Isolated points, duality and residues

Bernard Mourrain

Isolated points, duality and residues

B. Mourrain
INRIA, Projet SAFIR,
2004 routes des Lucioles, BP 93,
06902 Sophia-Antipolis,
mourrain@sophia.inria.fr

This work is dedicated to the memory of J. Morgenstern

June 1996

Abstract

In this paper, we are interested in the use of duality in effective computations on polynomials. We represent the elements of the dual of the algebra R of polynomials over the field $\mathbb{K}$ as formal series $\in \mathbb{K}[[\partial]]$ in differential operators. We use the correspondence between ideals of R and vector spaces of $\mathbb{K}[[\partial]]$, stable by derivation and closed for the (∂)-adic topology, in order to construct the local inverse system of an isolated point. We propose an algorithm, which computes the orthogonal D of the primary component of this isolated point, by integration of polynomials in the dual space $\mathbb{K}[\partial]$, with good complexity bounds. Then we apply this algorithm to the computation of local residues, the analysis of real branches of a locally complete intersection curve, the computation of resultants of homogeneous polynomials.

1 Introduction

Considering polynomials as algorithms (that compute a value at a given point) instead of lists of terms, has lead to recent interesting developments, as well from a practical or a theoretical point of view. In these approaches,

evaluations at points play an important role. We would like to pursue this idea further and to study evaluations by themselves. In other words, we are interested here, by the properties of the dual of the algebra of polynomials. Our objective is to understand the properties of the dual, which can be advantageous for effective computations on polynomials. Though from a mathematical point of view, working in the algebra of polynomials or in its dual are equivalent, from an effective point of view some operations (like localization, elimination of variables) are cheaper in the dual space. In this paper, we will focus on isolated points, where series in the local rings are replaced advantageously by polynomials in the dual space. The cornerstone of this duality consists to replace multiplication by derivation. We will exploit this idea, in order to devise an algorithm for the computation of the dual of $B = R/I$, which proceeds from bottom (with the evaluation at the isolated point defined by the ideal I) to the top (with a basis of the dual of B). Each step of this algorithm consists, roughly speaking, of integrating the preceding polynomials, and requires only linear algebra tools.

Our work is inspired by [10] or [15]. Recently, another method (inspired by [11]) was proposed in [18] for the computations of the local inverse system. We think that the present work is an improvement of this approach on the following points: a complete characterization of the elements constructed at each integration, a better complexity bound (of the same order than Gaussian elimination in the vector space B on $n^2 + m$ matrices), bounds for the size of the coefficients of a basis of $\hat{B}$, an explicit and effective correspondence between the structure of the inverse system of I and the algebraic structure of B, applications of these techniques to the computation of local residues and related bounds, to the local analysis of real complete intersection curves, to the computation of resultants.

In the first part of this paper, we describe the main (and classical) properties of the dual of the algebra, and the inverse systems. The next section deals with ideals I with an $\mathbf{m}_\zeta$-primary component Q_ζ (where $\mathbf{m}_\zeta$ is the maximal ideal defining the point ζ). We show how to extract this component and to recover the multiplicative structure of $B_\zeta = R/Q_\zeta$. Then, we construct the local inverse system, by characterizing the elements of degree d of $D = Q_\zeta^\perp$, when we know those of degree $d-1$, yielding an algorithm based on linear algebra with a better complexity than the one proposed in [18] and new bounds on the size of the coefficients. We illustrate this method with the computation of local residues, for locally complete intersection (based on [21],[14]) (the complexity and size for the coefficients of this residue are given), with yet

another way to compute resultants of homogeneous polynomials (based on [12],[13]) and with the analysis of real branches of locally complete intersection curves ([8], [19]). The implementation of these techniques, its practical comparison with the usual approach of local Gröbner bases computations, and its application to real problems are still under progress.

2 Duality between polynomials and differential operators

More details on the material of this section can be found in [10], [15].

2.1 Notations

Let $\mathbb{K}$ be a field of characteristic 0. The algebraic closure of $\mathbb{K}$ will be denoted by $\overline{\mathbb{K}}$. Let denote by $R = \mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[\mathbf{x}]$, the ring of polynomials in the variables $x_1, \ldots, x_n$ over $\mathbb{K}$. In this ring, we consider an ideal that we denote by I. The quotient of R by I is denoted by $B = R/I$. The class of an element $p \in R$ in B will be denoted by $\overline{p}$. For any element $p_1, \ldots, p_s \in R$, the $\mathbb{K}$-vector space generated by these elements is $\langle p_1, \ldots, p_s \rangle$.

Let $\hat{R}$ be the dual of the $\mathbb{K}$-vector space R, that is the space of linear forms

$$\begin{array}{rcl} \lambda : R & \to & \mathbb{K} \\ p & \mapsto & \lambda(p) \end{array}$$

We **fix here a point** $\zeta = (\zeta_1, \ldots, \zeta_n)$ **of** $\mathbb{K}^n$ and let $\mathbf{m}_\zeta = (x_1 - \zeta_1, \ldots, x_n - \zeta_n)$ be the maximal ideal of R, defining ζ. Among nice linear forms is certainly the *evaluation at* ζ:

$$\begin{array}{rcl} \partial_\zeta : R & \to & \mathbb{K} \\ p & \mapsto & p(\zeta) \end{array}$$

But for any $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$, we can also consider

$$\begin{array}{rcl} \partial_\zeta^{\mathbf{a}} : R & \to & \mathbb{K} \\ p & \mapsto & (d_{x_1})^{a_1} \cdots (d_{x_n})^{a_n} (p)(\zeta) \end{array} \tag{1}$$

where d_{x_i} is the derivation with respect to the variable x_i. We denote this linear form by $\partial_\zeta^{\mathbf{a}} = (\partial_{1,\zeta})^{a_1} \cdots (\partial_{n,\zeta})^{a_n}$.

Definition 2.1 — *The space of formal series in the variables $\partial_{i,\zeta}$ is denoted by $\mathbb{K}[[\partial_{1,\zeta},\ldots,\partial_{n,\zeta}]]$ or $\mathbb{K}[[\partial_\zeta]]$ or $\mathbb{K}[[\partial_1,\ldots,\partial_n]] = \mathbb{K}[[\partial]]$, if the point ζ is implicit. The ideal of $\mathbb{K}[[\partial_\zeta]]$ generated by $\partial_{1,\zeta},\ldots,\partial_{n,\zeta}$ is denoted by (∂_ζ).*

The next proposition shows how any linear form $\in \hat{R}$ can be seen as *formal series of differential operators "at" ζ*:

Proposition 2.2 — *There is a $\mathbb{K}$-isomorphism of topological spaces between $\hat{R}$ (with the topology of simple convergence for the trivial topology on $\mathbb{K}$[1]) and the set of formal series $\mathbb{K}[[\partial_\zeta]]$ (with (∂)-adic topology[2]).*

See [10]. Remark that for any $(a_1,\ldots,a_n)\in\mathbb{N}^n, (b_1,\ldots,b_n)\in\mathbb{N}^n$:

$$\frac{1}{\prod_{i=1}^n a_i!}\partial_{1,\zeta}^{a_1}\cdots\partial_{n,\zeta}^{a_n}\left(\prod_{i=1}^n (x_i-\zeta_i)^{b_i}\right) = \begin{cases} 1 \text{ if } \forall i, a_i = b_i, \\ 0 \text{ elsewhere.}\end{cases}$$

So that $(\frac{1}{\prod_{i=1}^n a_i!}\partial_\zeta^{\mathbf{a}})$ is the dual basis of the monomial basis $(\prod_{i=1}^n (x_i-\zeta_i)^{a_i})$. Let denote by $\mathbf{x}_\zeta^{\mathbf{a}}$, the product $\prod_{i=1}^n (x_i-\zeta_i)^{a_i}$ and $\mathbf{d}^{\mathbf{a}} = \frac{1}{\prod_{i=1}^n a_i!}\prod_{i=1}^n \partial_{i,\zeta}^{a_i}$ the elements of its dual basis. Caution must taken on this notation, which is not multiplicative: $\mathbf{d}^{\mathbf{a}}\,\mathbf{d}^{\mathbf{a}'} \neq \mathbf{d}^{\mathbf{a}+\mathbf{a}'}$. We have assume at the beginning that the characteristic of $\mathbb{K}$ is 0, but this is not mandatory. We can avoid the division by $a_i!$ by working directly in $\mathbb{K}[[\mathbf{d}]]$ instead of $\mathbb{K}[[\partial_\zeta]]$.

We can now identify any linear form $\lambda \in \hat{R}$ with a formal series in $\partial_{1,\zeta},\ldots,\partial_{n,\zeta}$, via its decomposition in the dual basis:

$$\begin{aligned}\lambda &= \sum_{(a_1,\ldots,a_n)\in\mathbb{N}^n} \lambda((x_1-\zeta_1)^{a_1}\cdots(x_n-\zeta_n)^{a_n})\frac{1}{\prod_{i=1}^n a_i!}\partial_\zeta^{\mathbf{a}} \\ &= \sum_{\mathbf{a}=(a_1,\ldots,a_n)\in\mathbb{N}^n} \lambda_{a_1,\ldots,a_n}\,\partial_{1,\zeta}^{a_1}\cdots\partial_{n,\zeta}^{a_n} \qquad (2)\end{aligned}$$

(this is just Taylor expansion formula at ζ). This defines a one-to-one correspondence between the series $\sum_{(a_1,\ldots,a_n)\in\mathbb{N}^n}\lambda_{a_1,\ldots,a_n}\partial_{1,\zeta}^{a_1}\cdots\partial_{n,\zeta}^{a_n}$ and the linear forms λ, which is compatible with the topology given in (2.2). From now on, **we will identify $\hat{R}$ with $\mathbb{K}[[\partial_{1,\zeta},\ldots,\partial_{n,\zeta}]]$**. The evaluation at ζ corresponds to the constant 1 in this formalism. It will also be denoted by $\partial_\zeta = \partial_\zeta^0$. Note

[1] $\lim_{n\to\infty}\lambda_n = 0$ iff $\forall p\in R, \exists N\in\mathbb{N}$ *st.* $\forall n\geq N, \lambda_n(p) = 0$

[2] The basic neighborhoods of 0 are the ideals $(\partial)^k$, see [3].

that these objects are connected with those which appear in the theory of $\mathcal{D}$-modules. In such a field, the coefficients are not necessarily constants $\in \mathbb{K}$, but belongs to a ring of functions. We refer to [17], [16], for more information on this topic.

2.2 The R-module $\hat{R}$

The space $\hat{R}$ has a natural structure of R-module as follows. For any $p \in R$ and $\lambda \in \hat{R}$, we define $p \cdot \lambda$ as

$$\begin{array}{rcl} p \cdot \lambda : R & \rightarrow & \mathbb{K} \\ q & \mapsto & \lambda(p\, q). \end{array}$$

Lemma 2.3 — *The multiplication by $x_i - \zeta_i$ in $\hat{R}$ corresponds to the derivation d_{∂_i} with respect to ∂_i in $\mathbb{K}[[\partial_\zeta]]$.*

Proof. Remark that for any elements $p \in R$ and $a \in \mathbb{N}$,

$$\begin{array}{rcl} (d_{x_i})^a \left((x_i - \zeta_i)\, p\right) & = & (d_{x_i})^{a-1} \left(p + (x_i - \zeta_i)\, d_{x_i} p\right) \\ & = & (d_{x_i})^{a-2} \left(2\, d_{x_i}(p) + (x_i - \zeta_i)\ (d_{x_i})^2 (p)\right) \\ & = & a\ (d_{x_i})^{a-1} (p) + (x_i - \zeta_i)\ (d_{x_i})^a (p) \end{array}$$

Consequently for any element $p \in R, \mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$, we have

$$\begin{array}{rcl} (x_i - \zeta_i) \cdot \partial^{\mathbf{a}}(p) & = & \partial^{\mathbf{a}}((x_i - \zeta_i)\, p) \\ & = & a_i \partial_1^{a_1} \cdots \partial_{i-1}^{a_{i-1}} \partial_i^{a_i - 1} \partial_{i+1}^{a_{i+1}} \cdots \partial_n^{a_n}(p) = d_{\partial_i}(\partial^{\mathbf{a}})(p) \end{array}$$

and $(x_i - \zeta_i)$ acts as a derivation on $\mathbb{K}[[\partial_\zeta]]$. □

Remark 2.4 *Similarly, we can check that the multiplication by $\partial_{i,\zeta}$ in $\mathbb{K}[[\partial_\zeta]]$ acts as a derivation on polynomials: For all $p \in R$, $\lambda \in \mathbb{K}[[\partial_\zeta]]$, $i = 1 \ldots n$, we have*

$$(\partial_{i,\zeta} \lambda)(p) = \lambda(d_{x_i} p).$$

2.3 Inverse system

Let I be an ideal of R.

Definition 2.5 (Macaulay [15][p. 65]) — *The inverse system of I is the vector space of $\hat{R}$:*

$$I^\perp = \{\lambda \in \hat{R} \ ; \ \forall p \in I, \lambda(p) = 0\}.$$

Note that $I^\perp$ is stable by derivation, for I is stable by multiplication (Lemma 2.3). The inverse system generated by elements $\beta_1, \ldots, \beta_d \in \hat{R} = \mathbb{K}[[\partial_\zeta]]$ will be, by definition, the vector space generated by these elements and their derivatives.

For any vector-space D of $\hat{R}$, we also denote by $D^\perp = \{p \in R; \ \forall \lambda \in D, \lambda(p) = 0\}$.

Note that there is a canonical $\mathbb{K}$-isomorphism between $I^\perp$ and the dual $\hat{B}$ of B, which is the transposed map of $R \twoheadrightarrow B = R/I$. Thus, we can see the elements of $\hat{B}$ as elements of $\hat{R}$ orthogonal to the elements of I. From now on, **we identify $I^\perp$ and $\hat{B}$**.

As corollary of proposition (2.2) and lemma (2.3), we have :

Proposition 2.6 — *The ideals of R are in one-to-one correspondence with the vector spaces of $\mathbb{K}[[\partial_\zeta]]$ stable by derivation and closed for the (∂)-adic topology.*

(see [10]). This theorem tells us that *the description of an ideal of R is equivalent to the description of its orthogonal in the space of formal series.*

3 Isolated points

We show in this section, how computations with series in the local ring of ζ can be replaced in the dual space by computations with polynomials in the variables ∂_ζ, for a $\mathbf{m}_\zeta$-primary ideal.

3.1 The $\mathbf{m}_\zeta$-primary component

The correspondence defined in (2.6) restricted to the $\mathbf{m}_\zeta$-primary ideals take the following form:

Theorem 3.1 — *The $\mathbf{m}_\zeta$-primary ideals are in one-to-one correspondence with the non-null vector spaces of finite dimension of $\mathbb{K}[\partial]$, which are stable by derivations.*

This result was attributed to Gröbner in [18]. See also [15] and [10] where we can find a more modern version of this result.

In practice, it is not frequent to deal directly with a $\mathbf{m}_\zeta$-primary ideal. More often, we have an ideal I, given by a set of generators, which has an $\mathbf{m}_\zeta$-primary component. This ideal needs not define a variety of dimension 0 (on the algebraic closure of $\mathbb{K}$), but we only require that the point ζ is an isolated point of this variety. We are interested here in the local properties at this point and we give now a way to "extract" the $\mathbf{m}_\zeta$-primary component of I and *forget what is not near the point* ζ.

Theorem 3.2 — *Let I be an ideal of R with an $\mathbf{m}_\zeta$-primary component Q_ζ, let D_ζ be $I^\perp \cap \mathbb{K}[\partial_{1,\zeta}, \ldots, \partial_{n,\zeta}]$. Then $D_\zeta^\perp = Q_\zeta$.*

This result, is not in the work of Macaulay, though it is underlying in some of his constructions (see [15][p 74]) and we have not find a reference where it appears explicitly.

Proof. As $I \subset Q_\zeta$, we have $Q_\zeta^\perp \subset I^\perp$. By the previous theorem, we also have $Q_\zeta^\perp \subset \mathbb{K}[\partial_\zeta]$. Therefore, $Q_\zeta^\perp \subset I^\perp \cap \mathbb{K}[\partial_\zeta] = D_\zeta$ and $D_\zeta^\perp \subset Q_\zeta$.

We prove now the inverse inclusion using the two following facts:

- The $\mathbf{m}_\zeta$-primary component Q_ζ of I is the set of polynomials f such that there exists $g \in R$ with $f\,g \in I$ and $g(\zeta) \neq 0$ (see [3]).
- For any $\lambda \in \mathbb{K}[\partial_i]$, for any $g \in R$, we have according to (2.3)

$$\begin{aligned} g \cdot \lambda(f) &= g(\zeta_1 + d_{\partial_1}, \ldots, \zeta_n + d_{\partial_n})(\lambda)(f) \\ &= \lambda(f)\, g(\zeta) + (g - g(\zeta))(\zeta_1 + d_{\partial_1}, \ldots, \zeta_n + d_{\partial_n})(\lambda)(f) \end{aligned} \tag{3}$$

Let us prove by induction on the degree of λ in ∂_i that if $\lambda \in D_\zeta$ then $\lambda \in Q_\zeta^\perp$.

If λ is of degree 0, then it is up to a scalar, the evaluation at ζ. So for any $\lambda \in E$, $f \in Q_\zeta$ and $g \in R$ such that $g(\zeta) \neq 0$ and $f\,g \in I$, $\lambda(f\,g) = 0 = f(\zeta)g(\zeta)$ implies $f(\zeta) = 0$. This means that $\lambda \in Q_\zeta^\perp$.

Let us assume now that any element of D_ζ of degree $< d$ is in $Q_\zeta^\perp$. According to the formula (3), for any $\lambda \in E$, $f \in Q_\zeta$ and $g \in R$ such that $g(\zeta) \neq 0$ and $f\,g \in I$, we have

$$\begin{aligned} \lambda(f\,g) = 0 &= \lambda(f)g(\zeta) + (g - g(\zeta))(\zeta_1 + d_{\partial_1}, \ldots, \zeta_n + d_{\partial_n})(\lambda)(f) \\ &= \lambda(f)g(\zeta) + \rho(f) \end{aligned}$$

As $\rho = (g - g(\zeta))(\zeta_1 + d_{\partial_1}, \ldots, \zeta_n + d_{\partial_n})(\lambda)$ is of degree less than d in ∂_i and in D_ζ (stable by derivation), we also have $\rho(f) = 0$ by induction. This proves that $\lambda(f) = 0$ and $\lambda \in Q_\zeta^\perp$.

Consequently, we have shown that $D_\zeta = Q_\zeta^\perp$ and $D_\zeta^\perp = Q_\zeta$. □

We can sum up this theorem as follows: *If we want to compute the $\mathbf{m}_\zeta$-primary component Q_ζ of I, it is enough to search in $\mathbb{K}[\partial_\zeta]$ the orthogonal D_ζ of I.* We connect now the maximal degree of the polynomials which appears in D_ζ with an intrinsic parameter of Q_ζ, as follows:

Lemma 3.3 — *The maximal degree of the elements of $I^\perp \cap \mathbb{K}[\partial_\zeta]$ is the nil-index of B_ζ, (ie. the maximal $N \in \mathbb{N}$ such that $\mathbf{m}_\zeta^N \not\subset Q_\zeta$).*

Proof. Let call M the maximal degree of the elements of $I^\perp \cap \mathbb{K}[\partial_\zeta]$. For all monomial $m \in \mathbf{m}_\zeta^{M+1}$ (in $(x_i - \zeta_i)$) and all $\lambda \in D$, we have $\lambda(m) = 0$ because λ is of degree $\leq M$. Therefore $\mathbf{m}_\zeta^{M+1} \subset D_\zeta^\perp = Q_\zeta$.

Conversely, let λ be an element of $I^\perp \cap \mathbb{K}[\partial_\zeta]$ of degree M. Then there exists a monomial $m \in R$ of degree M, such that $\lambda(m) \neq 0$. Consequently, $\overline{m} \neq 0$ in B_ζ and $\mathbf{m}_\zeta^M \not\subset Q_\zeta$. This two facts implies that M is the nil-index of B_ζ. □

Remark 3.4 *As consequence, we can find a basis of B_ζ among the monomials of degree $\leq N$ where N is the maximal degree of the elements of D_ζ, the monomials of bigger degree being in the ideal Q_ζ.*

3.2 Inverse systems and quotient rings

In this section, we explain how we can recover the structure of $B_\zeta R/Q_\zeta$, when we know $D_\zeta = Q_\zeta^\perp$.

Definitions 3.5 — *We denote by B_ζ the quotient R/Q_ζ of R by the $\mathbf{m}_\zeta$-primary component of I. Its dimension is denoted by μ. For simplicity, we set $D = D_\zeta = I^\perp \cap \mathbb{K}[\partial_\zeta]$.*

Let $\mathbb{K}[\mathbf{x}]_{\leq d}$ (resp. $\mathbb{K}[\partial_\zeta]_{\leq d}$) be the vector space of $\mathbb{K}[\mathbf{x}]$ (resp. $\mathbb{K}[\partial_\zeta]$) generated by the monomials of degree $\leq d$.

Let $D_d = D \cap \mathbb{K}[\partial_\zeta]_{\leq d}$ be the set of elements of D of degree $\leq d$.

Note that D_d is a vector space of finite dimension $\leq \mu = \dim_{\mathbb{K}}(D_\zeta) = \dim_{\mathbb{K}}(B_\zeta)$, where μ is the multiplicity of ζ in $V(I)$. The multiplicity μ can be bounded by d^n where d is maximum of the degrees of the polynomials p_i. We assume that this multiplicity is more than 1, ie. that the elements of I vanish at the point ζ. In practice, the point ζ will often be the origin (by translation).

Let $\beta_1, \ldots, \beta_\mu$ be a basis of D such that we have $D_d = \langle \beta_1, \ldots, \beta_{s_d} \rangle$ where $s_0 = 1 < s_1 < \cdots < s_\nu = \mu$. As for any $i \in [1, \mu], k \in [1, n]$ we have $d_{\partial_k}(\beta_i) \in \langle \beta_1, \ldots, \beta_{i-1} \rangle$,

$$d_{\partial_k}(\beta_i) = \sum_{j=1}^{\mu} \lambda_{i,j}^k \beta_j.$$

with $\lambda_{i,j}^k = 0$ for $j \geq i$. Therefore, the matrix $M_k = (\lambda_{i,j}^k)_{1 \leq i,j \leq \mu}$ is an upper-triangular matrix.

Theorem 3.6 — *The upper-triangular matrices M_k are the matrices of multiplication by $x_k - \zeta_k$ in the dual basis of (β_i) in B_ζ.*

Proof. Let $b_1, \ldots, b_\mu$ be the dual basis of $\beta_1, \ldots, \beta_\mu$ in B_ζ: $\beta_i(b_j) = \kappa_{i,j}$ where $\kappa_{i,j}$ is the Kronecker symbol. The coefficient of indices i, j of the matrix of multiplication by $(x_k - \zeta_k)$ in the basis (b_j) is given by

$$\begin{aligned} \beta_i((x_k - \zeta_k)\, b_j) &= ((x_k - \zeta_k) \cdot \beta_i)(b_j) \\ &= d_{\partial_k}(\beta_i)(b_j) = \sum_{l=1}^{\mu} \lambda_{i,l}^k \beta_l(b_j) = \lambda_{i,j}^k \end{aligned}$$

which proves that the matrix M_k is the matrix of multiplication by $x_k - \zeta_k$. □
The quotient B_ζ is completely described by these matrices of multiplication. *Their storage requires $\frac{1}{2}\, n\, \mu\, (\mu - 1)$ spaces for the coefficients $\lambda_{i,j}^k$ which may not be zero.* It is worth noting that though we do not know really the dual basis b_i, we have all the information to be able to compute in B_ζ: any polynomial $p \in R$ has a representative in B_ζ, whose coordinates in $(b_i)_{1 \leq i \leq \mu}$ are $[\beta_1(p), \ldots, \beta_\mu(p)]$. Equality to 0 in B_ζ is tested with the evaluations (β_i).

Nevertheless, there is an explicit way to establish a correspondence between B_ζ and D_ζ. Assume that the nil-index of B_ζ is N and let

$$\Delta_N = \sum_{|\mathbf{a}|\leq N} \mathbf{x}_\zeta^{\mathbf{a}} \otimes \mathbf{d}^{\mathbf{a}} \in \mathbb{K}[\mathbf{x}, \partial_\zeta]$$

where $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n, |\mathbf{a}| = \sum_{i=1}^n a_i, \mathbf{x}_\zeta^{\mathbf{a}} = \prod_{i=1}^n (x_i - \zeta_i)^{a_i}$. This operator, called the *diagonal operator*, has the property:

$$\begin{array}{l} \forall p \in \mathbb{K}[\mathbf{x}]_{\leq N}, \quad \Delta_N(p) = \sum_{|\mathbf{a}|\leq N} \mathbf{x}_\zeta^{\mathbf{a}}\, \mathbf{d}^{\mathbf{a}}(p) = p, \\ \forall \beta \in \mathbb{K}[\partial_\zeta]_{\leq N}, \quad \beta(\Delta_N) = \sum_{|\mathbf{a}|\leq N} \beta(\mathbf{x}_\zeta^{\mathbf{a}})\, \mathbf{d}^{\mathbf{a}} = \beta. \end{array}$$

Proposition 3.7 — *Let $>$ be a monomial order and (β_i) a basis of D_ζ such that*

$$\beta_i = \mathbf{d}^{\mathbf{a}_i} - \sum_{\mathbf{b}>\mathbf{a}_\mu, |\mathbf{b}|\leq N} \gamma_{i,\mathbf{b}}\, \mathbf{d}^{\mathbf{b}} \tag{4}$$

and $\mathbf{x}^{\mathbf{a}_1} = 1 < \mathbf{x}^{\mathbf{a}_2} < \cdots < \mathbf{x}^{\mathbf{a}_\mu}$. Let us denote by $g_{\mathbf{b}} = \mathbf{x}^{\mathbf{b}} + \sum_{i=1}^\mu \gamma_{i,\mathbf{b}}\, \mathbf{x}^{\mathbf{a}_i}$ for $\mathbf{b} \neq \mathbf{x}^{\mathbf{a}_i}$ and $|\mathbf{b}| \leq N$. Then $(g_{\mathbf{b}}) \cup (\mathbf{x}^{\mathbf{c}})_{|\mathbf{c}|=N+1}$ is a Gröbner basis of the ideal Q_ζ for the order $>$.

Proof. The monomials of $g_{\mathbf{b}}$ are such that $\mathbf{x}^{\mathbf{b}} > \mathbf{x}^{\mathbf{a}_i}$ and the leading term of $g_{\mathbf{b}}$ is $\mathbf{x}^{\mathbf{b}}$. The set of monomials $\{\mathbf{x}^{\mathbf{a}_1}, \mathbf{x}^{\mathbf{a}_2}, \ldots, \mathbf{x}^{\mathbf{a}_\mu}\}$ is stable by derivation, for the vector space $\langle \beta_i \rangle$ is stable by derivation. Thus the monomials $(\mathbf{x}_{\mathbf{a}_i})$ are *under a staircase*. Rewrite Δ_N (with the relations $\mathbf{x}^{\mathbf{a}_i} = \beta_i + \sum_{i=1}^\mu \gamma_{i,\mathbf{b}}\, \mathbf{x}^{\mathbf{a}_i}$) in the form

$$\Delta_N = \sum_{i=1}^\mu \mathbf{x}^{\mathbf{a}_i} \otimes \beta_i + \sum_{\mathbf{b}\neq\mathbf{x}^{\mathbf{a}_i}, |\mathbf{b}|\leq N} g_{\mathbf{b}} \otimes \mathbf{d}^{\mathbf{b}},$$

where $(\mathbf{x}^{\mathbf{a}_i}, g_{\mathbf{b}})$ is a linearly independent family which spans $\mathbb{K}[\mathbf{x}]_{\leq N}$.

Let first prove that $g_{\mathbf{b}} \in I$. As $\beta_i(\Delta_N) = \beta_i$, we have $\beta_i(g_{\mathbf{b}}) = 0$ and $g_{\mathbf{b}} \in Q_\zeta$. Moreover by definition of the nil-index, Q_ζ also contains $(\mathbf{x}^{\mathbf{c}})_{|\mathbf{c}|=N+1}$, and $B_\zeta = R/Q_\zeta$ is generated by $(\mathbf{x}^{\mathbf{a}_i})_{1\leq i\leq\mu}$. This family has $\mu = \dim_{\mathbb{K}}(B_\zeta)$ elements and therefore, it is a basis of B_ζ. On the other side, for any $p \in Q_\zeta \cap \mathbb{K}[\mathbf{x}]_{\leq N}$, we have $\beta_i(p) = 0$ and

$$\Delta_N(p) = p \in \langle g_{\mathbf{b}} \rangle_{\mathbf{b}\neq\mathbf{a}_i},$$

so that $Q_\zeta \cap \mathbb{K}[\mathbf{x}]_{\leq N} \subset \langle g_b \rangle_{\mathbf{b}\neq\mathbf{a}_i}$. This proves that Q_ζ is generated by $(g_{\mathbf{b}}) \cup (\mathbf{x}^{\mathbf{c}})_{|\mathbf{c}|=N+1}$.

As all monomials of degree less than N appear either in $(\mathbf{x}^{\mathbf{a}_i})$, or as the leading term $\mathbf{x}^{\mathbf{b}}$ of $g_{\mathbf{b}}$, we can reduce any polynomial modulo $(g_{\mathbf{b}}) \cup (\mathbf{x}^{\mathbf{c}})_{|\mathbf{c}|=N+1}$ (according to the order $>$) to a linear combination of the monomials $(\mathbf{x}^{\mathbf{a}_i})$. Therefore, as this set of monomials is a basis of the quotient $B_\zeta = R/Q_\zeta$, the reduction is canonical and the polynomials $(g_{\mathbf{b}}) \cup (\mathbf{x}^{\mathbf{c}})_{|\mathbf{c}|=N+1}$ are a Gröbner basis of the ideal Q_ζ. □

For other applications of this diagonal operator, we mention [20].

4 Construction of the local inverse system

Now, we describe an algorithm to compute $D = D_\zeta = I^\perp \cap \mathbb{K}[\partial]$. The cornerstone of this algorithm is the following remark. The space D_d is stable by derivation and for any $1 \leq i \leq n$, $d_{\partial_i}(D_d) \subset D_{d-1}$. Therefore, if we want to compute D_d, we have *of integrating the elements of D_{d-1}, and keep those which are orthogonal to the elements of I.* The first space D_0 being generated by ∂_ζ^0, we will construct by induction the spaces D_d. Each step of the algorithm will consist roughly to integrate the previous elements and the algorithm will stop when a generating set of the dual $\hat{B}$ is obtained.

4.1 Integrating differential operators

We consider here an ideal I of R, $D = I^\perp \in \mathbb{K}[\partial]$ the inverse system at ζ and $D_d = D \cap \mathbb{K}[\partial]_d$. We give a way to construct D_{d+1} when we know D_d.

Definitions 4.1 — *For any polynomial $p \in \mathbb{K}[\partial]$, we denote by $\int_i p$ the polynomial $q \in \mathbb{K}[\partial]$ such that $d_{\partial_i} q = p$ and $q(\partial_1, \ldots, \partial_{i-1}, 0, \partial_{i+1}, \ldots, \partial_n) = 0$ (a primitive with no constant term). For any polynomial $p \in \mathbb{K}[\partial]$, let $p_{|\partial_i=0}$ denotes $p(\partial_1, \ldots, \partial_{i-1}, 0, \partial_{i+1}, \ldots, \partial_n)$.*

Theorem 4.2 — *Assume that I is generated by $p_1, \ldots, p_m$ and that $d > 1$. Let $\beta_1, \ldots, \beta_s$ be a basis of D_{d-1}. Then the elements of D_d with no constant terms (in (∂_i)) are the elements Λ of the form*

$$\Lambda = \sum_{j=1}^{s} \lambda_j^1 \int_1 \beta_j|_{\partial_2=0,\ldots,\partial_n=0} + \sum_{j=1}^{s} \lambda_j^2 \int_2 \beta_j|_{\partial_3=0,\ldots,\partial_n=0} + \cdots + \sum_{j=1}^{s} \lambda_j^n \int_n \beta_j \quad (5)$$

such that

1. $\sum_{j=1}^{s} \lambda_j^k d_{\partial_l}\beta_j - \sum_{j=1}^{s} \lambda_j^l d_{\partial_k}\beta_j = 0$ *for* $1 \leq k < l \leq n$,

2. $\Lambda(p_i) = 0$ *for* $1 \leq i \leq m$.

Proof. Let $\Lambda \in D_d$ with no constant terms. It can be decomposed uniquely as

$$\Lambda = \Lambda_1(\partial_1, \ldots, \partial_n) + \Lambda_2(\partial_2, \ldots, \partial_n) + \cdots + \Lambda_n(\partial_n),$$

with $\Lambda_i \in \mathbb{K}[\partial_i, \ldots, \partial_n] \backslash \mathbb{K}[\partial_{i+1}, \ldots, \partial_n]$. This implies that $\int_i d_{\partial_i}(\Lambda_i) = \Lambda_i$. Then $d_{\partial_1}(\Lambda) = d_{\partial_1}(\Lambda_1) \in D_{d-1} = \langle \beta_1, \ldots, \beta_s \rangle$ and

$$\Lambda_1 = \sum_{j=1}^{s} \lambda_j^1 \int_1 \beta_j$$

for some $\lambda_j^1 \in \mathbb{K}$.

Consider now $d_{\partial_2}(\Lambda) = d_{\partial_2}(\Lambda_1) + d_{\partial_2}(\Lambda_2)$ which also belongs to $\langle \beta_1, \ldots, \beta_s \rangle$. Therefore,

$$\Lambda_2 = \int_2 d_{\partial_2}\Lambda_2 = \sum_{j=1}^{s} \lambda_j^2 \int_2 \beta_j - \int_2 d_{\partial_2}\Lambda_1 = \sum_{j=1}^{s} \lambda_j^2 \int_2 \beta_j - (\Lambda_1 - \Lambda_1|_{\partial_2=0}),$$

for some $\lambda_j^2 \in \mathbb{K}$ ($\int_2 d_{\partial_2}(\Lambda_1)$ is equal to the part of Λ_1 which depends on ∂_2) and we have

$$\Lambda_1 + \Lambda_2 = \sum_{j=1}^{s} \lambda_j^1 \int_1 \beta_j|_{\partial_2=0} + \sum_{j=1}^{s} \lambda_j^2 \int_2 \beta_j$$

Let us call $\Lambda_1 + \Lambda_2 = \sigma_2$. Applying the same computation to $d_{\partial_3}(\Lambda)$ yields

$$\Lambda_3 = \sum_{j=1}^{s} \lambda_j^3 \int_3 \beta_j - (\sigma_2 - \sigma_2|_{\partial_3=0})$$

and

$$\Lambda_1 + \Lambda_2 + \Lambda_3 = \sum_{j=1}^{s} \lambda_j^1 \int_1 \beta_j|_{\partial_2=0,\partial_3=0} + \sum_{j=1}^{s} \lambda_j^2 \int_2 \beta_j|_{\partial_3=0} + \sum_{j=1}^{s} \lambda_j^3 \int_3 \beta_j$$

Iterating this procedure, we obtain the formula (5) and for any $k, l \in \mathbb{N}$, we have

$$\sigma_k = \Lambda_1 + \cdots + \Lambda_k = \sum_{j=1}^{s} \lambda_j^1 \int_1 \beta_j|_{\partial_2=0,\ldots,\partial_k=0}$$

$$+ \sum_{j=1}^{s} \lambda_j^2 \int_2 \beta_j|_{\partial_3=0,\ldots,\partial_k=0} + \cdots + \sum_{j=1}^{s} \lambda_j^k \int_k \beta_j \tag{6}$$

and

$$\Lambda_l = \sum_{j=1}^{s} \lambda_j^l \int_l \beta_j - (\sigma_{l-1} - \sigma_{l-1}|_{\partial_l=0}) \tag{7}$$

This proves that Λ is *necessarily* of the form (3). Let us show now that we also have necessarily the relations 1 and 2. Up to now, we have not used the fact that $d_{\partial_k}\Lambda_l = 0$ for $k < l$. According to (7), $d_{\partial_l}\Lambda_k = 0$ implies that

$$\sum_{j=1}^{s} \lambda_j^l \int_l d_{\partial_k}\beta_j = d_{\partial_k}(\sigma_{l-1} - \sigma_{l-1}|_{\partial_l=0})$$

As both side of this equality have no constant terms in ∂_l, we obtain an equivalent relation by considering their derivative with respect to d_{∂_l}. As $d_{\partial_k}(\sigma_{l-1}) = d_{\partial_k}(\sigma_k)$ (for $k < l$) and according to (6), $d_{\partial_k}(\sigma_k) = \sum_{j=1}^{s} \lambda_j^k \beta_j$, so that we obtain a relation of the form

$$\sum_{j=1}^{s} \lambda_j^l d_{\partial_k}\beta_j - \sum_{j=1}^{s} \lambda_j^k d_{\partial_l}\beta_j = 0$$

which proves the point 1 of the theorem. The point 2 is a consequence of the fact that $\Lambda \in I^\perp$.

Conversely, let us prove that an element Λ of the form (5) which satisfies the conditions 1, 2 is in D_d. It can be decomposed as $\Lambda = \Lambda_1 + \cdots + \Lambda_n$, with $\Lambda_k = \sum_{j=1}^{s} \lambda_j^k \int_k \beta_j - (\sigma_{k-1} - \sigma_{k-1}|_{\partial_k=0})$ and $\sigma_k = \Lambda_1 + \cdots + \Lambda_k$. This implies by induction, the relation (6). As Λ satisfies the point 1 and according to the previous computation, we have $d_{\partial_k}(\Lambda_l) = 0$ for $k < l$ and $\Lambda_l \in \mathbb{K}[\partial_l, \ldots, \partial_n]$. Moreover, Λ_l has no constant term in ∂_l and it belongs to $\mathbb{K}[\partial_l, \ldots, \partial_n] \backslash \mathbb{K}[\partial_{l+1}, \ldots, \partial_n]$. According to (6), we have

$$d_{\partial_k}\Lambda = \sum_{j=1}^{s} \lambda_j^k \beta_j \in D_{d-1}. \tag{8}$$

Therefore, as the multiplication by $x_i - \zeta_i$ corresponds to the derivation with respect to ∂_i and as D_{d-1} is stable by derivation, the relation (8) implies that $\Lambda \in (\mathbf{m}_\zeta \langle p_1, \ldots, p_m \rangle)^\perp$. According to the point 2, we also have $\Lambda(p_k) = 0$ (for $1 \leq k \leq m$). Consequently, $\Lambda(p) = 0$ for all $p \in \langle p_1, \ldots, p_m \rangle + \mathbf{m}_\zeta \langle p_1, \ldots, p_m \rangle = I$, thus $\Lambda \in I^\perp$. $\square$ The condition 1 of this theorem can be replaced by the relation:

1'. $d_{\partial_l}(\Lambda) \in D_{d-1}$ for $1 \leq l \leq n$.

The two conditions 1' and 2 implies that $\Lambda \in I^\perp$ as we have just seen and formula (5) is a necessary form for $\Lambda \in I^\perp$. By this way, we can save some computations, for if some of the primitives are already in D_{d-1}, they will be subtracted directly from Λ.

4.2 Example

Before going into the details of the algorithm, we illustrate the method on a simple example, that we treat "by hand". Consider the isolated singular point $0 \in \mathbb{K}^2$ of the system

$$p_1 = 2\,x_1\,x_2^2 + 5\,x_1^4,\ p_2 = 2\,{x_1}^2\,x_2 + 5\,x_2^4.$$

For any $i, j \in \mathbb{N}$, let $\mathbf{d}_i^j = \frac{1}{j!}\partial_i^j$. We easily check that $I^\perp$ contains $1, \mathbf{d}_1, \mathbf{d}_2$, $\mathbf{d}_1^2, \mathbf{d}_1\mathbf{d}_2, \mathbf{d}_2^2, \mathbf{d}_1^3,\ \mathbf{d}_2^3$. In order to find a new element in $I^\perp$, we integrate the previous elements, according to the formula (5) and keep those which introduce new terms:

$$\Lambda = \lambda_1\,\mathbf{d}_1^4 + \lambda_2\,\mathbf{d}_1^2\mathbf{d}_2 + \lambda_3\,\mathbf{d}_1\mathbf{d}_2^2 + \lambda_4\,\mathbf{d}_2^4.$$

As we must have $\Lambda(p_1) = \Lambda(p_2) = 0$, we see that Λ is of the form $\Lambda = \lambda_1(2\,\mathbf{d}_1^4 - 5\,\mathbf{d}_1\mathbf{d}_2^2) + \lambda_2(2\,\mathbf{d}_1^4 - 5\,\mathbf{d}_1^2\mathbf{d}_2)$. A new element in $I^\perp$, will be of the form $\Lambda = \lambda_1\mathbf{d}_1^5 + \lambda_2(2\,\mathbf{d}_1^4\mathbf{d}_2 - 5\,\mathbf{d}_1\mathbf{d}_2^3) + \lambda_3(2\,\mathbf{d}_1^2\mathbf{d}_2^2 - 5\,\mathbf{d}_2^5)$ and must satisfies the points 1', 2. Therefore, we have

$$\Lambda = \lambda\,(5\,\mathbf{d}_1^2\mathbf{d}_2^2 - 2\,\mathbf{d}_1^5 - 2\,\mathbf{d}_2^5).$$

A new integration yields no new element satisfying the condition 1 and 2, so that $I^\perp$ is generated by

$$1, \mathbf{d}_1, \mathbf{d}_2, \mathbf{d}_1^2, \mathbf{d}_1\mathbf{d}_2, \mathbf{d}_2^2, \mathbf{d}_1^3, \mathbf{d}_2^3,$$
$$2\,\mathbf{d}_1^4 - 5\,\mathbf{d}_1\mathbf{d}_2^2, 2\,\mathbf{d}_2^4 - 5\,\mathbf{d}_1^2\mathbf{d}_2, 5\,\mathbf{d}_1^2\mathbf{d}_2^2 - 2\,\mathbf{d}_1^5 - 2\,\mathbf{d}_2^5$$

and 0 is of multiplicity 11.

4.3 An algorithm

Theorem (4.2) tells us that if we know D_{d-1}, we can construct the elements of D_d by solving a linear system in the $n \times \mu$ unknowns λ_j^i. We know $D_0 = \langle \partial_\zeta^0 \rangle$,

so that we can construct step by step each D_d from the previous D_{d-1}, up to the situation where no knew element is found and where D has be computed. This yields the following algorithm:

Input : $(p_1, \ldots, p_m) \in R^m$ and $\zeta \in \mathbb{K}^n$ such that $I = (p_1, \ldots, p_m)$ has an $\mathbf{m}_\zeta$-primary component Q_ζ.
Output : A basis of $Q_\zeta^\perp$ in $\mathbb{K}[\partial]$ and the matrix of multiplication by $x_k - \zeta_k$ in B_ζ.

▷ $D_0 := 1$; d := 0; s_0 := 1; test := true;
For k from 1 to n do
$U_k[1] := [0]$;
$A_k[1] := [\partial_k(p_1), \ldots, \partial_k(p_m)]$;
▷ while test do
1) S := system of equations 1, 2 in λ_j^k;
2) solve the system S;
3) if no new solution then test:= false
else
let $(\delta_1, \ldots, \delta_s)$ be a basis of the new solutions such that $d_{\partial_k}(\delta_i) = \sum_{j=1}^{s_d} \lambda_{j,s_d+i}\, \beta_j$;
$s_{d+1} := s_d + s$;
$D_{d+1} := D_d, \delta_1, \ldots, \delta_s = \beta_1, \ldots, \beta_{s_{d+1}}$;
for i from $s_d + 1$ to s_{d+1} do
for k from 1 to n do
$U_k[i] := [\lambda_{1,i}, \ldots, \lambda_{s_d,i}]$;
$A_k[i] := [\int_k \beta_i|_{\partial_{k+1}=\cdots=\partial_n=0}(p_1), \ldots, \int_k \beta_i|_{\partial_{k+1}=\cdots=\partial_n=0}(p_m)]$;
$d := d + 1$;
▷ return D_d and U_k for $1 \leq k \leq n$;

The vector $U_k[i]$ (resp. $A_k[i]$) represents the i$^{\text{th}}$ column of the matrix U_k (resp. A_k).

Let us now analyze in detail the complexity of this algorithm. We assume that we are at the step d of the algorithm and that $\beta_1, \ldots, \beta_{s_d}$ is the computed basis of D_d. The matrices $U_k = (u_{i,j}^k)_{1 \leq i,j \leq s_d}$ correspond to the derivation by d_{∂_k}:

$$d_{\partial_k}(\beta_j) = \sum_{i=1}^{s_d} u_{i,j}^k\, \beta_i.$$

As we have seen, these matrices are upper-triangular: $u^k_{i,j} = 0$ for $s_{l-1}+1 \leq j \leq s_l$, $i > s_{l-1}$. The matrices A_k are $m \times s_d$ matrices

$$(\int_k \beta_j|_{\partial_{k+1}=\cdots=\partial_n=0}(p_i))_{1\leq i\leq m, 1\leq j\leq s_d}.$$

4.4 Complexity

We assume here that the coefficients of these matrices have a size bounded by T_d.

Step 1: Let $v_l = (\lambda^l_1, \ldots, \lambda^l_{s_d})$ be n vectors of size s_d and $V = [v_1, \ldots, v_n]$. The equations 1 can be rewritten as

$$U_k\, v_l - U_l\, v_k = 0,\ 1 \leq k < l \leq n.$$

The equations 2 can be rewritten as

$$[A_1, \ldots, A_n].\, V = 0$$

Therefore, the system S obtained from the equations 1, 2 has the form

$$\begin{bmatrix}
U_n & & & & -U_1 \\
& U_n & & & -U_2 \\
& & \ddots & & \vdots \\
& & & U_n & -U_{n-1} \\
U_{n-1} & & & -U_1 & \\
& \ddots & & \vdots & \\
& & U_{n-1} & -U_{n-2} & \\
\vdots & \vdots & \vdots & & \\
U_2 & -U_1 & & & \\
A_1 & \cdots & \cdots & \cdots & A_n
\end{bmatrix} .\, V = 0$$

where the empty spaces correspond to zero coefficients. This matrix is of size $(\frac{1}{2}\, n\, (n-1)\, s_d + m) \times n\, s_d$.

Step 2: Assume that the vector spaces spanned by the rows of U_i are subspaces of the space spanned by the rows of U_n. We can always recover such a situation by replacing the matrices U_n (resp. the variable x_n) by a

good linear combination of the matrices $U_1, \ldots, U_n$ (resp. the variables $x_1, \ldots, x_n$).

By Gaussian elimination, we can put U_n and the matrix

$$\begin{bmatrix} U_n & & & -U_1 \\ & U_n & & -U_2 \\ & & \ddots & \vdots \\ & & U_n & -U_{n-1} \end{bmatrix} \tag{9}$$

in a row echelon shape. Then we can reduce the rows $U_{n-1}\, v_1 - U_1\, v_{n-1} = 0$ by the rows of the matrix (9). We obtain a system of the form $W_{1,n-1}\, v_n = 0$, where $W_{1,n-1}$ is a matrix of size $s_d \times s_d$. At each step of the loop, we add $s_d - s_{d-1}$ new columns to each matrix U_k. Therefore, we may assume by induction that pivoting and reduction has already been done for the s_{d-1} columns of the matrices U_k. Thus, putting the matrix (9) in a triangular form requires at most $\mathcal{O}(n\, s_d^d\, (s_d - s_{d-1}))$ new arithmetic operations and the reduction of the last $s_d - s_{d-1}$ columns of the system $U_{n-1}\, v_1 - U_1\, v_{n-1} = 0$ requires at most $\mathcal{O}(s_{d-1}^2 (s_d - s_{d-1}))$ new arithmetic operations. We apply the same computations the $\frac{1}{2}\,(n-1)\,(n-2) + m$ other non-zero blocks of the matrix and we obtain a system of the form

$$\begin{bmatrix} U_n & & & & -U_1 \\ & U_n & & & -U_2 \\ & & \ddots & & \vdots \\ & & & U_n & -U_{n-1} \\ & & & & W_{1,n-1} \\ & & & & \vdots \\ & & & & W_{1,2} \\ A'_1 & \cdots & \cdots & \cdots & A'_n \end{bmatrix} . V = 0$$

where the matrix $[A'_1, \ldots, A'_n]$ has a row-echelon shape and A'_i is reduced with respect to U_n.

As only the last $s_d - s_{d-1}$ columns of these matrix are not treated (by induction), the number of new arithmetic operations needed to obtain this matrix is therefore bounded by

$$\mathcal{O}((n^2 + m) \times s_d^2 \times (s_d - s_{d-1})). \tag{10}$$

Let W' be the submatrix of A'_n, whose corresponding rows in A'_i ($i = 1 \ldots n-1$) are zero and let

$$W = \begin{bmatrix} W_{1,n-1} \\ \vdots \\ W_{1,2} \\ W' \end{bmatrix}.$$

The number of rows of this matrix is bounded by $\frac{1}{2}(n-1)(n-2)\, s_d, +m$. The number of columns is s_d.

To obtain the new solutions of this system, we will first solve the system $W \,.\, v_n = 0$ and then report the solution in v_i ($i = 1 \ldots n-1$).

We need at most

$$\mathcal{O}((n^2\, s_d + m) \times s_d\,(s_d - s_{d-1})) \tag{11}$$

new arithmetic operations, to compute a triangular basis of the solutions of $W \,.\, v_n = 0$. The new solutions are those, for which the coefficients of indices $s_{d-1}+1, \ldots, s_d$ not all zero. Reporting the solutions in order to get v_i ($i = 1 \ldots n-1$) requires

$$\mathcal{O}(n\, s_d^2) \tag{12}$$

further operations.

As these solutions can be obtained as fractions of two determinants of size $2\, s_d$ of the matrix S, the size of their coefficients is bounded by

$$2\, s_d\, T_d + s_d \log(2\, s_d) \tag{13}$$

according to Hadamard's inequality.

Step 3: This step consists to add $s_{d+1} - s_d$ columns corresponding to the new solutions v_k (found in step 2), to each matrix U_k and to add $s_{d+1} - s_d$ new columns to the matrices A_k, corresponding to the evaluations $\int_k \beta_j|_{\partial_{k+1}=\cdots=\partial_n=0}(p_i)$. The number of new arithmetic operations, is therefore bounded by

$$n\, m\, (s_{d+1} - s_d)\, C \tag{14}$$

where C is a bound for computing $\int_k \beta_j|_{\partial_{k+1}=\cdots=\partial_n=0}(p_i)$.

Let us analyze more precisely the cost for computing these coefficients. Let us first note that

$$\forall \Lambda \in \mathbb{K}[[\partial_1, \ldots, \partial_k]],\ \forall p \in \mathbb{K}[\mathbf{x}],\ \Lambda(p) = \Lambda(p(x_1, \ldots, x_k, 0, \ldots, 0))$$
$$\forall \Lambda \in \mathbb{K}[[\partial]],\ \forall p \in \mathbb{K}[x_1, \ldots, x_k],\ \Lambda(p) = \Lambda(\partial_1, \ldots, \partial_k, 0, \ldots, 0)(p)$$

so that

$$\int_k \beta_j|_{\partial_{k+1}=\cdots=\partial_n=0}(p_i) = (\int_k \beta_j)(p_i(x_1, \ldots, x_k, 0, \ldots, 0)).$$

The integration $\int_i$ of monomials in ∂ corresponds to a multiplication by ∂_i up to a scalar depending on these monomials. Thus according to the remark (2.4), for $j = 1 \ldots s_d$ and $p \in \mathbb{K}[\mathbf{x}]$,

$$\int_k \beta_j|_{\partial_{k+1}=\cdots=\partial_n=0}(p) = \beta_j(\delta_k(p))$$

where δ_k is a linear operator on $\mathbb{K}[\mathbf{x}]$ and where $\delta_k(p)$ is a linear combination of the derivatives (with respect to x_k) of some monomials in p. Note that $\delta_i \circ \delta_j = 0$ if $i > j$.

The linear forms β_i are obtained themselves by iterated integration of $\beta_0 = \partial^0$, for they also satisfy the conditions 1, 2 of theorem (4.2). Therefore, each linear form β_j can be represented by

$$\beta_j = \partial^0 \left(\sum_{\mathbf{b} \in \mathbb{N}^n} \gamma_{\mathbf{b}}\, \delta^{\mathbf{b}} \right)$$

where $\delta^{(b_1,\ldots,b_n)} = \delta_1^{b_1} \circ \cdots \circ \delta_n^{b_n}$. Let us denote by $p_{j,k}$ the polynomial $\left(\sum_{\mathbf{b} \in \mathbb{N}^n} \gamma_{\mathbf{b}}\, \delta^{\mathbf{b}}\right)(p_k)$ so that $\beta_j(p_k) = \partial^0(p_{j,k}) = p_{j,k}(0)$. This polynomial $p_{j,k}$ is of the form

$$\sum_{\mathbf{b} \in \mathcal{M}} \gamma_{\mathbf{b},j,k}\, \frac{1}{\mathbf{b}!} \mathbf{x}^{\mathbf{b}}$$

where $\mathcal{M}$ is the set of all monomials obtained by derivations of the monomials of (p_k). Let L be the number of elements of $\mathcal{M}$.

According to theorem (4.2) and to the previous remarks, the new elements $p_{l,k}$ $(l = s_d + 1, \ldots, s_{d+1})$ will be linear combinations of the $n\, s_d$ elements $\delta_j(p_{i,k})$ $(i = 1, \ldots, s_d,\ j = 1, \ldots, n)$ (which are linear

combinations of the L monomials $\mathbf{x}^{\mathbf{b}}$ ($\mathbf{b} \in \mathcal{M}$)). Therefore, the number of arithmetic operations requires to construct one polynomial $p_{j,k}$ ($j = s_d+1, \ldots, s_{d+1}$) is $\mathcal{O}(n\, s_d\, L)$ and the cost for constructing the new $p_{j,k}$ and the $n\,(s_{d+1} - s_d)$ new columns of $[A_1, \ldots, A_n]$ is bounded by

$$\mathcal{O}((s_{d+1} - s_d)\, s_d\, n^2\, m\, L). \tag{15}$$

where L is the number of monomials in $\mathcal{M}$.

We assume here that T_d is also a bound for the size of $\gamma_{\mathbf{b},j,k}$. Thus the coefficients of the new $p_{j,k}$ are obtained as L sums of products $\gamma_{\mathbf{b},j,k}\lambda_i^k$. According to (13), this size is bounded by

$$(2\, s_d + 1)T_d + s_d \log(2\, s_d) + \log(L) \tag{16}$$

Proposition 4.1 — *The total number of arithmetic operations during the algorithm is bounded by*

$$\mathcal{O}((n^2 + m)\, \mu^3 + n\, m\, \mu\, C)$$

where C is the maximal cost for computing $\int_k \beta_j|_{\partial_{k+1}=\cdots=\partial_n=0}(p_i)$. C can be bounded by $\mathcal{O}(n\, \mu\, L)$, where L is the number of monomials obtained by derivation of the monomials of (p_i).

Proof. Let ν be the number of loops in this algorithm. As $(s_1 - s_0) + \cdots + (s_\nu - s_{\nu-1}) = s_\nu - s_0 = \mu - 1$, the sum of the partial costs (10), (11), (12), (14) or (15), is bounded by

$$\mathcal{O}((n^2 + m)\, \mu^3 + n\, m\, \mu\, C)$$

or

$$\mathcal{O}((n^2 + m)\, \mu^3 + n^2\, m\, L\, \mu^2).$$

□ This complexity is not too bad, for the big component μ^3 also corresponds to a bound of the number of steps for pivoting a linear endomorphism in the vector space B_0 of dimension μ.

Proposition 4.2 — *The size of the coefficients of the matrices U_k and of the polynomials $p_{i,k}$ is bounded by*

$$\mathcal{O}(T\, (\frac{2}{e}\, \mu + \frac{1}{e})^{\mu+1})$$

where T is a bound for the size of the coefficients of p_k.

Proof. If T_d is a bound for the coefficients in U_k and A_k at the step d, according to (13), (16), the size of the coefficients at the step $d+1$ is bounded by

$$T_{d+1} = (2\,s_d + 1)\,T_d + s_d \log(2\,s_d) + \log(L)$$

Therefore $T_{d+1} + \log(\mu) + \log(L) \leq (2\,s_d + 1)\,(T_d + \log(\mu) + \log(L))$ and

$$T_\nu + \log(\mu) + \log(T) \leq \prod_{d=1}^{\nu} (2\,s_d + 1)\,(T + \log(\mu) + \log(L))$$

As $\prod_{d=1}^{\nu}(2\,s_d + 1) \leq \frac{(2\,\mu+1)!}{2^\mu\,\mu!}$, according to Stirling's formula, we have

$$T_\nu \leq \mathcal{O}((\frac{2\,\mu+1}{e})^{2\,\mu+1}(\frac{e}{2\,\mu})^\mu T) = \mathcal{O}(T\,(\frac{2\,\mu+1}{e})^{\mu+1})$$

□ This estimation is quite rough and in many cases, for instance in local complete intersection cases, this bound is too big.

If we compare with the method proposed in [18], what is called there a continuation, corresponds here to a primitive $\in D_d$ for which all derivations are in D_{d-1}. The method proposed in [18], consists first to construct the possible continuations following a monomial order and then to take linear combinations of these elements which are orthogonal to the polynomial p_k. The construction of continuations does not have the same complexity, according to the monomial order you chose (the best bound for a step similar to (2) is $\mathcal{O}(n^3\,\mu^3)$ (or for a general $\mathcal{O}(n^4\,\mu^3)$ monomial ordering). This steps has to be done μ times, so that a bound for the algorithm proposed in [18] is $\mathcal{O}((n^3 + m)\,\mu^4)$.

Our construction does need a monomial order. Thanks to theorem (4.2), we are able to describe completely the step of integration in term of a simple linear system, which grows at each step of the algorithm. Therefore, we obtain a better complexity of the type $\mathcal{O}((n^2 + m)\,\mu^3)$, (just like Gaussian elimination in B_ζ).

5 Applications

5.1 Local residue

We are going now to give some applications of inverse systems, the first one being the construction of local residues.

5.1.1 Gorenstein Algebra

In this section, we recall the fundamental properties of Gorenstein algebras, which are useful to define residues. We denote by $R \otimes_{\mathbb{K}} R$ the tensor product of two copies of R over $\mathbb{K}$. It is also the polynomial ring $\mathbb{K}[\mathbf{x}, \mathbf{y}]$ where $\mathbf{y} = (y_1, \ldots, y_n)$ is a new set of variables. We will identify $R \otimes_{\mathbb{K}} R$ with $Hom_{\mathbb{K}}(\hat{R}, R)$ via the following map. For any $T = \sum_{i=1}^{s} a_i \otimes b_i = \sum_{i=1}^{s} a_i(\mathbf{x}) b_i(\mathbf{y}) \in R \otimes R$ and for $\lambda \in \hat{R}$,

$$\lambda \mapsto T(\lambda) = \sum_{i=1}^{s} a_i \lambda(b_i) \in Hom_{\mathbb{K}}(\hat{R}, R).$$

Similarly, for any finitely generated $\mathbb{K}$-algebra A (whose dual is denoted by $\hat{A}$), any element of $A \otimes_{\mathbb{K}} A$ will be identified (in the same way) with an element of $Hom_{\mathbb{K}}(\hat{A}, A)$.

If we focus on the elements of $Hom_{\mathbb{K}}(\hat{A}, A)$, which are compatible with the multiplication by elements of A, that is the elements of $Hom_A(\hat{A}, A)$, we have the following result.

Theorem 5.1 — *Assume that A is a finite dimensional vector space. Then A is Gorenstein if and only if there exists a A-isomorphism Δ between $\hat{A}$ and A.*

See [14][p. 362, p. 357, ex. 3] and [21][p. 182,184] for more details.

If this holds, then the element $1 \in A$ has an inverse image τ that we call **the residue associated to** Δ. In [14][p. 352] it is called a trace but we prefer to called it a residue to avoid the confusion with the natural trace. For a more algorithmic approach of this subject, we mention [6] or [9]. This algebraic definition of residues leads to the same object as the analytical residue defined by integrals, in the case where $\mathbb{K} = \mathbb{C}$ (See [5] for instance). It shares the same formal properties but can be defined on any field. If we translate the previous result in the formalism of section (2), we have

Lemma 5.2 — *Let Q_ζ be a $\mathbf{m}_\zeta$-primary component of the ideal I such that $B_\zeta = R/Q_\zeta$ is Gorenstein. Then $Q_\zeta^\perp$ is generated by* **one** *polynomial $\tau(\partial)$ and all its derivatives with respect to ∂_i.*

In other words, in the case of a Gorenstein Algebra, the primary component Q_ζ is described by one polynomial (ie. a residue).

Assume here that A is of the form $A = R/I$ for some ideal I of R and that A is Gorenstein. Let Δ be an element of $R \otimes_{\mathbb{K}} R$ such that its class $\overline{\Delta}$ in $A \otimes A$ defines an isomorphism between $\hat{A}$ and A. Then the residue is characterized as follows:

Theorem 5.3 — *The residue $\tau \in \hat{R}$ of A associated to Δ is the unique linear form such that*

1. $\tau = 0$ *on* I,
2. $\Delta(\tau) - 1 \in I$.

The first point means that $\tau \in \hat{A}$ and the second that $\overline{\Delta}(\tau) = 1$ in A.

5.1.2 Complete intersection

We consider now the case where the ideal $I = (p_1, \ldots, p_n)$ of $\mathbb{K}[x_1, \ldots, x_n]$ with an $\mathbf{m}_\zeta$-component Q_ζ. Let $B_\zeta = R/Q_\zeta$ and assume that it is a $\mathbb{K}$-vector space of finite dimension, denoted by μ. In other words, $(p_1, \ldots, p_n)$ defines a locally complete intersection. Then there is an explicit way to construct an element $\Delta \in R \otimes R$ such that $\overline{\Delta}$ is an isomorphism between $\widehat{B_\zeta}$ and B_ζ.

Let $X_{(0)} = (x_1, \ldots, x_n)$, $X_{(1)} = (y_1, x_2 \ldots, x_n), \ldots$, $X_{(n)} = (y_1, \ldots, y_n)$, where $y_1, \ldots, y_n$ are new variables. For any $P \in R$, we denote by $\theta_i(P) = \frac{P(X_{(i)}) - P(X_{(i-1)})}{y_i - x_i}$, the discrete derivative. Take now the discrete Jacobian

$$\Delta = \begin{vmatrix} \theta_1(p_1) & \cdots & \theta_n(p_1) \\ \vdots & & \vdots \\ \theta_1(p_n) & \cdots & \theta_n(p_n) \end{vmatrix} \tag{17}$$

Then we have the following result:

Theorem 5.4 — *The element $\overline{\Delta}$ is a B_ζ-isomorphism between $\widehat{B_\zeta}$ and B_ζ.*

See [14], [21][p. 180]. In this case, we will say that the residue of B_ζ associated with Δ is the residue of $\mathbf{P} = (p_1, \ldots, p_n)$. We will denote it by $\tau_{\mathbf{P}}$ and will call it **the local residue of P at** ζ.

5.1.3 Construction of the residue

We have now all the ingredients to construct the local residue at a point $\zeta \in \mathbb{K}^n$. Let $I = (p_1, \ldots, p_n)$ and assume that B_ζ is of finite dimension $\mu > 0$.

Input : $\mathbf{P} = (p_1, \ldots, p_n) \in R^n$ defining a quasi-regular sequence and ζ such that $(\mathbf{P}) = I \subset \mathbf{m}_\zeta$.
Output : The residue $\tau_{\mathbf{P}}$ of $\mathbf{P}$ at ζ.

- ▷ Construct a basis $\beta_1, \ldots, \beta_\mu$ of $I^\perp \cap \mathbb{K}[\partial]$ with the algorithm (4.3).
- ▷ Solve the system
  $$\beta_j(\textstyle\sum_{l=1}^{\mu} \lambda_l \, \Delta(\beta_l) - 1) = 0 \;\; (1 \leq j \leq \mu)\,.$$
- ▷ The residue $\tau_{\mathbf{P}}$ is $\sum_{l=1}^{\mu} \lambda_l \, \beta_l$ where (λ_l) is the solution of the previous system.

This algorithm consists essentially, to solve a linear system of size μ, once we know a basis of D_ζ. Thus the number of steps in this part of the algorithm is bounded by $\mathcal{O}(\mu^3)$, which has to be added to the $\mathcal{O}(n^2\,\mu^3 + n^2 \mu\, C)$ steps for the construction of a basis of D_ζ. Moreover, we also need to compute the bezoutians and the coefficients $\beta_j(\Delta(\beta_i))$, which we do not detail here. Each coefficient of Δ (corresponding to a $n \times n$- determinant) has a size bounded by $\mathcal{O}(n\,(T + \log(n))$. The size of the coefficients of β_i is bounded in proposition (4.2), say by T'. Therefore the size of λ_l is bounded by $\mathcal{O}(\mu\,(n\,T + T' + n\,\log(n) + \log(\mu)))$.

5.1.4 Example

We consider again the polynomials of the example (4.2). The polynomial $\Delta_{\mathbf{P}} \in \mathbb{K}[\mathbf{x}, \mathbf{y}]$ is

$$\begin{aligned}
&10\,{x_2}^5 + 25\,{x_1}^3\,{x_2}^3 + (10\,{x_2}^3 + 25\,{x_1}^3\,x_2)\;{y_2}^2 \\
&\quad + (10\,{x_2}^4 + 25\,{x_1}^3\,{x_2}^2)\;y_2 + (25\,{x_1}^2\,{x_2}^3 - 4\,x_1\,{x_2}^2)\;y_1 \\
&\quad + (-4\,x_2 + 25\,x_1\,{x_2}^2)\;{y_1}^2\,y_2 + (25\,{x_1}^2\,{x_2}^2 - 4\,x_1\,x_2)\;y_1\,y_2 \\
&\quad + (10\,{x_1}^3 + 25\,x_1\,{x_2}^3)\;{y_1}^2 + (10\,{x_2}^2 + 25\,{x_1}^3)\;{y_2}^3 \\
&\quad + (25\,{x_2}^3 + 10\,{x_1}^2)\;{y_1}^3 + 25\,{x_1}^2\,y_1\,{y_2}^3 + 25\,x_1\,{y_1}^2\,{y_2}^3 \\
&\quad + 25\,{x_1}^2\,x_2\,y_1\,{y_2}^2 + 25\,{x_2}^2\,{y_1}^3\,y_2 + 25\,{y_2}^2\,x_2\,{y_1}^3 \\
&\quad + 25\,x_1\,x_2\,{y_2}^2\,{y_1}^2 + 10\,x_1\,{y_1}^4 + 25\,{y_1}^3\,{y_2}^3 + 10\,{y_1}^5
\end{aligned}$$

The residue $\tau_{\mathbf{P}}$ is of the form

$$\begin{aligned} &u_1 + u_2\,\mathbf{d}_1 + u_3\,\mathbf{d}_2 + u_4\,{\mathbf{d}_1}^2 + u_5\,{\mathbf{d}_2}^2 + u_6\,\mathbf{d}_1\,\mathbf{d}_2 + u_7\,{\mathbf{d}_2}^3 + u_8\,{\mathbf{d}_1}^3 \\ &\quad + u_9\,\left(5\,\mathbf{d}_1\,{\mathbf{d}_2}^2 - 2\,{\mathbf{d}_1}^4\right) + u_{10}\,\left(5\,{\mathbf{d}_1}^2\,\mathbf{d}_2 - 2\,{\mathbf{d}_2}^4\right) \\ &\quad + u_{11}\,\left(5\,{\mathbf{d}_1}^2\,{\mathbf{d}_2}^2 - 2\,{\mathbf{d}_1}^5 - 2\,{\mathbf{d}_2}^5\right) \end{aligned}$$

and must satisfy the system

$$\begin{aligned} &-20\,u_{11} - 1 = -20\,u_9 = -20\,u_{10} = 10\,u_8 = 10\,u_7 \\ &= \quad 125\,u_{11} - 4\,u_6 = 10\,u_5 + 25\,u_8 = 10\,u_4 + 25\,u_7 \\ &= \quad -20\,u_2 + 625\,u_{10} = 625\,u_9 - 20\,u_3 = -20\,u_1 + 125\,u_6 = 0 \end{aligned}$$

This yields

$$\tau_{\mathbf{P}} = -\frac{625}{64} - \frac{25}{16}\,\mathbf{d}_1\,\mathbf{d}_2 - \frac{1}{4}\,{\mathbf{d}_1}^2\,{\mathbf{d}_2}^2 + \frac{1}{10}\,{\mathbf{d}_1}^5 + \frac{1}{10}\,{\mathbf{d}_2}^5$$

The multiplicity of 0 (or the dimension of $B_0 = R/Q_0$) is given by the value of $\tau_{\mathbf{P}}$ on the Jacobian of p_1, p_2: $-12\,{x_1}^2\,{x_2}^2 + 40\,{x_2}^5 + 40\,{x_1}^5 + 400\,{x_1}^3\,{x_2}^3$ (see [21][p. 186]. This result is a consequence of the relation between traces and residues. Here it yields $11 = (-12) \times (-\frac{1}{4}) + 40 \times \frac{1}{10} + 40 \times \frac{1}{10}$. In the general case of locally complete intersections, it gives a way to check the results of the algorithm 4.3.

We can check if $\mathbf{d}^{\mathbf{n}}$ is a monomial of maximal degree appearing in τ, then the *socle* of B_ζ (ie. the annihilator $Ann_{B_\zeta}(\mathbf{m}_\zeta)$ of the maximal ideal $\mathbf{m}_\zeta$) is generated by $\mathbf{x}_\zeta^{\mathbf{n}}$. In this case, we can take $\mathbf{x}_1^5$ or $\mathbf{x}_2^5$.

5.2 Yet another way to compute the resultant

We consider here a special case of the section (5.1.2). Let $p_1, \ldots, p_n$ be n generic homogeneous polynomials of degree $d_1, \ldots, d_n$ in the variables $\mathbf{x} = (x_1, \ldots, x_n)$. The polynomials p_i are of the form

$$p_i = \sum_{|\mathbf{m}|=d_i} a_{i,\mathbf{m}}\,\mathbf{x}^{\mathbf{m}},$$

where the $a_{i,\mathbf{m}}$ are new variables or "parameters". Let $A = \mathbb{K}[a_{i,\mathbf{m}}]$ be the polynomial ring generated by these parameters, K be the fraction field of A and $I \subset K[\mathbf{x}]$, the ideal generated by these polynomials. Generically, these polynomials have no common root in the projective space $\mathbb{P}(\overline{K}^n)$, which

means that these polynomials define the origin in $\overline{K}^n$. Therefore, we can apply the algorithm (4.3) with $\zeta = 0$, in order to construct $I^\perp = D$. Note that as the polynomials p_i are homogeneous, we can construct a basis of D, which is also homogeneous.

Let $\nu = \sum_i d_i - n$ and $\Delta_0 = \Delta(\mathbf{x}, 0)$ be the element Δ (defined in (17)) where $\mathbf{y}$ is substituted by the origin. It is a polynomial of degree ν in $\mathbf{x}$. The following theorem can be found in the works of J.P Jouanolou (see [12],[13]):

Theorem 5.1 — *Let ω the homogeneous element of $A[\partial] \cap D$ of degree ν and of smallest possible degree in $a_{i,\mathbf{m}}$. Then*

$$\omega(\Delta_0) = \mathcal{R}(p_1, \ldots, p_n)$$

where $\mathcal{R}(p_1, \ldots, p_n)$ is the resultant of the polynomials p_i.

As we are in a complete intersection case, there is an element $\tau_{\mathbf{P}}$ which generates the inverse system D. Using Euler-Jacobi theorem, we check that the degree of $\tau_{\mathbf{P}}$ is precisely ν. Therefore, there exists a unique homogeneous element of D_ν, with coefficients in A of smallest possible degree. According to [13], this element generates the module $Hom_A(B, A)$ and satisfies the relation

$$\omega(\Delta) = \omega(\Delta_0) = \mathcal{R}(p_1, \ldots, p_n).$$

In fact, the residue $\tau_{\mathbf{P}}$ is given by

$$\tau_{\mathbf{P}} = \frac{\omega}{\mathcal{R}(p_1, \ldots, p_n)},$$

for we must have $\tau_{\mathbf{P}}(\Delta) = 1$.

Note that the algorithm (4.3) yields a multiple of the element ω. To recover ω, we have to extract the primitive part of this last element. In general, the coefficients of the constructed basis β_i can be chosen in $A[\partial]$. Moreover we may assume that there is no common factor $\in A \backslash K$ of their coefficients. In this case, the last constructed element is precisely ω.

5.3 Branches of a curve at the origin

Assume here that $\mathbb{K} = \mathbb{R}$.

5.3.1 Local topological degree

A classical application of residues is the computation of the topological degree of a polynomial map via the *signature* of a local residue, by Eisenbud-Levin's theorem (see [8], [2][p. 85]). See also [4] for another presentation. In our case, the degree of such a map $\mathbf{P} = (p_1, \ldots, p_n)$ can be computed as follows. Let $\beta_1, \ldots, \beta_\mu$ be a basis of $\widehat{B_\zeta}$ and let $b_1, \ldots, b_\mu$ be its dual basis in B_ζ. We denote by $\langle \, | \, \rangle$ the inner non-degenerate product $(a, b) \to \langle a|b\rangle = \tau_{\mathbf{P}}(a\, b)$ associated to the local residue of $\mathbf{P}$. Then Δ has a decomposition in $B_\zeta \otimes B_\zeta$ of the form

$$\Delta = \sum_{i=1}^{\mu} a_i \otimes b_i$$

where (a_i) is the dual basis of (b_i) in B_ζ for $\langle \, | \, \rangle$. Moreover we have

$$a_i = \sum_{j=1}^{\mu} \langle a_i | a_j \rangle \, b_j,$$

therefore we also have

$$\beta_i(\Delta(\beta_j)) = \langle a_i | a_j \rangle$$

and *the signature of the symmetric matrix* $(\beta_i(\Delta(\beta_j)))_{1 \leq i,j \leq \mu}$ *is the signature of the quadratic form associated to* $\langle \, | \, \rangle$*, or the topological degree of* $\mathbf{P}$, according to Eisenbud-Levin's theorem. This matrix is precisely the matrix which appears in the construction (5.1.3) of the residue.

5.3.2 Branches of curves

We apply this result to the analysis of curves at a singular point. More of the material on this subject can be found in [19] or [1]. Let $p_1, \ldots, p_{n-1} \in R$ be polynomials defining locally a *reduced* curve $\mathcal{C}$ through the point 0. Let g be a polynomial such that $p_1, \ldots, p_{n-1}, g$ defines locally the point 0. We denote by

$$J_g := \begin{vmatrix} d_{x_1} p_1 & \ldots & d_{x_n} f_1 \\ \vdots & & \vdots \\ d_{x_1} p_{n-1} & \ldots & d_{x_n} p_{n-1} \\ d_{x_1} g & \ldots & d_{x_n} g \end{vmatrix}.$$

Let $\mathbf{F} = (p_1, \ldots, p_{n-1}, J_g)$. Then $\mathbf{F}$ is locally a complete intersection defining 0 (if $\mathcal{C}$ is reduced), so that it defines a local residue $\tau_{\mathbf{F}}$.

The function g being continuous, has a constant sign on each half branch of the curve in a neighborhood of the origin. Let N^+ (resp. N^-) be the number of half real branches of the curve $\mathcal{C}$ such that $g > 0$ (resp. $g < 0$).

Theorem 5.1 — *The signature of the quadratic form associated to the local residue $\tau_{\mathbf{F}}$ is*

$$\frac{1}{2}(N^+ - N^-).$$

This theorem can be generalized to vector fields $\gamma = \gamma_1(\mathbf{x})d_{x_1} + \cdots + \gamma_n(\mathbf{x})d_{x_n}$ where γ_i are functions defined in a neighborhood except perhaps at the origin. A regular point on the curve near the origin has two tangents. We chose the orientation of the half branch, accordingly with the tangent for whose inner product with the vector field γ is positive. This orientation is independent of the point chosen on the half-branch in a neighborhood of the origin. Therefore we can define N^+ outbound half-branches and N^- inbound half-branches. The same result is valid, except that we replace $d_{x_i}(g)$ by γ_i. See [19] for more details.

A special interesting case of this theorem is $g = x_1^2 + \cdots + x_n^2$ or $\gamma = x_1 d_{x_1} + \cdots + x_n d_{x_n}$, where $N^- = 0$ and N^+ is the number of real half-branches of the curve, at the origin. The signature of $\tau_{\mathbf{F}}$ will be $\frac{1}{2}N^+$.

5.3.3 Example

We consider the example of a curve defined by the polynomial $p_1 = 2\,x_1\,x_2^2 + 5\,x_1^4 = x_1\,(2\,x_2^2 + 5x_1^3)$. The number of real branches is given by twice the signature of the residue $\tau_{\mathbf{F}}$ where $\mathbf{F} = (p_1, \frac{1}{4}\,J_{x_1^2+x_2^2})$ and $\frac{1}{4}\,J_{x_1^2+x_2^2} = {x_2}^3 - 2\,{x_1}^2 x_2 + 10\,{x_1}^3 x_2$. The dual D is generated by

$$1, \mathbf{d}_1, \mathbf{d}_2, {\mathbf{d}_1}^2, \mathbf{d}_1\mathbf{d}_2, {\mathbf{d}_2}^2, {\mathbf{d}_1}^3, 2\,{\mathbf{d}_2}^3 + {\mathbf{d}_1}^2\mathbf{d}_2,$$
$$2\,{\mathbf{d}_1}^4 - 5\,\mathbf{d}_1{\mathbf{d}_2}^2, 2\,{\mathbf{d}_1}^5 - 10\,{\mathbf{d}_2}^4 - 5\,{\mathbf{d}_1}^2{\mathbf{d}_2}^2$$

and B is of dimension 10. The residue is

$$\begin{aligned}\tau_{\mathbf{F}} \;=\; & -\frac{151875}{2048} - \frac{10125\,\mathbf{d}_1}{512} - \frac{675\,{\mathbf{d}_1}^2}{128} + \frac{225\,{\mathbf{d}_2}^2}{64} - \frac{45\,{\mathbf{d}_1}^3}{32} \\ & -\frac{3\,{\mathbf{d}_1}^4}{8} + \frac{15\,\mathbf{d}_1{\mathbf{d}_2}^2}{16} - \frac{{\mathbf{d}_1}^5}{10} + \frac{{\mathbf{d}_2}^4}{2} + \frac{{\mathbf{d}_1}^2{\mathbf{d}_2}^2}{4}\end{aligned}$$

and the signature of the matrix $(\beta_i(\Delta(\beta_j)))$ is $6 - 4 = 2$, which is half the number of half branches at the origin, as it can be checked on a picture.

6 Conclusion

As we have seen the duality between polynomials and differential operators is particularly well-suited for the description of isolated points of a variety. In this case, the formal series representing the linear forms become polynomials. This formalism allows us to devise an algorithm which proceeds from bottom (with the evaluation at the isolated point) to the top (with a basis of the dual of B_ζ). Among its advantage, we can mention a good complexity of the algorithm, closely related to intrinsic quantities, and new interesting features such as residues (which allow us to represent B_ζ with one polynomial in the case of complete intersections), quadratic forms and signatures, which give topological information on B_ζ. For these reasons and for many open questions related to it, we think that this domain is worth investigating from an effective point of view and the present work is a step in this direction. In particular, we aim at implementing these technic, for the local analysis of isolated points and to compare it with the usual approach of Gröbner basis.

References

[1] Aoki, K., Fukuda, T., and Nishimura, T. On the number of branches of zero locus of a map germ $(\mathbb{R}^n, 0) \to (\mathbb{R}^{n-1}, 0)$. *Topology and Computer Science* (1987), 347–363.

[2] Arnold, V., Varchenko, A., and Goussein-Zad. *Singulartits des applications diffrentiables.* Edition Mir, Moscou, 1986.

[3] Atiyah, M., and MacDonald, I. *Introduction to Commutative Algebra.* Addison-Wesley, 1969.

[4] Becker, E., Cardinal, J., Roy, M., and Szafraniec, Z. Multivariate Bezoutians, Kronecker symbol and some applications to real Geometry. In *Effective Methods in Algebraic Geometry (MEGA)* (1994), Progress in Math., Birkhäuser. To appear.

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

[6] Cardinal, J., and Mourrain, B. Algebraic approach of residues and applications. In *Proc. AMS-SIAM Summer Seminar on Math. of Numerical Analysis* (Park City, Utah, July 1995), J. Renegar, M. Shub, and S. Smale, Eds.

[7] Eisenbud, D. *Commutative Algebra with a view toward Algebraic Geometry*, vol. 150 of *Graduate Texts in Math.* Springer-Verlag, 1994.

[8] Eisenbud, D., and Levine, H. An algebraic formula for the degree of a C^∞ map germ. *Ann. Math. 106* (1977), 19–44.

[9] Elkadi, M., and Mourrain, B. Approche Algbrique des Rsidus et Applications. Rapport de recherche 2884, INRIA, 1996.

[10] Emsalem, J. Géométrie des points épais. *Bull. Soc. Math. France 106* (1978), 399–416.

[11] Gröbner, W. *Algebrische Geometrie II*, vol. 737 of *Bib. Inst. Mannheim*. Hochschultaschenbücher, 1970.

[12] Jouanolou, J. Le formalisme du résultant. *Adv. in Maths 90*, 2 (1991), 117–263.

[13] Jouanolou, J. Formes D'inertie et Rsultants : Un formulaire. Prpublication de l' IRMA (Strasbourg), 1993.

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

[15] Macaulay, F. *The Algebraic Theory of Modular Systems*, vol. 19 of *Cambridge tracts in Math. and Math. Physics*. Stechert-Hafner Service Agency, 1964.

[16] Maisonobe, P. $\mathcal{D}$-modules: an overview towards effectivity. In *Computer Algebra and Differential Equations* (1994), E. Tournier, Ed., Cambridge Univ. Press, 21–55.

[17] Malgrange, B. Motivations and introduction to the theory of $\mathcal{D}$-modules. In *Computer Algebra and Differential Equations* (1994), E. Tournier, Ed., Cambridge Univ. Press, 1–20.

[18] Marinari, M., Mora, T., and Möller, H. Grobner duality and multiplicities in polynomial system solving. In *ISSAC'95* (1995), A. Levelt, Ed., ACM Press, 167–179.

[19] Montaldi, J., and Van Straten, D. One-forms on singular curves and the topology of real curve singularities. *Topology 29*, 4 (1990), 501–510.

[20] Perdersen, P. S. A Basis for Polynomial Solutions to Systems of Linear Constant Coefficient PDE's. *Adv. In Math. 117* (1996), 157–163.

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