Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Complexity 22 (2006) 396–430
Journal of COMPLEXITY
www.elsevier.com/locate/jco

On the complexity of the resolvent representation of some prime differential ideals☆

Lisi D'Alfonso, Gabriela Jeronimo, Pablo Solernó*

Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, 1428 Buenos Aires, Argentina

Received 16 February 2005; accepted 13 October 2005
Available online 28 December 2005

Abstract

We prove upper bounds on the order and degree of the polynomials involved in a resolvent representation of the prime differential ideal associated with a polynomial differential system for a particular class of ordinary first order algebraic-differential equations arising in control theory. We also exhibit a probabilistic algorithm which computes this resolvent representation within time polynomial in the natural syntactic parameters and the degree of a certain algebraic variety related to the input system. In addition, we give a probabilistic polynomial-time algorithm for the computation of the differential Hilbert function of the ideal.

Keywords: Differential algebra; Resolvent representation; Elimination theory; Probabilistic algorithms; Straight-line programs; Differential Hilbert function

1. Introduction

The notion of a resolvent representation of a prime differential ideal in a ring of differential polynomials was introduced by Ritt (see [28,27]) as a tool towards an algebraic elimination theory in the realm of differential equations, although it can be traced back to the work of Kronecker (see [24]). Roughly speaking, a resolvent representation of a prime differential ideal provides a parametrization of the generic zeros of the ideal by the general zeros of a single irreducible differential polynomial. This construction can be interpreted in several contexts, including the

☆ Partially supported by the following Argentinian research Grants: UBACyT X112 (2004–2007), and CONICET PIP 02461/01.

* Corresponding author.
E-mail addresses: lisi@dm.uba.ar (L. D'Alfonso), jeronimo@dm.uba.ar (G. Jeronimo), psolerno@dm.uba.ar (P. Solernó).

0885-064X/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.jco.2005.10.002

primitive element for field extensions, the cyclic vector for linear first order differential systems, and the shape lemma in algebraic and analytic geometry.

In order to illustrate the notion of resolvent representation, let us consider the following simple differential algebraic system (Σ) consisting of four equations in the four unknowns X_1, X_2, X_3, U (see [29, Section 4.4.2] or [6]):

$$(\Sigma) := \begin{cases} \dot{X}_1 = \alpha X_1 \\ \dot{X}_2 = \alpha X_2 \\ \dot{X}_3 = \beta X_3 + U X_1 \\ Y = X_2 + X_3 \end{cases}$$

where $\alpha, \beta \in \mathbb{Q}$, the variable Y is regarded as a parameter and the system is considered over the ground differential field $\mathbb{Q}(t)$ equipped with the usual derivation $t' = 1$. Set $\gamma := X_1 + tX_2$. Then, all the variables appearing in (Σ) can be written, using the equations of the system and their derivatives, as rational functions in $\mathbb{Q}(t, Y, \dot{Y})(\gamma, \dot{\gamma})$:

$$\begin{aligned} X_1 &= (1 + t\alpha)\gamma - t\dot{\gamma}, \\ X_2 &= \dot{\gamma} - \alpha\gamma, \\ X_3 &= Y - \dot{\gamma} + \alpha\gamma, \\ U &= \frac{(\beta - \alpha)\dot{\gamma} + (\alpha^2 - \alpha\beta)\gamma + \dot{Y} - \beta Y}{-t\dot{\gamma} + (1 + t\alpha)\gamma}. \end{aligned}$$

In addition, γ verifies the differential equation

$$\gamma^{(2)} - 2\alpha\dot{\gamma} + \alpha^2\gamma = 0,$$

which is called the *minimal equation* for γ. The set consisting of the irreducible polynomial giving this minimal equation and those providing the rational identities above is called a *resolvent representation* of the system (Σ) and γ its associated *primitive element* (for more examples of resolvent representations see [5]).

The present paper deals with the computation of resolvent representations of prime differential ideals associated with certain differential systems coming from control theory (see, for instance, [6,7]):

$$\begin{cases} \dot{X}_1 = f_1(X, U) \\ \quad \vdots \\ \dot{X}_n = f_n(X, U) \\ Y_1 = g_1(X, U, \dot{U}) \\ \quad \vdots \\ Y_r = g_r(X, U, \dot{U}) \end{cases}$$

where $f_1, \ldots, f_n \in k[X, U]$ and $g_1, \ldots, g_r \in k[X, U, \dot{U}]$ are polynomials in the variables $X := \{X_1, \ldots, X_n\}$ and $U := \{U_1, \ldots, U_m\}$ with coefficients in a zero-characteristic differential field k and total degrees bounded by an integer d, and $Y := \{Y_1, \ldots, Y_r\}$ is another set of variables. The variables X, U are the unknowns of the system, while the variables Y are regarded as parameters. Given a differential equation system as above, we consider the prime differential ideal Δ generated by the polynomials $f_i - \dot{X}_i$, $i = 1, \ldots, n$, and $g_j - Y_j$, $j = 1, \ldots, r$, in the differential polynomial ring $k\{Y, X, U\}$.

We prove the existence of a resolvent representation for the ideal Δ consisting of polynomials which involve derivatives of order at most $2n + 2r$ and whose degrees are bounded by the degree of the algebraic variety $\mathbb{V}$ defined by the input polynomials and their derivatives up to order $2n + 2r - 1$ (see Theorem 36). The Bezout inequality implies that $\deg(\mathbb{V})$ can always be bounded by $d^{2(n+r)^2}$.

In addition, if $k = \mathbb{Q}(t)$, we construct a bounded error probability algorithm which computes a resolvent representation of Δ. If the input polynomials are given by a straight-line program of length L over $\mathbb{Q}$ (see Section 2.2 for the definition of this data structure), the complexity of this algorithm is linear in L and polynomial in n, m, r, d and $\deg(\mathbb{V})$ (see Theorem 48). We remark that the upper bound for $\deg(\mathbb{V})$ due to the Bezout inequality leads to a single exponential worst-case complexity bound for our algorithm. The error probability of the algorithm is controlled by means of the Zippel–Schwartz zero test and degree upper bounds for the polynomials giving the genericity conditions under which our algorithm works.

As a byproduct, we present a probabilistic algorithm for the computation of the differential Hilbert function of the ideal Δ within complexity polynomial in n, m, r, d and linear in L (see Theorem 26), extending the results in [26] to positive-dimensional situations.

Our overall strategy consists in translating a differential (non-noetherian) problem into an algebraic (noetherian) one. In this sense, some finiteness results on characteristic sets of differential ideals appearing in [30,29] play a fundamental role. In a first step, we compute a differential transcendence basis of the differential field extension induced by our system in order to turn to a zero-dimensional differential situation, which is achieved by applying some techniques described in [26]. Then, we give an effective and algorithmic version of Seidenberg's proof of the existence of a primitive element (see [34]) in our situation, reducing the problem to the computation of an eliminating polynomial in an algebraic-geometric context. Finally, we apply an elimination procedure based on [17,31] to make our main computations.

The approach to differential polynomial equation systems through resolvent representations has been known to be effective since its origins in [28]. Ritt's treatment of the subject as well as its subsequent generalizations (see [5,4]) are based on rewriting techniques, namely Gröbner bases and characteristic sets. Even though a single exponential complexity upper bound was proved in [9] for the computation of a resolvent representation using these methods in the algebraic (non-differential) context, no complexity analysis is presented in any of the works concerning its differential counterpart. However, the complexity results on the computation of characteristic sets in the differential setting given in [30] seem to yield single exponential complexity bounds for a probabilistic algorithm computing a resolvent representation (see [4]) for the specific systems we consider. A different approach to effective elimination over ordinary differential fields can be found in [15], where a general quantifier elimination procedure with doubly exponential complexity bounds is exhibited.

We point out that our algorithms do not require the computation of Gröbner bases or characteristic sets. Based on the computation of algebraic eliminating polynomials, our approach enables us to obtain complexity estimates in terms of a geometric invariant, which are more precise than those depending only on syntactic parameters (see Example 38). Complexity bounds depending on this kind of parameters appeared before in several algebraic elimination procedures (see, for instance, [13,17,14,12]). We observe also that, in terms of the parameters n, m, r, d, the complexity of our algorithm is of order $(nmr)^{O(1)} d^{O((n+r)^2)}$, improving the complexity estimate $(n + r)^{O((n+m)(n+r))} d^{O((n+m)^3(n+r)^3)}$ of the rewriting procedure presented in [30, Theorem 28] when applied to our particular equation systems.

We hope that our techniques and results would contribute to the symbolic treatment of systems where the parameters Y's are replaced with given functions. We also expect that these results could be extended to more general cases such as partial derivative equation systems or positive characteristic differential fields (see [35]).

The paper is organized as follows: in Section 2, we recall some basic notions and results from differential algebra and we present the algorithmic model we will adopt. In Section 3, we introduce the differential equation systems we will consider and we show some elementary facts about them. Section 4 deals with the computation of the differential Hilbert function of the ideal associated with the system and of a differential transcendence basis of the induced differential field extension. In Section 5 we recall the notion of a resolvent representation of a prime differential ideal and we prove upper bounds for the orders and degrees of the involved polynomials. Section 6 is devoted to the algorithmic computation of resolvent representations. Finally, in Section 7 we present a slight generalization of the algorithmic results stated in the previous sections.

2. Preliminaries

This section gathers some basic notions from differential algebra that will be needed throughout the paper and presents the algorithmic model and the data structure we will use.

2.1. Differential algebra

We recall in this subsection some definitions and basic facts about differential rings and fields. For a more detailed account of the subject, we refer the reader to [28,21] (see also [20]).

2.1.1. Differential rings and fields

A *derivation* δ of a ring $\mathcal{A}$ is an additive map $\delta : \mathcal{A} \to \mathcal{A}$ satisfying the Leibniz rule $\delta(a \cdot b) = \delta(a) \cdot b + a \cdot \delta(b)$ for all $a, b \in \mathcal{A}$. A ring (respectively, a field) equipped with (at least) a derivation δ is called a *differential ring* (respectively, a *differential field*). We will work over rings and fields equipped with a single derivation, that is, *ordinary* differential rings and fields, and in the characteristic zero case. If η is an element of the differential ring $(\mathcal{A}, \delta)$, $\delta(\eta)$ will be denoted by $\dot{\eta}$, and for $i \geqslant 2$, $\delta^i(\eta)$ will be denoted by $\eta^{(i)}$.

Let $\mathcal{A}$ be a differential ring. An ideal $\mathcal{I}$ of $\mathcal{A}$ is a *differential ideal* if $\delta(a) \in \mathcal{I}$ for every $a \in \mathcal{I}$. If Σ is a subset of $\mathcal{A}$, the differential ideal generated by Σ (that is, the minimal differential ideal of $\mathcal{A}$ containing Σ) will be denoted by $[\Sigma]$.

Given a differential field (K, δ), we can construct the *ring of differential polynomials in the indeterminates* $X_1, \ldots, X_n$ *over* K, which we denote $K\{X_1, \ldots, X_n\}$, by considering the commutative polynomial ring over K in the infinite set of indeterminates $\{X_j^{(i)}, i \in \mathbb{N}_0, 1 \leqslant j \leqslant n\}$ and extending the derivation of K by letting $\delta(X_j^{(i)}) = X_j^{(i+1)}$. We will write $X := \{X_1, \ldots, X_n\}$ and, for every $i \in \mathbb{N}$, $X^{(i)} := \{X_1^{(i)}, \ldots, X_n^{(i)}\}$. For a polynomial $p \in K\{X\}$, we define the *order of* p *with respect to* X_j *as* $\mathrm{ord}(p, X_j) := \max\{i \in \mathbb{N}_0 : X_j^{(i)} \text{ appears in } p\}$, and the *order of* p as $\mathrm{ord}(p) := \max\{\mathrm{ord}(p, X_j) : 1 \leqslant j \leqslant n\}$.

A *differential field extension* $\mathcal{F} \hookrightarrow \mathcal{G}$ consists of two differential fields $(\mathcal{F}, \delta_{\mathcal{F}})$ and $(\mathcal{G}, \delta_{\mathcal{G}})$ such that $\delta_{\mathcal{F}}$ is the restriction to $\mathcal{F}$ of $\delta_{\mathcal{G}}$.

Let $\mathcal{F} \hookrightarrow \mathcal{G}$ be a differential field extension. An element $\zeta \in \mathcal{G}$ is said to be *differentially algebraic over* $\mathcal{F}$ if the family of its derivatives $\{\zeta^{(l)}\}_{l \in \mathbb{N}_0}$ is algebraically dependent over $\mathcal{F}$; otherwise, it

is said to be *differentially transcendental over* $\mathcal{F}$. The differential extension $\mathcal{F} \hookrightarrow \mathcal{G}$ is said to be *differentially algebraic* if every element of $\mathcal{G}$ is differentially algebraic over $\mathcal{F}$. Given a subset Σ of $\mathcal{G}$, $\mathcal{F}\langle\Sigma\rangle$ will denote the minimal differential subfield of $\mathcal{G}$ containing $\mathcal{F}$ and Σ. A subset Σ of $\mathcal{G}$ is *differentially algebraically independent over* $\mathcal{F}$ if the set $\{\zeta^{(l)} : \zeta \in \Sigma,\ l \in \mathbb{N}_0\}$ is algebraically independent over $\mathcal{F}$, and it is called a *differential transcendence basis of* $\mathcal{F} \hookrightarrow \mathcal{G}$ if it is a minimal subset of $\mathcal{G}$ such that the differential extension $\mathcal{F}\langle\Sigma\rangle \hookrightarrow \mathcal{G}$ is differentially algebraic. All the differential transcendence bases of a differential extension $\mathcal{F} \hookrightarrow \mathcal{G}$ have the same cardinality [21, Chapter II, Section 9, Theorem 4], which is called the *differential transcendence degree* of $\mathcal{F} \hookrightarrow \mathcal{G}$ and will be denoted by $\mathrm{difftrdeg}_{\mathcal{F}}(\mathcal{G})$.

Let K be a differential field, let X be a set of differential indeterminates (that is, a differentially algebraically independent set) over K and let $\mathcal{I} \subset K\{X\}$ be a prime differential ideal. A subset $W \subset X$ is a *maximal independent set modulo* $\mathcal{I}$ if $\mathcal{I} \cap K\{W\} = 0$ and $\mathcal{I} \cap K\{W, X_j\} \neq 0$ for all $X_j \notin W$. Let us observe that a maximal independent set modulo $\mathcal{I}$ is a differential transcendence basis of the differential extension $K \hookrightarrow \mathrm{Frac}(K\{X\}/\mathcal{I})$. Thus, we define the *differential dimension of the ideal* $\mathcal{I}$, denoted by $\mathrm{diffdim}(\mathcal{I})$, as the transcendence degree of this extension or, equivalently, as the cardinality of a maximal independent set modulo $\mathcal{I}$.

2.1.2. Rankings and characteristic sets

Let K be a differential field and let X be a set of differential indeterminates over K. A *ranking* on $K\{X\}$ is a total order $\succ$ on the set $\Theta X := \{X^{(l)} : l \in \mathbb{N}_0\}$ satisfying $\dot{u} \succ u$ for every $u \in \Theta X$ and $\dot{u} \succ \dot{v}$ if $u \succ v$ for $u, v \in \Theta X$. A ranking on $K\{X\}$ is an *orderly ranking* or *derivation ranking* if $X_i^{(r)} \succ X_j^{(s)}$ for $r > s$, and it is an *elimination ranking* if $X_i^{(r)} \succ X_j^{(s)}$ for $i > j$. If Y and Z are two sets of differential indeterminates and $\succ_Y$ and $\succ_Z$ are rankings on $K\{Y\}$ and $K\{Z\}$, respectively, the induced *elimination block ranking with* $Z \gg Y$ is the ranking on $K\{Y \cup Z\}$ defined by the conditions that any element of ΘZ is greater than any element of ΘY and two elements of ΘY (respectively, ΘZ) are ordered according to $\succ_Y$ (respectively, $\succ_Z$).

Assume that a ranking on $K\{X\}$ is fixed. Let $p \in K\{X\} \setminus K$. The *leader* of p, denoted by $\ell(p)$, is the greatest element of ΘX appearing in p. The leading coefficient of p in the variable $\ell(p)$, denoted by I_p, is called the *initial* of p, and $S_p := \partial p/\partial \ell(p)$ is the *separant* of p. If $\ell(p)$ is a derivative (possibly of order 0) of the variable X_j, then X_j is called the *leading variable of* p, and it is denoted by $vp(p)$. A polynomial $q \in K\{X\}$ is *reduced with respect to* p if $\deg_{\ell(p)}(q) < \deg_{\ell(p)}(p)$ and no proper derivative of $\ell(p)$ appears in q.

A subset $A \subset K\{X\} \setminus K$ is an *autoreduced* set if every element $p \in A$ is reduced with respect to all the elements of $A \setminus \{p\}$. If $A = \{A_1, \ldots, A_r\} \subset K\{X\} \setminus K$ is an autoreduced set, for every differential polynomial $f \in K\{X\}$, it is possible to obtain, by means of differentiations and pseudo-divisions, a differential polynomial $g \in K\{X\}$ reduced with respect to A (that is, reduced with respect to every element of A), and non-negative integers $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r$, such that $I_{A_1}^{\alpha_1} S_{A_1}^{\beta_1} \cdots I_{A_r}^{\alpha_r} S_{A_r}^{\beta_r} f - g \in [A_1, \ldots, A_r]$ (see [21, Chapter I, Section 9, Proposition 1]).

A *characteristic set of an ideal* $\mathcal{I} \subset K\{X\}$ is an autoreduced subset $\mathcal{C}$ of $\mathcal{I}$ with the property that no element of $\mathcal{I}$ is reduced with respect to all the elements of $\mathcal{C}$.

It follows from the definition that the leading variables of the elements of a characteristic set are pairwise different. If $\mathcal{C} = \{C_1, \ldots, C_r\}$ is a characteristic set of a differential ideal $\mathcal{I}$, the separants S_{C_j} and the initials I_{C_j} do not lie in $\mathcal{I}$. Moreover, if $\mathcal{I}$ is a prime ideal, the variables that are not leading variables of any element of $\mathcal{C}$ form a maximal differentially independent set modulo $\mathcal{I}$. Furthermore, if $H := \prod_{j=1}^{r} I_{C_j} S_{C_j}$, the reduction process mentioned above implies that $\mathcal{I}$ coincides with the saturation $[\mathcal{C}] : H^{\infty} := \{f \in K\{X\} : H^n f \in [\mathcal{C}] \text{ for some } n \in \mathbb{N}_0\}$.

More precisely, it can be shown that if $f \in \mathcal{I}$ is a differential polynomial with $\mathrm{ord}(f, vp(C_j)) \leqslant l$ for every $1 \leqslant j \leqslant r$, then f lies in the polynomial ideal $(C_j^{(k)};\ 1 \leqslant j \leqslant r,\ 0 \leqslant k \leqslant l) : H^\infty$ of $K\{X\}$ (see [28, Chapter I, Section 6]).

2.1.3. Differential Hilbert function

Definition 1. Let K be a differential field and let $\mathcal{I}$ be a prime differential ideal of $K\{X\}$. The *differential Hilbert function* $\mathcal{H}_{\mathcal{I},K} : \mathbb{N}_0 \to \mathbb{N}_0$ of $\mathcal{I}$ with respect to K is defined as

$$\mathcal{H}_{\mathcal{I},K}(i) = \mathrm{trdeg}_K \left(\mathrm{Frac}(K[X, \ldots, X^{(i)}]/\mathcal{I} \cap K[X, \ldots, X^{(i)}])\right).$$

The behavior of this function resembles that of the standard Hilbert function from algebraic geometry: if $\{C_1, \ldots, C_r\}$ is a characteristic set of a prime differential ideal $\mathcal{I}$ for an orderly ranking, for every $i \geqslant \max\{\mathrm{ord}(C_j),\ 1 \leqslant j \leqslant r\}$, we have

$$\mathcal{H}_{\mathcal{I},K}(i) = \mathrm{diffdim}(\mathcal{I})\,(i+1) + \mathrm{ord}_K(\mathcal{I}),$$

where $\mathrm{ord}_K(\mathcal{I}) := \sum_{j=1}^{r} \mathrm{ord}(C_j)$ (see [21, Chapter II, Section 12, Theorem 6]). Let us observe that the equality holds, in particular, for every $i \geqslant \mathrm{ord}_K(\mathcal{I})$.

The integer $\mathrm{ord}_K(\mathcal{I})$, which is called the *order* of the ideal $\mathcal{I}$, is an invariant of $\mathcal{I}$: it does not depend on either the characteristic set or the orderly ranking. Combining [29, Proposition 4.1.2] and [5, Theorem 4.11] we have the following well-known estimate:

Proposition 2. *Let $\mathcal{I} = [f_1, \ldots, f_s]$ be a prime differential ideal of $K\{X\}$ generated by polynomials $f_1, \ldots, f_s \in K[X, \ldots, X^{(l)}]$ (that is, $\mathrm{ord}(f_j) \leqslant l$ for every $1 \leqslant j \leqslant s$). Then, $\mathrm{ord}_K(\mathcal{I}) \leqslant l\,(\#\{X\} - \mathrm{diffdim}(\mathcal{I}))$.*

2.2. Data structures and algorithmic model

The algorithms we consider in this paper are described by arithmetic networks over the field $\mathbb{Q}$. An arithmetic network is represented by means of a directed acyclic graph. The external nodes of the graph correspond to the input and output of the algorithm. Each of the internal nodes of the graph is associated with either an arithmetic operation in $\mathbb{Q}$ or a comparison ($=$ or $\neq$) between two elements in $\mathbb{Q}$ followed by a selection of another node.

We assume that the cost of each operation and comparison is 1 and so, we define the *complexity* of the algorithm as the number of internal nodes of its associated graph. We will make use of some well-known subroutines to deal with polynomials and matrices. As our interest is mostly theoretical, it will be sufficient for us to apply the more naive procedures. For more advanced complexity results see [2] or [3].

Our algorithms work (that is, they compute the desired output) under certain genericity conditions depending on parameters whose values are chosen randomly. In this sense, we say that they are *probabilistic*. More precisely, each genericity condition is induced by a non-zero multivariate polynomial F (not necessarily explicitly given) such that every a with $F(a) \neq 0$ leads to a correct computation. Probability is introduced by choosing the coordinates of the parameter a at random with equidistributed probability in a set $\{0, \ldots, N-1\}$ for a positive integer N, which is achieved by means of a procedure that chooses the binary digits of an integer at random. The complexity of this procedure is $O(\log N)$, where here and in the sequel, log denotes logarithm in base 2. Thus, the error probability of the algorithm can be estimated by means of the Zippel–Schwartz zero-test

(see [36,32]), which states that, under the previous hypotheses, $\text{Prob}\big(F(a) = 0\big) \leqslant \deg(F)/N$. This estimation enables us to reduce the error probability of the algorithm as much as desired by choosing N big enough.

The objects our algorithms deal with are multivariate polynomials with coefficients in the base field $\mathbb{Q}$. The data structure we adopt to represent them is the (division-free) *straight-line program* encoding. Roughly speaking, a straight-line program over $\mathbb{Q}$ encoding a polynomial $f \in \mathbb{Q}[X_1, \ldots, X_n]$ is a program which enables one to evaluate f at any given point in $\mathbb{Q}^n$. Each of the instructions in this program is an addition, subtraction or multiplication between two pre-calculated elements in $\mathbb{Q}[X_1, \ldots, X_n]$, or an addition or multiplication by a scalar. The number of instructions in the program is called the *length* of the straight-line program. For the precise definitions and basic properties we refer the reader to [3] (see also [19]).

3. Generic algebraic-differential systems

Here, we introduce the objects we will deal with: we present the differential polynomial systems we will consider and their associated differential ideals.

We will use the following notation throughout the paper:

Notation 3. Let K be a differential field and let $Z := \{Z_1, \ldots, Z_\alpha\}$ be a differentially algebraically independent set over K. For every $i \geqslant 0$, $Z^{(i)}$ will denote the set $Z_1^{(i)}, \ldots, Z_\alpha^{(i)}$. For simplicity, we will write $Z = Z^{(0)}$ and $\dot{Z} = Z^{(1)}$. Finally, for every $i \geqslant 0$, $Z^{[i]}$ will denote the set $Z, \dot{Z}, \ldots, Z^{(i)}$. We will adopt a similar notation for differential polynomials: if $H := \{H_1, \ldots, H_\beta\} \subset K\{Z\}$, for every $i \geqslant 0$, we will write $H^{(i)} := H_1^{(i)}, \ldots, H_\beta^{(i)}$ and $H^{[i]} := H, \dot{H}, \ldots, H^{(i)}$, where $H = H^{(0)}$ and $\dot{H} = H^{(1)}$.

3.1. Definitions and basic properties

Let k be a differential field of characteristic 0 and let $X := \{X_1, \ldots, X_n\}$ and $U := \{U_1, \ldots, U_m\}$ be two families of differential indeterminates over k.

Let $f_1, \ldots, f_n$ be polynomials in $k[X, U]$, let r be a positive integer, $r \leqslant m$, and let $g_1, \ldots g_r \in k[X, U, \dot{U}]$. We consider a new family of differential indeterminates $Y := \{Y_1, \ldots, Y_r\}$ over the differential fraction field $k\langle X, U\rangle$ and the "generic" differential system

$$\begin{cases} \dot{X}_1 = f_1(X, U) \\ \quad \vdots \\ \dot{X}_n = f_n(X, U) \\ Y_1 = g_1(X, U, \dot{U}) \\ \quad \vdots \\ Y_r = g_r(X, U, \dot{U}) \end{cases} \tag{1}$$

We will work for the time being under the following assumption on the system, which will be removed later in Section 7:

Assumption 4. The polynomials $g_1, \ldots, g_r$ are differentially algebraically independent in $\text{Frac}(k\{Y, X, U\}/[f_1 - \dot{X}_1, \ldots, f_n - \dot{X}_n])$ over k.

We will deal with a differential ideal and some algebraic ideals associated with the system:

Notation 5. Let $F_i := f_i - \dot{X}_i \in k[X, \dot{X}, U]$ $(1 \leqslant i \leqslant n)$ and $G_j := g_j - Y_j \in k[Y, X, U, \dot{U}]$ $(1 \leqslant j \leqslant r)$, and let $\Delta := [F, G] \subset k\{Y, X, U\}$ be the differential ideal generated by the polynomials $F := F_1, \ldots, F_n$ and $G := G_1, \ldots, G_r$. For every $l \in \mathbb{N}$, let A_l be the polynomial ring $A_l := k[Y^{[l-1]}, X^{[l]}, U^{[l]}]$ and let $\Delta_l \subset A_l$ be the ideal of this ring generated by $F^{[l-1]}, G^{[l-1]}$. Finally, set $A_0 := k[X, U]$.

The following notation will be useful in the sequel:

Notation 6. For $i = 1, \ldots, n$, let $\tilde{f}_i^{(0)}(X, U) := f_i(X, U)$. Recursively, for $k > 0$ and $i = 1, \ldots, n$, let $\tilde{f}_i^{(k)}(X, U^{[k]})$ be the polynomial obtained from $f_i^{(k)}(X^{[k]}, U^{[k]})$ by substituting $X_h^{(l)} = \tilde{f}_h^{(l-1)}$ $(1 \leqslant h \leqslant n,\ 1 \leqslant l \leqslant k)$. Finally, we define polynomials $\tilde{g}_j^{(k)}(X, U^{[k+1]})$ by replacing $X_h^{(l)} = \tilde{f}_h^{(l-1)}$ $(1 \leqslant h \leqslant n,\ 1 \leqslant l \leqslant k)$ in the polynomials $g_j^{(k)}$.

Due to the particular structure of the polynomials F, G and their derivatives, it is easy to characterize the quotients A_l/Δ_l, for $l \in \mathbb{N}$, and $k\{Y, X, U\}/\Delta$:

Remark 7. Let l, i, s, t be positive integers with $i \leqslant l$, $1 \leqslant s \leqslant n$ and $1 \leqslant t \leqslant r$, and let $\mathfrak{p}_{i,s}$ and $\mathfrak{q}_{i,t}$ be the ideals of A_l defined as

$$\mathfrak{p}_{i,s} := (F, G, F^{(1)}, G^{(1)}, \ldots, F^{(i-2)}, G^{(i-2)}, F_1^{(i-1)}, \ldots, F_s^{(i-1)}),$$
$$\mathfrak{q}_{i,t} := (F, G, F^{(1)}, G^{(1)}, \ldots, F^{(i-2)}, G^{(i-2)}, F^{(i-1)}, G_1^{(i-1)}, \ldots, G_t^{(i-1)}).$$

In the quotient ring $A_l/\mathfrak{p}_{i,s}$, we have that $X_h^{(j)} = \tilde{f}_h^{(j-1)}$ $(1 \leqslant j \leqslant i-1,\ 1 \leqslant h \leqslant n$ and $j = i,\ 1 \leqslant h \leqslant s)$ and $Y_d^{(j)} = \tilde{g}_d^{(j)}$ $(0 \leqslant j \leqslant i-2,\ 1 \leqslant d \leqslant r)$, and similar identities hold in $A_l/\mathfrak{q}_{i,t}$. Therefore,

$$A_l/\mathfrak{p}_{i,s} \simeq k[Y^{(i-1)}, \ldots, Y^{(l-1)}, X, X_{s+1}^{(i)}, \ldots, X_n^{(i)}, X^{(i+1)}, \ldots, X^{(l)}, U^{[l]}],$$
$$A_l/\mathfrak{q}_{i,t} \simeq k[Y_{t+1}^{(i-1)}, \ldots, Y_r^{(i-1)}, Y^{(i)}, \ldots, Y^{(l-1)}, X, X^{(i+1)}, \ldots, X^{(l)}, U^{[l]}]$$

and so, $\mathfrak{p}_{i,s}$ and $\mathfrak{q}_{i,t}$ are prime ideals of A_l. In particular, Δ_l is prime, $A_l/\Delta_l \simeq k[X, U^{[l]}]$ and hence, its Krull dimension is $n + (l+1)m$.

With similar arguments, we deduce that the differential ideal $\Delta = [F, G] \subset k\{Y, X, U\}$ is prime and the differential ring $k\{Y, X, U\}/\Delta$ is isomorphic to the differential ring $k[X]\{U\}$ with the derivation induced by $\dot{X}_j := f_j(X, U)$.

Roughly speaking, Assumption 4 states that the set of variables Y is differentially algebraically independent modulo Δ (see also Proposition 8), and so, it seems quite reasonable to regard them as elements of an extended ground field. Then, we will be interested in the differential ideal generated by the polynomials F, G in the ring $k\langle Y\rangle\{X, U\}$.

We begin by considering some related polynomial ideals.

Proposition 8. *Under the same notation and assumptions as in Remark* 7, *we have that* $k[Y^{[l-1]}] \cap \mathfrak{p}_{i,s} = 0$, $k[Y^{[l-1]}] \cap \mathfrak{q}_{i,t} = 0$, *and the ideals* $k\langle Y\rangle \otimes \mathfrak{p}_{i,s}$ *and* $k\langle Y\rangle \otimes \mathfrak{q}_{i,t}$ *are prime ideals of the ring* $k\langle Y\rangle \otimes A_l$ (*here, the tensor product denotes scalar extension*). *In particular,* $k\langle Y\rangle \otimes \Delta_l$ *is a prime ideal of* $k\langle Y\rangle \otimes A_l$ *and there is a ring inclusion* $k[X, U^{[l]}] \simeq A_l/\Delta_l \hookrightarrow k\langle Y\rangle \otimes A_l/k\langle Y\rangle \otimes \Delta_l$.

Proof. Let us prove that $k[Y^{[l-1]}] \cap \mathfrak{p}_{i,s} = 0$ (the result for $\mathfrak{q}_{i,t}$ follows similarly): if $p \in k[Y^{[l-1]}] \cap \mathfrak{p}_{i,s}$, there exist polynomials $a_{q,h}, b_{j,k} \in A_l$ satisfying

$$p(Y^{[l-1]}) = \sum_{h=0}^{i-2} \sum_{q=1}^{n} a_{q,h}\, F_q^{(h)} + \sum_{q=1}^{s} a_{q,i-1}\, F_q^{(i-1)} + \sum_{k=0}^{i-2} \sum_{j=1}^{r} b_{j,k}\, G_j^{(k)}.$$

Substituting $Y_j^{(k)}$ for $g_j^{(k)}$ $(1 \leqslant j \leqslant r,\ 0 \leqslant k \leqslant l-1)$ in this identity, we deduce that

$$p(g_1, \ldots, g_r, \dot{g}_1, \ldots, \dot{g}_r, \ldots, g_1^{(l-1)}, \ldots, g_r^{(l-1)}) \in (F^{[i-1]}) \subset A_l$$

and so, the differential independence of $g_1, \ldots, g_r$ in the differential extension $k \hookrightarrow \mathrm{Frac}(k\{Y, X, U\}/[F])$ implies that $p = 0$.

Therefore, the extensions of the prime ideals $\mathfrak{p}_{i,s}$ and $\mathfrak{q}_{i,t}$ to $k(Y^{[l-1]}) \otimes A_l$ are also prime ideals; and the same happens to their extensions to the ring $k\langle Y\rangle \otimes A_l$, since the $Y^{(j)}$, with $j \geqslant l$, are transcendental over $k(Y^{[l-1]}) \otimes A_l$. □

From now on, we will use the same notation as in the previous proposition: the symbol $\otimes$ will denote scalar extensions that will be clear from the context.

Corollary 9. *For every positive integer l, we have that $F, G, F^{(1)}, G^{(1)}, \ldots, F^{(l-1)}, G^{(l-1)}$ is a regular sequence in $k\langle Y\rangle \otimes A_l$.*

Proof. Remark 7 enables the straightforward computation of the dimensions of $A_l/\mathfrak{p}_{i,s}$ and $A_l/\mathfrak{q}_{i,t}$ for every $i \leqslant l$, $1 \leqslant s \leqslant n$ and $1 \leqslant t \leqslant r$, which turn to drop successively by one when adding each polynomial of the sequence to the ideal generator set. Due to Proposition 8, the same happens for the corresponding prime ideals in $k\langle Y\rangle \otimes A_l$, which implies the statement. □

The differential analogue of Proposition 8 is the following:

Proposition 10. *Let $\Delta = [F, G] \subset k\{Y, X, U\}$ be the differential ideal introduced in Notation 5. Then $\Delta \cap k\{Y\} = 0$ and $k\langle Y\rangle \otimes \Delta$ is a prime ideal of $k\langle Y\rangle\{X, U\}$.*

According to Remark 7 and Proposition 10, the differential ideals Δ and $k\langle Y\rangle \otimes \Delta$ are prime ideals. Now, we will compute their differential dimensions.

Notation 11. Let $\mathcal{F}$ denote the common fraction field of the integral domains $k\{Y, X, U\}/\Delta$ and $k\langle Y\rangle\{X, U\}/k\langle Y\rangle \otimes \Delta$.

Proposition 12. *The differential transcendence degree of the differential field extension $k\langle Y\rangle \hookrightarrow \mathcal{F}$ is $m - r$.*

Proof. Due to Remark 7, there is an isomorphism between $\mathcal{F}$ and the differential field $k(X)\langle U\rangle$ with the derivation induced by $\dot{X}_j := f_j$ for $j = 1, \ldots, n$, and so,

$$\mathrm{difftrdeg}_k(\mathcal{F}) = \mathrm{difftrdeg}_k(k(X)\langle U\rangle) = \#U = m.$$

On the other hand, we have that $\mathrm{difftrdeg}_k(k\langle Y\rangle) = r$. Now, applying [21, Chapter II, Section 9, Corollary 2] to the tower of differential fields $k \hookrightarrow k\langle Y\rangle \hookrightarrow \mathcal{F}$, we conclude that $\mathrm{difftrdeg}_{k\langle Y\rangle}(\mathcal{F}) = m - r$. □

The above proposition and the fact that the ideal $k\langle Y\rangle \otimes \Delta$ is generated by polynomials of order less than or equal to 1 enable us to derive the following estimate by means of Proposition 2:

Remark 13. The order of the ideal $k\langle Y\rangle \otimes \Delta$ satisfies: $\mathrm{ord}_{k\langle Y\rangle}(k\langle Y\rangle \otimes \Delta) \leqslant n + r$.

3.2. Algebraic ideals vs. differential ideals

In this subsection we will establish a relation between contractions of the differential ideal $k\langle Y\rangle \otimes \Delta$ and contractions of the algebraic polynomial ideals $k\langle Y\rangle \otimes \Delta_l$ to the polynomial rings A_i. This relation is crucial to go from non-finitely generated algebraic ideals to finitely generated ones.

Lemma 14. *For every $i \geqslant 0$, we have* $(k\langle Y\rangle \otimes \Delta) \cap (k\langle Y\rangle \otimes A_i) = (k\langle Y\rangle \otimes \Delta_{i+n+r}) \cap (k\langle Y\rangle \otimes A_i)$.

Proof. We will show that $(k\langle Y\rangle \otimes \Delta) \cap (k\langle Y\rangle \otimes A_i) \subset (k\langle Y\rangle \otimes \Delta_{i+n+r}) \cap (k\langle Y\rangle \otimes A_i)$ holds (the converse is immediate from the fact that $\Delta_{i+n+r} \subset \Delta$).

First, let us observe that $\{F_1, \ldots, F_n, G_1, \ldots, G_r\}$ is a characteristic set of the ideal Δ for an elimination block ranking on $k\{Y, X, U\}$ with $Y \gg X \gg U$, and that $S_{F_h} = I_{F_h} = S_{G_j} = I_{G_j} = -1$, $\mathrm{ord}(F_h) = 1$ and $\mathrm{ord}(G_j) \leqslant 1$ for every $1 \leqslant h \leqslant n,\ 1 \leqslant j \leqslant r$.

Fix now an elimination block ranking $\succ$ with $X \gg U \gg Y$. From [30, Theorem 27], the previous conditions imply that there exists a characteristic set $C := \{C_1, \ldots, C_\ell\}$ of Δ with respect to $\succ$ such that $C_l \in (F^{[n+r-1]}, G^{[n+r-1]})$ for $l = 1, \ldots, \ell$. Set $H := \prod_l I_{C_l} S_{C_l}$.

Let $f \in (k\langle Y\rangle \otimes \Delta) \cap (k\langle Y\rangle \otimes A_i)$ and let $q \in k\{Y\}$, $q \neq 0$, with $qf \in \Delta \subset k\{Y, X, U\}$. Since $\Delta \cap k\{Y\} = 0$, for $l = 1, \ldots, \ell$, we have that $vp(C_l) \in \{X_1, \ldots, X_n, U_1, \ldots, U_m\}$ and so, $\mathrm{ord}(qf, vp(C_l)) \leqslant i$. Thus, $qf \in (C^{[i]}) : H^\infty$, where the ideal is taken in the ring $k\{Y, X, U\}$ (see Section 2.1.2). Now, $(C^{[i]}) : H^\infty \subset (F^{[i+n+r-1]}, G^{[i+n+r-1]}) : H^\infty = (F^{[i+n+r-1]}, G^{[i+n+r-1]})$, since this last ideal is prime and it does not contain H. Therefore, $qf \in (F^{[i+n+r-1]}, G^{[i+n+r-1]})$ and so, $f \in (F^{[i+n+r-1]}, G^{[i+n+r-1]})k\langle Y\rangle\{X, U\}$.

Finally, notice that if $f = \sum_{k=0}^{i+n+r-1} (\sum_{h=1}^{n} a_{h,k} F_h^{(k)} + \sum_{j=1}^{r} b_{j,k} G_j^{(k)})$ with $a_{h,k}, b_{j,k} \in k\langle Y\rangle\{X, U\}$, evaluating $X^{(l)} = 0$ and $U^{(l)} = 0$ for $l > i + n + r$ (these variables appearing only in $a_{h,k}, b_{j,k}$), we deduce that $f \in (F^{[i+n+r-1]}, G^{[i+n+r-1]})(k\langle Y\rangle \otimes A_{i+n+r}) = k\langle Y\rangle \otimes \Delta_{i+n+r}$, which completes the proof. □

4. Hilbert function and differential transcendence bases

This section is devoted to the computation of the differential Hilbert function of the ideal $k\langle Y\rangle \otimes \Delta$ and a differential transcendence basis of the extension $k\langle Y\rangle \hookrightarrow \mathcal{F}$ (see Notations 5 and 11).

The differential Hilbert function is obtained by means of the computation of Jacobian matrix ranks (see also [33,26]), relying on the well-known Jacobian criterion from commutative algebra [25, Chapter VI, Section 1, Theorem 1.15]. Regarding the computation of a differential transcendence basis, our results are based on a finiteness criterion proved in [30] concerning the order of characteristic set elements for an ideal, along with the above mentioned Jacobian criterion.

4.1. Hilbert function of $k\langle Y\rangle \otimes \Delta$ over $k\langle Y\rangle$

As stated in Definition 1, the differential Hilbert function of the ideal $k\langle Y\rangle \otimes \Delta \subset k\langle Y\rangle\{X, U\}$ is the function $\mathcal{H}_{k\langle Y\rangle \otimes \Delta,\, k\langle Y\rangle} : \mathbb{N}_0 \to \mathbb{N}_0$ defined by

$$\mathcal{H}_{k\langle Y\rangle \otimes \Delta,\, k\langle Y\rangle}(i) := \mathrm{trdeg}_{k\langle Y\rangle}\Big(\mathrm{Frac}(k\langle Y\rangle \otimes A_i \big/ (k\langle Y\rangle \otimes \Delta) \cap (k\langle Y\rangle \otimes A_i))\Big).$$

Due to Proposition 12 and Remark 13, we have that

$$\mathcal{H}_{k\langle Y\rangle\otimes\Delta,\,k\langle Y\rangle}(i) = (m-r)(i+1) + \mathrm{ord}_{k\langle Y\rangle}(k\langle Y\rangle\otimes\Delta) \quad \text{for every } i \geqslant n+r \tag{2}$$

(see Section 2.1.3); so, the function $\mathcal{H}_{k\langle Y\rangle\otimes\Delta,\,k\langle Y\rangle}$ is completely determined by the values it takes at $i = 0,\ldots,n+r$.

In order to compute this function we will deal with Jacobian matrices. We introduce here a notation that will be used in the sequel:

Notation 15. If $Z = \{Z_1,\ldots,Z_\alpha\}$ is a set of differential indeterminates over a field K and $H = \{H_1,\ldots,H_\beta\}$ is a set of differential polynomials over K depending on the variables Z, for every $l, k \geqslant 0$ we will denote by $\frac{\partial H^{(l)}}{\partial Z^{(k)}}$ the Jacobian matrix of the polynomials $H_1^{(l)},\ldots,H_\beta^{(l)}$ with respect to the variables $Z_1^{(k)},\ldots,Z_\alpha^{(k)}$, that is, $\left(\frac{\partial H^{(l)}}{\partial Z^{(k)}}\right)_{ij} := \frac{\partial H_i^{(l)}}{\partial Z_j^{(k)}}$ for $1\leqslant i\leqslant\beta$, $1\leqslant j\leqslant\alpha$. Similarly, for every $0\leqslant l_1\leqslant l_2, 0\leqslant k_1\leqslant k_2$, $\frac{\partial H^{[l_1,l_2]}}{\partial Z^{[k_1,k_2]}}$ will denote the Jacobian block matrix

$$\left(\frac{\partial H^{[l_1,l_2]}}{\partial Z^{[k_1,k_2]}}\right)_{ij} := \frac{\partial H^{(i+l_1-1)}}{\partial Z^{(j+k_1-1)}} \qquad (1\leqslant i\leqslant l_2-l_1+1,\ 1\leqslant j\leqslant k_2-k_1+1).$$

For the sake of simplicity, we will write $\frac{\partial H^{[l]}}{\partial Z^{[k]}} = \frac{\partial H^{[0,l]}}{\partial Z^{[0,k]}}$.

Now, the differential Hilbert function of $k\langle Y\rangle\otimes\Delta$ can be written in terms of ranks of suitable Jacobian matrices:

Proposition 16. *For $i = 0,\ldots,n+r$, let J_i be the Jacobian matrix $J_i := \frac{\partial\{F,G\}^{[i,\,2n+2r-1]}}{\partial\{X,U\}^{[i+1,\,2n+2r]}}$. Then, the differential Hilbert function of the ideal $k\langle Y\rangle\otimes\Delta$ over $k\langle Y\rangle$ is the function $\mathcal{H}_{k\langle Y\rangle\otimes\Delta,\,k\langle Y\rangle}: \mathbb{N}_0\to\mathbb{N}_0$ defined by*

$$\mathcal{H}_{k\langle Y\rangle\otimes\Delta,\,k\langle Y\rangle}(i) = \begin{cases} (n+m)(i+1) - (2n+2r)(n+r) + \mathrm{rank}(J_i) & \text{if } i\leqslant n+r,\\ (m-r)(i+1) + \mathrm{rank}(J_{n+r}) - (n+r)(n+r-1) & \text{if } i\geqslant n+r,\end{cases}$$

where the ranks of the matrices J_i are taken over the ring $k\langle Y\rangle\otimes(A_{2n+2r}/\Delta_{2n+2r})$.

Proof. Lemma 14 applied to $i = n+r$ states that

$$(k\langle Y\rangle\otimes\Delta)\cap(k\langle Y\rangle\otimes A_{n+r}) = (k\langle Y\rangle\otimes\Delta_{2n+2r})\cap(k\langle Y\rangle\otimes A_{n+r}).$$

Then, for every $i\leqslant n+r$, since $A_i\subset A_{n+r}$, we deduce that

$$\begin{aligned}(k\langle Y\rangle\otimes\Delta)\cap(k\langle Y\rangle\otimes A_i) &= (k\langle Y\rangle\otimes\Delta)\cap(k\langle Y\rangle\otimes A_{n+r})\cap(k\langle Y\rangle\otimes A_i)\\ &= (k\langle Y\rangle\otimes\Delta_{2n+2r})\cap(k\langle Y\rangle\otimes A_i)\end{aligned}$$

holds and so, we have the following ring inclusion:

$$k\langle Y\rangle\otimes A_i/(k\langle Y\rangle\otimes\Delta)\cap(k\langle Y\rangle\otimes A_i)\hookrightarrow k\langle Y\rangle\otimes(A_{2n+2r}/\Delta_{2n+2r}).$$

Set $\mathcal{F}_i := \mathrm{Frac}(k\langle Y\rangle\otimes A_i/(k\langle Y\rangle\otimes\Delta)\cap(k\langle Y\rangle\otimes A_i))$ and $\mathcal{G} := \mathrm{Frac}(k\langle Y\rangle\otimes(A_{2n+2r}/\Delta_{2n+2r}))$. The above ring inclusion induces a field extension $k\langle Y\rangle\hookrightarrow\mathcal{F}_i\hookrightarrow\mathcal{G}$, which implies that $\mathcal{H}_{k\langle Y\rangle\otimes\Delta,\,k\langle Y\rangle}(i) = \mathrm{trdeg}_{k\langle Y\rangle}(\mathcal{F}_i) = \mathrm{trdeg}_{k\langle Y\rangle}(\mathcal{G}) - \mathrm{trdeg}_{\mathcal{F}_i}(\mathcal{G})$.

By Corollary 9, the polynomials $F, G, \ldots, F^{(2n+2r-1)}, G^{(2n+2r-1)}$ are a regular sequence in $k\langle Y\rangle \otimes A_{2n+2r}$. Therefore, $\mathrm{trdeg}_{k\langle Y\rangle}(\mathcal{G}) = (2n+2r+1)(n+m) - (2n+2r)(n+r)$. In order to compute $\mathrm{trdeg}_{\mathcal{F}_i}(\mathcal{G})$, notice that $\mathcal{G}$ can be regarded as the fraction field of the quotient ring

$$\mathcal{F}_i[X^{(i+1)}, \ldots, X^{(2n+2r)}, U^{(i+1)}, \ldots, U^{(2n+2r)}]/(F^{(i)}, \ldots, F^{(2n+2r-1)}, G^{(i)}, \ldots, G^{(2n+2r-1)}).$$

Then, the Jacobian criterion [25, Chapter VI, Section 1, Theorem 1.15 and Proposition 1.5] implies that $\mathrm{trdeg}_{\mathcal{F}_i}(\mathcal{G}) = (2n+2r-i)(n+m) - \mathrm{rank}(J_i)$, where the rank is computed in $k\langle Y\rangle \otimes (A_{2n+2r}/\Delta_{2n+2r})$. We conclude that $\mathcal{H}_{k\langle Y\rangle\otimes\Delta,\, k\langle Y\rangle}(i) = (n+m)(i+1) - (2n+2r)(n+r) + \mathrm{rank}(J_i)$ for $i \leqslant n+r$.

In particular, $\mathcal{H}_{k\langle Y\rangle\otimes\Delta,\, k\langle Y\rangle}(n+r) = (n+m)(n+r+1) - (2n+2r)(n+r) + \mathrm{rank}(J_{n+r})$ and then, by identity (2), we deduce that $\mathrm{ord}_{k\langle Y\rangle}(k\langle Y\rangle \otimes \Delta) = \mathrm{rank}(J_{n+r}) - (n+r)(n+r-1)$ and, therefore, $\mathcal{H}_{k\langle Y\rangle\otimes\Delta,\, k\langle Y\rangle}(i) = (m-r)(i+1) + \mathrm{rank}(J_{n+r}) - (n+r)(n+r-1)$ for every $i \geqslant n+r$. □

4.2. Differential transcendence basis

Here we will show how to obtain a differential transcendence basis of the differential field extension $k\langle Y\rangle \hookrightarrow \mathcal{F}$. Taking into account the literature on algebraic observability (see, for instance, [33]), we will look for a differential transcendence basis involving only variables U, which is not restrictive as it is shown in the following:

Lemma 17. *There exists a differential transcendence basis W of the extension $k\langle Y\rangle \hookrightarrow \mathcal{F}$ with $W \subset U$.*

Proof. Let W be a maximal subset of U being differentially algebraically independent in $k\langle Y\rangle \hookrightarrow \mathcal{F}$. Then, the field subextension $k\langle Y, U\rangle$ of $k\langle Y, W\rangle \hookrightarrow \mathcal{F}$ is differentially algebraic over $k\langle Y, W\rangle$. On the other hand, the extension $k\langle U\rangle \hookrightarrow \mathcal{F}$ is also differentially algebraic, since $\mathcal{F} \simeq k(X)\langle U\rangle$, and so, the same holds for $k\langle Y, U\rangle \hookrightarrow \mathcal{F}$. Therefore, the extension $k\langle Y, W\rangle \hookrightarrow \mathcal{F}$ is differentially algebraic. □

The next proposition provides a finiteness criterion of differential transcendence in $\mathcal{F}$.

Proposition 18. *The element U_l is differentially transcendental in $k\langle Y\rangle \hookrightarrow \mathcal{F}$ if and only if the family $\{U_l, \ldots, U_l^{(n+r)}\}$ is algebraically independent in $k\langle Y\rangle \otimes A_{n+r}/(k\langle Y\rangle \otimes \Delta_{2n+2r}) \cap (k\langle Y\rangle \otimes A_{n+r})$ over $k\langle Y\rangle$.*

Proof. Assume that $\{U_l, \ldots, U_l^{(n+r)}\} \subset k\langle Y\rangle \otimes A_{n+r}/(k\langle Y\rangle \otimes \Delta_{2n+2r}) \cap (k\langle Y\rangle \otimes A_{n+r})$ is algebraically independent over $k\langle Y\rangle$.

Consider an elimination ranking on $k\langle Y\rangle\{X, U\}$ with $U_l \ll \{X, U\} \setminus \{U_l\}$. By [30, Lemma 19 and Theorem 24], there exists a characteristic set $\mathcal{C}$ of the ideal $k\langle Y\rangle \otimes \Delta$ with respect to this ranking, such that $\mathrm{ord}(C) \leqslant \mathrm{ord}_{k\langle Y\rangle}(k\langle Y\rangle \otimes \Delta) \leqslant n+r$ for every $C \in \mathcal{C}$ (Remark 13). Now, if U_l is differentially algebraic in $k\langle Y\rangle \hookrightarrow \mathcal{F}$, there exists $C \in \mathcal{C}$ with $C \in (k\langle Y\rangle \otimes \Delta) \cap k\langle Y\rangle[U_l^{[n+r]}] \subset (k\langle Y\rangle \otimes \Delta) \cap (k\langle Y\rangle \otimes A_{n+r}) = (k\langle Y\rangle \otimes \Delta_{2n+2r}) \cap (k\langle Y\rangle \otimes A_{n+r})$ (see Section 2.1.2), where the last identity is due to Lemma 14, contradicting the hypothesis of algebraic independence of $U_l, \ldots, U_l^{(n+r)}$. □

In order to apply the previous result we will use the following well-known technical lemma from commutative algebra:

Lemma 19. *Let K be a field of characteristic 0 and let $\wp \subset K[Z_1, \ldots, Z_\alpha]$ be a prime ideal generated by polynomials $f_1, \ldots, f_s$. Set R for the ring $K[Z_1, \ldots, Z_\alpha]/\wp$ and denote by $J \in R^{s\times\alpha}$ the Jacobian matrix of the system $f_1, \ldots, f_s$. For $j = 1, \ldots, \alpha$, set $J^{Z_j} \in R^{s\times(\alpha-1)}$ for the submatrix of J obtained by removing the column corresponding to derivatives with respect to the variable Z_j. Then, $Z_j \in R$ is transcendental over K if and only if* $\operatorname{rank}_R(J^{Z_j}) = \operatorname{rank}_R(J)$.

Proof. Assuming that Z_j is transcendental modulo $\wp$, we have inclusions $K(Z_j) \subset R \otimes K(Z_j) \subset \operatorname{Frac}(R)$. Therefore, by the Jacobian criterion (see [25, Chapter VI, Section 1, Theorem 1.15]), we have $\operatorname{rank}_R(J^{Z_j}) = (\alpha - 1) - \operatorname{trdeg}_{K(Z_j)}(\operatorname{Frac}(R)) = \alpha - 1 - (\operatorname{trdeg}_K(\operatorname{Frac}(R)) - 1) = \alpha - \operatorname{trdeg}_K(\operatorname{Frac}(R)) = \operatorname{rank}_R(J)$.

In order to prove the converse, assume that there exists a non-zero polynomial $f_{s+1} \in \wp$ pure in the variable Z_j with minimal degree. The rank of the Jacobian matrix $\mathcal{J}$ of the system $f_1, \ldots, f_s, f_{s+1}$ equals that of the Jacobian matrix J, since both are the codimension of $\wp$. On the other hand, we have that $\operatorname{rank}_R(\mathcal{J}) = \operatorname{rank}_R(J^{Z_j}) + 1$. Therefore, $\operatorname{rank}_R(J) = \operatorname{rank}_R(J^{Z_j}) + 1$. □

Now we are able to prove our main result on the computation of differential transcendence bases:

Proposition 20. *Let J be the Jacobian matrix $J := \frac{\partial\{F,G\}^{[2n+2r-1]}}{\partial\{X,U\}^{[2n+2r]}}$ (see Notation 15). Then, a set $W := \{U_{l_1}, \ldots, U_{l_{m-r}}\}$ with $m - r$ elements is a differential transcendence basis of $k\langle Y\rangle \hookrightarrow \mathcal{F}$ if and only if the columns of J corresponding to derivatives with respect to variables in $W^{[n+r]}$ can be removed with no change in rank (here, the ranks are taken over the ring $k\langle Y\rangle \otimes (A_{2n+2r}/\Delta_{2n+2r})$).*

Proof. Due to Proposition 18, an element U_l $(1 \leqslant l \leqslant m)$ belongs to a differential transcendence basis of $k\langle Y\rangle \hookrightarrow \mathcal{F}$ if and only if the set $\{U_l, \ldots, U_l^{(n+r)}\}$ is algebraically independent in $k\langle Y\rangle \otimes A_{n+r}/(k\langle Y\rangle \otimes \Delta_{2n+2r}) \cap (k\langle Y\rangle \otimes A_{n+r})$ over $k\langle Y\rangle$. Since the ring inclusion $k\langle Y\rangle \otimes A_{n+r}/(k\langle Y\rangle \otimes \Delta_{2n+2r}) \cap (k\langle Y\rangle \otimes A_{n+r}) \subset k\langle Y\rangle \otimes (A_{2n+2r}/\Delta_{2n+2r})$ holds, this condition is equivalent to the algebraic independence of $\{U_l, \ldots, U_l^{(n+r)}\}$ in $k\langle Y\rangle \otimes (A_{2n+2r}/\Delta_{2n+2r})$, which is met in turn if and only if the columns of the matrix J corresponding to derivatives with respect to variables in $U_l^{[n+r]}$ can be removed with no change in rank (Lemma 19).

Set l_1 for the minimum l $(1 \leqslant l \leqslant m)$ such that the last condition holds for U_l (its existence is ensured by Lemma 17 and the previous arguments).

Then, we can replace the differential base field $k\langle Y\rangle$ with the differential field $k\langle Y, U_{l_1}\rangle$ and look for a differential transcendence basis of the extension $k\langle Y, U_{l_1}\rangle \hookrightarrow \mathcal{F}$, whose transcendence degree is $m - r - 1$. That is, we consider the same problem on the input differential equation system regarded as a system in $k\langle U_{l_1}\rangle\{Y, X, U \setminus \{U_{l_1}\}\}$, and we repeat the process. □

4.3. The algorithms and their complexities

In this subsection, we present probabilistic algorithms for the computation of the differential Hilbert function of the ideal $k\langle Y\rangle \otimes \Delta$ and of a differential transcendence basis of the extension $k\langle Y\rangle \hookrightarrow \mathcal{F}$ following the theoretical results stated in Propositions 16 and 20.

Before going on, we show a very elementary example to illustrate how these results can be applied. Consider the differential system

$$\begin{cases} Y_1 = U_1 + \dot{U}_2 + \dot{U}_3 \\ Y_2 = \dot{U}_1 + U_2 + U_3 \end{cases}$$

In this case, $n = 0$, $r = 2$ and $m = 3$. Therefore, the matrix J defined in Proposition 20 is

$$J = \left(\begin{array}{ccc|cccccccccc} 1&0&0&0&1&1&0&0&0&0&0&0&0&0\\ 0&1&1&1&0&0&0&0&0&0&0&0&0&0\\ \hline 0&0&0&1&0&0&0&1&1&0&0&0&0&0\\ 0&0&0&0&1&1&1&0&0&0&0&0&0&0\\ \hline 0&0&0&0&0&0&1&0&0&0&1&1&0&0\\ 0&0&0&0&0&0&0&1&1&1&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&1&0&0&1&1\\ 0&0&0&0&0&0&0&0&0&0&1&1&1&0 \end{array}\right).$$

Clearly, $\operatorname{rank}(J_0) = 8$, $\operatorname{rank}(J_1) = 6$ and $\operatorname{rank}(J_2) = 4$, where J_0, J_1 and J_2 are the distinguished submatrices of J defined in Proposition 16, and then

$$\mathcal{H}_{k\langle Y\rangle\otimes\Delta,\, k\langle Y\rangle}(i) = (i+1) + 2 \quad \text{for } i \geqslant 0.$$

In order to apply the result in Proposition 20, we observe that the matrix J has full row rank and the same remains true when the columns corresponding to derivatives with respect to either the variables $U_2, \dot{U}_2, U_2^{(2)}$ or $U_3, \dot{U}_3, U_3^{(2)}$ are removed; however, the rank drops when removing the columns corresponding to $U_1, \dot{U}_1, U_1^{(2)}$. Therefore, both $\{U_2\}$ and $\{U_3\}$ are differential transcendence bases, but $\{U_1\}$ is not (in fact we have $U_1^{(2)} - U_1 - \dot{Y}_2 + Y_1 = 0$).

Now, we start with the description of the algorithms. For technical and algorithmic reasons, we will assume throughout this subsection that the base differential field k is the rational effective field $\mathbb{Q}(t)$ (with the standard derivation), and that the polynomials defining system (1) have coefficients in $\mathbb{Q}[t]$.

Our algorithms will deal not only with the input polynomials f, g (which will be encoded by straight-line programs), but also with their successive derivatives $\dot{f}, \dot{g}, f^{(2)}, g^{(2)}$ and so on. As pointed out in [26, Section 5.2], one can obtain short slp's for these successive derivatives from slp's for the input polynomials:

Lemma 21. *Let $Z := \{Z_1, \ldots, Z_\alpha\}$ be a set of differential indeterminates over $\mathbb{Q}(t)$ and let $f \in \mathbb{Q}[t][Z, \dot{Z}]$ be a polynomial encoded by a straight-line program of length L. Let $\nu \in \mathbb{N}$. Then, there exists a straight-line program of length $O(\nu^2(\nu\alpha + L))$ which computes $f^{(j)}$ for every $j < \nu$.*

Proof. Let T be a new variable. For $i = 1, \ldots, \alpha$, let $\eta_i(T) := \sum_{k=0}^{\nu} \frac{Z_i^{(k)}}{k!} T^k$. Denote $\eta := (\eta_1, \ldots, \eta_\alpha)$ and set $S(T) := f(T + t, \eta, \dot{\eta}) \in \mathbb{Q}[t, Z, \dot{Z}, \ldots, Z^{(\nu)}][T]$. The chain rule implies that $\frac{\partial^j S}{\partial T^j} = f^{(j)}(T + t, \eta, \dot{\eta}, \ldots, \eta^{(j+1)})$ for $j = 0, \ldots, \nu - 1$, and so, specializing $T = 0$, we obtain $\frac{\partial^j S}{\partial T^j}(0) = f^{(j)}(t, Z, \dot{Z}, \ldots, Z^{(j+1)})$ for $j = 0, \ldots, \nu - 1$. Then, if $S(T) = \sum_{j=0}^{\nu} s_j(t, Z, \dot{Z}, \ldots, Z^{(j+1)}) T^j$, the following identities hold:

$$f^{(j)}(t, Z, \dot{Z}, \ldots, Z^{(j+1)}) = j!\, s_j(t, Z, \dot{Z}, \ldots, Z^{(j+1)}), \quad j = 0, \ldots, \nu - 1. \tag{3}$$

These identities enable us to obtain an slp for the computation of these polynomials:

The first step consists in the computation of an slp encoding $S(T)$: we compute the monomials $\frac{T^k}{k!} = \frac{T}{k}\,\frac{T^{k-1}}{(k-1)!}$ for $k = 2, \ldots, v$ recursively with $2v-2$ operations, and then we obtain slp's for the polynomials $\eta_i, \dot{\eta}_i$ for $i = 1, \ldots, \alpha$ by multiplying these monomials by the corresponding coefficients $Z_i^{(k)}$ and adding the results. This requires $\alpha(4v-2)$ additional operations. Finally, an slp encoding $S(T)$ is obtained as the composition of the slp encoding f, an slp of length 1 computing $T+t$, and those obtained for $\eta_i, \dot{\eta}_i$ $(1 \leqslant i \leqslant \alpha)$. The total length of this slp is $\mathcal{L} := 2v - 1 + \alpha(4v-2) + L$.

In a second step, the procedure described in [22, Lemma 13] is applied to obtain an slp of length $v^2\mathcal{L}$ encoding all the coefficients s_j, $j = 0, \ldots, v-1$, of $S(T)$. Finally, the coefficients s_j are multiplied by the corresponding constant factors according to (3) in order to obtain the slp for the polynomials $f^{(j)}$, $j = 0, \ldots, v-1$. The total length of the slp obtained is bounded by $6\,v^3\alpha + v^2 L$. □

Notice that, due to the ring inclusion $\mathbb{Q}(t)[X, U^{[2n+2r]}] \hookrightarrow \mathbb{Q}(t)\langle Y\rangle \otimes (A_{2n+2r}/\Delta_{2n+2r})$ (see Proposition 8), the rank computations involved in Propositions 16 and 20 amount to rank computations in the polynomial ring $\mathbb{Q}[t, X, U^{[2n+2r]}]$: for $i = 0, \ldots, n+r$, let $\tilde{J}_i$ be the matrix with entries in $\mathbb{Q}[t][X, U^{[2n+2r]}]$ which is obtained by substituting $X_j^{(l)} = \tilde{f}_j^{(l-1)}$ (see Notation 6) for $j = 1, \ldots, n$, $l = 1, \ldots, 2n+2r$ in the entries of the matrix J_i defined in Proposition 16. Finally, set $\tilde{J}$ for the matrix with entries in $\mathbb{Q}[t][X, U^{[2n+2r]}]$ obtained by making this substitution in the Jacobian matrix J introduced in Proposition 20. Then, $\operatorname{rank}_{\mathbb{Q}(t)\langle Y\rangle \otimes (A_{2n+2r}/\Delta_{2n+2r})}(J_i) = \operatorname{rank}_{\mathbb{Q}[t][X, U^{[2n+2r]}]}(\tilde{J}_i)$, and the same holds for J and $\tilde{J}$.

Now, Propositions 16 and 20 can be restated as follows:

Corollary 22. *The Hilbert function of the ideal $\mathbb{Q}(t)\langle Y\rangle \otimes \Delta$ over $\mathbb{Q}(t)\langle Y\rangle$ is $\mathcal{H} : \mathbb{N}_0 \to \mathbb{N}_0$,*

$$\mathcal{H}(i) = \begin{cases} (n+m)(i+1) - (2n+2r)(n+r) + \operatorname{rank}(\tilde{J}_i) & \text{if } i \leqslant n+r, \\ (m-r)(i+1) + \operatorname{rank}(\tilde{J}_{n+r}) - (n+r)(n+r-1) & \text{if } i \geqslant n+r, \end{cases}$$

where the ranks of the matrices $\tilde{J}_i$ are taken over the polynomial ring $\mathbb{Q}[t, X, U^{[2n+2r]}]$.

Corollary 23. *A set $W \subset U$ with $m-r$ elements is a differential transcendence basis of the differential extension $\mathbb{Q}(t)\langle Y\rangle \hookrightarrow \mathcal{F}$ if and only if the columns of $\tilde{J}$ corresponding to derivatives with respect to variables in $W^{[n+r]}$ can be removed with no change in rank (where the ranks are taken over the ring $\mathbb{Q}[t, X, U^{[2n+2r]}]$).*

The rank computations over a polynomial ring involved in the previous corollaries will be reduced to rank computations over $\mathbb{Q}$ by means of the next result which follows easily from the Zippel–Schwartz zero-test (see Section 2.2):

Lemma 24. *Let $Z := \{Z_1, \ldots, Z_\alpha\}$ be a set of indeterminates over $\mathbb{Q}$ and let $A \in \mathbb{Q}[Z]^{p\times q}$ be a matrix whose entries satisfy $\deg(A_{ij}) \leqslant D_i$ for $i = 1, \ldots, p$. Then, if the coordinates of a point $z := (z_1, \ldots, z_\alpha)$ are chosen at random in the set $\{0, \ldots, N-1\}$, we have $\operatorname{rank}_{\mathbb{Q}[Z]}(A) = \operatorname{rank}_{\mathbb{Q}}(A(z))$ with error probability bounded by $\frac{1}{N}\sum_{i=1}^{p} D_i$.*

This lemma provides a straightforward probabilistic algorithm for the computation of the rank of a polynomial matrix: under the previous assumptions and notations, the algorithm chooses at random the coordinates of the point z in a set of type $\{0, \ldots, N-1\}$ for a sufficiently big integer

N and computes the rank of the matrix $A(z) \in \mathbb{Q}^{p\times q}$ applying any of the well-known algorithms for the computation of the rank of a matrix with rational entries. The random choice of the element z can be made within complexity $O(\alpha \log(N))$, while the complexity of computing $\operatorname{rank}(A(z))$ may be estimated as $O((p+q)^3)$ (see, for instance, [2, Chapter 2, Section 2, Problem 2.10]).

In order to estimate the error probability of our algorithms we will need an upper bound on the degrees of the polynomials involved:

Remark 25. For $h = 1, \ldots, n$, $j = 1, \ldots, r$ and $l \in \mathbb{N}_0$, let $\tilde{f}_h^{(l)}$, $\tilde{g}_j^{(l)}$ be the polynomials introduced in Notation 6. A recursive computation shows that, if $\deg(f_h) \leqslant d$ and $\deg(g_j) \leqslant d$ for every $1 \leqslant h \leqslant n$ and $1 \leqslant j \leqslant r$, then $d + l(d-1)$ is an upper bound for the degrees of $\tilde{f}_h^{(l)}$ and $\tilde{g}_j^{(l)}$ for every $l \in \mathbb{N}_0$.

Now, we are ready to prove our algorithmic result on the computation of the differential Hilbert function. We keep the same notations and assumptions as in Section 3.1:

Theorem 26. *Assume that $f_1, \ldots, f_n \in \mathbb{Q}[t, X, U]$ and $g_1, \ldots, g_r \in \mathbb{Q}[t, X, U, \dot{U}]$ have degrees bounded by d and are encoded by a straight-line program of length L. Then, there is a probabilistic algorithm which computes, for every $\varepsilon \in (0,1)$, the differential Hilbert function of the ideal $\mathbb{Q}(t)\langle Y\rangle \otimes \Delta$ over $\mathbb{Q}(t)\langle Y\rangle$ with error probability bounded by ε within complexity $O((\log(1/\varepsilon) + \log(d))(n+m)^3(n+r)^8 L)$.*

Proof. The algorithm is based on Corollary 22. Thus, for $i = 0, \ldots, n+r$, it computes the rank of the matrix $\tilde{J}_i \in (\mathbb{Q}[t][X, U^{[2n+2r]}])^{(n+r)(2n+2r-i)\times(n+m)(2n+2r-i)}$.

Fix i with $0 \leqslant i \leqslant n+r$. From the definition of $\tilde{J}_i$ and Remark 25, we deduce that for $l = 0, \ldots, 2n+2r-i-1$ and $j = 1, \ldots, n+r$, the entries in the $(l(n+r)+j)$th row of $\tilde{J}_i$ are polynomials in $\mathbb{Q}[t, X, U^{[2n+2r]}]$ with degrees bounded by $d + (l+i)(d-1)$. Therefore, by Lemma 24, the rank of the matrix $\tilde{J}_i$ can be computed with error probability bounded by $p_i := \frac{1}{N}\sum_{l=0}^{2n+2r-i-1}(n+r)(d+(l+i)(d-1)) \leqslant \frac{4}{N} d(n+r)^3$ by choosing the coordinates of a point $z_i := (z_{i,t}, z_{i,X}, z_{i,U^{[2n+2r]}})$ at random from the set $\{0, \ldots, N-1\}$. This random choice can be made within complexity $O(m(n+r)\log(N))$. Then, once the matrix $\tilde{J}_i(z_i)$ is obtained, its rank can be computed within complexity $O((n+m)^3(n+r)^3)$.

In order to compute the entries of the matrices $\tilde{J}_i(z_i)$, we proceed as follows: first, we derive slp's of length $O((n+r)^2((n+r)(n+m)+L))$ for the polynomials $F_h^{[2n+2r-1]}$, $G_j^{[2n+2r-1]}$ from the slp's encoding $f_1, \ldots, f_n, g_1, \ldots, g_r$, as stated in Lemma 21. The complexity of this step is of order $O((n+r)^3((n+r)(n+m)+L))$. Then, we compute slp's for the partial derivatives of these polynomials with respect to the variables $\{X, U\}^{[2n+2r]}$. A result due to Baur and Strassen (see, for instance, [3, Section 7.2]) enables us to obtain slp's of length $O((n+r)^2((n+r)(n+m)+L))$ for these partial derivatives within complexity $O((n+r)^4((n+r)(n+m)+L))$. Now, we obtain an slp of length $O(n(n+r)^3((n+r)(n+m)+L))$ for the polynomials $\tilde{f}_h^{(l)}$ $(1 \leqslant h \leqslant n,\ 0 \leqslant l \leqslant 2n+2r)$ and then, slp's of the same order for the entries of $\tilde{J}_i$, by composition. Finally, we compute the entries of $\tilde{J}_i(z_i)$ by specializing the slp's encoding the entries of $\tilde{J}_i$ into z_i. This can be done within complexity $O(n(n+r)^6(n+m)((n+r)(n+m)+L))$, which dominates the complexity of the whole computation.

Thus, we obtain the differential Hilbert function of the ideal $\mathbb{Q}(t)\langle Y\rangle \otimes \Delta$ with probability at least $\prod_{i=0}^{n+r}(1-p_i) \geqslant 1 - \sum_{i=0}^{n+r} p_i \geqslant 1 - \sum_{i=0}^{n+r} \frac{4}{N} d(n+r)^3 \geqslant 1 - \frac{8}{N} d(n+r)^4$ within complexity $O(m(n+r)^2\log(N) + (n+m)^3(n+r)^8 L)$.

In order that the error probability of the algorithm is bounded by ε, we take $N := \lceil 1/\varepsilon \rceil 8d(n+r)^4$. With this choice, the overall complexity of the procedure is of order $O((\log(1/\varepsilon)+\log(d))(n+m)^3(n+r)^8 L)$. □

The computation of a differential transcendence basis of $\mathbb{Q}(t)\langle Y\rangle \hookrightarrow \mathcal{F}$ follows the recursive procedure leading to the proof of Proposition 20. In fact, we will compute the *minimal index* differential transcendence basis of $\mathbb{Q}(t)\langle Y\rangle \hookrightarrow \mathcal{F}$, which we define to be the differentially algebraically independent subset $\{U_{l_1}, \ldots, U_{l_{m-r}}\}$ that is minimal with respect to the lexicographical ordering of the variables U in which $U_1 < U_2 < \cdots < U_m$.

Theorem 27. *There is a probabilistic algorithm which computes, for every $\varepsilon \in (0,1)$, the minimal index differential transcendence basis of $\mathbb{Q}(t)\langle Y\rangle \hookrightarrow \mathcal{F}$ with error probability bounded by ε within complexity $O((\log(1/\varepsilon)+\log(d))m(n+m)^3(n+r)^7 L)$.*

Proof. Let $\tilde{J}$ be the matrix introduced in the paragraph preceding Corollary 22. Note that, due to Corollary 9, $\tilde{J}$ has full row rank. In a first step, the algorithm chooses the coordinates of a point $z := (z_t, z_X, z_{U^{[2n+2r]}})$ at random from the set $\{0, \ldots, N-1\}$ for a sufficiently big integer N and computes $\operatorname{rank}(\tilde{J}(z))$. If $\tilde{J}(z)$ has not full row rank, it returns an error message. Otherwise, the algorithm proceeds recursively, starting with the set of variables W being the empty set.

For $k \leqslant m$, the kth recursive step is as follows: if $\#W < m-r$, the algorithm computes the rank of the matrix $\tilde{J}(z)^{W\cup\{U_k\}}$ which is obtained by removing the columns of $\tilde{J}(z)$ corresponding to derivatives with respect to the variables $(W \cup \{U_k\})^{[n+r]}$. If $\operatorname{rank}(\tilde{J}(z)^{W\cup\{U_k\}}) = \operatorname{rank}(\tilde{J}(z))$, the variable U_k is added to the set W. Otherwise, W is not modified. When $\#W = m-r$, the algorithm outputs the set W.

If the recursion finishes with $\#W < m-r$, the algorithm returns an error message.

Now let us estimate the error probability of this procedure: let W be the minimal index differential transcendence basis of $\mathbb{Q}(t)\langle Y\rangle \hookrightarrow \mathcal{F}$. Then, the matrix $\tilde{J}^W$ which is obtained from $\tilde{J}$ by removing the columns corresponding to derivatives with respect to the variables $W^{[n+r]}$ has full row rank, and so, it has a square submatrix of size $(n+r)(2n+2r)$ with non-zero determinant P_0. Therefore, any point $z := (z_t, z_X, z_{U^{[2n+2r]}})$ satisfying $P_0(z) \neq 0$ leads to a matrix $\tilde{J}(z)$ with full row rank for which the algorithm computes the desired minimal index differential transcendence basis. Since $\deg P_0 \leqslant 4d(n+r)^3$ (this estimate follows as in the proof of Theorem 26), we conclude that the error probability of the algorithm is at most $\frac{4}{N}d(n+r)^3$.

In order that the error probability of the algorithm is bounded by ε, we choose $N := \lceil 1/\varepsilon \rceil 4d(n+r)^3$. The complexity bound can be obtained as in the proof of Theorem 26. □

Remark 28. The algorithm in Theorem 27 may fail to compute the *minimal index* differential transcendence basis of the extension, but any set W output by the algorithm is a differential transcendence basis of $\mathbb{Q}(t)\langle Y\rangle \hookrightarrow \mathcal{F}$. If the algorithm is unable to obtain a set W with $m-r$ elements, it will return an error message.

5. Resolvent representation

This section is concerned with the notions of a primitive element of a differentially algebraic field extension and of a resolvent representation of a prime differential ideal introduced by Ritt (see [27]). We present these concepts following [34] in Section 5.1 and then, in the remaining

subsections, we study quantitative aspects, namely order and degree of these objects, for our particular system (1).

5.1. Existence of a primitive element and a resolvent representation

In this subsection we recall the notion of primitive element of a finite differentially algebraic field extension and the closely related concept of resolvent representation of a prime differential ideal.

Let K be a differential field with $\mathrm{char}(K) = 0$ containing a non-constant element ξ (i.e. $\dot{\xi} \neq 0$), and let $Z := \{Z_1, \ldots, Z_\alpha\}$ be a set of differential indeterminates over K. Let $\mathcal{I}$ be a prime differential ideal of $K\{Z\}$ with $\mathrm{diffdim}(\mathcal{I}) = 0$. Set $\mathcal{F} := \mathrm{Frac}(K\{Z\}/\mathcal{I})$ and consider the differential field extension $K \hookrightarrow \mathcal{F}$. Then, a differential analogue of the well-known theorem of the primitive element holds (see [28,34]). We include Seidenberg's proof [34, Theorem 1] since the arguments therein are the basis for several effective results we will prove later.

Theorem 29. *With the previous assumptions and notations, there exists $\gamma \in \mathcal{F}$ such that $\mathcal{F} = K\langle\gamma\rangle$. Moreover, γ can be chosen as a linear combination $\gamma = \lambda_1 Z_1 + \cdots + \lambda_\alpha Z_\alpha$, where λ_i is a polynomial in $\mathbb{Q}[\xi] \subset K$ for $i = 1, \ldots, \alpha$.*

Proof. Let $\Lambda := \{\Lambda_1, \ldots, \Lambda_\alpha\}$ be a set of indeterminates over $K\langle Z\rangle$. Let us observe that $\mathcal{F}\langle\Lambda\rangle$ is the fraction field of $K\langle\Lambda\rangle\{Z\}/K\langle\Lambda\rangle \otimes \mathcal{I}$ and $K\langle\Lambda\rangle \hookrightarrow \mathcal{F}\langle\Lambda\rangle$ is a differentially algebraic field extension. Then, if $\Gamma := \Lambda_1 Z_1 + \cdots + \Lambda_\alpha Z_\alpha$, the set of derivatives $\{\Gamma^{(l)} : l \in \mathbb{N}_0\} \subset \mathcal{F}\langle\Lambda\rangle$ is differentially algebraically dependent over $K\langle\Lambda\rangle$ and so, there exists a differential polynomial $\mathcal{X}$ in $K\langle\Lambda\rangle\{T\}$, where T is a new differential indeterminate over $K\langle\Lambda\rangle$, satisfying $\mathcal{X}(\Gamma) = 0$ in $\mathcal{F}\langle\Lambda\rangle$. Assume $\mathcal{X}$ to be of minimal order h and of minimal degree among the differential polynomials of order h vanishing at Γ.

Without loss of generality we may assume that the coefficients of $\mathcal{X}$ are polynomials in $K\{\Lambda\}$ and that $\mathcal{X}(\Gamma, \dot{\Gamma}, \ldots, \Gamma^{(h)}) \in K\{\Lambda\}\otimes\mathcal{I}$. Then, for $i = 1, \ldots, \alpha$, we have that $\partial\mathcal{X}(\Gamma, \ldots, \Gamma^{(h)})/\partial\Lambda_i^{(h)} \in K\{\Lambda\} \otimes \mathcal{I}$, that is,

$$\frac{\partial\mathcal{X}}{\partial T^{(h)}}(\Gamma, \ldots, \Gamma^{(h)})\, Z_i + \frac{\partial\mathcal{X}}{\partial\Lambda_i^{(h)}}(\Gamma, \ldots, \Gamma^{(h)}) \in K\{\Lambda\} \otimes \mathcal{I}. \tag{4}$$

Let $Q := \frac{\partial\mathcal{X}}{\partial T^{(h)}}(T, \ldots, T^{(h)}) \in K\{\Lambda\}\{T\}$. The minimality conditions set on $\mathcal{X}$ imply that, specializing the differential variable T into Γ, we obtain a non-zero polynomial $Q_\Lambda := \frac{\partial\mathcal{X}}{\partial T^{(h)}}(\Gamma, \ldots, \Gamma^{(h)})$ in $\mathcal{F}\{\Lambda\}$. Since $\xi \in \mathcal{F}$ is a non-constant element, a result in [28, Chapter 2, Section 22] shows the existence of elements $\lambda_i \in \mathbb{Q}[\xi]$ for $i = 1, \ldots, \alpha$, with $Q_\Lambda(\lambda_1, \ldots, \lambda_\alpha) \neq 0$. Now, if we take $\gamma := \lambda_1 Z_1 + \cdots + \lambda_\alpha Z_\alpha \in \mathcal{F}$, we deduce from identity (4) that $Z_i \in K\langle\gamma\rangle \subset \mathcal{F}$ for $i = 1, \ldots, \alpha$, which implies that $\mathcal{F} = K\langle\gamma\rangle$. □

Under the previous assumptions, an element $\gamma \in \mathcal{F}$ such that $\mathcal{F} = K\langle\gamma\rangle$ will be called a *primitive element* of the differential field extension $K \hookrightarrow \mathcal{F}$.

The following result shows that the order of a zero-dimensional prime differential ideal is an upper bound for the number of derivatives of the primitive element involved in a representation of an arbitrary element of the field extension.

Proposition 30. *Let γ be a primitive element of the extension $K \hookrightarrow \mathcal{F}$ as above. Let $s \in \mathbb{N}$ be the maximum positive integer such that $\{\gamma, \ldots, \gamma^{(s-1)}\} \subset \mathcal{F}$ is algebraically independent over K. Let T be a new differential variable. Then:*

(i) *For every $\zeta \in \mathcal{F}$, there exist polynomials P_ζ and $Q_\zeta \in K[T^{[s]}]$ such that $\zeta = P_\zeta(\gamma^{[s]})/Q_\zeta(\gamma^{[s]})$ in $\mathcal{F}$. In particular, $\{\gamma, \ldots, \gamma^{(s-1)}\}$ is a transcendence basis of $K \hookrightarrow \mathcal{F}$ and $\mathcal{F} = K(\gamma, \ldots, \gamma^{(s-1)}, \gamma^{(s)})$.*

(ii) *$s = \operatorname{ord}_K(\mathcal{I})$.*

Proof. In order to prove (i), let $\zeta \in \mathcal{F}$. Since $\mathcal{F} = K\langle\gamma\rangle$, there exist polynomials $P, Q \in K\{T\}$ such that $\zeta = P(\gamma)/Q(\gamma)$ in $\mathcal{F}$.

Now, the assumption on s implies the existence of a polynomial $M \in K[T^{[s]}]$ with $M(\gamma^{[s]}) = 0$ in $\mathcal{F}$. We may assume M to be of minimal degree in the variable $T^{(s)}$ so that $\frac{\partial M}{\partial T^{(s)}}(\gamma^{[s]}) \neq 0$ in $\mathcal{F}$. Let $I_M \in K[T^{[s-1]}]$ be the leading coefficient of M in the variable $T^{(s)}$ and let $S_M := \frac{\partial M}{\partial T^{(s)}} \in K[T^{[s]}]$. We have $I_M(\gamma) \neq 0$ and $S_M(\gamma) \neq 0$.

By a derivation and division process (see Section 2.1.2), it follows that there exist non-negative integers a_1, b_1, a_2, b_2 and polynomials R_P, $R_Q \in K[T^{[s]}]$ such that $I_M^{a_1} S_M^{b_1} P - R_P$ and $I_M^{a_2} S_M^{b_2} Q - R_Q$ belong to the differential ideal $[M] \subset K\{T\}$. Since $M^{(j)}(\gamma) = 0$ in the differential field $\mathcal{F}$ for every $j \geqslant 0$, we have that the identities $R_P(\gamma^{[s]}) = I_M^{a_1}(\gamma) S_M^{b_1}(\gamma) P(\gamma)$ and $R_Q(\gamma^{[s]}) = I_M^{a_2}(\gamma) S_M^{b_2}(\gamma) Q(\gamma)$ hold in $\mathcal{F}$. Thus, defining $P_\zeta := I_M^{a_2} S_M^{b_2} R_P \in K[T^{[s]}]$ and $Q_\zeta := I_M^{a_1} S_M^{b_1} R_Q \in K[T^{[s]}]$ we obtain the identity $\zeta = P_\zeta(\gamma^{[s]})/Q_\zeta(\gamma^{[s]})$ in $\mathcal{F}$, which finishes the proof of the first part of the proposition.

To prove (ii), we observe that the elements $\gamma, \ldots, \gamma^{(s)}$ can be regarded as elements of $\mathcal{L}_v := \operatorname{Frac}(K[Z^{[v]}]/\mathcal{I} \cap K[Z^{[v]}]) \subset \mathcal{F}$ for v big enough and so, we deduce from (i) that $\mathcal{L}_v = \mathcal{F}$. Therefore, $s = \operatorname{trdeg}_K(\mathcal{F}) = \operatorname{trdeg}_K(\mathcal{L}_v) = \mathcal{H}_{\mathcal{I},K}(v) = \operatorname{ord}_K(\mathcal{I})$, for v big enough, where the last equality is due to the fact that $\mathcal{I}$ is a zero-dimensional differential ideal. □

Let $\gamma \in K\{Z\}$ be such that its class in $\mathcal{F}$ is a primitive element of the differential field extension $K \hookrightarrow \mathcal{F}$. Set $s := \operatorname{ord}_K(\mathcal{I})$. By Proposition 30, $\{\gamma, \ldots, \gamma^{(s-1)}\}$ is a transcendence basis of $K \hookrightarrow \mathcal{F}$. Multiplying the minimal (monic) polynomial of $\gamma^{(s)}$ in the algebraic field extension $K(\gamma, \ldots, \gamma^{(s-1)}) \hookrightarrow \mathcal{F}$ by a non-zero element in $K(\gamma, \ldots, \gamma^{(s-1)})$ and renaming the variables $\gamma, \ldots, \gamma^{(s-1)}$ as $T, \ldots, T^{(s-1)}$, we can obtain an irreducible polynomial $M \in K[T, \ldots, T^{(s-1)}, T^{(s)}]$ with $M(\gamma, \ldots, \gamma^{(s-1)}, \gamma^{(s)}) = 0$ in $\mathcal{F}$. Any irreducible polynomial $M \in K[T, \ldots, T^{(s)}]$ with $M(\gamma, \ldots, \gamma^{(s)}) = 0$ in $\mathcal{F}$ will be called a *minimal polynomial* of γ in $K \hookrightarrow \mathcal{F}$.

Notice that, if $P \in K[T, \ldots, T^{(s)}]$ is a polynomial with $P(\gamma, \ldots, \gamma^{(s)}) = 0$ in $\mathcal{F}$, then a minimal polynomial M of γ divides P in $K(T, \ldots, T^{(s-1)})[T^{(s)}]$ and, M being primitive, it also divides P in $K[T, \ldots, T^{(s-1)}, T^{(s)}]$. Then, the set of all polynomials $P \in K[T, \ldots, T^{(s)}]$ with $P(\gamma, \ldots, \gamma^{(s)}) = 0$ in $\mathcal{F}$ is a principal ideal of $K[T, \ldots, T^{(s)}]$ which is generated by *any* minimal polynomial of γ in $K \hookrightarrow \mathcal{F}$. Thus, a minimal polynomial of γ in $K \hookrightarrow \mathcal{F}$ is uniquely determined up to scalar factors in $K \setminus \{0\}$.

On the other hand, for $i = 1, \ldots, \alpha$, there exist polynomials $p_i(T), q_i(T) \in K\{T\}$ with $q_i(\gamma) \neq 0$ in $\mathcal{F}$, such that $Z_i = p_i(\gamma)/q_i(\gamma)$ in $\mathcal{F}$. In other words, $q_i(\gamma) Z_i - p_i(\gamma) \in \mathcal{I}$ for $i = 1, \ldots, \alpha$ (in fact, due to Proposition 30, there exist polynomials p_i, q_i of order bounded by s satisfying these conditions).

Definition 31. Under the previous assumptions and notation, the set $\{M, q_1(T)Z_1 - p_1(T), \ldots, q_\alpha(T)Z_\alpha - p_\alpha(T)\}$, where M is a minimal polynomial of γ in $K \hookrightarrow \mathcal{F}$, is called a *resolvent representation* of the zero-dimensional prime differential ideal $\mathcal{I}$ with respect to the primitive element γ.

This notion can be extended to the positive-dimensional case: let $\mathcal{K}$ be a differential field containing a non-constant element and let $\mathcal{I}$ be a prime differential ideal of $\mathcal{K}\{Z\}$ with $\operatorname{diffdim}(\mathcal{I}) = r$. Consider a differential transcendence basis $W \subset Z$ of $\mathcal{K} \hookrightarrow \mathcal{F}$. Setting $K := \mathcal{K}\langle W\rangle$ and $\bar{Z} := Z \setminus W$, the ideal $K \otimes \mathcal{I}$ of $K\{\bar{Z}\}$ has differential dimension zero and the field $\mathcal{F}$ is the fraction field of $K\{\bar{Z}\}/K \otimes \mathcal{I}$. Then, the previous assumptions hold and so, there exist a primitive element γ of the extension $K \hookrightarrow \mathcal{F}$ and a resolvent representation $\{M, q_1(T)\bar{Z}_1 - p_1(T), \ldots, q_{\alpha-r}(T)\bar{Z}_{\alpha-r} - p_{\alpha-r}(T)\}$ of the ideal $K \otimes \mathcal{I}$. Without loss of generality, we may assume that $M \in \mathcal{K}\{W\}\{T\}$, and also that $q_i, p_i \in \mathcal{K}\{W\}\{T\}$ for $1 \leqslant i \leqslant \alpha$. The set $\{M, q_1(T)\bar{Z}_1 - p_1(T), \ldots, q_{\alpha-r}(T)\bar{Z}_{\alpha-r} - p_{\alpha-r}(T)\} \subset \mathcal{K}\{W\}\{T\}$ is called a *resolvent representation of the prime differential ideal $\mathcal{I}$ with respect to the transcendence basis W and the primitive element γ*.

A generalization of the notion of resolvent representation for the class of *regular* differential ideals, which will not be considered in this paper, can be found in [4,5].

5.2. Bounds for the order and degree of a minimal polynomial of a primitive element

In what follows, we go back to our particular situation arising from the differential equation system (1). We keep the same notations and assumptions as in Sections 3 and 4. We will assume further that our differential base field k contains a non-constant element and that a differential transcendence basis $W \subset U$ of $k\langle Y\rangle \hookrightarrow \mathcal{F}$ has been fixed.

First, we will prove an upper bound for the total order of a minimal polynomial of a primitive element of the extension $k\langle Y, W\rangle \hookrightarrow \mathcal{F}$. Then, we will show that this polynomial can be regarded as an eliminating polynomial associated to a suitable linear projection of a certain algebraic variety, which will enable us to deduce a degree upper bound.

Denote $\bar{U} := U \setminus W$ and $K := k\langle Y, W\rangle$. Then, $K \otimes \Delta$ is a zero-dimensional prime differential ideal of $K\{X, \bar{U}\}$. Let $\gamma := \lambda_1 X_1 + \cdots + \lambda_n X_n + \lambda_{n+1}\bar{U}_1 + \cdots + \lambda_{n+r}\bar{U}_r \in k[X, \bar{U}]$ be a linear form such that its class in $\mathcal{F}$ is a primitive element of the differential field extension $K \hookrightarrow \mathcal{F}$. Set $s := \operatorname{ord}_K(K \otimes \Delta)$; so, a minimal polynomial M of γ in $K \hookrightarrow \mathcal{F}$ lies in $K[T, \ldots, T^{(s)}]$ (see Proposition 30).

Now, we will show the existence of a minimal polynomial of γ in $K \hookrightarrow \mathcal{F}$ with 'low' order also in the variables Y, W.

Lemma 32. *There exists a minimal polynomial $M \in K[T, \ldots, T^{(s)}]$ of γ in $K \hookrightarrow \mathcal{F}$ such that $M \in k[Y^{[2n+2r-1]}, W^{[2n+2r]}][T^{[s]}]$ and $M(\gamma, \ldots, \gamma^{(s)}) \in \Delta_{2n+2r}$.*

Proof. As in the proof of Proposition 30 (ii), since γ has order 0 and $s \leqslant n + r$, we have that the field $\mathcal{F}$ coincides with the fraction field $\operatorname{Frac}(K \otimes A_{n+r}/(K \otimes \Delta) \cap (K \otimes A_{n+r}))$. Then, if $P \in K[T, \ldots, T^{(s)}]$ is a minimal polynomial of γ in $K \hookrightarrow \mathcal{F}$, we have that $P(\gamma, \ldots, \gamma^{(s)}) \in (K \otimes \Delta) \cap (K \otimes A_{n+r})$. Multiplying it by a non-zero element of K, we may assume $P \in k\{Y, W\}[T^{[s]}]$.

Now, with a proof analogous to that of Lemma 14, it can be shown that $(K \otimes \Delta) \cap (K \otimes A_{n+r}) \subset K \otimes \Delta_{2n+2r}$ and so, $P(\gamma, \ldots, \gamma^{(s)}) \in (K \otimes A_{n+r}) \cap (K \otimes \Delta_{2n+2r})$. Thus, there exist polynomials $a_{ik}, b_{jk} \in K \otimes A_{2n+2r}$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant r,\ 0 \leqslant k \leqslant 2n + 2r - 1)$ such that $P(\gamma, \ldots, \gamma^{(s)}) =$

$\sum_{k=0}^{2n+2r-1}(\sum_{i=1}^{n} a_{ik}F_i^{(k)}+\sum_{j=1}^{r} b_{jk}G_j^{(k)})$. Multiplying this identity by a polynomial in $k\{Y, W\}$, we may assume that $a_{ik}, b_{jk} \in k[Y^{[l]}, W^{[l]}, X^{[2n+2r]}, \bar{U}^{[2n+2r]}]$ and $P \in k[Y^{[l]}, W^{[l]}][T^{[s]}]$ for some $l \in \mathbb{N}$.

Let $I_P \in k[Y^{[l]}, W^{[l]}, T^{[s-1]}]$ be the leading coefficient of the polynomial P in the variable $T^{(s)}$, and let $y_0 := (y_{2n+2r}, \ldots, y_l)$, $w_0 := (w_{2n+2r+1}, \ldots, w_l)$ be rational vectors such that $I_P(Y^{[2n+2r-1]}, y_0, W^{[2n+2r]}, w_0, T^{[s-1]}) \not\equiv 0$. Making this substitution in all the coefficients of P and in the polynomials a_{ik}, b_{jk}, we obtain a non-zero polynomial $M \in k[Y^{[2n+2r-1]}, W^{[2n+2r]}][T^{[s]}]$ satisfying $M(\gamma, \ldots, \gamma^{(s)}) \in \Delta_{2n+2r}$. In particular, $M(\gamma, \ldots, \gamma^{(s)}) = 0$ in $\mathcal{F}$, and it follows straightforwardly that M is a minimal polynomial of γ in $K \hookrightarrow \mathcal{F}$. □

From the proof of the previous lemma, we can restate our result as follows:

Remark 33. Let σ be the minimum integer such that the identity $(K \otimes \Delta) \cap (K \otimes A_i) = (K \otimes \Delta_{i+\sigma}) \cap (K \otimes A_i)$ holds for every $i \in \mathbb{N}$. Then, there is a minimal polynomial $M \in k[Y^{[s+\sigma-1]}, W^{[s+\sigma]}][T^{[s]}]$ such that $M(\gamma, \ldots, \gamma^{(s)}) \in \Delta_{s+\sigma}$. Note that $\sigma \leqslant n + r$ (see proof of Lemma 32) and $s \leqslant n + r$ (see Proposition 2).

Lemma 32 enables us to characterize a minimal polynomial of a primitive element as any defining equation of an algebraic variety and thus, to estimate its degree.

In the sequel, unless otherwise stated, we will consider affine spaces over the field $\bar{k}$ equipped with their Zariski topologies over k, which will be denoted simply by $\mathbb{A}$.

Notation 34. Let $N_1 := r(2n+2r) + (n+m)(2n+2r+1)$ and let $\mathbb{V} \subset \mathbb{A}^{N_1}$ be the irreducible variety defined by the ideal $\Delta_{2n+2r} \subset A_{2n+2r}$ (see Remark 7).

Arbitrary points of the corresponding affine spaces will be denoted by

$$
\begin{aligned}
y &:= (y_1, \ldots, y_r, \ldots, y_1^{(2n+2r-1)}, \ldots, y_r^{(2n+2r-1)}) \in \mathbb{A}^{r(2n+2r)},\\
w &:= (w_1, \ldots, w_{m-r}, \ldots, w_1^{(2n+2r)}, \ldots, w_{m-r}^{(2n+2r)}) \in \mathbb{A}^{(m-r)(2n+2r+1)},\\
x &:= (x_1, \ldots, x_n, \ldots, x_1^{(2n+2r)}, \ldots, x_n^{(2n+2r)}) \in \mathbb{A}^{n(2n+2r+1)},\\
\bar{u} &:= (\bar{u}_1, \ldots, \bar{u}_r, \ldots, \bar{u}_1^{(2n+2r)}, \ldots, \bar{u}_r^{(2n+2r)}) \in \mathbb{A}^{r(2n+2r+1)}.
\end{aligned} \tag{5}
$$

Let $N_2 := r(2n+2r) + (m-r)(2n+2r+1) + s + 1$ and consider the linear map $\pi : \mathbb{V} \to \mathbb{A}^{N_2}$ defined by $\pi(y, w, x, \bar{u}) = (y, w, \gamma(x, \bar{u}), \ldots, \gamma^{(s)}(x, \bar{u}))$, where, for $l = 0, \ldots, s$,

$$
\gamma^{(l)} = \sum_{k=0}^{l} \binom{l}{k} \left(\sum_{i=1}^{n} \lambda_i^{(k)} X_i^{(l-k)} + \sum_{j=1}^{r} \lambda_{n+j}^{(k)} \bar{U}_j^{(l-k)} \right). \tag{6}
$$

Proposition 35. *The Zariski closure $\overline{\pi(\mathbb{V})}$ is an irreducible hypersurface in $\mathbb{A}^{N_2}$, and any irreducible polynomial $M \in k[Y^{[2n+2r-1]}, W^{[2n+2r]}, T^{[s]}]$ defining $\overline{\pi(\mathbb{V})}$ is a minimal polynomial of γ in the differential extension $k\langle Y, W\rangle \hookrightarrow \mathcal{F}$.*

Proof. Since $\mathbb{V}$ is an irreducible subvariety of $\mathbb{A}^{N_1}$, the Zariski closure $\overline{\pi(\mathbb{V})}$ is an irreducible subvariety of $\mathbb{A}^{N_2}$.

In order to prove that it is a hypersurface, let us observe first that if a non-zero polynomial $P \in k[Y^{[2n+2r-1]}, W^{[2n+2r]}, T^{[s-1]}]$ vanishes over $\pi(\mathbb{V})$, then $P(\gamma, \ldots, \gamma^{(s-1)}) = 0$ in $\mathcal{F}$, contradicting the algebraic independence of $\gamma, \ldots, \gamma^{(s-1)}$ in $k\langle Y, W\rangle \hookrightarrow \mathcal{F}$ (recall that $\Delta \cap k\{Y, W\} = 0$). This implies that $\overline{\pi(\mathbb{V})}$ has codimension at most 1. On the other hand, due to Lemma 32, there is a non-zero polynomial $M \in k[Y^{[2n+2r-1]}, W^{[2n+2r]}][T^{[s]}]$ such that $M(\gamma, \ldots, \gamma^{(s)}) \in \Delta_{2n+2r}$. Then, $\overline{\pi(\mathbb{V})} \subset \{M = 0\}$ and so, its codimension is at least 1.

It is clear that any irreducible polynomial defining $\overline{\pi(\mathbb{V})}$ is a minimal polynomial of γ in $k\langle Y, W\rangle \hookrightarrow \mathcal{F}$. □

Using [16, Lemma 2 and Theorem 1], we obtain an upper bound on the degree of the minimal polynomial given by the previous proposition:

Theorem 36. *Let $\gamma = \lambda_1 X_1 + \cdots + \lambda_n X_n + \lambda_{n+1}\bar{U}_1 + \cdots + \lambda_{n+r}\bar{U}_r$ be a primitive element of the differential field extension $k\langle Y, W\rangle \hookrightarrow \mathcal{F}$. Then, there is a minimal polynomial $M \in k[Y^{[2n+2r-1]}, W^{[2n+2r]}, T^{[s]}]$ of γ with total degree bounded by* $\deg(\mathbb{V})$. *In particular, if $d := \max\{\deg(f_i), \deg(g_j);\ 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant r\}$, due to the Bezout inequality, we have* $\deg(M) \leqslant d^{2(n+r)^2}$.

Following Remark 33, we are able to give a more precise degree upper bound for a minimal polynomial of a primitive element as in the previous theorem:

Remark 37. If $\mathbb{V}_{s+\sigma}$ denotes the variety defined by the ideal $\Delta_{s+\sigma}$, there is a minimal polynomial $M \in k[Y^{[s+\sigma-1]}, W^{[s+\sigma]}, T^{[s]}]$ with $\deg(M) \leqslant \deg(\mathbb{V}_{s+\sigma}) \leqslant d^{(n+r)(s+\sigma)}$.

The following example proves that the upper bounds stated in our previous results are optimal. In addition, it shows that for certain particular systems, our geometric upper bounds may be considerably smaller than the syntactic single exponential ones.

Example 38. Let us consider the following system over the differential field $k = \mathbb{Q}(t)$:

$$\begin{cases} \dot{X}_1 = X_1^2 \\ \dot{X}_2 = X_1^2 \\ \quad\vdots \\ \dot{X}_n = X_1^2 \end{cases}$$

Here, $r = m = 0$. It is easy to see that $s = \mathrm{ord}_k(\Delta) = n$ and that $\Delta \cap A_i = \Delta_i$ for every $i \in \mathbb{N}$ (and so, $\sigma = 0$). On the other hand, the degree of the variety $\mathbb{V}_n$ defined by the ideal Δ_n is $n+1$. Therefore, Remark 37 implies that any linear primitive element γ has a minimal polynomial $M \in k[T^{[n]}]$ with $\deg(M) \leqslant \deg(\mathbb{V}_n) = n+1$.

Actually, it is not too difficult to show that $\gamma := X_2 + tX_3 + \cdots + t^{n-2}X_n$ is a primitive element of $k \hookrightarrow \mathrm{Frac}(k\{X\}/\Delta)$ and that if $Q := 1 + t + \cdots + t^{n-2}$,

$$M := -n^n \left(T^{(n-1)}\right)^{n+1} + \sum_{j=0}^{n-2} \frac{(n-1)!}{j!}\, Q^{(j)} \left(nT^{(n-1)}\right)^j (T^{(n)})^{n-j}$$

is a minimal polynomial of γ. Let us observe that $\mathrm{ord}(M) = n = \mathrm{ord}_k(\Delta)$ and $\deg(M) = n+1 = \deg(\mathbb{V}_n)$.

5.3. The minimal polynomial of a generic primitive element

The algorithm we will present in Section 6 for the computation of a resolvent representation follows closely Seidenberg's proof of Theorem 29 relying on a construction based on the minimal polynomial of a generic primitive element. For this reason, we will need estimates for the order and degree of this polynomial also in the variables corresponding to the coefficients of this generic primitive element.

Let $\Lambda := \{\Lambda_1, \ldots, \Lambda_{n+r}\}$ be a set of new differential indeterminates over k. We change our base field k by $k_\Lambda := k\langle\Lambda\rangle$. Let $\Delta_\Lambda \subset k_\Lambda\{Y, X, U\}$ be the differential ideal generated by the differential polynomials F, G and let $\mathcal{F}_\Lambda := \mathcal{F}\langle\Lambda\rangle$, which is the fraction field of $k_\Lambda\{Y, X, U\}/\Delta_\Lambda$. The differential transcendence basis W of $k\langle Y\rangle \hookrightarrow \mathcal{F}$ continues to be a differential transcendence basis of $k_\Lambda\langle Y\rangle \hookrightarrow \mathcal{F}_\Lambda$ and so, by considering $K_\Lambda := k_\Lambda\langle Y, W\rangle$, we obtain a differential field extension $K_\Lambda \hookrightarrow \mathcal{F}_\Lambda$ which is finite and differentially algebraic. Furthermore, $\mathcal{F}_\Lambda$ is the fraction field of $K_\Lambda\{X, \bar{U}\}/K_\Lambda \otimes \Delta_\Lambda$, and the class in $\mathcal{F}_\Lambda$ of $\Gamma := \Lambda_1 X_1 + \cdots + \Lambda_n X_n + \Lambda_{n+1}\bar{U}_1 + \cdots + \Lambda_{n+r}\bar{U}_r \in k_\Lambda[X, \bar{U}]$ is a primitive element of $K_\Lambda \hookrightarrow \mathcal{F}_\Lambda$ (see the proof of Theorem 29).

Due to Proposition 30, $\{\Gamma, \ldots, \Gamma^{(s-1)}\}$ is a transcendence basis of $K_\Lambda \hookrightarrow \mathcal{F}_\Lambda$, where $s = \operatorname{ord}_{K_\Lambda}(K_\Lambda \otimes \Delta_\Lambda) = \operatorname{ord}_K(K \otimes \Delta)$, and $\mathcal{F}_\Lambda$ coincides with the fraction field of $K_\Lambda \otimes A_{n+r}/(K_\Lambda \otimes \Delta_\Lambda) \cap (K_\Lambda \otimes A_{n+r})$. Thus, Lemma 32 ensures the existence of a minimal polynomial M_Λ of Γ in $K_\Lambda \hookrightarrow \mathcal{F}_\Lambda$, such that $M_\Lambda \in k_\Lambda[Y^{[2n+2r-1]}, W^{[2n+2r]}][T^{[s]}]$ and $M_\Lambda(\Gamma, \ldots, \Gamma^{(s)}) \in (\Delta_\Lambda)_{2n+2r} := (F^{[2n+2r-1]}, G^{[2n+2r-1]}) \subset k_\Lambda[Y^{[2n+2r-1]}, X^{[2n+2r]}, U^{[2n+2r]}]$. Finally, Theorem 36 states that such a minimal polynomial M_Λ can be chosen with total degree bounded by the degree of the variety defined by the ideal $(\Delta_\Lambda)_{2n+2r}$ in the corresponding affine space over an algebraic closure of k_Λ.

Moreover, with the same arguments of specialization as in the proof of Lemma 32, the following result concerning the order in the variables Λ of a minimal polynomial M_Λ of Γ can be proved:

Proposition 39. *There is a minimal polynomial M_Λ of the generic primitive element Γ of the extension $K_\Lambda \hookrightarrow \mathcal{F}_\Lambda$ satisfying the degree upper bound of Theorem* 36 *in the variables $Y^{[2n+2r-1]}, W^{[2n+2r]}, T^{[s]}$, such that $M_\Lambda \in k[\Lambda^{[s]}, Y^{[2n+2r-1]}, W^{[2n+2r]}][T^{[s]}]$ is irreducible, and $M_\Lambda(\Gamma, \ldots, \Gamma^{(s)}) \in (F^{[2n+2r-1]}, G^{[2n+2r-1]}) \subset k[\Lambda^{[s]}, Y^{[2n+2r-1]}, X^{[2n+2r]}, U^{[2n+2r]}]$.*

As in the previous subsection, we will show that the polynomial M_Λ can be seen as an eliminating polynomial, which will enable us to give an upper bound on its degree.

Let N_1 and N_2 be as before and let $\mathbb{V}_\Lambda \subset \mathbb{A}^{N_1}(\overline{k(\Lambda^{[s]})})$ be the irreducible variety defined by the polynomials $F^{[2n+2r-1]}, G^{[2n+2r-1]}$. Consider the linear map $\pi : \mathbb{V}_\Lambda \to \mathbb{A}^{N_2}(\overline{k(\Lambda^{[s]})})$ defined by $\pi(y, w, x, \bar{u}) = (y, w, \Gamma(x, \bar{u}), \ldots, \Gamma^{(s)}(x, \bar{u}))$.

Then, from Proposition 39, we deduce the following analogue of Proposition 35:

Proposition 40. *The Zariski closure $\overline{\pi(\mathbb{V}_\Lambda)} \subset \mathbb{A}^{N_2}(\overline{k(\Lambda^{[s]})})$ is an irreducible hypersurface, and any irreducible polynomial $M_\Lambda \in k(\Lambda^{[s]})[Y^{[2n+2r-1]}, W^{[2n+2r]}, T^{[s]}]$ defining $\overline{\pi(\mathbb{V}_\Lambda)}$ is a minimal polynomial of Γ in $K_\Lambda \hookrightarrow \mathcal{F}_\Lambda$.*

Now we will obtain an upper bound for the *total* degree of a minimal polynomial of the generic primitive element Γ.

Theorem 41. *Let* $M_\Lambda \in k[\Lambda^{[s]}, Y^{[2n+2r-1]}, W^{[2n+2r]}, T^{[s]}]$ *be as in Proposition* 39 *and let* $\mathbb{V} \subset \mathbb{A}^{N_1}$ *be the algebraic variety introduced in Notation* 34. *Then, the total degree of* M_Λ *is bounded by* $(n+1+m(2n+2r+1))\deg(\mathbb{V})$.

Proof. First, let us observe that $\{Y^{[2n+2r-1]}, W^{[2n+2r]}, \Gamma^{[s-1]}\}$ is an algebraically independent set in $k_\Lambda \hookrightarrow \mathrm{Frac}(k_\Lambda \otimes A_{2n+2r}/(\Delta_\Lambda)_{2n+2r})$, which is a field extension with transcendence degree equal to $n+m(2n+2r+1)$ (see Remark 7). Then, there is a set $E \subset \{X, \bar{U}^{[2n+2r]}\}$ with $n+r-s$ elements such that $\{Y^{[2n+2r-1]}, W^{[2n+2r]}, \Gamma^{[s-1]}, E\}$ is a transcendence basis of this extension.

Throughout the proof, we will use the notation $\eta := (y, w, x, \bar{u})$ for the elements of $\mathbb{A}^{N_1}$ (keeping the notation introduced in (5)), and $\lambda := (\lambda_1, \ldots, \lambda_{n+r}, \ldots, \lambda_1^{(s)}, \ldots, \lambda_{n+r}^{(s)})$ for the elements of the affine space $\mathbb{A}^{(n+r)(s+1)}$.

Let $N_0 := n+1+m(2n+2r+1)$, and let $\pi_1 : \mathbb{A}^{(n+r)(s+1)} \times \mathbb{A}^{N_1} \to \mathbb{A}^{(n+r)(s+1)} \times \mathbb{A}^{N_0}$ be the (non-linear) map defined by $\pi_1(\lambda, \eta) = (\lambda, y, w, \Gamma(\lambda, x, \bar{u}), \ldots, \Gamma^{(s)}(\lambda, x, \bar{u}), e)$. Consider the irreducible variety $\mathbb{V}_1 := \mathbb{A}^{(n+r)(s+1)} \times \mathbb{V} \subset \mathbb{A}^{(n+r)(s+1)} \times \mathbb{A}^{N_1}$.

Notice that $\{\Lambda^{[s]}, Y^{[2n+2r-1]}, W^{[2n+2r]}, \Gamma^{[s-1]}, E\}$ is a transcendence basis of $k(\mathbb{V}_1)$ over k. This implies that $\overline{\pi_1(\mathbb{V}_1)}$ is a hypersurface in $\mathbb{A}^{(n+r)(s+1)} \times \mathbb{A}^{N_0}$. On the other hand, it is straightforward to check that a minimal polynomial $M_\Lambda \in k[\Lambda^{[s]}, Y^{[2n+2r-1]}, W^{[2n+2r]}, T^{[s]}]$ as in Proposition 39 vanishes over $\overline{\pi_1(\mathbb{V}_1)}$, and so, $\overline{\pi_1(\mathbb{V}_1)} \subset \{M_\Lambda = 0\}$. We conclude that $\overline{\pi_1(\mathbb{V}_1)} = \{M_\Lambda = 0\}$, both varieties being irreducible hypersurfaces. Therefore, $\deg(M_\Lambda) = \deg(\pi_1(\mathbb{V}_1))$.

In order to estimate $\deg(\pi_1(\mathbb{V}_1))$, we will give an alternative description of $\pi_1(\mathbb{V}_1)$. First, let us observe that $\dim(\mathbb{V}) = N_0 - 1$.

For $i = 1, \ldots, N_0$, let C_i be a set of N_1+1 new variables indexed by $Y^{[2n+2r-1]}$, $W^{[2n+2r]}$, $X^{[2n+2r]}$, $\bar{U}^{[2n+2r]}$ and 0 which stand for the coefficients of a generic affine linear form L_i in these variables (C_{i0} corresponds to the constant term of L_i). Consider the map $\phi : \mathbb{A}^{(N_1+1)N_0} \times \mathbb{V} \to \mathbb{A}^{(N_1+1)N_0} \times \mathbb{A}^{N_0}$ defined by $\phi(c, \eta) = (c, L_1(c_1, \eta), \ldots, L_{N_0}(c_{N_0}, \eta))$, where $c := (c_1, \ldots, c_{N_0})$.

The Zariski closure of $\phi(\mathbb{A}^{(N_1+1)N_0} \times \mathbb{V})$ is a hypersurface in $\mathbb{A}^{(N_1+1)N_0} \times \mathbb{A}^{N_0}$, which is defined by a multihomogeneous polynomial of degree $\deg(\mathbb{V})$ in each group of variables C_i for $i = 1, \ldots, N_0$ (see [23, Section 2.3.1]). Thus, $\deg(\phi(\mathbb{A}^{(N_1+1)N_0} \times \mathbb{V})) = N_0 \deg(\mathbb{V})$.

We will show that the variety $\pi_1(\mathbb{V}_1)$ can be obtained as a linear projection of the intersection of $\phi(\mathbb{A}^{(N_1+1)N_0} \times \mathbb{V})$ with a linear variety.

First, we define a linear variety $\mathbb{L} \subset \mathbb{A}^{(N_1+1)N_0}$ whose points correspond to the coefficient vectors of families of linear forms of type $Y^{[2n+2r-1]}$, $W^{[2n+2r]}$, $\gamma^{[s]}$, E; that is, a point c is in $\mathbb{L}$ if and only if its first coordinates are the coefficient vectors of the linear forms $Y^{[2n+2r-1]}$, $W^{[2n+2r]}$, its last coordinates are the coefficients of the linear forms E, and the remaining ones are the coefficients of $\gamma, \dot{\gamma}, \ldots, \gamma^{(s)}$ for the derivatives $\gamma^{(l)}$ of some linear form as in (6). Set $i_0 := r(2n+2r)+(m-r)(2n+2r+1)$, $i_1 := i_0+s+1$. Identifying $\Lambda^{(l)}$ with $C_{i_0+1+l,\{X,\bar{U}\}}$ for $l = 0, \ldots, s$, the variety $\mathbb{L}$ can be defined by means of the following equations (where $\varepsilon_1, \ldots, \varepsilon_{N_1+1}$ denote the vectors of the canonical basis of k^{N_1+1}):

- For $i = 1, \ldots, i_0$: $C_i = \varepsilon_i$.
- For $i = i_0+1, \ldots, i_1$: $C_{i,Y^{[2n+2r-1]}} = C_{i,W^{[2n+2r]}} = 0$, $C_{i,\{X,\bar{U}\}^{(j)}} = 0$ for $j \geqslant i-i_0$, $C_{i,\{X,\bar{U}\}^{(j)}} = \binom{i-i_0-1}{j} C_{i-j,\{X,\bar{U}\}^{(0)}}$ for $j < i-i_0$ (see identity (6)).
- For $i = i_1+1, \ldots, N_0$: $C_i := \varepsilon_{j_{i-i_1}}$, where ε_{j_k} is the vector of the canonical basis corresponding to the coefficient vector of E_k for $k = 1, \ldots, n+r-s$.

Let $\pi_\Lambda : \mathbb{A}^{(N_1+1)N_0} \times \mathbb{A}^{N_0} \to \mathbb{A}^{(n+r)(s+1)} \times \mathbb{A}^{N_0}$ be the linear projection defined by $\pi_\Lambda(c, b) = (c_{i_0+1,\{X,\bar{U}\}}, \ldots, c_{i_1,\{X,\bar{U}\}}, b)$.

Then, we have the following equality $\pi_\Lambda\left(\phi(\mathbb{A}^{(N_1+1)N_0} \times \mathbb{V}) \cap (\mathbb{L} \times \mathbb{A}^{N_0})\right) = \pi_1(\mathbb{V}_1)$.

Taking into account that the degree of a variety does not increase when intersecting it with an affine linear space [16, Remark 2] or under a linear projection [16, Lemma 2], we conclude that $\deg(M_\Lambda) = \deg(\pi_1(\mathbb{V}_1)) \leqslant \deg(\phi(\mathbb{A}^{(N_1+1)N_0} \times \mathbb{V}) \cap (\mathbb{L} \times \mathbb{A}^{N_0})) \leqslant \deg(\phi(\mathbb{A}^{(N_1+1)N_0} \times \mathbb{V})) = (n + 1 + m(2n + 2r + 1)) \deg(\mathbb{V})$. □

5.4. The resolvent representation

In this subsection we deduce some results concerning the choice of a primitive element of the extension $K \hookrightarrow \mathcal{F}$ (see Section 5.2) and the order and degrees of the polynomials involved in a resolvent representation of the prime differential ideal Δ.

Let $M_\Lambda \in k[\Lambda^{[s]}, Y^{[2n+2r-1]}, W^{[2n+2r]}][T^{[s]}]$ be a minimal (irreducible) polynomial of the *generic* primitive element $\Gamma = \Lambda_1 X_1 + \cdots + \Lambda_n X_n + \Lambda_{n+1}\bar{U}_1 + \cdots + \Lambda_{n+r}\bar{U}_r$ of $K_\Lambda \hookrightarrow \mathcal{F}_\Lambda$ as in Proposition 39. Let us observe that the polynomial $\mathcal{X}$ appearing in the proof of Theorem 29 can be taken as $\mathcal{X}=M_\Lambda$. Since $Q_\Lambda := \frac{\partial M_\Lambda}{\partial T^{(s)}}(\Gamma, \ldots, \Gamma^{(s)})$ is a polynomial in $k[\Lambda^{[s]}, Y^{[2n+2r-1]}, X^{[2n+2r]}, U^{[2n+2r]}]$ which is a non-zero element in $\mathcal{F}_\Lambda$, the proof of Theorem 29 provides a resolvent representation of the ideal $K_\Lambda \otimes \Delta$ by computing the partial derivatives of $M_\Lambda(\Gamma, \ldots, \Gamma^{(s)})$ with respect to $\Lambda_i^{(s)}$ for $i = 1, \ldots, n + r$ (see condition (4) in that proof). In particular, all the polynomials involved in this resolvent representation are elements of $k[\Lambda^{[s]}, Y^{[2n+2r-1]}, W^{[2n+2r]}, T^{[s]}]$ and have degrees bounded by that of M_Λ.

In addition, the proof of that theorem shows that a sufficient condition for an element $\gamma = \lambda_1 X_1 + \cdots + \lambda_n X_n + \lambda_{n+1}\bar{U}_1 + \cdots + \lambda_{n+r}\bar{U}_r$ to be a primitive element of $K \hookrightarrow \mathcal{F}$ is the non-vanishing in $\mathcal{F}$ of the specialization of the differential polynomial $Q_\Lambda \in \mathcal{F}\{\Lambda\}$ at $(\lambda_1, \ldots, \lambda_{n+r})$. As the order of Q_Λ in the variables Λ is bounded by s, the arguments in the proof of [28, Chapter 2, Section 22] imply:

Corollary 42. *Let $\xi \in k \subset K$ be a non-constant element. There exists a primitive element γ of the extension $K \hookrightarrow \mathcal{F}$ of type $\gamma = \lambda_1 X_1 + \cdots + \lambda_n X_n + \lambda_{n+1}\bar{U}_1 + \cdots + \lambda_{n+r}\bar{U}_r$ where $\lambda_i \in \mathbb{Q}[\xi]$ is a polynomial of degree bounded by $s = \mathrm{ord}_K(K \otimes \Delta)$ for $i = 1, \ldots, n + r$.*

Now, let $\lambda := (\lambda_1, \ldots, \lambda_{n+r})$ be an $(n + r)$-tuple with $Q_\Lambda(\lambda) \neq 0$ in $\mathcal{F}$. Then, by considering a minimal polynomial M of $\gamma := \Gamma(\lambda)$ as in Proposition 35 and specializing the differential variables Λ into λ in the polynomials $Q := \frac{\partial M_\Lambda}{\partial T^{(s)}}(T, \ldots, T^{(s)}) \in K\{\Lambda, T\}$ and $P_i := -\frac{\partial M_\Lambda}{\partial \Lambda_i^{(s)}}(T, \ldots, T^{(s)}) \in K\{\Lambda, T\}$ appearing in the generic resolvent representation, we obtain a resolvent representation of the ideal Δ with respect to the transcendence basis Y, W and the primitive element γ. We conclude:

Theorem 43. *There is a resolvent representation $\{M, q\,X_1 - p_1, \ldots, q\,X_n - p_n, q\,\bar{U}_1 - p_{n+1}, \ldots, q\,\bar{U}_r - p_{n+r}\}$ of the prime differential ideal Δ with respect to the transcendence basis Y, W and a primitive element $\gamma = \lambda_1 X_1 + \cdots + \lambda_n X_n + \lambda_{n+1}\bar{U}_1 + \cdots + \lambda_{n+r}\bar{U}_r$ of the differential field extension $k\langle Y, W\rangle \hookrightarrow \mathcal{F}$ satisfying: $M, q, p_i \in k[Y^{[2n+2r-1]}, W^{[2n+2r]}, T^{[s]}]$ for $i = 1, \ldots, n + r$ and their total degrees are bounded by* $\deg(\mathbb{V})$.

6. Algorithmic computation of a resolvent representation

The main goal of this section is the computation of a resolvent representation of the differential ideal Δ associated to system (1) (see Notation 5).

As in Section 4.3, we will consider the ground differential field k to be the rational effective field $\mathbb{Q}(t)$ (with the standard derivation). Furthermore, in order to make the presentation of our algorithm simpler, we will assume that the polynomials defining system (1) have coefficients in $\mathbb{Q}$. This assumption is not restrictive, since we may replace our original system over $\mathbb{Q}[t]$ by an equivalent one over $\mathbb{Q}$ by adding a new differential variable t and the equation $\dot{t} = 1$.

In the previous section we proved that the minimal polynomial of a primitive element can be seen as an eliminating polynomial of a suitable linear projection in the classical algebraic geometry context. Now, we will apply some well-known algorithmic techniques from computer algebra (mainly from [17,31]) to the computation of this polynomial.

6.1. Computing the generic minimal polynomial

As in Section 5.2, fix a differential transcendence basis $W \subset U$ of the field extension $\mathbb{Q}(t)\langle Y\rangle \hookrightarrow \mathcal{F}$ (see Notation 11), and consider the differentially algebraic field extension $\mathbb{Q}(t)\langle Y, W\rangle \hookrightarrow \mathcal{F}$. This transcendence basis W can be obtained by applying the algorithm underlying Theorem 27. Denote $\bar{U} := U \setminus W$ and $K := \mathbb{Q}(t)\langle Y, W\rangle$. We introduce a new set $\Lambda := \{\Lambda_1, \ldots, \Lambda_{n+r}\}$ of differential indeterminates over K and set $k_\Lambda := \mathbb{Q}(t)\langle\Lambda\rangle$, $\Delta_\Lambda := [F, G] \subset k_\Lambda\{Y, X, U\}$, $K_\Lambda := k_\Lambda\langle Y, W\rangle$ and $\mathcal{F}_\Lambda := \mathcal{F}\langle\Lambda\rangle$.

This subsection focuses on the computation of the minimal polynomial M_Λ of the generic primitive element $\Gamma := \Lambda_1 X_1 + \cdots + \Lambda_n X_n + \Lambda_{n+1}\bar{U}_1 + \cdots + \Lambda_{n+r}\bar{U}_r$ in $K_\Lambda \hookrightarrow \mathcal{F}_\Lambda$ satisfying the degree upper bound stated in Theorem 41.

First, we compute $s := \mathrm{ord}_K(K \otimes \Delta)$. We point out that, for an arbitrary differential transcendence basis W, $\mathrm{ord}_{\mathbb{Q}(t)\langle Y, W\rangle}(\mathbb{Q}(t)\langle Y, W\rangle \otimes \Delta) \leqslant \mathrm{ord}_{\mathbb{Q}(t)\langle Y\rangle}(\mathbb{Q}(t)\langle Y\rangle \otimes \Delta)$, and the equality may not hold. The computation of s can be made using the same techniques as those applied in Section 4 for the computation of the Hilbert function of $\mathbb{Q}(t)\langle Y\rangle \otimes \Delta$ over $\mathbb{Q}(t)\langle Y\rangle$: taking into account that $\mathrm{diffdim}(K \otimes \Delta) = 0$, we deduce from Proposition 2 that $s = \mathcal{H}_{K\otimes\Delta, K}(n + r)$. In order to compute this Hilbert function value we apply the following analogue of Lemma 14 that holds in our new framework with a similar proof: for every $i \geqslant 0$, we have $(K \otimes \Delta) \cap (K \otimes A_i) = (K \otimes \Delta_{i+n+r}) \cap (K \otimes A_i)$.

Arguing as in the proofs of Proposition 16 and Corollary 22, we obtain:

Proposition 44. *Let* $J^W_{n+r} := \frac{\partial\{F,G\}^{[n+r,\,2n+2r-1]}}{\partial\{X,\,U\setminus W\}^{[n+r+1,\,2n+2r]}}$ *(see Notation* 15*). Then, the following identity holds*: $\mathcal{H}_{K\otimes\Delta,\,K}(n + r) = \mathrm{rank}(J^W_{n+r}) - (n + r)(n + r - 1)$, *where the rank is taken over the polynomial ring* $\mathbb{Q}[t, X, U^{[2n+2r]}]$.

Let $E \subset \{X, U^{[2n+2r]}\}$ be a set with $n + r - s$ elements such that $\{Y^{[2n+2r-1]}, W^{[2n+2r]}, \Gamma^{[s-1]}, E\}$ is a transcendence basis of the field $\mathrm{Frac}(k_\Lambda \otimes A_{2n+2r}/(\Delta_\Lambda)_{2n+2r})$ over k_Λ. As in Notation 34, let $N_1 = r(2n + 2r) + (n + m)(2n + 2r + 1)$. Let us consider the variety $\mathcal{V} \subset \mathbb{A}^{(n+r)(s+1)} \times \mathbb{A}^{N_1} \times \mathbb{A}^s$ defined as

$$\begin{aligned}\mathcal{V} := \{(\lambda, y, w, x, \bar{u}, \tau) \in \mathbb{A}^{(n+r)(s+1)} \times \mathbb{A}^{N_1} \times \mathbb{A}^s : F^{[2n+2r-1]}(w, x, \bar{u}) = 0,\\ G^{[2n+2r-1]}(y, w, x, \bar{u}) = 0, \Gamma(\lambda, x, \bar{u}) = \tau_0, \ldots, \Gamma^{(s-1)}(\lambda, x, \bar{u}) = \tau_{s-1}\},\end{aligned}$$

which is irreducible of dimension $\mu := (n + r)(s + 1) + m(2n + 2r + 1) + n$. We have the ring inclusion $\mathbb{Q}\big[\Lambda^{[s]}, Y^{[2n+2r-1]}, W^{[2n+2r]}, E, T^{[s-1]}\big] \hookrightarrow \mathbb{Q}[\mathcal{V}]$ and that the cardinality of the

family $\Lambda^{[s]}, Y^{[2n+2r-1]}, W^{[2n+2r]}, E, T^{[s-1]}$ is μ. Thus, the linear projection $\pi : \mathcal{V} \to \mathbb{A}^{\mu}$ defined by $\pi(\lambda, y, w, x, \bar{u}, \tau) = (\lambda, y, w, e, \tau)$ is a dominant map with generically finite fibers.

Let $\varphi : \mathcal{V} \to \mathbb{A}^{\mu} \times \mathbb{A}^1$ be defined by $\varphi(\lambda, y, w, x, \bar{u}, \tau) = (\pi(\lambda, y, w, x, \bar{u}, \tau), \Gamma^{(s)}(\lambda, x, \bar{u}))$. Then, the Zariski closure $\overline{\varphi(\mathcal{V})}$ is a hypersurface and any square-free polynomial defining $\overline{\varphi(\mathcal{V})}$ is a minimal polynomial for the generic primitive element Γ.

We will consider the polynomial equation system defining $\mathcal{V}$ as a *parametric* system, where the parameters are $P := (\Lambda^{[s]}, Y^{[2n+2r-1]}, W^{[2n+2r]}, E, T^{[s-1]})$ and the variables—the set of which will be denoted Z in the sequel—are those variables in $X^{[2n+2r]}, \bar{U}^{[2n+2r]}$ that are not in the set of variables E. Thus, we obtain a polynomial system with $2(n+r)^2+s$ equations in $2(n+r)^2+s$ unknowns defining a zero-dimensional variety $\mathcal{V}_{\mathcal{K}}$ over the algebraic closure $\overline{\mathcal{K}}$ of $\mathcal{K} := \mathbb{Q}(P)$. Let us observe that the ideals $\mathcal{I} := (F^{[2n+2r-1]}, G^{[2n+2r-1]}, \Gamma - T, \ldots, \Gamma^{(s-1)} - T^{(s-1)}) \subset \mathbb{Q}[P, Z]$ and $\mathcal{I}_{\mathcal{K}} := \mathcal{K} \otimes \mathcal{I} \subset \mathcal{K}[Z]$ are the (prime) ideals of the varieties $\mathcal{V}$ and $\mathcal{V}_{\mathcal{K}}$, respectively.

The following result relates the minimal polynomial M_{Λ} we want to compute to the minimal polynomial of a $\mathcal{K}$-linear map.

Lemma 45. *Let $m_{\Gamma^{(s)}} : \mathcal{K}[Z]/\mathcal{I}_{\mathcal{K}} \to \mathcal{K}[Z]/\mathcal{I}_{\mathcal{K}}$ be the $\mathcal{K}$-linear map defined as $m_{\Gamma^{(s)}}(f) = \Gamma^{(s)} \cdot f$ and let $M_0 \in \mathcal{K}[T^{(s)}]$ be its minimal polynomial. Then, there exists $Q_0 \in \mathbb{Q}[P] - \{0\}$ such that $M_{\Lambda} = Q_0 \cdot M_0$.*

Proof. First, let us observe that $M_{\Lambda}(\Gamma^{(s)}) \in \mathcal{I}$ and so, $M_{\Lambda}(\Gamma^{(s)}) \in \mathcal{I}_{\mathcal{K}}$. Therefore, M_0 divides M_{Λ} in $\mathbb{Q}(P)[T^{(s)}]$. On the other hand, since $M_0(\Gamma^{(s)}) \in \mathcal{I}_{\mathcal{K}}$, there exists $Q \in \mathbb{Q}[P] - \{0\}$ with $Q \cdot M_0(\Gamma^{(s)}) \in \mathcal{I}$. Then, the fact that M_{Λ} is the polynomial with minimal degree in $\mathbb{Q}[P, T^{(s)}]$ satisfying $M_{\Lambda}(\Gamma^{(s)}) \in \mathcal{I}$ implies that M_{Λ} divides $Q \cdot M_0$ in $\mathbb{Q}[P, T^{(s)}]$. The lemma follows now from the irreducibility of M_{Λ} and the fact that M_0 is a monic polynomial. □

Since $\mathcal{I}_{\mathcal{K}}$ is a zero-dimensional prime ideal of $\mathcal{K}[Z]$, its extension $\mathcal{I}_{\overline{\mathcal{K}}}$ to $\overline{\mathcal{K}}[Z]$ is a zero-dimensional radical ideal. Then, the linear map $m_{\Gamma^{(s)}} : \overline{\mathcal{K}}[Z]/\mathcal{I}_{\overline{\mathcal{K}}} \to \overline{\mathcal{K}}[Z]/\mathcal{I}_{\overline{\mathcal{K}}}$ is diagonalizable and its characteristic polynomial is $\mathcal{X} := \prod_{i=1}^{D}(T^{(s)} - \Gamma^{(s)}(\mathcal{R}_i)) \in \mathcal{K}[T^{(s)}]$, where $D := \deg(\mathcal{V}_{\mathcal{K}})$ and $\mathcal{R}_1, \ldots, \mathcal{R}_D \in \overline{\mathcal{K}}^{2(n+r)^2+s}$ denote the points in $\mathcal{V}_{\mathcal{K}}$. Therefore, the minimal polynomial M_0 of $m_{\Gamma^{(s)}}$ can be obtained as the square-free part of $\mathcal{X}$.

Our algorithm for the computation of the polynomial M_{Λ} is based on an extension of the results in [17] (which hold for a *finite* morphism) to the case of a *dominant* map, which is achieved by using the techniques described in [31].

Proposition 46. *With the same notation as before, assume that $f_1, \ldots, f_n \in \mathbb{Q}[X, U]$, $g_1, \ldots, g_r \in \mathbb{Q}[X, U, \dot{U}]$ have degrees bounded by d and are encoded by an slp of length L. Then, there is a probabilistic algorithm which computes the minimal polynomial of the generic primitive element Γ in $K_{\Lambda} \hookrightarrow \mathcal{F}_{\Lambda}$ with error probability bounded by ε, with $0 < \varepsilon < 1$, within complexity $O(\log(1/\varepsilon)(n+r)^{20}(n+m)^6 d^2 \deg(\mathbb{V})^{10} L)$, where $\mathbb{V}$ is the algebraic variety introduced in Notation* 34.

Proof. First, we present a sketch of the algorithm:

(1) Take a point $p \in \mathbb{Q}^{\mu}$ at random and compute a geometric resolution of $\pi^{-1}(p)$, that is, a family of $2(n+r)^2+s+1$ univariate polynomials $q, v_1, \ldots, v_{2(n+r)^2+s}$ with coefficients in $\mathbb{Q}(P)$ such that $\pi^{-1}(p) = \{p\} \times \{(v_1(\zeta), \ldots, v_{2(n+r)^2+s}(\zeta)),\ q(\zeta) = 0\}$.

(2) Applying a symbolic version of Newton's algorithm to the geometric resolution, compute a polynomial $\mathcal{X}_\kappa \in \mathbb{Q}(P)[T^{(s)}]$ whose coefficients approximate the coefficients of the polynomial $\mathcal{X}$ as power series in $\bar{\mathbb{Q}}[[P-p]]$ with prescribed precision 2^κ for a suitably chosen $\kappa \in \mathbb{N}$.
(3) Compute a polynomial $\Upsilon_\kappa \in \mathbb{Q}(P)[T^{(s)}]$ whose coefficients approximate the coefficients of the square-free polynomial $\mathrm{red}(\mathcal{X}) := \frac{\mathcal{X}}{\gcd(\mathcal{X},\, \partial\mathcal{X}/\partial T^{(s)})} \in \mathbb{Q}(P)[T^{(s)}]$ with precision 2^κ in $\mathbb{Q}[[P-p]]$.
(4) By means of a Padé approximation type procedure, compute relatively prime polynomials Π_1 and Π_2 in $\mathbb{Q}[P, T^{(s)}]$ such that $\mathrm{red}(\mathcal{X}) = \Pi_1/\Pi_2$. The minimal polynomial $M_\Lambda \in \mathbb{Q}[P, T^{(s)}]$ is the numerator Π_1.

Now, we detail the procedures underlying each of the above mentioned steps of the algorithm, compute their complexities and estimate their error probability.

The first step of the algorithm consists in the computation of a geometric resolution of a fiber $\pi^{-1}(p)$ for a randomly chosen point $p \in \mathbb{Q}^\mu$. This point is chosen at random so that with high probability the fiber $\pi^{-1}(p)$ is zero-dimensional and unramified. In order to compute the geometric resolution of $\pi^{-1}(p)$, we apply the procedure for the resolution of zero-dimensional systems described in [18], which takes a reduced regular sequence as input (alternatively, this first step could be achieved by means of *any* algorithm solving zero-dimensional algebraic systems). We will also need the following technical assumption on the point p: $\#\{\Gamma^{(s)}(\eta) : \eta \in \pi^{-1}(p)\} = \#\{\Gamma^{(s)}(\mathcal{R}) : \mathcal{R} \in \mathcal{V}_\mathcal{K}\}$ (or, equivalently, the polynomial $M_\Lambda(p)$ is square-free). Both these conditions also hold for a generic $p \in \mathbb{A}^\mu$. Moreover, there is a non-zero polynomial $H_0 \in \mathbb{Q}[P]$ of degree bounded by $6d^{4(n+r)^2+2s}$ such that all the previous conditions hold for any point $p \in \mathbb{A}^\mu$ with $H_0(p) \neq 0$ (see [31, Section 3.4]). Thus, if we choose the coordinates of p at random in a set of cardinality $12\, d^{4(n+r)^2+2s}[1/\varepsilon]$, the conditions hold with error probability bounded by $\varepsilon/2$. These random choices can be made within complexity $O((n+r)^2 \log(d) + \log(1/\varepsilon))$.

Recall that the polynomials $F^{[2n+2r-1]}$, $G^{[2n+2r-1]}$ can be encoded by slp's of length $O((n+r)^3(n+m)L)$ (see Lemma 21). Assume that the randomly chosen point $p \in \mathbb{A}^\mu$ satisfies all the genericity conditions stated above. Then, if δ is the maximum of the degrees of the varieties successively defined by the equations of $\pi^{-1}(p)$, a geometric resolution of $\pi^{-1}(p)$ can be computed with error probability bounded by $\varepsilon/4$ within complexity $O(\log(1/\varepsilon)(n+m)(n+r)^{10} d\, \delta^4 L)$ (see [18, Theorem 1]). Let us observe that δ is bounded by the maximum of the degrees of the varieties successively defined by the ideals $\mathfrak{p}_{i,s}$, $\mathfrak{q}_{i,l}$ for $1 \leqslant i \leqslant 2n+2r$, $1 \leqslant s \leqslant n$, $1 \leqslant l \leqslant r$, introduced in Remark 7. It is easy to see that the degrees of these varieties form a non-decreasing sequence and so, their maximum is the degree of the last variety. Therefore, $\delta \leqslant \deg(\mathbb{V})$, and the complexity of step (1) can be estimated as $O(\log(1/\varepsilon)(n+m)(n+r)^{10} d\, \deg(\mathbb{V})^4 L)$.

Denote $q, v_1, \ldots, v_{2(n+r)^2+s} \in \mathbb{Q}[T]$ the polynomials appearing in the geometric resolution of $\pi^{-1}(p)$. Let $S := (F^{[2n+2r-1]}, G^{[2n+2r-1]}, \Gamma - T^{(0)}, \ldots, \Gamma^{(s-1)} - T^{(s-1)})$ be the polynomial system defining $\mathcal{V}$. Let $DS(Z)$ be the Jacobian matrix of S with respect to the variables Z and let J_S be its Jacobian determinant.

Our assumptions on $p \in \mathbb{A}^\mu$ state that the fiber $\pi^{-1}(p)$ is a zero-dimensional variety with exactly $D = \deg(\mathcal{V}_\mathcal{K})$ points and that, for every $\eta \in \pi^{-1}(p)$, we have $J_S(p, \eta) \neq 0$. Then, by the implicit function theorem (see, for instance, [17, Lemma 3] for a proof in this context), for every $\eta \in \pi^{-1}(p)$ there exists $\mathcal{R}_\eta \in \bar{\mathbb{Q}}[[P-p]]^{2(n+r)^2+s}$ such that $\mathcal{R}_\eta \in \mathcal{V}_\mathcal{K}$ and $\mathcal{R}_\eta(p) = \eta$. This implies that $\{\mathcal{R}_\eta : \eta \in \pi^{-1}(p)\} = \mathcal{V}_\mathcal{K}$, since both sets have the same cardinality. Moreover, the proof of [17, Lemma 3] shows that, for every $\eta \in \pi^{-1}(p)$, the corresponding point $\mathcal{R}_\eta \in$

$\bar{\mathbb{Q}}[[P-p]]^{2(n+r)^2+s}$ can be 'approximated' by applying successively to η the Newton operator associated to the system S, defined as $N_S(Z)^t := Z^t - DS(Z)^{-1}S(Z)^t$.

If N_S^κ denotes the κth iteration of N_S and $(P-p)$ is the maximal ideal of $\bar{\mathbb{Q}}[[P-p]]$, we have that $N_S^\kappa(\eta) \in \bar{\mathbb{Q}}[[P-p]]^{2(n+r)^2+s}$ and $(\mathcal{R}_\eta)_i - (N_S^\kappa(\eta))_i \in (P-p)^{2^\kappa}$ for $i = 1, \ldots, 2(n+r)^2+s$, that is, the ith coordinate of $N_S^\kappa(\eta)$ approximates with precision 2^κ the ith coordinate of $\mathcal{R}_\eta$ in the sense that their power series expansions coincide up to degree $2^\kappa - 1$. We conclude that the coefficients of the polynomial $\prod_{\eta\in\pi^{-1}(p)}(T^{(s)} - \Gamma^{(s)}(N_S^\kappa(\eta)))$ approximate the coefficients of $\mathcal{X}$ with precision 2^κ.

From the algorithmic viewpoint, we cannot apply Newton's operator to the points $\eta \in \pi^{-1}(p)$, since we cannot compute these points. However, we can obtain all the approximations 'simultaneously' in order to compute an approximation $\mathcal{X}_\kappa$ of the characteristic polynomial $\mathcal{X}$ by applying it to a geometric resolution of the fiber $\pi^{-1}(p)$.

Let $h_0, h_1, \ldots, h_{2(n+r)^2+s} \in \mathbb{Q}[P, Z]$ be polynomials with $N_S^\kappa = \left(\frac{h_1}{h_0}, \ldots, \frac{h_{2(n+r)^2+s}}{h_0}\right)$ and $h_0(p, \eta) \neq 0$ for every $\eta \in \pi^{-1}(p)$. Let $v := (v_1, \ldots, v_{2(n+r)^2+s})$ and let C_q be the companion matrix of the polynomial q. Then, the matrix $h_0(P, v(C_q))$ is invertible and, if $\mathcal{N}_i := h_0(P, v(C_q))^{-1}h_i(P, v(C_q))$ for $i = 1, \ldots, 2(n+r)^2 + s$, the characteristic polynomial of $\Gamma^{(s)}(P, \mathcal{N}_1, \ldots, \mathcal{N}_{2(n+r)^2+s})$ equals $\prod_{\eta\in\pi^{-1}(p)}(T^{(s)} - \Gamma^{(s)}(N_S^\kappa(\eta)))$ (see [17, Lemma 6]). In order to approximate this polynomial we first obtain straight-line programs of length $O(\kappa d^2(n+r)^{17}(n+m)L)$ for the polynomials $h_0, h_1, \ldots, h_{2(n+r)^2+s}$ by means of the procedure underlying [12, Lemma 30] and then we proceed as in [17, Proof of Theorem 2] to obtain a matrix whose entries approximate those of $\Gamma^{(s)}(P, \mathcal{N}_1, \ldots, \mathcal{N}_{2(n+r)^2+s})$ with the desired precision, but avoiding matrix inverse computations. Finally, we compute the characteristic polynomial $\mathcal{X}_\kappa$ of this matrix, whose coefficients approximate the coefficients of $\mathcal{X}$ in $\mathbb{Q}[[P-p]]$ with precision 2^κ. The overall complexity of this step is $O(\kappa 2^\kappa d^2(n+r)^{17}(n+m)D^4L)$, which is also the length of the slp obtained for the coefficients of the polynomial $\mathcal{X}_\kappa$.

Now, we describe the procedure to achieve the third step of our algorithm. The hypothesis $\#\{\Gamma^{(s)}(\eta) : \eta \in \pi^{-1}(p)\} = \#\{\Gamma^{(s)}(\mathcal{R}) : \mathcal{R} \in \mathcal{V}_\mathcal{K}\}$ ensures that, considering $\mathcal{X}$ and $\frac{\partial\mathcal{X}}{\partial T^{(s)}}$ as polynomials in the variable $T^{(s)}$, $\deg(\gcd(\mathcal{X}, \frac{\partial\mathcal{X}}{\partial T^{(s)}})) = \deg(\gcd(\mathcal{X}(p), \frac{\partial\mathcal{X}(p)}{\partial T^{(s)}}))$. Thus, we can obtain this degree by computing the characteristic polynomial of $\Gamma^{(s)}$ with respect to $\pi^{-1}(p)$ from the geometric resolution of $\pi^{-1}(p)$ and subresultants of $\mathcal{X}(p)$ and $\frac{\partial\mathcal{X}(p)}{\partial T^{(s)}}$ within complexity $O(D^5)$ (see, for instance, [1, Section 8.3]). By [1, Corollary 10.14], once this degree is known, the coefficients of a scalar multiple Υ of $\mathrm{red}(\mathcal{X})$ can be obtained by computing determinants of square submatrices of the Sylvester matrix of $\mathcal{X}$ and $\mathcal{X}'$, and, making the same computations with the Sylvester matrix of $\mathcal{X}(p)$, the polynomial $\Upsilon(p)$ is obtained. Since Υ and $\Upsilon(p)$ have the same degree, we conclude that the scalar factor is an invertible element of $\mathbb{Q}[[P-p]]$. Note that the previous procedure involves only polynomial computations in the coefficients of $\mathcal{X}$. Then, we apply it to the polynomial $\mathcal{X}_\kappa$ instead of $\mathcal{X}$ to obtain a polynomial Υ_κ whose coefficients approximate the coefficients of Υ with precision 2^κ. The complexity of this computation does not increase the order of the complexity of the previous steps.

In order to compute the polynomials Π_1 and Π_2 of step (4), we apply a slightly modified version of the multivariate Padé approximation procedure described in [31, Section 4.3.1], adapted to deal with the straight-line program encoding of polynomials. In fact, our main change consists in replacing the Euclidean extended algorithm with subresultant computations (see [11, Section 5.9, Corollary 6.49]). Note that the upper bound on the degree of the polynomial M_Λ proved

in Theorem 41 implies that the total degrees of the polynomials Π_1 and Π_2 are bounded by $(n+1+m(2n+2r+1))\deg(\mathbb{V})$. Therefore, they can be computed from the Taylor expansion centered at $P=p$, $T^{(s)}=0$ of $\mathrm{red}(\mathcal{X})$ up to degree $2(n+1+m(2n+2r+1))\deg(\mathbb{V})$, which can be obtained from the corresponding Taylor expansion of Υ_κ divided by its leading coefficient provided that $\kappa \geqslant \lceil \log(2(n+1+m(2n+2r+1))\deg(\mathbb{V}))\rceil + 1$. Then, the input for the Padé approximation procedure is the set of graded parts up to the required degree of Υ_κ divided by its leading coefficient, which is computed within complexity $O((n+r)^{20}(n+m)^4 d^2 \deg(\mathbb{V})^2 D^4 L)$.

The complexity of the entire step (4) is $O(\log(1/\varepsilon)(n+r)^{20}(n+m)^6 d^2 \deg(\mathbb{V})^6 D^4 L)$ and its output is an slp of length $O((n+r)^{20}(n+m)^6 d^2 \deg(\mathbb{V})^6 D^4 L)$ encoding Π_1 and Π_2 with error probability bounded by $\varepsilon/2$ provided that the previous computations are correct.

The announced complexity bound for the whole procedure follows by adding up the complexities of steps (1) to (4) and taking into account that $D \leqslant \deg(\mathbb{V})$. □

6.2. *Computation of a primitive element*

In what follows we show how to compute a primitive element of the differential field extension induced by system (1) with respect to a fixed differential transcendence basis within complexity polynomial in $n, m, r, d, \deg(\mathbb{V})$ and linear in L. The procedure follows closely the arguments in Section 5.4. We keep our previous assumptions and notations.

Let $M_\Lambda \in \mathbb{Q}[\Lambda^{[s]}, Y^{[2n+2r-1]}, W^{[2n+2r]}, T^{[s]}]$ be the minimal polynomial of the generic linear form $\Gamma = \Lambda_1 X_1 + \cdots + \Lambda_n X_n + \Lambda_{n+1}\bar{U}_1 + \cdots + \Lambda_{n+r}\bar{U}_r$ in the differential field extension $K_\Lambda \hookrightarrow \mathcal{F}_\Lambda$, and let $Q_\Lambda := \frac{\partial M_\Lambda}{\partial T^{(s)}}(\Gamma, \ldots, \Gamma^{(s)}) \in \mathbb{Q}[\Lambda^{[s]}, Y^{[2n+2r-1]}, X^{[2n+2r]}, U^{[2n+2r]}]$. As explained in Section 5.4, in order for a linear form $\gamma = \lambda_1 X_1 + \cdots + \lambda_n X_n + \lambda_{n+1}\bar{U}_1 + \cdots + \lambda_{n+r}\bar{U}_r$ to be a primitive element, it suffices that $Q_\Lambda(\lambda_1, \ldots, \lambda_{n+r}) \neq 0$ in $\mathcal{F}$. Furthermore, for every $1 \leqslant i \leqslant n+r$, λ_i can be chosen to be a polynomial in $\mathbb{Q}[t]$ of degree bounded by s.

For $i = 1, \ldots, n+r$, let A_{ij} $(0 \leqslant j \leqslant s)$ be new indeterminates which stand for the coefficients of a generic polynomial $\sum_{j=0}^{s} \frac{A_{ij}}{j!} t^j$ of degree s. Set $A := \{A_{ij} : 1 \leqslant i \leqslant n+r,\ 0 \leqslant j \leqslant s\}$. If we substitute the variables Λ_i $(1 \leqslant i \leqslant n+r)$ in the polynomial Q_Λ by these generic polynomials, we obtain a new polynomial $Q_0 \in \mathbb{Q}[t, A][Y^{[2n+2r-1]}, X^{[2n+2r]}, U^{[2n+2r]}]$ with the property that, for any specialization of the variables A in a set of rational numbers $a := (a_{ij})$ with $Q_0(a) \neq 0$ in $\mathcal{F}$, the polynomials $\lambda_i := \sum_{j=0}^{s} \frac{a_{ij}}{j!} t^j$ are the coefficients of a primitive element of the field extension $K \hookrightarrow \mathcal{F}$.

Let us observe that substituting $t = 0$ in Q_0 has the same effect as renaming $\Lambda_i^{(j)} = A_{ij}$ in Q_Λ. This implies that any family of rational numbers a with $Q_\Lambda(a) \neq 0$ in $\mathcal{F}$ yields a primitive element of the extension $K \hookrightarrow \mathcal{F}$. The procedure to test the non-vanishing of Q_Λ in $\mathcal{F}$ relies on the isomorphism $\mathcal{F} \simeq \mathbb{Q}(t)(X, U^{[2n+2r]})$: we substitute $X_h^{(l)} = \tilde{f}_h^{(l-1)}$ $(1 \leqslant h \leqslant n,\ 1 \leqslant l \leqslant 2n+2r)$ and $Y_j^{(k)} = \tilde{g}_j^{(k)}$ $(1 \leqslant j \leqslant r,\ 0 \leqslant k \leqslant 2n+2r-1)$ in the polynomial Q_Λ to obtain a new polynomial $\widetilde{Q}_\Lambda$ (see Notation 6), and we look for a tuple $(a, x, u^{[2n+2r]})$ of rational numbers that does not annihilate $\widetilde{Q}_\Lambda$ (this is done probabilistically by choosing their coordinates at random). The vector a of the first coordinates of this tuple yields the desired primitive element.

Assuming that the polynomial M_Λ is given, we obtain the following complexity result:

Proposition 47. *Assume that a differential transcendence basis W of the differential field extension induced by system* (1) *is fixed and that the minimal polynomial M_Λ with respect to W of the generic primitive element Γ is given by an slp of length $\mathcal{L}$. Then, we can compute a primitive*

element of the differential field extension $\mathbb{Q}(t)\langle Y, W\rangle \hookrightarrow \mathcal{F}$, *with error probability bounded by* ε, *within complexity* $O(\mathcal{L} + \log(\deg(\mathbb{V})/\varepsilon)(n+r)^4(n+m)L)$, *where* L *is the length of an slp encoding* $f_1, \ldots, f_n, g_1, \ldots, g_r$.

Taking into account the complexity estimate for the computation of M_Λ stated in Proposition 46, we can obtain complexity bounds for the probabilistic computation of a primitive element of the differential extension (see Theorem 48).

6.3. Computing a resolvent representation of the system

As it was shown in Proposition 47, a primitive element γ of the differential extension $\mathbb{Q}(t)\langle Y, W\rangle \hookrightarrow \mathcal{F}$ can be computed algorithmically. Let us observe that specializing the generic minimal polynomial M_Λ into the coefficients $\lambda_1, \ldots, \lambda_{n+r} \in \mathbb{Q}[t]$ of γ, we obtain a differential polynomial $M_\lambda \in \mathbb{Q}[t][Y^{[2n+2r-1]}, W^{[2n+2r]}, T^{[s]}]$ such that $M_\lambda(\gamma) = 0$ in $\mathcal{F}$ but, unfortunately, this polynomial need not be the minimal polynomial of γ.

However, the arguments in Section 5.4 give an algorithmic procedure, based on the computation of derivatives of M_Λ and specialization, to compute polynomials $q, p_1, \ldots, p_{n+r}$ in $\mathbb{Q}[t][Y^{[2n+2r-1]}, W^{[2n+2r]}, T^{[s]}]$ such that $q(\gamma)X_i - p_i(\gamma) \in \Delta$ for $i = 1, \ldots, n$ and $q(\gamma)\bar{U}_j - p_{n+j}(\gamma) \in \Delta$ for $j = 1, \ldots, r$.

Therefore, in order to obtain a resolvent representation of the ideal Δ with respect to the differential transcendence basis Y, W and the primitive element γ, only a minimal polynomial of γ remains to be computed. This can be achieved using the algorithm described in the previous subsections for the computation of the minimal polynomial of a generic primitive element within the same complexity.

Combining this procedure with Theorem 27 and Propositions 46 and 47, we deduce our main result:

Theorem 48. *Let* $f_1, \ldots, f_n \in \mathbb{Q}[t][X, U]$, $g_1, \ldots, g_r \in \mathbb{Q}[t][X, U, \dot{U}]$ *polynomials with degrees bounded by* d *and encoded by an slp of length* L. *Let* Δ *be the differential ideal associated with system* (1) *and let* $\mathbb{V}$ *be the algebraic variety defined by* Δ_{2n+2r} *introduced in Notation* 34. *Then, there is a probabilistic algorithm which computes*

- *a differential transcendence basis* W *of* $\mathbb{Q}(t)\langle Y\rangle \hookrightarrow \mathrm{Frac}(\mathbb{Q}(t)\{Y, X, U\}/\Delta)$,
- *a primitive element* γ *of* $\mathbb{Q}(t)\langle Y, W\rangle \hookrightarrow \mathrm{Frac}(\mathbb{Q}(t)\{Y, X, U\}/\Delta)$,
- *a resolvent representation of the differential ideal* Δ *with respect to the differential transcendence basis* Y, W *and the primitive element* γ,

with error probability bounded by ε, $0 < \varepsilon < 1$, *within complexity* $O(\log(1/\varepsilon)(n+r)^{20}(n+m)^6 d^2 \deg(\mathbb{V})^{10} L)$. *In particular, the complexity of the algorithm can be estimated as* $((n+r)(n+m)d^{(n+r)^2})^{O(1)} \log(1/\varepsilon)L$.

We point out that our complexity upper bound in terms of a geometric invariant (namely, $\deg(\mathbb{V})$) is more accurate than the one that can be stated using only syntactic parameters, as illustrated by the system considered in Example 38. In this case, $\deg(\mathbb{V}) = 2n + 1$; leading to a polynomial complexity bound for our algorithm. However, the upper bound 2^{2n^2} for this parameter would imply a single exponential complexity bound.

7. Over-determined differential systems

In the previous sections, we focused on the computation of a resolvent representation of the generic differential system (1) under Assumption 4 on the differential algebraic independence of the polynomials $g_1, \ldots, g_r$, which played a crucial role in our arguments. Now, we will drop that assumption. More precisely, we will consider a differential system of the form

$$\begin{cases} \dot{X}_1 = f_1(X, U) \\ \quad \vdots \\ \dot{X}_n = f_n(X, U) \\ Y_1 = g_1(X, U, \dot{U}) \\ \quad \vdots \\ Y_\rho = g_\rho(X, U, \dot{U}) \end{cases} \tag{7}$$

where $f_1, \ldots, f_n \in k[X, U]$ and $g_1, \ldots g_\rho \in k[X, U, \dot{U}]$ are arbitrary polynomials in the variables $X := \{X_1, \ldots, X_n\}$ and $U := \{U_1, \ldots, U_m\}$.

Our aim is to compute an alternative (resolvent-like) representation of system (7). In order to do this, we will modify the system so that the condition in Assumption 4 is met and compute a resolvent representation of the modified system together with a family of additional polynomials giving further information on the original system.

Since most of the proofs in this section are similar to those of the results we have presented so far, we will not give the details, but we will outline the main ideas involved.

7.1. Independent equations

Keeping our previous notation (see Section 3), let $F_i := f_i - \dot{X}_i \in k[X, \dot{X}, U]$ for $i = 1, \ldots, n$, and $G_j := g_j - Y_j \in k[Y, X, U, \dot{U}]$ for $j = 1, \ldots, \rho$.

Let $\Omega \subset k\{Y, X, U\}$ be the differential ideal $[F_1, \ldots, F_n, G_1, \ldots, G_\rho]$. For every $l \in \mathbb{N}$, let $A_l := k[Y^{[l-1]}, X^{[l]}, U^{[l]}]$ and $\Omega_l := (F^{[l-1]}, G^{[l-1]}) \subset A_l$.

The following analogues of Remark 7, Proposition 12 and Remark 13 hold in this context:

Remark 49. For every $l \in \mathbb{N}$, the ideal $\Omega_l \subset A_l$ is prime and $A_l/\Omega_l \simeq k[X, U^{[l]}]$. The differential ideal Ω is prime and $k\{Y, X, U\}/\Omega \simeq k[X]\{U\}$ with the derivation induced by $\dot{X}_j = f_j(X, U)$. Moreover, $\operatorname{diffdim}(\Omega) = m$ and $\operatorname{ord}_k(\Omega) \leqslant n + \rho$.

The fact that the ideal Ω might contain a non-zero polynomial involving only the variables $Y_1, \ldots, Y_\rho$ (since Assumption 4 is no longer valid) prevents us from considering these variables as being part of a differential transcendence basis of $k \hookrightarrow \mathcal{G} := \operatorname{Frac}(k\{Y, X, U\}/\Omega)$. Now we will show how to obtain a maximal differentially independent subset of the set $\{Y_1, \ldots, Y_\rho\}$.

In order to turn to a non-differential situation we will use the following technical result whose proof is straightforward: for every positive integer l, we have $\Omega \cap A_l = \Omega_l$.

Now, following the proof of Proposition 18, we are able to derive an algebraic condition for a set $\mathcal{Y} \subset \{Y_1, \ldots, Y_\rho\}$ to be differentially algebraically independent in the differential extension $k \hookrightarrow \mathcal{G}$:

Proposition 50. *The set $\mathcal{Y} \subset \{Y_1, \ldots, Y_\rho\}$ is differentially algebraically independent in $k \hookrightarrow \mathcal{G}$ if and only if $\mathcal{Y}^{[n+\rho]}$ is algebraically independent in $A_{n+\rho+1}/\Omega_{n+\rho+1}$ over k.*

Combining this proposition with Lemma 19, we deduce the following algorithmic criterion:

Proposition 51. *Let J_0 be the Jacobian matrix $J_0 := \left(\frac{\partial \{F,G\}^{[n+\rho]}}{\partial \{X,U\}^{[n+\rho+1]}} \;\middle|\; \frac{\partial \{F,G\}^{[n+\rho]}}{\partial Y^{[n+\rho]}} \right)$. Then, $\mathcal{Y} \subset \{Y_1, \ldots, Y_\rho\}$ is a differentially algebraically independent set in $k \hookrightarrow \mathcal{G}$ if and only if the columns of J_0 corresponding to derivatives with respect to variables in $\mathcal{Y}^{[n+\rho]}$ can be removed with no change in rank. Here, the ranks are taken over the polynomial ring $k[X, U^{[n+\rho]}] \simeq k[Y^{[n+\rho]}, X^{[n+\rho+1]}, U^{[n+\rho+1]}]/(F^{[n+\rho]}, G^{[n+\rho]})$.*

In the case when $k = \mathbb{Q}(t)$, this result enables us to obtain a maximal differentially algebraically independent subset $\mathcal{Y} \subset \{Y_1, \ldots, Y_\rho\}$ by means of a probabilistic recursive procedure (similar to the algorithm underlying the proof of Theorem 27) within complexity polynomial in the number of variables and equations, and linear in the logarithm of the maximum degree of the input polynomials and the length of a straight-line program encoding them.

7.2. Extended resolvent representation

In the sequel, we will assume that a maximal differentially algebraically independent subset $\mathcal{Y} \subset \{Y_1, \ldots, Y_\rho\}$ in $k \hookrightarrow \mathcal{G}$ has been chosen. In order to simplify notations, will assume that this set is $\mathcal{Y} = \{Y_1, \ldots, Y_r\}$.

The differential equation system obtained by removing from system (7) the equations corresponding to $Y_{r+1}, \ldots, Y_\rho$ satisfies Assumption 4 and so, it can be characterized by means of a resolvent representation as shown in Sections 5 and 6.

Furthermore, for $j = r+1, \ldots, \rho$, there is a non-zero polynomial $M_j \in k\{\mathcal{Y}\}\{T\}$ with $M_j(Y_j) \in \Omega$. Due to Proposition 50, $\{\mathcal{Y}^{[n+\rho]}, Y_j^{[n+\rho]}\}$ is algebraically dependent in $A_{n+\rho+1} / \Omega_{n+\rho+1}$ and so, we can choose $M_j \in k[\mathcal{Y}^{[n+\rho]}][T^{[n+\rho]}]$ with $M_j(\mathcal{Y}^{[n+\rho]}, Y_{r+j}^{[n+\rho]}) \in \Omega_{n+\rho+1}$. An irreducible polynomial $M_j \in k[\mathcal{Y}^{[n+\rho]}]\{T\}$ of minimal order in the variable T satisfying the previous condition will be called a *minimal polynomial for* Y_j.

We will be interested in providing a representation of system (7) of the following type:

Definition 52. An *extended resolvent representation* of system (7) consists of:

- A maximal differentially algebraically independent subset $\mathcal{Y} \subset \{Y_1, \ldots, Y_\rho\}$ in the differential extension $k \hookrightarrow \mathrm{Frac}(k\{Y, X, U\}/[F_1, \ldots, F_n, G_1, \ldots, G_\rho])$.
- Assuming $\mathcal{Y} = \{Y_1, \ldots, Y_r\}$, a differential transcendence basis W of the extension $k\langle\mathcal{Y}\rangle \hookrightarrow \mathcal{F} := \mathrm{Frac}(k\{\mathcal{Y}, X, U\}/[F_1, \ldots, F_n, G_1, \ldots, G_r])$ and a primitive element γ of $k\langle\mathcal{Y}, W\rangle \hookrightarrow \mathcal{F}$.
- A resolvent representation of the ideal $[F_1, \ldots, F_n, G_1, \ldots, G_r]$ with respect to the transcendence basis W and the primitive element γ.
- Minimal polynomials $M_{r+1}, \ldots, M_\rho \in k\{\mathcal{Y}\}\{T\}$ for the variables $Y_{r+1}, \ldots, Y_\rho$.

Denote $G := \{G_1, \ldots, G_r\}$. For $j = r+1, \ldots, \rho$, let $\Omega^j \subset k\{\mathcal{Y}, Y_j, X, U\}$ be the differential ideal $[F, G, G_j]$ and, for every non-negative integer l, let $\Omega_l^j := (F^{[l-1]}, G^{[l-1]}, G_j^{[l-1]})$ be the polynomial ideal defined in $k[\mathcal{Y}^{[l-1]}, X^{[l]}, U^{[l]}][Y_j^{[l-1]}]$.

Let s_j be the minimum non-negative integer h such that $\{\mathcal{Y}^{[n+\rho]}, Y_j^{[h]}\}$ is algebraically dependent in $A_{n+\rho+1}/\Omega_{n+\rho+1}$. The fact that for a minimal polynomial for Y_j we have $M_j(\mathcal{Y}^{[n+\rho]}, Y_j^{[s_j]}) \in \Omega_{n+\rho+1}$ implies straightforwardly that this polynomial is in $\Omega^j_{n+\rho+1}$, since it does not

depend on the variables $Y_k^{(h)}$ with $k > r$, $k \neq j$. Thus, in order to find the polynomial M_j it is enough to consider the differential system $F = 0, G = 0, G_j = 0$ and its associated ideals Ω^j and Ω_l^j, $l \geqslant 0$. This implies, in turn, the existence of a minimal polynomial $M_j \in k[\mathcal{Y}^{[n+r]}][T^{[s_j]}]$ for Y_j with $s_j \leqslant n + r$ and $M_j(\mathcal{Y}^{[n+r]}, Y_j^{[s_j]}) \in \Omega_{n+r+1}^j$.

Finally, we can estimate the total degree of the minimal polynomials M_j, $j = r + 1, \ldots, \rho$, by characterizing them as the defining equations of certain hypersurfaces. To do so, let $n_1 := (n+m+r+1)(n+r+1)+n+m$. Fix $j, r+1 \leqslant j \leqslant \rho$, let $\mathbb{V}_j$ be the irreducible variety defined in $\mathbb{A}^{n_1}$ by the ideal Ω_{n+r+1}^j and consider the linear map $\pi_j : \mathbb{V}_j \to \mathbb{A}^{r(n+r+1)+s_j+1}$ defined by $\pi_j(y^{[n+r]}, x^{[n+r+1]}, u^{[n+r+1]}, y_j^{[n+r]}) = (y^{[n+r]}, y_j^{[s_j]})$.

Proposition 53. *Under the previous assumptions and notations, for $j = r+1, \ldots, \rho$, the Zariski closure $\overline{\pi_j(\mathbb{V}_j)}$ is an irreducible hypersurface of $\mathbb{A}^{r(n+r+1)+s_j+1}$ and any irreducible polynomial $M_j \in k[\mathcal{Y}^{[n+r]}, T^{[s_j]}]$ defining $\overline{\pi_j(\mathbb{V}_j)}$ is a minimal polynomial for Y_j.*

We deduce:

Corollary 54. *For $j = r+1, \ldots, \rho$, a minimal polynomial $M_j \in k[\mathcal{Y}^{[n+r]}, T^{[s_j]}]$ for Y_j satisfies: $s_j \leqslant n + r$, $M_j(\mathcal{Y}^{[n+r]}, Y_j^{[s_j]}) \in \Omega_{n+r+1}^j$ and $\deg(M_j) \leqslant \deg(\mathbb{V}_j)$.*

From the algorithmic point of view (assuming $k = \mathbb{Q}(t)$), the order s_j of the minimal polynomial M_j can be computed with the same techniques of matrix rank computations as those used in Section 4 as the minimum non-negative integer h such that $\{\mathcal{Y}^{[n+r]}, Y_j^{[h]}\}$ is algebraically independent in $k[\mathcal{Y}^{[n+r]}, X^{[n+r+1]}, U^{[n+r+1]}, Y_j^{[n+r]}]/\Omega_{n+r+1}^j$ (using the Jacobian matrix of the generator system of Ω_{n+r+1}^j). Then, a minimal polynomial M_j can be computed as a polynomial defining $\overline{\pi_j(\mathbb{V}_j)}$ following the procedure underlying the proof of Proposition 46.

Therefore, we obtain a probabilistic algorithm that computes an extended resolvent representation of system (7) within the same order of complexity as for the computation of a resolvent representation under Assumption 4:

Corollary 55. *The computational complexity of an extended resolvent representation of system* (7) *is polynomial in the number of variables, the number of input polynomials, an upper bound for their degrees and the degree of an algebraic variety defined by these polynomials and their derivatives up to a fixed order, and linear in the length of a straight-line program encoding them.*

Acknowledgements

The authors thank the anonymous referees for their helpful suggestions and remarks.

References

[1] S. Basu, R. Pollack, M.-F. Roy, Algorithms in Real Algebraic Geometry. Algorithms and Computation in Mathematics, vol. 10, Springer, Berlin, 2003.
[2] D. Bini, V.Y. Pan, Polynomial and Matrix Computations, Fundamental Algorithms, Progress in Theoretical Computer Science, Birkhäuser, Boston, MA, 1994.
[3] P. Bürgisser, M. Clausen, M.A. Shokrollahi, Algebraic Complexity Theory, Grundlehren der Mathematischen Wissenschaften, vol. 315, Springer, Berlin, 1997.

[4] T. Cluzeau, E. Hubert, Resolvent representation for regular differential ideals, Technical Report RR-4200, INRIA Sophia Antipolis, 2001.
[5] T. Cluzeau, E. Hubert, Resolvent representation for regular differential ideals, AAECC 13 (2003) 395–425.
[6] S. Diop, M. Fliess, On nonlinear observability, in: C. Commault, D. Normand-Cyrot, J.M. Dion, L. Dugard, M. Fliess, A. Titli, G. Cohen, A. Benveniste, I.D. Landau (Eds.), Proceedings of the European Control Conference, vol. 1, Hermès, Paris, 1991, pp. 152–157.
[7] M. Fliess, J. Lévine, P. Martin, P. Rouchon, Index and decomposition of nonlinear implicit differential equations, in: Proceedings of IFAC Conference on System Structure and Control, Nantes, July 1995.
[9] G. Gallo, B. Mishra, The complexity of resolvent resolved, Proceedings of the Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, Arlington, VA, ACM, New York, 1994, pp. 280–289.
[11] J. von zur Gathen, J. Gerhard, Modern Computer Algebra, Cambridge University Press, New York, 1999.
[12] M. Giusti, K. Hägele, J. Heintz, J.L. Montaña, J.E. Morais, L.M. Pardo, Lower bounds for diophantine approximation, J. Pure Appl. Algebra 117, 118 (1997) 277–317.
[13] M. Giusti, J. Heintz, J.E. Morais, L.M. Pardo, When polynomial equation systems can be "solved" fast? Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995), Lecture Notes in Computer Science, vol. 948, Springer, Berlin, 1995, pp. 205–231.
[14] M. Giusti, G. Lecerf, B. Salvy, A Gröbner free alternative for polynomial system solving, J. Complexity 17 (1) (2001) 154–211.
[15] D. Grigoriev, Complexity of quantifier elimination in the theory of ordinary differential equations, Lecture Notes in Computer Science, vol. 378, Springer, Berlin, 1989, pp. 11–25.
[16] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, Theoret. Comput. Sci. 24 (3) (1983) 239–277.
[17] J. Heintz, T. Krick, S. Puddu, J. Sabia, A. Waissbein, Deformation techniques for efficient polynomial equation solving, J. Complexity 16 (1) (2000) 70–109.
[18] J. Heintz, G. Matera, A. Waissbein, On the time-space complexity of geometric elimination procedures, Appl. Algebra Eng. Comm. Comput. 11 (4) (2001) 239–296.
[19] J. Heintz, C.-P. Schnorr, Testing polynomials which are easy to compute, Monographie 30 de l'Enseignement Mathématique, 1982, 237–254.
[20] E. Hubert, Notes on triangular sets and triangulation decomposition algorithms II: differential systems, in: U. Langer, F. Winkler (Eds.), Lecture Notes in Computer Science, vol. 2630, Springer, Berlin, 2003, pp. 40–87.
[21] E.R. Kolchin, Differential Algebra and Algebraic Groups, Academic Press, New York, 1973.
[22] T. Krick, L.M. Pardo, A computational method for Diophantine approximation, Progr. Math. 143 (1996) 193–254.
[23] T. Krick, L.M. Pardo, M. Sombra, Sharp estimates for the arithmetic Nullstellensatz, Duke Math. J. 109 (3) (2001) 521–598.
[24] L. Kronecker, Grundzüge einer arithmetischen Theorie der algebraischen Grössen, J. Reine Angew. Math. 92 (1882) 1–122.
[25] E. Kunz, Introduction to Commutative Algebra and Algebraic Geometry, Birkhäuser, Boston, MA, 1985.
[26] G. Matera, A. Sedoglavic, Fast computation of discrete invariants associated to a differential rational mapping, J. Symbolic Comput. 36 (3–4) (2003) 473–499.
[27] J.F. Ritt, Differential equations from the algebraic standpoint, Amer. Math. Soc. Colloq. Publ. 14 (1932).
[28] J.F. Ritt, Differential algebra, Amer. Math. Soc. Colloq. Publ. 33 (1950).
[29] B. Sadik, Contributions à l'étude de la complexité du calcul d'un ensemble caractéristique en algèbre différentielle, Ph.D. Thesis, 1995.
[30] B. Sadik, A bound for the order of characteristic set elements of an ordinary prime differential ideal and some applications, Appl. Algebra Eng. Comm. Comput. 10 (3) (2000) 251–268.
[31] E. Schost, Computing parametric geometric resolutions, Appl. Algebra Eng. Comm. Comput. 13 (5) (2003) 349–393.
[32] J.T. Schwartz, Fast probabilistic algorithms for verification of polynomial identities, J. ACM 27 (1980) 701–717.
[33] A. Sedoglavic, A probabilistic algorithm to test local algebraic observability in polynomial time, Computer algebra (London, ON, 2001), J. Symbolic Comput. 33 (5) (2002) 735–755.
[34] A. Seidenberg, Some basic theorems in differential algebra (characteristic p arbitrary), Trans. Amer. Math. Soc. 73 (1952) 174–190.
[35] A. Seidenberg, Some basic theorems in partial differential algebra, Memoirs of the College of Science, University of Kyoto, Series A, vol. XXXI (1), 1958, Mathematics, pp. 1–8.
[36] R. Zippel, Probabilistic algorithms for sparse polynomials, in: Proceedings of EUROSAM'79, Lecture Notes in Computer Science, vol. 72, Springer, Berlin, 1979, pp. 216–226.