UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

Métodos simbólicos para sistemas de ecuaciones algebraico-diferenciales

Tesis presentada para optar al título de Doctor
de la Universidad de Buenos Aires
en el área Ciencias Matemáticas

María Elisabet D'Alfonso

Director de tesis: Pablo Solernó

Buenos Aires, 2006

Métodos simbólicos para sistemas de ecuaciones álgebro-diferenciales

Resumen

Esta tesis está dedicada al estudio de una clase particular de sistemas genéricos de ecuaciones álgebro-diferenciales ordinarias que surgen en la teoría de control no lineal pero que, además, pueden considerarse como ecuaciones que definen el gráfico de un morfismo diferencial o, simplemente, como una familia de ecuaciones polinomiales con un miembro genérico. Nos concentramos principalmente en una presentación alternativa de estos sistemas, la representación resolvente, introducida en el contexto diferencial por J. F. Ritt. Esta representación puede ser interpretada como el análogo diferencial del "shape lemma", una construcción bien conocida de la geometría algebraica, o del elemento primitivo de extensiones separables de cuerpos o del vector cíclico de sistemas diferenciales lineales de primer orden, y está dada por la codificación de los ceros del sistema por los de una única ecuación polinomial diferencial, via una equivalencia birracional. Encontramos cotas superiores para el orden y el grado de los polinomios involucrados en dicha representación, en términos del grado de una variedad algebraica intrínseca definida a partir de las derivadas, hasta un orden preestablecido, de las ecuaciones del sistema original, y mostramos con un ejemplo que estas cotas son óptimas. También exhibimos un algoritmo probabilístico que calcula esta representación resolvente en tiempo polinomial en los parámetros sintácticos naturales y en el grado de la variedad mencionada.

Nuestro enfoque conduce a nuevos resultados adicionales para los sistemas genéricos considerados, concerniendo dos invariantes discretos bien conocidos: el índice de diferenciación y la función de Hilbert-Kolchin diferencial. Primero, damos una definición precisa y puramente algebraica del índice de diferenciación y mostramos que la función de Hilbert-Kolchin siempre coincide con el polinomio asociado. Segundo, mostramos un algoritmo probabilístico que calcula estos invariantes en tiempo polinomial. Por último, establecemos algunos resultados cuantitativos y algorítmicos relativos a bases de trascendencia diferenciales y a variables ímplicitas y libres determinadas por el índice.

Palabras clave: Álgebra diferencial; Representación resolvente; Teoría de eliminación; Algoritmo probabilístico; Straight-line programs; Índice de diferenciación; Función de Hilbert-Kolchin diferencial.

Symbolic methods for differential algebraic equation systems

Abstract

This thesis is devoted to the study of a particular class of generic ordinary differential algebraic equations systems, arising in nonlinear control theory, but that can be considered also as the equations defining the graph of a differential morphism or, simply, as a family of differential polynomial equations with a generic member. We mainly focus on an alternative presentation for these systems, the resolvent representation, introduced in the differential context by J.F. Ritt. This representation may be considered as the differential analogue of the well-known shape lemma from algebraic geometry or of the primitive element of separable field extensions or of the cyclic vector for first-order linear differential equations, and is given by the encoding, via a birational equivalence, of the zeros of the differential system of equations with the zeros of a single polynomial differential equation. We show upper bounds for the order and the degree of the polynomials involved in this representation, in terms of the degree of an intrinsic algebraic variety defined from the derivatives of the original equations up to a preestablished order, and we show with an example that these upper bounds are optimal. We also exhibit a probabilistic algorithm which computes this resolvent representation within time polynomial in the natural syntactic parameters and the degree of the variety above mentioned.

Our approach leads us to additional new results for the differential systems we consider, concerning two well-known discrete invariants: the differentiation index and the Hilbert-Kolchin function. The results are as follows. First, we give a precise and purely algebraic definition of differentiation index and prove that the differential Hilbert-Kolchin function always coincides with its associated polynomial. Second, we give a probabilistic polynomial-time algorithm for the computation of these two invariants. Finally, some quantitative and algorithmic results concerning differential transcendence bases and implicit and free variables determined by the index are established.

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

Agradecimientos

A Pablo Solernó, por ser mi director.

A Willie Cortiñas.

A los jurados, Ricardo Durán, Evelyne Hubert, Guillermo Matera y François Ollivier, por sus correcciones y observaciones.

A Gabriela Jeronimo, por su colaboración.

A todos los que colaboraron de alguna forma en la realización de esta tesis.

Table of Contents

Table of Contents 7

Introducción 9

Introduction 17

1 Preliminaries 25
- 1.1 Basic differential algebra . . . 25
  - 1.1.1 Differential rings and fields . . . 25
  - 1.1.2 Differential Hilbert-Kolchin function . . . 27
- 1.2 Data structures and algorithmic model . . . 28

2 Differential algebraic equation systems 31
- 2.1 Definitions and basic properties . . . 32
- 2.2 Associated Jacobian sub-matrices . . . 37
- 2.3 The rank of matrices $\mathfrak{J}_{k,i}$ . . . 39

3 Differential Hilbert-Kolchin function and differential transcendence basis: quantitative and algorithmic aspects 47
- 3.1 The differentiation index . . . 47
- 3.2 The differential Hilbert-Kolchin function . . . 49
- 3.3 A differential transcendence basis . . . 50
- 3.4 The algorithms and their complexities . . . 53

4 Resolvent representation 61
- 4.1 Existence of a primitive element and a resolvent representation . . . 61
  - 4.1.1 Bounds for the order and degree of a minimal polynomial of a primitive element 65
  - 4.1.2 An example . . . 69
  - 4.1.3 The minimal polynomial of a generic primitive element . . . 71
  - 4.1.4 The resolvent representation . . . 74
- 4.2 Algorithmic computation of a resolvent representation . . . 75
  - 4.2.1 Computing the generic minimal polynomial . . . 76
  - 4.2.2 Computation of a primitive element . . . 80
  - 4.2.3 Computing a resolvent representation of the system . . . 82
- 4.3 Differential systems of higher order . . . 83

A Resolvent representation for over-determined differential systems **89**
A.1 Rankings and characteristic sets 90
A.2 Independent equations 90
A.3 Extended resolvent representation 92

B Differential index and implicit equations **97**
B.1 "Good" differential transcendence basis: a simple example 98
B.2 Implicit variables 100

C Bézout-type degree bounds for the resolvent representation of explicit systems **105**

List of Symbols **109**

Bibliography **113**

Introducción

Las ecuaciones diferenciales han demostrado ser una herramienta de gran utilidad en una amplia variedad de áreas como la ingeniería, la biología o la química. El tratamiento usual que se da a los sistemas de ecuaciones diferenciales puede dividirse en dos etapas: la primera consiste en transformar el sistema en otro equivalente pero de manejo más sencillo y la segunda, en encontrar las soluciones de este nuevo sistema. Algunas veces, la forma general de estas soluciones pueden ser determinadas desde un principio pero en la mayoría de los casos, la única manera posible de obtener una solución es aplicar alguno de los distintos métodos numéricos después de simplificar el sistema.

El conjunto de *todas* las ecuaciones que se pueden deducir de las ecuaciones originales por medio de manipulaciones algebraicas y derivaciones y que deben ser verificadas por todas las soluciones del sistema se llama el *ideal diferencial* asociado al sistema. Un punto clave es encontrar una descripción "simple" de este ideal. Esta idea fue una de las motivaciones del álgebra diferencial iniciada por J.F. Ritt [52] y continuada por E.R. Kolchin [38].

La noción de *representación resolvente* de un ideal diferencial primo en un anillo de polinomios diferenciales fue introducida por Ritt (ver [52, 51]) y ampliada a ideales diferenciales regulares por Cluzeau y Hubert en [13]. Este concepto es parte del proyecto del Ritt para el desarrollo de una teoría algebraica que permita el tratamiento de ecuaciones álgebro-diferenciales. Sus orígenes primarios pueden encontrarse en los trabajos de Kronecker correspondientes a la parametrización de variedades algebraicas. (ver [41]). A grandes rasgos, una *representación resolvente* de un ideal diferencial primo provee una parametrización de los ceros (genéricos) del ideal por medio de los ceros (genéricos) de un único polinomio diferencial irreducible. Este fenómeno es bastante general y puede ser interpretado en varios contextos, a priori diversos: la existencia del elemento primitivo de extensiones de cuerpos separables o de un vector cíclico en sistemas diferenciales lineales de primer orden, así también como el "shape lemma" en el ámbito de la geometría algebraica o analítica son ejemplos de "representaciones resolventes".

Para motivar e ilustrar la noción de representación resolvente que vamos a considerar en este trabajo,

veamos el siguiente sistema diferencial de cuatro ecuaciones con cuatro incógnitas X_1, X_2, X_3, U:

$$\begin{cases} \dot{X}_1 &= \alpha X_1 \\ \dot{X}_2 &= \alpha X_2 \\ \dot{X}_3 &= \beta X_3 + U X_1 \\ Y &= X_2 + X_3 \end{cases},$$

donde $\alpha, \beta \in \mathbb{Q}$, la variable Y es un parámetro y el cuerpo diferencial base del sistema es $\mathbb{Q}(t)$ provisto de la derivación usual, $t' = 1$. Llamemos $\gamma := X_1 + tX_2$. Todas las variables del sistema se pueden escribir, realizando operaciones elementales con las ecuaciones originales y sus derivadas, como funciones racionales en $\mathbb{Q}(t, Y, \dot{Y})(\gamma, \dot{\gamma})$:

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

Además, el elemento γ verifica la ecuación diferencial

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

A esta relación se la llama la *ecuación minimal* de γ. El conjunto formado por el polinomio diferencial irreducible que determina esta ecuación minimal y por los polinomios que representan la escritura de las variables como funciones racionales es la *representación resolvente* del sistema y γ, el *elemento primitivo* asociado. Más ejemplos de representaciones resolventes pueden encontrarse en la Sección 4.1.2 o en [13].

Este trabajo se concentra en el cálculo de representaciones resolventes de ideales diferenciales primos asociados a sistemas de ecuaciones diferenciales del siguiente tipo:

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

donde $f_1, \ldots, f_n \in k[X, U]$ son polinomios en las $n + m$ variables $X := \{X_1, \ldots, X_n\}$, $U := \{U_1, \ldots, U_m\}$ y $g_1, \ldots g_r \in k[X, U, \dot{U}]$, en variables X, U y en las variables derivadas $\dot{U} := \{\dot{U}_1, \ldots, \dot{U}_m\}$, con coeficientes

en un cuerpo diferencial k de característica cero y con grados totales acotados por un entero d. Las variables $Y := Y_1, \ldots, Y_r$ forman un nuevo conjunto de indeterminadas diferenciales que serán consideradas como parámetros (mientras que las variables X y U son las incógnitas del sistema). Así, las últimas r ecuaciones tienen primer miembro "genérico". Dado que el conjunto de variables Y es un conjunto de parámetros, resulta natural considerar el sistema sobre el cuerpo de base $k\langle Y\rangle$, el menor cuerpo diferencial que contiene a k y a todas las derivadas sucesivas del conjunto Y. Aunque nosotros no supondremos, como es usual, una situación 0-dimensional diferencial (consideraremos también el caso r estrictamente menor que m), en un principio asumiremos que las últimas r ecuaciones son "independientes" en cierto sentido natural cuya definición precisa puede encontrarse en Assumption 5. Esta hipótesis puede ser levantada preservando esencialmente todos los resultados, como se muestra en la Apéndice A.

Sistemas de ecuaciones algebro-diferenciales como (Σ) pueden ser interpretados desde varios puntos de vista; por ejemplo, este tipo de sistemas aparecen naturalmente en Teoría de Control (ver, entre otros, [18], [16], [19] y [9, Section 4]) o pueden ser considerados como las ecuaciones que definen el gráfico de un morfismo diferencial (ver [45]). El sistema (Σ) puede entenderse también como una familia usual de ecuaciones polinomiales algebro-diferenciales donde el primer miembro parametriza la familia y toma valores arbitrarios fuera de un conjunto cerrado Zariski propio (ver [53, Section 5.2]). En este último sentido decimos que el sistema (Σ) es *genérico*.

Los Resultados

Dado un sistema de ecuaciones diferenciales como (Σ), consideramos el ideal diferencial primo Δ generado por los polinomios $f_i - \dot{X}_i$, $i = 1, \ldots, n$, y $g_j - Y_j$, $j = 1, \ldots, r$, en el anillo de polinomios diferenciales $k\langle Y\rangle\{X, U\}$.

En este trabajo probamos la existencia de una representación resolvente para el ideal Δ constituida por polinomios que involucran derivadas de las variables Y, X y U hasta orden $2n + 2r$ y cuyos grados están acotados por el grado de una variedad algebraica $\mathbb{V}$ definida por los polinomios input y sus derivadas hasta orden $2n + 2r - 1$ (ver Teoremas 49 y 56). La desigualdad de Bézout implica que $\deg(\mathbb{V})$ puede ser acotada por $d^{2(n+r)^2}$, donde d es el máximo de los grados de los polinomios f_i, $i = 1, \ldots, n$, y g_j, $j = 1, \ldots, r$. Más aún, con el Ejemplo 51, mostramos que estas cotas superiores geométricas son óptimas.

En el caso $k = \mathbb{Q}(t)$, también construimos un algoritmo probabilístico, *con error acotado*, que calcula una representación resolvente de Δ. Si los polinomios input están dados por un straight-line program de longitud L sobre $\mathbb{Q}$ (ver Sección 1.2 para la definición de esta estructura de datos), la complejidad de este algoritmo es lineal en L y polinomial en n, m, r, d y $\deg(\mathbb{V})$ (ver Teorema 61). Observemos que la cota superior dada por la desigualdad de Bézout para $\deg(\mathbb{V})$ induce, en el peor de los casos, una complejidad simplemente exponencial para nuestro algoritmo. La probabilidad de error del algoritmo está controlada

por medio del clásico 0-test de Zippel-Schwartz (ver [63] y [56]) conjuntamente con las cotas de grado que a priori podemos estimar para aquellos polinomios que definen las condiciones de genericidad bajo las cuales corre nuestro algoritmo (sin necesidad de calcular dichos polinomios, ver Sección 1.2).

Para obtener los resultados mencionados, es necesario el estudio del comportamiento de dos invariantes discretos bien conocido y asociados al sistema: el *índice de diferenciación* del sistema (Σ) y la *función diferencial de Hilbert-Kolchin* del ideal Δ. Este estudio indujo, como productos colaterales de nuestros métodos, el desarrollo de nuevos resultados sobre estos invariantes.

El índice de diferenciación es un importante invariante asociado a un sistema de ecuaciones algebro-diferenciales, usualmente definido sólo para sistemas de primer orden 0-dimensionales. Existen diferentes definiciones de índices de diferenciación que no siempre resultan equivalentes (ver, por ejemplo, [7], [50], [9], [44], [18], [60], [58]). Nosotros nos concentraremos en el *índice de diferenciación global* (ver [7, Section 2.2]). Informalmente, el índice de diferenciación denota el numero mínimo de veces que deben derivarse las ecuaciones que forman un sistema álgebro-diferencial para despejar a las derivadas de las incógnitas como funciones (continuas, diferenciables, analíticas, etc.) dependientes de la propias incógnitas (ver [7, Definition 2.2.2]) y obtener así un sistema explícito. En cierto sentido, el índice representa una medida de la complejidad de un sistema de ecuaciones álgebro-diferenciales desde el punto de vista de su resolución numérica: por ejemplo, está estrechamente relacionado con el número de condición de la matriz de iteración en el método de Runge-Kutta implícito (ver [7, Theorem 5.4.1]).
En este trabajo damos una definición precisa de índice de diferenciación algebraico para sistemas de ecuaciones álgebro-diferenciales del tipo (Σ), *no necesariamente* 0*-dimensionales* (ver Definición 25), mediante propiedades de estacionalidad que verifican los rangos de ciertas submatrices jacobianas asociadas a (Σ) desarrolladas en la Sección 2.3 (ver también [58]). Otra definición equivalente del índice, en términos de una filtración natural dada por las sucesivas diferenciaciones de las ecuaciones input, está contenida implícitamente en el Teorema 26. En particular, esta última formulación muestra que el índice de diferenciación es también el número de derivadas necesarias para obtener *todas* las relaciones algebraicas que cualquier solución del sistema debe satisfacer.
Como hemos expresado arriba, la noción de índice de diferenciación está relacionada con la posibilidad de escribir a las derivadas de las incógnitas como funciones dependientes de las propias incógnitas. Desafortunadamente, en la mayoría de los casos, es imposible obtener este tipo de escritura usando solamente las ecuaciones originales. Por ejemplo, aún en un caso como el nuestro en el que todas las ecuaciones tienen orden a lo sumo uno, esta situación particularmente buena y cuya factibilidad está dada por el Teorema de las Funciones Implícitas, corresponde a aquellos sistemas cuyo índice es 0. Sin embargo, en el caso general, siempre es posible obtener dicha escritura si se utilizan las (tantas como el índice) derivadas sucesivas de las ecuaciones. Claramente, el nuevo sistema explícito escapa del

marco de los sistemas polinomiales o racionales. En nuestro caso, damos una descripción, en una forma polinomial simple, de la versión implícita del nuevo sistema y distinguimos a las variables de acuerdo a las relaciones que satisfacen entre ellas (es decir, "variables libre", " variables implícitas", etc.). Más aún, también estimamos cotas superiores para el grado y el orden de estas ecuaciones (Teorema 70) y mostramos un algoritmo que calcula el nuevo sistema (Proposición 73) dentro del mismos órdenes de complejidad que los descriptos para la representación resolvente.

E. Kolchin en [38, Chapter II] da por primera vez una definición formal de la función de Hilbert-Kolchin de un ideal diferencial como una forma de estimar, para cada entero no negativo i, el grado de libertad de las primeras i derivadas de las incógnitas módulo las relaciones inducidas por las ecuaciones del sistema original (ver Sección 1.1.2 para una definición precisa). Esta función está estrechamente relacionada con otros dos invariantes discretos del ideal, su *orden* y su *dimensión diferencial*. Estos invariantes ya habían sido considerados en los trabajos de J. Ritt, [52] y [51], y corresponden, respectivamente, al número de condiciones iniciales y al número de condiciones libres en el conjunto de soluciones del sistema diferencial asociado con el ideal.

La función de Hilbert-Kolchin, como sucede con la función de Hilbert clásica asociada a ideales polinomiales homogéneos (ver, por ejemplo, [1, Chapter 11]), deviene en un polinomio bien definido, para argumentos i suficientemente grandes, y en el caso diferencial ordinario este polinomio es extremadamente simple ya que su grado es a lo sumo 1. La *regularidad* de la función de Hilbert-Kolchin es el primer entero no negativo a partir del cual la función y el polinomio coinciden. Un resultado bien conocido afirma que esta regularidad puede ser descripta *exactamente* en términos de los órdenes de los elementos de un conjunto característico asociado a un ranking ordenado (ver la demostración de [38, Chapter II, Section 12, Theorem 6] o [10, Theorem 3.3]). Aquí (ver Teorema 28) mostramos que la regularidad de la función de Hilbert-Kolchin del sistema (Σ) sobre el cuerpo $k\langle Y\rangle$ es siempre 0, es decir, la función de Hilbert-Kolchin y el polinomio asociado coinciden para todo entero i.

Mostramos también un algoritmo probabilístico que calcula el índice de diferenciación del sistema (Σ) y la función de Hilbert-Kolchin diferencial del ideal Δ con complejidad polinomial en n, m, r, d y lineal en L (ver Teorema 37). Este algoritmo funciona a través del cálculo y la comparación de los rangos de ciertas matrices jacobianas. Este resultado es una extensión natural a una situación de dimensión positiva del algoritmo que puede encontrarse en [45] para el cálculo de la función de Hilbert-Kolchin.

Nuestro enfoque

Nuestra estrategia global consiste en trasladar un problema diferencial (no noetheriano) en uno algebraico (noetheriano) y, en este sentido, el Teorema 26 cumple un rol fundamental. El primer paso que desarrollamos hacia la obtención de la representación resolvente del ideal Δ es el cálculo de una base

de trascendencia diferencial de la extensión de cuerpos diferenciales inducida por nuestro sistema para poder ubicarnos en una situación 0-dimensional. Luego, mostramos una versión efectiva y algorítmica de la demostración de la existencia del elemento primitivo hecha por Seidenberg (ver [59]) adaptada a nuestro caso reduciendo así el problema al cálculo de un polinomio eliminante de una variedad en un contexto algebraico-geométrico. Finalmente, aplicamos un proceso de eliminación basado en los trabajos [30] y [55] para hacer nuestros cálculos principales.

Desde sus orígenes en [52], la representación resolvente de los sistemas de ecuaciones diferenciales polinomiales ha sido enfocada desde un punto de vista efectivo. El tratamiento del tema que propone Ritt, así como las generalizaciones subsiguientes ([13], [12]), están basadas en técnicas de reescrituras utilizando bases de Gröbner y conjuntos característicos (ver [4], [5] y [6]). En [23] se prueba que, en un contexto algebraico, el cálculo de la representación resolvente por medio de estos métodos tiene cota de complejidad simplemente exponencial, pero no existe ningún análisis de complejidad de la contraparte diferencial del problema en ninguno de los trabajos relacionados con el tema. Sin embargo, los resultados sobre la complejidad del cálculo de conjuntos característicos diferenciales dados en [53] inducen cotas de complejidad simplemente exponencial para un algoritmo probabilístico que calcule la representación resolvente de los sistemas que estamos considerando (ver [12]).

Vale la pena destacar que, contrario a los métodos utilizados hasta el momento, nuestros algoritmos no requieren del cálculo de bases de Gröbner ni de conjuntos característicos. Nuestro enfoque, basado en el cálculo de polinomios eliminantes algebraicos, nos permite obtener estimaciones de complejidad en términos de un invariante geométrico y que resultan ser mucho más precisas que las que sólo dependen de parámetros sintácticos (ver Sección 51). Este tipo de cotas de complejidad, dependiendo de este tipo de parámetros, aparecen previamente en varios procesos de eliminación algebraica, por ejemplo, [27], [30], [28]y [43]. Observamos también que, en términos de los parámetros n, m, r, d, la complejidad de nuestro algoritmo es de orden $(nmr)^{O(1)}d^{O((n+r)^2)}$, mejorando la complejidad del proceso de reescritura presentado en [53, Theorem 28] que, aplicado a nuestro caso da lugar a una complejidad algo peor, del orden de $(n+r)^{O((n+m)(n+r))}d^{O((n+m)^3(n+r)^3)}$.

Estructura de la tesis

Esta tesis se divide en cuatro capítulos.

En la primera parte del Capítulo 1 recordamos algunas nociones y resultados básicos del álgebra diferencial que serán necesarios a lo largo de todo el trabajo y en la segunda parte presentamos el modelo algorítmico que adoptaremos.

Al comienzo del Capítulo 2, describimos una vez más el sistema de ecuaciones diferenciales que consideraremos y mostramos las primeras propiedades elementales de estos sistemas, de los ideales diferenciales asociados y de las extensiones de cuerpos diferenciales relativos a estos ideales. En el mismo capítulo hacemos un estudio detallado del comportamiento de una sucesión de número enteros, asociada a los rangos de ciertas submatrices jacobianas de las ecuaciones input y sus derivadas. Esta sucesión induce una definición precisa y puramente algebraica del índice de diferenciación.

Comenzamos el Capítulo 3 mostrando en el Teorema 26 una relación entre el índice y la variedad de restricciones del sistema. Este teorema, como ya dijimos, contiene una descripción alternativa del índice de diferenciación y provee el resultado clave para el traslado de los problemas diferenciales a un contexto algebraico "noetheriano". El resto del capítulo está dedicado al cálculo de la función de Hilbert-Kolchin diferencial del ideal Δ, asociado al sistema (Σ), y de una base de trascendencia diferencial de la extensión de cuerpos inducida. En realidad, en este capítulo, mostramos la existencia y el cálculo de una base de trascendencia diferencial que verifica una propiedad particular de "buena localización" que nos ahorrará trabajo extra en nuestra búsqueda de la representación resolvente y que resultará necesaria para la descripción alternativa del sistema (Σ) que se deriva de las propiedades del índice de diferenciación.

Por último, el Capítulo 4 está enteramente dedicado a la prueba de la existencia y al cálculo de la representación resolvente del ideal Δ y se divide en tres secciones. En la Sección 4.1 recordamos la noción de representación resolvente de un ideal diferencial primo y probamos cotas superiores para los órdenes y los grados de los polinomios involucrados. La Sección 4.2 está destinada al cálculo algorítmico de la representación resolvente y en la Sección 4.3 se encuentra una generalización de estos resultados a sistemas diferenciales de orden superior.

Este trabajo contiene también tres apéndices.

En el Apéndice A presentamos una generalización de los resultados algorítmicos del último capítulo dejando de lado la hipótesis de "independencia" de las últimas r ecuaciones del sistema (Σ), es decir, dejando de lado Assumption 5, introducida en la Sección 2.1.

El Apéndice B está consagrado a la presentación alternativa del sistema (Σ), en el espíritu del Teorema de las Funciones Implícitas, que se deduce de los resultados obtenidos sobre el índice de diferenciación y a un algoritmo que permite calcular esta representación.

En el Apéndice C presentamos una mejora sobre las cotas de grados obtenidas en el Capítulo 4 para el caso particular y clásico de sistemas de ecuaciones diferenciales explícitos, de índice 0, de la forma $\dot{X} = F(X)$ (donde F es una función polinomial del espacio n-dimensional sobre un cuerpo diferencial, no necesariamente de constantes).

Introduction

Differential equations have proved to be useful in a broad range of areas such as engineering, biology, chemistry, etc. The general treatment applied to systems of differential equations is divided in two different stages: the first one is to transform the system in another one equivalent but easier to handle and the second one is to find the solutions of this new system. Sometimes one can determine from the beginning the general form of the solutions but in most cases the only way of obtaining a solution is to simplify the system and then apply numerical methods.

The set of *all* the equations that can be deduced from the original system by algebraic manipulations and derivations and that all the solution of the given system must verify is called the *differential ideal* associated to the system. A key point is to find a "simpler" description of this ideal. This idea was the foundation for the development of differential algebra initiated by J.F. Ritt [52] and followed by E.R. Kolchin [38].

The notion of a *resolvent representation* of a prime differential ideal in a ring of differential polynomials was introduced by Ritt (see [52, 51]) and extended to regular differential ideals by Cluzeau and Hubert in [13]. This concept is part of Ritt's project for the development of an algebraic theory for the study of differential algebraic equations and its primary origins can be traced back to Kronecker's works on the parametrization of algebraic varieties (see [41]). 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, a priori different: the existence of a primitive element of a separable field extensions or of a cyclic vector of linear first order differential systems, as well as the "shape lemma" in algebraic or analytic geometry are examples of "resolvent representations".

In order to illustrate the notion of resolvent representation considered in this work, let us look at the following simple differential algebraic system consisting of four equations in the four unknowns X_1, X_2, X_3, U:

$$\left\{ \begin{array}{rcl} \dot{X}_1 & = & \alpha X_1 \\ \dot{X}_2 & = & \alpha X_2 \\ \dot{X}_3 & = & \beta X_3 + U X_1 \\ Y & = & X_2 + X_3 \end{array} \right. ,$$

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 the system 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 and γ is its associated *primitive element*. For more examples of resolvent representations see Section 4.1.2 below or [13].

This present work deals with the computation of resolvent representations of prime differential ideals associated with certain differential systems of equations of the following type:

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

where $f_1, \ldots, f_n \in k[X, U]$ are polynomials in the $n+m$ variables $X := \{X_1, \ldots, X_n\}$ and $U := \{U_1, \ldots, U_m\}$ and $g_1, \ldots g_r \in k[X, U, \dot{U}]$, in the variables X, U and the derivatives $\dot{U} := \{\dot{U}_1, \ldots, \dot{U}_m\}$, with coefficients in a differential field k of characteristic zero and with total degrees bounded by an integer d. The variables $Y := Y_1, \ldots, Y_r$ are a new set of differential indeterminates that will be considered as parameters (while the variables X and U are the unknowns of the system) and thus the last r equations will be considered as having "generic" first members. Since the variables Y are regarded as parameters, it is natural to consider $k\langle Y\rangle$, the smaller field containing k and all the successive derivatives of Y, as our ground field and consider our input system as a system over $k\langle Y\rangle$. Even if we do not assume, as it is usual, a differential 0-dimensional situation (the case of r being strictly smaller than m will be also considered), we will first

suppose that the last r equations are "independent" in a suitable natural way defined in Assumption 5. This hypothesis can be dropped, preserving essentially the results, as we show in Appendix A.

Differential algebraic equations systems like (Σ) can be regarded from several points of view: for instance, this kind of systems arises in Control Theory (see, for instance, [18], [16], [19] and [9, Section 4]) or they may also be interpreted as the equations defining the graph of a differential morphism (see [45]). The system (Σ) may be viewed as a family of usual polynomial differential algebraic equations systems where the second member parametrizes the family and takes arbitrary values outside a suitable proper algebraic Zariski closed set (see [53, Section 5.2]). In this last sense we say that the system (Σ) is *generic*.

The Results

Given a system of differential equations like (Σ), 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 $k\langle Y\rangle\{X, U\}$.

In this work we prove the existence of a resolvent representation for the ideal Δ consisting of polynomials which involve derivatives of the variables Y, X and U up to order $2n + 2r$ 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 Theorems 49 and 56 below). The Bézout inequality implies that $\deg(\mathbb{V})$ can always be bounded by $d^{2(n+r)^2}$, where d ia an upper bound for the degrees of the polynomials f_i, $i = 1, \ldots, n$, and g_j, $j = 1, \ldots, r$. Moreover, we show with an example (Example 51 below) that these geometric upper bounds are optimal.

When $k = \mathbb{Q}(t)$, we also 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 1.2 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 61 below). We remark that the upper bound for $\deg(\mathbb{V})$ due to the Bézout 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 classical Zippel-Schwartz zero test (see [63] and [56]) together with the degree upper bounds, found a priori, for the polynomials giving the genericity conditions under which our algorithm works (this can be done without computing the actual polynomials, see Section 1.2).

In order to obtain the results above mentioned, it is crucial the study of the behavior of two well-known discrete invariants associated to the system: the *differentiation index* of the system (Σ) and the *differential Hilbert-Kolchin function* of the ideal Δ. This study leads us to the development of new results on these invariants as collateral products of our methods.

The differentiation index is an important invariant associated to a differential algebraic equations system (usually defined only for first order 0-dimensional systems). There are many different, not always equivalent, definitions of differentiation indices (see for instance [7], [50], [9], [44], [18], [60], [58]). Here we are interested in the so-called *global differentiation index* (see [7, Section 2.2]). Informally speaking, the differentiation index denotes the minimum number of times that the equations of a given differential algebraic system must be differentiated in order to determine the derivatives of the unknowns as (continuous, differential, analytic, etc.) functions of the unknowns themselves (see [7, Definition 2.2.2]), thus obtaining an explicit system. The index represents in some sense a measure of the complexity of the differential algebraic equation system from the point of view of its numerical resolution: for instance, it is closely related to the condition number of the iteration matrix in the implicit Runge-Kutta method (see [7, Theorem 5.4.1]).

In this work we give a precise algebraic definition of the index for differential algebraic equation systems as (Σ), *not necessarily* 0*-dimensional* (see Definition 25 below), by means of certain stationary properties of the rank of suitable Jacobian submatrices developed in Section 2.3 (see also [58]). Another equivalent definition of the index, in terms of a quite natural filtration given by the successive differentiation of the input equations, is implicitly contained in Theorem 26 below. In particular, this last formulation shows that the differentiation index is, also, the number of derivatives of the equations needed to obtain *all* the algebraic relations that any solution of the system must satisfy.

As we have already mentioned, the notion of differentiation index is closely related to the possibility of writing the derivatives of the unknowns in terms of the unknowns themselves. Unfortunately, in general, this cannot be done using only the original equations. For example, even if all the equations have order at most one, as it is our case, this particularly nice situation, which is usually ensured by the Theorem of Implicit Functions, corresponds to those systems whose associated index is 0. However, in the general case, by successive differentiations (as many as the index) we can always obtain such a situation. Evidently, the new explicit system comes out of the frame of the polynomial (or even rational) systems. In our case, we are able to give an implicit but simple polynomial way to describe the system, distinguishing the variables by their interrelations (namely, "free variables", "implicit variables", etc.). Moreover, we can estimate degree and order upper bounds for these equations (Theorem 70) and give an algorithm to compute them (Proposition 73) within the same complexity bounds as the ones described for the resolvent representation.

The Hilbert-Kolchin function of a differential ideal was formally defined for the first time by E. Kolchin in [38, Chapter II] in order to estimate, for each non-negative integer i, the degree of freeness of the first i-derivatives of the unknowns modulo the relations induced by the input equation system (see Section 1.1.2 below for a precise definition). This function is closely related to other two discrete invariants of the ideal, its *differential dimension* and its *order*. These invariants were already considered in the work of

J. Ritt, [52] and [51], and correspond, respectively, to the number of arbitrary conditions and the number of initial conditions in the set of solutions of the differential system associated to the ideal.

As it happens for the classical Hilbert function associated to homogeneous polynomial ideals (see for instance [1, Chapter 11]), the Hilbert-Kolchin function becomes a well defined polynomial for sufficiently big arguments i and, in the ordinary differential setting, this polynomial is extremely simple since its degree is at most 1. The *regularity* of the Hilbert-Kolchin function is defined to be the first non-negative integer from where the function and the polynomial coincide. It is well known that this regularity can be *exactly* described in terms of the orders of the elements in a characteristic set associated to any orderly ranking (see the proof of [38, Chapter II, Section 12, Theorem 6] or [10, Theorem 3.3]). Here (see Theorem 28 below) we show that the regularity of the Hilbert-Kolchin function for the system (Σ) over the field $k\langle Y\rangle$ is always 0; in other words, the Hilbert-Kolchin function and the associated polynomial coincide for all integers i.

We also show a probabilistic algorithm for the computation of the *differentiation index* of the system (Σ) and the *differential Hilbert-Kolchin function* of the ideal Δ within complexity polynomial in n, m, r, d and linear in L (see Theorem 37). This algorithm works by simple computation and comparison of ranks of certain Jacobian matrices. This result is a natural extension to a positive-dimensional situation of the algorithm found in [45] for the computation of the Hilbert-Kolchin function.

Our approach

Our overall strategy consists in translating a differential (non-noetherian) problem into an algebraic (noetherian) one and in this sense Theorem 26 below plays a fundamental role. In a first step towards the computation of the resolvent representation of the ideal Δ, we compute a differential transcendence basis of the differential field extension induced by our system in order to turn to a 0-dimensional differential situation. Then, we give an effective and algorithmic version of Seidenberg's proof of the existence of a primitive element (see [59]) 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 [30] and [55] 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 [52]. Ritt's treatment of the subject, as well as its subsequent generalizations (see, [13], [12]), are based on rewriting techniques, namely Gröbner bases and characteristic sets (see [4], [5], [6]). Even though a single exponential complexity upper bound was proved in [23] 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 [53] seem to yield single exponential complexity bounds for a probabilistic algorithm computing a resolvent representation (see [12]) for the specific systems we consider.

We point out that, unlike the previous methods, 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 Section 51). Complexity bounds depending on this kind of parameters appeared before in several algebraic elimination procedures (see for instance [27], [30], [28], [43]). 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 of the rewriting procedure presented in [53, Theorem 28] that, when applied to our particular systems, can be estimated in $(n+r)^{O((n+m)(n+r))}d^{O((n+m)^3(n+r)^3)}$.

Structure of the thesis

This thesis is divided in four chapters.

In the first part of Chapter 1 we recall some basic notions and results from Differential Algebra needed throughout the entire work and in the second part we present the algorithmic model we will adopt.

At the beginning of Chapter 2, we describe once more the systems of differential equations that we will consider and we show the first elementary facts about them, their associated differential ideals and the differential field extensions related to these ideals. In this same chapter there is a detailed study of the behavior of a sequence of integer numbers which are defined in relation to the rank of certain suitable Jacobian submatrices of the input equations and their derivatives. This sequence leads us to a precise and purely algebraic definition of the differentiation index.

We start Chapter 3 by showing a relation between the index and the manifold of constraints of the system in Theorem 26, which, as we have already said, gives an alternative description of the differentiation index and provides the key result for the translation of differential problems into an algebraic "noetherian" context. The remaining parts of this chapter are concerned with the computation of the differential Hilbert-Kolchin function of the ideal Δ associated to the system (Σ) and of a differential transcendence basis of the induced differential field extension. Actually, in this chapter, we show the existence and computation of a differential transcendence basis verifying a particular "good localization" property that will save us extra work in the search of the resolvent representation and that will become necessary for the alternative description of the system (Σ) derived from the properties of the differentiation index.

Finally, Chapter 4 is devoted to the existence and computation of the resolvent representation of the ideal Δ and is divided in three sections. In Section 4.1 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 4.2 is devoted to the algorithmic computation of resolvent representations and in Section 4.3 there is a study of the generalization to higher order systems of differential equations of this computation.

In addition, this work contains three appendices.

In Appendix A we present a slight generalization of the algorithmic results stated in the last chapter dropping the hypothesis of "independence" of the last r equation of the system (Σ); that is, dropping Assumption 5, introduced in Section 2.1.

Appendix B deals with the alternative presentation of the system (Σ) in the spirit of the Theorem of Implicit Functions, deduced from the results obtained on the differentiation index, together with an algorithm to compute it.

In Appendix C we present an improvement over the degree bounds obtained in Chapter 4 for the classical particular but important class of explicit square differential algebraic equation systems, with differentiation index 0, of the form $\dot{X} = F(X)$ (where F is polynomial map or the n-dimensional space over a differential field, not necessarily of constants).

Chapter 1

Preliminaries

In this chapter we will introduce some basic notions from Differential Algebra that will be needed throughout the whole work and we will also give a brief presentation of the algorithmic model and data structure we will be using.

1.1 Basic differential algebra

We give here a very brief summary of some basic notions and results from Differential Algebra. This does not constitute an exhaustive exposition on the subject, we rather concentrate on the concepts we need for our work. A more complete and detailed account on this topic can be found in [52] and [38].

1.1.1 Differential rings and fields

Before we begin this section, let us establish the following notation: we will write $\mathbb{N}$ for the set of natural numbers $\{1, 2, \ldots\}$ meanwhile $\mathbb{N}_0$ will be $\mathbb{N} \cup \{0\}$.
We now recall some definitions and basic facts about differential rings and fields.
A *derivation* δ on a ring $\mathcal{A}$ is an additive map $\delta : \mathcal{A} \to \mathcal{A}$ satisfying the Leibniz rule

$$\delta(a \cdot b) = \delta(a) \cdot b + a \cdot \delta(b) \quad \text{for all} \quad a, b \in \mathcal{A}.$$

A ring (respectively a field) equipped with (at least) a derivation δ is called a *differential ring* (respectively a *differential field*).
We 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 $i \geq 2$, $\delta^i(\eta)$ will be denoted by $\eta^{(i)}$.
If $(\mathcal{A}, \delta_{\mathcal{A}})$ and $(\mathcal{B}, \delta_{\mathcal{B}})$ are two differential rings, a ring homomorphism $f : \mathcal{A} \to \mathcal{B}$ is a differential homomorphism if $\delta_{\mathcal{B}}(f(a)) = f(\delta_{\mathcal{A}}(a))$ for all $a \in \mathcal{A}$.

An ideal $\mathcal{I}$ of a differential ring $\mathcal{A}$ is a *differential ideal* if

$$\delta(a) \in \mathcal{I} \quad \text{for every} \quad a \in \mathcal{I}.$$

If Ξ is a subset of $\mathcal{A}$, the differential ideal generated by Ξ (that is, the minimal differential ideal of $\mathcal{A}$ containing Ξ) will be denoted by $[\Xi]$.

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

Let $\mathcal{E} \hookrightarrow \mathcal{G}$ be a differential field extension. An element $\zeta \in \mathcal{G}$ is said to be *differentially algebraic over* $\mathcal{E}$ if the family of its derivatives $\{\zeta^{(l)}\}_{l \in \mathbb{N}_0}$ (where $\mathbb{N}_0$ is the set $\{0, 1, 2, \ldots\}$) is algebraically dependent over $\mathcal{E}$; otherwise, it is said to be *differentially transcendental over* $\mathcal{E}$. The differential extension $\mathcal{E} \hookrightarrow \mathcal{G}$ is said to be *differentially algebraic* if every element of $\mathcal{G}$ is differentially algebraic over $\mathcal{E}$.

Given a subset Ξ of $\mathcal{G}$, $\mathcal{E}\langle\Xi\rangle$ will denote the minimal differential subfield of $\mathcal{G}$ containing $\mathcal{E}$ and Ξ. A subset Ξ of $\mathcal{G}$ is *differentially algebraically independent over* $\mathcal{E}$ if the set $\{\zeta^{(l)} : \zeta \in \Xi,\ l \in \mathbb{N}_0\}$ is algebraically independent over $\mathcal{E}$, and it is called a *differential transcendence basis of* $\mathcal{E} \hookrightarrow \mathcal{G}$ if it is a minimal subset of $\mathcal{G}$ such that the differential extension $\mathcal{E}\langle\Xi\rangle \hookrightarrow \mathcal{G}$ is differentially algebraic.

All the differential transcendence bases of a differential extension $\mathcal{E} \hookrightarrow \mathcal{G}$ have the same cardinality ([38, Ch. II, Sec. 9, Th. 4]), which is called the *differential transcendence degree* of $\mathcal{E} \hookrightarrow \mathcal{G}$ and will be denoted by $\mathrm{difftrdeg}_{\mathcal{E}}(\mathcal{G})$.

Given a differential field $(\mathcal{E}, \delta)$, we introduce the *ring of differential polynomials in the indeterminates* $Z_1, \ldots, Z_\alpha$ *over* $\mathcal{E}$, $\mathcal{E}\{Z_1, \ldots, Z_\alpha\}$, by considering the polynomial ring over $\mathcal{E}$ in the infinite set of indeterminates $\Theta Z := \{Z_j^{(i)}, i \in \mathbb{N}_0,\ 1 \leq j \leq \alpha\}$ and extending the derivation of $\mathcal{E}$ by setting $\delta(Z_j^{(i)}) = Z_j^{(i+1)}$ (for simplicity $\delta(Z_j) := \dot{Z}_j$).

We will write $Z := \{Z_1, \ldots, Z_\alpha\}$ and, for every $i \in \mathbb{N}$, $Z^{(i)} := \{Z_1^{(i)}, \ldots, Z_\alpha^{(i)}\}$.

Thus, for any differential polynomial p lying in a polynomial differential ring $\mathcal{E}\{Z\}$ we define recursively the *l-th derivative* $p^{(l)}$ as follows:

$$\begin{aligned} p^{(0)} &:= p, \\ p^{(l)} &:= \delta(p^{(l-1)}) + \textstyle\sum_{i,j} \dfrac{\partial p^{(l-1)}}{\partial Z_j^{(i)}} Z_j^{(i+1)}, \qquad \text{for } l \geq 1, \end{aligned}$$

where $\delta(p^{(l-1)})$ denotes the polynomial obtained from $p^{(l-1)}$ by applying the derivative δ to all its coefficients (if $\mathcal{E}$ is a field of constants, that is, there are no elements in $\mathcal{E}$ whose derivatives are not zero, this term is always zero).

For a polynomial $p \in \mathcal{E}\{Z\}$, we define the *order of* p *with respect to the variable* Z_j as $\mathrm{ord}(p, Z_j) := \max\{i \in \mathbb{N}_0 : Z_j^{(i)} \text{ appears in } p\}$, and the *order of* p as

$$\mathrm{ord}(p) := \max\{\mathrm{ord}(p, Z_j) : 1 \leq j \leq n\},$$

the maximum order of derivation appearing in p.

If $\mathcal{I} \subset \mathcal{E}\{X\}$ is a prime differential ideal, a subset $W \subset Z$ is a *maximally independent set modulo* $\mathcal{I}$ if

$$\mathcal{I} \cap \mathcal{E}\{W\} = 0 \qquad \text{and} \qquad \mathcal{I} \cap \mathcal{E}\{W, Z_j\} \neq 0 \quad \text{for all} \quad Z_j \notin W.$$

Note that, if we denote by $\text{Frac}(\mathcal{E}\{Z\}/\mathcal{I})$ the fraction field of the differential integral domain $\mathcal{E}\{Z\}/\mathcal{I}$, a maximally independent set modulo $\mathcal{I}$ is a differential transcendence basis of the differential extension $\mathcal{E} \hookrightarrow \text{Frac}(\mathcal{E}\{Z\}/\mathcal{I})$. Thus, we define the *differential dimension of the ideal* $\mathcal{I}$, denoted by $\text{diffdim}_{\mathcal{E}}(\mathcal{I})$, as the transcendence degree of this extension or, equivalently, as the cardinality of a maximally independent set modulo $\mathcal{I}$.

Since we will work only with differential field extensions that are fields of fractions of quotients of certain polynomial rings by a differential prime ideal, we will talk about "differential transcendence basis" even if we only mean maximally independent set.

1.1.2 Differential Hilbert-Kolchin function

In this Section we will associate to a prime differential ideal $\mathcal{I} \subset \mathcal{E}\{Z\}$ a numerical function, the differential Hilbert-Kolchin function, that reflects some of the properties of the ideal. As it happens with the classical Hilbert function associated to homogeneous polynomial ideals (see for instance [1, Chapter 11]), this function becomes a well defined polynomial for sufficiently big arguments. Moreover, in the ordinary differential setting, this polynomial has degree at most 1. This polynomial carries certain invariants of the ideals with it.

The differential Hilbert-Kolchin function of a prime differential was introduced in [38, Chapter II] and it provides a way of measuring, for each non-negative integer i, the degree of freeness of the first i-derivatives of the unknowns modulo the relations induced by the system of equations given by equaling to zero the generators of the ideal.

Definition 1. *Let $\mathcal{E}$ be a differential field and let $\mathcal{I}$ be a prime differential ideal of $\mathcal{E}\{Z\}$. The* differential Hilbert-Kolchin function *(or differential transcendence function) $\mathcal{H}_{\mathcal{I},\mathcal{E}} : \mathbb{N}_0 \to \mathbb{N}_0$ of $\mathcal{I}$ with respect to the field $\mathcal{E}$ is defined as*

$$\mathcal{H}_{\mathcal{I},\mathcal{E}}(i) := trdeg_{\mathcal{E}} Frac(\mathcal{E}[Z, \ldots, Z^{(i)}]/(\mathcal{I} \cap \mathcal{E}[Z, \ldots, Z^{(i)}])),$$

the transcendence degree of the field extension $\mathcal{E} \hookrightarrow Frac(\mathcal{E}[Z, \ldots, Z^{(i)}]/(\mathcal{I} \cap \mathcal{E}[Z, \ldots, Z^{(i)}]))$.

As we have already mentioned, the behavior of this function resembles that of the Hilbert function from algebraic geometry: for $i \in \mathbb{Z}$ big enough we have

$$\mathcal{H}_{\mathcal{I},\mathcal{E}}(i) = \text{diffdim}(\mathcal{I})\,(i+1) + o$$

where o, the independent coefficient of this polynomial, is called the *order of the ideal* $\mathcal{I}$ and denoted by $\mathrm{ord}_{\mathcal{E}}(\mathcal{I})$. In other words, for i big enough the function $\mathcal{H}$ becomes a polynomial of degree one and the differential dimension of the ideal is its main coefficient. This polynomial is called the *differential Hilbert-Kolchin polynomial* of the ideal $\mathcal{I}$.

For a proof of this result we refer to [38, Ch. II, Sec. 12, Th. 6] from where we can also infer that this equality holds for every $i \geq \mathrm{ord}_{\mathcal{E}}(\mathcal{I})$.

If the ideal $\mathcal{I}$ is the differential ideal generated by a set Ξ and we consider the differential system of equations $\Xi = 0$, then $\mathrm{diffdim}(\mathcal{I})$ is the number of variables that can be given any arbitrary value for any order of derivation meanwhile $\mathrm{ord}_{\mathcal{E}}(\mathcal{I})$ is the number of initial conditions that can be arbitrarily fixed on the "tied" variables up to a certain order of derivation.

It is clear from their definitions that, once the ground field has been fixed, the differential Hilbert-Kolchin function and the differential dimension are invariants of the ideal $\mathcal{I}$ and thus, the order of the ideal is also an invariant. However all these notions depend strongly on the considered ground field, as the following example shows: let $\mathcal{I}$ be the differential ideal $[\dot{X}_1 - Y_1]$, we can see it as an ideal either in $\mathbb{Q}\{X_1, Y_1\}$ or in $\mathbb{Q}\langle X_1\rangle\{Y_1\}$ or even in $\mathbb{Q}\langle Y_1\rangle\{X_1\}$ and, in each case we have:

$$\begin{array}{llll}
\mathcal{H}_{\mathcal{I},\mathbb{Q}}(i) = (i+1)+1, & \mathrm{ord}_{\mathbb{Q}}(\mathcal{I}) = 1 & \text{and} & \mathrm{dimdiff}_{\mathbb{Q}}(\mathcal{I}) = 1; \\
\mathcal{H}_{\mathcal{I},\mathbb{Q}\langle X_1\rangle}(i) = 0, & \mathrm{ord}_{\mathbb{Q}\langle X_1\rangle}(\mathcal{I}) = 0 & \text{and} & \mathrm{dimdiff}_{\mathbb{Q}\langle X_1\rangle}(\mathcal{I}) = 0; \\
\mathcal{H}_{\mathcal{I},\mathbb{Q}\langle Y_1\rangle}(i) = 1, & \mathrm{ord}_{\mathbb{Q}\langle Y_1\rangle}(\mathcal{I}) = 1 & \text{and} & \mathrm{dimdiff}_{\mathbb{Q}\langle Y_1\rangle}(\mathcal{I}) = 0.
\end{array}$$

In this example $\{X_1\}$ and $\{Y_1\}$ are two possible differential transcendence basis of the field extension $\mathbb{Q} \hookrightarrow \mathrm{Frac}(\mathbb{Q}\{X_1, Y_1\}/\mathcal{I})$. In either case, if we add to the ground field a differential transcendence basis, the differential dimension of the ideal is 0, as expected, but the order of the ideal changes depending on the choice of the basis. In Chapter 3 we will show how to find a differential transcendence basis such that, once added to the ground field, the order of the ideal is not changed. This way of choosing a differential transcendence basis will avoid us computations in Chapter 4.

1.2 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.

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 given 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 [63] and [56]), which states that, under the previous hypotheses, $\text{Prob}(F(a) = 0) \leq \deg(F)/N$, where $\deg(F)$ is the total degree of the polynomial F. 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 *straight-line program without divisions* (or *slp*) 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 us to evaluate f at any given point in $\mathbb{Q}^n$. Each of the instructions in this program is an addition, a subtraction or a multiplication between two previously computed 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 [8] (see also [32]).

Let us observe that, from a vector of coefficients of a polynomial f it is easy to obtain a straight-line program encoding f. The length of this straight-line program is bounded by the number of coefficients of the polynomial (but, in fact, it can be significatively smaller). Conversely, from a straight-line program of length L encoding an n-variate polynomial f and a positive integer d which is an upper bound for its degree, the usual representation of the polynomial as a vector of coefficients can be computed by means of a straightforward procedure (see, for instance, [8] Lemma 21.25) within complexity $d^{o(n)}L$. This implies that our algorithm can be adapted so that it could be applied even when the input family is represented by vectors of coefficients, and also that the standard representation of the output by coefficients can be obtained with a controlled increase of complexity. However, the use of straight-line programs in the intermediate computations of the algorithms is crucial in order to avoid a complexity explosion.

Chapter 2

Differential algebraic equation systems

The extension of the seminal notions and results given by R.E. Kalman in [37] for linear models to nonlinear systems constitutes one of the mainstream fields of research in differential control theory. In Kalman's work we can find a complete description of the properties of the explicit linear models of the type:

$$\begin{cases} \dot{X} &= AX + BU \\ Y &= CX \end{cases}$$

where A, B, and C are constant matrices and X and U are vectors of unknowns.
In this work we will consider systems of equations that are given as differential polynomials (differential algebraic systems of equations) and we will concentrate on a particular class of these systems of equations that are a clear generalization of those studied by Kalman. Before we introduce them we will need the following notation that we will use throughout the paper:

Notation 2. *Let K be a differential field and let $Z := \{Z_1, \ldots, Z_\alpha\}$ be a differentially algebraically independent set over K.*
For every $i \geq 0$, $Z^{(i)}$ 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 $i \geq 0$, $Z^{[i]}$ will denote the string of elements $Z, \dot{Z}, \ldots, Z^{(i)}$.
We will use a similar notation for differential polynomials:
if $H := \{H_1, \ldots, H_\beta\} \subset K\{Z\}$, for every $i \geq 0$, 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 $\dot{H} = H^{(1)}$.

We consider then the following system of differential algebraic equations:

$$\begin{cases} \dot{X} &= F(X, U) \\ Y &= G(X, U, \dot{U}) \end{cases}$$

where $X := \{X_1, \ldots, X_n\}$ and $U := \{U_1, \ldots, U_m\}$ are two sets of variables (the unknowns) and $Y := \{Y_1, \ldots, Y_r\}$ is another set of variables that we consider as parameters. From the control theory point of

view, the polynomials $f_1, \ldots, f_n$ describe the physical constraints between the state variables X and the control variables U meanwhile the variables Y are considered as the output of the desired constraints.
Even though these are not exactly the systems one usually finds in the bibliography on the subject of control theory, we work with them because almost all the classical systems can be viewed as particular cases. For example, if the polynomials G do not depend on $\dot{U}$ we have the systems considered in [57] and letting $n = 0$ we have the systems studied in [18] and [45].
These systems also appear in the classical theory of *higher order differential equations* when transforming them into first order systems considering the derivatives of the unknowns as new variables. Thus, using this well-known method, we will be able to find a resolvent representation for higher order differential systems (see Chapter 4, Section 4.3 below).

2.1 Definitions and basic properties

We now give a precise description of the systems we will be considering and later on we study the first basic properties concerning them.
Let k be a differential field of characteristic 0 (for instance $k = \mathbb{Q}$ or $k = \mathbb{Q}(t)$ with the usual derivation) 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 $k[X, U]$, r a non-negative integer, $r \leq m$, and $g_1, \ldots g_r$ polynomials in $k[X, U, \dot{U}]$. We introduce a new family of differential indeterminates $Y := \{Y_1, \ldots, Y_r\}$ (the parameters) over the differential fraction field $k\langle X, U\rangle$ and the "generic" (or parametrized) differential system

$$(\Sigma) := \begin{cases} \dot{X}_1 &= f_1(X, U) \\ &\vdots \\ \dot{X}_n &= f_n(X, U) \\ Y_1 &= g_1(X, U, \dot{U}) \\ &\vdots \\ Y_r &= g_r(X, U, \dot{U}) \end{cases} \tag{2.1}$$

We will be mainly concerned with the computation of some discrete invariants of this system (essentially, the differential Hilbert-Kolchin function of the associated ideal, introduced in Subsection 1.1.2, and the differentiation index of the system, defined in Section 2.3) and of an alternative presentation of this system: the resolvent representation, that is, the parametrization of the zeros of the system by the general zeros of a single irreducible polynomial (see Definition 44 below).
In order to obtain information about this system we start with the study of some basic properties of the

differential ideal associated to it. Set

$$\begin{aligned} F_i &:= f_i - \dot{X}_i \in k[X, \dot{X}, U] \qquad i = 1, \ldots, n, \\ G_j &:= g_j - Y_j \in k[Y, X, U, \dot{U}] \qquad j = 1, \ldots, r, \end{aligned}$$

and let

$$[F, G] \subset k\{Y, X, U\}$$

be the differential ideal generated by set of polynomials $F := F_1, \ldots, F_n$ and $G := G_1, \ldots, G_r$.
Since the differential ring $k\{Y, X, U\}$ is (algebraically) non-noetherian there is no hope of finding a finite sets of generators for the ideal $[F, G]$ so we are forced to establish some kind of relation between this ideal and several finitely generated algebraic ideals in their corresponding polynomial ring: for every $l \in \mathbb{N}$, we consider the ideal $(F^{[l-1]}, G^{[l-1]}) \subset k[Y^{[l-1]}, X^{[l]}, U^{[l]}]$ generated by the $(n + r)l$ polynomials $F_1, \ldots, F_n, G_1, \ldots, G_r, \ldots, F_1^{(l-1)}, \ldots, F_n^{(l-1)}, G_1^{(l-1)}, \ldots, G_r^{(l-1)}$.
The following notation will be useful in the sequel:

Notation 3. *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 by substituting $X_h^{(l)}$ by $\tilde{f}_h^{(l-1)}$ $(1 \le h \le n,\ 1 \le l \le k)$ in the polynomials $f_i^{(k)}(X^{[k]}, U^{[k]})$.
In a similar way, we define polynomials $\tilde{g}_j^{(k)}(X, U^{[k+1]})$ by replacing $X_h^{(l)}$ by $\tilde{f}_h^{(l-1)}$ $(1 \le h \le n,\ 1 \le l \le k)$ in the polynomials $g_j^{(k)}(X^{[k]}, U^{[k]})$.

Due to the particular structure of the polynomials F, G and their derivatives, it is easy to characterize the quotients $k[Y^{[l-1]}, X^{[l]}, U^{[l]}]/(F^{[l-1]}, G^{[l-1]})$, for $l \in \mathbb{N}$, and $k\{Y, X, U\}/[F, G]$:

Remark 4. *Let l, i, s, t be positive integers with $i \le l$, $1 \le s \le n$ and $1 \le t \le r$, and let $\mathfrak{p}_{i,s}$ and $\mathfrak{q}_{i,t}$ be the ideals of $k[Y^{[l-1]}, X^{[l]}, U^{[l]}]$ defined as*

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

In the quotient ring $k[Y^{[l-1]}, X^{[l]}, U^{[l]}]/\mathfrak{p}_{i,s}$, we have that

$$\begin{aligned} X_h^{(j)} &= \tilde{f}_h^{(j-1)} \qquad \text{for } j = 1, \ldots i-1,\ h = 1, \ldots n \\ &\qquad\qquad\qquad \text{and } j = i,\ h = 1, \ldots, s \\ Y_d^{(j)} &= \tilde{g}_d^{(j)} \qquad \text{for } j = 0, \ldots, i-2,\ d = 1, \ldots, r \end{aligned}$$

and similar identities hold in $k[Y^{[l-1]}, X^{[l]}, U^{[l]}]/\mathfrak{q}_{i,t}$. Therefore,

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

and so, $\mathfrak{p}_{i,s}$ *and* $\mathfrak{q}_{i,t}$ *are prime ideals of* $k[Y^{[l-1]}, X^{[l]}, U^{[l]}]$.
In particular, $(F^{[l-1]}, G^{[l-1]}) = \mathfrak{q}_{l,r}$ *is prime (this is a well-known result which holds for any ideal describing the graph of an application, see, for instance [48, p.33]),*

$$k[Y^{[l-1]}, X^{[l]}, U^{[l]}]/(F^{[l-1]}, G^{[l-1]}) \simeq k[X, U^{[l]}]$$

and hence, its Krull dimension is $n + (l+1)m$.
The same arguments can be applied to the differential ideal $[F, G] \subset k\{Y, X, U\}$ *in order to show that it is a prime ideal and that the differential ring* $k\{Y, X, U\}/[F, G]$ *is isomorphic to the differential ring* $k[X]\{U\}$ *with the derivation induced by* $\dot{X}_j := f_j(X, U)$ *and* $X_h^{(l)} = \tilde{f}_h^{(l-1)}$ *where* $\tilde{f}_h^{(l-1)}$ *are the polynomials introduced in Notation 3.*
Using once more similar arguments, it can also be shown that $[f_1 - \dot{X}_1, \ldots, f_n - \dot{X}_n]$ *is a prime differential ideal of* $k\{Y, X, U\}$.

For technical reasons, we will make the following assumption for the time being. In Appendix A we will show how to remove it.

Assumption 5. *The polynomials* $g_1, \ldots, g_r$ *are differentially algebraically independent as elements of the ring* $k\{Y, X, U\}/[f_1 - \dot{X}_1, \ldots, f_n - \dot{X}_n]$ *over the field* k.

This assumption is equivalent to the fact that the set of variables Y is differentially algebraically independent modulo $[F, G]$ (see also Proposition 7 below). It also allows us to regard the system (2.1) as a family of differential-algebraic polynomial equations where the Y's parametrize this family and take arbitrary values outside a suitable proper algebraic Zariski closed set (in this sense, we say that the system is *generic*). It seems, then, quite reasonable to regard these variables as elements of an extended ground field. Thus, we introduce the following

Notation 6. *Let*

$$\Delta := [F, G] \subset k\langle Y\rangle\{X, U\}$$

be the differential ideal generated by the polynomials F, G *in the differential polynomial ring* $k\langle Y\rangle\{X, U\}$.
Also, for any $l \geq 0$, *let* A_l *be the polynomial ring* $k\langle Y\rangle[X^{[l]}, U^{[l]}]$ *and*

$$\Delta_l := (F^{[l-1]}, G^{[l-1]}) \subset A_l \quad \forall\, l \geq 1 \qquad \textit{and} \quad \Delta_0 = 0 \in A_0.$$

The ideals introduce in Notation 6 continue to be prime when considered as ideals over the polynomial with coefficients in $k\langle Y\rangle$:

Proposition 7. *Under the same notations and assumptions as in Remark 4, we have that:*

- $k[Y^{[l-1]}] \cap \mathfrak{p}_{i,s} = 0$ *and the extended ideals* $k\langle Y\rangle \otimes \mathfrak{p}_{i,s}$ *are prime ideals of the ring* A_l,
- $k[Y^{[l-1]}] \cap \mathfrak{q}_{i,t} = 0$ *and the extended ideals* $k\langle Y\rangle \otimes \mathfrak{q}_{i,t}$ *are prime ideals of the ring* A_l

(here, the tensor product denotes scalar extension).
In particular, $\Delta_l = k\langle Y\rangle \otimes \mathfrak{q}_{l,r}$ *is a prime ideal of* A_l *and there is a natural ring inclusion*

$$k[X, U^{[l]}] \simeq k[Y^{[l-1]}, X^{[l]}, U^{[l]}]/(F^{[l-1]}, G^{[l-1]}) \hookrightarrow A_l/\Delta_l.$$

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

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

and so, the differential independence of the polynomials $g_1, \ldots, g_r$ in the differential extension

$$k \hookrightarrow \mathrm{Frac}(k\{Y, X, U\}/[F])$$

(Assumption 5) implies that $p = 0$.
Therefore, the extensions of the prime ideals $\mathfrak{p}_{i,s}$ and $\mathfrak{q}_{i,t}$ to $k(Y^{[l-1]})[X^{[l]}, U^{[l]}]$ are also prime ideals; and the same happens to their extensions to the ring A_l, since the $Y^{(j)}$, with $j \ge l$, are transcendental over $k(Y^{[l-1]})[X^{[l]}, U^{[l]}]$.
Finally, it remains to prove the existence of a natural ring inclusion

$$k[Y^{[l-1]}, X^{[l]}, U^{[l]}]/(F^{[l-1]}, G^{[l-1]}) \hookrightarrow A_l/\Delta_l.$$

Suppose that there is a polynomial $q(Y^{[l-1]}, X^{[l]}, U^{[l]}) \in k[Y^{[l-1]}, X^{[l]}, U^{[l]}] \cap \Delta_l$. Then, there exist polynomials $\alpha_{q,h}, \beta_{j,k} \in A_l$ satisfying

$$q(Y^{[l-1]}, X^{[l]}, U^{[l]}) = \sum_{h=0}^{l-1}\sum_{q=1}^{n} \alpha_{q,h}\, F_q^{(h)} + \sum_{k=0}^{l-1}\sum_{j=1}^{r} \beta_{j,k}\, G_j^{(k)}.$$

The variables $Y_k^{(t)}$ with $t \ge l$ appear only in the polynomials $\alpha_{q,h}$ and $\beta_{j,k}$ and we can evaluate them into suitable values in the field k so that the denominators of the coefficients of this polynomials do not vanish. After doing this, we obtain that $q(Y^{[l-1]}, X^{[l]}, U^{[l]}) \in (F^{[l-1]}, G^{[l-1]})$ and the inclusion is proved. ■

Corollary 8. *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 A_l and the Krull dimension of the ideal $\Delta_l \subset A_l$ is $(l+1)(m-r)+n+r$.

Proof. The result follows easily from the fact that the polynomial $F^{[l-1]}, G^{[l-1]}$ generate a prime ideal in $k[Y^{[l-1]}, X^{[l]}, U^{[l]}]$ (Remark 4). This enables the straightforward computation of the dimensions of the quotient rings $k[Y^{[l-1]}, X^{[l]}, U^{[l]}]/\mathfrak{p}_{i,s}$ and $k[Y^{[l-1]}, X^{[l]}, U^{[l]}]/\mathfrak{q}_{i,t}$ for every $i \leq l$, $1 \leq s \leq n$ and $1 \leq t \leq r$, which turn to drop successively by one when adding each polynomial of the sequence to the ideal generator set. Due to Proposition 7, the same happens for the corresponding prime ideals in A_l, which implies that the Krull dimension of the ideal Δ_l is equal to the difference between the number of variables and the number of equations, that is $(l+1)(n+m) - l(n+r) = (l+1)(m-r)+n+r$. ■

Proposition 7 has a differential (not finitely generated) analogue version:

Proposition 9. *Let $[F, G] \subset k\{Y, X, U\}$ as before. Then $[F, G] \cap k\{Y\} = 0$ and the differential ideal $\Delta = [F, G] \subset k\langle Y\rangle\{X, U\}$ is prime.* ■

According to Remark 4 and Proposition 9, $[F, G] \subset k\{Y, X, U\}$ and $\Delta \subset k\langle Y\rangle\{X, U\}$ are both prime differential ideals and they have the same fraction field:

Notation 10. *Let $\mathcal{F}$ denote the common fraction field of the integral domains $k\{Y, X, U\}/[F, G]$ and $k\langle Y\rangle\{X, U\}/\Delta$.*

Assumption 5 and the previous result allow us now to compute the differential transcendence degree of the differential field extension $k\langle Y\rangle \hookrightarrow \mathcal{F}$ which, by definition, is the differential dimension of the ideal Δ:

Proposition 11. *The differential transcendence degree of the differential field extension*

$$k\langle Y\rangle \hookrightarrow \mathcal{F} \text{ is } m - r.$$

Proof. Due to Remark 4, 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,

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

On the other hand, we have that $\operatorname{difftrdeg}_k(k\langle Y\rangle) = r$.

Now, applying [38, Ch. II, Sec. 9, Cor. 2] to the tower of differential fields

$$\begin{array}{ccc} \mathcal{F} & \simeq & k(X)\langle U\rangle \\ | & & | \\ k\langle Y\rangle & \simeq & k\langle \widetilde{g_1}, \ldots, \widetilde{g_r}\rangle \\ | & & | \\ k & = & k \end{array}$$

we conclude that $\mathrm{difftrdeg}_{k\langle Y\rangle}(\mathcal{F}) = m - r$. ■

2.2 Associated Jacobian sub-matrices

We introduce now a family of Jacobian matrices and sub-matrices that appear in association to the main system (2.1). These matrices hide much more information about the system than what meets the eye and we try here to unveil some of it (see [15] for a generalization of these results to higher order differential systems).

For the sake of simplicity, and if no confusion arises, we will, in the sequel, denote in the same way a differential polynomial p in $k\langle Y\rangle\{X, U\}$, its class in the factor ring $k\langle Y\rangle\{X, U\}/\Delta$ and the image in $k(X)\langle U\rangle$ of this class by the isomorphism mentioned in Remark 4, respectively. Similarly, $\dot{p}$ will denote either the derivative of p in $k\langle Y\rangle\{X, U\}$ or its derivative as an element in $k(X)\langle U\rangle$.

We start by pointing out a basic fact which follows from the results of the previous section and that we will use several times later:

Remark 12. *Let $l \in \mathbb{N}$ be an arbitrary positive integer. Set $J_l \in k[X^{[l]}, U^{[l]}]^{l(n+r)\times(l+1)(n+m)}$ for the Jacobian matrix of the polynomials $F^{[l-1]}, G^{[l-1]}$ with respect to the variables $X^{[l]}, U^{[l]}$.*

Let $\mathfrak{J}_l \in k(X)\langle U\rangle^{l(n+r)\times(l+1)(n+m)}$ be the matrix with entries in $k[X, U^{[l]}]$ which is obtained by substituting $X_j^{(k)} = \tilde{f}_j^{(k-1)}$ (see Notation 3) for $j = 1, \ldots, n$ and $1 \leq k \leq l$, in the entries of the matrix J_l.

Then, the matrix $\mathfrak{J}_l \in k(X)\langle U\rangle^{l(n+r)\times(l+1)(n+m)}$ has full row rank.

Proof. From Proposition 7 and Corollary 8 the polynomials $F^{[l-1]}, G^{[l-1]}$ form a regular sequence in the ring A_l generating a prime ideal Δ_l. The Jacobian criterion in the generic point of the prime ideal Δ_l implies that the Jacobian matrix $\mathfrak{J}_l$ has full row rank over the ring A_l/Δ_l (see [42, Ch. VI, §1, Theorem 1.15]). Since the entries of this matrix belong to the ring $k[X^{[l]}, U^{[l]}] \subset k[Y^{[l-1]}, X^{[l]}, U^{[l]}]$, it has also full row rank if considered over the integral ring $k[Y^{[l-1]}, X^{[l]}, U^{[l]}]/(F^{[l-1]}, G^{[l-1]}) \hookrightarrow A_l/\Delta_l$. The Remark follows from the natural inclusion $k[Y^{[l-1]}, X^{[l]}, U^{[l]}]/(F^{[l-1]}, G^{[l-1]}) \hookrightarrow k(X) < U >$. ■

For the considered differential system (2.1), we introduce a family of sub-matrices constructed from the (infinite) Jacobian matrix associated to the (infinitely many) polynomials $F^{(l)}$ and $G^{(l)}$ with respect to the (infinitely many) variables $X^{(j)}$ and $U^{(j)}$ as follows:

Definition 13. *For each $k \in \mathbb{N}$ and $i \in \mathbb{N}_0$ let $J_{k,i} \in k\langle Y\rangle\{X,U\}^{k(n+r)\times k(n+m)}$ be the matrix defined as:*

$$J_{k,i} := \begin{pmatrix} \frac{\partial F^{(i)}}{\partial X^{(i+1)}} & \frac{\partial F^{(i)}}{\partial U^{(i+1)}} & 0 & 0 & \cdots & 0 & 0 \\ \frac{\partial G^{(i)}}{\partial X^{(i+1)}} & \frac{\partial G^{(i)}}{\partial U^{(i+1)}} & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{\partial F^{(i+k-1)}}{\partial X^{(i+1)}} & \frac{\partial F^{(i+k-1)}}{\partial U^{(i+1)}} & \frac{\partial F^{(i+k-1)}}{\partial X^{(i+2)}} & \frac{\partial F^{(i+k-1)}}{\partial U^{(i+2)}} & \cdots & \frac{\partial F^{(i+k-1)}}{\partial X^{(i+k)}} & \frac{\partial F^{(i+k-1)}}{\partial U^{(i+k)}} \\ \frac{\partial G^{(i+k-1)}}{\partial X^{(i+1)}} & \frac{\partial G^{(i+k-1)}}{\partial U^{(i+1)}} & \frac{\partial G^{(i+k-1)}}{\partial X^{(i+2)}} & \frac{\partial G^{(i+k-1)}}{\partial U^{(i+2)}} & \cdots & \frac{\partial G^{(i+k-1)}}{\partial X^{(i+k)}} & \frac{\partial G^{(i+k-1)}}{\partial U^{(i+k)}} \end{pmatrix}.$$

That is, $J_{k,i}$ is the Jacobian matrix of $F^{(i)}, G^{(i)}, \ldots, F^{(i+k-1)}, G^{(i+k-1)} \in k\langle Y\rangle[X^{[i+k]}, U^{[i+k]}]$ with respect to the variables $X^{(i+1)}, U^{(i+1)}, \ldots, X^{(i+k)}, U^{(i+k)}$.

Let $\mathfrak{J}_{k,i} \in k(X)\langle U\rangle^{k(n+r)\times k(n+m)}$ be the matrix with entries in $k[X, U^{[i+k]}]$ which is obtained by substituting $X_j^{(k)} = \tilde{f}_j^{(k-1)}$ (see Notation 3) for $j = 1, \ldots, n$ and $1 \leq k \leq i+k$, in the entries of the matrix $J_{k,i}$.

The matrices $\mathfrak{J}_{k,i}$ are strongly related with some important algebraic facts concerning the (algebraic) ideals Δ_l introduced in the previous section (Notation 6):

Proposition 14. *Let $i \in \mathbb{N}_0$ and $k \in \mathbb{N}$. Then:*

(i) The transcendence degree of the extension $Frac(A_i/(\Delta_{i+k} \cap A_i)) \hookrightarrow Frac(A_{i+k}/\Delta_{i+k})$ equals the dimension (as a $k(X)\langle U\rangle$-vector space) of the kernel of $\mathfrak{J}_{k,i}$.

(ii) The following identity holds:

$$trdeg_{k\langle Y\rangle}(Frac(A_i/\Delta_{i+k} \cap A_i)) = (m-r)(i+1) + n + r - \dim_{k(X)\langle U\rangle}(\ker(\mathfrak{J}_{k,i}^t))$$

where $\mathfrak{J}_{k,i}^t$ denotes the transpose of the matrix $\mathfrak{J}_{k,i}$.

Proof. In order to prove (i), notice first that the polynomials $F^{[i-1]}$ and $G^{[i-1]}$, that are part of the set of definition of the ideal Δ_{i+k}, have orders at most i and so they belong to A_i. Then, for any $i \in \mathbb{N}_0$, the field $\mathrm{Frac}(A_{i+k}/\Delta_{i+k})$ may be considered as the fraction field of the integral domain

$$\mathcal{R} := \mathcal{S}[X^{(i+1)}, \ldots, X^{(i+k)}, U^{(i+1)}, \ldots, U^{(i+k)}]/(F^{(i)}, \ldots, F^{(i+k-1)}, G^{(i)}, \ldots, G^{(i+k-1)})$$

where $\mathcal{S}$ denotes the field $\mathrm{Frac}(A_i/\Delta_{i+k} \cap A_i)$.

Then, the transcendence degree we want to compute is the difference between the number of columns and the rank of the Jacobian matrix associated to the $\mathcal{S}$-algebra $\mathcal{R}$, considering this matrix over the field $\mathrm{Frac}(\mathcal{R})$ (see, for instance, [42, Ch. VI, §1, Th. 1.15] or Lemma 38 below). In other words, the transcendence degree is the dimension, as a $\mathrm{Frac}(\mathcal{R})$-vector space, of the kernel of this Jacobian matrix. This matrix is exactly the matrix $\mathfrak{J}_{k,i}$.

To finish the proof of this part, it only remains to see that $\dim_{\mathrm{Frac}(\mathcal{R})} \ker \mathfrak{J}_{k,i} = \dim_{k(X)\langle U\rangle} \ker \mathfrak{J}_{k,i}$. For this, notice that the entries of $\mathfrak{J}_{k,i}$ are polynomials in the ring $k[X, U^{[i+k]}] \subset k(X)\langle U\rangle$, which is isomorphic to $k[Y^{[i+k-1]}, X^{[i+k]}, U^{[i+k]}]/(F^{[i+k-1]}, G^{[i+k-1]})$. From Proposition 7, there is a natural inclusion from this last ring in A_{i+k}/Δ_{i+k} and then, the rank of the matrix $\mathfrak{J}_{k,i}$ over the fraction field of $k[X, U^{[i+k]}]$ (and therefore, over $k(X)\langle U\rangle$) is equal to its rank over the fraction field of A_{i+k}/Δ_{i+k} (namely, $\mathrm{Frac}(\mathcal{R})$). This finishes the proof of the first part.

For the proof of (ii), we know from Corollary 8 that the Krull dimension of the ideal $\Delta_{i+k} \subset A_{i+k}$, and hence $\mathrm{trdeg}_{k\langle Y\rangle}(\mathrm{Frac}((A_{i+k}/\Delta_{i+k})))$, is equal to $(m-r)(i+k+1)+n+r$. The result follows by considering the tower of fields

$$k\langle Y\rangle \hookrightarrow \mathrm{Frac}(A_i/\Delta_{i+k} \cap A_i) \hookrightarrow \mathrm{Frac}(A_{i+k}/\Delta_{i+k})$$

and part (i), noticing that $\dim_{k(X)\langle U\rangle}(\ker(\mathfrak{J}_{k,i})) = \dim_{k(X)\langle U\rangle}(\ker(\mathfrak{J}_{k,i}^t)) + k(m-r)$. ■

2.3 The rank of matrices $\mathfrak{J}_{k,i}$

We now study more closely some properties related to the behavior of the ranks of the matrices $\mathfrak{J}_{k,i}$. These ranks contain quantitative information about the considered differential algebraic system. Our aim here is to understand the behavior when k and/or i run over $\mathbb{N}$ and $\mathbb{N}_0$ respectively. This will provide us with information about certain invariants of the system (2.1) (namely, the differential Hilbert-Kolchin function, its regularity and the so-called differentiation index (see Section 3)).
We introduce a sequence $(\mu_{k,i})_{k,i\in\mathbb{N}_0}$ of non-negative integers associated with the matrices $\mathfrak{J}_{k,i}$:

Definition 15. *For $k, i \in \mathbb{N}_0$ we define $\mu_{k,i} \in \mathbb{N}_0$ as follows:*

- $\mu_{0,i} := 0$ *for every* $i \in \mathbb{N}_0$.
- *For* $k \geq 1$, $\mu_{k,i} := \dim_{k(X)\langle U\rangle} \ker(\mathfrak{J}_{k,i}^t)$.

We focus, for the time being, on the study of some stationarity properties of the sequence $(\mu_{k,i})_{k,i}$. We begin by comparing the matrices $\mathfrak{J}_{k,i}$ for $k \in \mathbb{N}$ in order to analyze the changes of the sequence $(\mu_{k,i})_k$ when the index i is fixed and k moves.
First, let us observe the following recursive relation which holds for every $k \geq 1$:

$$\mathfrak{J}_{k+1,i} = \begin{pmatrix} \boxed{\mathfrak{J}_{k,i}} & \begin{matrix} 0 & 0 \\ 0 & 0 \\ \vdots & \vdots \\ \vdots & \vdots \end{matrix} \\ \begin{matrix} \frac{\partial F^{(i+k)}}{\partial X^{(i+1)}} & \frac{\partial F^{(i+k)}}{\partial U^{(i+1)}} \\ \frac{\partial G^{(i+k)}}{\partial X^{(i+1)}} & \frac{\partial G^{(i+k)}}{\partial U^{(i+1)}} \end{matrix} & \begin{matrix} \cdots & \frac{\partial F^{(i+k)}}{\partial X^{(i+k+1)}} & \frac{\partial F^{(i+k)}}{\partial U^{(i+k+1)}} \\ \cdots & \frac{\partial G^{(i+k)}}{\partial X^{(i+k+1)}} & \frac{\partial G^{(i+k)}}{\partial U^{(i+k+1)}} \end{matrix} \end{pmatrix}. \tag{2.2}$$

When the differential system (2.1) is linear (for instance, if $k = \mathbb{Q}$ and the system has the form $AU + B\dot{U} = Y$, with A and B matrices in $\mathbb{Q}^{r\times m}$), the matrices $\mathfrak{I}_{k,i}$ have a nice Hankel-block type form, but this is not necessarily our situation. However, there are two main relations arising from their underlying differential structure which enable us to study properties of this matrices in our (more general) setting:

Proposition 16. *Let $Z := Z_1, \dots, Z_\alpha$ be differential independent variables and let H be a differential polynomial in $k\{Z\}$. Denote by δ the derivation in $k\{Z\}$. For all $l, j \in \mathbb{N}_0$ the following relation holds:*

$$\delta\left(\frac{\partial H^{(l)}}{\partial Z^{(j+1)}}\right) = \frac{\partial H^{(l+1)}}{\partial Z^{(j+1)}} - \frac{\partial H^{(l)}}{\partial Z^{(j)}}. \tag{2.3}$$

In particular, if $H \in \{F, G\}$ and $Z \in \{X, U\}$, we have that $\dfrac{\partial H^{(l)}}{\partial Z^{(j+1)}} = 0$ for every $j \geq l + 1$, since the order of $H^{(l)}$ is at most $l + 1$, and therefore identity (2.3) implies that

$$\frac{\partial H^{(l+1)}}{\partial Z^{(j+1)}} = \frac{\partial H^{(l)}}{\partial Z^{(j)}} \qquad \forall\, j \geq l + 1. \tag{2.4}$$

Proof. A straightforward consequence of the Chain Rule. ■

Proposition 16 will be used in the field $k(X)\langle U\rangle$ after performing the evaluation introduced in Notation 3.

We are now ready to prove the first stationarity property of the sequence $(\mu_{k,i})_{k,i}$:

Proposition 17. *For each fixed $i \in \mathbb{N}_0$, the sequence $(\mu_{k,i})_{k\in\mathbb{N}_0}$ is non-decreasing and bounded by $n + r$. In particular, there exists $k \in \mathbb{N}_0$ (depending on i), $0 \leq k \leq n + r$, such that $\mu_{k,i} = \mu_{k+1,i}$.*

Proof. The fact that $(\mu_{k,i})_k$ is a non-decreasing sequence follows immediately from the fact that there is an inclusion $\ker(\mathfrak{I}^t_{k,i}) \times \{0\} \subseteq \ker(\mathfrak{I}^t_{k+1,i})$ for every $k \in \mathbb{N}$.
For every integer $k \in \mathbb{N}_0$, due to Proposition 14 and Definition 15, we have that

$$\operatorname{trdeg}_{k\langle Y\rangle}(\operatorname{Frac}(A_i/\Delta_{i+k} \cap A_i)) = (m - r)(i + 1) + n + r - \mu_{k,i}.$$

Now, since $\Delta_{i+k} \cap A_i \subset \Delta \cap A_i$,

$$\operatorname{trdeg}_{k\langle Y\rangle}(\operatorname{Frac}(A_i/\Delta_{i+k} \cap A_i)) \geq \operatorname{trdeg}_{k\langle Y\rangle}(\operatorname{Frac}(A_i/\Delta \cap A_i))$$

and so, the fact that the differential dimension of Δ is $m - r$, that is, any differential transcendence basis of the extension $k\langle Y\rangle \hookrightarrow \mathcal{F} = \operatorname{Frac}(k\langle Y\rangle\{X, U\}/\Delta)$ has $m - r$ elements, implies that there are at least $(m - r)(i + 1)$ variables in $\operatorname{Frac}(A_i/\Delta \cap A_i)$ that are algebraically independent over $k\langle Y\rangle$ and so

$$\operatorname{trdeg}_{k\langle Y\rangle}(\operatorname{Frac}(A_i/\Delta \cap A_i)) \geq (m - r)(i + 1).$$

We have the inequality

$$(m-r)(i+1)+n+r-\mu_{k,i} \geq (m-r)(i+1)$$

from where we conclude that $\mu_{k,i} \leq n+r$. ■

Remark 18. *It can be proved also that the amount of polynomials of order zero in the original system (2.1) is a lower bound for the sequence $(\mu_{k,i})_{k\in\mathbb{N}}$ (see [15] for a proof).*

In fact, we are able to show a more precise result than that of Proposition 17: the sequence $(\mu_{k,i})_k$ is *strictly* increasing up to a certain index $k_i \leq n+r$ where it becomes stationary (Theorem 20). A related result can be found in [58, Proposition 2].

For the sake of simplicity, for the time being, we will use the following notations:

Notation 19. *The variables X, U involved in system (2.1) are renamed in the following way:*

$$Z_i := X_i \text{ for } i = 1,\dots,n \text{ and } Z_{n+j} := U_j \text{ for } j = 1,\dots,m$$

(and the same is done for their corresponding formal derivatives). Analogously, the polynomials are renamed as:

$$H_i := F_i \text{ for } i = 1,\dots,n \text{ and } H_{n+j} := G_j \text{ for } j = 1,\dots,r.$$

With these notations, the matrix $\mathfrak{J}_{k,i}$ from Definition 15 involves exactly the derivatives of the polynomials $H^{(i+p)}$ with respect to the variables $Z^{(i+q)}$, with $p = 0,\dots,k-1$ and $q = 1,\dots,k$ conveniently ordered.

Theorem 20. *Let $k_i \in \mathbb{N}_0$ be the minimum of all the k's in $\mathbb{N}_0$ such that $\mu_{k+1,i} = \mu_{k,i}$ (this minimum is well defined by Proposition 17). Then $\mu_{k,i} = \mu_{k_i,i}$ for every $k \geq k_i$.*

Proof. According to Notation 19 we will rename variables and equations as $Z := (X, U)$ and $H := (F, G)$.

The result is clear for $k_i = 0$: in this case, $\mu_{1,i} = 0$, which is equivalent to the fact that the matrix $\mathfrak{J}_{1,i} = \dfrac{\partial H^{(i)}}{\partial Z^{(i+1)}}$ has full row rank. Therefore, by relation (2.4) and the triangular form of the matrices $\mathfrak{J}_{k,i}$ (with the same block $\mathfrak{J}_{1,i}$ in the diagonal), we conclude that $\mathfrak{J}_{k,i}$ has full row rank or, equivalently, that $\mu_{k,i} = 0$ for all k.

Now, let us assume that $k_i \geq 1$. In this case, it suffices to show that the equality $\mu_{k,i} = \mu_{k-1,i}$ for an arbitrary index $k \geq 2$, implies $\mu_{k+1,i} = \mu_{k,i}$.

In what is left of this proof, we will write v for a vector in $k(X)\langle U\rangle^{l(n+r)}$ and its description as a block vector $v = (v_1,\dots,v_l)$ where $v_j \in k(X)\langle U\rangle^{n+r}$ for all $j = 1,\dots,l$.

Due to the recursive relation (2.2), the identity

$$\ker(\mathfrak{J}_{k,i}^t) \times \{0\} = \ker(\mathfrak{J}_{k+1,i}^t) \cap \{v_{k+1} = 0\}$$

holds in $k(X)\langle U\rangle^{(k+1)(n+r)}$ for every $k \in \mathbb{N}$ and so, the equality $\mu_{k,i} = \mu_{k+1,i}$ is equivalent to the inclusion

$$\ker(\mathfrak{I}^t_{k+1,i}) \subset \{v_{k+1} = 0\}.$$

Then, the theorem is a consequence of the following recursive principle:

Claim: For all $k \in \mathbb{N}$, $\ker(\mathfrak{I}^t_{k,i}) \subset \{v_k = 0\}$ implies $\ker(\mathfrak{I}^t_{k+1,i}) \subset \{v_{k+1} = 0\}$.

Proof of the Claim.- We will show that if $(v_1, \ldots, v_{k+1}) \in \ker(\mathfrak{I}^t_{k+1,i})$ then, the vector

$$w = (w_1, \ldots, w_k) \in k(X)\langle U\rangle^{k(n+r)}$$

defined as

$$w_k = v_{k+1}, \qquad w_j = v_{j+1} - \dot{w}_{j+1}, \quad j = k-1, \ldots, 1,$$

lies in $\ker(\mathfrak{I}^t_{k,i})$, which implies the *Claim*.

Since $\dfrac{\partial H^{(i+\ell-1)}}{\partial Z^{(i+j)}} = 0$ for $\ell < j$, we have that $w \in \ker(\mathfrak{I}^t_{k,i})$ if and only if the identities

$$\sum_{\ell=j}^{k} w_\ell \, \frac{\partial H^{(i+\ell-1)}}{\partial Z^{(i+j)}} = 0$$

hold over $k(X)\langle U\rangle$ for every $1 \le j \le k$.

We will proceed recursively for $j = k, k-1, \ldots, 1$. For $j = k$, the definition of w and identity (2.4) imply that

$$w_k \, \frac{\partial H^{(i+k-1)}}{\partial Z^{(i+k)}} = v_{k+1} \, \frac{\partial H^{(i+k)}}{\partial Z^{(i+k+1)}} = 0.$$

Now, assume that $\displaystyle\sum_{\ell=j+1}^{k} w_\ell \, \frac{\partial H^{(i+\ell-1)}}{\partial Z^{(i+j+1)}} = 0$. Differentiating this identity in $k(X)\langle U\rangle$ and using identity (2.3) we get:

$$\sum_{\ell=j+1}^{k} \dot{w}_\ell \, \frac{\partial H^{(i+\ell-1)}}{\partial Z^{(i+j+1)}} + \sum_{\ell=j+1}^{k} w_\ell \left(\frac{\partial H^{(i+\ell)}}{\partial Z^{(i+j+1)}} - \frac{\partial H^{(i+\ell-1)}}{\partial Z^{(i+j)}} \right) = 0.$$

This implies that

$$\begin{aligned}
\sum_{\ell=j}^{k} w_\ell \, \frac{\partial H^{(i+\ell-1)}}{\partial Z^{(i+j)}} &= w_j \, \frac{\partial H^{(i+j-1)}}{\partial Z^{(i+j)}} + \sum_{\ell=j+1}^{k} \dot{w}_\ell \, \frac{\partial H^{(i+\ell-1)}}{\partial Z^{(i+j+1)}} + \sum_{\ell=j+1}^{k} w_\ell \, \frac{\partial H^{(i+\ell)}}{\partial Z^{(i+j+1)}} \\
&= \sum_{\ell=j+1}^{k} (\dot{w}_\ell + w_{\ell-1}) \, \frac{\partial H^{(i+\ell-1)}}{\partial Z^{(i+j+1)}} + w_k \, \frac{\partial H^{(i+k)}}{\partial Z^{(i+j+1)}} \\
&= \sum_{\ell=j+1}^{k+1} v_\ell \, \frac{\partial H^{(i+\ell-1)}}{\partial Z^{(i+j+1)}} = \sum_{\ell=1}^{k+1} v_\ell \, \frac{\partial H^{(i+\ell-1)}}{\partial Z^{(i+j+1)}} = 0,
\end{aligned}$$

where the second equality follows from identity (2.4) and the third one from the definition of w. This concludes the proof of the theorem. ■

So far, we have studied the behavior of the sequence $(\mu_{k,i})_k$ for an arbitrary (but fixed) index $i \in \mathbb{N}_0$. In the remaining part of the section we will analyze the sequence $(\mu_{k,i})_i$ fixing the index $k \in \mathbb{N}$.

We start exhibiting a (non $k(X)\langle U\rangle$-linear) bijection between the kernels of the matrices $\mathfrak{J}_{k,i}$ and $\mathfrak{J}_{k,i+1}$ for any index $k \in \mathbb{N}$.

Lemma 21. *Let $(v_1, \dots, v_k)$ and $(w_1, \dots, w_k)$ be arbitrary elements in $k(X)\langle U\rangle^{k(n+m)}$ (here v_j and w_j are vectors in $k(X)\langle U\rangle^{n+m}$ for every index j). Then, the function*

$$\theta : k(X)\langle U\rangle^{k(n+m)} \to k(X)\langle U\rangle^{k(n+m)}$$

defined as

$$\theta(v_1, \dots, v_k) = (v_1, v_2 - \dot{v}_1, v_3 - \dot{v}_2, \dots, v_k - \dot{v}_{k-1})$$

maps $\ker(\mathfrak{J}_{k,i+1})$ *into* $\ker(\mathfrak{J}_{k,i})$.

Moreover, θ is a bijection between $\ker(\mathfrak{J}_{k,i+1})$ *and* $\ker(\mathfrak{J}_{k,i})$*, whose inverse is given by*

$$\theta^{-1}(w_1, \dots, w_k) = (w_1, w_2 + \dot{w}_1, w_3 + \dot{w}_2 + w_1^{(2)}, \dots, w_k + \dot{w}_{k-1} + \cdots + w_1^{(k-1)}).$$

Proof. It is easy to see that θ is a bijection in $k(X)\langle U\rangle^{k(n+m)}$ with the inverse given in the statement of the Lemma. We first need to show that it maps $\ker(\mathfrak{J}_{k,i+1})$ onto $\ker(\mathfrak{J}_{k,i})$.

For arbitrary vectors $(v_1, \dots, v_k)$ and $(w_1, \dots, w_k)$ in $k(X)\langle U\rangle^{k(n+m)}$, consider the following two families of sums ($p = 0, \dots, k-1$):

$$E_p(v) := \sum_{j=1}^{k} \frac{\partial H^{(i+1+p)}}{\partial Z^{(i+1+j)}}\, v_j \quad \text{and} \quad D_p(w) := \sum_{j=1}^{k} \frac{\partial H^{(i+p)}}{\partial Z^{(i+j)}}\, w_j.$$

Note that $v \in \ker(\mathfrak{J}_{k,i+1})$ if and only if $E_p(v) = 0$ for $p = 0, \dots, k-1$ and $w \in \ker(\mathfrak{J}_{k,i})$ if and only if $D_p(w) = 0$ for $p = 0, \dots, k-1$.

We now compare the vectors $\mathfrak{J}_{k,i+1}.\, v$ and $\mathfrak{J}_{k,i}.\, \theta(v)$ for a given vector $v = (v_1, \dots, v_k)$ in $k(X)\langle U\rangle^{k(n+m)}$.

First, note that $E_0(v) = D_0(v) = D_0(\theta(v))$, since $\dfrac{\partial H^{(i+1)}}{\partial Z^{(i+1+j)}} = \dfrac{\partial H^{(i)}}{\partial Z^{(i+j)}} = 0$ for every $j \geq 2$ and $\theta(v)_1 = v_1$.

Now, for $p > 0$, we have:

$$\begin{aligned}
E_p(v) - (E_{p-1}(v))^{\cdot} &= \sum_{j=1}^{k} \left(\frac{\partial H^{(i+1+p)}}{\partial Z^{(i+1+j)}} - \left(\frac{\partial H^{(i+p)}}{\partial Z^{(i+1+j)}} \right)^{\cdot} \right) v_j - \sum_{j=1}^{k} \frac{\partial H^{(i+p)}}{\partial Z^{(i+1+j)}}\, \dot{v}_j \\
&= \sum_{j=1}^{k} \frac{\partial H^{(i+p)}}{\partial Z^{(i+j)}} v_j - \sum_{j=2}^{k+1} \frac{\partial H^{(i+p)}}{\partial Z^{(i+j)}}\, \dot{v}_{j-1} \\
&= \frac{\partial H^{(i+p)}}{\partial Z^{(i+1)}} v_1 + \sum_{j=2}^{k} \frac{\partial H^{(i+p)}}{\partial Z^{(i+j)}} (v_j - \dot{v}_{j-1}) \;=\; D_p(\theta(v)),
\end{aligned}$$

where the second equality follows from identity (2.3) and the third one from the fact that $\dfrac{\partial H^{(i+p)}}{\partial Z^{(i+1+k)}} = 0$ for $p \leq k-1$.

These equalities imply straightforwardly that θ maps $\ker(\mathfrak{J}_{k,i+1})$ into $\ker(\mathfrak{J}_{k,i})$.
In order to prove that it is onto, we may argue recursively: if $w \in \ker(\mathfrak{J}_{k,i})$, then $D_p(w) = 0$ for $p = 0, \ldots, k-1$. Now, $E_0(\theta^{-1}(w)) = E_0(w) = D_0(w) = 0$. Assuming that $E_{p-1}(\theta^{-1}(w)) = 0$ has already been proved, we deduce that

$$E_p(\theta^{-1}(w)) = D_p(w) + (E_{p-1}(\theta^{-1}(w)))'$$

also equals 0. We conclude that $\theta^{-1}(w) \in \ker(\mathfrak{J}_{k,i+1})$. ■

Even though the bijection θ between $\ker(\mathfrak{J}_{k,i+1})$ and $\ker(\mathfrak{J}_{k,i})$ shown in the previous Lemma is not a $k(X)\langle U\rangle$-linear map, it enables us to prove the following:

Proposition 22. *Let $k, i \in \mathbb{N}_0$ be arbitrary non negative integers. Then $\mu_{k,i} = \mu_{k,i+1}$.*

Proof. In order to prove that

$$\mu_{k,i} = \dim_{k(X)\langle U\rangle}(\ker(\mathfrak{J}_{k,i}^t)) = \dim_{k(X)\langle U\rangle}(\ker(\mathfrak{J}_{k,i+1}^t)) = \mu_{k,i+1},$$

it is enough to show that $\mathfrak{J}_{k,i}$ and $\mathfrak{J}_{k,i+1}$ have the same rank, since they are two matrices of the same size. For each pair of indices j, t, $1 \leq j \leq k$ and $1 \leq t \leq n+m$, set

$$C_{j,t} := \frac{\partial H^{[i,i+k-1]}}{\partial Z_t^{(i+j)}} \quad \text{and} \quad D_{j,t} := \frac{\partial H^{[i+1,i+k]}}{\partial Z_t^{(i+1+j)}}$$

for the corresponding columns of the matrices $\mathfrak{J}_{k,i}$ and $\mathfrak{J}_{k,i+1}$, respectively.
Assume that a column D_{j_0,t_0} of the matrix $\mathfrak{J}_{k,i+1}$ is a $k(X)\langle U\rangle$-linear combination of the columns $D_{j,t}$ to its right. Then, there exist elements $\alpha_{j,t} \in k(X)\langle U\rangle$ such that

$$D_{j_0,t_0} = \sum_{t=t_0+1}^{n+m} \alpha_{j_0,t} D_{j_0,t} + \sum_{j=j_0+1}^{k} \sum_{t=1}^{n+m} \alpha_{j,t} D_{j,t},$$

and so, the vector

$$v := (\overrightarrow{0}, \ldots, \overrightarrow{0}, -\alpha_{j_0}, -\alpha_{j_0+1}, \ldots, -\alpha_k) \in k(X)\langle U\rangle^{k(n+m)}$$

belongs to the kernel of the matrix $\mathfrak{J}_{k,i+1}$, where $\overrightarrow{0}$ denotes the vector in $k(X)\langle U\rangle^{n+m}$ with all its coordinates equal to 0,

$$\alpha_{j_0} := (0, \ldots, 0, 1, \alpha_{j_0,t_0+1}, \ldots, \alpha_{j_0,k}) \text{ and } \alpha_j := (\alpha_{j,1}, \ldots, \alpha_{j,k}) \text{ for } j \geq j_0 + 1.$$

By Lemma 21, the vector $\theta(v)$ belongs to the kernel of $\mathfrak{J}_{k,i}$ and, due to the particular form of the application θ, it turns out that the column C_{j_0,t_0} is a $k(X)\langle U\rangle$-linear combination of the columns to its right. We conclude that the rank of $\mathfrak{J}_{k,i}$ is lower or equal to the rank of $\mathfrak{J}_{k,i+1}$.
By means of the inverse map θ^{-1}, it can be proved in the same way that the rank of $\mathfrak{J}_{k,i+1}$ is lower or equal to the rank of $\mathfrak{J}_{k,i}$. ■

Remark 23. *The following simpler alternative proof of this proposition was kindly suggested by Prof. F. Ollivier: from [38, Prop. 10, Ch. IV] the integers $\mu_{k,i}$ and $\mu_{k,i+1}$ are, respectively, the differential dimensions of the ideals generated by the linear equations defined by the matrices $\mathfrak{J}_{k,i}$ and $\mathfrak{J}_{k,i+1}$ (equivalently, the transcendence differential degree of the fraction fields of the factor rings). Now, Proposition 22 follows since the bijection θ is actually a differential isomorphism between these fields.*

The previous Proposition states that the sequence $\mu_{k,i}$ does not depend on the index i and so Theorem 20 can be restated as follows:

Corollary 24. *There exists a non negative integer σ such that, for any $i \in \mathbb{N}_0$, $\mu_{k,i} < \mu_{k+1,i}$ if $k < \sigma$ and $\mu_{k,i} = \mu_{\sigma,i}$ if $k \geq \sigma$.*

Proof. Fix an index $i \in \mathbb{N}_0$. Proposition 22 states that

$$\mu_{k_i+1,i+1} = \mu_{k_i+1,i} \quad \text{and} \quad \mu_{k_i,i+1} = \mu_{k_i,i},$$

and the definition of k_i ensures that

$$\mu_{k_i+1,i} = \mu_{k_i,i}.$$

We deduce that

$$\mu_{k_i+1,i+1} = \mu_{k_i,i+1} \quad \text{and so,} \quad k_{i+1} \leq k_i.$$

On the other hand, we have that

$$\mu_{k_{i+1},i} = \mu_{k_{i+1},i+1} = \mu_{k_{i+1}+1,i+1} = \mu_{k_{i+1}+1,i}$$

(where the first and third equalities are due to Proposition 22, and the second one is the definition of k_{i+1}), which implies that $k_i \leq k_{i+1}$.
The Corollary follows because, for any index i, $k_i = k_0 = \sigma$. ■

We finish this section by introducing the notion of differentiation index of the system (2.1):

Definition 25. *The non negative integer σ of Corollary 24 is called the* differentiation index *of the system (2.1).*

Note that, due to Proposition 17, we have $0 \leq \sigma \leq n + r$. In addition, Corollary 24 states that, for every $i \in \mathbb{N}_0$, the differentiation index σ is the smallest non-negative integer where the sequence $(\mu_{k,i})_k$ becomes stationary.
For more general first-order differential systems there are many definitions of the differentiation index (see for instance [9], [44], [18]). The one we will be considering in this work states, roughly speaking, that it is the minimum number of times that the given differential system must be differentiated in order

to determine the derivatives of the unknowns as continuous functions of the unknowns themselves. We will show in Appendix B the relation between these two definitions.

Meanwhile, in the next chapter the differential index will allow us to prove an essential result for changing from a differential setting to an algebraic one (see Theorem 26 below).

Chapter 3

Differential Hilbert-Kolchin function and differential transcendence basis: quantitative and algorithmic aspects

In the first two sections of this chapter we will apply the properties of the matrices $\mathfrak{J}_{k,i}$ established above to the study of two well-known invariants in our system (2.1):

- the differentiation index,
- the differential Hilbert-Kolchin function.

Then we will focus on the properties that must be satisfied by a differential transcendence basis and finally we will show the algorithms for all the computations involved.
We begin by showing a relation between contractions of the differential ideal Δ and contractions of the algebraic polynomial ideals Δ_j to the polynomial rings A_i (see Notation 6), which is a crucial result to change from the non-noetherian (differential) context to a noetherian one.

3.1 The differentiation index

For every $i \in \mathbb{N}_0$, the differentiation index σ (Definition 25) is strongly related with the minimum number of derivatives of the system (2.1) required to obtain the intersection of the whole differential ideal Δ with the polynomial ring A_i, namely those polynomials in Δ which involve only derivatives up to order i. Similar versions of the Theorem 26 can be obtained by rewriting techniques following [53, Theorem 27] (see also [45, Lemma 9]).

Theorem 26. *Let $\sigma \in \mathbb{N}_0$ be the differentiation index of the system (2.1). Then, for every $i \in \mathbb{N}_0$, the equality of ideals*

$$\Delta_{i+\sigma} \cap A_i = \Delta \cap A_i$$

holds in the polynomial ring A_i. Moreover, for every index $i \in \mathbb{N}_0$, the differentiation index σ verifies:

$$\sigma = \min\{h \in \mathbb{N}_0 : \Delta_{i+h} \cap A_i = \Delta \cap A_i\}.$$

Note that, since $\sigma \leq n + r$ (see also Proposition 17), this theorem ensures that the identity

$$\Delta_{i+n+r} \cap A_i = \Delta \cap A_i$$

holds for every index $i \in \mathbb{N}_0$.

Proof. Fix an index $i \in \mathbb{N}_0$ and consider the increasing chain of prime ideals in the polynomial ring A_i:

$$(\Delta_{i+k} \cap A_i)_{k \in \mathbb{N}_0}.$$

From Proposition 14 and the definition of the sequence $\mu_{k,i}$, for every $k \in \mathbb{N}_0$, we have that

$$\operatorname{trdeg}_{k\langle Y\rangle}(\operatorname{Frac}(A_i/\Delta_{i+k} \cap A_i)) = (m - r)(i + 1) + n + r - \mu_{k,i}. \tag{3.1}$$

Since $\mu_{k,i}$ is stationary for $k \geq \sigma$ (see Theorem 20 and Corollary 24), the previous equality implies that all the prime ideals $\Delta_{i+k} \cap A_i$, for $k \geq \sigma$, have the same dimension and thus they coincide.
On the other hand, any finite system of generators of the prime ideal $\Delta \cap A_i \subset A_i$ belongs to $\Delta_{i+k} \cap A_i$ for all k big enough. This finishes the proof of the first assertion of the Theorem.
In order to prove the second part of the statement, for each $i \in \mathbb{N}_0$, let h_i be the smallest non-negative integer such that $\Delta_{i+h_i} \cap A_i = \Delta \cap A_i$. By the definition of h_i, the transcendence degrees $\operatorname{trdeg}_{k\langle Y\rangle}(\operatorname{Frac}(A_i/\Delta_{i+k} \cap A_i))$ coincide for $k \geq h_i$ and so, $\mu_{k,i}$ is constant for $k \geq h_i$ (see identity (3.1) above). This implies that $\sigma \leq h_i$. The equality follows from the first part of the statement and the minimality of h_i. ■

Theorem 26 provides an alternative definition of the differentiation index (see also [45, Section 3.2]). In particular, the fact that σ is the smallest non-negative integer verifying the identity $\Delta_\sigma \cap A_0 = \Delta \cap A_0$ gives the following interpretation of the differentiation index σ (see [18]):

Corollary 27. *If the differentiation index σ of system (2.1) equals 0, there are no constraints on initial conditions for the system. In the case when $\sigma \geq 1$, the quantity $\sigma - 1$ is the minimal number of derivatives of the equations needed to obtain all the relations that the initial conditions should verify (the so-called "manifold of constraints on initial conditions").* ■

Another property of the differentiation index, concerning the number of derivatives needed to distinguish dependent or independent variables, is considered in Appendix B (see Theorem 70 below).

3.2 The differential Hilbert-Kolchin function

We recall that the differential Hilbert-Kolchin function $H_{\Delta,k\langle Y\rangle} : \mathbb{N}_0 \to \mathbb{N}_0$ of the differential prime ideal $\Delta \subset k\langle Y\rangle\{X, U\}$ is defined as

$$H_{\Delta,k\langle Y\rangle}(i) := \text{trdeg}_{k\langle Y\rangle}(\text{Frac}(A_i/(\Delta \cap A_i)))$$

for every $i \in \mathbb{N}_0$. As was already mentioned in the Subsection 1.1.2, it is well known that, for i big enough, this function coincides with the (degree one) polynomial

$$H_{\Delta,k\langle Y\rangle}(i) = (m - r)(i + 1) + \text{ord}_{k\langle Y\rangle}(\Delta),$$

where $\text{ord}_{k\langle Y\rangle}(\Delta)$ (the *order* of the ideal) is a non-negative integer depending only on the differential ideal Δ, and that the regularity of the function, that is the first i from where this identity holds, is less or equal than $\text{ord}_{k\langle Y\rangle}(\Delta)$ (see [38, Ch. II, Sec. 12, Th. 6]). In our case, however, the results obtained so far enable us to prove a deeper result:

Theorem 28. *The differential Hilbert-Kolchin function of the differential ideal Δ verifies*

$$H_{\Delta,k\langle Y\rangle}(i) = (m - r)(i + 1) + ord_{k\langle Y\rangle}(\Delta)$$

for every $i \in \mathbb{N}_0$.

Proof. It is enough to show, for every $i \in \mathbb{N}_0$, that holds

$$H_{\Delta,k\langle Y\rangle}(i + 1) = H_{\Delta,k\langle Y\rangle}(i) + m - r.$$

Fix an index $i \in \mathbb{N}_0$. Due to Theorem 26, we have that

$$\Delta \cap A_i = \Delta_{i+\sigma} \cap A_i \quad \text{and} \quad \Delta \cap A_{i+1} = \Delta_{i+1+\sigma} \cap A_{i+1}$$

and so,

$$H_{\Delta,k\langle Y\rangle}(i + 1) = \text{trdeg}_{k\langle Y\rangle}(A_{i+1}/(\Delta_{i+1+\sigma} \cap A_{i+1}))$$

and

$$H_{\Delta,k\langle Y\rangle}(i) = \text{trdeg}_{k\langle Y\rangle}(A_i/(\Delta_{i+\sigma} \cap A_i)).$$

Using the results in Proposition 14 we obtain:

$$\begin{aligned} H_{\Delta,k\langle Y\rangle}(i + 1) &= (m - r)(i + 2) + n + r - \mu_{\sigma,i+1}, \\ H_{\Delta,k\langle Y\rangle}(i) &= (m - r)(i + 1) + n + r - \mu_{\sigma,i}. \end{aligned}$$

Hence, the equality

$$H_{\Delta,k\langle Y\rangle}(i + 1) = H_{\Delta,k\langle Y\rangle}(i) + m - r$$

is a consequence of the identity $\mu_{\sigma,i+1} = \mu_{\sigma,i}$ given by Proposition 22. ■

The following Corollary will give us a way of computing the differential Hilbert-Kolchin function and the order of the ideal Δ as a straightforward consequence of the computation of the rank of the matrix $\mathfrak{J}_{\sigma,0}$ (Definition 13). Similar results can be found in [45].

Corollary 29. *As an immediate consequence of the proof of this Theorem one infers that the equalities*

$$H_{\Delta,k\langle Y\rangle}(i+1) = (m-r)(i+1) + n + r - \mu_{\sigma,0}$$

$$ord_{k\langle Y\rangle}(\Delta) = n + r - \mu_{\sigma,0}.$$

hold. Moreover if σ is non-zero one has also that

$$H_{\Delta,k\langle Y\rangle}(i+1) = (m-r)(i+1) + rk_{k(X)\langle U\rangle}(\mathfrak{J}_{\sigma,0}) - (\sigma-1)(n+r)$$

$$ord_{k\langle Y\rangle}(\Delta) = n + r - \mu_{\sigma,0} = rk_{k(X)\langle U\rangle}(\mathfrak{J}_{\sigma,0}) - (\sigma-1)(n+r) \leq n + r. \blacksquare$$

Remark 30. *From Remark 18 and the previous corollary we deduce that the order of the ideal Δ is bounded by the amount of polynomials of order one in the original system (2.1). In particular $ord_{k\langle Y\rangle}(\Delta) \leq n + r$.*

For other bounds for the order of the differential ideal Δ in terms of the order of the defining equations see also [52, Ch. VII, p.135], [35] or [15].

3.3 A differential transcendence basis

Here we will show how to obtain a differential transcendence basis of the differential field extension $k\langle Y\rangle \hookrightarrow \mathcal{F}$ but before we go into this computation we would like to point out that there are bases that have an additional property that will be useful later. If W is a differential transcendence basis of this extension, since, by definition of a differential transcendence basis, there are no polynomials in Δ involving only the variables W, we can consider the localization of the polynomial ring at W, $k\langle Y, W\rangle\{\{X, U\} \setminus W\}$ and the differential ideal $\tilde{\Delta}$ generated by the polynomials F, G in this ring. The order of this new ideal is not always equal to the order of the original ideal Δ over the field $k\langle Y\rangle$ and, moreover, it depends on the choice of the set W, as we see in the following example.

Consider the system with only one equation $Y_1 = U_1 + \dot{U}_2$ the differential dimension of the extension $k\langle Y\rangle \hookrightarrow \mathcal{F}$ is 1 and either $\{U_1\}$ or $\{U_2\}$ may be considered as differential transcendence bases. However, if the chosen basis is $W = \{U_1\}$ then

$$\text{ord}_{k\langle Y,W\rangle}(\tilde{\Delta}) = \mathcal{H}_{\tilde{\Delta},k\langle Y,W\rangle}(1) = 1 = \text{ord}_{k\langle Y\rangle}(\Delta),$$

meanwhile if $W = \{U_2\}$,

$$\operatorname{ord}_{k\langle Y,W\rangle}(\tilde{\Delta}) = \mathcal{H}_{\tilde{\Delta},k\langle Y,W\rangle}(1) = 0.$$

Then, the order of an ideal may change after localization in a differential transcendence basis, nevertheless it is possible to show that, in our case, there exists a differential transcendence basis that preserves the order of the ideal Δ (see Lemma 32 and Proposition 33). When this is the case, we say that the differential transcendence basis W is a "good" basis. We will make use of this basis again in Appendix B where we will show another alternative presentation of the system 2.1.

The meaning of the expression "good" basis must be restrained to the purpose of this thesis and it should not be interpreted in this way in any other context. For instance, the seminal notion of flatness in control theory corresponds to our "worst" bases, that is the bases W for which $k\langle W\rangle$ is equal to the whole field extension associated to the system. For related bibliography on this subject see the classical works G. Monge [46], D. Hilbert [33], É. Cartan [11], P. Zervos [64] and the most recent ones [20] and [17].

Notation 31. *In what follows, we will denote $\mathcal{F}_i := Frac(A_i/(\Delta \cap A_i))$ for every $i \in \mathbb{N}_0$ and we will use the same notation for an element of A_i or its class in $\mathcal{F}_i$ whenever the ring in which it is considered is clear from the context.*

The fact that $\mathcal{F}_i \hookrightarrow \mathcal{F}_{i+1}$ for every $i \in \mathbb{N}_0$ allows us to consider any subset of $\mathcal{F}_i$ as a subset of $\mathcal{F}_j$ for every $j \geq i$, which will also be done without changing notations.

The following two results show the existence of a "good" differential transcendence basis and lay the grounds for the algorithm that computes it.

Lemma 32. *Let $\mathcal{B} \subset A_i$ be any finite set of elements and let $\zeta \in A_i$ be a polynomial such that its class $\zeta \in \mathcal{F}_i$ is algebraic over $k\langle Y\rangle(\mathcal{B})$. Then, $\dot{\zeta} \in \mathcal{F}_{i+1}$ is algebraic over $k\langle Y\rangle(\mathcal{B} \cup \dot{\mathcal{B}})$, where $\dot{\mathcal{B}}$ denotes the set of classes of all derivatives of elements in $\mathcal{B}$.*

In particular, if $k\langle Y\rangle(\mathcal{B}) \hookrightarrow \mathcal{F}_i$ is an algebraic field extension, then $k\langle Y\rangle(\mathcal{B}\cup\dot{\mathcal{B}}) \hookrightarrow \mathcal{F}_{i+1}$ is also algebraic.

Proof. The result is immediate if $\zeta \in \mathcal{B}$. So, let us consider the case when $\zeta \notin \mathcal{B}$.

Let $P \in k\langle Y\rangle(\mathcal{B})[T]$ be the minimal polynomial of ζ in $k\langle Y\rangle(\mathcal{B}) \hookrightarrow \mathcal{F}_i$. Multiplying it by a non-zero element in $k\langle Y\rangle[\mathcal{B}]$, we may assume that $P \in k\langle Y\rangle[\mathcal{B}, T]$ and has non-zero leading coefficient as a polynomial in the variable T.

We have $P(\mathcal{B}, \zeta) \in \Delta \cap A_i$, and so $\dot{P}(\mathcal{B} \cup \dot{\mathcal{B}}, \zeta, \dot{\zeta}) \in \Delta \cap A_{i+1}$. Now,

$$\dot{P}(\mathcal{B} \cup \dot{\mathcal{B}}, \zeta, \dot{\zeta}) = Q(\mathcal{B} \cup \dot{\mathcal{B}}, \zeta) + \frac{\partial P}{\partial T}(\mathcal{B}, \zeta)\,\dot{\zeta}$$

for some polynomial Q.

As $\deg_T(\frac{\partial P}{\partial T}) < \deg_T(P)$, the minimality of P implies that

$$\frac{\partial P}{\partial T}(\mathcal{B}, \zeta) \notin \Delta$$

and so, $\dot{P}(\mathcal{B} \cup \dot{\mathcal{B}}, \zeta, T)$ is a non-zero polynomial in $k\langle Y\rangle(\mathcal{B} \cup \dot{\mathcal{B}}, \zeta)[T]$ annihilating $\dot{\zeta}$ in $\mathcal{F}_{i+1}$. This implies that $\dot{\zeta}$ is algebraic over $k\langle Y\rangle(\mathcal{B} \cup \dot{\mathcal{B}}, \zeta)$.

Since the field sub-extension

$$k\langle Y\rangle(\mathcal{B} \cup \dot{\mathcal{B}}) \hookrightarrow k\langle Y\rangle(\mathcal{B} \cup \dot{\mathcal{B}}, \zeta)$$

of $k\langle Y\rangle(\mathcal{B} \cup \dot{\mathcal{B}}) \hookrightarrow \mathcal{F}_{i+1}$ is algebraic, we conclude that $\dot{\zeta}$ is algebraic over $k\langle Y\rangle(\mathcal{B} \cup \dot{\mathcal{B}})$. ■

Proposition 33. *Let $s := ord_{k\langle Y\rangle}(\Delta)$. There exist disjoint subsets $\{W_1, \ldots, W_{m-r}\}$ and $\{\xi_1, \ldots, \xi_s\}$ of the set $\{X_1, \ldots, X_n, U_1, \ldots, U_m\}$ such that*

$$\mathcal{B}_i := \{W_1^{[i]}, \ldots, W_{m-r}^{[i]}, \xi_1, \ldots, \xi_s\}$$

is a transcendence basis of the algebraic field extension $k\langle Y\rangle \hookrightarrow \mathcal{F}_i$ for every $i \in \mathbb{N}_0$.

Moreover, the set $\{W_1, \ldots, W_{m-r}\}$ is a "good" differential transcendence basis of the differential field extension $k\langle Y\rangle \hookrightarrow Frac(k\langle Y\rangle\{X, U\}/\Delta)$.

Proof. Let $\mathcal{B}_0 \subset \{X_1, \ldots, X_n, U_1, \ldots, U_m\}$ be a transcendence basis of $k\langle Y\rangle \hookrightarrow \mathcal{F}_0$.

Then, $k\langle Y\rangle(\mathcal{B}_0) \hookrightarrow \mathcal{F}_0$ is an algebraic field extension and so, due to Lemma 32, the extension

$$k\langle Y\rangle(\mathcal{B}_0 \cup \dot{\mathcal{B}}_0) \hookrightarrow \mathcal{F}_1$$

is also algebraic. Hence, $\mathcal{B}_0 \cup \dot{\mathcal{B}}_0$ contains a transcendence basis of $\mathcal{F}_1$ over $k\langle Y\rangle$.

Since $\mathcal{B}_0$ is algebraically independent over $k\langle Y\rangle$, and

$$\text{trdeg}_{k\langle Y\rangle}(\mathcal{F}_1) = m - r + \text{trdeg}_{k\langle Y\rangle}(\mathcal{F}_0)$$

(see Theorem 28), there exists a subset $\widetilde{\mathcal{B}_0} \subset \dot{\mathcal{B}}_0$ with $m - r$ elements such that $\mathcal{B}_1 := \mathcal{B}_0 \cup \widetilde{\mathcal{B}_0}$ is a transcendence basis of $k\langle Y\rangle \hookrightarrow \mathcal{F}_1$.

Let us denote $W_1, \ldots, W_{m-r}$ the variables whose first derivatives are all the elements in $\widetilde{\mathcal{B}_0}$ (note that $\{W_1, \ldots, W_{m-r}\} \subset \mathcal{B}_0$) and let $\{\xi_1, \ldots, \xi_s\} := \mathcal{B}_0 \setminus \{W_1, \ldots, W_{m-r}\}$. We will show that, for every $i \in \mathbb{N}$, the set $\mathcal{B}_i := \{W_1^{[i]}, \ldots, W_{m-r}^{[i]}, \xi_1, \ldots, \xi_s\}$ is a transcendence basis of $k\langle Y\rangle \hookrightarrow \mathcal{F}_i$.

The case when $i = 1$ follows from our previous construction.

Let us assume now that $\mathcal{B}_i$ is a transcendence basis of $k\langle Y\rangle \hookrightarrow \mathcal{F}_i$ for a fixed positive integer $i \in \mathbb{N}$. Then, by Lemma 32,

$$k\langle Y\rangle(\mathcal{B}_i \cup \dot{\mathcal{B}}_i) = k\langle Y\rangle(\mathcal{B}_{i+1} \cup \{\dot{\xi}_1, \ldots, \dot{\xi}_s\}) \hookrightarrow \mathcal{F}_{i+1}$$

is an algebraic field extension.

Now,

$$k\langle Y\rangle(\mathcal{B}_{i+1}) \hookrightarrow k\langle Y\rangle(\mathcal{B}_{i+1} \cup \{\dot{\xi}_1, \ldots, \dot{\xi}_s\})$$

is an algebraic sub-extension of $k\langle Y\rangle(\mathcal{B}_{i+1}) \hookrightarrow \mathcal{F}_{i+1}$, since each of the elements $\dot{\xi}_j$ is algebraic over $k\langle Y\rangle(\mathcal{B}_1) \subset k\langle Y\rangle(\mathcal{B}_{i+1})$. Therefore, $k\langle Y\rangle(\mathcal{B}_{i+1}) \hookrightarrow \mathcal{F}_{i+1}$ is an algebraic extension and, taking into account that $\mathrm{trdeg}_{k\langle Y\rangle}(\mathcal{F}_{i+1})$ equals the cardinality of $\mathcal{B}_{i+1}$, we conclude that $\mathcal{B}_{i+1}$ is a transcendence basis of $k\langle Y\rangle \hookrightarrow \mathcal{F}_{i+1}$.

Finally, since $s = \mathrm{ord}_{k\langle Y\rangle}(\Delta)$ is also the transcendence degree of the extension $k\langle Y, W\rangle \hookrightarrow \mathcal{F}_i$ for any $i \geq 0$, the set $\{W_1, \ldots, W_{m-r}\}$ is a "good" transcendence basis. ■

3.4 The algorithms and their complexities

In this section, we present probabilistic algorithms for the computation of the differentiation index, of the differential Hilbert-Kolchin function of the ideal Δ and of a "good" differential transcendence basis of the extension $k\langle Y\rangle \hookrightarrow \mathcal{F}$ following the theoretical results stated in Corollary 29 and Proposition 33.

We start with the description of the algorithms. For technical and algorithmic reasons, we will assume throughout this section that the based differential field k is the rational effective field $\mathbb{Q}(t)$ (with the standard derivation), and that the polynomials defining system (2.1) have coefficients in $\mathbb{Q}[t]$.

Due to the ring inclusion $\mathbb{Q}(t)[X, U^{[2n+2r]}] \hookrightarrow A_{2n+2r}/\Delta_{2n+2r}$ (see Proposition 7), the rank computations involved in Remark 29 amount to rank computations in the polynomial ring $\mathbb{Q}[t, X, U^{[2n+2r]}]$.

First, since our algorithms will deal not only with the input polynomials f, g, which will be encoded by straight-line programs (slp), but also with their successive derivatives $\dot{f}, \dot{g}, f^{(2)}, g^{(2)}$ and so on, we need to show a way of computing a slp program for these successive derivatives. As pointed out in [45, Section 5.2], this can be done in the following way:

Lemma 34. *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 and, 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

$$\frac{\partial^j S}{\partial T^j} = f^{(j)}(T + t, \eta, \dot{\eta}, \ldots, \eta^{(j+1)}) \qquad \text{for} \qquad j = 0, \ldots, \nu - 1$$

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:

$$f^{(j)}(t, Z, \dot{Z}, \ldots, Z^{(j+1)}) = j!\, s_j(t, Z, \dot{Z}, \ldots, Z^{(j+1)}), \qquad j = 0, \ldots, \nu - 1. \tag{3.2}$$

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

First we obtain an slp encoding $S(T)$ computing:

- the monomials $\frac{T^k}{k!} = \frac{T}{k}\,\frac{T^{k-1}}{(k-1)!}$ for $k = 2, \ldots, \nu$ recursively with $2\nu - 2$ operations.
- an 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 $\alpha(4\nu - 2)$ additional operations.
- an slp encoding $S(T)$ as the composition of the slp encoding f, an slp of length 1 computing $T + t$, and those obtained for $\eta_i, \dot{\eta}_i$ $(1 \leq i \leq \alpha)$. The total length of this slp is $\mathcal{L} := 2\nu - 1 + \alpha(4\nu - 2) + L$.

Then, the procedure described in [39, Lemma 13] is applied to obtain an slp of length $\nu^2\mathcal{L}$ encoding all the coefficients s_j, $j = 0, \ldots, \nu - 1$, of $S(T)$.
Finally, the coefficients s_j are multiplied by the corresponding constant factors according to (3.2) in order to obtain the slp for the polynomials $f^{(j)}$, $j = 0, \ldots, \nu - 1$. The total length of the slp obtained is bounded by $6\,\nu^3\alpha + \nu^2 L$. ■

The rank computations over a polynomial ring involved will be reduced to probabilistic rank computations over $\mathbb{Q}$ by means of the following result:

Lemma 35. *Let $Z := \{Z_1, \ldots, Z_\alpha\}$ be a set of indeterminates over $\mathbb{Q}$ and let $A = (A_{ij})$ be a matrix in $\mathbb{Q}[Z]^{p\times q}$ whose entries satisfy $\deg(A_{ij}) \leq D_i$ 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*

$$rank_{\mathbb{Q}[Z]}(A) = rank_{\mathbb{Q}}(A(z))$$

with error probability bounded by $\frac{1}{N}\sum_{i=1}^{p} D_i$.

Proof. First, let us observe that $\mathrm{rank}_{\mathbb{Q}}(A(z)) \leq \mathrm{rank}_{\mathbb{Q}[Z]}(A)$ for every $z \in \mathbb{Q}^\alpha$.
Now, if $\mathrm{rank}(A) = s$, there is a submatrix of A of size $s \times s$ with non-zero determinant $P_0 \in \mathbb{Q}[Z]$. Since $\deg(P_0) \leq \sum_{i=1}^{p} D_i$, by the Zippel-Schwartz zero-test (see Section 1.2), if we choose the coordinates of $z := (z_1, \ldots, z_\alpha)$ at random in the set $\{0, \ldots, N - 1\}$, we have $P_0(z) \neq 0$ (and consequently $\mathrm{rank}(A(z)) = s$) with error probability at most $\frac{1}{N}\sum_{i=1}^{p} D_i$. ■

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 $\mathrm{rank}(A(z))$ may be estimated as $O((p + q)^3)$ (see, for instance, [3, Ch. 2, Sec. 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 36. *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 3. A recursive computation shows that, if $\deg(f_h) \leq d$ and $\deg(g_j) \leq d$ for every $1 \leq h \leq n$ and $1 \leq j \leq r$, then, for every $l \in \mathbb{N}_0$,*

$$\deg(\tilde{f}_h^{(l)}) \leq d + l(d-1) \quad \textit{and} \quad \deg(\tilde{g}_j^{(l)}) \leq d + l(d-1).$$

Now, we are ready to prove our algorithmic result on the computation of the differentiation index and the differential Hilbert-Kolchin function. We keep the same notations and assumptions as in Section 2.1:

Theorem 37. *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 differentiation index σ and the differential Hilbert-Kolchin function of the ideal Δ over $\mathbb{Q}(t)\langle Y\rangle$ with error probability bounded by ε within complexity $O((\log(1/\varepsilon) + \log(d))(n + m)^3(n + r)^7 L)$.*

Proof. According to Definition 25, the invariant σ is the minimum of the set $\{k \in \mathbb{N}_0 \,/\, \mu_{k,0} = \mu_{k+1,0}\}$ and it can be obtained by comparing the ranks of the matrices $\mathfrak{J}_{k,0}$ for successive values of $k \in \mathbb{N}$. The algorithm finishes, since, from proposition 17, we know that $\sigma \leq n + r$.

Fix k with $0 \leq k \leq n + r$. From the definition of $\mathfrak{J}_{k,0}$ and Remark 36, we deduce that for $l = 0, \ldots, k-1$ and $j = 1, \ldots, n + r$, the entries in the $(l(n + r) + j)$th row of $\mathfrak{J}_{k,0}$ are polynomials in $\mathbb{Q}[t, X, U^{[n+r]}]$ with degrees bounded by $d + l(d-1)$. Each of this matrices has a submatrix whose determinant is not zero and we need to choose randomly a point z_k where this determinant doesn't vanish. Since the matrix $\mathfrak{J}_{k,0}$ is a submatrix of $\mathfrak{J}_{k+1,0}$, we can compute the rank of each of this matrices, by means of Lemma 35, with error probability bounded by $p := \frac{1}{N}\sum_{k=1}^{n+r}\sum_{l=0}^{k-1}(n + r)(d + l(d-1)) \leq \frac{4}{N}d(n + r)^3$ considering only one point $z := (z_{n+r,t}, z_{n+r,X}, z_{n+r,U^{[n+r]}})$ chosen at random from the set $\{0, \ldots, N-1\}$ and where the products of all the determinants doesn't vanish. This random choice can be made within complexity $O(m(n+r)\log(N))$. Then, once the matrix $\mathfrak{J}_{n+r,0}(z)$ is obtained, each one of this ranks can be computed within complexity $O(k^3((n + r)^3 + (n + m)^3)$ and all of them with $O((n + m)^3(n + r)^4)$.

In order to compute the entries of the matrices $\mathfrak{J}_{n+r,0}(z)$, we proceed as follows: first, we derive slp's of length $O((n + r)^2((n + r)(n + m) + L))$ for the polynomials $F_h^{[n+r-1]}$, $G_j^{[n+r-1]}$ from the slp's encoding $f_1, \ldots, f_n, g_1, \ldots, g_r$, as stated in Lemma 34. 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 $\{X, U\}^{[n+r]}$. The Bauer-Strassen algorithm (see, for instance, [8, 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 $\tilde{f}_h^{(l)}$ $(1 \leq h \leq n,\ 0 \leq l \leq n + r)$ and then, slp's of the same order for the entries of $\mathfrak{J}_{n+r,0}$, by composition. Finally, we compute the entries of $\mathfrak{J}_{n+r,0}(z)$ by specializing the slp's encoding the entries of

$\mathfrak{J}_{n+r,0}$ into z. 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 differentiation index of the ideal Δ with probability at least $1-p \geq 1-\frac{4}{N}d(n+r)^3$ within complexity $O(m(n+r)\log(N)+(n+m)^3(n+r)^7L)$.

To bound the error probability of the algorithm by ε, we take $N := \lceil 1/\varepsilon \rceil 4d(n+r)^3$. With this choice, the overall complexity of the procedure is of order $O((\log(1/\varepsilon)+\log(d))(n+m)^3(n+r)^7L)$.

From Remark 29 we have that

$$H_{\Delta,k\langle Y\rangle}(i+1) = (m-r)(i+1) + \mathrm{rk}_{k(X)\langle U\rangle}(\mathfrak{J}_{\sigma,0}) - (\sigma-1)(n+r)$$

and thus from the computation of σ we also obtain the Hilbert-Kolchin function of the ideal Δ and $\mathrm{ord}_{k\langle Y\rangle}(\Delta)$. ■

This finishes the presentation of the algorithm for the computation of the differential Hilbert-Kolchin function. In order to compute a differential transcendence basis we will use the following well-known result from commutative algebra:

Lemma 38. *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 $\mathrm{rank}_R(J^{Z_j}) = \mathrm{rank}_R(J)$.*

Proof. Assuming that Z_j is transcendental modulo $\wp$, we have inclusions $K(Z_j) \subset R \otimes K(Z_j) \subset \mathrm{Frac}(R)$. Therefore, by the Jacobian criterion (see [42, Ch. VI, §1, Theorem 1.15]), we have

$$\mathrm{rank}_R(J^{Z_j}) = (\alpha-1) - \mathrm{trdeg}_{K(Z_j)}(\mathrm{Frac}(R)) = \alpha - 1 - (\mathrm{trdeg}_K(\mathrm{Frac}(R)) - 1) =$$

$$= \alpha - \mathrm{trdeg}_K(\mathrm{Frac}(R)) = \mathrm{rank}_R(J).$$

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 system $f_1,\ldots,f_s,f_{s+1}$ is another set of generators of $\wp$ and then the rank of the its Jacobian matrix $\mathcal{J}$ equals that of the Jacobian matrix J, since both are the codimension of $\wp$. But

$$\mathcal{J} = \begin{pmatrix} \frac{\partial f_1}{\partial Z_1} & \cdots & \frac{\partial f_1}{\partial Z_j} & \cdots & \frac{\partial f_1}{\partial Z_\alpha} \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ \frac{\partial f_s}{\partial Z_1} & \cdots & \frac{\partial f_s}{\partial Z_j} & \cdots & \frac{\partial f_s}{\partial Z_\alpha} \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ 0 & \cdots & \frac{\partial f_{s+1}}{\partial Z_j} & \cdots & 0 \end{pmatrix} = \begin{pmatrix} J \\ 0\ldots\frac{\partial f_{s+1}}{\partial Z_j}\ldots 0 \end{pmatrix}$$

and then we have that $\text{rank}_R(\mathcal{J}) = \text{rank}_R(J^{Z_j}) + 1$. Therefore, $\text{rank}_R(J) = \text{rank}_R(J^{Z_j}) + 1$ and so $\text{rank}_R(J^{Z_j}) < \text{rank}_R(J)$. ■

We now show our main result on the computation of a differential transcendence basis. Since the algorithm is based on the results obtained in Proposition 33, it will be clear that the differential basis we will obtain is a "good" basis.

Theorem 39. *There is a probabilistic algorithm which computes, for every $\varepsilon \in (0,1)$, a "good" 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. The algorithmic computation of a differential transcendence basis of the differential field extension $k\langle Y\rangle \hookrightarrow \text{Frac}(k\langle Y\rangle\{X,U\}/\Delta)$ follows the procedure underlying the proof of Proposition 33. Let σ be the differential index and let $\mathfrak{J}_\sigma$ and $\mathfrak{J}_{\sigma+1}$ be the matrices introduced in Remark 12, from this same Remark these matrices has full row rank.

- In a first step, the algorithm chooses the coordinates of a point $z := (z_t, z_X, z_{U^{[\sigma+1]}})$ at random from the set $\{0,\ldots,N-1\}$ for a sufficiently big integer N and computes $\text{rank}(\mathfrak{J}_\sigma(z))$ and $\text{rank}(\mathfrak{J}_{\sigma+1}(z))$. If these matrices have not full row rank, it returns an error message.

  Otherwise, the algorithm proceeds recursively, starting with the set of variables $\mathcal{B}_0$ being the empty set:

- The set $\mathcal{B}_0$ is constructed recursively by adding one variable at a time. In order to determine whether a subset of variables in $\mathcal{F}_0$ is transcendental over the field $k\langle Y\rangle$, we use the fact that $\mathcal{F}_0 \hookrightarrow A_\sigma/\Delta_\sigma$. Thus, the problem amounts to determine whether a subset of variables in a quotient of a polynomial ring by a prime ideal is transcendental over the base field, which can be done applying the Lemma 38.

  Let us rename for a moment the variables $\{X_1,\ldots,X_n,U_1,\ldots,U_m\}$ as $\{V_1,\ldots,V_{n+m}\}$. For $k \le n+m$, the kth recursive step is as follows: if $\#\mathcal{B}_0 < m - r + \text{ord}(\Delta)$, the algorithm computes the rank of the matrix $\mathfrak{J}_\sigma(z)^{\mathcal{B}_0\cup\{V_k\}}$ which is obtained by removing the columns of $\mathfrak{J}_\sigma(z)$ corresponding to derivatives with respect to the variables $(\mathcal{B}_0 \cup \{V_k\})$. If $\text{rank}(\mathfrak{J}_\sigma(z)^{W\cup\{V_k\}}) = \text{rank}(\mathfrak{J}_\sigma(z))$, the variable V_k is added to the set $\mathcal{B}_0$. Otherwise, $\mathcal{B}_0$ is not modified. When $\#\mathcal{B}_0 = m - r + \text{ord}(\Delta)$, the algorithm outputs the set $\mathcal{B}_0$.

  If the recursion finishes with $\#\mathcal{B}_0 \neq m - r + \text{ord}(\Delta)$, the algorithm returns an error message.

- The last step is to choose a subset $\widetilde{\mathcal{B}_0} \subset \dot{\mathcal{B}}_0$ with $m - r$ elements such that $\mathcal{B}_1 := \mathcal{B}_0 \cup \widetilde{\mathcal{B}_0}$ is a transcendence basis of $k\langle Y\rangle \hookrightarrow \mathcal{F}_1$ using that $\mathcal{F}_1 \hookrightarrow A_{\sigma+1}/\Delta_{\sigma+1}$. To do this, the algorithm uses

the same procedure described above erasing columns of the matrix rank($\mathfrak{J}_{\sigma+1}(z)$) and comparing ranks.

Then, the variables $W_1, \ldots, W_{m-r}$ whose derivatives lie in $\widetilde{\mathcal{B}_0}$ are a "good" differential transcendence basis of $k\langle Y\rangle \hookrightarrow \mathrm{Frac}(k\langle Y\rangle\{X, U\}/\Delta)$.

Now let us estimate the error probability of this procedure: let W be the differential transcendence basis of $\mathbb{Q}(t)\langle Y\rangle \hookrightarrow \mathcal{F}$ computed in this way. Then, the matrix $\mathfrak{J}_\sigma^W$ which is obtained from $\mathfrak{J}_\sigma$ by removing the columns corresponding to derivatives with respect to the variables W has full row rank, and so, it has a square submatrix of size $(n+r)\sigma$ with non-zero determinant P_0. The same argument is applied to $\mathfrak{J}_{\sigma+1}$ to obtain a non-zero determinant of a submatrix of size $(n+r)(\sigma+1)$, P_1. Therefore, any point $z := (z_t, z_X, z_{U^{[\sigma+1]}})$ satisfying $P_0(z)P_1(z) \neq 0$ leads to matrices $\mathfrak{J}_\sigma(z)$ and $\mathfrak{J}_{\sigma+1}(z)$ with full row rank for which the algorithm computes the desired differential transcendence basis. Since $\deg P_0P_1 \leq 4d(n+r)^3$ (this estimate follows as in the proof of Theorem 37), we conclude that the error probability of the algorithm is at most $\frac{4}{N}d(n+r)^3$.

Choosing $N := \lceil 1/\varepsilon\rceil 4d(n+r)^3$, the error probability of the algorithm is bounded by ε. The complexity bound can be obtained as in the proof of Theorem 37. ■

Remark 40. *The algorithm in Theorem 39 probabilistically computes a differential transcendence basis of $\mathbb{Q}(t)\langle Y\rangle \hookrightarrow \mathcal{F}$, which is also the differentially algebraically independent subset of $\{X, U\}$ minimal with respect to the lexicographical ordering of the variables in which*

$$X_1 < X_2 < \cdots < X_n < U_1 < U_2 < \cdots < U_m.$$

But, even if it actually fails to compute this particular basis, 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.

We finish this chapter with a very simple (linear) example that illustrates how the results, obtained here, apply for the computation of the differential index, the differential Hilbert-Kolchin function and a "good" differential transcendence basis.

Consider the differential system:

$$(\tilde{\Sigma}) = \begin{cases} Y_1 &= U_1 + \dot{U}_2 + \dot{U}_3 \\ Y_2 &= \dot{U}_1 + U_2 + U_3 \end{cases}$$

In this case, $n = 0, r = 2$ and $m = 3$.

According to Theorem 37, the differential index and the differential Hilbert-Kolchin function of the ideal $\Delta = [Y_1 - U_1 + \dot{U}_2 + \dot{U}_3, Y_2 - \dot{U}_1 + U_2 + U_3] \subset k\langle Y\rangle\{U\}$ are obtained from the computation of the ranks of the associated matrices $\mathfrak{J}_{k,0}$ ($k \geq 0$).

The first one of these matrices,

$$\mathfrak{J}_{1,0} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

has full row rank 2 and then the dimension of $\ker(\mathfrak{J}_{1,0}^t) = 0$.

Following Definition 15 we deduce that $\mu_{1,0} = \mu_{0,0} = 0$ and so, the differentiation index of this system is $\sigma = 0$ (and $\mu_{\sigma,0} = 0$).

From this and Corollary 29, we conclude that $\mathcal{H}_{k\langle Y\rangle,\Delta}(i) = (m-r)(i+1) + n + r - \mu_{\sigma,0} = (i+1) + 2$.

Now we will apply to the system $(\tilde{\Sigma})$ the algorithm described in Theorem 39, based on the results from Proposition 33 and Lemma 38, to show how to find a "good" differential transcendence basis of the differential field extension $k\langle Y\rangle \hookrightarrow \mathrm{Frac}(k\langle Y\rangle\{U\}/\Delta)$.

From the computations above, we already know that the differential index σ is 0 and then $\Delta \cap A_0 = \Delta_0 = 0$, the order of the ideal Δ is 2 and $\mathrm{dimdiff}_{k\langle Y\rangle}(k\langle Y\rangle\{U\}/\Delta) = 1$.

Since $\mathcal{F}_0 = \mathrm{Frac}(A_0/\Delta \cap A_0) = \mathrm{Frac}(A_0) = \mathrm{Frac}(k\langle Y\rangle[U_1, U_2, U_3])$, the natural choice for the set $\mathcal{B}_0$ is $\{U_1, U_2, U_3\}$. The next step is to find a subset $\tilde{\mathcal{B}}_0 \subset \dot{\mathcal{B}}_0$ such that $\mathcal{B}_1 = \mathcal{B}_0 \cup \tilde{\mathcal{B}}_0$ is a transcendence basis of the extension $k\langle Y\rangle \hookrightarrow \mathcal{F}_1 = \mathrm{Frac}(A_1/\Delta \cap A_1) = \mathrm{Frac}(A_1/\Delta_1)$. To do this, let us apply Lemma 38 to the matrix

$$\mathfrak{J}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

This matrix has full row rank, and the same remains true when the columns corresponding to either the variables $\{U_1, U_2, U_3, \dot{U}_2\}$ or the variables $\{U_1, U_2, U_3, \dot{U}_3\}$ are removed. Therefore both $\{U_2\}$ and $\{U_3\}$ can be considered as differential transcendence bases.

However, the rank of $\mathfrak{J}_1$ drops when removing the columns corresponding to $\{U_1, U_2, U_3, \dot{U}_1\}$, this implies that $\{U_1\}$ cannot be chosen as a differential transcendence basis, in fact we have $U_1^{(2)} - U_1 - \dot{Y}_2 + Y_1 = 0$.

Chapter 4

Resolvent representation

In his seminal book [52], J.F. Ritt introduced a description of the generic zero of a prime differential ideal $\mathcal{I}$ as the zeros of a single ordinary differential polynomial M in a new variable *(primitive element)* obtained as a linear form on the old ones. Moreover, he showed that the generic zero of the original ideal is *birationally equivalent* to the general zero of M. Following his terminology, we call this polynomial M a *resolvent*. The resolvent together with rational relationships linking the non-singular zeros of M to the generic zero of the original prime ideal is call a *resolvent representation*. This type of alternative description of the generic zeros of a prime ideal in the purely algebraic context can be trace back to the work of Kronecker [41]. In other words, with a resolvent representation, finding all the solutions of the initial differential system boils down to solving a single independent equation, that is, the resolvent.
The main goal of this chapter is the computation of a resolvent representation of the ideal Δ (see Definition 6) associated to the system (2.1).
The beginning of the first section of this chapter is concerned with the notions of a primitive element of a differentially algebraic field extension and that of a resolvent representation of a prime differential ideal in general. We present these concepts following [59] in Subsection 4.1. In the remaining subsections, we study quantitative aspects, namely order and degree of these objects, for our particular system (2.1). The following section is devoted to the construction of a probabilistic algorithm for the computation of the resolvent representation. The final section studies a generalization of these results to the case of systems of higher order.

4.1 Existence of a primitive element and a resolvent representation

We recall here 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 $\operatorname{diffdim}(\mathcal{I}) = 0$. Set $\mathcal{F} := \operatorname{Frac}(K\{Z\}/\mathcal{I})$ 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 [52] and [59]).

Let us recall that, as we stated at the beginning of Section 2.2, we are denoting in the same way a differential polynomial in a differential polynomial ring, its class in the quotient ring by a differential prime ideal and the image in its field of fractions.

We include here a slightly modified version of Seidenberg's proof since the arguments therein are useful for several effective results we will prove later.

Theorem 41. *(see also [59, Theorem 1]) With the previous assumptions and notations, there exists $\gamma \in \mathcal{F}$ such that $\mathcal{F} = K\langle\gamma\rangle$. Moreover, $\gamma \in K\{Z\}$ 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 $K\langle Z\rangle$ and consider $\mathcal{F}\langle\Lambda\rangle$. This field $\mathcal{F}\langle\Lambda\rangle$ 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 finite differentially algebraic field extension.

Then, if

$$\Gamma := \Lambda_1 Z_1 + \cdots + \Lambda_\alpha Z_\alpha \ \in \ K\langle\Lambda\rangle\{Z\},$$

the set of derivatives

$$\left\{\Gamma^{(l)} = \sum_{i=1}^{\alpha}\sum_{j=0}^{l}\binom{l}{j}\Lambda_i^{(j)} Z_i^{(l-j)} : l \in \mathbb{N}_0\right\} \subset \mathcal{F}\langle\Lambda\rangle$$

is differentially algebraically dependent over $K\langle\Lambda\rangle$ and so, there exists a differential polynomial $\mathcal{X}(T) \in K\langle\Lambda\rangle\{T\}$, 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, $\mathcal{X}(\Gamma, \dot{\Gamma}, \ldots, \Gamma^{(h)}) = 0$ in $\mathcal{F}\langle\Lambda\rangle$ and so, also $\partial\mathcal{X}(\Gamma, \ldots, \Gamma^{(h)})/\partial\Lambda_i^{(h)} = 0$ in $\mathcal{F}\langle\Lambda\rangle$, for $i = 1, \ldots, \alpha$. In other words,

$$\partial\mathcal{X}(\Gamma, \ldots, \Gamma^{(h)})/\partial\Lambda_i^{(h)} = \frac{\partial\mathcal{X}}{\partial T^{(h)}}(\Gamma, \ldots, \Gamma^{(h)})\, Z_i + \frac{\partial\mathcal{X}}{\partial\Lambda_i^{(h)}}(\Gamma, \ldots, \Gamma^{(h)}) \in K\{\Lambda\} \otimes \mathcal{I}, \tag{4.1}$$

where $\partial\mathcal{X}(\Gamma, \ldots, \Gamma^{(h)})/\partial\Lambda_i^{(h)}$ on the left hand side of the equality is the partial derivation of $\mathcal{X}(\Gamma, \ldots, \Gamma^{(h)})$ with respect to $\Lambda_i^{(h)}$ and $\dfrac{\partial\mathcal{X}}{\partial\Lambda_i^{(h)}}(\Gamma, \ldots, \Gamma^{(h)})$ on the right hand side is the evaluation in $\Gamma, \ldots, \Gamma^{(h)}$ of the polynomial obtained by applying the partial derivation with respect to $\Lambda_i^{(h)}$ to $\mathcal{X}(T)$.

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 polynomial in $\mathcal{F}\{\Lambda\}$

$$Q_\Lambda(\Lambda_1, \ldots, \Lambda_\alpha) := \frac{\partial \mathcal{X}}{\partial T^{(h)}}(\Gamma, \ldots, \Gamma^{(h)}) \neq 0.$$

Since $\xi \in \mathcal{F}$ is a non-constant element, a result in [52, Ch. 2, §22] shows the existence of elements $\lambda_i \in \mathbb{Q}[\xi]$, for $i = 1, \ldots, \alpha$, such that $Q_\Lambda(\lambda_1, \ldots, \lambda_\alpha) \neq 0$.
Now, if we take $\gamma := \lambda_1 Z_1 + \cdots + \lambda_\alpha Z_\alpha \in K\{Z\}$, we deduce from Identity (4.1) that $Z_i \in K\langle\gamma\rangle \subset \mathcal{F}$ for $i = 1, \ldots, \alpha$, which implies that $\mathcal{F} = K\langle\gamma\rangle$. ■

Let us point out that this theorem doesn't hold if we remove the hypothesis that K has a non constant element: for if we suppose that all the elements of K were constants, let us consider the differential ideal $\mathcal{I} = [\dot{Z}_1, \dot{Z}_2] \subset K\{Z_1, Z_2\}$. The differential fields $\mathcal{F} = \mathrm{Frac}(K\{Z_1, Z_2\}/\mathcal{I})$ and $K(Z_1, Z_2)$, where $K(Z_1, Z_2)$ is viewed as a differential field by setting every derivative equal to 0, are isomorphic. Then, for any $\gamma \in \mathcal{F}$, $K\langle\gamma\rangle = K(\gamma)$ and $K(Z_1, Z_2) = K\langle Z_1, Z_2\rangle = K(\gamma)$ is clearly impossible since $\mathrm{trdeg}_K K(Z_1, Z_2) = 2$ and $\mathrm{trdeg}_K K(\gamma) = 1$.

Definition 42. *With the same assumptions and notations as before, 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 0-dimensional prime differential ideal (see Definition 1) 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 43. *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 (this maximum exists because the extension is assumed to be of differential dimension 0). Let T be a new differential variable. Then:*

i) For every $\zeta \in K\{Z\}$, there exist polynomials P_ζ and $Q_\zeta \in K[T^{[s]}]$ such that

$$\zeta = P_\zeta(\gamma^{[s]})/Q_\zeta(\gamma^{[s]}) \text{ in } \mathcal{F}.$$

In particular, $\{\gamma, \ldots, \gamma^{(s-1)}\}$ is an algebraic transcendence basis of the extension $K \hookrightarrow \mathcal{F}$ and $\mathcal{F} = K(\gamma, \ldots, \gamma^{(s-1)}, \gamma^{(s)})$.

ii) $s = ord_K(\mathcal{I})$.

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 $S_M \in K[T^{[s]}]$ the polynomial $S_M := \frac{\partial M}{\partial T^{(s)}}$. We have $I_M(\gamma) \neq 0$ and $S_M(\gamma) \neq 0$ in $\mathcal{F}$. By a simplified version of the derivation and division process described in [38, Ch. I, Sec. 9, Proposition 1], 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 $M^{(j)}(\gamma) = 0$ for every $j \geq 0$, we have that the following identities hold $\mathcal{F}$:

$$R_P(\gamma^{[s]}) = I_M^{a_1}(\gamma) S_M^{b_1}(\gamma) P(\gamma) \quad \text{and} \quad R_Q(\gamma^{[s]}) = I_M^{a_2}(\gamma) S_M^{b_2}(\gamma) Q(\gamma).$$

Thus, defining

$$P_\zeta := I_M^{a_2} S_M^{b_2} R_P \in K[T^{[s]}] \quad \text{and} \quad Q_\zeta := I_M^{a_1} S_M^{b_1} R_Q \in K[T^{[s]}]$$

we obtain the identity in $\mathcal{F}$

$$\zeta = P_\zeta(\gamma^{[s]})/Q_\zeta(\gamma^{[s]}),$$

which finishes the proof of the first part of the proposition.

To prove *ii)*, we observe that, for ν big enough, the elements $\gamma, \ldots, \gamma^{(s)}$ can be regarded as elements of

$$\mathcal{L}_\nu := \mathrm{Frac}(K[Z^{[\nu]}]/\mathcal{I} \cap K[Z^{[\nu]}]) \subset \mathcal{F},$$

and so, we deduce from *i)* that $\mathcal{L}_\nu = \mathcal{F}$. Therefore,

$$s = \mathrm{trdeg}_K(\mathcal{F}) = \mathrm{trdeg}_K(\mathcal{L}_\nu) = \mathcal{H}_{\mathcal{I},K}(\nu) = \mathrm{ord}_K(\mathcal{I}),$$

for ν big enough, where the last equality is due to the fact that $\mathcal{I}$ is a 0-dimensional differential ideal. ■

Let $\gamma \in K\{Z\}$ be a primitive element of the differential field extension $K \hookrightarrow \mathcal{F}$ and set $s := \mathrm{ord}_K(\mathcal{I})$. By Proposition 43, $\{\gamma, \ldots, \gamma^{(s-1)}\}$ is a transcendence basis of the extension $K \hookrightarrow \mathcal{F}$. 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 $\mathcal{F}$ (that is, $M(\gamma, \ldots, \gamma^{(s)}) \in \mathcal{I}$). 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 any minimal polynomial M of γ divides P in $K(T, \ldots, T^{(s-1)})[T^{(s)}]$ and, being M 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 43, there exist polynomials p_i, q_i of order bounded by s satisfying these conditions).

Definition 44. *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* 0*-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 $\tilde{Z} := Z \setminus W = \{\tilde{Z}_1, \ldots, \tilde{Z}_{\alpha-r}\}$, the ideal $K \otimes \mathcal{I}$ of $K\{\tilde{Z}\}$ has differential dimension zero and the field $\mathcal{F}$ is the fraction field of $K\{\tilde{Z}\}/K \otimes \mathcal{I}$. Then, the previous assumptions hold and so, there exist a primitive element $\gamma \in K\{\tilde{Z}\}$ of the extension $K \hookrightarrow \mathcal{F}$ and a resolvent representation $\{M, q_1(T)\tilde{Z}_1 - p_1(T), \ldots, q_{\alpha-r}(T)\tilde{Z}_{\alpha-r} - p_{\alpha-r}(T)\}$ 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 $1 \leq i \leq \alpha$. The set

$$\{M, q_1(T)\tilde{Z}_1 - p_1(T), \ldots, q_{\alpha-r}(T)\tilde{Z}_{\alpha-r} - p_{\alpha-r}(T)\} \subset \mathcal{K}\{W\}\{T\}$$

is called a *resolvent representation of the prime differential ideal $\mathcal{I}$ with respect to the transcendence basis W and the primitive element γ.*

4.1.1 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 (2.1). We keep the same notations and assumptions as in Chapters 2 and 3. We will further assume that our differential base field k contains a non-constant element and that a "good" differential transcendence basis $W \subset \{X, U\}$ of $k\langle Y\rangle \hookrightarrow \mathcal{F}$ has been fixed (see Section 3.3).
First, we will prove an upper bound for the total order, that is, the order of derivation of all the variables involved, 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 (see Proposition 48 and Theorem 49 below).

Denote $V = \{V_1, \dots, V_{n+r}\} := \{X, U\} \setminus W$ and $K := k\langle Y, W\rangle$. From Proposition 9 and the fact that W is a differential transcendence basis we deduce that the differential ideal generated by the polynomials F and G, is a 0-dimensional prime differential ideal of $K\{V\}$ that we will denote by $\tilde{\Delta} := [F, G]$.

Let $\gamma := \lambda_1 V_1 + \cdots + \lambda_{n+r} V_{n+r} \in k[V]$ be a linear form such that $\gamma \in \mathcal{F}$ is a primitive element of the differential field extension $K \hookrightarrow \mathcal{F}$.

Since W was chosen as a "good" basis, $\mathrm{ord}_{k\langle Y\rangle}(\Delta) = \mathrm{ord}_K(\tilde{\Delta})$. Set $s := \mathrm{ord}_K(\tilde{\Delta})$; so, a minimal polynomial M of γ in $K \hookrightarrow \mathcal{F}$ lies in $K[T, \dots, T^{(s)}]$ (see Proposition 43).

From now on, we will denote for $i \geq 0$, $\tilde{A}_i := K[V^{[i]}]$ and $\tilde{\Delta}_i := (F^{[i-1]}, G^{[i-1]}) \subset \tilde{A}_i$.

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 45. *There exists a minimal polynomial $M \in K[T, \dots, T^{(s)}]$ of γ in $K \hookrightarrow \mathcal{F}$ such that M belongs to the polynomial ring $k[Y^{[2n+2r-1]}, W^{[2n+2r]}][T^{[s]}]$ and*

$$M(\gamma, \dots, \gamma^{(s)}) \in (F^{[2n+2r-1]}, G^{[2n+2r-1]}) \subset k[Y^{[2n+2r-1]}, X^{[2n+2r]}, U^{[2n+2r]}].$$

Proof. As in the proof of Proposition 43 *-ii)*, since the primitive element γ has order 0 and $s \leq n + r$ (Corollary 29), we have that the field $\mathcal{F}$ coincides with the field $\mathrm{Frac}(\tilde{A}_{n+r}/\tilde{\Delta} \cap \tilde{A}_{n+r})$. Then, if $P \in K[T, \dots, T^{(s)}]$ is a minimal polynomial of γ in $K \hookrightarrow \mathcal{F}$, we have that

$$P(\gamma, \dots, \gamma^{(s)}) \in \tilde{\Delta} \cap \tilde{A}_{n+r}.$$

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 Theorem 26, it can be shown that

$$\tilde{\Delta} \cap \tilde{A}_{n+r} = \tilde{\Delta}_{2n+2r} \cap \tilde{A}_{n+r}$$

and so,

$$P(\gamma, \dots, \gamma^{(s)}) \in \tilde{A}_{n+r} \cap \tilde{\Delta}_{2n+2r}.$$

Thus, for $1 \leq i \leq n$, $1 \leq j \leq r$, $0 \leq k \leq 2n + 2r - 1$, there exist polynomials $a_{ik}, b_{jk} \in \tilde{A}_{2n+2r}$ such that

$$P(\gamma, \dots, \gamma^{(s)}) = \sum_{k=0}^{2n+2r-1} \left(\sum_{i=1}^{n} a_{ik} F_i^{(k)} + \sum_{j=1}^{r} b_{jk} G_j^{(k)} \right).$$

If $l \in \mathbb{N}$ is the biggest order of derivation appearing in this identity, multiplying it by a polynomial in $k\{Y, W\}$, we may assume that a_{ik}, b_{jk} belong to the polynomial ring $k[Y^{[l]}, W^{[l]}, V^{[2n+2r]}]$ and that $P \in k[Y^{[l]}, W^{[l]}][T^{[s]}]$.

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 $y_0 := (y_{2n+2r}, \dots, y_l)$ and $w_0 := (w_{2n+2r+1}, \dots, w_l)$ be rational vectors such that the specialization $I_P(Y^{[2n+2r-1]}, y_0, W^{[2n+2r]}, w_0, T^{[s-1]})$ is not the zero-polynomial in the variables $Y^{[2n+2r-1]}, W^{[2n+2r]}, T^{[s-1]}$.

Making this same 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

$$M(\gamma, \ldots, \gamma^{(s)}) \in (F^{[2n+2r-1]}, G^{[2n+2r-1]}).$$

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 give a more precise statement of the result in terms of the differentiation index, as follows:

Remark 46. *Let σ be differentiation index (see Definition 25). As in Theorem 26, σ is the minimum integer such that the identity $\tilde{\Delta} \cap \tilde{A}_i = \tilde{\Delta}_{i+\sigma} \cap \tilde{A}_i$ holds for every $i \in \mathbb{N}$. Then, there is a minimal polynomial*

$$M \in k[Y^{[s+\sigma-1]}, W^{[s+\sigma]}][T^{[s]}] \text{ such that } M(\gamma, \ldots, \gamma^{(s)}) \in \Delta_{s+\sigma}.$$

Note that $\sigma \leq n + r$ (see Proposition 17) and $s \leq n + r$ (see Remark 29).

We have now all the ingredients we need 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 $\bar{k}$, the algebraic closure of k, which will be denoted simply by $\mathbb{A}$. This affine spaces will be equipped with their Zariski topologies over k, that is, the polynomial defining this topology will be taken with coefficients in k .

Notation 47. *Let $N_1 := r(2n + 2r) + (n + m)(2n + 2r + 1)$ and $\mathbb{V} \subset \mathbb{A}^{N_1}$ be the irreducible variety defined by the ideal $(F^{[2n+2r-1]}, G^{[2n+2r-1]}) \subset k[Y^{[2n+2r-1]}, W^{[2n+2r]}, V^{[2n+2r]}]$ (see Remark 4).*

Arbitrary points of the corresponding affine spaces will be denoted by

$$\begin{array}{rcccl} y & := & (y_1, \ldots, y_r, \ldots, y_1^{(2n+2r-1)}, \ldots, y_r^{(2n+2r-1)}) & \in & \mathbb{A}^{r(2n+2r)} \\ w & := & (w_1, \ldots, w_{m-r}, \ldots, w_1^{(2n+2r)}, \ldots, w_{m-r}^{(2n+2r)}) & \in & \mathbb{A}^{(m-r)(2n+2r+1)} \\ v & := & (v_1, \ldots, v_{n+r}, \ldots, v_1^{(2n+2r)}, \ldots, v_{n+r}^{(2n+2r)}) & \in & \mathbb{A}^{n(2n+2r+1)} \end{array} \tag{4.2}$$

Let $N_2 := r(2n + 2r) + (m - r)(2n + 2r + 1) + s + 1$ and consider the linear map

$$\begin{array}{rccc} \pi : & \mathbb{V} & \longrightarrow & \mathbb{A}^{N_2} \\ & (y, w, v) & \mapsto & (y, w, \gamma(v), \ldots, \gamma^{(s)}(v)), \end{array}$$

where, for $l = 0, \ldots, s$,

$$\gamma^{(l)} := \sum_{k=0}^{l} \binom{l}{k} \left(\sum_{i=1}^{n+r} \lambda_i^{(k)} V_i^{(l-k)}\right) \tag{4.3}$$

(recall that $\gamma := \lambda_1 V_1 + \cdots + \lambda_{n+r} V_{n+r} \in k[V]$ is a linear form such that $\gamma \in \mathcal{F}$ is a primitive element of the differential field extension $K \hookrightarrow \mathcal{F}$).

The following proposition describes a minimal polynomial of a primitive element as the defining equation describing the image of the variety $\mathbb{V}$ by the algebraic morphism π:

Proposition 48. *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 the primitive element 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, on the one hand we have 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, in particular, $P(\gamma, \ldots, \gamma^{(s-1)}) = 0$ in $\mathcal{F}$, contradicting the algebraic independence of $\gamma, \ldots, \gamma^{(s-1)}$ in $k\langle Y, W\rangle \hookrightarrow \mathcal{F}$ (recall that $[F, G] \cap k\{Y, W\} = 0$) and this implies that $\overline{\pi(\mathbb{V})}$ has, at most, codimension 1.

On the other hand, due to Lemma 45, we have that there is a non-zero polynomial M, belonging to $k[Y^{[2n+2r-1]}, W^{[2n+2r]}][T^{[s]}]$, such that $M(\gamma, \ldots, \gamma^{(s)}) \in (F^{[2n+2r-1]}, G^{[2n+2r-1]})$; thus, $\overline{\pi(\mathbb{V})}$ is a subvariety of $\{M = 0\}$ and so, its codimension is at least 1.

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

Using [29, Lemma 2 and Theorem 1], we obtain an upper bound on the degree of the minimal polynomial given by the previous proposition:

Theorem 49. *Let $\gamma = \lambda_1 V_1 + \cdots + \lambda_{n+r} V_{n+r}$ 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 $d := \max\{\deg(f_i), \deg(g_j);\ 1 \le i \le n,\ 1 \le j \le r\}$, due to the Bézout inequality, we deduce that the degree of the polynomial M is bounded by $d^{2(n+r)^2}$. ■

The estimation of the degree of the minimal polynomial of this last theorem will be improved in Appendix C for the particular case of a system (2.1) with $r = 0$, that is, with no polynomials g's involved, which are the systems typically consider in the classical theory of ordinary differential equations. This improvement will be obtained by computing a more accurate upper bound for the degree of the variety $\pi(\mathbb{V})$ for this particular case than the one obtained applying Bézout inequality.

Following Remark 46, 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 50. *If $\mathbb{V}_{s+\sigma}$ denotes the variety defined by the ideal $(F^{[s+\sigma-1]}, G^{[s+\sigma-1]})$, there is a minimal polynomial $M \in k[Y^{[s+\sigma-1]}, W^{[s+\sigma]}, T^{[s]}]$ with degree bounded by*

$$\deg(M) \le \deg(\mathbb{V}_{s+\sigma}) \le d^{(n+r)(s+\sigma)}.$$

4.1.2 An example

The following is an example where the upper bounds for the order and the degree of the minimal polynomial in terms of the geometric degree stated in the previous section are reached. In addition, it shows that for certain particular systems, our geometric upper bounds may be considerably smaller than the syntactic single exponential ones. Bézout-type degree bounds for the polynomials involved in the resolvent representation of the classical, explicit systems without parametric equations g's will be studied in Appendix C.

Example 51. *Let us consider the following system over the differential field $k = \mathbb{Q}(t)$:*

$$(\Sigma) = \left\{ \begin{array}{rcl} \dot{X}_1 & = & X_1^2 \\ \dot{X}_2 & = & X_1^2 \\ & \vdots & \\ \dot{X}_n & = & X_1^2 \end{array} \right. .$$

Here, $r = m = 0$ (that is, there are no variables Y or U involved and no polynomials G) and so $k = K$, $\Delta = \tilde{\Delta} = [F]$, $V = X$ and $\mathcal{F} = \mathrm{Frac}(k\{X\}/[F])$ (thus, $\mathrm{dimdiff}_K(\mathcal{F}) = 0$).

It is clear that

$$\Delta \cap K[X^{[i]}] = [F] \cap k[X^{[i]}] = (F^{[i-1]}) = \Delta_i \text{ for every } i \in \mathbb{N}$$

(and so the differentiation index σ of Definition 25 is 0). This implies that

$$\mathcal{H}_{k,[F]}(i) = \mathrm{trdeg}_k \mathrm{Frac}(k[X^{[i]}]/(F^{[i-1]})) = n$$

and then, $s = \mathrm{ord}_k([F]) = \mathrm{ord}_K(\Delta) = n$.

In order to apply the results of Remark 50 we need to compute the degree of the variety $\mathbb{V}_n \subset \mathbb{A}^{n^2}$ defined by the ideal $(F^{(n-1)})$:

$$\mathbb{V}_n = \left\{ (z_1, \ldots, z_n, \underbrace{z_1^2, \ldots, z_n^2}_{n\text{-times}}, \underbrace{2z_1^3, \ldots, 2z_n^3}_{n\text{-times}}, \ldots, \underbrace{n!z_1^{n+1}, \ldots, n!z_n^{n+1}}_{n\text{-times}}) \text{ with } (z_1, \ldots, z_n) \in \mathbb{A}^n \right\}.$$

Claim: The degree of the variety $\mathbb{V}_n$ is $n + 1$.

Proof: The variety $\mathbb{V}_n$ is isomorphic to $\mathbb{A}^{n-1} \times \mathbb{W}_n$ where

$$\mathbb{W}_n := \left\{ (z_1, \underbrace{z_1^2, \ldots, z_1^2}_{n\text{-times}}, \underbrace{2z_1^3, \ldots, 2z_1^3}_{n\text{-times}}, \ldots, \underbrace{n!z_1^{n+1}, \ldots, n!z_1^{n+1}}_{n\text{-times}}) \text{ with } z_1 \in \mathbb{A}^1 \right\}$$

via an invertible linear application which doesn't change the degree. Then, it is enough to compute $\deg \mathbb{W}_n$.

Since $\dim \mathbb{W}_n = 1$, to estimate its degree, we need to intersect with one (generic) linear form in $(n-1)n+1$ variables. The amount of points of this (generic) intersection will be the degree of the variety. This

intersection is represented by the roots of a generic univariate polynomial of degree $n+1$ obtained by replacing the variables of the linear form by the parametrization of $\mathbb{W}_n$ and so $\deg \mathbb{W}_n = n+1$. Thus, we deduce that the degree of the variety $\mathbb{V}_n$ defined by the ideal $(F^{[n-1]})$ is $n+1$. ■

The result above and Remark 50 imply that any linear primitive element γ has a minimal polynomial $M \in k[T^{[n]}]$ with $\deg(M) \leq \deg(\mathbb{V}_n) = n+1$.

Our next step will be to show a primitive element:

Claim: Let $n \geq 2$ then the element $\gamma := X_2 + tX_3 + \cdots + t^{n-2}X_n$ is a primitive element of the differential field extension $\mathbb{Q}(t) \hookrightarrow \mathcal{F} = \mathrm{Frac}(k\{X\}/[F])$.

Proof: In this proof we will use the following notation: given a vector $v = (v_1, \ldots, v_m)$ of m coordinates and a polynomial $H := a_1 + a_2 t + \cdots + a_m t^{m-1}$, we will write

$$\langle H, v\rangle := a_1 v_1 + a_2 v_2 t + \cdots + a_m v_m t^{m-1}.$$

With this notation we have that, if $Q := 1 + t + \cdots + t^{n-2}$, $\gamma = \langle Q, (X_2, X_3, \ldots, X_n)\rangle$.

For each $l \in \mathbb{N}$, modulo the differential ideal Δ, the following relation holds:

$$\gamma^{(l)} = \left\langle Q^{(l)}, (X_{l+2}, \ldots, X_n)\right\rangle + \sum_{j=0}^{l-1} \frac{l!}{j!} Q^{(j)} X_1^{l+1-j} \tag{4.4}$$

and, in particular, since $Q^{(n-1)} = Q^{(n)} = 0$,

$$\gamma^{(n-1)} = \sum_{j=0}^{n-2} \frac{(n-1)!}{j!} Q^{(j)} X_1^{n-j} \quad \text{and} \quad \gamma^{(n)} = \sum_{j=0}^{n-1} \frac{n!}{j!} Q^{(j)} X_1^{n+1-j}$$

from where we deduce that $nX_1\gamma^{(n-1)} = \gamma^{(n)}$ and then $X_1 = \dfrac{\gamma^{(n)}}{n\gamma^{(n-1)}}$ in $\mathcal{F}$.

Replacing X_1 in (4.4) for $l = n-2$, we have that

$$\gamma^{(n-2)} = (n-2)!X_n + \sum_{j=0}^{n-3} \frac{(n-2)!}{j!} Q^{(j)} \left(\frac{\gamma^{(n)}}{n\gamma^{(n-1)}}\right)^{n-1-j}.$$

Then, X_n can be written in $\mathcal{F}$ as a quotient of polynomials involving only γ and its derivatives, more precisely

$$X_n = \frac{1}{(n-2)!}\left(\gamma^{(n-2)} - \sum_{j=0}^{n-3} \frac{(n-2)!}{j!} Q^{(j)} \left(\frac{\gamma^{(n)}}{n\gamma^{(n-1)}}\right)^{n-1-j}\right).$$

Applying successively the identities in (4.4) for $l = n-3, \ldots, 1$, all the variables can be written as quotient of polynomials in $\gamma, \ldots, \gamma^{(n)}$. This shows that γ is a primitive element of the field extension $\mathbb{Q}(t) \hookrightarrow \mathcal{F} = \mathrm{Frac}(k\{X\}/[F])$. ■

From this last proof, we have that if $Q := 1 + t + \cdots + t^{n-2}$, then

$$\gamma^{(n-1)} = \sum_{j=0}^{n-2} \frac{(n-1)!}{j!} Q^{(j)} X_1^{n-j} \quad \text{and} \quad X_1 = \frac{\gamma^{(n)}}{n\gamma^{(n-1)}}.$$

Replacing X_1 in the first formula, we obtain a polynomial

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

such that $M(\gamma^{[n]}) \in \Delta$.

In order to show that M is a minimal polynomial of γ, we need to prove that:

Claim: $M \in k[t][T^{[n]}]$ is an irreducible polynomial.

Proof: Let us suppose that this is not the case, then M can be factored as the product of two polynomials in the ring $k[t, T^{(n-1)}][T^{(n)}]$ of positive degree in the variable $T^{(n)}$.

The same should happen if we evaluate $t = 0$, and so, the polynomial

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

could be written as the product of two polynomials in $k[T^{(n-1)}, T^{(n)}]$.

But $\sum_{j=0}^{n-2} (n-1)! \left(nT^{(n-1)}\right)^j (T^{(n)})^{n-j}$ and $-n^n \left(T^{(n-1)}\right)^{n+1}$ are homogeneous polynomials, with consecutive degrees and no common factors, then their sum is irreducible ([21, Exercise 2-34]). ■

Finally, let us observe that, since $\operatorname{ord}(M) = n = \operatorname{ord}_k([F])$ and $\deg(M) = n + 1 = \deg(\mathbb{V}_n)$, the bounds obtained in this section for the degree and the order of the minimal polynomial are optimal.

4.1.3 The minimal polynomial of a generic primitive element

The algorithm we will present in Section 4.2 for the computation of a resolvent representation follows closely Seidenberg's proof of Theorem 41 relying on a construction based on the minimal polynomial of a generic primitive element (that is, a linear combination with parameters as scalars). 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 $\Delta_\Lambda := [F, G] \subset k_\Lambda\{Y, X, U\}$ 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 $k\langle Y\rangle \hookrightarrow \mathcal{F}$ is also 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, if we denote by $\tilde{\Delta}_\Lambda$ the differential ideal generated by F, G in $K_\Lambda\{V\}$, the differential field $\mathcal{F}_\Lambda$ is also the fraction field of $K_\Lambda\{V\}/\tilde{\Delta}_\Lambda$ and the class in $\mathcal{F}_\Lambda$ of $\Gamma := \Lambda_1 V_1 + \cdots + \Lambda_{n+r} V_{n+r} \in k_\Lambda[V]$ is a primitive element of $K_\Lambda \hookrightarrow \mathcal{F}_\Lambda$ (see the proof of Theorem 41).

Due to Proposition 43, since $s = \mathrm{ord}_{K_\Lambda}(\tilde{\Delta}_\Lambda) = \mathrm{ord}_K(\tilde{\Delta})$, the set $\{\Gamma, \ldots, \Gamma^{(s-1)}\}$ is a transcendence basis of $K_\Lambda \hookrightarrow \mathcal{F}_\Lambda$ and $\mathcal{F}_\Lambda = \mathrm{Frac}(K_\Lambda[V^{[n+r]}]/(K_\Lambda \otimes \Delta_\Lambda) \cap (K_\Lambda[V^{[n+r]}]))$. Thus, Lemma 45 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

$$M_\Lambda(\Gamma, \ldots, \Gamma^{(s)}) \in (F^{[2n+2r-1]}, G^{[2n+2r-1]})_\Lambda \subset k_\Lambda[Y^{[2n+2r-1]}, X^{[2n+2r]}, U^{[2n+2r]}].$$

Finally, Theorem 49 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 $(F^{[2n+2r-1]}, G^{[2n+2r-1]})_\Lambda$ 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 45, the following result concerning the order in the variables Λ of a minimal polynomial M_Λ of Γ can be proved:

Proposition 52. *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 49 in the variables $Y^{[2n+2r-1]}$, $W^{[2n+2r]}$, $T^{[s]}$, such that*

$$M_\Lambda \in k[\Lambda^{[s]}, Y^{[2n+2r-1]}, W^{[2n+2r]}][T^{[s]}] \text{ is irreducible, and}$$

$$M_\Lambda(\Gamma, \ldots, \Gamma^{(s)}) \in (F^{[2n+2r-1]}, G^{[2n+2r-1]}) \subset k[\Lambda^{[s]}, Y^{[2n+2r-1]}, X^{[2n+2r]}, U^{[2n+2r]}]. \blacksquare$$

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

Let N_1 and N_2 be as before (Notation 47), $\mathbb{A}^{N_1}(\overline{k(\Lambda^{[s]})})$ be the N_1-dimensional affine space over any algebraic closure of the extended field $k(\Lambda^{[s]})$ and $\mathbb{V}_\Lambda \subset \mathbb{A}^{N_1}(\overline{k(\Lambda^{[s]})})$ be the irreducible variety defined by the polynomials $F^{[2n+2r-1]}, G^{[2n+2r-1]}$. Consider the linear map

$$\begin{array}{rccc} \pi: & \mathbb{V}_\Lambda & \longrightarrow & \mathbb{A}^{N_2}(\overline{k(\Lambda^{[s]})}) \\ & (y, w, v) & \mapsto & (y, w, \Gamma(v), \ldots, \Gamma^{(s)}(v)). \end{array}$$

From Proposition 52, we obtain the following analogue of Proposition 48:

Proposition 53. *The Zariski closure of $\pi(\mathbb{V}_\Lambda)$, $\overline{\pi(\mathbb{V}_\Lambda)} \subset \mathbb{A}^{N_2}(\overline{k(\Lambda^{[s]})})$, 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 $K_\Lambda \hookrightarrow \mathcal{F}_\Lambda$.* $\blacksquare$

Now we are able to show an upper bound for the *total* degree of a minimal polynomial of the generic primitive element Γ.

Theorem 54. *Let $M_\Lambda \in k[\Lambda^{[s]}, Y^{[2n+2r-1]}, W^{[2n+2r]}, T^{[s]}]$ be as in Proposition 52 and let $\mathbb{V} \subset \mathbb{A}^{N_1}$ be the algebraic variety from Notation 47.*

Then, the total degree of M_Λ is bounded by $(n + 1 + m(2n + 2r + 1))\deg(\mathbb{V})$.

Proof. First, note that $\{Y^{[2n+2r-1]}, W^{[2n+2r]}, \Gamma^{[s-1]}\}$ is an algebraically independent set in the field extension $k_\Lambda \hookrightarrow \mathrm{Frac}(k_\Lambda[Y^{[2n+2r-1]}, X^{[2n+2r]}, U^{[2n+2r]}]/(F^{[2n+2r-1]}, G^{[2n+2r-1]})_\Lambda)$ whose transcendence degree is $n + m(2n + 2r + 1)$ (see Remark 4). Then, there is a set $E \subset \{V^{[2n+2r]}\}$ of $n + r - s$ many 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 $\eta := (y, w, v)$ for the elements of $\mathbb{A}^{N_1}$ (keeping the notation introduced in (4.2)), and $\lambda := (\lambda_1, \dots, \lambda_{n+r}, \dots, \lambda_1^{(s)}, \dots, \lambda_{n+r}^{(s)})$ for the elements of the affine space $\mathbb{A}^{(n+r)(s+1)}$.

Let $N_0 := n + 1 + m(2n + 2r + 1)$ and consider the (non-linear) map

$$\pi_1 : \mathbb{A}^{(n+r)(s+1)} \times \mathbb{A}^{N_1} \to \mathbb{A}^{(n+r)(s+1)} \times \mathbb{A}^{N_0}$$

$$\pi_1(\lambda, \eta) = (\lambda, y, w, \Gamma(\lambda, v), \dots, \Gamma^{(s)}(\lambda, v), e)$$

and the irreducible variety

$$\mathbb{V}_1 := \mathbb{A}^{(n+r)(s+1)} \times \mathbb{V} \subset \mathbb{A}^{(n+r)(s+1)} \times \mathbb{A}^{N_1}.$$

Since $\{\Lambda^{[s]}, Y^{[2n+2r-1]}, W^{[2n+2r]}, \Gamma^{[s-1]}, E\}$ is a transcendence basis of the extension $k \hookrightarrow k(\mathbb{V}_1)$, $\overline{\pi_1(\mathbb{V}_1)}$ 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 an irreducible minimal polynomial M_Λ in the ring $k[\Lambda^{[s]}, Y^{[2n+2r-1]}, W^{[2n+2r]}, T^{[s]}]$ as in Proposition 52 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) and therefore, $\deg(M_\Lambda) = \deg(\pi_1(\mathbb{V}_1))$.

In order to estimate the degree of $\pi_1(\mathbb{V}_1)$, we will give an alternative description of this variety.

For $i = 1, \dots, N_0 = \dim(\mathbb{V}) + 1$, let C_i be a set of $N_1 + 1$ new variables indexed by $Y^{[2n+2r-1]}$, $W^{[2n+2r]}$, $V^{[2n+2r]}$ 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) and consider the map

$$\phi : \mathbb{A}^{(N_1+1)N_0} \times \mathbb{V} \to \mathbb{A}^{(N_1+1)N_0} \times \mathbb{A}^{N_0}$$

$$\phi(c, \eta) = (c, L_1(c_1, \eta), \dots, L_{N_0}(c_{N_0}, \eta)),$$

where $c := (c_1, \dots, c_{N_0})$.

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 $i = 1, \dots, N_0$ (see [40, 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 between $\phi(\mathbb{A}^{(N_1+1)N_0} \times \mathbb{V})$ and a linear variety.

First, we define a linear variety $\mathcal{L} \subset \mathbb{A}^{(N_1+1)N_0}$ 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 $\mathcal{L}$ 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 (4.3).

Setting $i_0 := r(2n+2r) + (m-r)(2n+2r+1)$ and $i_1 := i_0 + s + 1$ and identifying $\Lambda^{(l)}$ with $C_{i_0+1+l,\{X,\tilde{U}\}}$ for $l = 0, \ldots, s$, the variety $\mathcal{L}$ can be defined by means of the following equations (where $\epsilon_1, \ldots, \epsilon_{N_1+1}$ denote the vectors of the canonical basis of k^{N_1+1}):

- for $i = 1, \ldots, i_0$: $C_i = \epsilon_i$.
- for $i = i_0 + 1, \ldots, i_1$:

$$\begin{cases} C_{i,Y^{[2n+2r-1]}} = C_{i,W^{[2n+2r]}} = 0 & \\ C_{i,\{V\}^{(j)}} = 0 & \text{for } j \geq i - i_0 \\ C_{i,\{V\}^{(j)}} = \binom{i-i_0-1}{j} C_{i-j,\{V\}^{(0)}} & \text{for } j < i - i_0 \text{ (see Identity (4.3))} \end{cases}$$

- for $i = i_1 + 1, \ldots, N_0$: $C_i := \epsilon_{j_{i-i_1}}$, 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

$$\pi_\Lambda(c, b) = (c_{i_0+1,\{X,\tilde{U}\}}, \ldots, c_{i_1,\{X,\tilde{U}\}}, b).$$

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

Taking into account that the degree of a variety does not increase when intersecting it with an affine linear space [29, Remark 2] or under a linear projection [29, Lemma 2], we conclude that

$$\deg(M_\Lambda) = \deg(\pi_1(\mathbb{V}_1)) \leq \deg(\phi(\mathbb{A}^{(N_1+1)N_0} \times \mathbb{V}) \cap (\mathcal{L} \times \mathbb{A}^{N_0})) \leq$$

$$\leq \deg(\phi(\mathbb{A}^{(N_1+1)N_0} \times \mathbb{V})) = (n + 1 + m(2n + 2r + 1)) \deg(\mathbb{V}).$$

■

4.1.4 The resolvent representation

We will now deduce some results concerning the choice of a primitive element of the extension $K \hookrightarrow \mathcal{F}$ (see Section 4.1.1) and the order and degrees of the polynomials involved in a resolvent representation of the prime differential ideal $[F, G]$.

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 $\Gamma = \Lambda_1 V_1 + \cdots + \Lambda_{n+r} V_{n+r}$ of $K_\Lambda \hookrightarrow \mathcal{F}_\Lambda$ as in Proposition 52 and Theorem 54.

The polynomial $\mathcal{X}$ appearing in the proof of Theorem 41 can be taken as $\mathcal{X} = M_\Lambda$ and since $Q_\Lambda := \frac{\partial M_\Lambda}{\partial T^{(s)}}(\Gamma, \ldots, \Gamma^{(s)})$ is a polynomial in $k[\Lambda^{[s]}, Y^{[2n+2r-1]}, X^{[2n+2r]}, U^{[2n+2r]}]$ whose class is a non-zero element

in $\mathcal{F}_\Lambda$, the proof of this theorem provides a resolvent representation of the ideal $\tilde{\Delta}$ 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 (4.1) in the proof).
In particular, all the polynomials involved in this resolvent representation are elements of the polynomial ring $k[\Lambda^{[s]}, Y^{[2n+2r-1]}, W^{[2n+2r]}, T^{[s]}]$ and have degrees bounded by that of M_Λ.
In addition, that same proof shows that it is enough for an element $\gamma = \lambda_1 V_1 + \cdots + \lambda_{n+r} V_{n+r}$ to be a primitive element of $K \hookrightarrow \mathcal{F}$ the non-vanishing in $\mathcal{F}$ of the class 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 [52, Ch. 2, §22] imply:

Corollary 55. *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 $\gamma = \lambda_1 V_1 + \cdots + \lambda_{n+r} V_{n+r}$ where $\lambda_i \in \mathbb{Q}[\xi]$ is a polynomial of degree bounded by $s = ord_K(\tilde{\Delta})$ 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 48 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 $[F, G]$ with respect to the transcendence basis Y, W and the primitive element γ. We conclude:

Theorem 56. *There is a resolvent representation*

$$\{M,\ q\,X_1 - p_1, \ldots, q\,X_n - p_n, q\,\tilde{U}_1 - p_{n+1}, \ldots, q\,\tilde{U}_r - p_{n+r}\}$$

of the prime differential ideal Δ with respect to the transcendence basis Y, W and a primitive element $\gamma = \lambda_1 V_1 + \cdots + \lambda_{n+r} V_{n+r}$ of the differential field extension $k\langle Y, W\rangle \hookrightarrow \mathcal{F}$ with M, q, p_i (for $i = 1, \ldots, n+r$) in the polynomial ring $k[Y^{[2n+2r-1]}, W^{[2n+2r]}, T^{[s]}]$ and with their total degrees bounded by $\deg(\mathbb{V})$. ■

4.2 Algorithmic computation of a resolvent representation

The main goal of this section is the computation of a resolvent representation of the differential ideal $[F, G]$ associated to system (2.1).
As in Section 3.4, 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 (2.1) 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 sections 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 [30] and [55]) to the computation of this polynomial.

4.2.1 Computing the generic minimal polynomial

As in Section 4.1.1, fix a "good" differential transcendence basis $W \subset \{X, U\}$ of the field extension $\mathbb{Q}(t)\langle Y\rangle \hookrightarrow \mathcal{F}$, and consider the differentially algebraic extension $\mathbb{Q}(t)\langle Y, W\rangle \hookrightarrow \mathcal{F}$. This transcendence basis W can be obtained by applying the algorithm underlying Theorem 39. Denote $V := \{X, U\} \setminus W$ 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 section focuses on the computation of the minimal polynomial M_Λ of the generic primitive element $\Gamma := \Lambda_1 V_1 + \cdots + \Lambda_{n+r} V_{n+r}$ in $K_\Lambda \hookrightarrow \mathcal{F}_\Lambda$ satisfying the degree upper bound stated in Theorem 54.
Let $E \subset \{V^{[2n+2r]}\}$ 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 extension

$$k_\Lambda \hookrightarrow \mathrm{Frac}(k_\Lambda[Y^{[2n+2r-1]}, X^{[2n+2r]}, U^{[2n+2r]}]/(F^{[2n+2r-1]}, G^{[2n+2r-1]})_\Lambda).$$

As in Notation 47, let $N_1 = r(2n+2r)+(n+m)(2n+2r+1)$. Consider the variety $\mathcal{V} \subset \mathbb{A}^{(n+r)(s+1)} \times \mathbb{A}^{N_1} \times \mathbb{A}^s$ defined as

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

which is irreducible of dimension $\mu := (n + r)(s + 1) + m(2n + 2r + 1) + n$.
We have then the ring inclusion

$$\mathbb{Q}[\Lambda^{[s]}, Y^{[2n+2r-1]}, W^{[2n+2r]}, E, T^{[s-1]}] \hookrightarrow \mathbb{Q}[\mathcal{V}]$$

and the cardinality of the family $\Lambda^{[s]}$, $Y^{[2n+2r-1]}$, $W^{[2n+2r]}$, E, $T^{[s-1]}$ is μ. Thus, the linear projection

$$\pi : \mathcal{V} \to \mathbb{A}^\mu$$

$$\pi(\lambda, y, w, v, \tau) = (\lambda, y, w, e, \tau)$$

is a dominant map with generically finite fibers.
Let $\varphi : \mathcal{V} \to \mathbb{A}^\mu \times \mathbb{A}^1$ be defined by $\varphi(\lambda, y, w, v, \tau) = (\pi(\lambda, y, w, v, \tau), \Gamma^{(s)}(\lambda, v))$. 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 $V^{[2n+2r]}$ 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 0-dimensional variety $\mathcal{V}_{\mathcal{K}}$ over the algebraic closure $\overline{\mathcal{K}}$ of $\mathcal{K} := \mathbb{Q}(P)$. Note 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

$$\mathcal{I}_{\mathcal{K}} := (F^{[2n+2r-1]}, G^{[2n+2r-1]}, \Gamma - T, \ldots, \Gamma^{(s-1)} - T^{(s-1)}) \subset \mathcal{K}[Z]$$

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 57. *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 the homotecy $m_{\Gamma^{(s)}}(f) = \Gamma^{(s)} f$ and let $M_0 \in \mathcal{K}[T^{(s)}]$ be its minimal polynomial. Then, there exists $Q_0 \in \mathbb{Q}[P] - \{0\}$ with minimal degree such that $M_\Lambda = Q_0 M_0$.*

Proof. First, note that $M_\Lambda(\Gamma^{(s)}) \in \mathcal{I}$ so $M_\Lambda(\Gamma^{(s)}) \in \mathcal{I}_{\mathcal{K}}$ and 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 a polynomial $Q \in \mathbb{Q}[P] - \{0\}$ of minimal degree with $QM_0(\Gamma^{(s)}) \in \mathcal{I}$. 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 QM_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 0-dimensional prime ideal of $\mathcal{K}[Z]$, its extension $\mathcal{I}_{\overline{\mathcal{K}}}$ to $\overline{\mathcal{K}}[Z]$ is a 0-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 $\mathcal{R}_1, \ldots, \mathcal{R}_D \in \overline{\mathcal{K}}^{2(n+r)^2+s}$ are 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 [30] (which hold for a *finite* morphism) to the case of a (generically finite) *dominant* map, which is achieved by using the techniques described in [55].

Proposition 58. *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 $O(\log(1/\varepsilon)(n+r)^{20}(n+m)^6 d^2 \deg(\mathbb{V})^{14} L)$, where $\mathbb{V}$ is the algebraic variety introduced in Notation 47.*

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 0-dimensional and unramified. In order to compute the geometric resolution of $\pi^{-1}(p)$, we apply the procedure for the resolution of 0-dimensional systems described in [31] (see also [28] and [26]), which takes a reduced regular sequence as input. 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 [55, 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 34). 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 [31, 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 $1 \leq i \leq 2n+2r$, $1 \leq s \leq n$, $1 \leq l \leq r$, introduced in Remark 4. 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, $\delta \leq \deg(\mathbb{V})$, 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 0-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, [30, 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 [30, 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 [30, 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 [26, Lemma 30] and then we proceed as in [30, 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, [2, Section 8.3]). By [2, 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 [55, 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 [25, Section 5.9 and Corollary 6.49]). Note that the upper bound on the degree of the polynomial M_Λ proved in Theorem 54 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 $\kappa \geq \lceil \log(2(n+1+m(2n+2r+1))\deg(\mathbb{V}))\rceil + 1$. 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 complexity bound for the whole procedure follows by adding up the complexities of steps (1) to (4) and taking into account that $D \leq \deg(\mathbb{V})$. ■

4.2.2 Computation of a primitive element

In what follows we show how to compute a primitive element of the differential field extension induced by system (2.1) 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 4.1.4. 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

$$\Gamma = \Lambda_1 V_1 + \cdots + \Lambda_{n+r} V_{n+r}$$

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 4.1.4, in order for a linear form

$$\gamma = \lambda_1 V_1 + \cdots + \lambda_{n+r} V_{n+r}$$

to be a primitive element, it suffices that $Q_\Lambda(\lambda_1, \ldots, \lambda_{n+r}) \neq 0$ in $\mathcal{F}$. Furthermore, for every $1 \leq i \leq n+r$, λ_i can be chosen to be a polynomial in $\mathbb{Q}[t]$ of degree bounded by s (see [52, Ch. II, §22]).

For $i = 1, \ldots, n+r$, let A_{ij} $(0 \leq j \leq s)$ 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 $A := \{A_{ij} : 1 \leq i \leq n+r,\ 0 \leq j \leq s\}$. If we substitute the variables Λ_i $(1 \leq i \leq n+r)$ 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 $\mathcal{F} \simeq \mathbb{Q}(t)(X), \langle U \rangle$: we substitute $X_h^{(l)} = \tilde{f}_h^{(l-1)}$ $(1 \leq h \leq n,\ 1 \leq l)$ and $Y_j^{(k)} = \tilde{g}_j^{(k)}$ $(1 \leq j \leq r,\ 0 \leq k)$ in the polynomial Q_Λ to obtain a new polynomial $\widetilde{Q}_\Lambda \in \mathbb{Q}[\Lambda^{[s]}, X, U^{[2n+2r]}]$ (see Notation 3), 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.

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

Proposition 59. *Assume that a "good" differential transcendence basis W of the differential field extension induced by system (2.1) 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 58, we deduce:

Corollary 60. *Let the assumptions and notations be as in Proposition 58. Then, there is a probabilistic algorithm which computes a primitive element of the differential field extension $\mathbb{Q}(t)\langle Y, W\rangle \hookrightarrow \mathcal{F}$ induced*

by system (2.1) (for a given differential transcendence basis W) with error probability bounded by ε, $0 < \varepsilon < 1$, within complexity $O(\log(1/\varepsilon)(n+r)^{20}(n+m)^6 d^2 \deg(\mathbb{V})^{14} L)$. ■

4.2.3 Computing a resolvent representation of the system

As it was shown in Proposition 59, there is an algorithm for the computation of a primitive element γ of the differential field extension $\mathbb{Q}(t)\langle Y, W\rangle \hookrightarrow \mathcal{F}$. 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_λ, 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 4.1.4 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 $q(\gamma)V_i - p_i(\gamma) \in [F, G]$ for $i = 1, \ldots, n+r$.
Therefore, in order to obtain a resolvent representation of the ideal $[F, G]$ 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 done using the algorithm described in the previous sections for the computation of the minimal polynomial of a generic primitive element within the same complexity.
Combining this procedure with Theorem 39 and Corollary 60, we deduce our main result:

Theorem 61. *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 $[F, G]$ be the differential ideal associated to system (2.1) and let $\mathbb{V}$ be the algebraic variety defined by $(F^{[2n+2r]}, G^{[2n+2r]})$ introduced in Notation 47. Then, there is a probabilistic algorithm which computes:*

- *a "good" differential transcendence basis W of $\mathbb{Q}(t)\langle Y\rangle \hookrightarrow Frac(\mathbb{Q}(t)\{Y, X, U\}/[F, G])$,*
- *a primitive element γ of $\mathbb{Q}(t)\langle Y, W\rangle \hookrightarrow Frac(\mathbb{Q}(t)\{Y, X, U\}/[F, G])$,*
- *a resolvent representation of the differential ideal $[F, G]$ 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

$$O(\log(1/\varepsilon)(n+r)^{20}(n+m)^6 d^2 \deg(\mathbb{V})^{14} L).$$

In particular, the complexity of the algorithm can be bounded by

$$((n+r)(n+m)d^{(n+r)^2})^{O(1)} \log(1/\varepsilon) L.$$ ■

Remark 62. *We point out that our complexity upper bound in terms of geometric invariants is more accurate than the one that can be stated using only syntactic parameters, as illustrated by the system*

considered in Example 51. 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.*

4.3 Differential systems of higher order

Up to this point, we have only considered first-order differential systems like (2.1), however, the order of derivation appearing in the equations of the system is not a real obstacle in our work. In this section we will show how to handle higher-order differential systems in order to obtain a resolvent representation for them.

As it is usual in the well-known classical theory of ordinary differential equations, the method employed to treat systems of order $e > 1$ is to transform them into first-order systems by introducing the derivative, the second derivative and so on up to the $e - 1$ derivative of the variables as a part of a new enlarged set of variables and then study the first-order systems associated.

To simplify the notations, we will only consider a version of the "generic" part of the system (2.1) but the same arguments can be applied to the whole system. Let K be a differential field with $\mathrm{char}(K) = 0$ containing a non-constant element ξ (i.e. $\dot{\xi} \neq 0$), $Z := \{Z_1, \ldots, Z_m\}$ be a set of differential indeterminates over K and consider the system

$$\begin{cases} g_1(Z, \dot{Z}, \ldots, Z^{(e)}) &= Y_1 \\ g_2(Z, \dot{Z}, \ldots, Z^{(e)}) &= Y_2 \\ & \vdots \\ g_r(Z, \dot{Z}, \ldots, Z^{(e)}) &= Y_r \end{cases} \tag{4.5}$$

where polynomials $g_1, \ldots, g_r \in k[Z^{[e]}]$ are differentially algebraically independent as elements of the ring $k\{Y, Z\}$ over the field k.

This system can be seen as a first-order system adding $m(e + 1)$ new variables

$$X := \{X_{ij},\ 1 \leq i \leq e - 1,\ 1 \leq j \leq m\} \text{ and } U := \{U_1, \ldots, U_m, \dot{U}_1, \ldots, \dot{U}_m\}$$

and considering the following change of variables, for each $j = 1, \ldots, m$:

$$\begin{cases} X_{1,j} &= Z_j \\ X_{2,j} &= \dot{Z}_j \\ & \vdots \\ X_{e-1,j} &= Z_j^{(e-2)} \\ U_j &= Z_j^{(e-1)} \\ \dot{U}_j &= Z_j^{(e)} \end{cases} \tag{4.6}$$

which transform the original system (4.5) into the following first-order system of differential equations:

$$\begin{cases} \dot{X}_{i,j} & = & X_{i+1,j} & \forall j = 1,\dots,m \quad \forall i = 1,\dots e-2 \\ \dot{X}_{e-1,j} & = & U_j & \forall j = 1,\dots,m \\ g_1(X,U,\dot{U}) & = & Y_1 & \\ g_2(X,U,\dot{U}) & = & Y_2 & \\ & \vdots & & \\ g_r(X,U,\dot{U}) & = & Y_r & \end{cases} \tag{4.7}$$

Unfortunately, not all the invariants we have computed in the previous chapters remain the same for both systems. For example, if we consider the system with only one equation

$$Y_1 = Z^{(3)},$$

the first-order system associated to it is:

$$\begin{cases} \dot{X}_1 & = & X_2 \\ \dot{X}_2 & = & U_1 \\ \dot{U}_1 & = & Y_1 \end{cases}$$

So, to this particular system we have associated different differential ideals in different differential polynomial rings. The first equation yields the ideals $[Y_1 - Z^{(3)}] \subset k\{Y_1, Z\}$ and

$$\Delta_1 = [Y_1 - Z^{(3)}] \subset k\langle Y_1\rangle\{Z\},$$

meanwhile the second system induces the ideals $[\dot{X}_1 - U_1, \dot{X}_2 - X_1, Y_1 - \dot{U}_1] \subset k\{Y_1, U_1, X_1\}$ and

$$\Delta_2 = [\dot{X}_1 - U_1, \dot{X}_2 - X_1, Y_1 - \dot{U}_1] \subset k\langle Y_1\rangle\{U_1, X_1\}.$$

Clearly, the Hilbert-Kolchin functions of this two ideals are not the same since

$$\mathcal{H}_{\Delta_1, k\langle Y_1\rangle}(1) = \mathrm{trdeg}_{k\langle Y_1\rangle}(\mathrm{Frac}(k\langle Y_1\rangle[Z,\dot{Z}]/\Delta_1 \cap k\langle Y_1\rangle[Z,\dot{Z}]) = \mathrm{trdeg}_{k\langle Y_1\rangle}(\mathrm{Frac}(k\langle Y_1\rangle[Z,\dot{Z}]) = 2$$

and

$$\mathcal{H}_{\Delta_2, k\langle Y_1\rangle}(1) = \mathrm{trdeg}_{k\langle Y_1\rangle}(\mathrm{Frac}(k\langle Y_1\rangle[U_1, X_1, X_2, \dot{U}_1, \dot{X}_1, \dot{X}_2]/\Delta_2 \cap k\langle Y_1\rangle[U_1, X_1, X_2, \dot{U}_1, \dot{X}_1, \dot{X}_2]) = 3.$$

However, going back to the general case, we can find a resolvent representation for the system (4.5) computing one for the system (4.7) with some restrictions.
Let us consider the differential ideals

$$\Delta_1 := [Y_1 - g_1(Z^{[e]}), \dots, Y_r - g_r(Z^{[e]})] \subset k\langle Y\rangle\{Z\}$$

and

$$\Delta_2 := [\dot{X}_{i,j} - X_{i+1,j}, \dot{X}_{e-1,j} - U_j, Y_k - g_k(X, U, \dot{U}); 1 \leq i \leq e-2, 1 \leq j \leq m, 1 \leq k \leq r] \subset k\langle Y\rangle\{X, U\}$$

associated to the systems (4.5) and (4.7) respectively.

As a first step, we need to show how the Hilbert-Kolchin polynomials and the orders of these two ideal are related and how to obtain a differential transcendence basis that can be transported from one differential extension to the other.

Since the conversion from one system to the other is made via a change of variables, it is clear that, for every $l \geq e$ there is a (non-differential) ring isomorphism

$$k\langle Y\rangle[Z^{[l]}]/\Delta_1 \cap k\langle Y\rangle[Z^{[l]}] \simeq k\langle Y\rangle[X^{[l-e+1]}, U^{[l-e+1]}]/\Delta_2 \cap k\langle Y\rangle[X^{[l-e+1]}, U^{[l-e+1]}].$$

These isomorphisms imply that, even though the Hilbert-Kolchin polynomial of the systems are not the same, they are closely related:

$$\mathcal{H}_{k\langle Y\rangle,\Delta_1}(l) = \mathcal{H}_{k\langle Y\rangle,\Delta_2}(l-e+1) \qquad \forall\, l \geq e-1.$$

From Proposition 11, we know that $\operatorname{dimdiff}_{k\langle Y\rangle}(\operatorname{Frac}(k\langle Y\rangle\{X, U\}/\Delta_2) = m - r$ and the same proof follows straightforwardly to show that $\operatorname{dimdiff}_{k\langle Y\rangle}(\operatorname{Frac}(k\langle Y\rangle\{Z\}/\Delta_1) = m - r$, then the orders of the ideals satisfy that $\operatorname{ord}_{k\langle Y\rangle,\Delta_1} = \operatorname{ord}_{k\langle Y\rangle,\Delta_2} - (m-r)(e-1)$.

The change of variables we have made to obtain a first-order differential system induces a non-differential isomorphism between the differential fields

$$\tau : \operatorname{Frac}(k\langle Y\rangle\{Z\}/\Delta_1) \longrightarrow \operatorname{Frac}(k\langle Y\rangle\{X, U\}/\Delta_2).$$

Although τ is not a differential isomorphism it does respect in some way the order of derivation of the polynomials, for every $l \geq e$:

$$p \in k\langle Y\rangle[Z^{[l]}]/\Delta_1 \cap k\langle Y\rangle[Z^{[l]}] \Leftrightarrow \tau(p) \in k\langle Y\rangle[X^{[l-e+1]}, U^{[l-e+1]}]/\Delta_2 \cap k\langle Y\rangle[X^{[l-e+1]}, U^{[l-e+1]}]$$

and for $l \leq e-1$:

$$p \in k\langle Y\rangle[Z^{[l]}]/\Delta_1 \cap k\langle Y\rangle[Z^{[l]}] \Leftrightarrow$$

$$\tau(p) \in k\langle Y\rangle[X_{1,j}, \ldots, X_{l+1,j}; 1 \leq j \leq m]/\Delta_2 \cap k\langle Y\rangle[X_{1,j}, \ldots, X_{l+1,j}; 1 \leq j \leq m].$$

In particular,

$$p \in k\langle Y\rangle[Z]/\Delta_1 \cap k\langle Y\rangle[Z^{[l]}] \Leftrightarrow \tau(p) \in k\langle Y\rangle[X_{1,1}, \ldots, X_{1,m}]/\Delta_2 \cap k\langle Y\rangle[X_{11}, \ldots, X_{1,m}].$$

Because of this relation, if we are able to obtain a differential transcendence basis for the field extension $k\langle Y\rangle \hookrightarrow \operatorname{Frac}(k\langle Y\rangle\{X, U\}/\Delta_2)$ from the set of variables $\{X_{1,1}, \ldots, X_{1,m}\}$ (which clearly contains one

since the other variables are dependent), we will also obtain a differential transcendence basis for the extension $k\langle Y\rangle \hookrightarrow \mathrm{Frac}(k\langle Y\rangle\{Z\}/\Delta_1)$ applying the isomorphism τ^{-1}. In the same way, once the differential transcendence basis W has been fixed and added to the ground field, if we construct a primitive element for the first extension involving only the variables of the set $\{X_{1,1},\ldots,X_{1,m}\}$ that are not part of the differential transcendence basis, applying τ^{-1}, we obtain a primitive element of the original extension $k\langle Y, W,\rangle \hookrightarrow \mathrm{Frac}(k\langle Y\rangle\{Z\}/\Delta_1)$.

For the first condition, Remark 40 assures that the transcendence basis obtained by applying the algorithm in Theorem 39 is extracted from the set of variables $\{X_{1,1},\ldots,X_{1,m}\}$. The second condition is satisfied since Theorem 41, which is valid for any prime differential ideal, can be applied to the field extension $k\langle Y\rangle \hookrightarrow \mathrm{Frac}(k\langle Y\rangle\{Z\}/\Delta_1)$. This ensures the existence of a primitive element of the field extension $k\langle Y\rangle \hookrightarrow \mathrm{Frac}(k\langle Y\rangle\{X,U\}/\Delta_2)$ involving only the remaining variables in the set $\{X_{1,1},\ldots,X_{1,m}\}$.

As we have already mentioned, the transformation from the system (4.5) to the system (4.7) described in (4.6) is a linear change of variables, and this allows us to reformulate the results obtained in Theorem 56 for the system (4.5) in the following proposition:

Proposition 63. *Let $g_1,\ldots,g_r \in \mathbb{Q}[t][X,U,\dot{U}]\mathbb{Q}[t,Z^{[e]}]$ be polynomials with degrees bounded by an integer d.*

Let W be a differential transcendence basis of the differential field extension $k\langle Y\rangle \hookrightarrow Frac(k\langle Y\rangle\{Z\}/\Delta_1)$. Let us rename the set of variables $V=\{V_1,\ldots,V_r\} := Z\setminus W$ and let $\gamma=\lambda_1V_1+\cdots+\lambda_rV_r$ be a primitive element of the 0-dimensional differential field extension $k\langle Y,W\rangle \hookrightarrow Frac(k\langle Y,W\rangle\{V\}/\Delta_1)$.

Let $s := ord_{k\langle Y\rangle,\Delta_1} \leq re$, $N := r(m(e+3)+r(e+1)-1)+m(m(e+3)+r(e+1)+e-1)$ and $\tilde{\mathbb{V}}\subset\mathbb{A}^N$ the irreducible variety defined by the $r(m(e+3)+r(e+1))$ polynomial equations

$$(Y_1-g_1(Z^{[e]}))^{[m(e+3)+r(e+1)-1]}=0,\ldots,(Y_r-g_r(Z^{[e]}))^{[m(e+3)+r(e+1)-1]}=0.$$

Then, there is a resolvent representation

$$\{M,\ q\,V_1-p_1,\ldots,q\,V_r-p_r\}$$

of the prime differential ideal Δ_1 with respect to the transcendence basis Y,W and a primitive element γ with $M,q,p_i \in k[Y^{[m(e+3)+r(e+1)-1]},W^{[m(e+3)+r(e+1)-1]},T^{[s]}]$ for $i=1,\ldots,r$ and their total degrees bounded by $\deg(\tilde{\mathbb{V}})\leq d^{(rm+r^2)(e+1)+2rm}$. ■

All the algorithms described to this last two sections apply in the case of the system (4.5) assuming that $g_1,\ldots,g_r\in\mathbb{Q}[t,Z^{[e]}]$ have degrees bounded by d and are encoded by a straight-line program of length L. This probabilistic algorithms will compute

- a differential transcendence basis W of the differential field extension

$$\mathbb{Q}(t)\langle Y\rangle \hookrightarrow \mathrm{Frac}(\mathbb{Q}(t)\{Y,Z\}/[Y_1-g_1(Z^{[e]}),\ldots,Y_r-g_r(Z^{[e]})]),$$

- a primitive element γ of $\mathbb{Q}(t)\langle Y, W\rangle \hookrightarrow \mathrm{Frac}(\mathbb{Q}(t)\{Y, Z\}/[Y_1 - g_1(Z^{[e]}), \ldots, Y_r - g_r(Z^{[e]})])$,
- a resolvent representation of the differential ideal $[Y_1 - g_1(Z^{[e]}), \ldots, Y_r - g_r(Z^{[e]})]$ with respect to the differential transcendence basis Y, W and the primitive element γ,

within the same order of complexity as for the computation of the resolvent representation of system (2.1). Actually, the precise expression of this complexity can be obtained replacing n by $m(e + 1)$ in the estimations of Theorem 61.

Appendix A

Resolvent representation for over-determined differential systems

In the previous chapters, we focused on the computation of a resolvent representation of the generic differential system (2.1) under Assumption 5 on the differential algebraic independence of the polynomials $g_1, \ldots, g_r$, which played a key role in our arguments. Now, we will drop that assumption and we will look for a (resolvent-like) representation of the system. More precisely, we will consider differential systems of the form:

$$\begin{cases} \dot{X}_1 &= f_1(X, U) \\ &\vdots \\ \dot{X}_n &= f_n(X, U) \\ Y_1 &= g_1(X, U, \dot{U}) \\ &\vdots \\ Y_\rho &= g_\rho(X, U, \dot{U}) \end{cases} \tag{A.1}$$

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 sets of variables $X := \{X_1, \ldots, X_n\}$, $U := \{U_1, \ldots, U_m\}$ and $\dot{U} := \{\dot{U}_1, \ldots, \dot{U}_m\}$.

Our aim is to compute an alternative resolvent representation of system (A.1). In order to do this, we will modify the system so that the condition in Assumption 5 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.

As a first step for the construction of this representation, we will need to decide which of the polynomials $g_1, \ldots, g_\rho$ are differentially algebraically independent as elements of the differential quotient ring $k\{Y, X, U\}/[f_1 - \dot{X}_1, \ldots, f_n - \dot{X}_n]$ over the field k, in other words, which of them satisfy Assumption 5 in Section 2.1. This is done in Proposition 65 below but for its proof we need to introduce first some well-known concepts from differential algebra such us rankings and characteristic sets. Since many of

the other proofs in this appendix are similar to those of the results we have presented so far, we will not show all the details, but we will outline the main ideas involved.

A.1 Rankings and characteristic sets

In this section we introduce briefly the classical notions of rankings and characteristic set. A more detailed description can be found in [38], [52] and [34]. Even though these concepts constitute some of the basic tools of differential algebra, we have tried to avoid them in this work due to the unsatisfactory complexity bounds that their manipulation carries with it. However, we need them now for the proof of one of the main results we are about to show (see Proposition 65 below).

Let $\mathcal{E}$ be a differential field and let Z be a set of differential indeterminates over $\mathcal{E}$. A *ranking* on $\mathcal{E}\{Z\}$ is a total order $\succ$ on the set $\Theta Z := \{Z^{(l)} : l \in \mathbb{N}_0\}$ satisfying

$$\dot{u} \succ u \quad \text{for every} \quad u \in \Theta Z \qquad \text{and}$$

$$\dot{u} \succ \dot{v} \quad \text{if} \quad u \succ v \quad \text{for} \quad u, v \in \Theta Z.$$

A ranking $\succ$ on $\mathcal{E}\{Z\}$ such that $Z_i^{(r)} \succ Z_j^{(s)}$ if $i > j$ is called an *elimination ranking*.

Assume that a ranking on $\mathcal{E}\{Z\}$ has been fixed. Let $p \in \mathcal{E}\{Z\} \setminus \mathcal{E}$. The *leader* of p, denoted by $\ell(p)$, is the greatest element of ΘZ 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 of the variable Z_j, then Z_j is called the *leading variable of* p, and it is denoted by $vp(p)$.

A polynomial $q \in \mathcal{E}\{Z\}$ is *reduced with respect to* p if no proper derivative of $\ell(p)$ appears in q and $\deg_{\ell(p)}(q) < \deg_{\ell(p)}(p)$.

A subset $A \subset \mathcal{E}\{Z\} \setminus \mathcal{E}$ is an *autoreduced* set if every element $p \in A$ is reduced with respect to all the elements of $A \setminus \{p\}$.

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

A.2 Independent equations

Keeping our notation from the previous chapters (see Chapter 2), 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 $\Omega_l := (F^{[l-1]}, G_1^{[l-1]}, \ldots, G_\rho^{[l-1]}) \subset k[Y^{[l-1]}, X^{[l]}, U^{[l]}]$.

The following analogues of Remark 4 and Proposition 11 hold in this context:

Remark 64. *For every $l \in \mathbb{N}$, the ideal $\Omega_l \subset k[Y^{[l-1]}, X^{[l]}, U^{[l]}] \subset k[Y^{[l]}, X^{[l]}, U^{[l]}]$ is prime and*

$$k[Y^{[l]}, X^{[l]}, U^{[l]}]/\Omega_l \simeq k[X, U^{[l]}].$$

The differential ideal $\Omega \subset k\{Y, X, U\}$ is prime and

$$k\{Y, X, U\}/\Omega \simeq k[X]\{U\}$$

with the derivation induced by $\dot{X}_j = f_j(X, U)$ and thus

$$diffdim(\Omega) = m.$$

Substituting the variables not involved in the corresponding polynomial rings by suitable polynomials or values in k, as it is done for instance in Proposition 7, it is clear that

$$\Omega \cap k[Y^{[l-1]}, X^{[l]}, U^{[l]}] = \Omega_l \qquad and \qquad \Omega \cap k[Y^{[l]}, X^{[l]}, U^{[l]}] = \Omega_{l+1} \cap k[Y^{[l]}, X^{[l]}, U^{[l]}].$$

Moreover, for all $l \geq 0$,

$$\mathcal{H}_{\Omega,k}(l) = trdeg_k(Frac(k[Y^{[l]}, X^{[l]}, U^{[l]}]/k[Y^{[l]}, X^{[l]}, U^{[l]}] \cap \Omega)) = m(l+1) + o$$

where $o = ord_k(\Omega) \leq n + \rho$.

The fact that the ideal Ω might contain a non-zero polynomial involving only the variables $Y_1, \ldots, Y_\rho$ (since Assumption 5 is no longer valid) prevents us from considering these variables as being part of a differential transcendence basis of the differential field extension

$$k \hookrightarrow \mathcal{G} := \text{Frac}(k\{Y, X, U\}/\Omega).$$

We will show now how to obtain a maximal differentially independent subset of the set $\{Y_1, \ldots, Y_\rho\}$.
To do this, we need 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 65. *The set $\mathcal{Y} \subset \{Y_1, \ldots, Y_\rho\}$ is differentially algebraically independent in $k \hookrightarrow \mathcal{G}$ if and only $\mathcal{Y}^{[n+\rho]}$ is algebraically independent in $k[Y^{[n+\rho]}, X^{[n+\rho+1]}, U^{[n+\rho+1]}]/\Omega_{n+\rho+1}$ over k.*

Proof. Assume that $\{Y_{l_1}^{[n+\rho]}, \ldots, Y_{l_t}^{[n+\rho]}\} \subset k[Y^{[n+\rho]}, X^{[n+\rho+1]}, U^{[n+\rho+1]}]/\Omega_{n+\rho+1}$ is algebraically independent over k.
Fix an order on the set $Y \setminus \{Y_{l_1}, \ldots, Y_{l_t}\}$ and consider the ranking $\ll$ on $k\{Y, X, U\}$ given by:

- $Y_{l_1} \ll \ldots \ll Y_{l_t} \ll Y \setminus \{Y_{l_1}, \ldots, Y_{l_t}\} \ll X_1 \ll \ldots \ll X_n \ll U_1 \ll \ldots \ll U_m$
- if $Z_i, Z_j \in \{Y, X, U\}$ then $Z_i^{(r)} \ll Z_j^{(s)}$ if $Z_i \ll Z_j$, for all $r, s \in \mathbb{N}$.

By [53, Lemma 19 and Theorem 24], there exists a characteristic set C of the ideal Ω with respect to this ranking, such that $\operatorname{ord}(C) \leq \operatorname{ord}_k(\Omega) \leq n + \rho$ for every $C \in C$.

Now, if $Y_{l_1}, \ldots, Y_{l_t}$ are differentially algebraic in $k \hookrightarrow \mathcal{G}$, there exists $C \in C$ with

$$C \in \Omega \cap k[Y_{l_1}^{[n+\rho]}, \ldots, Y_{l_t}^{[n+\rho]}] \subset \Omega \cap k[Y^{[n+\rho]}, X^{[n+\rho+1]}, Y^{[n+\rho+1]}] = \Omega_{n+\rho+1},$$

contradicting the hypothesis of algebraic independence of $Y_{l_1}^{[n+\rho]}, \ldots, Y_{l_t}^{[n+\rho]}$. ■

Combining this proposition with Lemma 38, we deduce the following algorithmic criterion:

Proposition 66. *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 39) 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.

A.3 Extended resolvent representation

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

The differential equation system obtained by removing from system (A.1) the equations corresponding to $Y_{r+1}, \ldots, Y_\rho$ satisfies Assumption 5 and so, it can be characterized by means of a resolvent representation as shown in Chapter 4, Section 4.2.

Furthermore, for each $j = r + 1, \ldots, \rho$, there is a non-zero polynomial

$$M_j \in k\{\mathcal{Y}\}\{T\} \text{ with } M_j(Y_j) \in \Omega.$$

Due to Proposition 65, $\{\mathcal{Y}^{[n+\rho]}, Y_j^{[n+\rho]}\}$ is algebraically dependent in

$$k[Y^{[n+\rho]}, X^{[n+\rho+1]}, U^{[n+\rho+1]}]/\Omega_{n+\rho+1}$$

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 (A.1) of the following type:

Definition 67. *An* extended resolvent representation *of system (A.1) consists of:*

- *A maximal differentially algebraically independent subset* $\mathcal{Y} \subset \{Y_1, \ldots, Y_\rho\}$ *in the differential extension*
$$k \hookrightarrow Frac(k\{Y, X, U\}/[F_1, \ldots, F_n, G_1, \ldots, G_\rho]).$$
- *Assuming* $\mathcal{Y} = \{Y_1, \ldots, Y_r\}$*, a differential transcendence basis* W *of the extension*
$$k\langle\mathcal{Y}\rangle \hookrightarrow \mathcal{F} := Frac(k\{\mathcal{Y}, X, U\}/[F_1, \ldots, F_n, G_1, \ldots, G_r])$$
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* $Y_{r+1}, \ldots, Y_\rho$*.*

We have already shown how to obtain the elements of the first three items. Since the algorithm that computes the polynomials $M_{r+1}, \ldots, M_\rho$ of the fourth items follows very closely the methods applied to the computation of the minimal polynomial of the resolvent representation, we will sketch briefly this procedure.
Denote $G := \{G_1, \ldots, G_r\}$. For $j = r+1, \ldots, \rho$, let
$$\Omega^j := [F, G, G_j] \subset k\{\mathcal{Y}, Y_j, X, U\}$$
and, for every non-negative integer l, let
$$\Omega_l^j := (F^{[l-1]}, G^{[l-1]}, G_j^{[l-1]}) \subset k[\mathcal{Y}^{[l-1]}, X^{[l]}, U^{[l]}][Y_j^{[l-1]}].$$
Let now s_j be the minimum non negative integer h such that $\{\mathcal{Y}^{[n+\rho]}, Y_j^{[h]}\}$ is algebraically dependent in $k[Y^{[n+\rho]}, X^{[n+\rho+1]}, Y^{[n+\rho+1]}]/\Omega_{n+\rho+1}$.
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 lies in $\Omega_{n+\rho+1}^j$, 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 of equations $F = 0, G = 0, G_j = 0$ and its associated ideals Ω^j and Ω^j_l, $l \geq 0$. 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 $s_j \leq n + r$ and

$$M_j(\mathcal{Y}^{[n+r]}, Y_j^{[s_j]}) \in \Omega^j_{n+r+1}.$$

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, $r + 1 \leq j \leq \rho$, let $\mathbb{V}_j$ be the irreducible variety defined in $\mathbb{A}^{n_1}$ by the ideal Ω^j_{n+r+1} 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 68. *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 69. *For $j = r + 1, \ldots, \rho$, a minimal polynomial $M_j \in k[\mathcal{Y}^{[n+r]}, T^{[s_j]}]$ for Y_j satisfies:*

$$s_j \leq n + r, \quad M_j(\mathcal{Y}^{[n+r]}, Y_j^{[s_j]}) \in \Omega^j_{n+r+1} \quad \textit{and} \quad \deg(M_j) \leq \deg(\mathbb{V}_j).$$

■

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 Chapter 3, as the minimum non negative integer h such that $\{\mathcal{Y}^{[n+r]}, Y_j^{[h]}\}$ is algebraically independent in

$$k[\mathcal{Y}^{[n+r]}, X^{[n+r+1]}, U^{[n+r+1]}, Y_j^{[n+r]}]/\Omega^j_{n+r+1}$$

(using the Jacobian matrix of the generator system of Ω^j_{n+r+1}). 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 58.

Therefore, we obtain a probabilistic algorithm that computes an extended resolvent representation of system (A.1) within the same order of complexity as for the computation of a resolvent representation under Assumption 5; namely, 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.

Appendix B

Differential index and implicit equations

As we have already mentioned at the end of Chapter 2, in the literature, there are many different definitions of the differentiation index of a first-order differential algebraic system ([9], [44], [18] and others). Among all of them, we focus on the one that, roughly speaking, defines it as the minimum number of times that the given differential algebraic system must be differentiated in order to determine the derivatives of the unknowns as continuous functions of the unknowns themselves. This definition is clear when we consider the following simple examples (see also [7]):

Example 1: Given a differentiable function $F : \mathbb{R} \times \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$, consider the differential system of equations $F(t, X, \dot{X}) = 0$, where $F := (F_1, \ldots, F_n)$ and $X := (X_1, \ldots, X_n)$. Then the Implicit Function Theorem says that the differential index of the system is 0 if the matrix $\left(\dfrac{\partial F_i}{\partial X_j}\right)_{i,j}$ is regular.

Example 2: Let $f, g : \mathbb{R}^3 \to \mathbb{R}$ be two differentiable functions and consider the differential system of equations given by

$$\begin{cases} \dot{X}_1 &= f(t, X_1, X_2) \\ 0 &= g(t, X_1, X_2). \end{cases}$$

Then, if $\dfrac{\partial g}{\partial X_2} \neq 0$ the differential index of the system is 1 since from the second equation, by differentiation, we obtain the relation $0 = \dfrac{\partial g}{\partial t} + \dfrac{\partial g}{\partial X_1}\dot{X}_1 + \dfrac{\partial g}{\partial X_2}\dot{X}_2$.

We have already given a definition for the differentiation index of the system 2.1 by means of the the stationary properties of the rank of certain matrices (Definition 25). In this appendix we prove some additional results about this invariant and we show that, if we consider algebraic equations instead of continuous functions in the first case, both definitions coincide in this particular case. These results will also allow us to give an alternative representation, different from the resolvent representation, of this system. This new representation can be seen as the generalization of the Implicit Function Theorem.

We go back now to our original system (2.1)

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

keeping all the notations and assumptions introduced in Chapter 2 Section 2.1.

First let us recall that the differentiation index σ of the system (2.1) (see Definition 25) is the non-negative integer such that for any $i \in \mathbb{N}_0$, $\mu_{k,i} < \mu_{k+1,i}$ if $k < \sigma$ and $\mu_{k,i} = \mu_{\sigma,i}$ if $k \geq \sigma$ (see Definition 15).

When the field extension associated to the system 2.1 is of positive dimension, as in the case for the resolvent representation, the first step towards the construction of this alternative Implicit Function Theorem-like presentation of the system (2.1) is the obtention of a differential transcendence basis to be added to the ground field in order to change to a 0-dimensional situation. In Sections 3.3 and 3.4 we have defined a "good" differential transcendence basis and have shown an algorithm for its computation. These differential bases, that have the additional property of not changing the order of the ideal Δ after adding the variables to the ground field, have proved useful for the computation of the resolvent representation saving us the computation of this order a second time. In the case of the presentation that we are about to show, they play an even more helpful role that we will illustrate with a simple example in the following section.

B.1 "Good" differential transcendence basis: a simple example

Before stating any precise result, let us consider the following example of a 1-dimensional differential algebraic equation system with coefficients in $k := \mathbb{Q}$, borrowed essentially from [18, Section 3.4]:

$$\begin{cases} Y_1 &= U_1 + \dot{U}_m \\ Y_2 &= U_2 + \dot{U}_1 \\ &\vdots \\ Y_{m-1} &= U_{m-1} + \dot{U}_{m-2} \end{cases} \tag{B.1}$$

with $m > 2$.

Here, we have $n = 0$ and $r = m - 1$. The associated matrix needed for the computation of the differentiation index, $\mathfrak{J}_{1,0} \in \mathbb{Q}\langle U\rangle^{(m-1)\times m}$, is

$$\begin{pmatrix} 0 & \cdots & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 & 0 \end{pmatrix},$$

which has full row rank $m - 1$. Hence, by Definition 15, we have $\mu_{1,0} = \mu_{0,0} = 0$ and so, from Definition 25, the differentiation index σ of the system (B.1) is equal to 0.

Following the slightly informal definition of the differentiation index given in the Introduction and at the beginning of this Appendix, the fact that $\sigma = 0$ should imply that, after choosing one of the variables as a differential transcendence basis of the field extension, all the derivatives of the remaining variables can be written in terms of the variables $U_1, \ldots, U_m$ manipulating only the equations (i.e., the variables $Y_1, \ldots, Y_{m-1}$).

This rewriting of the equations is trivially true for all the variables different from U_{m-1},

$$\begin{aligned} \dot{U}_m &= Y_1 - U_1 \\ \dot{U}_1 &= Y_2 - U_2 \\ &\vdots \\ \dot{U}_{m-2} &= Y_{m-1} - U_{m-1}. \end{aligned} \tag{B.2}$$

Then, it is quite natural to consider $\{U_{m-1}\}$ as the differential transcendence basis and to interpret the previous system as a 0-dimensional system over the field $k_1 := \mathbb{Q}\langle U_{m-1}\rangle$. Now, the matrix $\mathfrak{J}_{1,0}$ is the $(m-1)$-square matrix

$$\begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix},$$

which is clearly non singular. Hence $\mu_{1,0} = \mu_{0,0} = 0$ and so, the new associated differentiation index σ_1 is equal to 0, coinciding with the differentiation index σ of the system considered over k. The relations (B.2) can be seen now as a full rewriting of the derivatives in terms of the variables. Furthermore, the order of the ideal associated to the system does not change by the extension of the ground field from $\mathbb{Q}$ to $\mathbb{Q}\langle U_{m-1}\rangle$: following Corollary 29, we have $\mathrm{ord}_{k\langle Y\rangle\langle U_{m-1}\rangle}(\Delta) = \mathrm{ord}_{k\langle Y\rangle}(\Delta) = m - 1$, since the sequence $(\mu_k)_k$ is the same in both cases, and $\{U_{m-1}\}$ is a "good" differential transcendence basis.

However, not every choice of the free variables is a "good" basis and preserves the properties of the input system. Another possible choice is to take U_m as the free variable for the system (B.1), but it is not a "good" basis since $\mathrm{ord}_{k\langle Y\rangle\langle U_m\rangle}(\Delta) = 0 \neq m - 1 = \mathrm{ord}_{k\langle Y\rangle}(\Delta)$. In this case the original system is considered

as an $(m-1)$-square 0-dimensional system over the ground differential field $k_2 := \mathbb{Q}\langle U_m\rangle$. Then, the new matrix $\mathfrak{J}_{1,0}$ is the $(m-1)$-square matrix

$$\begin{pmatrix} 0 & \cdots & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix},$$

which has rank $m-2$. So, $\mu_{1,0} \neq 0 = \mu_{0,0}$ and therefore, the differentiation index σ_2 of the system (B.1) over k_2 is strictly positive. In fact, it is easy to see that $\sigma_2 = m-1$. Now, the variables $U_1, U_2, \ldots, U_{m-1}$ can be written in terms of derivatives of the equations (i.e. the variables $Y_1, \ldots, Y_{m-1}$) and elements of the base field k_2 as follows:

$$\begin{aligned} U_1 &= Y_1 - \dot{U}_m \\ U_2 &= Y_2 - \dot{Y}_1 + U_m^{(2)} \\ U_3 &= Y_3 - \dot{Y}_2 + Y_1^{(2)} - U_m^{(3)} \\ &\vdots \\ U_{m-1} &= Y_{m-1} - \dot{Y}_{m-2} + \cdots + (-1)^{m-2} Y_1^{(m-2)} + (-1)^{m-1} U_m^{(m-1)}. \end{aligned}$$

From these identities, we can see that the order of derivatives of the equations required to express the derivatives $\dot{U}_1, \ldots, \dot{U}_{m-1}$ in terms of $U_1, \ldots, U_{m-1}$ (in this particular case, simply as elements of the base field $k\langle Y\rangle\langle U_m\rangle$) is exactly $m-1$, which is the differentiation index σ_2 of the system (B.1) interpreted over the field k_2.

The previous example shows once more that different differential transcendence bases of the differential field $\mathrm{Frac}(k\langle Y\rangle\{X, U\}/\Delta)$ over $k\langle Y\rangle$ (in the example, $\{U_{m-1}\}$ and $\{U_m\}$) may lead to very different quantitative properties of the 0-dimensional system obtained after localization. From this point of view, the first localization of the system (B.1) in a "good" differential basis seems to follow the behavior of the original system more closely than the second one.

In the next section we will show the relations between a "good" differential transcendence basis, whose existence has been proved in Section 3.3, and the remaining differential dependent variables using "few" (as many as the differentiation index) derivatives of the equations.

B.2 Implicit variables

We start this section by stating a result that is a straightforward corollary of Theorem 28 and Proposition 33. This gives us an "implicit function type" result in terms of the differentiation index σ of the system 2.1 (see also [18, Section 3]):

Theorem 70. *The variables X, U split into three different subsets: $W := \{W_1, \ldots, W_{m-r}\}$ ($m - r = dimdiff_{k\langle Y\rangle}\mathcal{F}$), $\xi := \{\xi_1, \ldots, \xi_s\}$ ($s = ord_{k\langle Y\rangle}(\Delta)$) and $\eta := \{\eta_1, \ldots, \eta_{n+r-s}\}$ where*

- *W is a differential transcendence basis of $k\langle Y\rangle \hookrightarrow Frac(k\langle Y\rangle\{X, U\}/\Delta)$.*
- *$W^{[i]} \cup \xi$ is an algebraic transcendence basis of $k\langle Y\rangle \hookrightarrow \mathcal{F}_i$ for all $i \in \mathbb{N}_0$ (see Notation 31).*
- *There exist non-zero polynomials P_t, Q_j, $1 \leq t \leq n + r - s$, $1 \leq j \leq s$, with coefficients in the base field k, such that*
  - $P_t(Y^{[\sigma-1]}, W, \xi, \eta_t) \in (F^{[\sigma-1]}, G^{[\sigma-1]}) \subset k[Y^{[\sigma-1]}, X^{[\sigma]}, U^{[\sigma]}]$,
  - $Q_j(Y^{[\sigma]}, W, \dot{W}, \xi, \dot{\xi}_j) \in (F^{[\sigma]}, G^{[\sigma]}) \subset k[Y^{[\sigma]}, X^{[\sigma+1]}, U^{[\sigma+1]}]$.

Proof. Let W and ξ be subsets of variables as in Proposition 33. Then, the first and second conditions in the statement hold. Let $\eta := \{\eta_1, \ldots, \eta_{n+r-s}\}$ be the set of the remaining variables X, U (i.e., those different from the W's and the ξ_j's).
For every t, $1 \leq t \leq n + r - s$, the element $\eta_t \in \mathcal{F}_0$ is algebraic over $k\langle Y\rangle(W \cup \xi)$, since $W \cup \xi$ is a transcendence basis of $k\langle Y\rangle \hookrightarrow \mathcal{F}_0$. Hence, there is a non-zero polynomial $\widehat{P}_t$ with coefficients in $k\langle Y\rangle$ such that $\widehat{P}_t(W, \xi, \eta_t) \in \Delta \cap A_0 = \Delta_\sigma \cap A_0$ (see Theorem 26). In the same way, the fact that $W \cup \dot{W} \cup \xi$ is a transcendence basis of $k\langle Y\rangle \hookrightarrow \mathcal{F}_1$ ensures the existence of non-zero polynomials $\widehat{Q}_j$ ($j = 1, \ldots, s$) with coefficients in $k\langle Y\rangle$ verifying: $\widehat{Q}_j(W, \dot{W}, \xi, \dot{\xi}_j) \in \Delta \cap A_1 = \Delta_{\sigma+1} \cap A_1$.
The polynomials P_t's and Q_j's that satisfy the third condition of the statement can be easily obtained from the previous $\widehat{P}_t$'s and $\widehat{Q}_j$'s, by multiplying them by adequate factors in $k\{Y\}$ and evaluating the superfluous variables $Y^{[l]}$ at suitably chosen elements of the base field k (for all $l \geq \sigma$ in the case of $\widehat{P}_t$ and for all $l \geq \sigma + 1$ for the polynomials $\widehat{Q}_j$). ■

Formally, the third statement of the previous Theorem makes no sense if the differentiation index σ is zero. However this is exactly the case where the Implicit Function Theorem can be applied in order to write each derivative of the variables $\{X, U\} \setminus \{W\}$ in terms of the same variables (obviously neither as a polynomial nor as a rational function). So, the first item of the third condition must be empty (there are no variables η). More precisely:

Remark 71. *Under the conditions of Theorem 70, suppose that the differentiation index σ is zero, then the statement of the third item of the theorem admits a natural interpretation also in this case. Following Corollary 29, the Hilbert-Kolchin polynomial of the ideal Δ over $k\langle Y\rangle$ is $\mathcal{H}_{\Delta,k\langle Y\rangle}(i) = (m - r)(i + 1) + (n + r)$ and its order is $n + r$ (recall that $\mu_{k,0}$ is always defined as 0). So, no variables η appear, or equivalently $\xi = \{X, U\} \setminus \{W\}$. Then there exist non-zero polynomials Q_j, for $j = 1, \ldots, n + r$, such that $Q_j(Y, W, \dot{W}, \xi, \dot{\xi}_j) \in (F, G) \subset k[Y, X, \dot{X}, U, \dot{U}]$.*

The non-zero polynomials P_t and Q_j introduced in Theorem 70 are not uniquely determined without any additional requirements (as minimality of order and degree, irreducibility, etc.). However, the conditions stated in this theorem allow us to choose a family of such polynomials that can be regarded as eliminating polynomials of suitable algebraic-geometric situations and thus, repeating the arguments and the notation we used in the Subsection 4.1.3, estimate their degrees.

Recall that, for each $N \in \mathbb{N}$ we denote $\mathbb{A}^N$ the affine space $\bar{k}^N$, where $\bar{k}$ is a fixed algebraic closure of the ground field k, with the Zariski topology.

Set $N_0 := (r+n+m)\sigma + n + m$ and $N_1 := (r+n+m)(\sigma+1) + n + m$ and let $\mathbb{V}_0 \subset \mathbb{A}^{N_0}$ and $\mathbb{V}_1 \subset \mathbb{A}^{N_1}$ be the algebraic varieties defined by the ideals $(F^{[\sigma-1]}, G^{[\sigma-1]}) \subset k[Y^{[\sigma-1]}, X^{[\sigma]}, U^{[\sigma]}]$ and $(F^{[\sigma]}, G^{[\sigma]}) \subset k[Y^{[\sigma]}, X^{[\sigma+1]}, U^{[\sigma+1]}]$ respectively, that is:

$$\mathbb{V}_0 := \{F^{[\sigma-1]} = 0\,,\ G^{[\sigma-1]} = 0\} \qquad \text{and} \qquad \mathbb{V}_1 := \{F^{[\sigma]} = 0\,,\ G^{[\sigma]} = 0\}.$$

Note that both varieties are irreducible complete intersection and their dimensions are, respectively, $m(\sigma+1)+n$ and $m(\sigma+2)+n$.

Let $W := \{W_1, \ldots, W_{m-r}\}$, $\xi := \{\xi_1, \ldots, \xi_s\}$ and $\eta := \{\eta_1, \ldots, \eta_{n+r-s}\}$ be as in Theorem 70. For t with $1 \le t \le n+r-s$, and j with $1 \le j \le s$, we define linear projections π_t and θ_j as follows:

$$\begin{aligned} \pi_t &: \mathbb{V}_0 \to \mathbb{A}^{r(\sigma-1)+m+s+1}, \qquad \pi_t(y^{[\sigma-1]}, x^{[\sigma]}, u^{[\sigma]}) := (y^{[\sigma-1]}, w, \xi, \eta_t); \\ \theta_j &: \mathbb{V}_1 \to \mathbb{A}^{r(\sigma-1)+2m+s+1}, \qquad \theta_j(y^{[\sigma]}, x^{[\sigma+1]}, u^{[\sigma+1]}) := (y^{[\sigma]}, w, \dot{w}, \xi, \dot{\xi}_j). \end{aligned}$$

From Proposition 33, we deduce that the set $\{Y^{[\sigma-1]}, W, \xi\}$ (resp. the set $\{Y^{[\sigma]}, W, \dot{W}, \xi\}$) is algebraically independent in the fraction field $k(\mathbb{V}_0)$ (resp. $k(\mathbb{V}_1)$). On the other hand, due to Theorem 70, the set $\{Y^{[\sigma-1]}, W, \xi, \eta_t\}$ (resp. $\{Y^{[\sigma]}, W, \dot{W}, \xi, \dot{\xi}_j\}$) is algebraically dependent in the same field. Thus, the closure of the image of the map π_t (resp. θ_j) is a k-definable irreducible hypersurface in the corresponding space and so, it can be defined by a single polynomial lying in the ideal $(F^{[\sigma-1]}, G^{[\sigma-1]})$ (resp. $(F^{[\sigma]}, G^{[\sigma]})$) whose total degree (see [29, Lemma 2]) is bounded by $\deg \mathbb{V}_0$ (resp. $\deg \mathbb{V}_1$).

Therefore, we obtain the following upper bounds for the degrees of polynomials P_t and Q_j providing implicit equations for the dependent variables:

Proposition 72. *With the previous assumptions and notations, there exist polynomials P_t and Q_j meeting the conditions of Theorem 70 with total degrees bounded by* $\deg \mathbb{V}_0$ *and* $\deg \mathbb{V}_1$ *respectively. In particular, if d is an upper bound for the total degree of the polynomials in system (2.1), we have* $\deg P_t \le d^{\sigma(n+r)}$ *and* $\deg Q_j \le d^{(\sigma+1)(n+r)}$.

Proof. The first degree upper bounds stated are those previously obtained. The (non-intrinsic) upper bounds in terms of d follow straightforwardly from the Bézout inequality (see, for instance, [29, Theorem 1]) applied to estimate $\deg \mathbb{V}_0$ and $\deg \mathbb{V}_1$. ■

Following the same arguments applied in Section 4.2 we can show not only degree upper bound for the polynomials P_t and Q_j, but also effective procedures for their computation.
Once again, for simplicity, suppose $k := \mathbb{Q}$ and assume that the input polynomials F, G have degree bounded by d and they are given by a straight line program of length L. Then, the following complexity result can be obtained :

Proposition 73. *There is a probabilistic algorithm which computes the polynomials P_t's and Q_j's introduced in Theorem 70 with error probability bounded by ε, with $0 < \varepsilon < 1$, and within complexity $O(\log(1/\varepsilon)d^2L)\ \Pi(n+m, \max_i \deg \mathbb{V}_i))$, where Π is a suitable two-variate universal polynomial.*

The complete proof of this result follows almost exactly the proof of the Proposition 58 and so we omit it now.

Appendix C

Bézout-type degree bounds for the resolvent representation of explicit systems

In this appendix we will consider a particular kind of differential algebraic equation systems. These systems, which are a special case of the system (2.1) with differential index 0, are the ones usually considered in the classical theory of ordinary differential equation.

We will obtain for these systems a more accurate syntactic bound for the degree of the minimal polynomial of a primitive element. This bound is a consequence of a more precise computation of the degree of the constructible algebraic set $\pi(\mathbb{V})$ (see Notation 47), which bounds the degree of the minimal polynomial, than the Bézout bound for the degree of the variety $\mathbb{V}$ stated, for instance, in Theorem 49 above (see also Theorem 61 and Example 51).

The particular systems we will consider here are the following:

$$\begin{cases} \dot{X}_1 &= f_1(X, U) \\ &\vdots \\ \dot{X}_n &= f_n(X, U) \end{cases}, \tag{C.1}$$

where, as before, $X := X_1, \ldots, X_n$ and $U := U_1, \ldots, U_m$ are differential unknowns and the polynomials $f_1, \ldots, f_n \in k[X, U]$ (k a differential field with a non constant element) have their total degrees bounded by an integer d. Again, for $i = 1, \ldots n$, we set $F_i = f_i - \dot{X}_i \in k[X, \dot{X}, U]$. In other words, (C.1) is the special case of (2.1) with $r = 0$.

In Section 4 we have stated all our degree and algorithmic upper bounds in terms of the degree of the algebraic variety $\mathbb{V}$ introduced in Notation 47 (or alternatively in syntactic terms by means of the Bézout inequality). However, the invariant which really bounds the quantities already mentioned is the degree of the image of the variety $\mathbb{V}$ under a suitable projection π (see, for instance, Proposition 48).

Here we will find a more precise syntactic, "Bézout-type" upper bound for $\deg \pi(\mathbb{V})$ for systems of type (C.1) and this will improve the estimations given in Theorems 49 & 61.

We keep the notations of Section 4 for the particular class of systems considered in this appendix (recalling that now $r = 0$ and so $K = k$). In this case, the differential transcendence basis W is just the set of variables U. Moreover, as it is the case in the example 51, we have that if $\Delta = [F]$, $\Delta \cap k[X^{[i]}, U^{[i]}] = (F^{[i]})$ (and so $\sigma = 0$) and its differential Hilbert-Kolchin polynomial is $\mathcal{H}_{k,\Delta}(i) = (m+1)i + n$, in particular $s = \mathrm{ord}_k(\Delta) = n$. So, if we set $N_1 := (n+m)(n+1)$ (see Notation 47 and Remark 46), the variety $\mathbb{V}$ contained in $\mathbb{A}^{N_1}$ is defined by the ideal $(F^{[n-1]}) \subset k[U^{[n]}, X^{[n]}]$.

Therefore, let $\gamma := \lambda_1 X_1 + \cdots + \lambda_n X_n$ be a primitive element of the extension $k\langle U\rangle \hookrightarrow \mathcal{F}$, $N_2 := m(n+1) + n + 1$ (recall that now $r = 0$ and $s = n$) and $\pi : \mathbb{V} \to \mathbb{A}^{N_2}$ be the projection $(u^{[n]}, x^{[n]}) \to (u^{[n]}, \gamma(x), \ldots, \gamma^{(n)}(x))$, where, for $l = 0, \ldots, n$, we have $\gamma^{(l)} = \sum_{k=0}^{l} \binom{l}{k} (\sum_{i=1}^{n} \lambda_i^{(k)} X_i^{(l-k)})$ according to Leibniz's formula.

Under these notations, the following inequality holds:

Proposition 74. $\deg \pi(\mathbb{V}) \leq \prod_{i=1}^{n} (i(d-1)+1)$.

Proof. Consider the dominant morphism $\pi : \mathbb{V} \to \overline{\pi(\mathbb{V})} \subset \mathbb{A}^{N_2}$. Since $\dim \pi(\mathbb{V}) = N_2 - 1 = m(n+1) + n$, Remark 4 implies that $\dim \pi(\mathbb{V}) = \dim \mathbb{V}$. Hence, the Theorem of Fibers (see for instance [61, Ch. I, Sec. 6, Th. 7]) implies that the typical (i.e. generic) fiber of the morphism π is 0-dimensional. More precisely, there exist Zariski dense open sets $\mathcal{V} \subset \mathbb{V}$ and $\mathcal{U} \subset \pi(\mathbb{V})$ such that $\pi(\mathcal{V}) \subset \mathcal{U}$ and $\pi|_{\mathcal{V}} : \mathcal{V} \to \mathcal{U}$ has all its fibers 0-dimensional (in particular no empty).

Let $L \subset \mathbb{A}^{N_2}$ be a generic 1-dimensional linear variety such that $L \cap \mathcal{U}$ is finite and its cardinal is exactly $\deg \pi(\mathbb{V})$.

If we set U_{ij}, T_k with $1 \leq i \leq m$, $0 \leq j \leq n$ and $0 \leq k \leq n$ for the coordinates of the affine space $\mathbb{A}^{N_2}$, the linear variety L is defined by $N_2 - 1$ linear (non-homogeneous) equations $\ell_p = 0$, $p = 1, \ldots, N_2 - 1$, in these variables. Moreover, because of the genericity of L, the equations can be chosen in a 'triangular' form. More precisely,

- If $p = 1, \ldots, n+1$, we have $\ell_p = b_p + T_{p-1} + \sum_{i=1}^{m} \sum_{j=0}^{n} a_{pij} U_{ij}$, with $b_p, a_{pij} \in k$.
- If $p = n+2, \ldots, N_2 - 1$, we have $\ell_p = b_p + \sum_{i=1}^{m} \sum_{j=0}^{n} a_{pij} U_{ij}$, with $b_p, a_{pij} \in k$.

Set $\mathbb{W} := \pi^{-1}(L \cap \pi(\mathbb{V}))$.

Since $L \cap \mathcal{U}$ is finite and has as many points as $\deg \pi(\mathbb{V})$, we infer that $L \cap \mathcal{U} = L \cap \pi(\mathbb{V})$. Therefore, $\mathbb{W} \subset \mathbb{V}$ is also a finite set (recall that $\pi|_{\mathcal{V}}$ has finite fibers). Moreover, the inequality

$$\deg \pi(\mathbb{V}) \leq \#(\mathbb{W}) \tag{C.2}$$

holds.

Explicitly, the closed set $\mathbb{W}$ is given by the equations defining $\mathbb{V}$ and $\pi^{-1}(L)$:

$$\mathbb{W} = \left\{ \begin{array}{rcl} F & = & 0 \\ \vdots & & \vdots \\ F^{(n-1)} & = & 0 \\ b_p + \sum_{k=0}^{p-1} \binom{p-1}{k} (\sum_{i=1}^{n} \lambda_i^{(k)} X_i^{(p-1-k)}) + \sum_{i=1}^{m} \sum_{j=0}^{n} a_{pij} U_i^{(j)} & = & 0, \quad 1 \leq p \leq n+1 \\ b_p + \sum_{i=1}^{m} \sum_{j=0}^{n} a_{pij} U_i^{(j)} & = & 0, \qquad n+2 \leq p \end{array} \right. \tag{C.3}$$

Taking the successive derivatives of the equations appearing (C.1) we have that, for all $i = 1, \ldots n$ and $j \in \mathbb{N}_0$, there exists a polynomial $h_{ij} \in k[X, U, \ldots, U^{(j-1)}]$ such that

$$X_i^{(j)} \equiv h_{ij}(X, U, \ldots, U^{(j-1)}) \qquad (\mathrm{mod}\ (F^{[j-1]})). \tag{C.4}$$

Moreover, the polynomials h_{ij} can be taken verifying the following recursion:

$$h_{i0} := X_i \qquad \text{for} \qquad i = 1, \ldots, n$$

$$h_{ij} := \sum_{k=1}^{n} \frac{\partial h_{i,j-1}}{\partial X_k} f_k + \sum_{k=1}^{m} \sum_{l=1}^{j-2} \frac{\partial h_{i,j-1}}{\partial U_k^{(l)}} U_k^{(l+1)} \qquad \text{for} \quad 1 \leq i \leq n \ \text{ and } j \geq 1.$$

In other words, these polynomials can be obtained by differentiating and replacing the variables $\dot{X}_i$ by the polynomials f_i $(i = 1, \ldots, n)$.

From this construction we observe that the total degree of the polynomials h_{ij} can be easily estimated:

$$\deg h_{ij} \leq j(\deg f_i - 1) + 1, \qquad \text{for all } i = 1, \ldots, n \text{ and } j \in \mathbb{N}_0. \tag{C.5}$$

From (C.4), the equations defining (C.3) which correspond to the first n equations defining $\pi^{-1}(L)$ can be replaced by:

$$b_p + \sum_{k=0}^{p-1} \binom{p-1}{k} (\sum_{i=1}^{n} \lambda_i^{(k)} h_{i,p-1-k}) + \sum_{i=1}^{m} \sum_{j=0}^{n} a_{pij} U_i^{(j)} = 0,$$

for $1 \leq p \leq n+1$.

Hence, according to (C.5), the p-th equation of this type has total degree bounded by

$$\max\{(p-1-k)(\deg f_i - 1) + 1\ ,\ k = 0, \ldots, p-1\} \leq (p-1)(d-1) + 1, \tag{C.6}$$

where $d := \max_i \deg f_i$.

Now, let $\mathcal{W} \subset \mathbb{A}^{(n+1)m+n}$ be the algebraic set defined by

$$\mathcal{W} := \left\{ \begin{array}{rcll} b_p + \sum_{k=0}^{p-1} \binom{p-1}{k} (\sum_{i=1}^{n} \lambda_i^{(k)} h_{i,p-1-k}) + \sum_{i=1}^{m} \sum_{j=0}^{n} a_{pij} U_i^{(j)} & = & 0, & 1 \leq p \leq n+1 \\ b_p + \sum_{i=1}^{m} \sum_{j=0}^{n} a_{pij} U_i^{(j)} & = & 0, & n+2 \leq p \end{array} \right. \tag{C.7}$$

(observe that the system only involves the variables $U^{[n]}$ and X and so, the variety $\mathcal{W}$ may be interpreted in the $(n+1)m+n-$dimensional affine space).

By comparing (C.3) and (C.7) we observe that $\mathcal{W}$ is a finite set and $\#(\mathcal{W}) = \#(\mathbb{W})$ since the the variables $X^{(1)}, \ldots, X^{(n)}$ are uniquely determined by the equations $F = 0, \ldots, F^{(n-1)} = 0$.

Finally, by Bézout inequality and the upper degree bound (C.6), we infer that $\#(\mathcal{W}) \leq \prod_{p=1}^{n+1}((p-1)(d-1)+1)$ and then, from (C.2) we deduce the inequality:

$$\deg \pi(\mathbb{V}) \leq \prod_{i=1}^{n} (i(d-1)+1).$$

■

This Proposition shows that the degree of the minimal polynomial of a primitive element of the field extension associated to the system (C.1) is bounded by $\prod_{i=1}^{n}(i(d-1)+1)$.

Finally, let us remark that this single exponential degree upper bound for the minimal polynomial induces, for this particular case, a more accurate estimation for the degree bounds in the resolvent representation than the double exponential bounds found in 49 & 61 by means of the Bézout inequality.

List of Symbols

$\mathbb{N}$	the set of natural numbers $\{1, 2, \ldots\}$, page 25
$\mathbb{N}_0$	the set $\mathbb{N} \cup \{0\}$, page 25
$[\Xi]$	the differential ideal generated by the set Ξ, page 26
$\mathcal{E}\langle\Xi\rangle$	the minimal differential field containing the differential field $\mathcal{E}$ and Ξ, page 26
$\dot{Z}_j$	the first derivative of the variable Z_j, page 26
$Z_j^{(i)}$	the i-th derivative of the variable Z_j, page 26
ΘZ	the set of variables $\{Z_j^{(i)}, i \in \mathbb{N}_0, \}$, page 26
Z	the set of variables $\{Z_1, \ldots, Z_\alpha\}$, page 26
$Z^{(i)}$	the set of variables $Z_1^{(i)}, \ldots, Z_\alpha^{(i)}$, page 26
$p^{(l)}$	the l-th derivative of the differential polynomial p, page 26
$\mathrm{ord}(p, Z_j)$	the order of the maximal derivative of X_j that appears in p, page 27
$\mathrm{ord}(p)$	the maximal order of derivation that appears in p, page 27
$\mathrm{Frac}(\mathcal{E}\{Z\}/\mathcal{I})$	the fraction field of the differential integral domain $\mathcal{E}\{Z\}/\mathcal{I}$, page 27
$\mathrm{diffdim}_{\mathcal{F}}(\mathcal{I})$	the differential dimension of the differential ideal $\mathcal{I}$ over $\mathcal{E}$, page 27
$\mathcal{H}_{\mathcal{I},\mathcal{E}}$	the Hilbert-Kolchin function of $\mathcal{I}$ with respect to $\mathcal{E}$, page 27
$\mathrm{trdeg}_{\mathcal{E}}$	the transcendence degree of over $\mathcal{E}$, page 27
$\mathrm{ord}_{\mathcal{E}}(\mathcal{I})$	the order of $\mathcal{I}$ with respect to $\mathcal{E}$, page 28
$\deg(f)$	the total degree of the polynomial f, page 29
$Z^{[i]}$	the set of variables $Z, \dot{Z}, \ldots, Z^{(i)}$, page 31
H	the set of functions $H_1, \ldots, H_\beta$, page 31
$\dot{H}_j$	the first derivative of the function H_j, page 31
$H^{(i)}$	the set of functions $H_1^{(i)}, \ldots, H_\beta^{(i)}$, page 31

$H^{[i]}$	the set of functions $H, \dot{H}, \ldots, H^{(i)}$, page 31
X	the set of differential variables $X_1, \ldots, X_n$, page 32
U	the set of differential variables $U_1, \ldots, U_m$, page 32
Y	the set of differential parameters $Y_1, \ldots, Y_r$, page 32
k	a differential field of charasteristic 0, page 32
(Σ)	the differential algebraic system considered throughout this thesis, page 32
F_i	the polynomials $f_i - \dot{X}_i \in k[X, \dot{X}, U]$, page 33
G_j	the polynomials $g_j - Y_j \in k[Y, X, U, \dot{U}]$, page 33
$(F^{[l-1]}, G^{[l-1]})$	the polynomial ideal generated by $F^{[l-1]}, G^{[l-1]}$, page 33
$\tilde{f}_i^{(k)}$	the polynomial obtained by replacing $X_h^{(l)} = \tilde{f}_h^{(l-1)}$ in $f_i^{(k)}$, page 33
$\tilde{g}_j^{(k)}$	the polynomial obtained by replacing $X_h^{(l)} = \tilde{f}_h^{(l-1)}$ in $g_j^{(k)}$, page 33
$\mathfrak{p}_{i,s}$	the polynomial ideal generated by $F^{[i-1]}, G^{[i-1]}, F_1^{(i-1)}, \ldots, F_s^{(i-1)}$, page 33
$\mathfrak{q}_{i,t}$	the polynomial ideal generated by $F^{[i-2]}, G^{[i-2]}, F^{(i-1)}, G_1^{(i-1)}, \ldots, G_t^{(i-1)}$, page 33
Δ	the differential ideal in $k\langle Y\rangle\{X, U\}$ generated by F, G, page 34
A_l	the polynomial ring $k\langle Y\rangle[X^{[l]}, U^{[l]}]$, page 34
Δ_l	the polynomial ideal in A_l generated by $F^{[l-1]}, G^{[l-1]}$, page 34
$\mathcal{F}$	the fraction field of $k\{Y, X, U\}/[F, G]$ and $k\langle Y\rangle\{X, U\}/\Delta$, page 36
J_l	the Jacobian matrix of the polynomials $F^{[l-1]}, G^{[l-1]}$ with respect to the variables $X^{[l]}, U^{[l]}$, page 37
$\mathfrak{J}_l$	the matrix obtained by replacing $X_j^{(k)} = \tilde{f}_j^{(k-1)}$ in J_l, page 37
$J_{k,i}$	the Jacobian matrix of the polynomials $F^{(i)}, G^{(i)}, \ldots, F^{(i+k-1)}, G^{(i+k-1)}$ with respect to the variables $X^{(i+1)}, U^{(i+1)}, \ldots, X^{(i+k)}, U^{(i+k)}$, page 38
$\mathfrak{J}_{k,i}$	the matrix obtained by replacing $X_j^{(k)} = \tilde{f}_j^{(k-1)}$ in $J_{k,i}$, page 38
$\mathfrak{J}_{k,i}^t$	the transpose of $\mathfrak{J}_{k,i}$, page 38
$\mu_{k,i}$	the dimension of the kernel of $\mathfrak{J}_{k,i}^t$, page 39
σ	the differential index , page 45
$\mathcal{F}_i$	the fraction field of $A_i/(\Delta \cap A_i)$, page 51
W	a subset $\{W_1, \ldots, W_{m-r}\} \subset \{X, U\}$ which is a "good" differential transcendence basis of the field extension $k\langle Y\rangle \hookrightarrow \mathcal{F}$, page 53

K	the differential field $k\langle Y, W\rangle$, page 66
V	the set of $n + r$ variables $\{X, U\} \setminus W$, page 66
γ	a primitive element of the field extension $K \hookrightarrow \mathcal{F}$, page 66
M	a minimal polynomial for γ, page 66
$\tilde{\Delta}$	the differential ideal in $K\{V\}$ generated by F and G, page 66
$\tilde{A}_i$	the polynomial ring $K[V^{[i]}]$, page 66
$\tilde{\Delta}_i$	the polynomial ideal in $\tilde{A}_i$ generated by $F^{[i-1]}, G^{[i-1]}$, page 66
$\mathbb{A}^n$	the n-dimensional affine space with the Zariski topology, page 67
$\mathbb{V}$	the algebraic variety defined by the ideal Δ_{2n+2r}, page 67
$\deg(\mathbb{V})$	the degree of $\mathbb{V}$, page 68
Λ	a set $\{\Lambda_1, \ldots, \Lambda_{n+r}\}$ of differential indeterminates over k, page 71
k_Λ	the differential field $k\langle\Lambda\rangle$, page 71
Δ_Λ	the differential ideal of $k_\Lambda\{Y, X, U\}$ generated by F, G, page 71
$\mathcal{F}_\Lambda$	the differential field $\mathcal{F}\langle\Lambda\rangle$, page 71
$\tilde{\Delta}_\Lambda$	the differential ideal of $K_\Lambda\{V\}$ generated by F, G, page 71
Γ	a primitive element of $K_\Lambda \hookrightarrow \mathcal{F}_\Lambda$, page 71
M_Λ	a minimal polynomial for Γ, page 72
$\mathbb{A}^{N_1}(\overline{k(\Lambda^{[s]})})$	the N_1-dimensional affine space over any algebraic closure of field $k(\Lambda^{[s]})$ with the Zariski topology, page 72
$\mathbb{V}_\Lambda$	the algebraic variety of $\mathbb{A}^{N_1}(\overline{k(\Lambda^{[s]})})$ defined by the polynomials $F^{[2n+2r-1]}, G^{[2n+2r-1]}$, page 72
Ω	the differential ideal generated by $F_1, \ldots, F_n, G_1, \ldots, G_\rho$, page 90
Ω_l	the algebraic ideal generated by $F^{[l-1]}, G_1^{[l-1]}, \ldots, G_\rho^{[l-1]}$, page 90
$\mathcal{G}$	the fraction field of $k\{Y, X, U\}/\Omega$, page 91
$\mathcal{Y}$	a differentially algebraically independent subset of $\{Y_1, \ldots, Y_\rho\}$, page 91
M_j	a minimal polynomial for Y_j, page 93
Ω^j	the differential ideal generated by F, G, G_j, page 93
Ω_l^j	the algebraic ideal generated by $F^{[l-1]}, G^{[l-1]}, G_j^{[l-1]}$, page 93
V_j	the algebraic variety defined by Ω_{n+r+1}^j, page 94

Bibliography

[1] M. Atiyah, I. Macdonald, Introduction to Commutative Algebra. Addison-Wesley, 1969.

[2] S. Basu, R. Pollack, M.-F. Roy, Algorithms in Real Algebraic Geometry. Algorithms and Computation in Mathematics 10, Springer-Verlag, Berlin, 2003.

[3] D. Bini, V.Y. Pan, Polynomial and Matrix Computations. Vol. 1. Fundamental Algorithms, Progress in Theoretical Computer Science, Birkhäuser Boston, Inc., Boston, MA, 1994.

[4] F. Boulier, D. Lazard, F. Ollivier et M. Petitot., Computing representations for radicals of finitely generated differential ideals, Publication interne IT-306 (1997) du LIFL.

[5] F. Boulier, D. Lazard, F. Ollivier et M. Petitot., Representation for the radical of a finitely generated differential ideal, Proceedings of ISSAC textbf95 (juillet 1995, Montréal).

[6] F. Boulier, Étude et implantation de quelques algorithmes en algèbre différentielle, Thèse de l'Université de Lille, 27 juin 1994.

[7] K. Brenan, S. Campbell, L. Petzold, Numerical Solution of Initial-Value Problems in Differential-Algebraic Equations, SIAM's Classics in Applied Mathematics, Philadelphia 1996.

[8] P. Bürgisser, M. Clausen, M.A. Shokrollahi, Algebraic Complexity Theory, Grundlehren der Mathematischen Wissenschaften 315, Springer-Verlag, Berlin, 1997.

[9] S. Campbell, W. Gear, The index of general nonlinear DAE's. Numerishe Mathematik **72** (1995), 173–196.

[10] G. Carrà Ferro, Some Upper Bounds for the Multiplicity of an autoreduced Subset of N^m and its applications. Algebraic Algorithms and Error Correcting Codes, AAECC-3, Grenoble, July 1985 (J. Calmet, ed.), Lect. Notes in Comp. Sci. **229** (1986), 306–315.

[11] É. Cartan, Sur l'intégration de certains systèmes indéterminés d'équations différentielles, Journal für die reine und angewandte Mathematik **145**, 86–91, 1915.

[12] T. Cluzeau, E. Hubert, Resolvent Representation for Regular Differential Ideals, Technical Report RR-4200, INRIA Sophia Antipolis, 2001.

[13] T. Cluzeau, E. Hubert, Resolvent representation for regular differential ideals, AAECC 13 (2003) 395–425.

[14] L. D'Alfonso, G. Jeronimo, P. Solernó, On the Complexity of the Resolvent Representation of Some Prime Differential Ideals. Journal of Complexiy 22 (2006) 396–430.

[15] L. D'Alfonso, G. Jeronimo, P. Solernó, A linear algebra approach to the differentiation index of generic differential algebraic equation systems. Preprint.

[16] S. Diop, M. Fliess, On nonlinear observability, Proceedings of the European Control Conference 1991, 152-157, Commault, C. and Normand-Cyrot, D. and Dion, J. M. and Dugard, L. and Fliess, M. and Titli, A. and Cohen, G. and Benveniste, A. and Landau, I. D., Paris, Hermès.

[17] M. Fliess, J. Lévine, P. Martin, P. Rouchon, A Lie-Bäcklund approach to equivalence and flatness of nonlinear systems, IEEE AC. **44**, 922-937, 1999.

[18] M. Fliess, J. Lévine, P. Martin, P. Rouchon, Implicit Differential Equations and Lie-Bäcklund mappings. Proc. of the 34th. Conf. on Decision & Control, New Orleans, December 1995, 2704–2709.

[19] 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.

[20] M. Fliess, J. Lévine, P. Martin, P. Rouchon, Flatness and defect of nonlinear systems: introductory theory and applications, Internat. J. Control **61**, 1995, p. 1327-1887.

[21] W. Fulton, Algebraic Curves. W.A. Benjamin (1969).

[22] G. Gallo, B. Mishra, Efficient algorithms and bounds for Wu-Ritt characteristic sets, Effective methods in algebraic geometry (Castiglioncello, 1990), 119–142, Progr. Math. **94**, Birkhäuser Boston, Boston, MA, 1991.

[23] G. Gallo, B. Mishra, The complexity of resolvent resolved, Proceedings of the Fifth Annual ACM-SIAM Symposium on Discrete Algorithms (Arlington, VA, 1994), 280–289, ACM, New York, 1994.

[24] J. von zur Gathen, Parallel arithmetic computations: a survey, in Proc. 12th FOCS, Bratislava, 1986, Springer LNCS **33** (1986) 93–112.

[25] J. von zur Gathen, J. Gerhard, Modern Computer Algebra, Cambridge University Press, New York, 1999.

[26] 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.

[27] 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), Springer LNCS 948 (1995) 205–231.

[28] M. Giusti, G. Lecerf, B. Salvy, A Gröbner free alternative for polynomial system solving, J. Complexity 17 (2001), No. **1**, 154–211.

[29] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, Theoret. Comput. Sci. **24** (3) (1983) 239–277.

[30] J. Heintz, T. Krick, S. Puddu, J. Sabia, A. Waissbein, Deformation techniques for efficient polynomial equation solving, J. Complexity **16** (2000), No. 1, 70–109.

[31] J. Heintz, G. Matera, A. Waissbein, On the time-space complexity of geometric elimination procedures, Appl. Algebra Engrg. Comm. Comput. **11** (2001), No. 4, 239–296.

[32] J. Heintz, C.-P. Schnorr, Testing polynomials which are easy to compute, Monographie **30** de l'Enseignement Mathématique (1982) 237–254.

[33] D. Hilbert, Über den Begriff der Klasse von Differentialgleichungen, Mathematische Annalen **73**, 95–108, 1912.

[34] 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. 4087.

[35] C. Jacobi, De investigando ordine systematis aequationum differentialum vulgarium cujuscunque, C. G. J. Jacobi's gesammelte Werke, fünfter Band, herausgegeben von K. Weierstrass, Berlin, Bruck und Verlag von Georg Reimer, 1890, 193–216. Translated from latin by F. Ollivier (Ecole Polytechnique, Palaiseau) in `http://www.lix.polytechnique.fr/~ollivier/JACOBI/jacobiEngl.htm`

[36] C. Jacobi, De aequationum differentialum systemate non normali ad formam normalem revocando, [Of the reduction in normal form of a non normal system of differential equations], published by A. Clebsch, *C.G.J. Jacobi's gesammelte Werke, fünfter Band*, herausgegeben von K. Weierstrass, Berlin, Bruck und Verlag von Georg Reimer, 1890, p. 485-513.

[37] R. E. Kalman, On the general theory of control systems, Proceedings of the first international congress on automatic control, Moscow, USSR, (1961), vol. **1**, Butterworths, London, 481–492.

[38] E.R. Kolchin, Differential Algebra and Algebraic Groups, Academic Press, New York, 1973.

[39] T. Krick, L.M. Pardo, A computational method for Diophantine approximation, Progr. Math. **143** (1996) 193–254.

[40] T. Krick, L.M. Pardo, M. Sombra, Sharp estimates for the arithmetic Nullstellensatz, Duke Math. J. 109 (2001), No. **3**, 521–598.

[41] L. Kronecker, Grundzüge einer arithmetischen Theorie der algebraischen Grössen, J. Reine Angew. Math. **92** (1882) 1–122.

[42] E. Kunz, Introduction to Commutative Algebra and Algebraic Geometry, Birkhäuser Boston, Inc., Boston, MA, 1985.

[43] G. Lecerf. Une alternative aux méthodes de réécriture pour la résolution des systèmes algébriques. PhD thesis, École polytechnique, 2001.

[44] G. Le Vey, Differential Algebraic Equations: a new look at the index. Rapp. Rech. **2239**, INRIA, (1994).

[45] G. Matera, A. Sedoglavic, Fast computation of discrete invariants associated to a differential rational mapping, International Symposium on Symbolic and Algebraic Computation (ISSAC'2002) (Lille), J. Symbolic Comput. **36** (2003), No. 3-4, 473–499.

[46] G. Monge, Supplément où l'on fait voir que les équations aux différences ordinaires, pour lesquelles les conditions d'intégrabilité ne sont pas satisfaites, sont susceptibles d'une véritable intégration, *Histoire de l'Académie royale des sciences*, Paris, Imprimerie royale, 1784. http://gallica.bnf.fr/

[47] S. Moutaouakil, F. Ollivier, B. Sadik, Applications of Jacobi's bound for computing characteristic sets of ordinary differential and difference systems. Preprint (2005).

[48] F. Ollivier, Le problème de l'identifiabilité structurelle globale: approche théorique, méthodes effectives et bornes de complexité. PhD Thesis, Ecole Polytechnique 1990.

[49] F. Ollivier, B. Sadik, An effective weak generalization of Lüroth-Ritt theorem. International Conference on Polynomial System Solving Paris (2004).

[50] P. Rabier, W. Rheinboldt, A Geometric Treatment of Implicit Differential-Algebraic Equations. J. of Diff. Equations **109**, (1994), 110-146.

[51] J.F. Ritt, Differential equations from the algebraic standpoint, Amer. Math. Soc. Colloq. Publ., Vol. **14**, New York, 1932.

[52] J.F. Ritt, Differential Algebra, Amer. Math. Soc. Colloq. Publ., Vol. **33**, New York, 1950.

[53] B. Sadik, A bound for the order of characteristic set elements of an ordinary prime differential ideal and some applications, Appl. Algebra Engrg. Comm. Comput. 10 (2000), No. **3**, 251–268.

[54] B. Sadik, Contributions à l'étude de la complexité du calcul d'un ensemble caractéristique en algèbre différentielle, PhD. Thesis, 1995.

[55] E. Schost, Computing parametric geometric resolutions, Appl. Algebra Engrg. Comm. Comput. **13** (2003), No. 5, 349–393.

[56] J.T. Schwartz, Fast probabilistic algorithms for verification of polynomial identities, J. ACM **27** (1980) 701–717.

[57] A. Sedoglavic, A probabilistic algorithm to test local algebraic observability in polynomial time, Computer algebra (London, ON, 2001), J. Symbolic Comput. **33** (2002), No. 5, 735–755.

[58] A. Sedoglavic, A mixed symbolic-numeric method to study prime ordinary differential ideals, Preprint, École Polytechnique, 2000, http://www.medicis.polytechnique.fr/ sedoglav/Load/Sedoglavic2000.pdf.

[59] A. Seidenberg, Some basic theorems in differential algebra (characteristic p arbitrary), Trans. Amer. Math. Soc. **73** (1952) 174–190.

[60] W. Seiler, Indices and Solvability of General Systems of Differential equations. Comput. Algebra in Scientific Comput., CASC 99 (V. Ghanza, E. Mayr, E. Vorozhtsov, eds.), Springer (1999), 365–385.

[61] I.R. Shafarevich, Basic Algebraic Geometry, Grundlehren der mathematischen Wissenschaften **213**, Springer-Verlag 1977.

[62] G. Thomas, Symbolic computation of the index of quasilinear differential-algebraic equations. Proc. of the 1996 International Symposium on Symbolic and Algebraic Computation, Zurich, Switzerland (Y. Lakshman, ed.), ACM Press, New York (1996), 196–203.

[63] R. Zippel, Probabilistic algorithms for sparse polynomials, Proc. EUROSAM'79, Springer LNCS **72** (1979) 216–226.

[64] P. Zervos, Le problème de Monge, Mémorial des Sciences Mathématiques, fascicule LIII, Gauthier-Villars, Paris, 1932.