Fast computation of discrete invariants associated to a differential rational mapping

Guillermo Matera, Alexandre Sedoglavic

Fast computation of discrete invariants associated to a differential rational mapping

G. Matera [a,b,*,1] A. Sedoglavic [c]

[a] *Instituto de Desarrollo Humano, Universidad Nacional de General Sarmiento, Campus Universitario, José M. Gutiérrez 1150 (1613) Los Polvorines, Pcia. de Buenos Aires, Argentina.*

[b] *Member of the National Council of Science and Technology (CONICET), Argentina.*

[c] *LIFL, Université Lille I, F-59655 Villeneuve d'Ascq CEDEX France.*

Abstract

We exhibit probabilistic algorithms which compute the differentiation index, the differential Hilbert function and an algebraic parametric set associated to a differential rational mapping. These algorithms are based on a process of linearization and specialization in a generic solution, and have polynomial time complexity.

Key words: Differential rational mapping, discrete invariants, Kähler differentials, probabilistic algorithm, straight–line program.
1991 MSC: 12H05, 13N10, 68W30.

1 Introduction

Let k be a field and let $x_1, \ldots, x_n$ be (ordinary) differential indeterminates over k, depending on a single variable t. For $1 \leq i \leq n$, let $\dot{x}_i$ denote the first derivative of the differential indeterminate x_i with respect to the variable t. Let be given rational functions $f_1, \ldots, f_n$ of $k(X, \dot{X}) := k(x_1, \ldots, x_n, \dot{x}_1, \ldots, \dot{x}_n)$ which are differentially algebraically independent over k, and suppose that we

* Corresponding author.
Email addresses: gmatera@ungs.edu.ar (G. Matera), Alexandre.Sedoglavic@lifl.fr (A. Sedoglavic).

[1] Research was partially supported by the following Argentinian grants: UBACyT X198, PIP CONICET 2461, UNGS 30/3003.

want to *solve* the following system of (ordinary) algebraic–differential equations:

$$\begin{cases} f_1(X, \dot{X}) = 0, \\ \qquad\quad \vdots \\ f_n(X, \dot{X}) = 0. \end{cases} \tag{1}$$

If the Jacobian determinant $J_F := \det \partial(f_1, \ldots, f_n)/\partial(\dot{x}_1, \ldots, \dot{x}_n)$ is a nonzero element of $k(X, \dot{X})$, then the implicit function theorem allows us to locally rewrite system (1) into the following *explicit* equivalent form:

$$\begin{cases} \dot{x}_1 = \widetilde{f}_1(X), \\ \quad \vdots \\ \dot{x}_n = \widetilde{f}_n(X), \end{cases} \tag{2}$$

where $\widetilde{f}_1, \ldots, \widetilde{f}_n$ are analytic functions. In such a case, given a suitable value t_0 in k, and a suitable set of initial conditions $\{x_i(t_0); 1 \leq i \leq n\}$, the (unique) solution $(\varphi_1, \ldots, \varphi_n)$ of system (1) satisfying $\varphi_i(t_0) = x_i(t_0)$ for $1 \leq i \leq n$, can be numerically approximated in a neighborhood of t_0. We call such a process a *numerical integration* of system (1).

On the other hand, if the Jacobian determinant J_F is the zero rational function in $k(X, \dot{X})$, then the implicit function theorem cannot be applied in order to obtain an explicit system (2), which is locally equivalent to our input system (1). In such a case, system (1) is called *implicit*, and several difficulties arise in the process of its numerical integration (see e.g. (Brenan et al., 1989)).

In order to numerically integrate system (1) in the implicit case, it is necessary to know certain *discrete* information. In particular, it is necessary to know the *differentiation index* of system (1), which may be roughly described as the minimal number ν of derivatives of the rational functions $f_1, \ldots, f_n$ needed to (locally) obtain an equivalent explicit form of system (1) (see (Campbell and Gear, 1995), (Fliess et al., 1995b) and Section 3.3), and to describe the variety of *constraints*, i.e. the algebraic equations satisfied by the variables $x_1, \ldots, x_n$.

Furthermore, it is also necessary to know a maximal subset $\mathcal{C}$ of the set of derivatives $\Theta_\nu X := \{x_i^{(j)}; 1 \leq i \leq n,\ 0 \leq j \leq \nu\}$ whose initial conditions must be fixed in order to (locally) assure existence and uniqueness of solutions of system (1). We call such a set an *algebraic parametric set* of system (1).

In order to obtain these informations, one may consider a *generic* perturbation of system (1) (compare with (Campbell and Gear, 1995), (Fliess et al., 1995b)):

$$\begin{cases} f_1(X, \dot{X}) = y_1, \\ \qquad\qquad \vdots \\ f_n(X, \dot{X}) = y_n, \end{cases} \tag{3}$$

where the right–hand side terms of the equations defining system (1) are replaced by a set of ordinary differential indeterminates $y_1, \ldots, y_n$ over $k(X, \dot{X})$. Under the assumption of certain *well–posedness* condition (cf. (Fliess et al., 1995b)), it turns out that the discrete invariants associated to system (1) mentioned above can be easily extracted from system (3).

Example. The following system (taken from (Fliess et al., 1995a)):

$$\begin{cases} x_1 = y_1, \\ \dot{x}_1 + x_2 = y_2, \\ \qquad\vdots \\ \dot{x}_{n-2} + x_{n-1} = y_{n-1}, \\ \dot{x}_n + \dot{x}_{n-1} = y_n, \end{cases} \tag{4}$$

can be easily rewritten as a vector field

$$\dot{x}_n = y_n - \dot{y}_{n-1} + \ldots + (-1)^n y_1^{(n-1)},$$

on the *constraint* variety defined by the following equations:

$$\begin{cases} x_1 &= y_1, \\ x_2 &= y_2 - \dot{y}_1, \\ &\vdots \\ x_{n-1} &= y_{n-1} - \dot{y}_{n-2} + \ldots + (-1)^{n-2}\, y_1^{(n-2)}. \end{cases}$$

We conclude that the differentiation index of system (4) is $n-1$, the initial condition on the variable x_n can be arbitrarily fixed, and the quantities $x_1, \ldots, x_{n-1}$ and $\dot{x}_n$ depend algebraically on the variables $y_1, \ldots, y_n$ and their derivatives.

Related work. This discrete information is usually determined by a process of *completion*, which computes the variety of constraints associated to system (3) by applying successive steps of formal differentiation and elimination

to the input equations. A completion can be performed by applying a symbolic algorithm, based on the computation of a Gröbner basis or a triangular set, such as the Rosenfeld–Gröbner algorithm (see e.g. (Boulier et al., 1995), (Hubert, 2000)), or the rewriting algorithms of Mansfield (1991), Maârouf et al. (1998), Sadik (2000), Reid et al. (2001), Hausdorf and Seiler (2002). As shown in (Sadik, 2000), these algorithms have exponential complexity if differential polynomials are encoding using the usual dense representation model. On the other hand, a numeric–symbolic algorithm which computes the completion using the straight–line program representation of polynomials was proposed in (Reid et al., 2002).

Main contribution. In this article, we adopt a different point of view, which consists in determining the *discrete* information mentioned above, *without* computing the completion of system (3). More precisely, we shall exhibit *probabilistic polynomial–time* algorithms that determine the following data:

- the differentiation index of system (3),
- the differential Hilbert function associated to system (3),
- an algebraic parametric set of system (3).

These algorithms take as input a straight–line program of length $\mathcal{L}$ computing the input rational functions $f_1, \ldots, f_n$, and compute the above mentioned data with time complexity $\mathcal{L}n^{O(1)}$ (see Section 5).

Our algorithms are of *Monte Carlo* or *BPP* type (see e.g. (Balcázar et al., 1988), (Zippel, 1993), (Pardo, 1995), (von zur Gathen and Gerhard, 1999)) i.e. they return the correct output with a probability of at least a fixed value strictly greater than 1/2. This means that the error probability can be made arbitrarily small by iteration of the algorithms. On the other hand, our algorithms do not seem to be of *Las Vegas* or *ZPP* type i.e. we have no means of checking the correctness of our output results. Let us observe that the probabilistic aspect of our algorithms is related to the random choice of a certain point outside a Zariski closed subset of suitable affine space, which is explicitly estimated.

Outline of the paper. This paper gives detailed proofs of the results presented in the conference paper (Matera and Sedoglavic, 2002). Furthermore, we extend these contributions by estimating the probability of success of our algorithms. Our approach is based on a linearization process that reduces our problems to the determination of the dimension of certain $\mathcal{F}$–vector spaces of Kähler differentials (see Section 4), where $\mathcal{F}$ is the function field of the solution set of system (3). These $\mathcal{F}$–vector spaces are described as the cokernel of certain Jacobian matrices, which can be easily obtained from the input polynomials. Therefore, their dimensions can be expressed in terms of the ranks over $\mathcal{F}$ of the corresponding Jacobian matrices (see Theorems 10, 11 and 12).

In order to compute the $\mathcal{F}$–rank of these Jacobian matrices, we describe the solution set of system (3) as the Zariski closure of the graph of the differential rational mapping defined by the rational functions $f_1, \ldots, f_n$ (see Section 3). Applying techniques of Ollivier (1990), we shall obtain an explicit generic point η of this graph. Taking into account that the rank of these Jacobian matrices does not change by evaluation of the variables $X, \dot{X}$ into the generic point η, we obtain an efficient algorithm computing these ranks.

Let us finally remark that our approach makes an essential use of the (strong) hypothesis of the differentially algebraically independence of the input rational functions $f_1, \ldots, f_n$. Therefore, it cannot be easily generalized to more general situations. On the other hand, our approach can be extended with minor changes to any system of ordinary algebraic–differential equations defined by n differentially algebraically independent rational functions $f_1, \ldots, f_n$ of $k(X, \ldots, X^{(e)})$ of arbitrary order e.

2 Notions and notations

Let us recall some standard notions and notations of differential algebra and differential algebraic geometry, which can be found in e.g. (Ritt, 1950) and (Kolchin, 1973). Let k be a field of characteristic zero, which we think "effective" with respect to addition, subtraction, multiplication and division. Let $x_1, \ldots, x_n$ be a set of indeterminates over k, and let $X := (x_1, \ldots, x_n)$. The *differential k–algebra* $k\{X\}$ is defined as the k–algebra of (differential) polynomials in an infinite set of indeterminates

$$\Theta X := \left\{ x_j^{(i)}; 1 \leq j \leq n,\, i \geq 0 \right\},$$

equipped with the k–derivation δ defined by the rule $\delta x_j^{(i)} = x_j^{(i+1)}$ for $i \geq 0$ and $1 \leq j \leq n$. We shall use the classical notation $\dot{u} := \delta u$ and $u^{(i)} := \delta^i u$. Further, for any $\ell \geq 0$, we shall frequently use the notation

$$\Theta_\ell X := \left\{ x_j^{(i)} \,; 1 \leq j \leq n,\, 0 \leq i \leq \ell \right\}.$$

We observe that $k\{X\}$ is an integral domain. Its *differential fraction field* $k\langle X \rangle$ is defined as the fraction field of the k–algebra $k\{X\}$, equipped with the derivation provided by the (unique) extension of the derivation δ (which we also denote δ). A *differential ideal* of the differential k–algebra $k\{X\}$ is an (algebraic) ideal of the k–algebra $k\{X\}$ which is closed under derivation. Given a subset P of $k\{X\}$, we define the *differential ideal* $[P]$ *generated by* P as the minimal differential ideal of $k\{X\}$ containing the set P.

2.1 Differential Hilbert function: dimension, order and regularity

Let $\mathcal{I}$ be a prime differential ideal of $k\{X\}$. We define the *differential Hilbert function* $\mathcal{H}_k : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ of the ideal $\mathcal{I}$ (with respect to k) as follows: for any positive integer i, we define $\mathcal{H}_k(i)$ as the Krull dimension of the (algebraic) ideal $\mathcal{I} \cap k[\Theta_i X]$. The following result shows that this function has a similar behavior as the standard Hilbert function of algebraic geometry (see (Kolchin, 1973, Chapter II, Theorem 6)).

Theorem 1 *Let $\mathcal{I}$ be a prime differential ideal of $k\{X\}$ and let $\mathcal{H}_k$ be the differential Hilbert function of $\mathcal{I}$ with respect to k. Then there exists positive integers $\dim_k \mathcal{I}$ and $\operatorname{ord}_k \mathcal{I}$ with the following property: for $i \geq 0$ large enough, we have the identity*

$$\mathcal{H}_k(i) = \dim_k \mathcal{I} \cdot (i+1) + \operatorname{ord}_k \mathcal{I}. \tag{5}$$

The integers $\dim_k \mathcal{I}$ and $\operatorname{ord}_k \mathcal{I}$ are invariants associated to the ideal $\mathcal{I}$, called the *dimension* and the *order* of $\mathcal{I}$ with respect to k, respectively. According to Ritt (1950), these invariants correspond to what are classically known as the number of arbitrary functions and the number of initial conditions in the solution set of the ordinary differential system associated to the ideal $\mathcal{I}$. For example, if $\mathcal{I}$ is the differential ideal generated by $\dot{y} - x$ then $\dim_k \mathcal{I} = 1$ and $\operatorname{ord}_k \mathcal{I} = 1$. Observe that these notions are strongly dependent on the ground field k, namely $\dim_{k\langle Y\rangle} \mathcal{I} = 0$ and $\operatorname{ord}_{k\langle Y\rangle} \mathcal{I} = 0$.

The least integer ℓ such that the identity (5) holds for any $i \geq \ell$ is called the *regularity* of the differential Hilbert function $\mathcal{H}_k$.

2.2 Generic zeros

Let $\mathcal{I}$ be a prime differential ideal of $k\{X\}$ and let K denote the fraction field of the quotient ring $k\{X\}/\mathcal{I}$. Then K, equipped with the derivation induced by δ, is a differential field. An element η of K^n is called a *generic zero* of the ideal $\mathcal{I}$ if the identity $\mathcal{I} = \{p \in k\{X\}; p(\eta) = 0\}$ holds.

For example, the formal power series $\eta := \sum_{i\geq 0} (-1)^i \, {x_0}^{i+1} t^i$ is a generic zero of the prime differential ideal $[\dot{x} + x^2]$ in $k\{x\}$, while $\eta := 0$ is not.

Finally, let $\eta = (\eta_1, \ldots, \eta_n)$ be the element of K^n whose j–th coordinate η_j is the quotient class of K defined by x_j. Then η is a generic zero of the ideal $\mathcal{I}$.

2.3 Rankings: orderly and elimination rankings, characteristic sets

A *ranking* over $k\{X\}$ is a total order $\geq$ on the set ΘX such that $\dot{u} \geq u$ holds for any u in ΘX. A ranking over $k\{X\}$ is an *orderly ranking* if $x_i^{(r)} \geq x_j^{(s)}$ holds whenever $r \geq s$ holds. Let X_1, X_2 be two subsets of X such that $X_1 \cup X_2 = X$ holds. Suppose that the algebras $k\{X_1\}$ and $k\{X_2\}$ are endowed with two rankings. The *elimination ranking* $X_1 \ll X_2$ induced by the given rankings over $k\{X_1\}$ and $k\{X_2\}$ is the ranking over $k\{X\}$ that extends the rankings over $k\{X_1\}$ and $k\{X_2\}$ and satisfies $z_1 \leq z_2$ for any z_1 in ΘX_1 and any z_2 in ΘX_2.

Let us fix a ranking over $k\{X\}$. For a given element p of $k\{X\}$, we define the *leader* u_p and the *initial* i_p of p as the highest ranking derivative appearing in p and the coefficient of its highest power in p respectively. The *separant* s_p of p is defined as $s_p := \partial p / \partial u_p$. A differential polynomial q in $k\{X\}$ is *reduced with respect to* p if no proper derivative of u_p appears in q and the condition $\deg_{u_p} q < \deg_{u_p} p$ holds.

Let us fix a subset A of $k\{X\}$. We shall denote by I_A and S_A the set of initials and separants of the elements of A respectively. Let $H_A := I_A \cup S_A$. The set A is an *autoreduced set* if any element p of A is reduced with respect to all the elements of $A \setminus \{p\}$. The set A is called a *characteristic set* of a differential ideal $\mathcal{I}$ of $k\{X\}$ if it is autoreduced and there is no nonzero element p in $\mathcal{I}$ reduced with respect to A.

3 Differential ideals associated to a differential rational mapping

Let $p_1, q_1, \ldots, p_n, q_n$ be polynomials in $k[X, \dot{X}]$ such that p_j/q_j is a reduced fraction for $1 \leq j \leq n$, and let f_j denote the rational function $f_j := p_j/q_j$. Assume that the set of rational functions $\{f_1, \ldots, f_n\}$ is differentially algebraically independent over k, i.e. there does not exist a nonzero differential polynomial p in $k\{X\}$ for which $p(f_1, \ldots, f_n) = 0$ holds. As expressed at the introduction, our aim is to determine certain discrete information associated to the following system of ordinary differential equations in $k\langle X, Y\rangle$:

$$\begin{cases} f_1(X, \dot{X}) = y_1, \\ \qquad\qquad \vdots \\ f_n(X, \dot{X}) = y_n. \end{cases} \tag{6}$$

For this purpose, we introduce the following system of ordinary differential equations and inequalities in $k\{X, Y\}$, equivalent to system (6):

$$\begin{cases} p_1\big(X, \dot{X}\big) - y_1\, q_1\big(X, \dot{X}\big) = 0, \\ \qquad\qquad\qquad\qquad \vdots \\ p_n\big(X, \dot{X}\big) - y_n\, q_n\big(X, \dot{X}\big) = 0, \\ \qquad\qquad \prod_{j=1}^{n} q_j\big(X, \dot{X}\big) \neq 0. \end{cases} \tag{7}$$

We may regard the solution set of system (6), or equivalently of system (7), as the *graph* of the differential rational mapping defined by $f_1, \ldots, f_n$.

In Section 3.1, we shall analyze the Zariski closure of this graph, which has better geometric properties than the graph itself and still uniquely characterizes the underlying differential rational mapping. For this purpose, we shall consider the differential ideal defining the Zariski closure of the graph associated to systems (6) and (7), and a suitable localization Γ of it.

Then, in Section 3.2 we discuss a definition in the setting of differential algebra that corresponds to the intuitive notion of differentiation index presented in the introduction.

Finally, in Section 3.3 we shall introduce a further differential ideal Δ, isomorphic to Γ, which shares the same discrete invariants as Γ and has a generic zero with a simple and explicit description. As it will be clear in Section 5, such generic zero will play a crucial role in our algorithmic approach.

3.1 Zariski closure of a graph and an associated field extension

Let $\mathcal{I}$ be the differential ideal of $k\{X, Y\}$ generated by the polynomials

$$\widetilde{g}_1 := p_1 - y_1 q_1, \ \ldots, \ \widetilde{g}_n := p_n - y_n q_n,$$

let $\mathcal{S} := \{q_1, \ldots, q_n\}$, and let $\mathcal{S}^\infty \subset k\{X, Y\}$ be the multiplicatively closed subset of $k\{X\}$ generated by 1 and the elements of the set $\mathcal{S}$. We associate to system (7) the *saturation* $(\mathcal{I} : \mathcal{S}^\infty)$ of the differential ideal $\mathcal{I}$ in $k\{X, Y\}$ by the set $\mathcal{S}$, which is defined in the following way:

$$(\mathcal{I} : \mathcal{S}^\infty) := \{p \in k\{X, Y\}; \exists\, s \in \mathcal{S}^\infty \text{ with } sp \in \mathcal{I}\}\,.$$

The saturation $(\mathcal{I} : \mathcal{S}^\infty)$ is a differential ideal. Furthermore, we have the following result (compare with (Ollivier, 1990)):

Lemma 2 *$(\mathcal{I} : \mathcal{S}^\infty)$ is a prime differential ideal of $k\{X, Y\}$.*

PROOF.– Let us fix an elimination ranking over $k\{X, Y\}$ with $X \ll Y$.We observe that the polynomial $\widetilde{g}_j := p_j - y_j q_j$ has degree 1 in its leader y_j, and that $s_{g_j} = i_{g_j} = q_j$ for $1 \leq j \leq n$. Then $H_{\mathcal{I}}^\infty = \mathcal{S}^\infty$ and applying (Ritt, 1950, Chapter IV, §17–20), we conclude that $(\mathcal{I} : H_{\mathcal{I}}^\infty) = (\mathcal{I} : \mathcal{S}^\infty)$ is a prime differential ideal of $k\{X, Y\}$. ∎

Our next purpose is to consider a "generic specialization" of the variables Y. In order to do this, we localize the ideal $(\mathcal{I} : \mathcal{S}^\infty)$ at the multiplicatively closed set $k\{Y\} \setminus \{0\}$. We observe that $(\mathcal{I} : \mathcal{S}^\infty) \cap k\{Y\} = \{0\}$ holds. Indeed, any nonzero polynomial p in $(\mathcal{I} : \mathcal{S}^\infty) \cap k\{Y\}$ would induce a nontrivial relation $p(f_1, \ldots, f_n) = 0$, contradicting thus the fact that the rational functions $f_1, \ldots, f_n$ are differentially algebraically independent over k. Therefore, the resulting localization

$$\Gamma := k\langle Y\rangle \otimes_{k\{Y\}} (\mathcal{I} : \mathcal{S}^\infty)$$

is a nontrivial prime differential ideal of the differential $k\langle Y\rangle$–algebra $k\langle Y\rangle\{X\}$.

In what follows, we shall consider the following extension of differential k–algebras:

$$k\langle Y\rangle \hookrightarrow \frac{k\langle Y\rangle\{X\}}{\Gamma}. \tag{8}$$

We shall see that the discrete invariants we want to compute can be obtained by considering this extension. First of all, we have the following remark:

Lemma 3 *The differential k–algebra extension $k\langle Y\rangle \hookrightarrow k\langle Y\rangle\{X\}/\Gamma$ has differential transcendence degree 0.*

PROOF.– Since the rational functions $f_1, \ldots, f_n$ in $k\langle X\rangle$ are differentially algebraically independent over k, we conclude that the field extension

$$k\langle f_1, \ldots, f_n\rangle \hookrightarrow k\langle X\rangle$$

is differentially algebraic. This implies that for $1 \leq j \leq n$ there exists a nonzero differential polynomial a_j in $k\{f_1, \ldots, f_n\}[Z]$ such that $a_j(f_1, \ldots, f_n, x_j) = 0$ holds. Rewriting this identity, we obtain a congruence relation $a_j(Y, x_j) \equiv 0$ (modulo $[y_1 - f_1, \ldots, y_n - f_n]$). Multiplying this relation by a suitable power m of $q := q_1 \cdots q_n$ we conclude that $q^m a_j(Y, x_j)$ belongs to the ideal $[\widetilde{g}_1, \ldots, \widetilde{g}_n]$. We deduce that $a_j(Y, x_j)$ belongs to the ideal Γ for $1 \leq j \leq n$. This implies that the differential k–algebra extension $k\langle Y\rangle \hookrightarrow k\langle Y\rangle\{X\}/\Gamma$ has differential transcendence degree 0. ∎

3.2 On the differentiation index

One may ask for the minimal number of derivatives of the input polynomials $\widetilde{g}_1, \ldots, \widetilde{g}_n$ necessary to obtain an explicit system in the sense of the introduction. For this purpose, we have the following result:

Lemma 4 *Let ℓ denote the regularity of the Hilbert function of the differential ideal Γ with respect to the differential field $k\langle Y\rangle$. Then there exists elements $h_1, \ldots, h_n$ of the (algebraic) ideal $\Gamma_\ell := \Gamma \cap k\langle Y\rangle[\Theta_\ell X]$ with the following property:*

$$\det\left(\frac{\partial(h_1, \ldots, h_n)}{\partial X^{(\ell)}}\right) \neq 0 \quad \text{modulo } \Gamma_\ell. \tag{9}$$

We may interpret condition (9) as the fact that $h_1, \ldots, h_n$ define an explicit system. As it will be shown by the proof of this lemma, the existence of such polynomials $h_1, \ldots, h_n$ is a consequence of the equality

$$\mathcal{H}_{k\langle Y\rangle}(\ell) = \mathrm{ord}_{k\langle Y\rangle}\Gamma = \dim_{k\langle Y\rangle}\Gamma_\ell,$$

where $\dim_{k\langle Y\rangle}\Gamma_\ell$ denotes the Krull dimension of the (algebraic) ideal Γ_ℓ. This suggests that the completion process mentioned at the introduction will be certainly achieved once a system of generators of Γ_ℓ, or of a suitable localization of Γ_ℓ, is obtained.

Therefore, we define the *differentiation index* of system (6) as the least positive integer ν for which the identity

$$\dim_{k\langle Y\rangle}\Gamma_\ell = \dim_{k\langle Y\rangle}(\mathcal{S}^\infty)^{-1}(\widetilde{G}, \ldots, \widetilde{G}^{(\nu)}) \cap (\mathcal{S}^\infty)^{-1}k\langle Y\rangle[\Theta_\ell X]$$

holds, where $(\widetilde{G}, , \ldots, \widetilde{G}^{(\nu)})$ denotes the (algebraic) ideal of $k\langle Y\rangle[\Theta_{\nu+1}X]$ spanned by $\widetilde{G}^{(i)} := \{\widetilde{g}_1^{(i)}, \ldots, \widetilde{g}_n^{(i)}\}$ for $0 \leq i \leq \nu$. The reasons why we consider localizations at $\mathcal{S}^\infty$ will become apparent in Section 4.2.

Proof of Lemma 4.– Let $\mathcal{H}_{k\langle Y\rangle}$ denote the differential Hilbert function of the ideal Γ with respect to $k\langle Y\rangle$, and let ℓ be its regularity (see Section 2.1). Lemma 3 shows that the differential dimension of Γ over $k\langle Y\rangle$ is equal to zero. Hence, from identity (5) we see that $\mathcal{H}_{k\langle Y\rangle}(i) = \mathrm{ord}_{k\langle Y\rangle}\Gamma$ holds for any $i \geq \ell$. Let us fix an orderly ranking on the set ΘX. Then the ideal Γ_ℓ contains a characteristic set of the differential ideal Γ with respect to the orderly ranking chosen (see e.g. Cluzeau and Hubert, 2003, Section 4.2). Hence, there exists a subset $\mathcal{C}$ of $\Theta_{\ell-1}X$ such that the k–algebra extension

$$k\langle Y\rangle[\mathcal{C}] \hookrightarrow \frac{k\langle Y\rangle[\Theta_\ell X]}{\Gamma_\ell} \tag{10}$$

is algebraic. Applying (Matsumura, 1986, Theorem 26.3) we deduce that the ideal $\Gamma_\ell \otimes k\langle Y\rangle(\mathcal{C})$ is a radical zero–dimensional ideal of $k\langle Y\rangle(\mathcal{C})[\Theta_\ell X \backslash \mathcal{C}]$. This implies that there exist $s := \#(\Theta_\ell X \backslash \mathcal{C})$ elements $\widetilde{h}_1, \ldots, \widetilde{h}_s$ that span the ideal $\Gamma_\ell \otimes k\langle Y\rangle(\mathcal{C})$ in $k\langle Y\rangle(\mathcal{C})[\Theta_\ell X \backslash \mathcal{C}]$ (see e.g. Kunz, 1986, Corollary V.1.5). Therefore, from the Jacobian criterion (Eisenbud, 1995, Corollary 16.20) we deduce that the $(s \times s)$–Jacobian matrix $\partial(\widetilde{h}_1, \ldots, \widetilde{h}_s)/\partial(\Theta_\ell X \backslash \mathcal{C})$ is nonsingular. In particular, we have that there exist indices $i_1, \ldots, i_n \in \{1, \ldots, s\}$ such that $\partial(\widetilde{h}_{i_1}, \ldots, \widetilde{h}_{i_n})/\partial(X^{(\ell)})$ is nonsingular. Since $\Gamma_\ell \otimes k\langle Y\rangle(\mathcal{C}) \cap k\langle Y\rangle[\Theta_\ell X]$ is equal to Γ_ℓ, multiplying $\widetilde{h}_{i_1}, \ldots, \widetilde{h}_{i_n}$ by suitable elements of $k\langle Y\rangle[\mathcal{C}]$ we obtain elements $h_1, \ldots, h_n$ of Γ_ℓ satisfying condition (9). □

3.3 Generic section of a graph

In order to efficiently compute the discrete invariants associated to the differential k–algebra extension (8), following Ollivier (1990) we associate to the differential ideal Γ another prime differential ideal, isomorphic to Γ, which has a generic zero with a simple and explicit description.

Let $\widetilde{x}_1, \ldots, \widetilde{x}_n$ be differential indeterminates over k, let $\widetilde{X} := (\widetilde{x}_1, \ldots, \widetilde{x}_n)$, and let K denote the differential field extension of k generated by the differential rational functions $f_1(\widetilde{X}, \dot{\widetilde{X}}), \ldots, f_n(\widetilde{X}, \dot{\widetilde{X}})$ i.e.

$$K := k\langle f_1(\widetilde{X}, \dot{\widetilde{X}}), \ldots, f_n(\widetilde{X}, \dot{\widetilde{X}})\rangle.$$

Observe that K has differential transcendence degree n over k, because the rational functions $f_1, \ldots, f_n$ are differentially algebraically independent over k. Let $\psi : k\langle Y\rangle\{X\} \to K\{X\}$ be the differential homomorphism defined in the following way:

$$\begin{aligned} \psi(x_j) &:= \quad x_j\,, \qquad (1 \le j \le n) \\ \psi(y_j) &:= f_j(\widetilde{X}, \dot{\widetilde{X}}). \quad (1 \le j \le n) \end{aligned}$$

Let $g_i := \psi(\widetilde{g}_i)$ in $K\{X\}$ for $1 \le j \le n$ and let $\Delta := \psi(\Gamma)$. Observe that

$$\begin{aligned} \Delta &= ([g_1, \ldots, g_n] : \mathcal{S}^\infty) \\ &= \left(p_1(X, \dot{X}) - \tfrac{p_1(\widetilde{X}, \dot{\widetilde{X}})}{q_1(\widetilde{X}, \dot{\widetilde{X}})}\, q_1(X, \dot{X}), \ldots, p_n(X, \dot{X}) - \tfrac{p_n(\widetilde{X}, \dot{\widetilde{X}})}{q_n(\widetilde{X}, \dot{\widetilde{X}})}\, q_n(X, \dot{X}) : \mathcal{S}^\infty\right) \end{aligned}$$

holds. Therefore, the morphism ψ allows us to replace the set of variables Y by a set of n "symmetric" variables $\widetilde{X}$. Our next result shows that the discrete invariants we want to compute can be obtained by considering the differential ideal Δ, and that the vector $(\widetilde{x}_1, \ldots, \widetilde{x}_n)$ is a generic solution of the ideal Δ.

Lemma 5 *We have the following properties:*

(*i*) Δ *is a nontrivial prime differential ideal of* $K\{X\}$.
(*ii*) *The differential Hilbert function of the ideal* Δ *with respect to* K *is equal to the differential Hilbert function of the ideal* Γ *with respect to* $k\langle Y\rangle$.
(*iii*) *The element* $(\widetilde{x}_1, \ldots, \widetilde{x}_n)$ *is a generic zero of the differential ideal* Δ.

PROOF.– Since the morphism ψ acts as the identity mapping on the set ΘX, and maps isomorphically the differential field $k\langle Y\rangle$ onto the differential field K, we conclude that the ideal $\Delta := \psi(\Gamma)$ is a nontrivial prime differential ideal of $K\{X\}$. This shows assertion (*i*). Furthermore, for any $i \geq 0$, we have the identity

$$\psi(\Gamma \cap k\langle Y\rangle[\Theta_i X]) = \Delta \cap K[\Theta_i X].$$

This shows assertion (*ii*). In order to prove assertion (*iii*), we consider the differential homomorphism $\varphi : K\{X\} \to k\langle\widetilde{X}\rangle$ that maps x_j to $\widetilde{x}_j$ for $1 \leq j \leq n$. We have that $\mathrm{Ker}(\varphi) = \Delta$ holds (see Ollivier, 1990, II §4.2, Proposition 3) and the image of φ contains the differential k-algebra $k\{\widetilde{X}\}$. This implies that the fraction field of the quotient ring $K\{X\}/\Delta$ is isomorphic to $k\langle\widetilde{X}\rangle$. This shows assertion (*iii*). ∎

4 Linearization of the completion process

For the sake of clarity, we recall some notations and hypotheses introduced in Section 3. Let $f_1, \ldots, f_n$ be rational functions of $k\langle X\rangle$ of order 1 which are differentially algebraically independent over k. For $1 \leq j \leq n$, let p_j, q_j be the numerator and denominator in $k[X, \dot{X}]$ of a reduced representation $f_j := p_j/q_j$ of f_j. Let $\widetilde{X} := (\widetilde{x}_1, \ldots, \widetilde{x}_n)$ be new differential indeterminates, and let g_j be the differential rational function

$$g_j := p_j(X, \dot{X}) - f_j(\widetilde{X}, \dot{\widetilde{X}})q_j(X, \dot{X})$$

in $k\langle\widetilde{X}\rangle\{X\}$ for $1 \leq j \leq n$. Let $K := k\langle f_1(\widetilde{X}, \dot{\widetilde{X}}), \ldots, f_n(\widetilde{X}, \dot{\widetilde{X}})\rangle$, let $\mathcal{S}$ be the set $\{q_1(X, \dot{X}), \ldots, q_n(X, \dot{X})\}$ and let Δ be the differential ideal of $K\{X\}$ defined as the saturation $\Delta := ([g_1, \ldots, g_n] : \mathcal{S}^\infty)$.

In Section 3, we show that the discrete invariants we want to compute can be obtained by considering the differential ring extension $K \hookrightarrow K\{X\}/\Delta$. In order to analyze this extension, in this section we are going to show that the computation of the differentiation index of system (6), and the differential Hilbert function and an algebraic parametric set of the (prime) differential ideal Δ with respect to K, can be reduced to the computation of the dimension of certain vector spaces. These vector spaces can be easily described in terms of the input polynomials $g_1, \ldots, g_n$. For this purpose, we are going to

"linearize" our problems, using the theory of Kähler differentials (cf. (Eisenbud, 1995), (Kunz, 1986) in the purely algebraic case, and (Johnson, 1969), (Johnson, 1974) in the setting of differential algebra).

4.1 Kähler differentials

For a given K–algebra A, the *module of Kähler differentials of A over K* is defined as the unique A–module $\Omega_{A/K}$, together with an A–derivation d from A into $\Omega_{A/K}$ that satisfies the following universal property: for any A–module B and any K–derivation $\mathrm{D} : A \to B$, there exists a unique homomorphism of A–modules $\varphi : \Omega_{A/K} \to B$ such that $\varphi \circ \mathrm{d} = \mathrm{D}$. If A is a differential K–algebra, then $\Omega_{A/K}$ has a (unique) canonical structure of differential A–module such that $\delta \circ \mathrm{d}(a) = \mathrm{d} \circ \delta(a)$ for any derivation $\delta : A \to A$ and any a in A (see (Johnson, 1969, §1)). Our interest on modules and vector spaces of Kähler differentials is mainly based on the following result (Eisenbud, 1995, Theorem 16.14):

Theorem 6 *Let $K \hookrightarrow F$ be a finitely generated field extension of K. A subset $\{\eta_1, \ldots, \eta_r\}$ of F is a transcendence basis of F over K if and only if the set $\{\mathrm{d}\eta_1, \ldots, \mathrm{d}\eta_r\}$ is a basis of the F-vector space $\Omega_{F/K}$.*

Boulier (1999) and Sedoglavic (2002) (see also (Sedoglavic, 2001)) make use of the theory of Kähler differentials in order to develop algorithms of differential algebra in a similar way as here.

Notations. Let us fix some notations we are going to use in the sequel. Let $A := K\{X\}$ and let $A_i := K[\Theta_i X]$. From the fact that Δ is a prime differential ideal of A we easily conclude that $\Delta \cap A_i$ is a prime (algebraic) ideal of A_i and the quotient ring $A_i/(\Delta \cap A_i)$ is a domain for any $i \geq 0$. We shall denote by $\mathcal{F}$ the (differential) fraction field of the quotient ring A/Δ, and by $(\mathcal{F}_i)_{i\geq 0}$ the sequence of (algebraic) fraction fields of the quotient rings $A_i/(\Delta \cap A_i)$. In symbols:

- $A := K\{X\}$;
- $A_i := K[\Theta_i X] = K[X, \ldots, X^{(i)}]$;
- $\mathcal{F} :=$ Fraction field of A/Δ;
- $\mathcal{F}_i :=$ Fraction field of $A_i/(\Delta \cap A_i)$.

For any $i \geq 0$, we have a canonical inclusion $\mathcal{F}_i \hookrightarrow \mathcal{F}$. Finally, let $\Omega_{\mathcal{F}/K}$ denote the $\mathcal{F}$–vector space of Kähler differentials of $\mathcal{F}$ over K, and let $\Omega_{\mathcal{F}_i/K}$ denote the $\mathcal{F}_i$–vector space of Kähler differentials of $\mathcal{F}_i$ over K for any $i \geq 0$.

Kähler differentials, discrete invariants and algebraic parametric sets. First, we observe that the computation of the differential Hilbert func-

tion of the differential ideal Δ with respect to K can be easily reduced to the analysis of certain vector spaces of Kähler differentials. Indeed, from the definition of the Hilbert function $\mathcal{H}_K$ of the differential ideal Δ with respect to K, we conclude that the following identity holds for any $i \geq 0$:

$$\mathcal{H}_K(i) = \dim_{\mathcal{F}_i} \Omega_{\mathcal{F}_i/K}. \tag{11}$$

Now, we explain how one may describe an *algebraic parametric set* of the differential ideal Δ with respect to K using Kähler differentials.

Let us fix an orderly ranking on the set ΘX. Then the ideal $\Delta \cap A_\ell$ contains a characteristic set of the differential ideal Δ with respect to the orderly ranking chosen (see e.g. Cluzeau and Hubert, 2003, Section 4.2), where ℓ denotes the regularity of the Hilbert function $\mathcal{H}_K$. Therefore, there exists a subset $\mathcal{C}$ of $\Theta_{\ell-1}X$ of cardinality $\mathrm{ord}_K\Delta$ which is a transcendence basis of the field $\mathcal{F}_\ell$ over K. We call such a set an algebraic parametric set of the ideal Δ with respect to K. Observe that such a subset $\mathcal{C}$ represents a maximal set of derivatives of ΘX whose initial conditions must be fixed in order to assure existence and uniqueness of solutions of the input system (6). Applying Theorem 6 we conclude that such a set $\mathcal{C}$ is characterized by the following condition:

$$\dim_{\mathcal{F}_\ell} \mathrm{Span}(\mathrm{d}(\mathcal{C})) = \#(\mathcal{C}) = \dim_{\mathcal{F}_\ell} \Omega_{\mathcal{F}_\ell/K}, \tag{12}$$

where $\mathrm{Span}(\mathrm{d}(\mathcal{C}))$ denotes the linear subspace of $\Omega_{\mathcal{F}_i/K}$ spanned by the elements of the set $\mathrm{d}(\mathcal{C})$.

Identities (11) and (12) show that the discrete invariants we want to compute can be obtained from an explicit description of the $\mathcal{F}_i$–vector spaces $\Omega_{\mathcal{F}_i/K}$.

4.2 An explicit representation of $\Omega_{\mathcal{F}_i/K}$

In order to obtain a simpler description of the $\mathcal{F}_i$–vector space $\Omega_{\mathcal{F}_i/K}$, it would be desirable to have a simpler description of the field $\mathcal{F}_i$. Let us recall that $\mathcal{F}_i$ is the fraction field of the quotient ring $A_i/(\Delta \cap A_i)$, where Δ denotes $([g_1, \ldots, g_n] : \mathcal{S}^\infty)$. Therefore, in order to manipulate the elements of the field $\mathcal{F}_i$, it would be desirable to have an explicit system of generators of the ideal Δ. Unfortunately, it is not clear how one may efficiently obtain such a system of generators. In order to circumvent this inconvenience, we consider the localization $(\mathcal{S}^\infty)^{-1}\Delta$, which has an *explicit* system of generators, namely $(\mathcal{S}^\infty)^{-1}\Delta = (\mathcal{S}^\infty)^{-1}[g_1, \ldots, g_n]$.

Lemma 7 *The total ring of fractions of the quotient ring*

$$\frac{(\mathcal{S}^\infty)^{-1}A_i}{(\mathcal{S}^\infty)^{-1}[g_1,\ldots,g_n]\cap(\mathcal{S}^\infty)^{-1}A_i}$$

is isomorphic to the field $\mathcal{F}_i$ for any $i>0$.

PROOF.– Since $\mathcal{S}$ is not a subset of A_0, we shall suppose first that $i\geq 1$. Since $\mathcal{S}^\infty$ is a multiplicatively closed subset of A_i that does not meet the ideal $\Delta\cap A_i$, $(\mathcal{S}^\infty)^{-1}(\Delta\cap A_i)$ is a nontrivial prime ideal of $(\mathcal{S}^\infty)^{-1}A_i$. From the definition of the ideals $\Delta:=([g_1,\ldots,g_n]:\mathcal{S}^\infty)$ and $[g_1,\ldots,g_n]$ we deduce the following identity of localized ideals in the ring $(\mathcal{S}^\infty)^{-1}A_i$ (see e.g. Matsumura, 1986, §4):

$$(\mathcal{S}^\infty)^{-1}(\Delta\cap A_i)=(\mathcal{S}^\infty)^{-1}([g_1,\ldots,g_n]\cap A_i)=(\mathcal{S}^\infty)^{-1}[g_1,\ldots,g_n]\cap(\mathcal{S}^\infty)^{-1}A_i.$$

Therefore, applying standard properties of localizations (see e.g. Matsumura, 1986, Theorem 4.2), we have the following ring isomorphism:

$$\begin{aligned}(\mathcal{S}^\infty)^{-1}\left(\frac{A_i}{\Delta\cap A_i}\right)\simeq&\quad\frac{(\mathcal{S}^\infty)^{-1}A_i}{(\mathcal{S}^\infty)^{-1}(\Delta\cap A_i)}\\=&\quad\frac{(\mathcal{S}^\infty)^{-1}A_i}{(\mathcal{S}^\infty)^{-1}[g_1,\ldots,g_n]\cap(\mathcal{S}^\infty)^{-1}A_i}.\end{aligned}\tag{13}$$

Applying (Matsumura, 1986, Theorem 4.3) we deduce that $\mathcal{F}_i$ is isomorphic to the total ring of fractions of the ring $(\mathcal{S}^\infty)^{-1}\left(A_i/(\Delta\cap A_i)\right)$. Combining this with isomorphism (13) shows that $\mathcal{F}_i$ isomorphic to the total ring of fractions of the ring $(\mathcal{S}^\infty)^{-1}A_i/((\mathcal{S}^\infty)^{-1}[g_1,\ldots,g_n]\cap(\mathcal{S}^\infty)^{-1}A_i)$. ∎

Now let $i=0$, and let $\widehat{\mathcal{S}}:=\mathcal{S}\cap K[X]$. Then the previous argumentation, replacing $\mathcal{S}$ by $\widehat{\mathcal{S}}$, shows that the total ring of fractions of the quotient ring

$$\frac{(\widehat{\mathcal{S}}^\infty)^{-1}A_0}{(\widehat{\mathcal{S}}^\infty)^{-1}[g_1,\ldots,g_n]\cap(\widehat{\mathcal{S}}^\infty)^{-1}A_0}$$

is isomorphic to the field $\mathcal{F}_0$. Lemma 7 shows that $(\mathcal{S}^\infty)^{-1}[g_1,\ldots,g_n]\cap(\mathcal{S}^\infty)^{-1}A_i$ is a prime ideal of $(\mathcal{S}^\infty)^{-1}A_i$ for any $i\geq 0$. Furthermore, a similar argument as above shows that $(\mathcal{S}^\infty)^{-1}[g_1,\ldots,g_n]$ is a prime ideal of $(\mathcal{S}^\infty)^{-1}A$ and the total ring of fractions of the quotient ring $(\mathcal{S}^\infty)^{-1}A/(\mathcal{S}^\infty)^{-1}[g_1,\ldots,g_n]$ is isomorphic to the differential field $\mathcal{F}$. Hence, the ideal $(\mathcal{S}^\infty)^{-1}[g_1,\ldots,g_n]$ satisfies the statement of Lemma 5. This means that the discrete invariants associated to the ideals Δ and $(\mathcal{S}^\infty)^{-1}[g_1,\ldots,g_n]$ coincide, and the point $\widetilde{X}$ is a generic zero of the ideal $(\mathcal{S}^\infty)^{-1}[g_1,\ldots,g_n]$. Therefore, in the sequel we shall also consider the differential ideal $(\mathcal{S}^\infty)^{-1}[g_1,\ldots,g_n]$, which has an explicit system of generators.

4.3 Completion process and Jacobian matrices

In this section we discuss how the computation of the differentiation index ν, the differential Hilbert function $\mathcal{H}_K$ and an algebraic parametric set of the ideal Δ with respect to K can be reduced to linear algebra computations over the field $\mathcal{F}$. More precisely, we shall describe this discrete data in terms of the $\mathcal{F}$–ranks of certain Jacobian matrices related to the input differential polynomials $g_1, \ldots, g_n$. Let i and j be integers with $j \leq i+1$, and let $J(i,j)$ denote the following Jacobian (block) $(n(i+1) \times n(i-j+2))$–matrix with entries in $K\{X\}$:

$$J(i,j) := \begin{pmatrix} \dfrac{\partial G^{(i)}}{\partial X^{(i+1)}} & \dfrac{\partial G^{(i)}}{\partial X^{(i)}} & \cdots & \dfrac{\partial G^{(i)}}{\partial X^{(j)}} \\ \vdots & \vdots & & \vdots \\ \dfrac{\partial G}{\partial X^{(i+1)}} & \dfrac{\partial G}{\partial X^{(i)}} & \cdots & \dfrac{\partial G}{\partial X^{(j)}} \end{pmatrix},$$

where $\partial G^{(h)}/\partial X^{(l)}$ denotes the following $(n \times n)$–matrix with entries in $K\{X\}$:

$$\frac{\partial G^{(h)}}{\partial X^{(l)}} := \begin{pmatrix} \dfrac{\partial {g_1}^{(h)}}{\partial {x_1}^{(l)}} & \cdots & \dfrac{\partial {g_1}^{(h)}}{\partial {x_n}^{(l)}} \\ \vdots & & \vdots \\ \dfrac{\partial {g_n}^{(h)}}{\partial {x_1}^{(l)}} & \cdots & \dfrac{\partial {g_n}^{(h)}}{\partial {x_n}^{(l)}} \end{pmatrix}.$$

The Jacobian matrices $J(i,0)$ are closely related to the (algebraic) ideals Δ_i of A_{i+1} spanned by the set of polynomials $\{G, \ldots, G^{(i)}\}$. In the sequel, we shall rather consider the localizations $(\mathcal{S}^\infty)^{-1}\Delta_i$, which have better geometric properties than the ideals Δ_i and describe a Zariski–dense open subset of the graph defined by our input differential rational mapping. In fact, we have the following result :

Lemma 8 *$(\mathcal{S}^\infty)^{-1}\Delta_i$ is a prime ideal of $(\mathcal{S}^\infty)^{-1}A_{i+1}$ for any $i \geq 0$.*

Proof.– Following the notations of Section 3, let $\widetilde{g}_j := p_j(X, \dot{X}) - y_j q_j(X, \dot{X})$ for $1 \leq j \leq n$, let $\widetilde{G} := \{\widetilde{g}_1, \ldots, \widetilde{g}_n\}$, and let $\widetilde{\Gamma}_i \subset k[\Theta_{i+1}X, \Theta_i Y]$ be the (algebraic) ideal spanned by the set $\{\widetilde{G}, \ldots, \widetilde{G}^{(i)}\}$ for $i \geq 0$. Then (Ritt, 1950, Chapter IV, §17–20) shows that for any $i \geq 0$ the saturation ideal $(\widetilde{\Gamma}_i : \mathcal{S}^\infty)$ is a prime ideal of $k[\Theta_{i+1}X, \Theta_i Y]$, where $\mathcal{S} := \{q_1, \ldots, q_n\}$. From the arguments of Section 3.1 we deduce that $\widetilde{\Gamma}_i \cap k\{Y\} = \widetilde{\Gamma}_i \cap k\{X\} = \{0\}$ holds. Therefore, we have that the localized ideal $(\mathcal{S}^\infty)^{-1}\widetilde{\Gamma}_i$ is a prime ideal of $(\mathcal{S}^\infty)^{-1}k[\Theta_{i+1}X, \Theta_i Y]$. We conclude that $(\mathcal{S}^\infty)^{-1}\Delta_i = (\mathcal{S}^\infty)^{-1}\psi(\widetilde{\Gamma}_i)$ is a prime ideal of $(\mathcal{S}^\infty)^{-1}A_{i+1}$, where $\psi : k\langle Y\rangle\{X\} \to K\{X\}$ denotes the homomorphism of Section 3.3. This concludes the proof of the lemma. ∎

The consideration of the ideals $(\mathcal{S}^\infty)^{-1}\Delta_i$ will allow us to control the number of derivatives of the set of polynomials G which are required for the computation of the discrete invariants associated to the ideal Δ. More precisely, we have the following result :

Lemma 9 *For $0 \leq i \leq \ell$, the following identity of Krull dimensions holds :*

$$\dim_K \left((\mathcal{S}^\infty)^{-1}\Delta_{2n-2} \cap (\mathcal{S}^\infty)^{-1}A_i\right) = \dim_K (\Delta \cap A_i). \tag{14}$$

PROOF.– Let us fix an arbitrary orderly ranking over $K\{X\}$. Then, (Sadik, 2000, Theorem 27) shows that the (algebraic) ideal Δ_{n-1} contains a characteristic set $H := \{h_1, \ldots, h_s\}$ of Δ with respect to the orderly ranking chosen. Then we have $\Delta = [H] : (\mathcal{S}_H)^\infty$, where $\mathcal{S}_H$ denotes the set of initials and separants of the elements of H. Let h be an arbitrary element of $\Delta \cap A_n$. Then (Sadik, 2000, Lemma 26) shows that h belongs to $(H, \ldots, H^{(n-1)} : \mathcal{S}_H^\infty)$, and hence to $(\Delta_{2n-2} : \mathcal{S}_H^\infty)$. We conclude that

$$(\Delta_{2n-2} : \mathcal{S}_H^\infty) \cap A_n = (\Delta_{2n-2} \cap A_n : \mathcal{S}_H^\infty) = (\Delta \cap A_n : \mathcal{S}_H^\infty) = \Delta \cap A_n$$

holds. Then we have $(\Delta_{2n-2} : \mathcal{S}_H^\infty) \cap A_i = \Delta \cap A_i$ for $0 \leq i \leq \ell$; this implies that $(\mathcal{S}^\infty)^{-1}\left((\Delta_{2n-2} : \mathcal{S}_H^\infty) \cap A_i\right)$ is equal to $(\mathcal{S}^\infty)^{-1}(\Delta \cap A_i)$ for $0 \leq i \leq \ell$.

Let us fix $0 \leq i \leq \ell$. Then

$$\begin{aligned}
(\mathcal{S}^\infty)^{-1}(\Delta \cap A_i) &= (\mathcal{S}^\infty)^{-1}\left((\Delta_{2n-2} : \mathcal{S}_H^\infty) \cap A_i\right) \\
&= (\mathcal{S}^\infty)^{-1}(\Delta_{2n-2} : \mathcal{S}_H^\infty) \cap (\mathcal{S}^\infty)^{-1}A_i \\
&= ((\mathcal{S}^\infty)^{-1}\Delta_{2n-2} : \mathcal{S}_H^\infty)) \cap (\mathcal{S}^\infty)^{-1}A_i \\
&= (\mathcal{S}^\infty)^{-1}\Delta_{2n-2} \cap (\mathcal{S}^\infty)^{-1}A_i,
\end{aligned} \tag{15}$$

the last equality being consequence of the fact that $(\mathcal{S}^\infty)^{-1}\Delta_{2n-2}$ is a prime ideal (Lemma 9). From Lemma 7, we see that the dimension of $\Delta \cap A_i$ over K is equal to $\dim_K(\mathcal{S}^\infty)^{-1}(\Delta \cap A_i)$. Combining this equality with equality (15) we deduce the statement of Lemma 9. ∎

Now we show how the values of the differential Hilbert function $\mathcal{H}_K$ of the differential ideal Δ with respect to K can be expressed in terms of the Jacobian matrices $J(i, j)$.

Theorem 10 *For $0 \leq i \leq \ell$, the value of the differential Hilbert function $\mathcal{H}_K(i)$ of the differential ideal Δ with respect to K satisfies the following identity:*

$$\mathcal{H}_K(i) = n(i+1) - \operatorname{rank}_{\mathcal{F}} J(2n-2, 0) + \operatorname{rank}_{\mathcal{F}} J(2n-2, i+1).$$

PROOF.– Combining Lemma 7 and identities (13) and (15) we see that $\mathcal{F}_i$ is isomorphic to the fraction field of the quotient ring

$$\frac{(\mathcal{S}^\infty)^{-1}A_i}{(\mathcal{S}^\infty)^{-1}\Delta_{2n-2}\cap(\mathcal{S}^\infty)^{-1}A_i}.$$

Therefore, (Eisenbud, 1995, §16.1) shows that the dimension of the $\mathcal{F}_i$–vector space $\Omega_{\mathcal{F}_i/K}$ satisfies the following identity:

$$\dim_{\mathcal{F}_i}\Omega_{\mathcal{F}_i/K} = n(i+1) - \operatorname{rank}_{\mathcal{F}_i} J((\mathcal{S}^\infty)^{-1}\Delta_{2n-2}\cap(\mathcal{S}^\infty)^{-1}A_i), \tag{16}$$

where $J((\mathcal{S}^\infty)^{-1}\Delta_{2n-2}\cap(\mathcal{S}^\infty)^{-1}A_i)$ denotes the Jacobian matrix of any system of generators of the ideal $(\mathcal{S}^\infty)^{-1}\Delta_{2n-2}\cap(\mathcal{S}^\infty)^{-1}A_i$. Since the matrix rank does not change by field extension, we conclude that

$$\operatorname{rank}_{\mathcal{F}_i} J((\mathcal{S}^\infty)^{-1}\Delta_{2n-2}\cap(\mathcal{S}^\infty)^{-1}A_i) = \operatorname{rank}_{\mathcal{F}} J((\mathcal{S}^\infty)^{-1}\Delta_{2n-2}\cap(\mathcal{S}^\infty)^{-1}A_i)$$

holds. We observe that the $\mathcal{F}$–rank of the matrix $J((\mathcal{S}^\infty)^{-1}\Delta_{2n-2}\cap(\mathcal{S}^\infty)^{-1}A_i)$ equals the dimension of the $\mathcal{F}$–vector subspace of $\Omega_{\mathcal{F}/K}$ spanned by the set

$$\mathrm{d}((\mathcal{S}^\infty)^{-1}\Delta_{2n-2}\cap(\mathcal{S}^\infty)^{-1}A_i).$$

In order to describe the dimension of this vector space in terms of the Jacobian matrices $J(i,j)$ introduced above, we see that any element of the set $\mathrm{d}((\mathcal{S}^\infty)^{-1}\Delta_{2n-2})$ is generated by an $\mathcal{F}$–linear combination of the coordinates of the column vector

$$J(2n-2,0)\begin{pmatrix}\mathrm{d}X^{(2n-1)}\\ \vdots\\ \mathrm{d}X\end{pmatrix}.$$

Hence, we have the identity

$$\dim_{\mathcal{F}}\operatorname{Span}\Big(\mathrm{d}((\mathcal{S}^\infty)^{-1}\Delta_{2n-2})\Big) = \operatorname{rank}_{\mathcal{F}} J(2n-2,0). \tag{17}$$

Let $\widetilde{J}(2n-2,0)$ denotes the (unique) reduced row–echelon form of the matrix $J(2n-2,0)$. Let us write $\widetilde{J}(2n-2,0) := (J_1|J_2)$, where J_1 and J_2 are the submatrices of $\widetilde{J}(2n-2,0)$ consisting of the first $(2n-i-1)n$ columns and the last $(i+1)n$ columns of $\widetilde{J}(2n-2,0)$ respectively. Since the matrix denoted by $J(2n-2,i+1)$ is the submatrix of $J(2n-2,0)$ consisting of the first $(2n-1-i)n$ columns of $J(2n-2,0)$, by elementary properties of the reduced row–echelon form of a matrix we conclude that the identity

$$\operatorname{rank}_{\mathcal{F}} J(2n-2,i+1) = \operatorname{rank}_{\mathcal{F}} J_1$$

holds. On the other hand, the elements of $\Omega_{\mathcal{F}/K}$ corresponding to the rows of $\widetilde{J}(2n-2,0)$ whose first $(2n-1-i)n$ coordinates are zero, span the subspace $\mathrm{d}((\mathcal{S}^\infty)^{-1}\Delta_{2n-2}\cap(\mathcal{S}^\infty)^{-1}A_i)$. We conclude that denoting by C the dimension of $\mathrm{d}((\mathcal{S}^\infty)^{-1}\Delta_{2n-2}\cap(\mathcal{S}^\infty)^{-1}A_i)$ over $\mathcal{F}$, we have

$$\begin{aligned} C &= \mathrm{rank}_{\mathcal{F}}\,\widetilde{J}(2n-2,0) - \mathrm{rank}_{\mathcal{F}}\,J_1, \\ &= \mathrm{rank}_{\mathcal{F}}\,J(2n-2,0) - \mathrm{rank}_{\mathcal{F}}\,J(2n-2,i+1). \end{aligned} \tag{18}$$

Taking into account that $\mathcal{H}_K(i)$ is equal to $\dim_{\mathcal{F}_i}\Omega_{\mathcal{F}_i/K}$ and combining identities (16) and (18) completes the proof of Theorem 10. ∎

Let us observe that, combining Theorem 1 and Lemma 3, we see that for $i\geq\ell$ the identity $\mathcal{H}_K(i)=\mathcal{H}_K(\ell)$ holds. Since $\ell\leq n-1$ holds (see e.g. Sadik, 2000, § 5.2)), this furnishes a practical method to compute the regularity ℓ of the Hilbert function $\mathcal{H}_K$.

In Section 3.3, we define the *differentiation index* of system (6) as the least positive integer ν such that the identity

$$\mathrm{ord}_{k\langle Y\rangle}\Gamma = \dim_{k\langle Y\rangle}(\mathcal{S}^\infty)^{-1}(\widetilde{G},,\ldots,\widetilde{G}^{(\nu)})\cap(\mathcal{S}^\infty)^{-1}k\langle Y\rangle[\Theta_\ell X]$$

holds. From the definition of the differential homomorphism ψ from $k\langle Y\rangle[X]$ into $K\{X\}$ of Section 3.3 we easily conclude that ν is the least positive integer such that

$$\mathrm{ord}_K\Delta = \dim_K\left((\mathcal{S}^\infty)^{-1}\Delta_\nu\cap(\mathcal{S}^\infty)^{-1}A_\ell\right)$$

holds. We have the following result:

Theorem 11 *The differentiation index of system (6) is the least positive integer ν such that the following identity holds:*

$$\mathcal{H}_K(\ell) = \mathrm{rank}_{\mathcal{F}}\,J(\nu,0) - \mathrm{rank}_{\mathcal{F}}\,J(\nu,\ell+1).$$

Proof.– From the above remarks we see that the differentiation index ν is the least positive integer such that the identity

$$\mathrm{ord}_K\Delta = \dim_K\left((\mathcal{S}^\infty)^{-1}\Delta_\nu\cap(\mathcal{S}^\infty)^{-1}A_\ell\right)$$

holds. On one hand, we have $\mathrm{ord}_K\Delta=\mathcal{H}_K(\ell)=\mathrm{d}(\Delta\cap A_\ell)$. On the other hand, arguing as in the proof of Theorem 10 we see that the identity

$$\dim_K\left((\mathcal{S}^\infty)^{-1}\Delta_\nu\cap(\mathcal{S}^\infty)^{-1}A_\ell\right) = \mathrm{rank}_{\mathcal{F}}\,J(\nu,0) - \mathrm{rank}_{\mathcal{F}}\,J(\nu,\ell+1)$$

holds. Combining both identities completes the proof of Theorem 11. ∎

Finally, we discuss how one may determine in $\Theta_{\ell-1}X$ an algebraic parametric set $\mathcal{C}$ of the ideal Δ with respect to K. Let us recall that such an algebraic parametric set is characterized by the conditions $\#(\mathcal{C}) = \mathrm{ord}_K\Delta$ and the $\mathcal{F}_\ell$–vector subspace $\mathrm{Span}(\mathrm{d}(\mathcal{C}))$ of $\Omega_{\mathcal{F}_\ell/K}$ spanned by the set $\mathrm{d}(\mathcal{C})$ has dimension

$$\dim_{\mathcal{F}_\ell} \mathrm{Span}(\mathrm{d}(\mathcal{C})) = \mathcal{H}_K(\ell) = \mathrm{ord}_K\Delta.$$

Let be given a subset $\mathcal{C}$ of $\Theta_{\ell-1}X$, and let $J^{(\mathcal{C})}(\nu, 0)$ denote the submatrix of the Jacobian matrix $J(\nu, 0)$ obtained by deleting the columns of $J(\nu, 0)$ corresponding to the derivatives in $\mathcal{C}$. We have the following result:

Theorem 12 *For a given subset $\mathcal{C}$ of $\Theta_{\ell-1}X$, $\mathcal{C}$ is an algebraic parametric set of Δ if, and only if, the following identities hold:*

$$\#(\mathcal{C}) = \mathrm{ord}_K\Delta \quad \text{and} \quad \mathrm{rank}_{\mathcal{F}}\, J^{(\mathcal{C})}(\nu, 0) = \mathrm{rank}_{\mathcal{F}}\, J(\nu, 0).$$

Proof.– Let be given a subset $\mathcal{C}$ of $\Theta_{\ell-1}X$ with $\#(\mathcal{C}) = \mathrm{ord}_K\Delta$. Arguing as in the proof of Theorem 10, replacing the K–algebra $(\mathcal{S}^\infty)^{-1}A_i$ by $(\mathcal{S}^\infty)^{-1}K[\mathcal{C}]$, we obtain the identity:

$$\dim_{\mathcal{F}} \mathrm{Span}\Big(d((\mathcal{S}^\infty)^{-1}\Delta_\nu \cap (\mathcal{S}^\infty)^{-1}K[\mathcal{C}])\Big) = \mathrm{rank}_{\mathcal{F}}\, J(\nu, 0) - \mathrm{rank}_{\mathcal{F}}\, J^{(\mathcal{C})}(\nu, 0).$$

From this we deduce the following identity:

$$\begin{aligned} \dim_{\mathcal{F}} \mathrm{Span}(\mathrm{d}(\mathcal{C})) &= \mathrm{ord}_K\Delta - \dim_{\mathcal{F}} \mathrm{Span}\,\mathrm{d}\Big((\mathcal{S}^\infty)^{-1}\Delta_\nu \cap (\mathcal{S}^\infty)^{-1}K[\mathcal{C}]\Big) \\ &= \mathrm{ord}_K\Delta - \mathrm{rank}_{\mathcal{F}}\, J(\nu, 0) + \mathrm{rank}_{\mathcal{F}}\, J^{(\mathcal{C})}(\nu, 0). \end{aligned} \tag{19}$$

Identity (19) immediately implies that $\dim_{\mathcal{F}_\ell} \mathrm{Span}(\mathrm{d}(\mathcal{C})) = \mathrm{ord}_K\Delta$ holds if, and only if, $\mathrm{rank}_{\mathcal{F}}\, J(\nu, 0) = \mathrm{rank}_{\mathcal{F}}\, J^{(\mathcal{C})}(\nu, 0)$ holds. This completes the proof of Theorem 12. ∎

5 Computational aspects

Let notations and assumptions be as in Section 4. In this section we exhibit efficient algorithms which compute the following items:

- The differentiation index ν of the input system (6).
- The differential Hilbert function $\mathcal{H}_K$ of the differential ideal Δ with respect to K.
- An algebraic parametric set of the differential ideal Δ with respect to K.

Algorithms in differential algebra are usually described using the standard dense or sparse complexity model, i.e. encoding multivariate polynomials by means of the vector of all or of all nonzero coefficients. Taking into account that a generic n–variate polynomial of degree d has $\binom{d+n}{n} = \mathcal{O}(d^n)$ nonzero coefficients, we see that the dense or sparse representation of multivariate polynomials requires an exponential size, and their manipulation usually requires an exponential number of arithmetic operations with respect to the parameters d and n. In order to avoid this exponential behavior, we are going to use an alternative encoding of input, output and intermediate results of our computations, by means of straight–line programs (cf. (Heintz, 1989), (Strassen, 1990), (Pardo, 1995), (Bürgisser et al., 1997)). A *straight–line program* β in $k(\Theta X)$ is a finite sequence of rational functions $(b_1, \ldots, b_s)$ in $k(\Theta X)^s$ such that for $1 \leq i \leq s$ the rational function b_i is either an element of the set ΘX, or an element of k (a *parameter*), or there exist $1 \leq i_1, i_2 < i$ such that $b_i = b_{i_1} \circ_i b_{i_2}$ holds, where $\circ_i$ is one of the arithmetic operations $+, -, \times, \div$. The straight–line program β is called *division–free* if $\circ_i$ is different from $\div$ for $1 \leq i \leq s$. A basic measure of the complexity of β is the number s, which is called the *length* of the straight–line program β. We say that the straight–line program β *computes* or *represents* a subset $\mathcal{T}$ of $k(\Theta X)$ if the inclusion $\mathcal{T} \subset \{b_1, \ldots, b_s\}$ holds.

Let us suppose that the input polynomials $p_1, q_1, \ldots, p_n, q_n$ are represented by a division–free straight–line program β in $k(X, \dot{X})$ of length $\mathcal{L}$. Observe that there exists a straight–line program $\widetilde{\beta}$ of length $\mathcal{O}(\mathcal{L} + n)$ computing the polynomials $\widetilde{g}_1 := p_1(X, \dot{X}) - y_1 q_1(X, \dot{X}), \ldots, \widetilde{g}_n := p_n(X, \dot{X}) - y_n q_n(X, \dot{X})$.

In the sequel, we shall need to compute the Jacobian matrix of the polynomials $\widetilde{g}_1, \ldots, \widetilde{g}_n$. For this purpose, we have the following constructive result:

Theorem 13 ((Baur and Strassen, 1983),(Morgenstern, 1984))
Let be given a straight–line program of length L computing a rational function f in $k(\Theta X)$. Then there exists a straight–line program of length $3L$ that computes f and all its first order derivatives.

A difficult point in the manipulation of multivariate polynomials represented by straight–line programs is the so–called *identity testing problem*: given two polynomials f and g in $k[\Theta X]$ represented by straight–line programs of length at most L, decide whether f is equal to g. Indeed, all known deterministic algorithms solving this problem have exponential complexity at least $\mathcal{O}(2^L)$. In this article, we are going to use *probabilistic* algorithms to solve the identity testing problem, based on the following result:

Theorem 14 ((Schwartz, 1980), (Zippel, 1979), (Zippel, 1993))
Let be given a nonzero polynomial f in $k[\Theta_i X]$ of degree at most d, and let be given a finite subset $\mathcal{A}$ of k. Then the set $\mathcal{A}^{n(i+1)}$ contains at most $d\#(\mathcal{A})^{n(i+1)-1}$ zeros of f.

For the analysis of our algorithms, we shall interpret the statement of Theorem 14 in terms of probabilities. More precisely, given a fix nonzero polynomial f in $k[\Theta_i X]$ of degree at most d, and given a fix subset $\mathcal{A}$ of k, from Theorem 14 we conclude that the probability of choosing randomly a point a in $\mathcal{A}^{n(i+1)}$ such that $f(a) = 0$ holds is bounded from above by $d/\#(\mathcal{A})$. Here, we assume a uniform distribution of probability on the elements of the set $\mathcal{A}^{n(i+1)}$.

We shall applied this result in the following way: given a straight–line program of length L representing a polynomial f in $k[\Theta_i X]$ of degree at most d, we compute the value $f(a)$, where a is a point in $k^{n(i+1)}$ whose coordinates are chosen randomly in a given finite subset $\mathcal{A}$ of k. Then, if $f(a) = 0$ we conclude that $f = 0$, which holds true with probability at least $1 - d/\#(\mathcal{A})$. Such a probabilistic test is called the Zippel–Schwartz test. We remark that the Zippel–Schwartz test requires L arithmetic operations.

Our model of computation is based on the concept of straight–line programs. However, a model of computation consisting *only* of straight–line programs is not expressive enough for our purposes. Therefore our model of computation has to include decisions and selections (subject to previous decisions). For this reason we shall consider computation trees instead of straight–line programs. A *computation tree* is nothing but a straight–line program which includes selections, subject to previous equal–to–zero decisions, i.e. a straight–line program with *branchings*. The length of a given computation tree is defined analogously as in the case of straight–line programs (see e.g. (Bürgisser et al., 1997) for more details on the notion of computation trees).

5.2 Specialization in a generic point

Theorems 10, 11 and 12 show that the computation of the differentiation index of system (6), the differential Hilbert function $\mathcal{H}_K$ and an algebraic parametric set of the differential ideal Δ with respect to K can be easily reduced to the computation of the $\mathcal{F}$–rank or certain submatrices of the Jacobian matrix $J(2n-2, 0)$. The definition of this matrix involves the set of polynomials $G, \ldots, G^{(2n-2)}$, and hence requires the computation of iterative derivatives of the polynomials $g_1, \ldots, g_n$ up to order $2n-2$. Unfortunately, according to Valiant (1982), such a computation cannot be performed in polynomial time, unless Valiant's arithmetic analogue of Cook's P≠NP conjecture, Valiant's Hypothesis, is false (see (Valiant, 1979), (Valiant, 1982), (von zur

Gathen, 1987), (Bürgisser et al., 1997), (Bürgisser, 2000) for background on Valiant's Hypothesis). This shows that it is very unlikely that there exists a polynomial–time algorithm computing the entries of the matrix $J(2n-2,0)$, even in the straight–line program complexity model.

Furthermore, even if we were given a straight–line program representing the entries of the matrix $J(2n-2,0)$, the statements of Theorems 10, 11 and 12 would still require the computation of the $\mathcal{F}$–rank of certain submatrices of the matrix $J(2n-2,0)$. Since arithmetic operations with elements of the field $\mathcal{F}$ cannot be performed at unit cost, usual linear algebra routines cannot be applied in a straightforward way.

In order to solve these problems, we shall apply a strategy which is based on the observation that the rank of a matrix with polynomial entries does not change by specialization of these entries in a generic point. More precisely, we observe that the entries of the matrix $J(2n-2,0)$ belong to the differential K–algebra $K\{X\}$, and the computation of the $\mathcal{F}$–rank of a given submatrix M of $J(2n-2,0)$ can be reduced to determine whether the determinant h of certain minor of M vanishes in $\mathcal{F}$, the fraction field of the quotient ring $K\{X\}/\Delta$. Observe that this determinant is an element of $K\{X\}$ whose quotient class in $\mathcal{F}$ is the zero quotient class if, and only if, h is in Δ. Therefore, applying Lemma 5 (*iii*) we conclude that h vanishes in $\mathcal{F}$ if, and only if, $h(\widetilde{X})$ is the zero element of $k\langle\widetilde{X}\rangle$, where $\widetilde{X}$ denotes the set of "symmetric" variables introduced in Section 3.3.

Let t be a new indeterminate over k. In order to effectively test the vanishing of $h(\widetilde{X})$ in $k\langle\widetilde{X}\rangle$, we observe that $h(\widetilde{X})=0$ if, and only if, the specialization $h(\eta)$ of h in a vector of generic power series η in $k[\![t]\!]^n$ vanishes in $k[\![t]\!]$. Furthermore, from the genericity of η we deduce that $h(\eta)=0$ if, and only if, the constant term $h(\eta)$ mod (t) of the power series $h(\eta)$ in $k[\![t]\!]$ vanishes.

For a given matrix M in $k\langle\widetilde{X}\rangle\{X\}^{r\times s}$, we denote by $M(\eta)$ the matrix in $k[\![t]\!]^{r\times s}$ obtained by specialization of the variables $X,\widetilde{X}$ of the entries of the matrix M into the value $X=\eta$ and $\widetilde{X}=\eta$. In order to apply the above strategy, we first exhibit an efficient algorithm computing the constant term of the entries of the matrix $J(2n-2,0)$ specialized in a given vector of power series η in $k[\![t]\!]^n$. This algorithm avoids the (inefficient) computation of the derivatives of the polynomials $g_1,\ldots,g_n$ up to order $2n-2$, by dealing with a specialization of the matrix $J(2n-2,0)$ in a given vector of power series.

The complexity estimate of this algorithm will be given in terms of quantity

$$\mathtt{M}(n) := \mathcal{O}(n\log(n)\log\log n),$$

that represents an upper bound for the number of arithmetic operations in k necessary to compute the product of two power series in $k[\![t]\!]$ up to order n,

and to invert a power series of $k[\![t]\!]$ up to order n (see e.g. (von zur Gathen and Gerhard, 1999), (Bini and Pan, 1994)).

Proposition 15 *Let be given the expansion of a vector of power series η in $k[\![t]\!]^n$ up to order $2n$. Then there exists a straight–line program computing the entries of the matrix $J(2n-2,0)(\eta)$ mod (t) with*

$$O((\mathcal{L}+n)\mathtt{M}(n)+n^4)$$

arithmetic operations in k.

Proof.– Let g_i denotes the polynomial $p_i(X,\dot{X}) - f_i(\widetilde{X},\dot{\widetilde{X}})q_i(X,\dot{X})$ in $K[X,\dot{X}]$ for $1 \leq i \leq n$, and let $G := \{g_1,\ldots,g_n\}$. Taking into account that the polynomials $p_1,q_1,\ldots,p_n,q_n$ are represented by a straight–line program of length $\mathcal{L}$, we conclude that there exists a straight–line program of length $\mathcal{O}(\mathcal{L}+n)$ representing the polynomials $g_1,\ldots,g_n$. Therefore, applying Baur–Strassen's Theorem 13 we see that there exists a straight–line program of length $\mathcal{O}(\mathcal{L}+n)$ that computes the entries of the Jacobian matrices $\partial G/\partial X$ and $\partial G/\partial \dot{X}$. The rows of these Jacobian matrices represent the coordinates of the set of Kähler differentials $\mathrm{d}G$ with respect to the basis $\{\mathrm{d}X,\mathrm{d}\dot{X}\}$ of the $K[X,\dot{X}]$–module $\Omega_{K[X,\dot{X}]/K}$. More precisely, we have the following matrix identity:

$$\mathrm{d}G = \frac{\partial G}{\partial X}\,\mathrm{d}X + \frac{\partial G}{\partial \dot{X}}\,\mathrm{d}\dot{X}. \tag{20}$$

Let us fix h with $1 \leq h \leq 2n-2$, and let $A_{h+1} := K[\Theta_{h+1}X]$. Taking into account the identity $\mathrm{d}(f') = (\mathrm{d}f)'$, from the definition of the A_{h+1}–module of Kähler differentials $\Omega_{A_{h+1}/K}$, we conclude that the following identity holds:

$$(\mathrm{d}G)^{(h)} = \mathrm{d}(G^{(h)}) = \sum_{j=0}^{h+1} \frac{\partial G^{(h)}}{\partial X^{(j)}}\,\mathrm{d}X^{(j)}. \tag{21}$$

This shows that the coordinates of the differentials $\mathrm{d}G,\ldots,\mathrm{d}G^{(2n-2)}$ in the basis $\{\mathrm{d}X,\ldots,\mathrm{d}X^{(2n-1)}\}$ of $\Omega_{A_{2n-1}/K}$ represent all the entries of the Jacobian matrix $J(2n-2,0)$. In order to compute these coordinates, we observe that applying Leibniz's rule to identity (20) we obtain the following identity:

$$\begin{aligned}
(\mathrm{d}G)^{(h)} &= \left(\frac{\partial G}{\partial X}\,\mathrm{d}X\right)^{(h)} + \left(\frac{\partial G}{\partial \dot{X}}\,\mathrm{d}\dot{X}\right)^{(h)} \\
&= \frac{\partial G}{\partial \dot{X}}\mathrm{d}X^{(h+1)} + \left(\frac{\partial G}{\partial X}\right)^{(h)}\mathrm{d}X + \\
&\quad + \sum_{j=1}^{h}\left(\binom{h}{j-1}\left(\frac{\partial G}{\partial X}\right)^{(j-1)} + \binom{h}{j}\left(\frac{\partial G}{\partial \dot{X}}\right)^{(j)}\right)\mathrm{d}X^{(h-j+1)},
\end{aligned} \tag{22}$$

where the symbols $(\partial G/\partial X)^{(j)}$ and $(\partial G/\partial \dot{X})^{(j)}$ mean the j–th order entry–wise derivative of the matrices $\partial G/\partial X$ and $\partial G/\partial \dot{X}$. This shows that any submatrix $\partial G^{(h)}/\partial X^{(j)}$ of the Jacobian matrix $J(2n-2,0)$ occurring in identity (21) can be expressed as the sum of at most two derivatives of the matrices $\partial G/\partial X$, $\partial G/\partial \dot{X}$ of order at most h.

Now we estimate the complexity of computing the constant term of the entries of the matrices $(\partial G/\partial X)^{(j)}(\eta), (\partial G/\partial \dot{X})^{(j)}(\eta)$, assuming that these matrices are well–defined and their entries belong to $k[\![t]\!]$. Suppose that we are given the expansion of the vector of power series η up to order $2n$, i.e. we are given a vector of polynomials η_{2n-1} in $k[t]$ of degree at most $2n-1$, satisfying the congruence relation $\eta \equiv \eta_{2n-1} \bmod (t^{\,2n})$ in $k[\![t]\!]^n$. Then, we conclude that the following congruence relations hold in $k[\![t]\!]^{n\times n}$ for $0 \le j \le 2n-2$:

$$\begin{aligned}\left(\frac{\partial G}{\partial X}\right)^{(j)}(\eta) &\equiv \left(\frac{\partial G}{\partial X}\right)^{(j)}(\eta_{2n-1}) \mod (t^{\,2n-j-1}),\\ \left(\frac{\partial G}{\partial \dot{X}}\right)^{(j)}(\eta) &\equiv \left(\frac{\partial G}{\partial \dot{X}}\right)^{(j)}(\eta_{2n-1}) \mod (t^{\,2n-j-1}).\end{aligned}$$

In particular, we have for $0 \le j \le 2n-2$:

$$\begin{aligned}\left(\frac{\partial G}{\partial X}\right)^{(j)}(\eta) &\equiv \left(\frac{\partial G}{\partial X}\right)^{(j)}(\eta_{2n-1}) \mod (t),\\ \left(\frac{\partial G}{\partial \dot{X}}\right)^{(j)}(\eta) &\equiv \left(\frac{\partial G}{\partial \dot{X}}\right)^{(j)}(\eta_{2n-1}) \mod (t).\end{aligned} \tag{23}$$

Since there exists a straight–line program β of length $\mathcal{O}(\mathcal{L}+n)$ computing the entries of the matrices $\partial G/\partial X$ and $\partial G/\partial X$, we conclude that the entries of the matrices $(\partial G/\partial X)(\eta_{2n-1})$, $(\partial G/\partial X)(\eta_{2n-1})$ up to order $2n-1$ can be computed by executing the straight–line program β, with the variables $X, \widetilde{X}$ instantiated into the values $X=\eta$ and $\widetilde{X}=\eta$, and performing arithmetic operations in $k[\![t]\!]$ modulo $(t^{\,2n-1})$. This procedure requires $\mathcal{O}((\mathcal{L}+n)\mathtt{M}(n))$ arithmetic operations in k, and outputs the dense representation of the entries of the matrices $(\partial G/\partial X)(\eta_{2n-1})$ and $(\partial G/\partial X)(\eta_{2n-1})$ modulo $(t^{\,2n-1})$. Using this data, for $1 \le j \le 2n-2$ the dense representation of the entries of the matrices $(\partial G/\partial X)^{(j)}(\eta_{2n-1})$, $(\partial G/\partial \dot{X})^{(j)}(\eta_{2n-1})$ up to order $2n-j-1$ can be easily computed with $O(n^3)$ additional arithmetic operations in k. Finally, using identities (21), (22) and (23) we conclude that the constant term of the entries of the matrices $(\partial G^{(h)}/\partial X^{(j)})(\eta)$ can be computed with $O(n^4)$ additional arithmetic operations in k. Adding the complexity estimates of all the steps of this procedure, we deduce the complexity estimate stated in Proposition 15. ∎

Proposition 15 is the key point which allows us to obtain efficient algorithms computing the discrete invariants mentioned at the beginning of this section. These algorithms depend on the (random) choice of a vector of power series η satisfying certain genericity condition, whose probability of success we estimate. The complexity of these algorithms will be measured in terms of the complexity $\mathcal{O}(n^\omega)$ of the multiplication of two $(n \times n)$–matrices with entries in k. We have the estimate $\omega \leq 2.376$ (see Coppersmith and Winograd, 1990).

Theorem 16 *Let notations and assumptions be as above. There exists a computation tree of length* $\mathcal{O}(\mathcal{L}\,\mathtt{M}(n) + (n)^{1+2\omega})$ *computing the differential Hilbert function* $\mathcal{H}_K$ *of the differential ideal* Δ *with respect to* K*. Furthermore, for any* κ *in* $\mathbb{N}$*, the parameters of such a computation tree can be randomly chosen in the set* $\{1, \ldots, 2\kappa dn(n+1)^3\}$ *with a probability of success of at least* $1 - 1/(2\kappa)$*, where* d *is an upper bound for the degrees of the polynomials* $p_1, q_1, \ldots, p_n, q_n$*.*

Proof.– Applying Theorem 10 we conclude that the computation of the differential Hilbert function $\mathcal{H}_K$ can be reduced to the computation of the $\mathcal{F}$–ranks of the matrices $J(2n-2,0), \ldots, J(2n-2,n)$. Let us fix for the moment a nonsingular square submatrix M_i of maximal size of the matrix $J(2n-2,i)$ for $0 \leq i \leq n$. Observe that the matrix M_i has size at most $n(2n-i) \times n(2n-i)$. Suppose that we are given a vector of power series η in $k[\![t]\!]^n$ such that the following conditions are satisfied for $0 \leq i \leq n$:

(i) the matrices $J(2n-2,i)(\eta)$ and $M_i(\eta)$ are well–defined and have their entries in $k[\![t]\!]$,
(ii) $\det\left(M_i(\eta)\right) \bmod (t) \neq 0$.

We conclude that the identity

$$\operatorname{rank}_{\mathcal{F}} J(2n-2,i) = \operatorname{rank}_k\Big(J(2n-2,i)(\eta) \bmod (t)\Big)$$

holds for $0 \leq i \leq n$.

Now we estimate the probability of finding of vector of power series η in $k[\![t]\!]$ satisfying conditions (i) and (ii). According to Proposition 15, if we are given the development η_{2n-1} up to order $2n$ of the vector of power series η, then the constant terms of the entries of the matrix $J(2n-2,0)$, and hence of the matrices $M_0, \ldots, M_{n-1}$, can be efficiently determined.

Let us denotes by η_{2n-1} the polynomial $\sum_{i=0}^{2n-1} \eta_{2n-1}^{(i)} t^i$. From the definition of the matrices $\partial G^{(h)}/\partial X^{(l)}$ it is easy to see that the (reduced) denominator of any entry of such matrices is an element of $k[\widetilde{X}, \dot{\widetilde{X}}]$ divisible by a power of the poly-

nomial $q := \prod_{j=1}^{n} q_j$. Therefore, condition (i) will be fulfilled if $q(\eta_{2n-1}) \neq 0$ holds. On the other hand, if p denotes the numerator of a reduced representation of the rational function $\prod_{i=0}^{n-1} \det M_i$, then it is clear that condition (ii) is satisfied if the constant term $\widehat{p}(\eta_{2n-1}^{(0)}, \ldots, \eta_{2n-1}^{(2n-1)})$ of the polynomial $p(\eta_{2n-1})$ in $k[t]$ does not vanish. Therefore, conditions (i) and (ii) are satisfied if the following condition holds:

$$(q\widehat{p})\left(\eta_{2n-1}^{(0)}, \ldots, \eta_{2n-1}^{(2n-1)}\right) \neq 0. \tag{24}$$

Since the degrees of the polynomials $p_1, q_1, \ldots, p_{n-1}, q_{n-1}$ are bounded by $d>0$, it is easy to see that the degrees of the numerator and denominator of a reduced representation of the rational function $(p_l/q_l)^{(i)}$ are bounded by $d(i+1)$. From this we conclude that any entry of the matrix $\partial G^{(i)}/\partial X^{(j)}$ is a rational function of $k\langle\widetilde{X}\rangle\{X\}$ of degree at most $d(i+2)$. Therefore, $\det M_i$ is a rational function of $k\langle\widetilde{X}\rangle\{X\}$ of degree at most $dn(2n-i)(i+2)$, and the numerator p of the product $\prod_{i=0}^{n} \det M_i$ has degree at most $dn^2(n+1)^2$. We conclude that the product $(q\widehat{p})(\eta_{2n-1}^{(0)}, \ldots, \eta_{2n-1}^{(2n-1)})$ is a nonzero polynomial of degree at most $dn(n+1)^3$ in the coordinates of the vectors $\eta_{2n-1}^{(0)}, \ldots, \eta_{2n-1}^{(2n-1)}$. Applying the Zippel–Schwartz test (Theorem 14), we conclude that the coordinates of the vectors $\eta_{2n-1}^{(0)}, \ldots, \eta_{2n-1}^{(2n-1)}$ can be randomly chosen in the set $n\{1, \ldots, 2\kappa dn(n+1)^3\}$ with a probability of success of at least $1 - 1/(2\kappa)$.

Assume that we are given such a vector of polynomials η_{2n-1}. Applying Proposition 15 we see that there exists a straight–line program of length

$$O((\mathcal{L}+n)\,\mathtt{M}(n) + n^4)$$

computing the constant term of the entries of the matrix $J(2n-2, i)(\eta_{2n-1})$. Since the matrices $J(2n-2, 0), \ldots, J(2n-2, n)$ have size at most $2n^2 \times 2n^2$, the ranks

$$\mathrm{rank}_k\Big(J(2n-2,0)(\eta_{2n-1}) \bmod (t)\Big), \ldots, \mathrm{rank}_k\Big(J(2n-2,n)(\eta_{2n-1}) \bmod (t)\Big)$$

can be computed using $\mathcal{O}(n(n^2)^\omega)$ arithmetic operations in k. Therefore, the differential Hilbert function $\mathcal{H}_K$ can be computed with $\mathcal{O}(\mathcal{L}\,\mathtt{M}(n) + n^{1+2\omega})$ arithmetic operations in k. ∎

Suppose now that we are given the differential Hilbert $\mathcal{H}_K$ of the differential ideal Δ with respect to K. We describe an efficient algorithm computing the differentiation index of system (6).

Theorem 17 *Let notations and assumptions be as above. There exists a computation tree of length $\mathcal{O}(\mathcal{L}\,\mathtt{M}(n) + n^{1+2\omega})$ computing the differentiation index of system (6). Furthermore, for any κ in $\mathbb{N}$, the parameters of such a computation tree can be randomly chosen in the set $\{1, \ldots, 2\kappa dn(n+1)^3\}$ with a probability of success of at least $1 - 1/(2\kappa)$.*

PROOF.– Theorem 11 shows that the differentiation index ν is the least positive integer such that the following condition is satisfied:

$$\mathcal{H}_K(\ell) = \mathrm{rank}_{\mathcal{F}} J(\nu, 0) - \mathrm{rank}_{\mathcal{F}} J(\nu, \ell+1).$$

Therefore, in order to compute the number ν, we have to compute the $\mathcal{F}$–ranks of the matrices $J(\ell, 0), \ldots, J(2n-2, 0), J(\ell, \ell+1), \ldots, J(2n-2, \ell+1)$.

In order to compute these ranks, arguing as in the proof of Theorem 16, we see that

$$\mathrm{rank}_{\mathcal{F}} J(i,j) = \mathrm{rank}_k\Big(J(i,j)(\eta_{2n-1}) \bmod (t)\Big)$$

holds for $\ell \leq i \leq 2n-2$ and j in $\{0, \ell+1\}$, where η_{2n-1} represents in $k[t]^n$ the development up to order $2n$ of a power series η in $k[\![t]\!]$ which satisfies the following conditions for $\ell \leq i \leq 2n-2$ and j in $\{0, \ell+1\}$:

(i) the matrix $J(i,j)(\eta)$ is well–defined and has their entries in $k[\![t]\!]$,
(ii) if $M_{i,j}$ denotes a nonsingular square submatrix of $J(i,j)$ of maximal size, then $\det\left(M_{i,j}(\eta)\right) \bmod (t) \neq 0$.

With the same arguments as in the proof of Theorem 17, we deduce that the coordinates of the coefficients $\eta_{2n-1}^{(0)}, \ldots, \eta_{2n-1}^{(2n-1)}$ of η_{2n-1} can be randomly chosen in the set $\{1, \ldots, 2\kappa n d (n+1)^3\}$ with a probability of success of at least $1 - 1/(2\kappa)$.

Suppose that we are given such a vector η_{2n-2}. Then Proposition 15 shows that there exists a straight–line program of length $O(\mathcal{L}\,\mathtt{M}(n) + n^4)$ computing the constant terms of the entries of the matrices $J(i,j)(\eta_{2n-1})$ for $\ell \leq i \leq 2n-2$ and j in $\{0, \ell+1\}$. Since these are matrices of size at most $2n^2 \times 2n^2$, their ranks can be computed using $\mathcal{O}(n^{1+2\omega})$ arithmetic operations in k. Therefore, the differentiation index of system (6) can be computed with $\mathcal{O}(\mathcal{L}\,\mathtt{M}(n) + n^{1+2\omega})$ arithmetic operations in k. ∎

Finally, suppose that we are given the differentiation index ν of system (6) and the differential Hilbert function $\mathcal{H}_K$ of the differential ideal Δ with respect to K. We describe an algorithm computing an algebraic parametric set of the ideal Δ with respect to K:

Theorem 18 *Let notations and assumptions be as above. There exists a computation tree of length $\mathcal{O}(\mathcal{L}\,\mathtt{M}(\nu) + n\ell(\nu n)^\omega)$ computing an algebraic parametric set of the differential ideal Δ with respect to the differential field K. Furthermore, for any κ in $\mathbb{N}$, the parameters of such a computation tree can be randomly chosen in the set $\{1, \ldots, 2\kappa d \ell n^2 (\nu+2)^3\}$ with a probability of success of at least $1 - 1/(2\kappa)$.*

PROOF.– Theorem 12 shows that any subset $\mathcal{C}$ of $\Theta_{\ell-1}X$ satisfying the conditions

$$\#(\mathcal{C}) = \mathrm{ord}_K\Delta \quad \text{and} \quad \mathrm{rank}_{\mathcal{F}} J^{(\mathcal{C})}(\nu, 0) = \mathrm{rank}_{\mathcal{F}} J(\nu, 0),$$

is an algebraic parametric set of Δ with respect to K, where $J^{(\mathcal{C})}(\nu, 0)$ denotes the submatrix of the Jacobian matrix $J(\nu, 0)$ obtained by deleting the columns of $J(\nu, 0)$ corresponding to the derivatives in $\mathcal{C}$.

The algorithm computing an algebraic parametric set $\mathcal{C}$ of the ideal Δ proceeds in at most $n(\ell + 1)$ steps, starting with the matrix $J_0 := J(\nu, 0)$ and $\mathcal{C}_0 := \emptyset$. In the i–th step, let $\widetilde{J}_i$ be the submatrix of the matrix J_{i-1} of the previous step obtained by deleting the $(n(\nu + 2) - i)$–th column of J_{i-1}, and denote z_i the derivative corresponding to the $(n(\nu + 2) - i)$–th column of $J(\nu, 0)$. Then we define $J_i := \widetilde{J}_i$ and $\mathcal{C}_i := \mathcal{C}_{i-1} \cup \{z_i\}$, if $\mathrm{rank}_{\mathcal{F}} \widetilde{J}_i$ is equal to $\mathrm{rank}_{\mathcal{F}} J_{i-1}$, and $J_i =: J_{i-1}$ and $\mathcal{C}_i := \mathcal{C}_{i-1}$ otherwise. This procedure stops when the condition $\#(\mathcal{C}_i) = \mathrm{ord}_K\Delta$ is satisfied.

We claim that when the procedure stops, after $N \leq n(\ell + 1)$ steps, the resulting set $\mathcal{C}_N$ is an algebraic parametric set of Δ with respect to K. Indeed, arguing as in the proof of identity (19), we see that $\mathrm{rank}_{\mathcal{F}} J_i = \mathrm{rank}_{\mathcal{F}} J_{i-1}$ if, and only if, z_i in $\mathcal{F}$ is not algebraic over $(\mathcal{S}^\infty)^{-1}K[\mathcal{C}_{i-1}]$. Therefore, for any $i \geq 0$ the set $\mathcal{C}_i$ is algebraically independent over K, and the set $\mathcal{C}_N$ must be a transcendence basis of the field extension $K \subset \mathcal{F}$. The procedure stops since there exist algebraic parametric sets of Δ. This shows our claim.

This procedure requires the computation of the $\mathcal{F}$–ranks of $N \leq n(\ell + 1)$ submatrices of the matrix $J(\nu, 0)$. Arguing as in the proof of Theorem 16, we see that

$$\mathrm{rank}_{\mathcal{F}} J_i = \mathrm{rank}_k\Big(J_i(\eta_{\nu+1}) \bmod (t)\Big)$$

holds for $0 \leq i \leq N$, where $\eta_{\nu+1}$ represents in $k[t]^n$ the development up to order $\nu + 2$ of a power series η in $k[\![t]\!]$ whose coordinates can be randomly chosen in the set $\{1, \ldots, 2\kappa d\ell n^2(\nu + 2)^2\}$ with a probability of success of at least $1 - 1/(2\kappa)$. Assume that we are given such a vector of polynomials $\eta_{\nu+1}$.

With the same arguments as in the proof of Proposition 15 we see that there exists a straight–line program of length $O((\mathcal{L} + n)\,\mathtt{M}(\nu) + n^2\nu^2)$ computing the constant terms of the entries of the matrix $J(\nu, 0)(\eta_{\nu+1})$. Since the matrices $J_0, \ldots, J_N$ have size at most $n(\nu + 2) \times n(\nu + 3)$, the ranks

$$\mathrm{rank}_k\Big(J_0(\eta_{\nu+1}) \bmod (t)\Big), \ldots, \mathrm{rank}_k\Big(J_N(\eta_{\nu+1}) \bmod (t)\Big)$$

can be computed using $\mathcal{O}(n\ell(\nu n)^\omega)$ arithmetic operations in k. Therefore, an algebraic parametric set of the differential ideal Δ with respect to K can be computed with $\mathcal{O}(\mathcal{L}\,\mathtt{M}(n) + n\ell(\nu n)^\omega)$ arithmetic operations in k. ∎

6 Conclusions

Algorithms for the symbolic solution of systems of differential equations are usually based on rewriting techniques, which output *complete* symbolic information of the underlying solution set. Therefore, they are *universal solvers* in the sense of Castro et al. (2003) and hence they have exponential–time complexity in worst case. Furthermore, numerical continuation methods which approximate *all* the solutions of a given differential equation system such as those of Reid et al. (2002) also fall in this category. This calls for the development of algorithms which are able to compute *partial* information about the solution set of the input differential equation system.

In this article we exhibit *efficient* (polynomial–time) probabilistic algorithms which compute *discrete* information relevant for the numerical integration of the solution set (see also (Sedoglavic, 2002)). We hope that our approach may be combined with numerical integration procedures in order to obtain fast and reliable algorithms for computing *one* solution of certain differential equation systems.

Acknowledgments. The authors are grateful to L. d'Alfonso and to the anonymous referees for many useful suggestions which helped to considerably improve the correctness and presentation of this paper.

References

J.L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I*, volume 11 of *EATCS Monographs on Theoretical Computer Science*. Springer Verlag, Berlin Heidelberg New York, 1988.

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

D. Bini and V. Pan. *Polynomial and Matrix Computations*. Progress in Theoretical Computer Science. Birkhäuser, Boston, 1994.

F. Boulier. Efficient computation of regular differential systems by change of rankings using Kähler differentials. Prépublication 1999–14, LIFL, Université de Lille I, 1999.

F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Representation for the radical of a finitely generated differential ideal. In A.H.M. Levelt, editor, *Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation, ISSAC'95, July 10–12, 1995, Montreal, Canada*, ACM Press, pages 158–166, New York, 1995. ACM.

K.E. Brenan, S.L. Campbell, and L.R. Petzold. *Numerical Solution of Initial–Value Problems*. Elsevier, Amsterdam, 1989.

P. Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory*, volume 7

of *Algorithms and Computation in Mathematics*. Springer, Berlin Heidelberg New York, 2000.

P. Bürgisser, M. Clausen, and M.A. Shokrollahi. *Algebraic Complexity Theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften*. Springer, Berlin Heidelberg New York, 1997.

S.L. Campbell and C.W. Gear. The index of general nonlinear DAEs. *Numerische Mathematik*, 72(2):173–196, 1995.

D. Castro, M. Giusti, J. Heintz, G. Matera, and L.M. Pardo. On the hardness of polynomial equation solving. To appear in *Foundations of Computational Mathematics*. École polytechnique, France, 2003.

T. Cluzeau and É. Hubert. Resolvent representation for regular differential ideals. *Applicable Algebra in Engineering, Communication and Computing*, 13(5):395–425, 2003.

D. Coppersmith and S. Winograd. Matrix multiplication via arithmetic progressions. *Journal of Symbolic Computation*, 9(3):251–280, 1990.

D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer, Berlin Heidelberg New York, 1995.

M. Fliess, J. Lévine, P. Martin, and P. Rouchon. Implicit differential equations and Lie–Bäcklund mapping. In *Proceedings of 34th IEEE Conference on Decision and Control New Orleans, LA, 13–15 December 1995*, IEEE Press. IEEE, 1995a.

M. Fliess, J. Lévine, P. Martin, and P. Rouchon. Index and decomposition of nonlinear implicit differential equations. In *Proceedings of IFAC Conference on System Structure and Control Nantes, July 1995*, 1995b.

M. Hausdorf and W.M. Seiler. An efficient algebraic algorithm for the geometric completion to involution. *Applicable Algebra in Engineering, Communication and Computing*, 13:163–207, 2002.

J. Heintz. On the computational complexity of polynomials and bilinear mappings. A survey. In L. Huguet and A. Poli, editors, *Proceedings 5th International Symposium on Applied Algebra, Algebraic Algorithms and Error–Correcting Codes, AAECC–5, Menorca, Spain, June 15–19, 1987*, volume 356 of *Lecture Notes in Computer Science*, pages 269–300, Berlin Heidelberg New York, 1989. Springer.

É. Hubert. Factorization–free decomposition algorithms in differential algebra. *Journal of Symbolic Computation*, 29(4& 5):641–662, 2000.

J. Johnson. Kähler differentials and differential algebra. *Annals of Mathematics*, 89 (1):92–98, 1969.

J. Johnson. Kähler differentials and differential algebra in arbitrary characteristic. *Transactions of the American Mathematical Society*, 192:201–208, 1974.

E. Kolchin. *Differential Algebra and Algebraic Groups*, volume 54 of *Pure and Applied Mathematics*. Academic Press, New York London, 1973.

E. Kunz. *Kähler Differentials*. Advanced Lectures in Mathematics. Vieweg Verlag, 1986.

H. Maârouf, A. Kandry Rody, and M. Ssafini. Triviality and dimension of a system of algebraic differential equations. *Journal of Automated Reasoning*, 20(3):365–385, 1998.

E.L. Mansfield. *Differential Gröbner bases*. PhD thesis, University of Sydney, 1991.

G. Matera and A. Sedoglavic. The differential Hilbert function of a differential

rational mapping can be computed in polynomial time. In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, Lille, France, July 07–10, 2002*, ACM Press, pages 184–191, New York, 2002.

H. Matsumura. *Commutative Ring Theory*. Cambridge University Press, 1986.

J. Morgenstern. How to compute fast a function an all its derivatives. A variation on the theorem of Baur–Strassen. *SIGACT News*, 16(4):60–62, 1984.

F. Ollivier. *Le problème de l'identifiabilité globale: étude théorique, méthodes effectives et bornes de complexité*. PhD thesis, École polytechnique, France, 1990. n

L.M. Pardo. How lower and upper complexity bounds meet in elimination theory. In G. Cohen, M. Giusti, and T. Mora, editors, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings of AAECC–11*, volume 948 of *Lecture Notes in Computer Science*, pages 33–69, Berlin Heidelberg New York, 1995. Springer.

G. Reid, P. Lin, and A.D. Wittkopf. Differential elimination–completion algorithms for DAE and PDAE. *Studies in Applied Mathematics*, 106(1):1–45, 2001.

G. Reid, C. Smith, and J. Verschelde. Geometric completion of differential systems using numeric–symbolic continuation. *SIGSAM Bulletin*, 36(2):1–17, 2002.

J.F. Ritt. *Differential Algebra*, volume XXXIII of *Colloquium Publications*. American Mathematical Society, New York, 1950.

B. Sadik. A bound for the order of characteristic set elements of an ordinary prime differential ideal and some applications. *Applicable Algebra in Engineering, Communication and Computing*, 10(3):251–268, 2000.

J.T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the Association for Computing Machinery*, 27(4):701–717, 1980.

A. Sedoglavic. *Méthodes seminumériques en algèbre différentielle ; applications à l'étude des propriétés structurelles de systèmes différentiels algébriques en automatique*. PhD thesis, École polytechnique, 2001.

A. Sedoglavic. A probabilistic algorithm to test local algebraic observability in polynomial time. *Journal of Symbolic Computation*, 33(5):735–755, 2002.

V. Strassen. Algebraic complexity theory. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, chapter 11, pages 634–671. Elsevier, Amsterdam, 1990.

L. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8:189–201, 1979.

L. Valiant. Reducibility by algebraic projections. *L'Enseignement mathématique*, 28(3–4):253–268, 1982.

J. von zur Gathen. Feasible arithmetic computations: Valiant's Hypothesis. *Journal of Symbolic Computation*, 4(2):137–172, 1987.

J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, Cambridge, 1999.

R. Zippel. Probabilistic algorithms for sparse polynomials. In *EUROSAM '79: Proceedings of International Symposium on Symbolic and Algebraic Computation, Marseille 1979*, volume 72 of *Lecture Notes in Computer Science*, pages 216–226. Springer, 1979.

R. Zippel. *Effective Polynomial Computation*. Kluwer Academic Publishers, Boston Dordrecht London, 1993.