J. Symbolic Computation (2002) **33**, 679–699
doi:10.1006/jsco.2002.0530
Available online at http://www.idealibrary.com on IDEAL®

Relations Between Roots and Coefficients, Interpolation and Application to System Solving

BERNARD MOURRAIN† AND OLIVIER RUATTA†

INRIA, GALAAD, BP 93, 06902 Sophia-Antipolis, France

We propose an algebraic framework to represent zero-dimensional algebraic systems. In this framework, we give new interpolation formulæ. We use this good representation of the algebraic systems to develop a generalization of Weierstrass's method to the multivariate systems. This method allows us to approximate simultaneously all the roots of an algebraic system. We obtain an effective iteration function with a quadratic convergence in a neighbourhood of the solutions. We use this Weierstrass iteration function in a continuation method to obtain a global method. Experiments are exposed to underline the efficiency of the approach.

1. Introduction

The relations between roots and coefficients of a univariate polynomial, involving the elementary symmetric functions, are well known. Exploiting their properties yields efficient methods to approximate the roots of the polynomial, which consist in applying Newton's method to those relations. These methods are known under the names of Weierstrass's method (Weierstrass, 1903), Durand–Kerner's method (Durand, 1960; Kerner, 1966) and, in a similar way, Aberth's method (Bellido, 1992; Bini, 1996; Aberth, 1973; Yakoubsohn, 2000).

In this paper we generalize Weierstrass's method in the zero-dimensional multivariate setting. Our approach completes and improves the early work of Bellido (1992, 1994). We use the coordinate algebra of the iteration points as interpolation space and we give explicit interpolation formulæ in this space. As a result we obtain a new iteration function. We directly extend the univariate method by using a general algebraic framework based on the representation of quotient algebra, duality and interpolation formulæ. We give new formulæ for Lagrange and Hermite's interpolation problems following the terminology of Lascoux (2001), Lorentz and Lorentz (1990) and de Boor and Ron (1990). Furthermore we describe some relations between the roots and the coefficients of an algebraic system. We use this work on representation and interpolation to generalize Weierstrass's method. We propose a symbolic-numeric approach which needs a monomial basis of the quotient. This computation can be performed efficiently by several ways, see Faugère (1999) and Mourrain and Trébuchet (2000). The numerical part is an iterative method to approximate simultaneously all roots of an algebraic system. We obtain a local method with a quadratic convergence. We use the iteration function in a continuation method following the works in Dedieu and Smale (1998), Smale (1997),

†E-mail: mourrain,oruatta@sophia.inria.fr

0747–7171/02/050679 + 21 $35.00/0

Huber and Sturmfels (1995), Li (1997) and Verschelde *et al.* (1994) in order to obtain a more global method. Our approach presents several advantages. The iteration function is the same for algebraic system sharing the same basis for the quotient algebra. So the computation of a basis can be a preprocessing step for such a class of problems and so the actual solving part is reduced to a numerical continuation method. The inversion of a multivariate Vandermonde's system still remains a numerical limitation in our method and several alternatives are mentioned, but the problem is not analysed in detail in this paper.

Part of this work has already been presented in Ruatta (2001). In this paper we complete the description of quotient algebras, we give new interpolation formulæ for Hermite's problem and for the relations between roots and coefficients. We present more complete experimentations in the C++ environment SYNAPS[†] for symbolic and numeric computations. These experimentations also illustrate the potential power of this approach.

Hereafter $\delta_{i,j}$ denotes the Kronecker symbol (it equals 1 if $i = j$ and 0 otherwise). We denote by $\mathbb{K}$ a field of characteristic 0 and by $\mathcal{R} = \mathbb{K}[x_1, \ldots, x_n]$ the ring of polynomials in the variables $x_1, \ldots, x_n$, with coefficients in $\mathbb{K}$. For $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, $\mathbf{x}^\alpha$ is the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. The subspace generated by the elements $v_1, \ldots, v_k$ of a $\mathbb{K}$-vector space is denoted by $\langle v_1, \ldots, v_k \rangle$.

2. Univariate Case

Weierstrass's method is an iterative method which allows to approximate simultaneously all the roots of an algebraic equation. Other reformulations of this method are also known as Durand–Kerner or Dochev's method. Nowadays, there are several methods that generalize this approach in the univariate case (see Frommer, 1988; Bellido, 1992; Sendov *et al.*, 1994, Bini, 1996, Pan, 1997; or Fortune, 2001 for a good survey). There are several ways to introduce this method. A particularly interesting one is to construct the iteration function by applying Newton's method to a suitable multivariate function. We focus on the case of a polynomial with simple complex roots only.

Let $f \in \mathbb{K}[x]$ be a polynomial of the form $f(x) = x^d + a_1 x^{d-1} + \cdots + a_d = \prod_{i=1}^{d} (x - \zeta_i)$. We denote by $\zeta = (\zeta_1, \ldots, \zeta_d) \in \mathbb{K}^d$. A multivariate system of equations which admits, as a set of solutions, vectors formed with the coordinates of ζ (i.e. the roots of f), is constructed as follows.

For any $\mathbf{z} \in \mathbb{K}^d$, $\mathbf{z} = (z_1, \ldots, z_d)$, we denote by $\sigma_k(\mathbf{z}) = (-1)^k \sum_{0 \le i_1 < \cdots < i_k \le d} z_{i_1} \cdots z_{i_k}$ the kth elementary symmetric function. By expanding the expression $\prod_{i=1}^{d} (x - \zeta_i)$, we obtain the following multivariate system:

$$\Sigma(\mathbf{z}) = \begin{pmatrix} \sigma_1(\mathbf{z}) - a_1 \\ \vdots \\ \sigma_d(\mathbf{z}) - a_d \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{1}$$

This system defines the well known relations between roots and coefficients. Its solutions are all obtained by permutations of the coordinate of ζ and all such vectors are solutions of the system. Applying Newton's method to $\Sigma(\mathbf{z})$ and using an explicit formula

[†] `http://www-sop.inria.fr/galaad/logiciels/SYNAPS/`

for the inverse of the Jacobian matrix, we obtain the following iteration function:

$$\forall i \in \{1,\ldots,d\},\ z_i^{(k+1)} = \mathbf{I}_i^{DK}(\mathbf{z}) = z_i^{(k)} - \frac{f(z_i^{(k)})}{\prod_{j\neq i}(z_i^{(k)} - z_j^{(k)})} \tag{2}$$

where $\mathbf{z}^{(k)} = (z_1^{(k)},\ldots,z_n^{(k)})$ denotes the sequence of iteration points after k iterations of this function. The key ingredients of the underground computation are the Lagrange interpolation basis and its dual basis. The multivariate case, though more intricate, follows the same lines as we will see.

3. Algebraic Structure

In this section we recall elementary results on algebraic sets, ideals and their decomposition. We develop new algorithms and formulæ for interpolation and relation between roots and coefficients. Let $f_1,\ldots,f_m$ be polynomials of $\mathbb{K}[x_1,\ldots,x_n]$. We denote by $\mathcal{I} = (f_1,\ldots,f_m)$ the ideal that they generate and by $Z(\mathcal{I}) = \{\mathbf{z} \in \overline{\mathbb{K}}^n \mid g(\mathbf{z}) = 0,\ \forall g \in \mathcal{I}\} = \{\mathbf{z} \in \mathbb{K}^n \mid f_i(\mathbf{z}) = 0, \forall i \in \{1,\ldots,m\}\}$ the algebraic set they define. We denote by $\mathcal{A}$ the quotient algebra $\mathbb{K}[x_1,\ldots,x_n]/(f_1,\ldots,f_m)$.

Hypothesis 3.1. We assume that $Z(f_1,\ldots,f_m)$ is a finite set $\{\zeta_1,\ldots,\zeta_d\}$.

Under the Hypothesis 3.1, the ideal $\mathcal{I}$ is 0-dimensional and the minimal primary decomposition of $\mathcal{I}$ is $\mathcal{I} = Q_{\zeta_1} \cap \cdots \cap Q_{\zeta_d}$ where Q_{ζ_i} is $\mathbf{m}_{\zeta_i}$-primary and $\mathbf{m}_{\zeta_i}$ is the maximal ideal defining ζ_i (Vasconcelos, 1998).

3.1. Decomposition of the quotient algebra

We denote by $\mathcal{A}_{\zeta_i} = ((\mathbf{0}) : Q_{\zeta_i}/\mathcal{I})$ (i.e. $\mathcal{A}_{\zeta_i} = \{a \in \mathcal{A} \mid \forall q \in Q_{\zeta_i}/\mathcal{I},\ ap = 0\}$). It is an ideal of $\mathcal{A}$. Because Q_{ζ_i} is a primary ideal for the maximal ideal $\mathbf{m}_{\zeta_i}$ we have the following proposition (Atiyah and MacDonald, 1969; Vasconcelos, 1998; Elkadi and Mourrain, 2002):

Proposition 3.2. *The algebra $\mathcal{A}$ is the direct sum of its sub-algebras $\mathcal{A}_{\zeta_1},\ldots,\mathcal{A}_{\zeta_d}$, i.e. $\mathcal{A} = \mathcal{A}_{\zeta_1} \oplus \cdots \oplus \mathcal{A}_{\zeta_d}$.*

Definition 3.3. The multiplicity of the root $\zeta_i \in Z(\mathcal{I})$ is the dimension of the subspace $\mathcal{A}_{\zeta_i}$ of $\mathcal{A}$. It is denoted by μ_i. The root is simple if $\mu_i = 1$ and multiple if $\mu_i > 1$.

From this definition and the previous proposition we deduce that the dimension of $\mathcal{A}$ as a $\mathbb{K}$-vector space is the number of roots (i.e. element of $Z(\mathcal{I})$) counted with their multiplicities. That is to say that $\dim_{\mathbb{K}}(\mathcal{A}) = \mu_{\zeta_1} + \cdots + \mu_{\zeta_d}$.

There exists a unique duple $(\mathbf{e}_{\zeta_1},\ldots,\mathbf{e}_{\zeta_d}) \in \mathcal{A}_{\zeta_1} \times \cdots \times \mathcal{A}_{\zeta_d}$ such that $1 = \mathbf{e}_{\zeta_1} + \cdots + \mathbf{e}_{\zeta_d}$. Then we have $1 = \mathbf{e}_{\zeta_1} + \cdots + \mathbf{e}_{\zeta_d} = 1^2 = \mathbf{e}_{\zeta_1}^2 + \cdots + \mathbf{e}_{\zeta_d}^2 + 2\sum_{1\leq i<j\leq d} \mathbf{e}_{\zeta_i}\mathbf{e}_{\zeta_j}$. Because $\mathbf{e}_{\zeta_i}\mathbf{e}_{\zeta_j} \in \mathcal{A}_{\zeta_i} \cap \mathcal{A}_{\zeta_j} = (\mathbf{0})$ if $i \neq j$, then we deduce that $\mathbf{e}_{\zeta_i}\mathbf{e}_{\zeta_j} = 0$ and $\mathbf{e}_{\zeta_i}^2 = \mathbf{e}_{\zeta_i}$. The polynomials $\mathbf{e}_{\zeta_i}$ are called the fundamental system of idempotents of $\mathcal{A}$. As we will see, they generalize the Lagrange interpolation polynomials.

Proposition 3.4. *For $i \in \{1,\ldots,d\}$, we have $\mathcal{A}_{\zeta_i} = \mathcal{A}\mathbf{e}_{\zeta_i}$ and so $\mathbf{e}_{\zeta_i}$ is the neutral element of the sub-algebra $\mathcal{A}_{\zeta_i}$.*

PROOF. If $a \in \mathcal{A}_{\zeta_i}$, then $a = a\,1 = a\mathbf{e}_{\zeta_1} + \cdots + a\mathbf{e}_{\zeta_d} = a\mathbf{e}_{\zeta_i}$. The reciprocal is easy. □

PROPOSITION 3.5. *The idempotents* $\mathbf{e}_{\zeta_1}, \ldots, \mathbf{e}_{\zeta_d}$ *of* $\mathcal{A}$ *are such that* $\mathbf{e}_{\zeta_i}(\zeta_j) = \delta_{i,j}$.

PROOF. For $i, j \in \{1, \ldots, d\}$ and $j \neq i$, there exists $q \in Q_{\zeta_i}$ such that $q(\zeta_j) \neq 0$. Indeed, if there is no such polynomial then $Q_{\zeta_i} \subset \cup_{j \neq i} \mathbf{m}_{\zeta_i}$ and Q_{ζ_i} must be included in one of the $\mathbf{m}_{\zeta_j}$ with $j \neq i$. It yields to a contradiction since Q_{ζ_i} is $\mathbf{m}_{\zeta_i}$-primary. Now, because $q\mathbf{e}_{\zeta_i} = 0$, we have $\mathbf{e}_{\zeta_i}(\zeta_j) = 0$. Now we have $1 = \mathbf{e}_{\zeta_1}(\zeta_i) + \cdots + \mathbf{e}_{\zeta_d}(\zeta_i) = \mathbf{e}_{\zeta_i}(\zeta_i)$ and the proposition is proved. □

We know that if $\mu_i > 1$, then $\mathcal{A}_{\zeta_i}$ is a $\mathbb{K}$-vector space of dimension $\mu_i > 1$ and $\mathcal{A}_{\zeta_i} = \mathcal{A}\mathbf{e}_{\zeta_i}$ is a $\mathcal{A}$-module of rank one. To have a better understanding of the structure we will first consider the projection map of $\mathcal{A}$ on $\mathcal{A}_{\zeta_i}$ defined by $\pi_{\zeta_i} : a \in \mathcal{A} \mapsto a\mathbf{e}_{\zeta_i} \in \mathcal{A}_{\zeta_i}$.

PROPOSITION 3.6. $\mathrm{Ker}(\pi_{\zeta_i}) = \oplus_{j \neq i} \mathcal{A}_{\zeta_j} = Q_{\zeta_i}/\mathcal{I}$.

PROOF. $\oplus_{j \neq i} \mathcal{A}_{\zeta_j} = \big((0) : \cap_{j \neq i} Q_{\zeta_j}/\mathcal{I}\big) = Q_{\zeta_i}/\mathcal{I} = \mathrm{Ker}(\pi_{\zeta_i})$. □

Henceforth, we identify $\mathcal{A}_{\zeta_i}$ with $\mathcal{A}/\mathrm{Ker}(\pi_{\zeta_i})$. But $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ and $\mathrm{Ker}(\pi_{\zeta_i}) = Q_{\zeta_i}/\mathcal{I}$ and so $\mathcal{A}_{\zeta_i} = \mathbb{K}[x_1, \ldots, x_n]/Q_{\zeta_i}$. This expression allows us to have a good representation of $\mathcal{A}_{\zeta_i}$ thanks to the following proposition:

PROPOSITION 3.7. *The map* $\Phi_{\zeta_i} : \left\{ \begin{array}{ccc} \mathbb{K}[x_1, \ldots, x_n]/Q_{\zeta_i} & \longrightarrow & \mathcal{A}_{\zeta_i} \\ a & \longmapsto & a\mathbf{e}_{\zeta_i} \end{array} \right.$ *is an isomorphism of* $\mathbb{K}$*-algebras.*

It shows in particular that $\mathcal{A}_{\zeta_i}$ is a local ring of maximal ideal $(\mathbf{m}_{\zeta_i}/Q_{\zeta_i})\,\mathbf{e}_{\zeta_i}$. See Atiyah and MacDonald (1969), Vasconcelos (1998) and Cox *et al.* (1992) for more details.

To completely describe the structure of $\mathcal{A}_{\zeta_i}$ as a $\mathbb{K}$-vector space we introduce hereafter some tools of duality.

3.2. DUALITY AND ORTHOGONALITY

DEFINITION 3.8. We denote by $\widehat{\mathcal{R}} = \mathrm{Hom}_{\mathbb{K}}(\mathcal{R}, \mathbb{K})$, the dual space of $\mathcal{R}$. It is the set of $\mathbb{K}$-linear forms on $\mathcal{R}$.

We recall the interpretation of the $\mathbb{K}$-linear forms as differential operators (we refer to Mourrain, 1996). We denote by ∂_i the operator $\frac{d}{dx_i}$ and for all $\alpha \in \mathbb{N}^n$ we denote by $\partial^\alpha = \frac{d^{\alpha_1}}{dx_1{}^{\alpha_1}} \cdots \frac{d^{\alpha_n}}{dx_n{}^{\alpha_n}}$ with the convention $\partial^{\mathbf{0}} = 1$. We denote by $\mathbb{K}[[\partial_1, \ldots, \partial_n]]$ the set of formal power series in the variables $\partial_1, \ldots, \partial_n$. For any $\xi \in \mathbb{K}^n$, we consider the following bilinear map:

$$\langle ., . \rangle_\xi : \left\{ \begin{array}{ccc} \mathbb{K}[[\partial_1, \ldots, \partial_n]] \times \mathcal{R} & \longrightarrow & \mathbb{K} \\ (\Lambda, f) & \longmapsto & \langle \Lambda, f \rangle_\xi = \Lambda(f)(\xi) \end{array} \right.$$

where if $\Lambda = \sum_{\alpha \in \mathbb{N}^n} \lambda_\alpha \partial^\alpha$, then $\Lambda(f)(\xi) = \sum_{\alpha \in \mathbb{N}^n} \lambda_\alpha (\partial^\alpha f)(\xi)$.

The map $\Theta_\xi : \left\{ \begin{array}{ccc} \mathbb{K}[[\partial_1, \ldots, \partial_n]] & \longrightarrow & \widehat{\mathcal{R}} \\ \Lambda & \longrightarrow & \Lambda \circ 1_\xi = \langle \Lambda, . \rangle_\xi \end{array} \right.$ is an isomorphism of $\mathbb{K}$-vector spaces which allows us to identify $\widehat{\mathcal{R}}$ with $\mathbb{K}[[\partial_1, \ldots, \partial_n]]$.

For any $f \in \mathcal{R}$ and $\Lambda \in \widehat{\mathcal{R}}$, we define $f \cdot \Lambda : g \in \mathcal{R} \mapsto \Lambda(fg) \in \mathbb{K}$, so that $\widehat{\mathcal{R}}$ has a natural structure of $\mathcal{R}$-module. We can show that the multiplication by $x_i - \xi_i$ acts on $\widehat{\mathcal{R}}$ as $\partial_{\partial_i} = \frac{d}{d\partial_i}$.

One can remark that, if $\mathbb{K}$ has the characteristic zero, $\langle \partial^\beta, (\mathbf{x}-\xi)^\alpha \rangle_\xi = \delta_{\alpha,\beta}\, \alpha!$ and so $\left(\frac{1}{\alpha!}\partial^\alpha\right)_{\alpha\in\mathbb{N}^n}$ and $\left((\mathbf{x}-\xi)^\alpha\right)_{\alpha\in\mathbb{N}^n}$ are dual bases for the bilinear form $\langle .,. \rangle_\xi$.

We denote by $e^{(\xi,\partial)} = \sum_{\alpha\in N^n} \frac{\xi^\alpha \partial^\alpha}{\alpha!}$. Let $\Lambda \in \widehat{\mathcal{R}}$ be a linear form. One can show that $\Theta_{\mathbf{0}}^{-1}(\Lambda) = e^{(\xi,\partial)}\Theta_\xi^{-1}(\Lambda)$.

We will now define a notion of orthogonality:

Definition 3.9.

- For any $\mathcal{I} \subset \mathcal{R}$ being an ideal, we define the sub-vector space $\mathcal{I}^\perp \subset \widehat{\mathcal{R}}$ orthogonal to $\mathcal{I}$ (also called the inverse system of $\mathcal{I}$ (Macaulay, 1916)) by:
$$\mathcal{I}^\perp = \{\Lambda \in \widehat{\mathcal{R}} \,|\, \Lambda(f) = 0,\, \forall f \in \mathcal{I}\}.$$
- For any D being a subspace of $\widehat{\mathcal{R}}$, we define the subspace $D^\perp$ of $\mathcal{R}$ orthogonal to D by:
$$D^\perp = \{f \in \mathcal{R} \,|\, \Lambda(f) = 0,\, \forall \Lambda \in D\}.$$

Proposition 3.10. *Let $\mathcal{I}$ be an ideal of $\mathcal{R}$ and $\mathcal{A} = \mathcal{R}/\mathcal{I}$, then the projection $\pi : \mathcal{R} \to \mathcal{A}$ induces an isomorphism $\pi_* : \widehat{\mathcal{A}} \to \mathcal{I}^\perp$.*

Theorem 3.11. (Emsalem, 1978) *There is a one-to-one correspondence between ideals of $\mathcal{R}$ and subspaces of $\widehat{\mathcal{R}}$ stable by derivation and closed for the $(\partial_1, \ldots, \partial_n)$-adic topology.*

Let $\mathcal{I}$ be an ideal of $\mathcal{R}$ and D a closed subspace of $\widehat{\mathcal{R}}$ stable by derivation, we have $\mathcal{I}^{\perp\perp} = \mathcal{I}$ and $D^{\perp\perp} = D$.

We refer to Mourrain (1996) for a more complete description of this formalism. We just recall that if $\mathcal{I}$ and $\mathcal{J}$ are two ideals of $\mathcal{R}$ then $\mathcal{I}^{\perp\perp} = \mathcal{I}$, $\mathcal{I} \subset \mathcal{J}$ if and only if $\mathcal{J}^\perp \subset \mathcal{I}^\perp$, $(\mathcal{I} \cap \mathcal{J})^\perp = \mathcal{I}^\perp + \mathcal{J}^\perp$ and $(\mathcal{I} + \mathcal{J})^\perp = \mathcal{I}^\perp \cap \mathcal{J}^\perp$. The properties of orthogonality with respect to ideal division give the following proposition.

Proposition 3.12. *Let $\mathcal{I}$ be an ideal of $\mathcal{R}$ such that $Z(\mathcal{I}) = \{\zeta_1, \ldots, \zeta_d\}$, then, if we denote by $\mathcal{A} = \mathcal{R}/\mathcal{I}$ we have $\widehat{\mathcal{A}} = D_{\zeta_1} \oplus \cdots \oplus D_{\zeta_d}$ where $D_{\zeta_i} = Q_{\zeta_i}^\perp$, Q_{ζ_i} is the $\mathbf{m}_{\zeta_i}$-primary component of $\mathcal{I}$.*

We have $\mathcal{A}_{\zeta_i} = Q_{\zeta_i}/\mathcal{I}$ and we can show that $\widehat{\mathcal{A}}_{\zeta_i} = Q_{\zeta_i}^\perp \subset \mathcal{I}^\perp$. This basic fact allows us to compute the inverse system "locally", i.e. we look at ζ_i as an isolated point of the variety and we can compute the inverse system associated to this point (Mourrain, 1996).

Proposition 3.13. *Let Q_{ζ_i} be a $\mathbf{m}_{\zeta_i}$-primary component of $\mathcal{I}$, then $\mathcal{I}^\perp \subset \Theta_{\zeta_i}(\mathbb{K}[\partial])$.*

We recall that μ_i denotes the multiplicity of ζ_i, then we have the following theorem:

Theorem 3.14. *Let $\mathcal{I} = (f_1, \ldots, f_n)$ such that $Z(\mathcal{I}) = \{\zeta_1, \ldots, \zeta_d\}$, for all $i \in \{1, \ldots, d\}$ there is a family $\{\Lambda_1^{(i)}, \ldots, \Lambda_{\mu_i}^{(i)}\} \subset D_{\zeta_i} \subset \mathbb{K}[\partial]$ with $\Lambda_1^{(i)} = 1$, such that for all $\Lambda \in \mathcal{I}^\perp$*

we have $\Lambda(\partial) = \sum_{i=1}^{d} e^{(\zeta_i,\partial)} \sum_{j=1}^{\mu_i} \Lambda_j^{(i)}(\partial)$. *Furthermore if* $f \in \mathcal{A}$, *we have* $\Lambda(f) = \sum_{i=1}^{d} \sum_{j=1}^{\mu_i} \langle \Lambda_j^{(i)}, f\rangle_{\zeta_i}$.

As a consequence, the family $(\Lambda_j^{(i)} e^{(\zeta_i,\partial)})_{1\le i\le d, 1\le j\le \mu_i}$ is a basis of $\widehat{\mathcal{A}} = \mathcal{I}^{\perp}$. We will hereafter assume that we have the polynomials $(\Lambda_j^{(i)})_{1\le i\le d, 1\le j\le \mu_i}$ as an input of our method.

The knowledge of these local dual spaces allows us to construct a global duality as follows:

Definition 3.15. The bilinear form $\langle .,. \rangle_{Z(\mathcal{I})} : \widehat{\mathcal{A}} \times \mathcal{A} \longrightarrow \mathbb{K}$ is defined by associating to $\Lambda \in \widehat{\mathcal{A}}$ and $p \in \mathcal{A}$ the scalar $\sum_{i=1}^{d} \langle \Lambda_i, p\rangle_{\zeta_i}$ where $\Lambda = \Lambda_1 \oplus \cdots \oplus \Lambda_d$ with $\Lambda_i \in D_{\zeta_i}$.

A fundamental property of this bilinear form is given by the following proposition :

Proposition 3.16. *The bilinear form* $\langle .,. \rangle_{Z(\mathcal{I})}$ *is non-degenerated.*

4. Multivariate Interpolation

4.1. introduction

The classical interpolation problem consists in finding polynomials with given values at fixed points $\zeta_1, \ldots, \zeta_d$ and with a fixed support. The general interpolation problem, also called the Hermite interpolation problem, consists in computing the set of polynomials p satisfying tangential conditions $\langle \Lambda_j^{(i)}(\partial), p\rangle_{\zeta_i} = v_{i,j}$ $j = 1, \ldots, \mu_i$ at fixed points $\zeta_1, \ldots, \zeta_d$, where $\Lambda_j^{(i)}(\partial)$ is a polynomial in the derivatives ∂. Hereafter, we will also denote by $\Lambda_j^{(i)}$ the corresponding linear form $p \mapsto \langle \Lambda_j^{(i)}(\partial), p\rangle_{\zeta_i}$. The sequence of all linear forms $\Lambda_j^{(i)}$ will also be denoted by $\Lambda_1, \ldots, \Lambda_D$ where $D = \mu_1 + \cdots + \mu_d$. The general interpolation problem can thus be reformulated as the problem of computing in $\mathcal{R}$ the orthogonal vector space $(\Lambda_i)_{i=1,\ldots,D}^{\perp}$ and a complementary space. The basis of interpolation is the basis of this complementary space, which is dual to $(\Lambda_i)_{i=1,\ldots,D}$.

In order to be in an algebraic setting, we will consider hereafter the case where $(\Lambda_i)_{i=1,\ldots,D}^{\perp}$ *is an ideal of* $\mathcal{R}$. According to Theorem 3.11, it is equivalent to say that each set of polynomials $\langle \Lambda_j^{(i)}(\partial)\rangle_{j=1,\ldots,\mu_i}$ is stable by derivation by ∂_{∂_i}. Hereafter the ideal $(\Lambda_i)^{\perp}$ is also denoted by I_Λ and $\mathcal{A}_\Lambda = \mathcal{R}/\mathcal{I}_\Lambda$.

Under this condition we have the following property:

Proposition 4.1. *The generalized interpolation problem* $\Lambda_i(p) = v_{i,j}$, $i = 1, \ldots, D$, *has a unique solution in* $\langle \mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_D}\rangle$ *if and only if the determinant of the matrix* $V_{\Lambda,E} = (\Lambda_i(\mathbf{x}^{\alpha_j}))_{i,j=1,\ldots,D}$ *does not vanish.*

This matrix allows us to solve the interpolation problem, using the following proposition:

Proposition 4.2. *Assume that the matrix* $V_{\Lambda,E}$ *is invertible and let* $W_{\Lambda,E} = V_{\Lambda,E}^{-1}$. *Then the representatives, in the basis* $\{\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_D}\}$, *of the dual basis of* $(\Lambda_i)_{i=1,\ldots,D}$ *are* $\mathbf{w}_i = \sum_i W_{i,j}\, \mathbf{x}^{\alpha_j}$.

PROOF. Let $\mathbf{w}_i$ be these representatives in the basis $\{\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_D}\}$ of $\mathcal{A}_\Lambda$. They satisfy $\Lambda_i(\mathbf{w}_j) = \delta_{i,j}$. Denoting by $w_{i,j}$ their coefficients with respect to the basis $\mathbf{x}^{\alpha_j}$ ($\mathbf{w}_j = \sum_{k=1}^{D} w_{j,k}\, \mathbf{x}^{\alpha_k}$), we have $\Lambda_i(\mathbf{w}_j) = \sum_{k=1}^{D} w_{j,k} \Lambda_i(\mathbf{x}^{\alpha_k})$, which means that the matrix $(w_{j,k})$ is the inverse of $V_{\Lambda,E}$. □

And it allows us to answer directly to the interpolation problem.

THEOREM 4.3. *The interpolation problem $\Lambda_j(p) = v_j$ for $j = 1, \ldots, D$ has a unique solution in the vector space $\langle \mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_D} \rangle$ if and only if $det(V_{\Lambda,E}) \neq 0$. In such a case, the solution is given by $p = \sum_{i=1}^{D} v_i\, \mathbf{w}_i$, where $\mathbf{w}_i = \sum_i W_{i,j}\, \mathbf{x}^{\alpha_j}$ and $(W_{i,j})$ is the inverse matrix of $V_{\Lambda,E}$.*

PROOF. We check directly that $\Lambda_i(p) = v_i$ and that $\mathbf{w}_i \in \langle \mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_D} \rangle$. □

See, for instance, de Boor and Ron (1990) for more details. We are now going to give an explicit formula for such a solution in terms of the monomials $\mathbf{x}^{\alpha_i}$ and the linear forms Λ_j.

4.2. SIMPLE ROOTS

Let us first detail the case of *simple roots* $\mathbf{z} = \{\zeta_1, \ldots, \zeta_D\}$ for which the linear forms Λ_i are the evaluations 1_{ζ_i}, $i = 1, \ldots, d$ at the roots $\zeta_i \in \mathbb{K}^n$. We easily check that $\langle 1_{\zeta_i} \rangle$ is stable by derivation since $x_i \cdot 1_{\zeta_j} = \zeta_{j,i}\, 1_{\zeta_j}$ so that $(\Lambda)^\perp$ is an ideal (indeed the ideal of polynomials vanishing at the points $\zeta_1, \ldots, \zeta_d$). Let us denote it by $I_\mathbf{z}$ and the corresponding quotient algebra by $\mathcal{A}_\mathbf{z} = \mathcal{R}/I_\mathbf{z}$.

By Proposition 3.4, the local ring associated with ζ_i is $\mathcal{A}_{\zeta_i} = \mathbb{K}\, \mathbf{e}_{\zeta_i}$ and we obtain the following proposition:

PROPOSITION 4.4. *The quotient algebra $\mathcal{A}_\mathbf{z}$ is a d-dimensional $\mathbb{K}$-vector space that admits the set of idempotents $(\mathbf{e}_{\zeta_i})_{i \in \{1,\ldots,d\}}$ as basis. Its dual basis in $\widehat{\mathcal{A}}$ is $(1_{\zeta_i})_{i \in \{1,\ldots,d\}}$.*

This proposition is in fact a consequence of the Cauchy formula: $\forall a \in \mathcal{A}$,

$$a = \sum_{i=1}^{d} 1_{\zeta_i}(a)\, \mathbf{e}_{\zeta_i} = \sum_{i=1}^{d} a(\zeta_i)\, \mathbf{e}_{\zeta_i}$$

which also yields an interpolation formula, generalizing the Lagrange interpolation formula. This representation of $\mathcal{A}_\mathbf{z}$ has several advantages. One of them is the simplicity of the multiplicative structure. Indeed, $\forall a$ and $b \in \mathcal{A}$ we have $ab = \sum_{i=1}^{d} 1_{\zeta_i}(ab)\, \mathbf{e}_{\zeta_i} = \sum_{i=1}^{d} a(\zeta_i)\, b(\zeta_i)\, \mathbf{e}_{\zeta_i}$.

DEFINITION 4.5. Let $\mathbf{z} = \{\zeta_1, \ldots, \zeta_d\}$. Let $E = \{\alpha_1, \ldots, \alpha_d\} \subset \mathbb{N}^n$, and let $\mathbf{x}^E = \{\mathbf{x}^\alpha | \alpha \in E\}$. We call the following matrix Vandermonde's matrix associated to E and $\{\zeta_1, \ldots, \zeta_d\}$:

$$V_{\mathbf{z},E} = \begin{pmatrix} \zeta_1^{\alpha_1} & \cdots & \zeta_1^{\alpha_d} \\ \vdots & \ddots & \vdots \\ \zeta_d^{\alpha_1} & \cdots & \zeta_d^{\alpha_d} \end{pmatrix}. \tag{3}$$

The Vandermonde's determinant associated to E and $\mathbf{z}$ is $\mathbf{v}_{\mathbf{z},E} = \det(V_{\mathbf{z},E})$.

According to Proposition 4.1, we have:

PROPOSITION 4.6. *Let $\mathbf{z} = \{\zeta_1, \ldots, \zeta_d\}$ and let $E = \{\alpha_1, \ldots, \alpha_d\} \subset \mathbb{N}^n$. The set $\mathbf{x}^E$ is a monomial basis of $\mathcal{A}_\mathbf{z} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}_\mathbf{z}$ if and only if the Vandermonde's determinant associated to E and $\mathbf{z}$ is not zero.*

We denote by $\mathbb{K}[x_1, \ldots, x_n]_E = \left\{p \in \mathbb{K}[x_1, \ldots, x_n] \,|\, p = \sum_{\alpha \in E} p_\alpha \mathbf{x}^\alpha\right\}$, i.e. the set of polynomials with monomial support in $\mathbf{x}^E$.

DEFINITION 4.7. Let $\mathbf{z} = \{\zeta_1, \ldots, \zeta_d\}$ and let $E = \{\alpha_1, \ldots, \alpha_d\} \subset \mathbb{N}^n$ such that $\det(V_{\mathbf{z},E}) \neq 0$($\mathbf{x}^E$ is a monomial basis of $\mathcal{A}_\mathbf{z}$). We define the pseudo-Lagrange's polynomial associated with ζ_i by:

$$\mathbf{e}_i = -\frac{1}{V_{\mathbf{z},E}} \begin{vmatrix} \mathbf{x}^{\alpha_1} & \cdots & \mathbf{x}^{\alpha_d} \\ \zeta_1^{\alpha_1} & \cdots & \zeta_1^{\alpha_d} \\ \vdots & & \vdots \\ \zeta_{i-1}^{\alpha_1} & \cdots & \zeta_{i-1}^{\alpha_d} \\ \zeta_{i+1}^{\alpha_1} & \cdots & \zeta_{i+1}^{\alpha_d} \\ \vdots & & \vdots \\ \zeta_d^{\alpha_1} & \cdots & \zeta_d^{\alpha_d} \end{vmatrix}. \tag{4}$$

PROPERTIES 4.8. *The class of $\mathbf{e}_i$ in $\mathcal{A}$ is the idempotent associated with the root ζ_i and $\mathbf{e}_i \in \mathbb{K}[x_1, \ldots, x_n]_E$, for $i = 1, \ldots, d$.*

PROOF. Let us denote by $\mathbf{e}'_i$ the determinant polynomial defined in (4). We check that $\mathbf{e}'_i(\zeta_j) = \delta_{i,j}$, so that according to Proposition 3.5, $\mathbf{e}_i \equiv \mathbf{e}'_i$. □

This property yields the solution to the interpolation problem as follows:

THEOREM 4.9. *Let us assume that $\det(V_{\mathbf{z},E})$ is not zero. Then for any value $v_i \in \mathbb{K}$, there exists a unique polynomial $p \in \mathbb{K}[x_1, \ldots, x_n]_E$ such that $p(\zeta_i) = v_i$. It is given by $p(\mathbf{x}) = \sum_{i=1}^d v_i \, \mathbf{e}_i$.*

4.3. ROOTS WITH MULTIPLICITIES

We now describe explicitly the general case of Hermite interpolation. Let us consider μ_i tangential conditions $\Lambda_{i,j}(p) = v_i$ at points ζ_i, for $i = 1, \ldots, d$. They are of the form $\langle \Lambda_j^{(i)}(\partial), p\rangle_{\zeta_i} = v_i$ where $\Lambda_j^{(i)}(\partial)$ is a polynomial in ∂.

We assume that each $(\Lambda_j^{(i)})_{j=1,\ldots,\mu_i}$ is *stable by derivation* so that $(\Lambda)^\perp = (\Lambda_{i,j})^\perp := I_\Lambda$ is an ideal of R. We denote by $\mathcal{A}_\Lambda = \mathcal{R}/I_\Lambda$ the associated quotient algebra.

The dual space associated with the local algebra $\mathcal{A}_{\zeta_i}$ is $(\Lambda_j^{(i)})_{j=1,\ldots,\mu_i}$. Because these elements are polynomials in ∂_i, and the vector space is stable by derivation by ∂_{∂_i}, it contains the element 1. We assume, without loss of generality, that $\Lambda_1^{(i)} = 1$ *and that the* $\Lambda_j^{(i)}(\partial)$ *have no constant terms* (it can be done by subtraction of a scalar multiple of $\Lambda_1^{(i)} = 1$).

Definition 4.10. With the above assumptions and notations, we define the following matrix as Vandermonde's matrix associated to E and $\Lambda = \left(\Lambda_j^{(i)}\right)_{i=1,\ldots,d,\ j=1,\ldots,\mu_i}$:

$$V_{\Lambda,E} = \begin{pmatrix} \langle \Lambda_1^{(1)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_1} & \cdots & \langle \Lambda_1^{(1)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_1} \\ \vdots & & \vdots \\ \langle \Lambda_{\mu_1}^{(1)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_1} & \cdots & \langle \Lambda_{\mu_1}^{(1)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_1} \\ \vdots & & \vdots \\ \langle \Lambda_1^{(d)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_d} & \cdots & \langle \Lambda_1^{(d)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_d} \\ \vdots & & \vdots \\ \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_d} & \cdots & \langle \Lambda_{\mu_{\zeta_d}}^{(1)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_d} \end{pmatrix}.$$

The Vandermonde's determinant associated to $Z(\mathcal{I})$ and E is $\mathbf{v}_{\Lambda,E} = \det(V_{\Lambda,E})$.

According to Proposition 4.1, we have:

Theorem 4.11. *Let $\mathbf{z} = \{\zeta_1, \ldots, \zeta_d\} \in \mathbb{K}^n$ and let $E = \{\alpha_1, \ldots, \alpha_D\} \subset \mathbb{N}^n$. Therefore, $\mathbf{x}^E$ is a basis of $\mathcal{A}_\Lambda = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}_\Lambda$ if and only if the Vandermonde's determinant $\det(V_{\Lambda,E}) \neq 0$.*

Definition 4.12. Let $\mathbf{z} = \{\zeta_1, \ldots, \zeta_d\} \subset \mathbb{K}^n$ and let $E = \{\alpha_1, \ldots, \alpha_D\} \subset \mathbb{N}^n$ such that $\mathbf{x}^E$ is a basis of $\mathcal{A}_\Lambda = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}_\Lambda$. We define the pseudo-Lagrange's polynomials $\mathbf{e}_i^{(j)}, j = 1, \ldots, \mu_i$ associated to the root ζ_i in the following way:

$$\mathbf{e}_i^{(j)} = -\frac{1}{\mathbf{v}_{\Lambda,E}} \det \begin{pmatrix} \mathbf{x}^{\alpha_1} & \cdots & \mathbf{x}^{\alpha_D} \\ \langle \Lambda_1^{(1)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_1} & \cdots & \langle \Lambda_1^{(1)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_1} \\ \vdots & & \vdots \\ \langle \Lambda_{j-1}^{(i)}, \mathbf{x}^{\alpha_i} \rangle_{\zeta_i} & \cdots & \langle \Lambda_{j-1}^{(i)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_i} \\ \langle \Lambda_{j+1}^{(i)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_1} & \cdots & \langle \Lambda_{j+1}^{(i)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_1} \\ \vdots & & \vdots \\ \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_d} & \cdots & \langle \Lambda_{\mu_d}^{(1)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_d} \end{pmatrix}.$$

For all $i \in \{1, \ldots, d\}$ and $j \in \{1, \ldots, \mu_i\}$.

Proposition 4.13. *The polynomial $\mathbf{e}_{\zeta_i}^{(1)}$ is the idempotent associated with ζ_i and $\mathbf{e}_i^{(1)}, \ldots, \mathbf{e}_i^{(\mu_i)}$ is a basis of the local ring $\mathcal{A}_{\zeta_i}$.*

Proof. We remark that

$$\langle \Lambda_j^{(i)}, \mathbf{e}_{i'}^{(j')} \rangle_{\zeta_i} = \frac{1}{\mathbf{v}_{\Lambda,E}} \det \begin{pmatrix} \langle \Lambda_j^{(i)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_i} & \cdots & \langle \Lambda_j^{(i)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_i} \\ \langle \Lambda_2^{(i)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_i} & \cdots & \langle \Lambda_2^{(i)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_i} \\ \vdots & & \vdots \\ \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_i} & \cdots & \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_i} \end{pmatrix} = \delta_{i,i'} \delta_{j,j'}.$$

Therefore the elements $\mathbf{e}_i^{(j)}$ $j = 1, \ldots, \mu_i$ are the dual basis of the basis $\Lambda_j^{(i)}$ of $\widehat{\mathcal{A}}$. Moreover, as $\mathbf{e}_i^{(1)}$ is the dual element of $\Lambda_1^{(i)} = 1$ and because $\Lambda_j^{(i)}$ $j = 2, \ldots, \mu_i$ have no

constant term, $\mathbf{e}_i^{(j)}$ are in the maximal ideal $\mathbf{m}_{\zeta_i}$ of $\mathcal{A}_{\zeta_i}$, for $j = 2, \ldots, \mu_i$. Therefore $\mathbf{e}_i^{(1)}$ is the idempotent associated with ζ_i. □

This yields the solution to the generalized Hermite interpolation problem:

PROPOSITION 4.14. *With the above assumptions and notations, for all $f \in \mathcal{A}$, we have $f = \sum_{i=1}^{d} \sum_{j=1}^{\mu_i} v_{i,j}\, \mathbf{e}_i^{(j)}$ where $\mathbf{e}_i^{(j)}$ is the polynomial of Definition* 4.12*, $v_{i,j} = \langle \Lambda_j^{(i)}, f \rangle_{\zeta_i}$, for $i = 1, \ldots, d$ and $j = 1, \ldots, \mu_i$.*

In order to completely answer the interpolation problem, we need to describe the polynomials for which the tangential condition vanishes, that is the polynomials of I_Λ. Just as for the idempotents, they will be described by determinantal expressions. Let Q be a polynomial of $\mathbb{K}[x_1, \ldots, x_n]$. We denote by $N_Q(\mathbf{x}) = \sum_{\alpha \in E} n_{Q,\alpha} \mathbf{x}^\alpha$ the normal form of the polynomial Q in the basis $\mathbf{x}^E$. We consider the polynomial $P_Q(\mathbf{x}) = Q(\mathbf{x}) - N_Q(\mathbf{x})$. Then $P_Q \in \mathcal{I}$.

DEFINITION 4.15. We define the polynomial $R_Q(Z(\mathcal{I}), \mathbf{x})$ as the following determinant:

$$R_Q(\Lambda, \mathbf{x}) = \begin{vmatrix} Q(\mathbf{x}) & \mathbf{x}^{\alpha_1} & \cdots & \mathbf{x}^{\alpha_D} \\ \langle \Lambda_1^{(1)}, Q(\mathbf{x}) \rangle_{\zeta_1} & \langle \Lambda_1^{(1)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_1} & \cdots & \langle \Lambda_1^{(1)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_1} \\ \vdots & \vdots & & \vdots \\ \langle \Lambda_{\mu_d}^{(d)}, Q(\mathbf{x}) \rangle_{\zeta_d} & \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_d} & \cdots & \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_d} \end{vmatrix}. \tag{5}$$

We check that we have the following properties:

PROPERTIES 4.16.

- $R_Q(\Lambda, \zeta_i) = 0$,
- $R_Q(\Lambda, \mathbf{x}) = \mathbf{v}_{\Lambda,E} P_Q(\mathbf{x})$.

We now define a function associated to this relation:

DEFINITION 4.17. We define the following polynomial:

$$F_Q(\Lambda, \mathbf{x}) = \frac{R_Q(\Lambda, \mathbf{x})}{\mathbf{v}_{\Lambda,E}} - P_Q(\mathbf{x}). \tag{6}$$

For all $i \in \{1, \ldots, n\}$, we denote by $\nu_i = (\delta_{i,j})_{j \in \{0,\ldots,n\}} \in \mathbb{N}^n$. Let $Q \notin \mathbb{K}[x_1, \ldots, x_n]_E$. The partial derivative functions of R_Q, relative to the coordinates of ζ_i, have a strong property that we will use hereafter.

PROPOSITION 4.18. *We have:*

$$\frac{\partial R_Q}{\partial \zeta_{i,j}}(\Lambda, \mathbf{x}) = \sum_{j=1}^{\mu_{\zeta_i}} \left\langle \Lambda_j^{(i)}, \frac{\partial R_Q}{\partial x_j}(\Lambda, \mathbf{x}) \right\rangle_{\zeta_i} \mathbf{e}_{\zeta_i}^j \in \mathcal{A}_{\zeta_i}. \tag{7}$$

PROOF. By definition of $R_Q(\Lambda, \mathbf{x})$, we have the following equality :

$$\frac{\partial R_Q}{\partial \zeta_{i,j}}(\Lambda, \mathbf{x}) = \begin{vmatrix} Q(\mathbf{x}) & \mathbf{x}^{\alpha_1} & \cdots & \mathbf{x}^{\alpha_D} \\ \langle \Lambda_1^{(1)}, Q(\mathbf{x}) \rangle_{\zeta_1} & \langle \Lambda_1^{(1)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_1} & \cdots & \langle \Lambda_1^{(1)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_1} \\ \vdots & \vdots & & \vdots \\ \langle \Lambda_1^{(i)}, \frac{\partial}{\partial \zeta_{i,j}} Q(\mathbf{x}) \rangle_{\zeta_i} & \langle \Lambda_1^{(i)}, \frac{\partial}{\partial \zeta_{i,j}} \mathbf{x}^{\alpha_1} \rangle_{\zeta_1} & \cdots & \langle \Lambda_1^{(i)}, \frac{\partial}{\partial \zeta_{i,j}} \mathbf{x}^{\alpha_D} \rangle_{\zeta_1} \\ \vdots & \vdots & & \vdots \\ \langle \Lambda_{\mu_i}^{(i)}, \frac{\partial}{\partial \zeta_{i,j}} Q(\mathbf{x}) \rangle_{\zeta_i} & \langle \Lambda_{\mu_i}^{(i)}, \frac{\partial}{\partial \zeta_{i,j}} \mathbf{x}^{\alpha_1} \rangle_{\zeta_1} & \cdots & \langle \Lambda_{\mu_i}^{(i)}, \frac{\partial}{\partial \zeta_{i,j}} \mathbf{x}^{\alpha_D} \rangle_{\zeta_1} \\ \vdots & \vdots & & \vdots \\ \langle \Lambda_{\mu_d}^{(d)}, Q(\mathbf{x}) \rangle_{\zeta_d} & \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_d} & \cdots & \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_d} \end{vmatrix}.$$

Then we remark that $\frac{\partial}{\partial \zeta_{i,j}} R_Q(\Lambda, \zeta_k) = 0$ if $k \neq i$. Then $\frac{\partial}{\partial \zeta_{i,j}} R_Q(\Lambda, \zeta_k) \in \mathcal{A}_{\zeta_i}$. □

COROLLARY 4.19. *If ζ_i is a simple root, then:*

$$\frac{\partial R_Q}{\partial \zeta_{i,j}}(\Lambda, \mathbf{x}) = \left\langle 1, \frac{\partial R_Q}{\partial x_j}(\Lambda, \mathbf{x}) \right\rangle_{\zeta_i} \mathbf{e}_{\zeta_i} = \frac{\partial R_Q}{\partial x_j}(\Lambda, \zeta_i)\, \mathbf{e}_{\zeta_i}. \tag{8}$$

4.4. RELATIONS BETWEEN ROOTS AND COEFFICIENTS

In this section, we give some relations between the coefficients of an algebraic system that defines a zero-dimensional complete intersection and the roots of the system. Those relations extend naturally the well known relations between elementary symmetric functions of the roots and the coefficients of a univariate equation.

Let $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ such that $\mathcal{I} = (f_1, \ldots, f_n)$ is a zero-dimensional complete intersection. We denote by $\mathbf{z} = \{\zeta_1, \ldots, \zeta_d\}$ the associated algebraic set and $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ its coordinate algebra. We assume that we know a monomial basis $\mathbf{x}^E$ of $\mathcal{A}$ and a basis $(\Lambda_j^{(i)})_{j \in \{1, \ldots, \mu_i\}}$ of the dual space of each local algebra $\mathcal{A}_{\zeta_i}$. Those bases are such that $\Lambda_1^{(i)} = 1$, $\forall i \in \{1, \ldots, d\}$.

Let Q be a polynomial of $\mathbb{K}[x_1, \ldots, x_n]$, we denote by $N_Q(\mathbf{x}) = \sum_{\alpha \in E} n_{Q,\alpha} \mathbf{x}^\alpha$ the normal form of Q in $\mathcal{A}$ with respect to the basis $\mathbf{x}^E$. We recall that a property of 4.16 gives $\frac{R_{f_i}(\Lambda, \mathbf{x})}{\mathbf{v}_{\Lambda,E}} = f_i(\mathbf{x})$ for all $i \in \{1, \ldots, d\}$. Let us decompose each $f_i = \sum_{\alpha \in \mathbb{N}^n} f_{i,\alpha} \mathbf{x}^\alpha$ in the following way: $f_i(\mathbf{x}) = \overline{f_i} + \sum_{\alpha \in E} f_{i,\alpha} \mathbf{x}^\alpha$ with $\overline{f_i}$ with monomial support disjoint of $\mathbf{x}^E$. We have $\frac{R_{\overline{f_i}}(\Lambda, E)}{\mathbf{v}_{\Lambda,E}} = \overline{f_i}(\mathbf{x}) - N_{\overline{f_i}}(\mathbf{x}) = f_i(\mathbf{x})$ since $N_{f_i}(\mathbf{x}) = 0$, and therefore $\sum_{\alpha \in E} f_{i,\alpha} \mathbf{x}^\alpha = N_{\overline{f_i}}$. So we deduce that $\frac{R_{\overline{f_i}}(\Lambda, \mathbf{x})}{\mathbf{v}_{\Lambda,E}} - \overline{f_i} = \sum_{\alpha \in E} f_{i,\alpha} \mathbf{x}^\alpha$.

We denote by $|R_{\overline{f_i}}(\Lambda, \mathbf{x})|_{\alpha_i}$ the minor of the matrix obtained by removing the first row and the column corresponding to $\mathbf{x}^{\alpha_i}$, $\forall i \in \{1, \ldots, D\}$. The following proposition is, now, easy to check :

THEOREM 4.20. *Let $i \in \{1, \ldots, D\}$, we have $\frac{|R_{\overline{f_i}}(\Lambda, \mathbf{x})|_{\alpha_i}}{\mathbf{v}_{\Lambda,E}} = f_{i,\alpha}$.*

The equality of this proposition generalizes the well know relation between elementary symmetric functions and coefficients of a univariate algebraic equation.

4.5. relation polynomials and interpolation

We are now interested in a variant of Hermite's interpolation problem. Given a set of points $\{\zeta_1, \ldots, \zeta_d\} \subset \mathbb{K}^n$ and tangential conditions described by $\Lambda = (\Lambda_j^{(i)}) \in \mathbb{K}[\partial]^D$, find a set of generators of I_Λ. We assume moreover that a monomial basis $\mathbf{x}^E$ of $\mathcal{A}_\Lambda$ (such that $\mathbf{v}_{\Lambda,E} \neq 0$) is given.

Definition 4.21. We denote by $\Omega = \{\beta \in \mathbb{N}^n | \exists \alpha \in E \text{ and } k \in \{1, \ldots, n\},$ $x^\beta = x_k * \mathbf{x}^\alpha \text{ and } \beta \notin E\}$. We call this set the frontier of the quotient algebra.

Proposition 4.22. *Assume that* $1 \in \mathbf{x}^E$. *Then the polynomials* $R_{\mathbf{x}^\beta}(\Lambda, \mathbf{x})$, $\beta \in \Omega$, *generate the ideal* $\mathcal{I}_\Lambda = (R_{\mathbf{x}^\beta}(\Lambda, \mathbf{x}))_{\beta \in \Omega}$.

Proof. Let us denote by I_Ω the ideal generated by the polynomials $(R_{\mathbf{x}^\beta}(\Lambda, \mathbf{x}))_{\beta \in \Omega}$ and by $\mathcal{A}_\Omega = \mathbb{K}[x_1, \ldots, x_n]/I_\Omega$. Since $\langle \Lambda_j^{(i)}, R_{\mathbf{x}^\beta}(\Lambda, \mathbf{x}) \rangle_{\zeta_i} = 0$, we have $I_\Omega \subset I_\Lambda$ and $\dim_{\mathbb{K}}(\mathcal{A}_\Lambda) \leq \dim_{\mathbb{K}}(\mathcal{A}_\Omega)$.

As for any $\mathbf{x}^\alpha \in \mathbf{x}^E$ and any variable x_i, the product $\mathbf{x}^\alpha x_i = \mathbf{x}^\beta$ is in $\mathbf{x}^\Omega$, it can be reduced modulo $R_{\mathbf{x}^\beta}(\Lambda, \mathbf{x})$ to an element of $\langle \mathbf{x}^E \rangle$. Inductively, we prove that the multiplication of any element of $\langle \mathbf{x}^E \rangle$ by any polynomial of $\mathbb{K}[x_1, \ldots, x_n]$ can be reduced modulo I_Ω to an element of $\langle \mathbf{x}^E \rangle$. Since $1 \in \mathbf{x}^E$, this induces that $\mathbf{x}^E$ is a generating set of $\mathcal{A}_\Omega$. We deduce that $\dim_{\mathbb{K}}(\mathcal{A}_\Omega) \leq \#(E) = \dim_{\mathbb{K}}(\mathcal{A}_\Lambda)$ and thus that $I_\Omega = I_\Lambda$. □

As a corollary, we deduce that I_Λ is generated by all the relations $R_p(\Lambda, \mathbf{x})$ for $p \in \mathbb{K}[x_1, \ldots, x_n]$. In the following, we are especially interested by ideals I_Λ, which can be generated by n polynomials, that is complete intersections, corresponding to square systems. The forthcoming developments are thus stated with n polynomials in n variables, but they can be extended to $m \geq n$ polynomials at the cost of dealing with rectangular linear systems.

5. Weierstrass's Method

In this section we give a generalization of Weierstrass's method for the multivariate case for a complete intersection that defines only simple roots. We construct an iteration function by a direct extension of the methodology exposed in Section 2. We do it thanks to the representation of the quotient algebra given in Sections 3 and 4. The iteration function gives a local method with a quadratic convergence. To obtain a global method, we will use this local method in a continuation process.

Hereafter $\mathcal{I} = (f_1, \ldots, f_n)$ is a complete intersection zero-dimensional ideal of $\mathbb{K}[x_1, \ldots, x_n]$ that defines only simple roots $Z(\mathcal{I}) = \{\zeta_1, \ldots, \zeta_D\}$.

Hypothesis 5.1. We assume that we know a set $E = \{\alpha_1, \ldots, \alpha_D\} \subset \mathbb{N}^n$ such that $\mathbf{x}^E$ is a monomial basis of $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$. (This can be done, for instance, by the computation of a Gröbner basis using modular arithmetic with a high probability of success.)

5.1. ITERATION FUNCTION

We begin by the construction of an equivalent system to the initial algebraic system. We define the following application:

$$\mathcal{F}: \begin{cases} \left(\mathbb{K}^n\right)^D & \longrightarrow & \left(\mathbb{K}[x_1,\ldots,x_n]_E\right)^n \\ \\ \mathbf{z} & \longmapsto & \mathcal{F}(\mathbf{z},\mathbf{x}) = \begin{pmatrix} F_{f_1} \\ \vdots \\ F_{f_n} \end{pmatrix}. \end{cases} \tag{9}$$

We can associate the equation $\mathcal{F}(\mathbf{z}) = 0$ with a system described hereafter. If we look at the polynomial $F_{f_i}(\mathbf{z},\mathbf{x}) = \frac{R_{f_i}(\mathbf{z},\mathbf{x})}{\mathbf{v}_{Z(\mathcal{I}),E}} - f_i$, we remark that its support is in $\mathbf{x}^E$, $\forall i \in \{1,\ldots,n\}$. So we have $F_{f_i}(\mathbf{z},\mathbf{x}) = \sum_{\alpha\in E} \psi_{i,\alpha}(\mathbf{z})\,\mathbf{x}^\alpha$, $\forall i \in \{1,\ldots,n\}$. Then we obtain the following square $nD \times nD$ system:

$$(\Psi) \begin{cases} \psi_{i,\alpha}(\mathbf{z}) = 0 \\ \forall i \in \{1,\ldots,n\} \text{ and } \alpha \in E. \end{cases} \tag{10}$$

By construction we have $\psi_{i,\alpha}(Z(\mathcal{I})) = 0$, $\forall i \in \{1,\ldots,n\}$ and $\alpha \in E$. System (10) is analogous to system (1) for the multivariate case. The idea is again to apply Newton's method to system (10). As in the univariate case, we will exploit the structure of the problem to explicitly inverse the Jacobian of the system and give a simple iteration function.

COMPUTATION OF THE ITERATION FUNCTION

We consider the following maps:

$$\Phi : P = \sum_{\alpha\in E} p_\alpha \mathbf{x}^\alpha \in \mathbb{K}[x_1,\ldots,x_n]_E \;\mapsto\; (p_\alpha)_{\alpha\in E} \in \mathbb{K}^D$$

$$\overrightarrow{\mathcal{F}} : \mathbf{z} \in \left(\mathbb{K}^n\right)^D \;\mapsto\; \overrightarrow{\mathcal{F}}(\mathbf{z}) = \left(\Phi(F_{f_1}),\ldots,\Phi(F_{f_n})\right) \in \left(\mathbb{K}^D\right)^n.$$

We have that $\overrightarrow{\mathcal{F}}(\mathbf{z}) = 0$ if and only if $\{\mathbf{z}_1,\ldots,\mathbf{z}_d\} = \{\zeta_1,\ldots,\zeta_d\}$.

The idea is to apply Newton's method to $\overrightarrow{\mathcal{F}}$ and to do that we need to compute the sequence of Newton's iteration points:

$$\mathbf{z}^{(k+1)} = \mathbf{z}^{(k)} - J_{\overrightarrow{\mathcal{F}}}\left(\mathbf{z}^{(k)}\right)^{-1} \overrightarrow{\mathcal{F}}(\mathbf{z}^{(k)}). \tag{11}$$

THEOREM 5.2. *In the above situation, to apply a Newton's iteration to $\overrightarrow{\mathcal{F}}$, for $i \in \{1,\ldots,D\}$, we only need to compute*

$$\mathbf{z}_i^{(k+1)} = \mathbf{z}_i^{(k)} - \begin{pmatrix} \frac{\frac{\partial R_{f_1}}{\partial x_1}(\mathbf{z}^{(k)},\,\mathbf{z}_i^{(k)})}{\mathbf{v}_{\mathbf{z}^{(k)},E}} & \cdots & \frac{\frac{\partial R_{f_1}}{\partial x_n}(\mathbf{z}^{(k)},\,\mathbf{z}_i^{(k)})}{\mathbf{v}_{\mathbf{z}^{(k)},E}} \\ \vdots & \ddots & \vdots \\ \frac{\frac{\partial R_{f_n}}{\partial x_1}(\mathbf{z}^{(k)},\,\mathbf{z}_i^{(k)})}{\mathbf{v}_{\mathbf{z}^{(k)},E}} & \cdots & \frac{\frac{\partial R_{f_n}}{\partial x_n}(\mathbf{z}^{(k)},\,\mathbf{z}_i^{(k)})}{\mathbf{v}_{\mathbf{z}^{(k)},E}} \end{pmatrix}^{-1} \begin{pmatrix} f_1(\mathbf{z}_i^{(k)}) \\ \vdots \\ f_n(\mathbf{z}_i^{(k)}) \end{pmatrix}. \tag{12}$$

And the sequence $\left(\mathbf{z}^{(k)}\right)_{k\in\mathbb{N}}$ converges quadratically in a neighbourhood of the solutions of the system.

REMARK 5.3. Because of the linearity of Φ we have $\frac{\partial}{\partial z_{i,j}}\Phi\left(F_{f_k}\left(\mathbf{z}\right)\right) = \Phi\big(\frac{\partial}{\partial z_{i,j}}F_{f_k}\left(\mathbf{z}\right)\big)$ for j and $k \in \{1,\ldots,n\}$ and $i \in \{1,\ldots,D\}$.

PROOF. Let us solve $J_{\overrightarrow{\mathcal{F}}}\left(\mathbf{z}\right)\mathbf{u} = \overrightarrow{\mathcal{F}}\left(\mathbf{z}\right)$. By Corollary 4.19, for all $k \in \{1,\ldots,n\}$ we have

$$\Phi\left(\sum_{i=1}^{D}\sum_{j=1}^{n} -\frac{\frac{\partial R_{f_k}}{\partial x_j}\left(\mathbf{z},\mathbf{z}_i\right)}{\mathbf{v}_{\mathbf{z},E}} u_{i,j}\mathbf{e}_i\left(\mathbf{z},\mathbf{x}\right)\right) = \Phi\left(\sum_{i=1}^{D} F_{f_k}\left(\mathbf{z},\mathbf{z}_i\right)\mathbf{e}_i\left(\mathbf{z},\mathbf{x}\right)\right).$$

Or equivalently

$$\sum_{i=1}^{D}\sum_{j=1}^{n} -\frac{\frac{\partial R_{f_k}}{\partial z_{i,j}}\left(\mathbf{z},\mathbf{z}_i\right)}{\mathbf{v}_{\mathbf{z},E}} u_{i,j}\mathbf{w}_i = \sum_{i=1}^{D} F_{f_k}\left(\mathbf{z},\mathbf{z}_i\right)\mathbf{w}_i.$$

So for each $i \in \{1,\ldots,D\}$, we have the following system

$$\begin{cases} \displaystyle\sum_{j=1}^{n} -\frac{\frac{\partial R_{f_k}}{\partial x_j}\left(\mathbf{z},\mathbf{z}_i\right)}{\mathbf{v}_{\mathbf{z},E}} u_{i,j} = F_{f_k}\left(\mathbf{z},\mathbf{z}_i\right) \\ \qquad\qquad \forall k \in \{1,\ldots,n\} \end{cases}. \tag{13}$$

Then for each $i \in \{1,\ldots,D\}$, we define

$$\Delta_{\mathbf{z}_i}\overrightarrow{\mathcal{F}}\left(\mathbf{z}\right) = \begin{pmatrix} -\frac{\frac{\partial R_{f_1}}{\partial x_1}\left(\mathbf{z},\mathbf{z}_i\right)}{\mathbf{v}_{\mathbf{z},E}} & \cdots & -\frac{\frac{\partial R_{f_1}}{\partial x_n}\left(\mathbf{z},\mathbf{z}_i\right)}{\mathbf{v}_{\mathbf{z},E}} \\ \vdots & \ddots & \vdots \\ -\frac{\frac{\partial R_{f_n}}{\partial x_1}\left(\mathbf{z},\mathbf{z}_i\right)}{\mathbf{v}_{\mathbf{z},E}} & \cdots & -\frac{\frac{\partial R_{f_n}}{\partial x_n}\left(\mathbf{z},\mathbf{z}_i\right)}{\mathbf{v}_{\mathbf{z},E}} \end{pmatrix}.$$

Following these definitions and since $F_{f_k}\left(\mathbf{z},\mathbf{z}_i\right) = -P_{f_k}\left(\mathbf{z}_i\right)$, system (13) can be written

$$\begin{pmatrix} u_{i,1} \\ \vdots \\ u_{i,n} \end{pmatrix} = \Delta_{\mathbf{z}_i}\overrightarrow{\mathcal{F}}\left(\mathbf{z}\right)^{-1}\begin{pmatrix} f_1\left(\mathbf{z},\mathbf{z}_i\right) \\ \vdots \\ f_n\left(\mathbf{z},\mathbf{z}_i\right) \end{pmatrix}.$$

The formula of the theorem is proved. The convergence of the method comes from the fact that this method is equivalent to Newton's method and that all roots are assumed to be simple. □

REMARK 5.4. If there is only one root to the system, then formula (12) is the Newton's iteration formula, and if there is only one variable, formula (12) is the formula of the classical Weierstrass's method (2).

5.2. ALGORITHM AND ARITHMETIC COMPLEXITY

Recall that we assume to know a monomial basis of the $\mathbb{K}$-vector space $\mathcal{A}$ and the normal forms in this basis of n polynomials that are not in this basis. We use the notations of the preceding subsections.

ALGORITHM

The starting points are given thanks to a matrix $\mathbf{z}$ that has its columns equal to the vector of the coordinates of the starting points.

Algorithm 5.5. (Weierstrass's iteration)

- *Input: The matrix* $\mathbf{z}$ *formed with the coordinates of the initial points.*
- *Step 1. We compute the matrices (specialized at* $\mathbf{z}$*)*

$$MV_E(\mathbf{z}) = \begin{pmatrix} \mathbf{z}_1^{\alpha_1} & \dots & \mathbf{z}_1^{\alpha_D} \\ \vdots & \ddots & \vdots \\ \mathbf{z}_D^{\alpha_1} & \dots & \mathbf{z}_D^{\alpha_D} \end{pmatrix},$$

$$MR_{f_k}(\mathbf{z}, \mathbf{x}) = \begin{pmatrix} \mathbf{z}_1^{\alpha_1} & \dots & \mathbf{z}_1^{\alpha_D} & f_1(\mathbf{z}_1) \\ \vdots & \ddots & \vdots & \vdots \\ \mathbf{z}_D^{\alpha_1} & \dots & \mathbf{z}_D^{\alpha_D} & f_n(\mathbf{z}_D) \end{pmatrix}$$

for $k = 1, \dots, n$*. After we compute the rows:*

$$dv_{f_k}^{(i)}(\mathbf{x}) = \left(\frac{\partial}{\partial x_i} x^{\alpha_1}, \dots, \frac{\partial}{\partial x_i} x^{\alpha_D}, \frac{\partial}{\partial x_i} f_k(\mathbf{x}) \right)$$

for $i \in \{1, \dots, n\}$ *and* $k \in \{1, \dots, n\}$*.*
- *Step 2. Make the LU-decomposition of* $MV_E(\mathbf{z})$*. Use it to compute the kernels of the matrices* MR_{f_k}*. This gives us the vectors* $r_{f_k} \in \mathbb{K}^{D+1}$*, for each* $i \in \{1, \dots, n\}$*. If the dimension of the kernel of* $MV_E(\mathbf{z})$ *does not vanish, stop the algorithm with an error setting.*
- *Step 3. For each* $i \in \{1, \dots, D\}$*, we construct the matrices* $\Delta_{\mathbf{z}_i} \overrightarrow{\mathcal{F}}(\mathbf{z})$ *by computing their coefficients as follows: we specialize* $dv_{f_k}^{(i)}$ *at* $\mathbf{z}_i$*, compute its product with* $r_{\beta_k}(\mathbf{z})$ *and normalize it by its last coefficient (that is the value of the pseudo-Vandermonde determinant), for each* $k \in \{1, \dots, n\}$*. Then we obtain:* $\Delta_{\mathbf{z}_i} \overrightarrow{\mathcal{F}}(\mathbf{z})$*.*
- *Step 4. For each* $i \in \{1, \dots, D\}$ *we solve the system*

$$(f_1(\mathbf{z}_i), \dots, f_n(\mathbf{z}_i))^t = \Delta_{\mathbf{z}_i} \overrightarrow{\mathcal{F}}(\mathbf{z})\, \mathbf{z}'_i,$$

where $\mathbf{z}'_i$ *is the column indexed by* i *of the output matrix.*
- *Output: The matrix* $\mathbf{z}'$*.*

arithmetic complexity for an iteration

Proposition 5.6. *The arithmetic complexity of an iteration of Algorithm* 5.5 *is bounded by* $\mathcal{O}\left(D^3 + n^2D^2 + Dn^3\right)$ *arithmetic operations.*

Proof. We detail here the cost of the different steps:

- In step 1, we start making n specializations of $D \times (D+1)$, which gives us $\mathcal{O}\left(nD^2\right)$ arithmetic operations.
- In steps 2 and 3, we compute the LU-decomposition the matrix $MV_E(\mathbf{z})$. This yields the complexity bound of $\mathcal{O}(D^3)$. Finally we use this decomposition to compute the kernels of the n matrices MR_{f_k}, this costs $\mathcal{O}(nD^2)$ arithmetic operations. We specialize nD vectors of length $D+1$, which gives a $\mathcal{O}(nD^2)$ complexity. After, we compute n^2D inner products of vectors of length $D+1$, and we obtain a complexity term $\mathcal{O}(n^2D^2)$.

- In step 4, we specialize D vectors of length n. It gives us a complexity $\mathcal{O}(nD)$. We solve D linear systems of size $n \times n$, this costs $\mathcal{O}(Dn^3)$ arithmetic operations. Finally we compute n products of $n \times n$ matrices by vectors and we have a complexity $\mathcal{O}(n^2)$. If we denote by L the maximal cost of the evaluation of a P_{f_k} there is also a contribution in $\mathcal{O}(nL)$ arithmetic operations, but this contribution is marginal.

With all these elements we obtain a $\mathcal{O}\left(D^3 + n^2D^2 + Dn^3\right)$ arithmetic complexity. □

Remark 5.7. In step 2, we do not use the pseudo-Vandermonde's structure of the matrices $MV_E(\mathbf{z})$. However the use of this structure could give a better complexity. We refer to Mourrain and Pan (2000) for the use of the matrix structure for solving systems.

5.3. weierstrass's iteration with continuation

Hereafter we use the Weierstrass's iteration function as "predictor-corrector" in a path following method (see Allgower and Georg, 1990). We propose an analogy of a "global Newton's method" to approximate all (or a subset of) the roots of an algebraic system. The method proposed here is derived from the work exposed in Dedieu and Smale (1998) and Smale (1997). In those paper the complexity of the global Newton's method is studied in the BCSS model approach (see Blum *et al.*, 1998, 1989). Supplementary difficulties occur.

Let $g_1, \ldots, g_n \in \mathbb{K}[x_1, \ldots, x_n]$, we define a polynomial (resp. rational) homotopy from $g_1, \ldots, g_n$ to $f_1, \ldots, f_n$ as a function $\mathcal{H} \in \mathbb{K}[x_1, \ldots, x_n][t]^n$ (resp. $\mathbb{K}[x_1, \ldots, x_n](t)^n$) such that $\mathcal{H}(0) = (g_1, \ldots, g_n)$ and $\mathcal{H}(1) = (f_1, \ldots, f_n)$. To each $t \in [0, 1]$ we associate an algebra $\mathcal{A}_t = \mathbb{K}[x_1, \ldots, x_n]/(\mathcal{H}(t))$. We say that the homotopy is flat on $[0, 1]$ if $\mathcal{A}_t \cong \mathcal{A}_{t'}$ for all t and $t' \in [0, 1]$ as $\mathbb{K}$-vector space. Flatness is difficult to show. A major problem in our setting is that the number of roots can change (i.e. the dimension of $\mathcal{A}_t$ changes with t). This difficulty can be handled by considering an additional equation f_{n+1} but leads to the treatment of a rectangular system. We do not describe these developments here and will consider hereafter only one-parameter families of polynomials for which the dimension of $\mathcal{A}_t$ is not changing. Let $\mathbf{z}^{(0)} \in (\mathbb{K}^n)^D$, we choose $g_1(x) = R_{f_1}(\mathbf{z}^{(0)}, \mathbf{x}), \ldots, g_1(x) = R_{f_n}(\mathbf{z}^{(0)}, \mathbf{x})$ and $\mathcal{H}(t) = t(f_1, \ldots, f_n) + (1 - t)(g_1, \ldots, g_n)$. Then we propose the following algorithm:

Algorithm 5.8.

- *Input:* Δt, $\mathbf{z}^{(0)}$.
- *For i from 1 to* $\frac{1}{\Delta t}$ *do* $\mathbf{z}^{(i)} = Weierstrass\left(\mathcal{H}(i\Delta t), \mathbf{z}^{(i-1)}\right)$.
- *Return* $\mathbf{z}^{\left(\frac{1}{\Delta t}\right)}$.

Here the function $Weierstrass$ is the iteration function of the multivariate Weierstrass method of the previous algorithm. But flatness is not guaranteed, unless the whole system reaches the Bézout bound. So we restrict our study to systems with the maximal number of roots or to systems with structural properties easy to check.

Remarks 5.9.

- If we have only one root, this algorithm is Newton's method with continuation, just as defined in Smale (1997).

- The singular locus for this method is given by the vanishing locus of the Vandermonde determinant. This is a complex algebraic variety of codimension 1 in complex space, i.e. of codimension 2 as a real variety. The continuation method uses a one-dimensional real path. Then, starting from a random initial system insures that the path will not meet the singular locus, with a high probability.
- An alternative way to insure the flatness is to use overconstrained systems by introducing a supplementary algebraic equation to control the structure of all the systems. Overconstrained systems can be treated using Weierstrass's method by modifying the iteration function. This leads to several new problems and developments which are the objects of current work.

6. Experiments

6.1. implementation

We have implemented those algorithms in C^{++} using the tools available in the SYNAPS library. The library SYNAPS is a set of C^{++} template functions for scientific computation with polynomial and linear algebra. All our functions only use double-precision floating point arithmetic (or complex numbers using this arithmetic). But adaptations to several other arithmetics are possible.

The continuation algorithm begins by a step of interpolation. This is done by interpolation using relation polynomials from random points. The interpolation process is very efficient and does not limit the method. So we focus on the approximation step. Furthermore, for implementation reasons, we are particularly interested in the use of the double-precision floating point arithmetic. We just make a few remarks on the use of extended arithmetic. The symbol ∞ is used when the results are not significant.

6.2. numerical experiences of Weierstrass's method

The aim is to study the impact of the two following parameters:

- the number of steps made during the continuation (denoted by nbstep hereafter)
- the number of Weierstrass's iterations made at each step of the continuation (denoted nbiter hereafter).

Experience reveals other basic facts on the behaviour of the proposed methods. The time is given in seconds and the accuracy (denoted prec) is evaluate by the norm of the vector form by the evaluations of polynomials of the system evaluated at the approximations given by the algorithm (backward error).

intersections of quadrics

We compute an approximation of the eight roots of a system consisting of three generic quadrics in 3 variables.

nbiter	10		7		5		3	
nbstep	time	prec	time	prec	time	prec	time	prec
55	0.15	10^{-21}	0.1	10^{-22}	0.05	10^{-18}	0.04	10
60	0.18	10^{-21}	0.12	10^{-22}	0.08	10^{-20}	0.05	1
75	0.2	10^{-22}	0.15	10^{-22}	0.12	10^{-22}	0.08	10^{-1}
100	0.2	10^{-22}	0.17	10^{-22}	0.15	10^{-22}	0.09	10^{-2}

We compute an approximations of the 24 roots of a system consisting of four generic quadrics in four variables. We treat two different problems to illustrate the impact of the conditioning of the roots.

nbiter	5		3	
nbstep	time	prec	time	prec
First problem				
300	7	10^{-21}	4	10^{-10}
250	6	10^{-22}	3	10^{-12}
Second problem				
200	4	10^{-7}	3	10^{-1}
300	6	10^{-9}	5	10^{-2}
400	8	10^{-9}	6	10^{-2}

We remark that we do not lose much accuracy when we reduce the number of steps, but, for instance, here we need to keep an accuracy of 10^{-10} at least to converge globally. So we are not able to make less than 250 steps in the considered problem.

INTERSECTION OF A CUBIC WITH QUADRICS

We compute approximations of the 12 roots of a system consisting of two generic quadrics and a cubic in three variables. We treat two different examples with different conditioning of the roots.

nbiter	10		7		5	
nbstep	time	prec	time	prec	time	prec
First problem						
10	0.7	10^{-17}	0.4	10^{-17}	∞	∞
25	1.2	10^{-17}	0.7	10^{-17}	∞	∞
50	1.9	10^{-17}	1	10^{-17}	0.9	10^{-16}
100	5	10^{-18}	1.7	10^{-18}	1.5	10^{-18}
Second problem						
20	0.5	10^{-19}	0.4	10^{-20}	0.1	10^{-18}
30	0.6	10^{-20}	0.5	10^{-20}	0.1	10^{-19}

INTERSECTIONS OF THREE CUBICS

We compute the approximations of the 27 roots of a system consisting of three generic cubics in three variables. We treat an algebraic set including a disc centred at the origin and with a radius of 10 to control the size of the Vandermonde determinant. The method is sometimes faster than with less roots because, in the previous tests, the roots can have very large and very small coordinates. Here the problem has good properties.

nbiter	10		7		5		3	
nbstep	time	prec	time	prec	time	prec	time	prec
10	1	10^{-14}	0.2	10^{-14}	0.1	10^{-1}	∞	∞
20	2	10^{-17}	0.5	10^{-15}	0.1	10^{-4}	∞	∞
30	3	10^{-17}	0.8	10^{-17}	0.2	10^{-17}	0.1	10^{-8}

6.3. OTHER EXPERIMENTS

We also treat systems formed by three cubics and a quadric (54 solutions) and some particular instance of the problem of the Stewart's platform. But we reach here the limits of the method using only double-precision floating point arithmetic. For instance, for the Stewart's platform, we compute all roots. The real roots are good conditioned but some of the complex roots are huge and the Vandermonde determinant overflows the arithmetic.

A first implementation with extended arithmetic was done and allows us to treat bigger problems but it needs to be improved.

6.4. CONCLUSIONS OF EXPERIMENTS

The experiments show the efficiency of the proposed method. Some great improvements are possible. For instance, we can control the size of the step and the needed precision dynamically during the execution. Another possible improvement is to change the representation of the quotient algebra. In the present work, we use a generalization of Lagrange's polynomials by using idempotents. We imagine that the use of a generalization of Newton's polynomials will have better numerical properties.

The results exposed here and the possibility of improvements show the interest of the proposed method.

7. Conclusion

In this paper we describe an algebraic framework for the representation of zero-dimensional complete intersection algebraic systems. We give some interpolation formulæ that allow us to develop an iterative method to approximate simultaneously all roots of an algebraic system. We cite experiments that show the efficiency of the method.

Acknowledgements

We would like to specially thank J.-C. Yackoubsohn and A.-M. Bellido for interesting discussions.

References

Aberth, O. (1973). Iteration methods for finding all zeros of a polynomial simultaneously. *Math. Comput.*, **27**, 339–344.

Allgower, E. L., Georg, K. (1990). *Numerical Path Following*, Springer.

Atiyah, M., MacDonald, I. (1969). *Introduction to Commutative Algebra*, Addison-Wesley.

Bellido, A.-M. (1992). Construction de fonctions d'itération pour le calcul simultané des solutions d'équations et de systèmes d'équations algébriques. Ph.D. Thesis, Université Paul Sabatier de Toulouse.

Bellido, A.-M. (1994). Construction of iteration functions for the simultaneous computation of the solutions of equations and algebraic systems. *Numer. Algorithms*, **6**, 313–351.

Bini, D. (1996). Numerical computation of polynomial zeros by means of Aberth's method. *Numer. Algorithms*, **13**, 179–200.

Blum, L., Crucker, F., Shub, M., Smale, S. (1998). *Complexity and Real Computation*, Springer.

Blum, L., Shub, M., Smale, S. (July 1989). On a theory of computation and complexity over the real numbers: Np-completeness, recursive functions and universal machines. *Bull. Am. Math. Soc.*, **21**, 1–46.

Cox, D., Little, J., O'Shea, D. (1992). *Ideals, Varieties, and Algorithms: An Introduction to ComputationalAlgebraic Geometry and Commutative Algebra*, *Undergraduate Texts in Mathematics*, New York, Springer.

de Boor, C., Ron, A. (1990). On multivariate polynomial interpolation. *Constructive Approximation*, **6**, 287–302.

Dedieu, J.-P., Smale, S. (1998). Some lower bounds for the complexity of continuation methods. *J. Complexity*, **14**, 454–465.

Durand, E. (1960). *Solutions Numériques des Equations Algébriques*. Paris, Masson.

Elkadi, M., Mourrain, B. (2002). Géométrie algébrique effective en dimension 0. Notes de cours, Univ. de Nice.

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

Faugère, J. (1999). A new efficient algorithm for computing Gröbner Basis (F4). *J. Pure Appl. Algebra*, **139**, 61–88.

Fortune, S. (2001). Polynomial root finding using iterated eigenvalue computation. In Mourrain, B. ed., *Proceedings of ISSAC*, pp. 121–128. New York, ACM Press.

Frommer, A. (1988). A unified approach to methods for the simultaneous computation of all zeros of generalized polynomials. *Numer. Math.*, **54**, 105–116.

Huber, B., Sturmfels, B. (1995). A polyhedral method for solving sparse polynomial systems. *Math. Comput.*, **64**, 1542–1555.

Kerner, I. (1966). Ein Gesamtschrittverfahrenzur Berechnung der Nullstellen vonPolynomen. *Numer. Math.*, **8**, 290–294.

Lascoux, A. (2001). Note on interpolation in one and several variables. http://schubert.univ-mlv.fr/ al/.

Li, T. (1997). Numerical solution of multivariate polynomial systems by homotopycontinuation methods. *Acta Numerica*, **6**, 399–436.

Lorentz, G., Lorentz, R. (1990). Bivariate hermite interpolation and application to algebraic geometry. *Numerish Mathematik*, **57**, 669–680.

Macaulay, F. (1916). *The Algebraic Theory of Modular Systems*, Cambridge University Press.

Mourrain, B. (1996). Isolated points, duality and residues. *J. Pure Appl. Algebra*, **117 & 118**, 469–493. Special issue for the Proceedings of the 4th Int. Symp. on Effective Methods in Algebraic Geometry (MEGA).

Mourrain, B., Pan, V. Y. (2000). Multivariate polynomials, duality and structured matrices. *J. Complexity*, **16**, 110–180.

Mourrain, B., Trébuchet, P. (2000). Solving projective complete intersection faster. In Traverso, C. ed., *Proceedings of International Symposium on Symbolic and AlgebraicComputation*, pp. 231–238. New York, ACM Press.

Pan, V. (1997). Solving a polynomial equation: some history and recent progress. *SIAM Rev.*, **39**, 187–220.

Ruatta, O. (2001). A multivariate Weierstrass iterative rootfinder. In Mourrain, B. ed., *Proceedings of Annual ACM International Symposium on Symbolic andAlgebraic Computation*, pp. 276–283. New York, ACM Press.

Sendov, B., Andreev, A., Kjusrkiev, N. (1994). *Handbook of Numerical Analysis*, volume 3, Elsevier, Chap. Numerical solution of polynomial equation, pp. 628–777. Solution of Equations in $\mathbb{R}^n$ (part 2).

Smale, S. (1997). Complexity theory and numerical analysis. *Acta Numerica*, **6**, 523–551.

Vasconcelos, W. (1998). *Computational Methods in Commutative Algebra and Algebraic Geometry,*volume 2 of *Algorithms and Computation in Mathematics*, Springer.

Verschelde, J., Verlinden, P., Cools, R. (1994). Homotopies exploiting Newton polytopes for solving sparse polynomialsystems. *SIAM J. Numer. Anal.*, **31**, 915–930.

Weierstrass, K. (1903). Neuer Beweis des Satzes, dass Jede Ganze Rationale Function einer Veränderlichen Dargestellt werden kann als ein Productaus Linearen Functionen derselben Veränderlichen. *Mathematische Werke*, Tome 3.
Yakoubsohn, J.-C. (2000). Finding a cluster of zeros of univariate polynomials. Complexity theory, real machines, and homotopy. *J. Complexity*, **16**, 603–638.

Received 14 November 2001
Accepted 27 February 2002