoutian matrix.

As for generic equations f_1, f_2, f_3, the number of points in $\mathcal{Z}(f_0 = f_1 = 0)$, $\mathcal{Z}(f_0 = f_2 = 0)$, $\mathcal{Z}(f_1 = f_2 = 0)$ is 4 (see for instance [31]), $\mathrm{Res}_{\mathcal{Q}}(f_0, f_1, f_2)$ is homogeneous of degree 4 in the coefficients of each of the equations f_i. Thus, it corresponds to the last factor, containing 1011 monomials.

The factor $\left({c_{0,2}}^2 + {c_{0,1}}^2\right)$ corresponds to an extraneous factor of the resultant over the closure of $\gamma(\mathbb{A}^2)$ in $\mathbb{P}^3$. If we work in $\mathbb{P}^3$ instead of $\mathcal{T}$, the point 2 of the conditions 6.2 is not satisfied and the projection of W_X is not irreducible but still of codimension 1.

8 Rational representation of the isolated points

The goal of this section is to show how to compute a rational representation of the isolated roots of an affine variety defined by n equations, directly from Bezoutian matrices and to deduce bounds on the size of the coefficients in this representation.

Let $I = (f_1, \ldots, f_n)$ and $\mathcal{V}_0(I)$ the set of isolated points of the variety defined by I.

Definition 8.1 — *The Chow form of $\mathcal{V}_0(I)$ is*

$$\mathcal{C}_{f_1,\ldots,f_n}(u) = \prod_{\zeta \in \mathcal{V}_0(f_1,\ldots,f_n)} (u_0 + u_1\zeta_1 + \cdots + u_n\zeta_n)^{\mu_\zeta},$$

where μ_ζ is the multiplicity of $\zeta \in \mathcal{Z}$. The reduced Chow form is square-free part of the Chow form (with no μ). It will be denoted by $\mathcal{C}^r_{f_1,\ldots,f_n}(u)$.

As the commuting matrices M_{z_i} of multiplication by the variables z_i in $\mathcal{A} = R/(f_1, \ldots, f_n)$ can be put in a triangular form in a same basis and their eigenvalues are the i^{th} coordinates of the roots, counted with multiplicity, the Chow form $\mathcal{C}_{f_1,\ldots,f_n}(u)$ is also the determinant of $u_0\mathbb{I} + u_1 M_{z_1} + \cdots + u_n M_{z_n}$.

The following result is a direct generalization of the methods of [35], [2], [36] to the case where we have a multiple of the Chow form.

Theorem 8.2 — *Let $\Delta(u)$ be a multiple of the reduce Chow form $\mathcal{C}^r_f(u)$ of the isolated points of $\mathcal{V}_0(I)$. Then for a generic vector $(t_0, \ldots, t_n) \in \mathbb{K}^{n+1}$ and for $t+u = (t_0+u_0, \ldots, t_n+u_n)$, we have*

$$\frac{\Delta}{gcd(\Delta, \frac{\partial \Delta}{\partial_{u_0}})}(t+u) = d_0(u_0) + u_1 d_1(u_0) + \cdots + u_n d_n(u_0) + R(u)$$

with $R(u) \in (u_1, \ldots, u_n)^2$, $gcd(d_0(u_0), d_0'(u_0)) = 1$ and for all $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathcal{Z}$,

$$d_0'(\zeta_0)\, \zeta_i - d_i(\zeta_0) = 0,\ i = 1, \ldots, n$$

for some root $\zeta_0 = -t(\zeta)$ *of* $d_0(u_0) = 0$.

This proposition describes the coordinates of the isolated points $\zeta \in \mathcal{V}_0(I)$ as the values of rational fractions $\frac{d_i(u_0)}{d_0'(u_0)}$ at some of the roots of $d_0(u_0) = 0$. It does not imply that all the roots of $d_0(u_0)$ yield a point in $\mathcal{V}(I)$, so that this representation may be redundant. We will show hereafter how to remove the extraneous factors. Before proving this result, we need the following lemma:

Lemma 8.3 — *Let* $A(u)$ *and* $B(u)$ *be two polynomials in* $u = (u_0, u_1, \ldots, u_n)$*, which are relatively prime. Then for a generic vector* $(t_0, \ldots, t_n) \in \mathbb{K}^{n+1}$ *and for* $w = (t_0 + u_0, t_1, \ldots, t_n)$*,* $A(w) \in \mathbb{K}[u_0]$ *and* $B(w) \in \mathbb{K}[u_0]$ *are relatively prime.*

Proof. The roots of $A(w)$ (resp. $B(w)$) correspond to the points of intersection of the line L_t parameterized by $L_t(u_0) = (t_0 + u_0, t_1, \ldots, t_n)$ with the hypersurface $\mathcal{Z}(A(u) = 0)$ (resp. $\mathcal{Z}(B(u) = 0)$) of $\mathbb{K}^{n+1}$. The intersection of $\mathcal{Z}(A(u) = B(u) = 0)$ is of codimension 2, because the two polynomials $A(u)$ and $B(u)$ are relatively prime. Thus, for generic values of $(t_0, t_1, \ldots, t_n)$, the line L_t does not meet the variety $\mathcal{Z}(A(u) = B(u) = 0)$ and the polynomials $A(w), B(w) \in \mathbb{K}[u_0]$ have no common root (over $\overline{\mathbb{K}}$), which proves the lemma. □

Proof of the theorem 8.2. We denote by $\mathcal{Z}_0$ the set of isolated points of $\mathcal{Z}(f_1, \ldots, f_n)$. Let us decompose $\Delta(u)$ as

$$\Delta(u) = \prod_{\zeta \in \mathcal{Z}_0} (u_0 + u_1\zeta_1 + \cdots + u_n\zeta_n)^{n_\zeta} H(u),$$

in such a way that the two polynomials $\prod_{\zeta \in \mathcal{Z}_0}(u_0 + u_1\zeta_1 + \cdots + u_n\zeta_n)^{n_\zeta}$ and $H(u)$ are relatively prime. We denote by $d(u) = \frac{\Delta(u)}{gcd(\Delta(u), \frac{\partial \Delta}{\partial u_0}(u))}$. It is a polynomial of the form

$$d(u) = \prod_{\zeta \in \mathcal{Z}_0} (u_0 + u_1\zeta_1 + \cdots + u_n\zeta_n)\, h(u)$$

where $\prod_{\zeta \in \mathcal{Z}_0}(u_0 + u_1\zeta_1 + \cdots + u_n\zeta_n)$ and $h(u)$ are relatively prime. Let $t = (t_0, \ldots, t_n)$ be a vector of $\mathbb{K}^{n+1}$. Substituting u by $t + u = (t_0 + u_0, t_1 + u_1, \ldots, t_n + u_n)$ in d and h yields the polynomials

$$\begin{aligned} d(t+u) &= d_0(u_0) + u_1 d_1(u_0) + \cdots + u_n d_n(u_0) + R(u) \\ &= \prod_{\zeta \in \mathcal{Z}_0} (t(\zeta) + u_0 + u_1\zeta_1 + \cdots + u_n\zeta_n) h(t+u), \\ h(t+u) &= h_0(u_0) + u_1 h_1(u_0) + \cdots + u_n h_n(u_0) + S(u), \end{aligned}$$

where $t(\zeta) = t_0 + t_1\zeta_1 + \cdots + t_n\zeta_n$, and $R(u), S(u) \in (u_1, \ldots, u_n)^2$. By identification of the coefficients of the monomials in $(u_1, \ldots, u_n)$, we obtain

$$d_0(u_0) = \prod_{\zeta \in \mathcal{Z}_0} (t(\zeta) + u_0)\; h_0(u_0)$$

$$d_i(u_0) = \left(\sum_{\zeta \in \mathcal{Z}_0} \zeta_i \prod_{\zeta' \neq \zeta} (t(\zeta') + u_0) \right) h_0(u_0) + \prod_{\zeta \in \mathcal{Z}_0} (t(\zeta) + u_0) \; h_i(u_0).$$

Moreover, we also have

$$d_0'(u_0) = \left(\sum_{\zeta \in \mathcal{Z}_0} \prod_{\zeta' \neq \zeta} (t(\zeta') + u_0) \right) h_0(u_0) + \prod_{\zeta \in \mathcal{Z}_0} (t(\zeta) + u_0) \; h_0'(u_0).$$

According to lemma 8.3, for generic values of $t \in \mathbb{K}^{n+1}$, the polynomials $\prod_{\zeta \in \mathcal{Z}_0} (t(\zeta) + u_0)$ and $h_0(u_0) = h(t_0 + u_0, t_1, \ldots, t_n)$ are relatively prime, because $\prod_{\zeta \in \mathcal{Z}_0} (u_0 + u_1 \zeta_1 + \cdots + u_n \zeta_n)$ and $h(u)$ are relatively prime. Thus for any $\zeta \in \mathcal{Z}_0$, $h_0(-t(\zeta)) \neq 0$ and

$$\begin{aligned} d_0'(-t(\zeta)) &= \prod_{\zeta' \neq \zeta} (t(\zeta') - t(\zeta)) \; h_0(-t(\zeta)) \\ d_i(-t(\zeta)) &= \zeta_i \prod_{\zeta' \neq \zeta} (t(\zeta') - t(\zeta)) \; h_0(-t(\zeta)). \end{aligned}$$

As $gcd(d_0(u_0), d_0'(u_0)) = 1$, $d_0'(-t(\zeta)) \neq 0$. Thus, the i$^{\text{th}}$ coordinate of ζ is given by

$$\zeta_i = \frac{d_i(\zeta_0)}{d_0'(\zeta_0)},$$

where $\zeta_0 = -t(\zeta)$ is a root of $d_0(u_0) = 0$, which concludes the proof. □

In practice, instead of expanding completely the polynomial $d(t + u)$, it would advantageous to consider $u_1, \ldots, u_n$ as infinitesimal numbers (i.e. $u_i^2 = u_i u_j = 0$) in order to get only the first terms $d_0(u_0) + u_1 d_1(u_0) + \cdots + u_n d_n(u_0)$ of the expansion. The genericity condition on t is satisfied as soon as $gcd(d_0(u_0), d_0'(u_0)) = 1$. This can be checked effectively when $\Delta(u)$ is known. In this case, t is necessarily a separating form, $h(u_0)$ and $\prod_{\zeta \in \mathcal{Z}_0} (t(\zeta) + u_0)$ have no common root. Other techniques, like in [36], can also be used to construct a separating element and this rational representation, when the quotient is known, for instance through a Gröbner basis.

Remark 8.4 — In order to remove the extraneous factors of $d_0(u_0)$, notice that as the polynomials $d_0(u_0)$ and $d_0'(u_0)$ are relatively prime, the rational functions $\xi_i(u_0) = \frac{d_i(u_0)}{d_0'(u_0)}$ $(i = 0, \ldots, n)$ are well defined at the roots of $d_0(u_0) = 0$. The good roots are those for which $g_i(u_0) = f_i(\xi_1(u_0), \ldots, \xi_n(u_0)) = 0$, that is the roots of the irreducible factors of $d_0(u_0)$ which divide the numerator of $g_i(u_0)$. Thus we can proceed as follows. First, we factorise $d_0(u_0)$ into irreducible factors $p_1, \ldots, p_s$. Secondly, we substitute z_i by $\xi_i(u_0) = \frac{d_i(u_0)}{d_0'(u_0)}$ in $f_1, \ldots, f_n$ in order to get the reduced rational functions $g_1(u_0), \ldots, g_n(u_0)$. Finally, we keep the irreducible factors $p_j(u_0)$, which divide the numerators of the fractions $g_i(u_0)$ (for $i = 1, \ldots, n$).

Just as in the previous section, we show now that a multiple $\Delta(u)$ of the Chow form $\mathcal{C}_{f_1,\ldots,f_n}(u)$ can be obtained from a non-zero maximal minor of the Bezoutian matrix. This approach has the advantage to yield an "explicit" formulation for this polynomial $\Delta(u)$, so that its structure can be handled more carefully (for instance, by working directly on the matrix form, instead of dealing with the expansion of the minor).

A similar formulation, derived for resultant matrices, can be found for instance in [13]. As explained at the beginning, our approach is not specific to Bezoutian matrices. It also applies to other kind of resultant matrices (like toric resultant matrices, see [17]). In such a case, the matrix is square, the determinant is exactly the Chow form of $f_1,\ldots,f_n$ (for generic systems $f_1=\cdots=f_n=0$), and the roots are (generically) simple.

Proposition 8.5 — *Any maximal minor $\Delta(u)$ of the Bezoutian matrix $B_{u_0+u_1z_1+\cdots+u_nz_n}$ of $(u_0+u_1z_1+\cdots+u_nz_n, f_1,\ldots,f_n)$ is divisible by $\mathcal{C}_{f_1,\ldots,f_n}(u)$.*

Proof. According to lemma 2.6, there exists a basis of $R\otimes R$, such that for all $f_0\in R$, the matrix of the Bezoutian matrix B_{f_0} in this basis is of the form

$$B_{f_0}=\begin{pmatrix} M_{f_0} & 0 \\ 0 & L_{f_0}\end{pmatrix}$$

where M_{f_0} is the matrix of multiplication by f_0. Thus any maximal minor of the matrix $u_0B_1+u_1B_{z_1}+\cdots+u_nB_{z_n}=B_{u_0+u_1z_1+\cdots+u_nz_n}$ is divisible by

$$\det(u_0\mathbb{I}+u_1M_{z_1}+\cdots+u_nM_{z_n})=\mathcal{C}_{f_1,\ldots,f_n}(u).$$

□

This leads to the following algorithm:

Algorithm 8.6 — Minimal univariate rational representation of a complete intersection $f_1,\ldots,f_n$.

1. Compute a non-zero maximal minor $\Delta(u)$ of the Bezoutian matrix $B_{u_0+u_1z_1+\cdots+u_nz_n,f_1,\ldots,f_n}$.
2. Choose a random vector $t=(t_0,\ldots,t_n)$ of $\mathbb{K}^{n+1}$, compute the square-free part $d(u)$ of $\Delta(u)$, the first terms $d(t+u)=d_0(u_0)+u_1d_1(u_0)+\cdots+u_nd_n(u_0)+\cdots$ and set $\xi_i(u)=\frac{d_i(u_0)}{d_0'(u_0)}$ (for $i=1,\ldots,n$).
3. Factorise $d_0(u_0)$ and keep the irreducible factors $p_1(u_0),\ldots,p_k(u_0)$ which divide the numerators of the rational fractions $g_i(u_0)=f_i(\xi_1(u_0),\ldots,\xi_n(u_0))$, for $i=1,\ldots,n$.
4. Reduce the numerator and denominator of $\xi_i(u_0)$ by $p_j(u_0)$ and call it $\tilde{\xi}_{i,j}(u_0)$. Return the representation
$$p_j(u_0)=0, z_i=\tilde{\xi}_{i,j}(u_0), i=1,\ldots,n,$$
for $j=1,\ldots,k$.

As in section 3, we can deduce bounds on degree and the heights of $\Delta(u)$. We use the notations of lemma 2.7.

Proposition 8.7 — *The polynomial $\Delta(u)$ given by theorem 3.1 is at most of degree $(e\,d)^n$ and the height of its coefficients is bounded by*

$$(n+1)\,(e\,d)^n\ \left(T + (n+1)\,\log(d+1) + \log(n+1) + 2\right).$$

Proof. The proof proceeds exactly as in proposition 3.3, for the Bezoutian matrix is also linear in u, of size bounded by $(e\,d)^n$ and of the form $B_{f_0} = u_0\,M_0 + \cdots + u_n\,M_n$. □

9 Geometric decomposition

In this section, we are interested in systems of equations $f_1 = \cdots = f_n = 0$ such that the variety $\mathcal{Z}(f_1 = \cdots = f_n = 0)$ is not necessarily of dimension 0. We assume here that this variety has isolated components of dimension 0 but also components of higher dimension. We show how to recover the zero dimensional part and the other components, from the Bezoutian, extending the approach of [8] to the context of affine varieties.

The rational representation of the previous section allows us to recover the Chow form of the isolated points of the variety, and by using the algorithm 8.6, to compute a rational representation of these points. Once we have a description of these isolated points, we would like to compute the isolated components of higher dimension. For this purpose, we describe now a method which will proceed inductively from the lowest dimensional components to the components of highest dimension.

We first reduce the description of isolated components of dimension 1, to a zero dimensional problem, by considering one variable (say z_1) as a parameter. We assume that the projection from the isolated curves onto the line $z_2 = \cdots = z_n = 0$ is dominant, or that these curves are in Noether position, with respect to the variable z_1 (see [19] for more details on this problem). Let $K = \mathbb{K}(z_1)$ be the fraction field in z_1. Then, these curves correspond to "isolated points" in $K[z_2, \ldots, z_n]/(f_1, \ldots, f_n)$. In order to get a square system, we will replace the input polynomial system $f_1, \ldots, f_n$ by generic combinations of them $f'_i = \sum_j \lambda_{i,j} f_j$, for $i = 1, \ldots, n-1$. To ensure that the "isolated points" of $\mathcal{Z}_{\overline{K}}(f = 0)$ are still isolated in $\mathcal{Z}_{\overline{K}}(f'_1 = \cdots = f'_{n-1} = 0)$, we need the following lemma:

Lemma 9.1 — *Let A be a local ring and $(f_1, \ldots, f_m) \subset A$ an ideal of A such that the quotient $A/(f_1, \ldots, f_m)$ is of codimension c. Then for generic values of $(\lambda_{i,j}) \in \mathbb{K}^{c\,m}$, the sequence $f'_i = \sum_{j=1}^{m} \lambda_{i,j} f_j$, $(i = 1, \ldots, c)$ is a regular sequence of A.*

(see [29][chap. 6]).

Thus if p is an isolated point of $\mathcal{Z}(f_1 = \cdots = f_m = 0)$, and $A = K[z_2, \ldots, z_n]_p$ is the localization of $K[z_2, \ldots, z_n]$ at p, then the quotient $A/(f_1, \ldots, f_m)$ is of dimension 0 and for $n-1$ generic combinations $f'_1, \ldots, f'_{n-1}$ of the polynomials $f_1, \ldots, f_m$, the quotient

$A/(f'_1, \ldots, f'_{n-1})$ will still be of dimension 0. Consequently, p will be an isolated component of $\mathcal{Z}_{\overline{K}}(f'_1, \ldots, f'_{n-1})$.

Therefore, we can apply the perturbation techniques described in this section, in order to compute the isolated components of this variety, which will give us the isolated curves of the initial variety. Hiding a new variable and iterating this procedure will give us the components of dimension 2, 3 and so on. This yields the following algorithm:

Algorithm 9.2 — GEOMETRIC DECOMPOSITION OF A VARIETY.
Let $f_1, \ldots, f_m$ be m equations, in n variables, with coefficients in a field K.

1. If $m > n$, choose random combinations $f'_1, \ldots, f'_n$ of the input polynomials. If $n = 0$, then stop.
2. Compute the Bezoutian matrix of $f_0 = u_0 + u_1\, z_1 + \cdots + u_n z_n,\ {f'}_1, \ldots, {f'}_n$, a maximal non-zero minor $\Delta(u)$ of this matrix.
3. According to algorithm 8.6, compute a minimal rational representation of the roots of the system from $\Delta(u)$.
4. Choose one variable (say z_1) as a parameter and proceed to step 1, with n replaced by $n-1$ and K replaced by $K(z_1)$.

This decomposition is not necessarily minimal for some of the output components may be included into components of higher dimension.

The following examples have been computed by S. Tonelli, who implemented in MAPLE the previous algorithm[1] during her DEA.

Example 9.3 *Intersection of a circle with an hyperbola. We consider the following equations, where a, b, c are parameters:*

$$lp := [{z_1}^2 + {z_2}^2 - 1, (z_1 - a)\,(z_2 - b) - c].$$

The 4 (isolated) points are given by the formulas:

```
> decomp(lp,[z[1],z[2]],0);
```

$$\begin{aligned}
[&\frac{10000}{10201}\,{u_0}^4 + (\frac{20000}{10201} - \frac{20000}{10201}\,b - \frac{2000}{10201}\,a)\,{u_0}^3 \\
&\quad +(-\frac{30000}{10201}\,b - \frac{4000}{10201}\,c + \frac{4000}{10201}\,a\,b + \frac{100}{101}\,b^2 - \frac{3000}{10201}\,a + \frac{100}{101}\,a^2 + \frac{4900}{10201})\,{u_0}^2 + (\frac{100}{101}\,b^2 \\
&\quad - \frac{5100}{10201} - \frac{4000}{10201}\,c + \frac{4000}{10201}\,a\,b - \frac{1480}{10201}\,a - \frac{200}{101}\,a^2\,b + \frac{20}{101}\,b\,c - \frac{20}{101}\,b^2\,a + \frac{100}{101}\,a^2 \\
&\quad + \frac{5000}{10201}\,b + \frac{200}{101}\,a\,c)u_0 + \frac{7500}{10201}\,b - \frac{240}{10201}\,a + \frac{1020}{10201}\,c + c^2 - \frac{75}{101}\,b^2 + \frac{24}{101}\,a^2 + \frac{10}{101}\,b\,c
\end{aligned}$$

[1] see `http://www.inria.fr/saga/logiciels/multires.html`

$$+ a^2 b^2 + \frac{1000}{10201} a b - \frac{100}{101} a^2 b + \frac{100}{101} a c - \frac{1800}{10201} - \frac{10}{101} b^2 a - 2 a b c,$$

$$(-1000 u_0{}^3 a + (-100 + 2000 a b - 2000 c + 100 b^2 + 100 a^2 - 1500 a) u_0{}^2 + (-720 a + 200 a c$$
$$- 1030 b^2 a + 100 b^2 - 100 - 2000 c + 2000 a b + 1030 b c + 100 a^2 - 200 a^2 b) u_0 + 75$$
$$- 110 a + 530 c - 404 a b c - 75 b^2 - 77 a^2 + 500 a b + 202 c^2 - 100 a^2 b + 100 a c$$
$$- 515 b^2 a + 202 a^2 b^2 + 515 b c) \Big/ (-2000 u_0{}^3 + (3000 b - 3000 + 300 a) u_0{}^2$$
$$+ (-490 - 400 a b + 300 a + 400 c - 1010 b^2 - 1010 a^2 + 3000 b) u_0 - 250 b + 74 a$$
$$+ 200 c + 1010 a^2 b - 1010 a c - 101 b c + 101 b^2 a - 200 a b - 505 a^2 + 255 - 505 b^2),$$

$$(-1000 u_0{}^3 b + (-200 c - 1000 + 200 a b + 1000 a^2 + 1000 b^2 - 1500 b) u_0{}^2 + (-200 c$$
$$- 200 b^2 a + 1000 b^2 + 3010 a c - 1000 + 200 b c + 2250 b + 200 a b - 3010 a^2 b$$
$$+ 1000 a^2) u_0 + 1375 b + 251 c - 4040 a b c - 240 + 50 a b - 100 b^2 a + 2020 c^2$$
$$- 1760 b^2 + 240 a^2 + 100 b c + 2020 a^2 b^2 - 1505 a^2 b + 1505 a c) \Big/ (-2000 u_0{}^3$$
$$+ (3000 b - 3000 + 300 a) u_0{}^2$$
$$+ (-490 - 400 a b + 300 a + 400 c - 1010 b^2 - 1010 a^2 + 3000 b) u_0 - 250 b + 74 a$$
$$+ 200 c + 1010 a^2 b - 1010 a c - 101 b c + 101 b^2 a - 200 a b - 505 a^2 + 255 - 505 b^2)]$$

The first polynomial is the equation in u_0 defining the 4 points, the other terms are the rational fractions in u_0 and in the parameter a, b, c expressing the coordinates of the solution with respect to u_0.

Example 9.4 *This is an example containing points, a curve and a surface, and defined by*

$$lp :=$$
$$[(z_1 z_3 - z_2{}^2)(z_1 z_2 z_3 - 1),\ (z_2 - z_1{}^2)(z_1 z_2 z_3 - 1),\ (z_3 - z_1{}^3)(z_3{}^2 - z_1 - 1)(z_1 z_2 z_3 - 1)]$$

```
> decomp(lp,  [z[1],  z[2],  z[3]]);
```

$$\Delta = u_0{}^7 u_1{}^6 u_2{}^8 u_3{}^{13} (u_0 - u_3)(u_0 + u_3)(u_3 u_2 u_0 - u_2{}^2 u_1 + u_3 u_1{}^2)$$
$$d = (u_0 - u_3)(u_0 + u_3)(u_3 u_2 u_0 - u_2{}^2 u_1 + u_3 u_1{}^2) u_0$$
$$d1 = -\frac{113}{2500} (5 u_0 + 9)(5 u_0 + 1)(u_0 + 1)$$
$$d2 = \frac{2}{625} (5 u_0 + 1)(10 u_0 + 17)(5 u_0 + 9)(u_0 + 1)$$
$$d3 = \frac{1}{1250} (2825 u_0{}^2 + 1345 u_0 - 1381 + 875 u_0{}^3)(u_0 + 1)$$

The factorization of d_0 is

$$[\frac{14}{25}, [[u_0 + \frac{9}{5}, 1], [u_0 + \frac{1}{5}, 1], [u_0 + 1, 1], [u_0 + \frac{221}{140}, 1]]].$$

The minimal rational representation of points is given by

$$[u_0 + \frac{9}{5}, 0, 0, 1], [u_0 + \frac{1}{5}, 0, 0, -1], [u_0 + 1, 0, 0, 0]$$

where the first term of each list is the univariate polynomial and the others are the simplified rational fractions. In this case, we have 3 *points* $(0,0,0)$, $(0,0,1)$, $(0,0,-1)$.

For the component(s) of dimension 1, *taking* z_1 *as parameter we obtain*

$$\begin{aligned}
\Delta =& \frac{1}{216} {z_1}^{12}\, u_1\, {u_2}^3\, (u_0 + {z_1}^2 u_1 + {z_1}^3 u_2)(3042\, {u_2}^2 {u_1}^3 {z_1}^2 - 1183\, {u_2}^2 {u_1}^3 z_1 + 720\, {u_2}^4 u_1 z_1 \\
& - 1872\, {u_0}^2 {u_2}^2 u_1 - 432\, {u_0}^3 {u_2}^2 z_1 - 936\, u_0 {u_2}^3 u_1 {z_1}^4 - 1638\, u_0 {u_2}^2 {u_1}^2 z_1 \\
& - 936\, u_0 {u_2}^3 u_1 {z_1}^3 - 3042\, u_0 {u_2}^2 {u_1}^2 + 1872\, u_0 {u_2}^2 {u_1}^2 {z_1}^2 - 792\, {u_0}^2 {u_2}^2 u_1 z_1 \\
& - 432\, {u_0}^2 {u_2}^3 {z_1}^4 + 432\, {u_2}^5 {z_1}^4 + 216\, {u_2}^5 {z_1}^5 + 936\, u_2 {u_1}^2 {z_1}^5 {u_0}^2 + 432\, {u_2}^2 u_1 {z_1}^2 {u_0}^2 \\
& + 2808\, u_2 {u_1}^3 z_1 u_0 + 432\, {u_2}^2 u_1 {z_1}^3 {u_0}^2 + 864\, u_2 {u_1}^2 z_1 {u_0}^2 + 936\, {u_2}^3 u_1 {z_1}^2 u_0 \\
& + 1014\, u_2 {u_1}^2 {z_1}^3 {u_0}^2 + 2736\, {u_2}^2 {u_1}^2 {z_1}^3 u_0 + 216\, {u_2}^4 u_0 - 864\, u_2 {u_1}^3 {z_1}^4 u_0 + 468\, {u_2}^3 {u_0}^2 \\
& + 2028\, u_2 {u_1}^3 {z_1}^5 u_0 + 864\, {u_2}^2 {u_1}^2 {z_1}^4 u_0 + 864\, {u_2}^2 {u_1}^2 {z_1}^5 u_0 - 1152\, u_2 {u_1}^4 {z_1}^4 \\
& - 864\, u_2 {u_1}^3 {z_1}^3 u_0 + 648\, {u_2}^5 {z_1}^3 - 432\, {u_2}^3 {z_1}^2 {u_0}^2 - 432\, {u_2}^2 {u_0}^3 + 432\, {u_2}^4 z_1 u_0 \\
& + 216\, {u_2}^4 {z_1}^2 u_0 - 936\, {u_1}^3 {z_1}^4 {u_0}^2 - 216\, u_1 {z_1}^2 {u_0}^4 - 468\, {u_1}^5 {z_1}^2 + 216\, u_2 {z_1}^3 {u_0}^4 \\
& - 2197\, {u_2}^2 {u_1}^3 + 936\, u_2 {z_1}^3 u_1 {u_0}^3 - 1014\, {u_1}^5 {z_1}^6 + 216\, {u_1}^5 {z_1}^5 + 3042\, {u_1}^3 {z_1}^2 {u_0}^2 \\
& + 4178\, {u_1}^4 {z_1}^2 u_0 - 252\, {u_1}^5 {z_1}^3 - 216\, {u_1}^4 {z_1}^3 u_0 + 2413\, {u_1}^5 {z_1}^4 + 1404\, u_1 {u_0}^4 + 3042\, {u_1}^2 {u_0}^3 \\
& + 2197\, {u_1}^3 {u_0}^2 + 1092\, u_2 {u_1}^4 {z_1}^2 - 468\, {u_2}^5 - 432\, {u_2}^4 u_1 {z_1}^3 - 1014\, {u_2}^3 {u_1}^2 {z_1}^3 \\
& - 936\, u_2 {u_1}^4 {z_1}^3 - 432\, {u_2}^3 {z_1}^3 {u_0}^2 + 468\, {u_2}^4 u_1 + 432\, {u_2}^5 {z_1}^2 - 252\, {u_2}^5 z_1 - 216\, u_2 {u_1}^4 {z_1}^5 \\
& + 36\, {u_2}^4 u_1 {z_1}^2 - 216\, u_2 {u_1}^4 {z_1}^6 + 936\, {u_2}^3 {u_1}^2 {z_1}^6 + 1014\, u_2 {u_1}^4 {z_1}^7 + 1728\, u_2 {u_1}^3 {z_1}^2 u_0 \\
& + 2028\, u_2 {u_1}^4 z_1 + 216\, {u_0}^5 - 216\, {u_2}^4 u_1 {z_1}^4 + 2574\, {u_2}^2 {u_1}^3 {z_1}^3 + 936\, {u_2}^3 {u_1}^2 {z_1}^5 \\
& - 1014\, {u_1}^4 {z_1}^4 u_0 + 864\, u_2 {u_1}^2 {z_1}^2 {u_0}^2 - 78\, {u_2}^3 {u_1}^2 {z_1}^4)
\end{aligned}$$

The numerators are

$$\begin{aligned}
d1 =& -\frac{571}{22500} u_0 {z_1}^6 + \frac{279}{25000} {z_1}^9 + \frac{169}{12500} {z_1}^{10} + \frac{2096}{5625} u_0 {z_1}^4 - \frac{1043}{6000} {z_1}^3 {u_0}^2 \\
& + \frac{493}{150000} {z_1}^8 + \frac{1153}{75000} {z_1}^6 + \frac{1577}{112500} {z_1}^7 + \frac{3509}{120000} {z_1}^4 + \frac{22139}{90000} u_0 {z_1}^5 + \frac{47549}{1800000} {z_1}^5 \\
& + \frac{26}{25} {z_1}^5 {u_0}^3 + \frac{39}{100} {z_1}^6 {u_0}^3 + \frac{141}{50} {z_1}^2 {u_0}^3 + \frac{91}{30000} u_0 - \frac{2399}{600000} z_1 + \frac{2351}{4500} {z_1}^4 {u_0}^2 \\
& - \frac{38023}{1800000} {z_1}^2 - \frac{433}{120000} {z_1}^3 + \frac{567}{5000} u_0 {z_1}^8 + \frac{39}{250} {u_0}^2 {z_1}^8 + \frac{3}{20} z_1 {u_0}^3 + \frac{13}{4} {z_1}^3 {u_0}^4 + \frac{949}{225000}
\end{aligned}$$

$$- \frac{2669}{30000} u_0 {z_1}^3 - \frac{24397}{180000} u_0 {z_1}^2 + \frac{2947}{30000} u_0 {z_1}^7 - \frac{2197}{6000} {u_0}^2 + \frac{531}{500} {z_1}^5 {u_0}^2 + \frac{13}{5} {z_1}^2 {u_0}^4$$
$$- \frac{2}{5} {z_1}^4 {u_0}^4 + \frac{7307}{18000} {z_1}^2 {u_0}^2 - \frac{13}{150} {z_1}^6 {u_0}^2 + \frac{3}{20} z_1 {u_0}^2 + \frac{143}{150} {z_1}^3 {u_0}^3 - \frac{9}{25} {z_1}^4 {u_0}^3 + \frac{143}{60} {u_0}^4$$
$$- \frac{2093}{1800} {u_0}^3 + \frac{1409}{60000} u_0 z_1 + \frac{13}{2} {u_0}^5$$

$$d2 = \frac{253}{3750} u_0 {z_1}^6 + \frac{111}{6250} {z_1}^9 + \frac{169}{37500} {z_1}^{10} + \frac{3883}{15000} u_0 {z_1}^4 + \frac{1027}{27000} {z_1}^3 {u_0}^2$$
$$+ \frac{5087}{150000} {z_1}^8 + \frac{4951}{150000} {z_1}^6 + \frac{24619}{675000} {z_1}^7 + \frac{6383}{450000} {z_1}^4 + \frac{47369}{135000} u_0 {z_1}^5 + \frac{118193}{2700000} {z_1}^5$$
$$+ \frac{26}{75} {z_1}^5 {u_0}^3 + \frac{7}{25} {z_1}^6 {u_0}^3 - \frac{19}{50} {z_1}^2 {u_0}^3 - \frac{296}{5625} u_0 + \frac{23}{120000} z_1 + \frac{3}{125} {z_1}^4 {u_0}^2 - \frac{1783}{75000} {z_1}^2$$
$$- \frac{45739}{1350000} {z_1}^3 + \frac{253}{3750} u_0 {z_1}^8 + \frac{13}{125} {u_0}^2 {z_1}^8 + \frac{1}{5} z_1 {u_0}^3 + \frac{7}{6} {z_1}^3 {u_0}^4 + 2 {z_1}^3 {u_0}^5 + \frac{353}{33750} u_0 {z_1}^3$$
$$- \frac{77}{45000} u_0 {z_1}^2 + \frac{44}{5625} u_0 {z_1}^7 - \frac{331}{2000} {u_0}^2 + \frac{6311}{900000} + \frac{109}{750} {z_1}^5 {u_0}^2 - \frac{27}{125} {u_0}^2 {z_1}^7 + \frac{3}{5} {z_1}^6 {u_0}^4$$
$$- \frac{6}{5} z_1 {u_0}^4 + \frac{637}{1000} {z_1}^2 {u_0}^2 - \frac{67}{300} {z_1}^6 {u_0}^2 + \frac{3}{20} z_1 {u_0}^2 - \frac{224}{225} {z_1}^3 {u_0}^3 - \frac{27}{25} {z_1}^4 {u_0}^3 - \frac{6}{5} {u_0}^4$$
$$+ \frac{1}{40} {u_0}^3 - \frac{1063}{60000} u_0 z_1$$

The factorization of d_0 is

$$[1, [[u_0 - \frac{1}{10} + \frac{1}{5} {z_1}^2 + \frac{3}{10} {z_1}^3, 1], [- \frac{377}{45000} u_0 {z_1}^4 - \frac{13}{600} {z_1}^3 {u_0}^2$$
$$+ \frac{607}{225000} {z_1}^6 + \frac{169}{75000} {z_1}^7 + \frac{15091}{2700000} {z_1}^4 + \frac{199}{7500} u_0 {z_1}^5 + \frac{1133}{300000} {z_1}^5 + \frac{2}{25} {z_1}^2 {u_0}^3$$
$$- \frac{1759}{54000} u_0 + \frac{671}{600000} z_1 - \frac{133}{1500} {z_1}^4 {u_0}^2 + \frac{9619}{1350000} {z_1}^2 + \frac{13}{3125} {z_1}^3 - \frac{9}{50} z_1 {u_0}^3 + \frac{3}{10} {z_1}^3 {u_0}^4$$
$$+ \frac{149}{15000} u_0 {z_1}^3 + \frac{22981}{270000} u_0 {z_1}^2 - \frac{3409}{54000} {u_0}^2 - \frac{3539}{675000} + \frac{13}{250} {z_1}^5 {u_0}^2 - \frac{1}{5} {z_1}^2 {u_0}^4$$
$$+ \frac{49}{375} {z_1}^2 {u_0}^2 + \frac{9}{250} z_1 {u_0}^2 + \frac{7}{50} {z_1}^3 {u_0}^3 + \frac{4}{5} {u_0}^4 - \frac{11}{300} {u_0}^3 + \frac{183}{10000} u_0 z_1 + {u_0}^5, 1]]]$$

After simplification, we obtain the following rational parameterization of the unique component of dimension 1:

$$[u_0 - \frac{1}{10} + \frac{1}{5} {z_1}^2 + \frac{3}{10} {z_1}^3,\ {z_1}^2,\ {z_1}^3]$$

The first term is the equation in u_0 with parameter z_1 and the parameterization of the curve is $[z_1, {z_1}^2, {z_1}^3]$ (independent of u_0, because of the choice of the parameter z_1).

For the components of dimension 2, we have

$$\Delta = - \frac{4102893}{500000000} {z_1}^3 {z_2}^3 (u_0 z_1 z_2 + u_1)(185 {u_0}^3 + 185 {z_1}^3 u_1 {u_0}^2 - 59 z_1 u_0 {u_1}^2 - 185 u_0 {u_1}^2$$
$$- 185 {u_1}^3 {z_1}^4 - 185 {u_1}^3 {z_1}^3 + 88 {u_1}^3 {z_1}^2 + 126 {u_1}^3 {z_2}^2 - 88 z_2 {u_1}^3)$$

$$\begin{aligned}
d1 = &\frac{22315635027}{25000000000} z_1{}^5 z_2 + \frac{19886722371}{25000000000} z_1{}^4 z_2 + \frac{6634377981}{15625000000} z_1 z_2{}^2 \\
&- \frac{1694494809}{15625000000} z_1{}^2 z_2 - \frac{37996892073}{62500000000} z_2{}^3 z_1 - \frac{6634377981}{15625000000} z_1{}^3 z_2 - \frac{1062649287}{625000000} u_0 z_1 z_2 \\
&- \frac{52069815063}{25000000000} z_1{}^4 + \frac{6634377981}{6250000000} u_0 z_1 z_2{}^2 - \frac{37996892073}{25000000000} u_0 z_2{}^3 z_1 \\
&+ \frac{15028897059}{10000000000} u_0 z_1{}^4 z_2 + \frac{15028897059}{10000000000} u_0 + \frac{35584390989}{125000000000} z_1 + \frac{88659414837}{62500000000} z_2{}^2 \\
&- \frac{15480215289}{15625000000} z_2 + \frac{15480215289}{15625000000} x_1{}^2 - \frac{43568620767}{25000000000} z_1{}^3 - \frac{6634377981}{6250000000} u_0 z_1{}^3 z_2 \\
&+ \frac{22315635027}{10000000000} u_0 z_1{}^5 z_2 + \frac{1062649287}{500000000} z_1{}^3 u_0{}^2 + \frac{1062649287}{625000000} z_1{}^3 u_0 \\
&- \frac{455421123}{250000000} z_1{}^4 z_2 u_0{}^2 - \frac{1694494809}{2500000000} z_1{}^2 z_2 u_0{}^2 - \frac{1694494809}{3125000000} z_1{}^2 z_2 u_0 \\
&- \frac{151807041}{100000000} z_1{}^4 z_2 u_0{}^3 - \frac{1062649287}{3125000000} z_1 z_2 + \frac{19886722371}{25000000000} - \frac{1062649287}{500000000} z_1 z_2 u_0{}^2 \\
&- \frac{455421123}{250000000} u_0{}^2 - \frac{151807041}{100000000} u_0{}^3 + \frac{35584390989}{50000000000} u_0 z_1
\end{aligned}$$

The factorization of d_0 is

$$\begin{aligned}
[&\frac{-151807041}{100000000}, [[u_0{}^3 + \frac{6}{5} u_0{}^2 - \frac{7}{10} z_1{}^3 u_0{}^2 - \frac{2891}{18500} u_0 z_1 - \frac{14}{25} z_1{}^3 u_0 \\
&- \frac{1}{100} u_0 + \frac{343}{1000} z_1{}^4 + \frac{231}{1000} z_1{}^3 - \frac{3773}{23125} z_1{}^2 - \frac{2891}{46250} x_1 - \frac{21609}{92500} z_2{}^2 + \frac{3773}{23125} z_2 - \frac{33}{250}, 1], \\
&[\frac{2}{5} z_1 z_2 + u_0 z_1 z_2 - \frac{7}{10}, 1]]]
\end{aligned}$$

which yields the following rational representation for the component of dimension 2*:*

$$[\frac{2}{5} z_1 z_2 + u_0 z_1 z_2 - \frac{7}{10}, \frac{1}{z_1 z_2}]$$

References

[1] L.A. Aizenberg and A. M. Kytmanov. Multdimensional analogues of newtons formulas for systems of nonlinear algebraic equations and some of their applications. *Trans. from Sib. Mat. Zhurnal*, 22(2):19–39, 1981.

[2] M.E. Alonso, E. Becker, M.F. Roy, and T. Wörmann. Zeros, multiplicities and idempotents for zero dimensional systems. In L. González and T. Recio, editors, *Algorithms in Algebraic Geometry and Applications*, volume 143 of *Prog. in Math.*, pages 1–15. Birkhäuser, Basel, 1996.

[3] H. Bass, F.H. Conell, and D. Wright. The Jacobian Conjecture: reduction of degree and formal expansion of the inverse. *Bull. Amer. Math. Soc.*, 7:287–330, 1982.

[4] E. Becker, J.P. Cardinal, M.F. Roy, and Z. Szafraniec. Multivariate Bezoutians, Kronecker symbol and Eisenbud-Levin formula. In L. González and T. Recio, editors, *Algorithms in Algebraic Geometry and Applications*, volume 143 of *Prog. in Math.*, pages 79–104. Birkhäuser, Basel, 1996.

[5] C.A. Berenstein, R. Gay, A. Vidras, and A. Yger. *Residue Currents and Bezout Identities*, volume 114 of *Prog. in Math.* Birkhäuser, 1993.

[6] E. Bézout. *Théorie Générale des Équations Algébriques.* Paris, 1779.

[7] Berenstein C.A. and A. Yger. Residue calculus and Effective Nullstellensatz. Technical report, University of Maryland, 1996.

[8] J. Canny. Generalised characteristic polynomials. *J. Symbolic Computation*, 9:241–250, 1990.

[9] J.P. Cardinal and B. Mourrain. Algebraic approach of residues and applications. In J. Renegar, M. Shub, and S. Smale, editors, *Proc. AMS-SIAM Summer Seminar on Math. of Numerical Analysis, (Park City, Utah, 1995)*, volume 32 of *Lectures in Applied Math.*, pages 189–210. Am. Math. Soc. Press, 1996.

[10] E. Cattani and A. Dickenstein. A global view of residues in the torus. *J. of Pure and Applied Algebra*, 117 & 118:119–144, 1996.

[11] E. Cattani, A. Dickenstein, and B. Sturmfels. Computing multidimensional residues. In L. González-Vega and T. Recio, editors, *Algorithms in Algebraic Geometry and Applications*, volume 143 of *Prog. in Math.* Birkhäuser, Basel, 1996.

[12] J. Chadzynski and T. Krasinski. On the Lojasiewicz exponent at infinity for polynomial mappings of $\mathbb{C}^2$ into $\mathbb{C}^2$ and components of polynomial automorphisms of $\mathbb{C}^2$. *Ann. Pol. Math.*, pages 291–302, 1992.

[13] M. Chardin. Multivariate subresultants. *J. Pure and Appl. Alg.*, 101:129–138, 1995.

[14] A. Dickenstein and C. Sessa. An effective residual criterion for the membership problem in $\mathbb{C}[z_1, \ldots, z_n]$. *J. Pure Appl. Algebra*, 74:149–158, 1991.

[15] M. Elkadi. Bornes pour les Degrés et les Hauteurs dans le Problème de Division. *Michigan Math. J.*, 40:609–618, 1993.

[16] M. Elkadi and B. Mourrain. Approche Effective des Résidus Algébriques. Rapport de Recherche 2884, INRIA, 1996.

[17] I.Z. Emiris and J.F. Canny. Efficient incremental algorithms for the sparse resultant and the mixed volume. *J. Symbolic Computation*, 20(2):117–149, August 1995.

[18] I.M. Gelfand, M.M. Kapranov, and A.V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants.* Birkhäuser, Boston-Basel-Berlin, 1994.

[19] M. Giusti and J. Heintz. La détermination des points isolés et de la dimension d'une variété algebrique peut se faire en temps polynomial. In *Proc Int. Meeting on Commutative Algebra*, volume XXXIV of *Symp. Mathematica*, pages 216–255, Cortona,1991.

[20] M. Giusti, J. Heintz, K. Hägele, J.E. Morais, L.M. Pardo, and S.L. Montaña. Lower bounds for diophantine approaximations. *J. of Pure and Applied Algebra*, 117 & 118:119–144, 1996.

[21] L. González-Vega and G. Trujillo. Using symmetric functions to describe the solution of a zero dimensional ideal. In G. Cohen, M. Giusti, and T. Mora, editors, *AAECC'95*, volume 948 of *LNCS*, pages 232–247. Springer-Verlag, 1995.

[22] Ph. Griffiths and J. Harris. *Principles of Algebraic Geometry.* Wiley Interscience, New York, 1978.

[23] W. Gröbner. *Moderne algebraische Geometrie.* Springer-Verlag, 1949.

[24] L. Habsieger. Sur un problème combinatoire. Communication personnelle, 1998.

[25] J. Harris. *Algebraic Geometry, a fisrt course*, volume 133 of *Graduate Texts in Math.* Springer, 1992.

[26] T. Krick and L.M. Pardo. A computational method for diophatine approximation. In L. González-Vega and T. Recio, editors, *Algorithms in Algebraic Geometry and Applications*, volume 143 of *Prog. in Math.*, pages 193–254. Birkhäuser, Basel, 1996.

[27] E. Kunz. *Kähler differentials.* Advanced lectures in Mathematics. Friedr. Vieweg and Sohn, 1986.

[28] S. Lang. *Algebra.* Addison-Wesley, 1980.

[29] H. Matsumura. *Commutative Algebra.* Mathematics Lecture Notes Series. The Benjamin/Cummings Publishing Company, 1980.

[30] E. Mayr and A. Meyer. The complexity of the word problem for commutative semigroups and polynomial ideals. *Adv. in Math.*, 127:305–329, 1998.

[31] B. Mourrain. Enumeration problems in Geometry, Robotics and Vision. In L. Gonzáles and T. Recio, editors, *Algorithms in Algebraic Geometry and Applications*, volume 143 of *Prog. in Math.*, pages 285–306. Birkäuser, Basel, 1996.

[32] B. Mourrain. Computing isolated polynomial roots by matrix methods. *J. Symbolic Computation, Special Issue on Symbolic-Numeric Algebra for Polynomials*, Dec. 1998.

[33] A. Ploski. On the growth of proper polynomial mappings. *Ann. Pol. Math.*, 45:297–309, 1985.

[34] A. Ploski. Algebraic dependence and polynomial automorphisms. *Bull. Pol. Acad. Sci. Math.*, 34:653–659, 1986.

[35] J. Renegar. On the computational complexity and geometry of the first order theory of reals (I, II, III). *J. Symbolic Computation*, 13(3):255–352, 1992.

[36] F. Rouillier. *Algorithmes efficaces pour l'étude des zéros réels des systèmes polynomiaux.* PhD thesis, Université de Rennes, 1996.

[37] F. Rouillier. Solving zero-dimensional polynomial systems throuhg Rational Univariate Representation. Technical Report 3426, INRIA, Lorraine, France, May 1998.

[38] G. Scheja and U. Storch. Über Spurfunktionen bei vollständigen Durschnitten. *Journal Reine Angew Mathematik*, 278:174–190, 1975.

[39] I.R. Shafarevitch. *Basic Algebraic Geometry.* Springer Verlag, 1974.

[40] B.L. Van der Waerden. *Modern algebra, Vol. II.* Frederick Ungar Publishing Co, 1948.

[41] W.V. Vasconcelos. *Computational Methods in Commutative Algebra and Algebraic Geometry*, volume 2 of *Algorithms and Computation in Mathematics.* Springer, 1998.

Unité de recherche INRIA Sophia Antipolis
2004, route des Lucioles - B.P. 93 - 06902 Sophia Antipolis Cedex (France)

Unité de recherche INRIA Lorraine : Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - B.P. 101 - 54602 Villers lès Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38330 Montbonnot St Martin (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 Le Chesnay Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, B.P. 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399