The differential Hilbert function of a differential rational mapping can be computed in polynomial time

Guillermo Matera, Alexandre Sedoglavic

The differential Hilbert function of a differential rational mapping can be computed in polynomial time

Guillermo Matera
IDH, Univ. Nacional de General Sarmiento
Campus Universitario, J.M. Gutiérrez 1150
(1613) Los Polvorines, Buenos Aires, Argentina
gmatera@ungs.edu.ar

Alexandre Sedoglavic
Projet Algorithmes
INRIA – Rocquencourt
F-78153 Le Chesnay Cedex, France
Alexandre.Sedoglavic@inria.fr

ABSTRACT

We present a probabilistic seminumerical algorithm that computes the differential Hilbert function associated to a differential rational mapping. This algorithm explicitly determines the set of variables and derivatives which can be arbitrarily fixed in order to locally invert the differential mapping under consideration. The arithmetic complexity of this algorithm is polynomial in the input size.

Keywords

Differential algebra, differential Hilbert function, seminumerical algorithm.

1. INTRODUCTION

In this paper, we consider systems of ordinary algebraic differential equations

$$\begin{cases} f_1\left(x_1{}^{(e)}, \ldots, x_n{}^{(e)}, \ldots, x_1, \ldots, x_n\right) &= y_1, \\ & \vdots \\ f_n\left(x_1{}^{(e)}, \ldots, x_n{}^{(e)}, \ldots, x_1, \ldots, x_n\right) &= y_n, \end{cases} \quad (1)$$

with *generic second members* i.e. the y_i's are differentially algebraically independent. Here e and n denote two positive integers and the f_i's denote rational fractions.

When the jacobian matrix of $(f_1, \ldots, f_n)$ w.r.t. the higher order indeterminates (its symbol) has full rank, the system (1) can be locally rewritten as an equivalent *explicit system* using the Implicit Function Theorem. In fact, each $x_i{}^{(e)}$ may be locally expressed as a function of the y_i's and of some lower order derivatives of the x_i's. Hence, if the y_i's and enough initial conditions are given, one can obtain numerical approximations for the x_i's as a consequence of Cauchy Theorem. Hence, the mapping (1) is *numerically invertible*.

In *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation* (Lille, France, Jan. 2002), T. Mora, Ed., ACM, ACM press, pp. 184–191.

If the symbol of the system (1) is singular, the solution of such a Cauchy problem is not straightforward. A formal process which involves differentiation and elimination is usually applied in order to obtain an explicit system equivalent to (1) in this case. This process can be done using rewriting techniques such as the Rosenfeld – Gröbner algorithm [3, 8] or the algorithm presented in [13]. The complexity of these procedures is not precisely known but it is likely to be exponential in the input size.

Here we adopt a different point of view and propose an algorithm which determines only some specific information concerning the *prime ordinary differential ideal* associated to the system (1). This information does not include the computation of an explicit system equivalent to (1). Nevertheless, our algorithm determines

- the highest order ν of derivatives of the equations in (1) which must be computed in order to (locally) obtain an equivalent explicit form of system (1). This—non intrinsic—number ν is usually called the *differentiation index* of the system (1) (see [4] for more details about this notion);
- for each order of derivation i, the number of independent initial conditions which can be arbitrarily fixed in the set of derivatives $\{x_1{}^{(i)}, \ldots, x_n{}^{(i)}\}$'s. This number is given by the *differential Hilbert function* associated to the rational mapping defined by the system (1).
- more precisely, our algorithm explicitly determines a maximal set of variables whose initial conditions can be arbitrarily fixed and therefore, a set of variables which are algebraic w.r.t. them (see Example 1 below).

Our algorithm is based on the computation of formal derivatives and ranks of generically specialized matrices. It avoids the computation of characteristic sets and its arithmetic complexity is polynomial in the *input size*.

Our interest in these questions is due to the fact that the above information can be used as a basis for an elimination algorithm inspired by the techniques developed by the TERA group [11, 6, 7]. This elimination algorithm, which is not based on rewriting techniques, takes system (1) as input and returns a program computing a numerical approximation

of the x_i's, given the values of the y_i's and enough initial conditions. Furthermore, its complexity is precisely known (see Section 4 in [16] for more details); this result will be the subject of a forthcoming work.

We finish this introduction by presenting three simple examples of differential rational mappings which illustrate the notions introduced above.

Example 1. Our first example is the following linear system introduced by M. Fliess and col.

$$\left\{\begin{array}{rcl} x_1 & = & y_1, \\ \dot{x}_1 + x_2 & = & y_2, \\ & \vdots & \\ \dot{x}_{n-2} + x_{n-1} & = & y_{n-1}, \\ \dot{x}_n + \dot{x}_{n-1} & = & y_n, \end{array}\right. \tag{2}$$

When the y_i's are specialized into arbitrary functions of the time variable t, this system describes a vector field

$$\dot{x}_n = y_n - \dot{y}_{n-1} + \cdots + (-1)^n {y_1}^{(n-1)}, \tag{3}$$

on the *constraint* variety defined by the following relations

$$\left\{\begin{array}{rcl} x_1 & = & y_1, \\ x_2 & = & y_2 - \dot{y}_1, \\ & \vdots & \\ x_{n-1} & = & y_{n-1} - \dot{y}_{n-2} + \cdots + (-1)^{n-2} {y_1}^{(n-2)}. \end{array}\right. \tag{4}$$

This example shows that it is necessary to compute derivatives of the original equations—and thus, some higher order derivatives of the variables y_i's—to obtain an equivalent explicit form of our original system.

The differentiation index of system (3) – (4) is $n-1$, the initial condition of variable x_n can be arbitrarily fixed and the variables $x_1, \ldots, x_{n-1}$ and $\dot{x}_n$ are algebraic w.r.t. the field extension generated by the y_i's and their derivatives. Our algorithm provides this information without computing the equivalent explicit system (3) – (4).

Example 2. The following system is an involutive differential transformation originally introduced by P. Rouchon.

$$\left\{\begin{array}{l} \dot{x}_2/\ddot{x}_1 = y_1, \\ (\dot{x}_2/\ddot{x}_1)' x_1 - \dot{x}_1 \dot{x}_2/\ddot{x}_1 + x_2 = y_2. \end{array}\right.$$

Our algorithm indicates that the differentiation index is 3, and determines that x_1 and x_2 are algebraic over the extension field generated by the y_i's and their derivatives. In fact, using differentiation and elimination, one can retrieve the following relations:

$$x_1 = \dot{y}_2/\ddot{y}_1, \qquad x_2 = (\dot{y}_2/\ddot{y}_1)' y_1 - \dot{y}_1 \dot{y}_2/\ddot{y}_1 + y_2.$$

Hence, if we suppose that $\ddot{y}_1$ is different from 0, the x_i's are—non differential—rational functions of the y_i's and their derivatives. Hence, there is no need of fixing initial conditions for the x_i's in this example.

Example 3. Let us consider a curve C in a three dimensional space with coordinates x_1, x_2 and x_3. The following classical system expresses—the square of—the speed y_1, the curvature y_2 and the torsion y_3 of the curve C in terms of its parametrization.

$$\left\{\begin{array}{rcl} {\dot{x}_1}^2 + {\dot{x}_2}^2 + {\dot{x}_3}^2 & = & y_1, \\ \dfrac{\left|\begin{array}{cc} \dot{x}_1 & \dot{x}_2 \\ \ddot{x}_1 & \ddot{x}_2 \end{array}\right|^2 + \left|\begin{array}{cc} \dot{x}_2 & \dot{x}_3 \\ \ddot{x}_2 & \ddot{x}_3 \end{array}\right|^2 + \left|\begin{array}{cc} \dot{x}_3 & \dot{x}_1 \\ \ddot{x}_3 & \ddot{x}_1 \end{array}\right|^2}{\left({\dot{x}_1}^2 + {\dot{x}_2}^2 + {\dot{x}_3}^2\right)^3} & = & y_2, \\ \dfrac{\left|\begin{array}{ccc} \dot{x}_1 & \dot{x}_2 & \dot{x}_3 \\ \ddot{x}_1 & \ddot{x}_2 & \ddot{x}_3 \\ {x_1}^{(3)} & {x_2}^{(3)} & {x_3}^{(3)} \end{array}\right|}{\left|\begin{array}{cc} \dot{x}_1 & \dot{x}_2 \\ \ddot{x}_1 & \ddot{x}_2 \end{array}\right|^2 + \left|\begin{array}{cc} \dot{x}_2 & \dot{x}_3 \\ \ddot{x}_2 & \ddot{x}_3 \end{array}\right|^2 + \left|\begin{array}{cc} \dot{x}_3 & \dot{x}_1 \\ \ddot{x}_3 & \ddot{x}_1 \end{array}\right|^2} & = & y_3. \end{array}\right. \tag{5}$$

Unlike Example 2, the explicit form of the system (5) can not be easily determined by hand computations. Our method allows us to retrieve the following well-known property of a space curve: a smooth curve is locally uniquely determined by this system if the speed, the curvature, the torsion and six initial conditions are given. There are also similar systems which describe the same situation in higher dimensional ambient spaces.

Although the solution of the above examples does not require any sophisticated algorithm, it is easy to see that a slightly different situation may become intractable for real–world computers. In fact, from the above examples it is possible to construct implicit systems whose equivalent explicit forms cannot be computed by the available computer algebra software packages, based on rewriting techniques. This is the reason why our algorithm, whose complexity is polynomial in the input size, avoids rewriting techniques. In the next sections we give a precise statement of our assertions and the outline of the paper.

1.1 Differential-Algebraic Setting

Let us recall some conventions and introduce some notation. Hereafter, considering $t = y_t$ as an equation of our original problem, we may restrict ourselves to study the autonomous case. We denote by e the order of our system and by n the dimension of its configuration space. Capital letters stand for vector-valued objects; thus, $X^{(i)}$ stands for the i-th derivatives $\left({x_1}^{(i)}, \ldots, {x_n}^{(i)}\right)$ of the configuration variables.

Differential algebra can be seen as a generalization to the setting of differential equations of the concepts of commutative algebra and algebraic geometry. We refer to [14] and [10] for a thorough presentation of differential algebra, and briefly recall here some notions which we are going to use in the sequel. Let k denote a field containing the field of rational numbers. The differential algebra $k\{X\}$ is the k-algebra of polynomials defined by an infinite set of indeterminates $\left(X^{(i)}\right)_{i\in\mathbb{N}}$, equipped with a derivation δ defined by $\delta x^{(i)} = x^{(i+1)}$ for any $i \geq 0$. Its differential fraction field is denoted by $k\langle X\rangle$. For a given finite set $P := \{p_1, \ldots, p_n\}$ of polynomials of $k\{X\}$, we denote by $[P]$ the differential ideal generated by P in $k\{X\}$, i.e. the minimal ideal of $k\{X\}$ containing the set P and closed under derivation.

In Section 2, we associate a prime differential ideal $\mathcal{I}$ to the

system (1). In this situation, one can define the differential transcendence function $\mathcal{H}_k$ associated to $\mathcal{I}$ w.r.t. to k as follows: $\mathcal{H}_k(i)$ is the Krull dimension of the non-differential prime ideal $\mathcal{I} \cap k\big[X^{(i)}, \ldots, X\big]$ in the algebra $k\big[X^{(i)}, \ldots, X\big]$.

The following theorem shows that this function has a similar behavior as the standard Hilbert function of algebraic geometry (compare [10, Chapter II, Theorem 6]).

THEOREM 1. *For any integer i large enough, the differential transcendence function $\mathcal{H}_k(i)$ of a differential ideal $\mathcal{I}$ w.r.t. the field k, is equal to the* differential dimension polynomial $(i+1)\dim_k \mathcal{I} + \mathrm{ord}_k \mathcal{I}$, *where* $\dim_k \mathcal{I}$ *denotes the* differential dimension *of the ideal $\mathcal{I}$ over k and* $\mathrm{ord}_k \mathcal{I}$ *denotes its* order.

The function $\mathcal{H}_k$ is also called the differential Hilbert function of the ideal $\mathcal{I}$ w.r.t. k. Notice that the number $\dim_k \mathcal{I}$ is an invariant of $\mathcal{I}$ over k. Indeed, any solution of $\mathcal{I}$ depends on $\dim_k \mathcal{I}$ arbitrary functions and, when they are selected, on $\mathrm{ord}_k \mathcal{I}$ arbitrary constants. If $\mathcal{I}$ is a zero-dimensional ideal over k, the number $\mathrm{ord}_k \mathcal{I}$ is an invariant of $\mathcal{I}$ and it is an upper bound for the sum of the order of the elements in any *characteristic set* of $\mathcal{I}$. In [15], the author shows that the complexity of the computation of a characteristic set of a given ideal $\mathcal{I}$ requires single exponential time (we refer to [3, 8] for more details on these computations).

In our framework, the least integer ν such that the value of the Hilbert function $\mathcal{H}_k(\nu)$ equals the differential dimension polynomial $(\nu+1)\dim_k \mathcal{I} + \mathrm{ord}_k \mathcal{I}$ is called the differentiation index of the ideal $\mathcal{I}$ (see Proposition 2 for more details). In the case of system (1), our assumptions on the genericity of the variables $y_1, \ldots, y_n$ imply that $\dim_k \mathcal{I}$ is n. Furthermore, taking into account that any equivalent explicit form of a given system F is a characteristic set of the ideal defined by the system F for a suitable ranking of the variables, the computation of the number $\mathrm{ord}_k \mathcal{I}$ provides an upper bound for the order of any explicit form equivalent to system (1).

1.2 Main Result and Outline of the Paper

Hereafter, we use intensively a common encoding of multivariate polynomials in numerical analysis (see [11, 6, 7, 17] for other applications in computer algebra). A polynomial f in $k[x_1, \ldots, x_n]$ may be represented by the vector of its coefficients or by the polynomial function it defines. A *straight-line program* representing f is a program which evaluates f at any point x in k^n. Its *complexity* is measured by its length (i.e. number of arithmetic operations) L_f. For example, the polynomial $f := (x+1)^5$ may be represented by the following sequence of instructions:

$$t_1 := x + 1, \quad t_2 := {t_1}^2, \quad t_3 := {t_2}^2, \quad f := t_3 t_1.$$

In this case, the length L_f is 4 (see Section 4.1). The following theorem summarizes the contribution of this paper.

THEOREM 2. *Let be given the system of ordinary algebraic differential equations with generic second members represented by system (1). Suppose that the rational functions defining this system are represented by a straight-line program of length L. There exists a probabilistic algorithm which computes the differentiation index and the differential Hilbert function associated to system (1). Furthermore, this algorithm finds a maximal set of variables whose initial conditions can be arbitrarily fixed. The arithmetic complexity of this algorithm is*

$$\mathcal{O}\Big(n\big((L + n^3e^2)\mathcal{M}(ne) + e\,\mathcal{N}(n^2e)\big)\Big),$$

where $\mathcal{M}(i)$ $\big($resp. $\mathcal{N}(i)\big)$ denotes the complexity of the multiplication of two univariate power series in $k[[t]]$ up to order $i+1$ (resp. of $(i \times i)$-matrix multiplication).

Outline of the paper. In the next Section, we introduce a prime differential ideal associated to system (1) which has an *evident* generic solution. Then, in Section 3, we restate our problems in terms of a suitable module of Kähler differentials, showing thus that the differential Hilbert function and the information we want to compute can be determined by rank computations. Finally, in Section 4 we exhibit an algorithm, based on specialization techniques, which proves the statement of Theorem 2.

2. DIFFERENTIAL IDEALS ASSOCIATED TO A DIFFERENTIAL RATIONAL MAPPING

In the next section, we introduce a differential ideal Γ which represents the Zariski closure of the graph associated to the rational mapping induced by system (1). Then, we define an ideal Δ which has the same differential Hilbert function as Γ and an evident generic solution.

2.1 Zariski Closure of a Graph

Let $\mathcal{I}$ be a differential ideal of $k\{X\}$, let S be a finite subset of $k\{X\}$ and let S^∞ denote the multiplicative semigroup generated by the elements in S. We define the saturation $(\mathcal{I} : S^\infty)$ of the ideal $\mathcal{I}$ by the set S as

$$(\mathcal{I} : S^\infty) = \big\{p \in k\{X\} \mid \exists\, s \in S^\infty,\ sp \in \mathcal{I}\big\}.$$

We observe that $(\mathcal{I} : S^\infty)$ is a differential ideal which contains $\mathcal{I}$ (see [10] for more details).

We now associate a saturation to system (1). For any i with $1 \le i \le n$, let us denote the numerator and denominator of the rational function f_i of system (1) by p_i and q_i respectively. System (1) is equivalent to the following system of polynomial equations and inequations:

$$\left\{\begin{array}{rcl} p_1\Big(X^{(e)}, \ldots, X\Big) - q_1\Big(X^{(e)}, \ldots, X\Big)\, y_1 &=& 0, \\ & \vdots & \\ p_n\Big(X^{(e)}, \ldots, X\Big) - q_n\Big(X^{(e)}, \ldots, X\Big)\, y_n &=& 0, \\ q_1\Big(X^{(e)}, \ldots, X\Big) &\neq& 0, \\ & \vdots & \\ q_n\Big(X^{(e)}, \ldots, X\Big) &\neq& 0. \end{array}\right.$$

Let $\mathcal{I}$ be the differential ideal generated by the differential polynomials $p_i - y_i q_i$ for $1 \le i \le n$, let $S := \{q_1, \ldots, q_n\}$ and let Γ denote the saturation of the ideal $\mathcal{I}$ by the set S in $k\{X, Y\}$. The solutions of this differential ideal constitute the Zariski closure of the graph associated to the rational mapping defined by system (1). Taking into account

that this graph is an irreducible variety, we deduce that the differential ideal $\Gamma := (\mathcal{I} : S^\infty)$ is a prime ideal of $k\{X\}$.

We consider now another ideal that provides the same information as Γ, having nevertheless an evident generic solution.

2.2 Generic Section of a Graph

Let $\widetilde{x}_1, \ldots, \widetilde{x}_n$ be new indeterminates and let ψ be the morphism defined from $k\langle Y\rangle$ into $k\langle \widetilde{X}\rangle$ that maps the fraction $\psi(y_i)$ to $f_i\big(\widetilde{X}^{(e)}, \ldots, \widetilde{X}\big)$ for $1 \leq i \leq n$. Let $\mathcal{K}$ denote the image of this morphism. Then we have:

$$\mathcal{K} = k\Big\langle\, p_i\big(\widetilde{X}^{(e)}, \ldots, \widetilde{X}\big)/q_i\big(\widetilde{X}^{(e)}, \ldots, \widetilde{X}\big),\ 1 \leq i \leq n \Big\rangle.$$

Let us denote by $\mathcal{A}$ the differential field $\mathcal{K}\langle X\rangle$ and let us consider the following morphism of differential algebras:

$$\begin{array}{rccc} \psi\ : & k\{Y, X\} & \to & \mathcal{K}\{X\} \\ & x_i & \mapsto & x_i, \\ & y_i & \mapsto & p_i\big(\widetilde{X}^{(e)},\ldots,\widetilde{X}\big)/q_i\big(\widetilde{X}^{(e)},\ldots,\widetilde{X}\big). \end{array}$$

We denote by Δ the image of Γ under the morphism ψ. The following proposition gives the main properties of Δ that we will need in the sequel.

PROPOSITION 1. *Δ is a nontrivial prime differential ideal of $\mathcal{K}\{X\}$. The differential Hilbert function of Δ w.r.t. $\mathcal{K}$ is equal to the differential Hilbert function of Γ w.r.t. $k\langle Y\rangle$. Furthermore, the element $\widetilde{X}$ of $k\langle \widetilde{X}\rangle$ is a generic solution of the differential ideal Δ.*

PROOF. Since we have supposed that $k\{Y\} \cap \Gamma = \{0\}$, the localization $k\langle Y\rangle \otimes_{k\{Y\}} \Gamma$ is a nontrivial differential ideal of the $k\langle Y\rangle$-algebra $k\langle Y\rangle\{X\}$. From the primality of Γ, we deduce that $k\langle Y\rangle \otimes_{k\{Y\}} \Gamma$ is a prime ideal. Since the morphism ψ is identity on $\mathcal{S}$ and its maps isomorphically the field $k\langle Y\rangle$ into the field $\mathcal{K}$, we conclude that the ideal $\psi(\Gamma)$ denoted by Δ is a prime differential ideal of $\mathcal{K}\{X\}$. This proves the first two assertions. In order to prove the last assertion, we consider the morphism $\varphi : \mathcal{K}\{X\} \to k\langle \widetilde{X}\rangle$ that maps x_i to $\widetilde{x}_i$ for $1 \leq i \leq n$. We remark that $\mathrm{Ker}(\varphi) = \Delta$ and the image of φ contains the k-algebra $k\{\widetilde{X}\}$. This implies that the fraction field of the quotient ring $\mathcal{K}\{X\}/\Delta$ is isomorphic to $k\langle \widetilde{X}\rangle$. This shows the last assertion. □

Remark 1. In what follows, we are going to assume without loss of generality that system (1) has order $e = 1$. Indeed, adding new variables to represent higher order derivatives (and the corresponding new relations) we can easily obtain a first-order system equivalent to the original system under consideration. Let us also remark that if the original has singular symbol then the first-order system obtained by the procedure explained above has also singular symbol. Furthermore, this observation allows us to be more precise in our definition of an explicit system. We remark that the differential mapping defined by $\dot{x}_1 = y_1$ and $x_2 = y_2$ is explicit even if its symbol—defined in introduction—is always singular. Hence, a system is *implicit* if it is not a characteristic set for an elimination ordering such that the x_i's are greater than the y_i's. Last, we need a technical hypothesis, namely that differential ideal under consideration is supposed to be *regular* (see [3] for more details).

3. LINEARIZATION OF A COMPLETION PROCESS

The Kähler differentials constitute an algebraic analogue of the linearization process of differential geometry. In this section, we are going to show how the differential Hilbert function of the prime differential ideal Δ defined in the previous section can be computed working in a suitable module of Kähler differentials. Furthermore, as shown by Example 1, in order to determine this differential Hilbert function it may be necessary to compute derivatives of the original equations up to order ν, the differentiation index associated to the system defined by the ideal Δ. We also show how this index ν can be effectively determined.

3.1 Module of Kähler differentials

Let $\mathcal{F}$ denote the fraction field of the quotient ring $\mathcal{K}\{X\}/\Delta$, which is a finitely generated extension of the field $\mathcal{K}$. Let us consider the following two $\mathcal{F}$-vector spaces:

- the space $\mathrm{Der}_{\mathcal{K}}(\mathcal{F}, \mathcal{F})$ is the set of all $\mathcal{K}$-linear derivations $\partial : \mathcal{F} \to \mathcal{F}$;
- the space $\Omega_{\mathcal{F}/\mathcal{K}}$ of Kähler differentials may be defined by the following universal property: for any $\mathcal{F}$-vector space $\mathcal{G}$ we have an isomorphism $\mathrm{Der}_{\mathcal{K}}(\mathcal{F}, \mathcal{G}) \cong \mathrm{Hom}_{\mathcal{F}}(\Omega_{\mathcal{F}/\mathcal{K}}, \mathcal{G})$. In fact, let $\mathrm{d}f$ be the image of an element f of the field $\mathcal{F}$ by the universal derivation d from $\mathcal{F}$ into $\Omega_{\mathcal{F}/\mathcal{K}}$. For any ∂ in $\mathrm{Der}_{\mathcal{K}}(\mathcal{F}, \mathcal{G})$, there exist a unique linear homomorphism δ from $\Omega_{\mathcal{F}/\mathcal{K}}$ into $\mathcal{G}$ such that $\delta(\mathrm{d}z)$ is equal to ∂z.

We refer to [5, Chapter 16] for standard definitions and properties of these vector spaces, and to [9] for analogous constructions in differential algebra. In the setting of effective differential algebra this approach was already applied in [2, 17]. We observe that the space $\Omega_{\mathcal{F}/\mathcal{K}}$ of Kähler differentials possesses a canonical structure of $\mathcal{F}$-differential vector space, defined in the following way: for any f in $\mathcal{F}$, we define $(\mathrm{d}f)' := \mathrm{d}\dot{f}$. Our computations are mainly based on the following result (see [5, Theorem 16.14]):

THEOREM 3. *Let $\mathcal{K} \subset \mathcal{F}$ be a finitely generated extension of fields of characteristic zero. For any collection of elements $\{x_\lambda\}$ in $\mathcal{F}$, the collection $\{\mathrm{d}x_\lambda\}$ is a basis of $\Omega_{\mathcal{F}/\mathcal{K}}$ as $\mathcal{F}$-vector space if, and only if, $\{x_\lambda\}$ is a transcendence basis of $\mathcal{F}$ over $\mathcal{K}$.*

Now we explain the relationship between the differential Hilbert function of the ideal Δ and the $\mathcal{F}$-vector space $\Omega_{\mathcal{F}/\mathcal{K}}$. First, we define the order of an element of $\mathcal{K}\{X\}$ as its order w.r.t. the X variables (for example, the element $x\widetilde{x}^{(h)}$ has order 0 for any $h \geq 0$). Next, we define the order of an equivalence class f in $\mathcal{K}\{X\}/\Delta$ as the minimal order of the elements belonging to the equivalence class f. Finally we define a sequence $(\mathcal{F}_i)_{i\in\mathbb{N}}$ of (non-differential) subfields of the field $\mathcal{F}$ in the following way: $\mathcal{F}_i = \big\{f \in \mathcal{F} \mid \mathrm{ord}\, f \leq i\big\}$ for any integer i. It can be easily shown that $\mathcal{F}_i$ is isomorphic to the fraction field of $\mathcal{K}\big[X, \ldots, X^{(i)}\big]/\Delta \cap \mathcal{K}\big[X, \ldots, X^{(i)}\big]$.

Remark 2. On one hand, the value $\mathcal{H}_{\mathcal{K}}(i)$ of the differential Hilbert function is equal to the (algebraic) transcendence degree of $\mathcal{F}_i$ over $\mathcal{K}$. Therefore, from Theorem 3 we

deduce that the computation of $\mathcal{H}_{\mathcal{K}}(i)$ can be reduced to the computation of the dimension of $\Omega_{\mathcal{F}_i/\mathcal{K}}$ as $\mathcal{F}_i$-vector space. On the other hand, we remark that the initial condition satisfied by any element z in $\mathcal{F}$ can be arbitrarily fixed if and only if the element z is transcendental over $\mathcal{K}$ i.e. if the transcendence degrees of $\mathcal{F}$ over $\mathcal{K}$ and of $\mathcal{F}$ over $\mathcal{K}(z)$ are different. This shows that our problems can be reduced to linear algebra computations in the $\mathcal{F}$-vector space $\Omega_{\mathcal{F}/\mathcal{K}}$. These computations are described in the next section.

3.2 Representation of $\Omega_{\mathcal{F}/\mathcal{K}}$

We introduce some notations. We denote by A and $\mathcal{A}$ the $\mathcal{K}$-algebra $A := \mathcal{K}\{X\}$ and its fraction field by $\mathcal{A}:=Fr(\mathcal{K}\{X\})$. We are going to study the transcendence degree of some field extensions associated to the prime differential ideal $\Delta \subseteq A$ of Section2.2. Using the notations,

$$g_i := p_i\big(\dot{X}, X\big) - f_i\big(\dot{\widetilde{X}}, \widetilde{X}\big)\, q_i\big(\dot{X}, X\big) \quad \text{for} \quad 1 \leq i \leq n,$$

and $\mathcal{S} := \{q_1, \ldots, q_n\}^{\infty}$, it is easy to see that the ideal Δ equals the saturation of the differential ideal $[g_1, \ldots, g_n]$ by the multiplicative set $\mathcal{S}$ in A. Furthermore, using the universal property of localizations (see e.g. [5, Chapter 2]) it can be shown the fraction field of the quotient rings $Fr(\mathcal{K}\{X\}/\Delta)$ and $Fr\big(\mathcal{K}\{X\}/[g_1, \ldots, g_n]\big)$ are isomorphic. For the sake of simplicity of notations we shall assume in the sequel that Δ is the differential ideal generated by $g_1, \ldots, g_n$. Finally, we recall that $\mathcal{F} := Fr(A/\Delta)$ denotes the fraction field of the quotient algebra A/Δ.

In our next argumentation we will deal with the $\mathcal{F}$-vector space $\mathcal{F} \otimes_A \Omega_{A/\mathcal{K}}$, obtained from the A-module $\Omega_{A/\mathcal{K}}$ by tensorization by the field $\mathcal{F}$. We observe that this vector space is not isomorphic to the vector space $\Omega_{\mathcal{F}/\mathcal{K}}$. In fact, we have the following conormal sequence of $\mathcal{F}$-vector spaces (see [5, Chapter 16]):

$$\mathcal{F} \otimes_A \big(\Delta/\Delta^2\big) \longrightarrow \mathcal{F} \otimes_A \Omega_{A/\mathcal{K}} \longrightarrow \Omega_{\mathcal{F}/\mathcal{K}} \longrightarrow 0. \quad (6)$$

In order to effectively study the $\mathcal{F}$-vector space $\Omega_{\mathcal{F}/\mathcal{K}}$, for any integer $i \geq 1$ we are going to consider the $\mathcal{K}$-algebra defined as $A_i := \mathcal{K}\big[X, \ldots, X^{(i)}\big]$ and the non-differential ideal Δ_i, generated by the polynomials $G, \ldots, G^{(i-1)}$ in A_i. We also denote by $\mathcal{A}_i := Fr(A_i/\Delta_i)$ the fraction field of the quotient algebra A_i/Δ_i. We observe that the ideals Δ_i are prime as a consequence of the genericity of second members of system (1). Similarly to (6), the relation between the $\mathcal{F}$-vector spaces $\Omega_{A_i/\mathcal{K}}$ and $\Omega_{\mathcal{A}_i/\mathcal{K}}$ is explained by the following associated conormal sequence of $\mathcal{F}$-vector spaces:

$$\mathcal{F} \otimes_{A_i} \big(\Delta_i/{\Delta_i}^2\big) \to \mathcal{F} \otimes_{A_i} \Omega_{A_i/\mathcal{K}} \to \mathcal{F} \otimes_{\mathcal{A}_i} \Omega_{\mathcal{A}_i/\mathcal{K}} \to 0. \quad (7)$$

Our computations will rely on the following two key points:

- We have an explicit representation of $\mathcal{F} \otimes_{\mathcal{A}_i} \Omega_{\mathcal{A}_i/\mathcal{K}}$. Let $h,\ i$ and j be integers such that $j \leq h \leq i-1$, and let $J(h,i,j)$ denote the following Jacobian (block) matrix:

$$\begin{pmatrix} \frac{\partial G^{(h)}}{\partial X^{(i)}} & \frac{\partial G^{(h)}}{\partial X^{(i-1)}} & \cdots & \frac{\partial G^{(h)}}{\partial X^{(j)}} \\ \vdots & \vdots & & \vdots \\ \frac{\partial G}{\partial X^{(i)}} & \frac{\partial G}{\partial X^{(i-1)}} & \cdots & \frac{\partial G}{\partial X^{(j)}} \end{pmatrix},$$

where the submatrix $\partial G^{(h)}/\partial X^{(i)}$ is given by

$$\begin{pmatrix} \frac{\partial {g_1}^{(h)}}{\partial {x_1}^{(i)}} & \cdots & \frac{\partial {g_1}^{(h)}}{\partial {x_n}^{(i)}} \\ \vdots & & \vdots \\ \frac{\partial {g_n}^{(h)}}{\partial {x_1}^{(i)}} & \cdots & \frac{\partial {g_n}^{(h)}}{\partial {x_n}^{(i)}} \end{pmatrix}.$$

Then the $\mathcal{F}$-vector space $\mathcal{F} \otimes_{\mathcal{A}_i} \Omega_{\mathcal{A}_i/\mathcal{K}}$ is represented by the cokernel of the Jacobian matrix $J(i-1,i,0)$ (see [5, §16.1]). In fact, this space is isomorphic to the quotient of the $\mathcal{F}$-vector space $\Omega_{\mathcal{A}/\mathcal{K}}$ by the subspace generated by $\mathrm{d}G, \ldots, \mathrm{d}G^{(i)}$ i.e. by the image of the $\mathcal{F}$-morphism encoded by $J(i,i+1,0)$;

- The field $\mathcal{F}_i = \big\{f \in \mathcal{F} \mid \operatorname{ord} f \leq i\big\}$ of the previous section and the field $\mathcal{A}_i$ may not coincide (see Example 1). This is due to the fact that the non-differential ideals $\Delta \cap A_i$ and Δ_i of the $\mathcal{K}$–algebra A_i, which define the fields $\mathcal{F}_i$ and $\mathcal{A}_i$, may differ for $1 < i \leq n-1$. Hence, the dimension of the vector space $\mathcal{F} \otimes_{A_i} \Omega_{\mathcal{A}_i/\mathcal{K}}$ arising in the conormal sequence (7) may differ from the dimension of $\Omega_{\mathcal{F}_i/\mathcal{K}}$ and therefore, may differ from the value of the differential Hilbert function $\mathcal{H}_{\mathcal{K}}(i)$.

Nevertheless, for any sufficiently large integer i, the—non-differential—ideals $\Delta \cap A_i$ and Δ_i coincide. We are now going to show how we can determine the least integer ν such that for any $i \geq \nu$ this property holds, and how to compute the dimension of $\mathcal{F} \otimes_{A_i} \Omega_{\mathcal{A}_i/\mathcal{K}}$ for $i < \nu$.

For this purpose, instead of analyzing the behavior of the sequence of ideals $(\Delta_i)_{i\in\mathbb{N}}$, we are going to study the sequence of matrices $\big(J(i,i+1,0)\big)_{i\in\mathbb{N}}$. First, let us consider the sequence of fraction fields $(\pi_i)_{i\in\mathbb{N}}$ associated to the prime ideals $\Delta_i \cap \mathcal{K}[X]$ i.e. for any i we define $\pi_i = \big\{f \in \mathcal{A}_i \mid \operatorname{ord} f = 0\big\}$. Since the ideals $\Delta_i \cap \mathcal{K}[X]$ form an ascending chain of prime ideals in a Noetherian ring, there exists an integer ν ($\nu \leq n$) such that the sequence $(\pi_i)_{i\in\mathbb{N}}$ becomes stationary. More precisely, we have the following proposition.

PROPOSITION 2. *Let $\phi : \mathbb{N} \to \mathbb{N}$ be the function s.t. $\phi(i)$ is equal to the transcendence degree of the field π_i over $\mathcal{K}$ for any $i \geq 0$. Then ϕ is strictly decreasing for $1 \leq i \leq \nu$ and is stationary for $i \geq \nu$. Furthermore, ν is the differentiation index of the ideal Δ.*

PROOF. We just give a sketch of the proof, which is based on the analysis of the properties of the matrices $J(i,i+1,0)$. These properties remain *generically* valid after the specialization of the matrix $J(i,i+1,0)$ at generic solution of Δ. Since Proposition 1 shows that the variables $\widetilde{X}$ define a generic solution in $k\langle\widetilde{X}\rangle$ of Δ, this field is isomorphic to $\mathcal{F}$ (see also Example 4 in Section 4.2). We conclude that it suffices to consider that, for any integer i, the matrices $J(i,i+1,0)$ encode $k\langle\widetilde{X}\rangle$-linear mappings.

We are going to argue by induction, starting with the analysis of the matrix $J(0,1,0)$. This is an $n \times 2n$-matrix whose i-th row is defined by the coordinates of the Kähler differential

$$\mathrm{d}g_i = \frac{\partial g_i}{\partial x_1}\,\mathrm{d}x_1 + \cdots + \frac{\partial g_i}{\partial x_n}\,\mathrm{d}x_n + \frac{\partial g_i}{\partial \dot{x}_1}\,\mathrm{d}\dot{x}_1 + \cdots + \frac{\partial g_i}{\partial \dot{x}_n}\,\mathrm{d}\dot{x}_n,$$

with respect to the basis defined by $\big\{\mathrm{d}X, \mathrm{d}\dot{X}\big\}$. In order to determine the dimension of the cokernel of $J(0,1,0)$, we

consider the vector space $\mathrm{Span}(\mathrm{d}G)$ generated by the $\mathrm{d}g_i$'s. Let us now fix an orderly admissible ordering on derivatives, i.e. an ordering of the variables such that $\alpha < \beta$ implies $\mathrm{d}x_h{}^{(\alpha)} < \mathrm{d}x_j{}^{(\beta)}$ and $\mathrm{d}x_h < \mathrm{d}x_j$ implies $\mathrm{d}x_h{}^{(\alpha)} < \mathrm{d}x_j{}^{(\alpha)}$. Using a simplified version of differential standard basis algorithm (see [12] for details), we obtain a basis $\{e_{0,0,h}\}$ of the vector space $E_{0,0} := \mathrm{Span}(\mathrm{d}G) \cap \mathrm{Span}(\mathrm{d}X)$ (observe that the differentials $e_{0,0,h}$ are of the form $\sum a_i \mathrm{d}x_i$). By construction, the dimension of $E_{0,0}$ is equal to $n - \phi(0)$ and the dimension of $\mathrm{Span}(\mathrm{d}G)$ is equal to $2n - \dim \Omega_{\mathcal{A}_0/\mathcal{K}}$. Now we complete the basis $\{e_{0,0,h}\}$ of $E_{0,0}$, adding elements $e_{0,1,h}$ of $\mathrm{Span}(\mathrm{d}G)$, to a basis of $\mathrm{Span}(\mathrm{d}G)$. Let us denote by $E_{0,1}$ the space generated by the $\{e_{0,1,h}\}$. Then we have $E_{0,0} \oplus E_{0,1} = \mathrm{Span}(\mathrm{d}G)$.

Now we analyze the matrix $J(1,2,0)$, which is associated to the vector space $\mathrm{Span}\big(\mathrm{d}G, \mathrm{d}G'\big)$ in $\mathrm{Span}\big(\mathrm{d}X, \mathrm{d}X', \mathrm{d}X''\big)$. From the identity $(\mathrm{d}g)' = \mathrm{d}g'$ we conclude that the set of differentials $\{e_{0,0,h}, \dot{e}_{0,0,h}, e_{0,1,h}, \dot{e}_{0,1,h}\}$ defines a basis of the space $\mathrm{Span}\big(\mathrm{d}G, \mathrm{d}G'\big)$. Now we obtain a reduced basis $\{e_{1,0,h}\}$ of $E_{1,0} = \mathrm{Span}(\mathrm{d}G, \mathrm{d}G') \cap \mathrm{Span}(\mathrm{d}X)$, and complete this basis to bases of $\mathrm{Span}(\mathrm{d}G, \mathrm{d}G') \cap \mathrm{Span}(\mathrm{d}X, \mathrm{d}X')$ and $\mathrm{Span}(\mathrm{d}G, \mathrm{d}G')$, adding elements $\{e_{1,1,h}\}$ and $\{e_{1,2,h}\}$ of the vector space $\mathrm{Span}(\mathrm{d}G, \mathrm{d}G')$. Let us denote by $E_{1,1}$ and $E_{1,2}$ the vector spaces defined by these elements respectively. Then we have $E_{1,0} \oplus E_{1,1} \oplus E_{1,2} = \mathrm{Span}(\mathrm{d}G, \mathrm{d}G')$. By construction, the dimension of $\mathrm{Span}(\mathrm{d}G, \mathrm{d}G')$ is equal to $3n - \dim \Omega_{\mathcal{A}_1/\mathcal{K}}$ and the dimension of $E_{1,0}$ is $n - \phi(1)$. Inductively we define for any $i \geq 0$ and any $j \leq i+1$ vector spaces $E_{i,j}$ with analogous properties, associated to the matrices $J(i, i+1, 0)$.

We claim that we have the following properties:

- for any positive integer i, the dimension of $E_{i,0}$ is equal to $n - \phi(i)$ and the dimension of the space $\Omega_{\mathcal{A}_i/\mathcal{K}}$ is equal to $n(i+1) - \sum_{j=0}^{i+1} \dim E_{i,j}$;
- for any integers $i \geq 0$ and $j \geq 1$, the dimension of $E_{i+1,j}$ is equal to the dimension of $E_{i,j-1}$;
- The sequence $(\dim E_{i,0})_{i \in \mathbb{N}}$ is strictly increasing for any integer i s.t. $1 \leq i \leq \nu$ and for $i > \nu$.

Our first claim is a direct consequence of the definition of the $E_{i,j}$ and sequence (7). In fact, the field π_i is the fraction field of the quotient algebra $A_0/(\Delta_i \cap A_0)$ and the $e_{i,0,h}$'s form a basis of the associated Kähler differentials. Similar results hold for the $E_{i,j}$.

Let us consider the subset $\mathrm{Ld}\, E_{i,j}$ of $\big\{\mathrm{d}X^{(i)}\big\}$ of leading monomials of the elements in $\{e_{i,j,h}\}$. For any $j \geq i+2$, the spaces $E_{i,j}$ are reduced to $\{0\}$ and for any $i \geq 0$ we have $\mathrm{Ld}\, E_{i,i+1} = \mathrm{Ld}\, \big\{e_{0,1,h}{}^{(i)}\big\}$. We remark that $\mathrm{Ld}\, E_{1,1}$ is equal to $\mathrm{Ld}\, E_{0,1} \cup \mathrm{Ld}\, \{\dot{e}_{0,0,h}\}$ and thus, the set $\mathrm{Ld}\, \{\dot{e}_{1,1,h}\}$ contains the set $\mathrm{Ld}\, \{\dot{e}_{0,1,h}\}$. Since $\mathrm{Ld}\, E_{1,2}$ is $\mathrm{Ld}\, \{\dot{e}_{0,1,h}\}$ and $\mathrm{Ld}\, E_{2,2} = \mathrm{Ld}\, E_{1,2} \cup \mathrm{Ld}\, \{\dot{e}_{1,1,h}\}$ hold, we see that $\mathrm{Ld}\, E_{2,2}$ is $\mathrm{Ld}\, \{\dot{e}_{1,1,h}\}$. A similar argument allows us to prove the identity $\mathrm{Ld}\, E_{i+1,i+1} = \mathrm{Ld}\, \{e_{1,1,h}{}^{(i)}\}$ and, more generally, we have $\mathrm{Ld}\, E_{i+j,i+j} = \mathrm{Ld}\, \{e_{j,1,h}{}^{(i)}\}$. Since the cardinal of the set $\mathrm{Ld}\, E_{i+1,i+1}$ is the dimension of $E_{i+1,i+1}$, we have proved that $\dim E_{i+j,i+j} = \dim E_{j,1}$, that is our second claim.

In order to prove our last claim, we observe that the sequence of vector spaces $(E_{i,0})_{i \in \mathbb{N}}$ is an ascending chain of vector spaces in the finite dimensional space $\mathrm{Span}\,(\mathrm{d}X)$. Hence, this sequence is stationary and there exists an integer ν such that $\mathrm{Ld}\, E_{\nu,0}$ is equal to $\mathrm{Ld}\, E_{\nu+1,0}$. There is no new eliminations between the elements of $\{\dot{e}_{\nu+1,0,h}\}$ and the elements of $\{e_{\nu+1,1,h}\}$. Therefore, for any $j \geq 0$ we have $E_{\nu,0} = E_{\nu+j,0}$ and $E_{\nu,1} = E_{\nu+j,1}$. This proves our last claim and the proposition. □

Let us observe that the differentiation index ν introduced above is bounded by ne, where e is the order of the original system (1). The following proposition gives the formulae which permits the computation of the differential Hilbert function.

PROPOSITION 3. *For any integer $i \geq 0$, we have the relation: $\phi(i) = n - \mathrm{rank}_{\mathcal{F}} J(i, i+1, 0) + \mathrm{rank}_{\mathcal{F}} J(i, i+1, 1)$. Furthermore, for any $1 \leq i \leq \nu$, the value of the differential Hilbert function $\mathcal{H}_{\mathcal{K}}(i)$ is given by*

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

The order of the differential ideal Δ over $\mathcal{K}$ is $\mathcal{H}_{\mathcal{K}}(\nu)$.

PROOF. From Theorem 3 we easily deduce that the number $\phi(i) = \text{tr-deg}_{\mathcal{K}}(\pi_i)$ equals the codimension of the $\mathcal{F}$-vector subspace $E_{i,0} := \mathrm{Span}\big(\mathrm{d}G, \ldots, \mathrm{d}G^{(i)}\big) \cap \mathrm{Span}(\mathrm{d}X)$ in the $\mathcal{F}$-vector space $\mathrm{Span}(\mathrm{d}X)$. Let us observe that the matrix $J(i, i+1, 0)$ describes the space $\mathrm{Span}\big(\mathrm{d}G, \ldots, \mathrm{d}G^{(i)}\big)$. Therefore, we have the identity

$$\dim_{\mathcal{K}} E_{i,0} = \mathrm{rank}_{\mathcal{F}} J(i, i+1, 0) - \mathrm{rank}_{\mathcal{F}} J(i, i+1, 1).$$

For our second assertion, from the definition of the differentiation index ν we deduce the identity $\Delta \cap A_\nu = \Delta_\nu$. As above, we deduce that the number

$$\mathrm{rank}_{\mathcal{F}} J(\nu, \nu+1, 0) - \mathrm{rank}_{\mathcal{F}} J(\nu, \nu+1, i)$$

equals the codimension of the subspace

$$\mathrm{Span}\big(\mathrm{d}G, \ldots, \mathrm{d}G^{(\nu)}\big) \cap \mathrm{Span}\big(\mathrm{d}X, \ldots, \mathrm{d}X^{(i)}\big).$$

Therefore from this remark and Theorem 3 we deduce as above the identity

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

□

Observe that, as the matrix $J(i, i+1, 0)$ encodes the vector space $\Omega_{\mathcal{A}_i/\mathcal{K}}$, the submatrix obtained by suppressing the column associated to $\mathrm{d}X$ in $J(i, i+1, 0)$ encode the vector space $\Omega_{\mathcal{A}_i/\mathcal{K}(x)}$. This shows that the transcendence degree presented in Remark 2 can all be computed using rank computations presented above. But, let us recall that all the matrices introduced in this section encode linear mappings over the field $\mathcal{F} = \mathrm{Fr}(\mathcal{K}\{X\}/\Delta)$. Unfortunately, elementary arithmetic operations in $\mathcal{F}$ cannot be performed at unit cost. In the next section we show how we can reduce this cost by using a specialization in a generic solution of the ideal Δ.

4. COMPUTATIONAL ASPECTS

In the next section we describe the data encoding of multivariate polynomials and rational functions used in our algorithm. We also show how all mathematical entities introduced in the previous sections can be represented by a straight-line program. Then, we show how we can compute the differential Hilbert function $\mathcal{H}_{\mathcal{K}}$ using a specialization in a generic solution. Finally, we give an estimate of the complexity of the evaluation of the specialized Jacobian matrix $J(h, h+1, 0)$ arising in our computations.

4.1 Data Encoding and Complexity Model

All the results presented up to now can be expressed in the dense complexity model, i.e. representing any multivariate polynomial by the vector of its coefficients. Instead of this, we are going to adopt the straight-line program model, in which polynomials are represented by the polynomial functions they define. This is the classical point of view of numerical analysis, and it has been also applied in computer algebra for complexity issues or the development of practical algorithms (see [11, 6, 7] and the references therein). More precisely, we have the following definition:

Definition 1. Let $\mathcal{V}$ be a finite set of variables over a field k. A straight-line program over $k[\mathcal{V}]$ is a finite sequence of assignments $b_i \leftarrow b' \circ_i b''$, where $\circ_i \in \{+, -, \times, \div\}$ and $\{b', b''\} \in \bigcup_{j=1}^{i-1}\{b_j\} \cup \mathcal{V} \cup k$. Its complexity is measured by its length (number of arithmetic operations $\circ_i$). Hereafter, we use the abbreviation SLP for straight-line program.

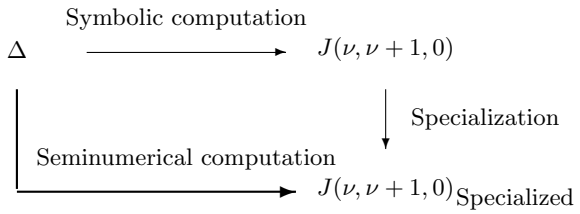
We say that a SLP β represents a rational function f in $k(X)$ if, on input η in k^n, β computes the value $f(\eta)$ whenever this value is well-defined. Hereafter, we are going to represent some Jacobian matrices by means of *division-free* SLP. For this purpose, we must be able to compute the numerator, denominator and the gradient ∇f of a given rational function f. The following constructive results allows us to handle these questions.

THEOREM 4 ([1], [11]). *Let be given a* SLP β *of length* L *computing a rational function* f. *Then, there exists a* SLP β_1 *of length* $5L$ *which computes the gradient* ∇f *and there exists a* SLP β_2 *of length* $4L$ *which computes polynomials* f_1 *and* f_2 *such that* $f = f_1/f_2$.

The next section presents the computational strategy that allows us to compute the differential Hilbert function and the related information we want to compute with complexity polynomial in the input size.

4.2 Specialization on a Generic Solution

Up to now, all the mathematical entities introduced in the previous sections may be computed by any standard computer algebra system. Indeed, Proposition 3 shows how we can reduce the computation of the differential Hilbert function $\mathcal{H}_\mathcal{K}$ and the related information we want to compute to some rank computations involving the matrices $J(\nu, \nu+1, 0)$ in a suitable field. Now, we are going to prove that these rank computations can be performed in polynomial time in the input size. Unfortunately, as showed in [18], the arithmetic complexity of computing multiple partial derivatives is likely to be exponential in the order of derivation i. If the equations defining system (1) are represented by a SLP of length L, Theorem 4 shows that the computation of the matrix $J(\nu, \nu+1, 0)$ requires at least $(5n)^i L$ arithmetic operations. Hence, applying purely symbolic techniques cannot lead to a polynomial time algorithm. Furthermore, the computation of the rank of the matrices $J(\nu, \nu+1, 0)$ introduced in the previous sections are also cumbersome because they are performed working in the field $\mathcal{F}$. Nevertheless, the variables X can be specialized into a generic solution of the ideal Δ and the desired ranks can be computed numerically



with high probability of success. This strategy is represented in the above figure by the thin arrows. In Proposition 4, we propose an alternative strategy based on the same idea which avoids the computation of the entries $\partial {g_r}^{(h)}/\partial {x_s}^{(i)}$ in $\mathcal{F}$ of the matrix $J(\nu, \nu+1, 0)$. It is represented in the above figure by the thick arrow. In order to describe this strategy we show in an example how we can simplify the computations in $\mathcal{F}$ by specialization in a generic solution of the ideal Δ.

Example 4. Let us consider the prime differential ideal generated by $\dot{x} + x^2$ in $k\{x\}$. The solution 0 is not generic while the formal power series $\eta = \sum_{i\in\mathbb{N}} (-1)^i\, {x_0}^{i+1} t^i$ is a generic solution of this differential ideal. Hence, the differential field $k\langle\eta\rangle$ and the fraction field $\mathcal{F}$ associated to the quotient algebra $k\{x\}/[\dot{x} + x^2]k\{x\}$ are isomorphic. Arithmetic operations and derivation in $\mathcal{F}$ can be done using rewriting techniques, while these operations can be easily in $k\langle\eta\rangle$ manipulating formal power series as usual. The computations presented below are based on this remark.

Let us recall that our rank computations are done in the field $\mathrm{Fr}(\mathcal{K}\{X\}/\Delta)$ and that we have proved that the variables $\widetilde{X}$ form a generic solution of Δ in $k\langle\widetilde{X}\rangle$. Hence, replacing the variables $\widetilde{X}$ by a vector of formal power series $\eta = \sum c_i\, t^i/i!$ defined by generic sequences $(c_i)_{i\in\mathbb{N}}$ with coefficients in k we also obtain a generic solution of Δ. The following proposition shows how we can compute the matrix $J(h, h+1, 0)$ specialized in such formal power series.

PROPOSITION 4. *Let us assume that the set* $\{g_1, \ldots, g_n\}$ *of differential polynomials in* $k\{X, \dot{X}\}$ *is represented by a* SLP *of length* L. *Then there exists a* SLP β *that takes the first* h *coefficients of* n *formal power series* η *as input and returns the constant coefficient of the power series obtained by specialization of the matrix* $J(h, h+1, 0)$ *in the power series* η. *The arithmetic complexity of the* SLP β *is*

$$\mathcal{O}\Big(n(L + nh^2)\mathcal{M}(h)\Big),$$

where $\mathcal{M}(i)$ *denotes the complexity of multiplication of two power series with coefficients in* k *up to order* $i+1$.

PROOF. Since the set of polynomials $\{g_1, \ldots, g_n\}$ is represented by a SLP of complexity L, Theorem 4 shows that there exists a SLP of length $3nL$ which evaluates the Jacobian matrix whose rows are the *coordinates* of the differentials $\mathrm{d}(g_i(\dot{X}, X))$ in the basis $\{\mathrm{d}X, \mathrm{d}\dot{X}\}$, namely

$$\tfrac{\partial g_i}{\partial \dot{x}_1}\,\mathrm{d}\dot{x}_1 + \cdots + \tfrac{\partial g_i}{\partial \dot{x}_n}\,\mathrm{d}\dot{x}_n + \tfrac{\partial g_i}{\partial x_1}\,\mathrm{d}x_1 + \cdots + \tfrac{\partial g_i}{\partial x_n}\,\mathrm{d}x_n.$$

Furthermore, from the identity $\mathrm{d}(f') = (\mathrm{d}f)'$, we deduce the

following expression of the differential $\mathrm{d}g_i{}'$:

$$\begin{aligned}\mathrm{d}g_i{}' = \tfrac{\partial g_i}{\partial \dot{x}_1}\,\mathrm{d}\ddot{x}_1 \quad + \cdots + \quad \tfrac{\partial g_i}{\partial \dot{x}_n}\,\mathrm{d}\ddot{x}_n \quad + \\ \left(\left(\tfrac{\partial g_i}{\partial \dot{x}_1}\right)' + \tfrac{\partial g_i}{\partial x_1}\right)\mathrm{d}\dot{x}_1 + \cdots + \left(\left(\tfrac{\partial g_i}{\partial \dot{x}_n}\right)' + \tfrac{\partial g_i}{\partial x_n}\right)\mathrm{d}\dot{x}_n + \\ \left(\tfrac{\partial g_i}{\partial x_1}\right)'\mathrm{d}x_1 \quad + \cdots + \quad \left(\tfrac{\partial g_i}{\partial x_n}\right)'\mathrm{d}x_n.\end{aligned}$$

Analogously, one can express the coordinates of the differentials $\mathrm{d}g_i^{(j)}$ as sums of of $\partial g/\partial x_i$, $\partial g/\partial \dot{x}_i$ and their derivatives. We now estimate the evaluation complexity of $\mathrm{d}g_i^{(j)}$. First, we observe that the first $h-j$ coefficients of the power series $(\partial g/\partial x_i)^{(j)}(\eta)$ and $(\partial g/\partial \dot{x}_i)^{(j)}(\eta)$ can be obtained in linear time from the first h coefficients of the power series $(\partial g/\partial x_i)(\eta)$ and $(\partial g/\partial \dot{x}_i)(\eta)$. We also observe that, if the first $h-j$ coefficients of the coordinates of the differential $\mathrm{d}g_i^{(j)}$ are known, the Leibniz rule shows that the first $h-j-1$ coefficients of the coordinates of the differential $\mathrm{d}p_i^{(j+1)}$ can be computed with jn additional operations on formal power series. Each such operation requires $\mathcal{M}(h)$ arithmetic operations in the base field k. Hence, by a recurrence argument, we conclude that the constant term of the coordinates of the differentials $\mathrm{d}g^{(j)}$ for $0 \le j \le h$ can be computed with $\mathcal{O}\big((L+nh^2)\mathcal{M}(h)\big)$ arithmetic operations. Since there are n such expressions to compute, we deduce the complexity result of Proposition 4. □

The above proposition gives an estimate of the complexity of computing the constant term of a specialization of the matrix $J(\nu, \nu+1, 0)$. We have reduced the determination of the differentiation index ν, the differential Hilbert function $\mathcal{H}_{\mathcal{K}}$ and of a—maximal—set of initial conditions to the computation of the rank of some suitably specialized submatrices of the matrix $J(\nu, \nu+1, 0)$ (see Section 3.2 and the remarks before Proposition 4). We observe that, in order to determine these ranks, it suffices to compute the constant term of the specialization of some suitably chosen minors of the matrices $J(\nu, \nu+1, 0)$. Therefore, Proposition 4 immediately implies the complexity result of Theorem 2.

Acknowledgments. This work was partially supported by the program ECOS-SECyT (action n°A99E06) between Argentina and France. G. Matera is supported by the Argentinian grants UBACyT X–198 and CONICET PIP 4571. G. Matera thanks to the Facultad de Ing., Ciencias Exactas y Naturales, Univ. Favaloro, where he did part of this work.

5. REFERENCES

[1] Baur, W., and Strassen, V. The complexity of partial derivatives. *Theor. Comp. Sc. 22*, 3 (1983).

[2] Boulier, F. Efficient computation of regular differential systems by change of rankings using Kähler differentials. Preprint 1999-14, Univ. de Lille I, 1999.

[3] Boulier, F., Lazard, D., Ollivier, F., and Petitot, M. Representation for the radical of a finitely generated differential ideal. In *Proceedings of ISSAC* (1995), ACM, pp. 158–166.

[4] Campbell, S., and Gear, C. The index of general nonlinear DAE's. *Numer. Math. 72*, 2 (1995), 173–196.

[5] Eisenbud, D. *Commutative algebra with a view toward algebraic geometry*. 150 in GTM. Springer, 1994.

[6] Giusti, M., Lecerf, G., and Salvy, B. A Gröbner free alternative for polynomial systems solving. *Journal of Complexity 17*, 1 (2001), 154–211.

[7] Heintz, J., Matera, G., and Waissbein, A. On the time-space complexity of geometric elimination procedures. *AAECC 11*, 4 (2001), 239–296.

[8] Hubert, É. Factorisation free decomposition algorithms in differential algebra. *Journal of Symbolic Computation 29*, 4 & 5 (Apr./May 2000), 641–662.

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

[10] Kolchin, E. R. *Differential algebra and algebraic groups*, vol. 54 of *Pure and applied Mathematics*. Academic press, New York, 1973.

[11] Matera, G. Probabilistic algorithms for geometric elimination. *AAECC 9*, 6 (1999), 463–520.

[12] Ollivier, F. Standard bases of differential ideals. In *Proceedings of AAECC-8* (1990), S. Sakata, Ed., vol. 508 of *LNCS*, Springer, pp. 304–321.

[13] Reid, G., Lin, P., and Wittkopf, A. Differential elimination-completion algorithms for DAE and PDAE. *Stud. Appl. Math. 106*, 1 (2001), 1–45.

[14] Ritt, J. F. *Differential algebra*. Dover Publ., 1966.

[15] Sadik, B. A bound for the order of characteristic set elements of an ordinary prime differential ideal and some applications. *AAECC 10*, 3 (2000), 251–268.

[16] Sedoglavic, A. A mixed symbolic-numeric method to study prime ordinary differential ideal. Manuscript 2000-04, GAGE laboratory, Jan. 2000. Available at http://www.medicis.polytechnique.fr/~sedoglav.

[17] Sedoglavic, A. A probabilistic algorithm to test local algebraic observability in polynomial time. In *Proceedings of ISSAC* (2001), ACM, pp. 309–316.

[18] Valiant, L. G. Reducibility by algebraic projections. *L'enseig. Math. IIe Séries 28*, 3-4 (1982), 253–268.