Notes on Triangular Sets and Triangulation-Decomposition Algorithms II: Differential Systems

Evelyne Hubert

INRIA - Projet CAFE
2004 route des lucioles BP 93
F-06902 Sophia Antipolis
Evelyne.Hubert@inria.fr

Abstract. This is the second in a series of two tutorial articles devoted to triangulation-decomposition algorithms. The value of these notes resides in the uniform presentation of triangulation-decomposition of polynomial and differential radical ideals with detailed proofs of all the presented results.We emphasize the study of the mathematical objects manipulated by the algorithms and show their properties independently of those. We also detail a selection of algorithms, one for each task. The present article deals with differential systems. It uses results presented in the first article on polynomial systems but can be read independently.

1 Introduction

Given a system of partial differential equations we wish to compute a representation that is equivalent but for which we can analyze the solution set. The first essential problem arising is whether the system admits any solution, analytic or in terms of formal power series. The second central problem is to describe the arbitrariness coming into the solution set i.e. how many initial conditions can be chosen to ensure the existence and uniqueness of a solution. Those problems were addressed in the late nineteenth century by Cartan and Riquier with different viewpoints [18, 57]. We will not attempt here any historical review but wish to report on recent algorithmic development in *differential algebra* in the line of the work of Ritt and Kolchin [60, 40], that is partly based on the work of Riquier. Few bridges have been established between the different algebraic approaches and their algorithmic developments. W. Seiler gives a review of the different algebraic and algorithmic approaches in [67] and B. Malgrange advocates some mutual interaction in [45]. The article by A. Buium and P. J. Cassidy [15] gives an excellent account of the emergence and development of differential algebra and the collections of surveys and tutorials [39, 30] show the implications of differential algebra and the work of J. F. Ritt and E. Kolchin with diverse branches of mathematics. In particular the reader shall find the tutorial [68], that was communicated to the author late in the preparation of these notes, complementary to the present one.

Differential algebra is an extension of polynomial algebra aimed at the analysis of systems of ordinary or partial differential equations that are polynomially nonlinear. To a differential equation we associate a differential polynomial and to a differential system we associate a radical differential ideal. Questions about the solution set of the differential system are best expressed in terms of that radical differential ideal. There are differential analogues to the Nullstellensatz, the Hilbert basis theorem and the decomposition into prime ideals. The latter point gives light to the old problem of singular solution of a single differential equation: the radical differential ideal of a single differential polynomial may split into several prime differential ideals. One of those describes the general solution and the others the singular solutions.

Loosely speaking, a triangulation-decomposition algorithm takes as input a system of differential equations and outputs a finite set of differential systems with specific shape and properties. The set of solutions of the original system is equal to the union of the nonsingular solutions of the output systems. The output systems are given by *coherent differential triangular sets* of differential polynomials. The notion of *differential triangular sets* relies on the definition of a ranking that is a total order on the derivatives compatible with derivation. For any ranking, existence and uniqueness of formal power series solutions are secured for coherent differential triangular systems [63] but convergence of these power series depends on the ranking in use [42]. Also, for so called orderly ranking, we can compute the *differential dimension polynomial* [40] of a coherent differential triangular set. It has some resemblance with the Hilbert polynomial and measures the arbitrariness coming into the nonsingular solutions i.e. the number of arbitrary functions. Triangulation-decomposition algorithms also belong to the class of differential elimination algorithm. For a system of differential equations $\Sigma = 0$ and an appropriate choice of ranking we can answer the following typical questions:

- is a differential equation (not apparent in $\Sigma = 0$) satisfied by all the solutions of the system $\Sigma = 0$?
- what are the differential equations satisfied by the solutions of $\Sigma = 0$ in a subset of the dependent variables? If Σ is a differential system in the unknown functions $y_1, \ldots, y_n$, one might be interested in knowing the equations governing the behavior of the component y_1 independently of the others.
- what are the lower order differential equations satisfied by the solutions of $\Sigma = 0$? In particular, one might inquire if the solutions of the system are constrained by purely algebraic equations i.e. differential equations of order zero.
- what are the ordinary differential equations in one of the independent variables satisfied by the solution set of $\Sigma = 0$? If $\Sigma = 0$ is a differential system where $t_1, \ldots, t_m$ are the independent variables, finding the ordinary differential equations in t_1 satisfied by the solutions might be used to solve explicitly the system.

In Section 8 we give examples on how those questions arise in some applications. The reader might want to look at that section for motivation.

All those questions require in fact, a way or another, a membership test to the radical differential ideal generated by the set of differential polynomials Σ. We consider thus that we have a good representation for the radical differential ideal generated by a finite set of differential polynomials if it provides a membership test. We shall seek a representation of that radical differential ideal as an intersection of *characterizable differential ideals*. In practice, characterizable differential ideals are defined by regular differential chains, i.e. a special kind of coherent differential triangular sets, that allow testing membership through *differential reduction*. That final decomposition is called a characteristic decomposition. To compute the characteristic decomposition of the radical differential ideal generated by a finite set of differential polynomials we shall proceed as follow in this paper: First compute a decomposition into differential ideals defined by a regular differential systems, i.e. a system consisting of a coherent differential triangular set of equations and some inequations. Then, a characteristic decomposition of each of the found *regular differential ideals* can be computed by purely algebraic means, i.e. without performing any differentiation [33]. For the decomposition into regular differential ideals we expose the Rosenfeld-Gröbner algorithm by Boulier *et al.* taken from [10]. Other alternatives are the factorization free versions of the algorithm of Ritt and Kolchin [40, IV.9] proposed in [33] and [13]. Rosenfeld-Gröbner is essentially different from those as the splitting scheme owes to the elimination theory of Seidenberg [66]. For the decomposition of regular differential ideals into characterizable differential ideals we apply the pseudo-gcd algorithm of Kalkbrener [37, 34]. There are also known alternatives [33, 11].

Ritt's approach was essentially constructive and already in [58] he gave a triangulation-decomposition algorithm for finitely generated radical differential ideals in the case of ordinary differential equations. The components of the output there were prime differential ideals instead of the wider class of characterizable ideals. Later Ritt gave a triangulation-decomposition algorithm for partial differential equations based on Riquier's notion of passivity [57, 36, 60] and Kolchin gave a triangulation-decomposition algorithm based on Rosenfeld's notion of coherence [61, 40]. Algorithmic aspects of differential algebra have drawn attention again around 1990 in view of applications to theorem proving, control theory, analysis of over determined differential systems and computation of Lie symmetries [74, 46, 27, 55, 56]. For want of effectiveness, the primality of the decomposition that requires factorization in towers of extension was to be removed. A key point for factorization free triangulation-decomposition algorithms was revealed in [9]. It is a new application of a lemma by Rosenfeld [61]. Rosenfeld's lemma establishes a bridge between differential algebra and polynomial algebra through *coherent autoreduced sets* and by generalization through *regular differential systems*, defined in [9]. Gröbner basis approaches to the problem of representation of differential ideals have been studied in [16, 52, 46]. Those approaches have practical interests and theoretical difficulties as *differential Gröbner bases* can be infinite.

This paper is organized as follows.

In Section 2 the fundamental definitions and results in differential algebra are reviewed. We introduce radical differential ideals and their decomposition into prime differential ideals. We state the differential basis theorem and discuss the differential Nullstellensatz. This section is all based on the reference books [60, 40].

In Section 3 we define differential rankings and show that they are well orders. We then define the central objects that are the differential triangular sets and give the algorithm of reduction by them. We also introduce differential characteristic sets.

Section 4 introduces coherence for differential triangular sets and proves Rosenfeld's lemma. Rosenfeld's lemma allows us to lift results about ideals defined by triangular sets in polynomial algebra to results about differential ideals defined by regular differential systems. These are the structure theorems on which effective algorithms rely. They first appeared in [9, 10].

Section 5 introduces characterizable differential ideals and *differential regular chains* as a way of constructing all such differential ideals. We show the fundamental principle that allows to compute a characteristic decomposition of a regular differential ideals by purely algebraic means. This result appeared in [33].

Section 6 presents the Rosenfeld-Gröbner algorithm of [10] to compute a decomposition into differential ideals defined by regular differential systems. The presentation is basically the original one. We nonetheless left out the delicate implementation of the analogue of the second Buchberger criterion.

Section 7 then gives an algorithm based on Kalkbrener's pseudo-gcd to refine the decomposition into a characteristic decomposition.

We give in Section 8 a couple of by now classical examples of applications of differential elimination algorithms. These include solving ordinary differential systems, index reduction of differential-algebraic equations, observability in control theory and symmetry analysis. Small examples computed with the MAPLE *diffalg* package [8] are presented. Many of these applications appeared and were given successful achievements with other algorithms and related software that are cited in the text.

For this paper we take the risk of introducing a new notation for the radical differential ideal generated by a set Σ. The classical notation $\{\Sigma\}$ can indeed induce confusion between sets and radical differential ideals. We suggest the notation $[\![\Sigma]\!]$, given that the differential ideal generated by Σ is $[\Sigma]$.

The algorithms presented are described by pseudo-code in the MAPLE style.

2 Differential algebra

Consider the differential system

$$y_{ss}^2 - 2\,y_t y_{st} = y_t^2 - 1, \quad y_s^2 + y_t^2 = 1$$

where y is a function of s and t and subscripts indicate derivation w.r.t. these variables. The differential system is defined by the *differential polynomials* $p =$

$y_{ss}^2 - 2\, y_t y_{st} - y_t^2 + 1$ and $q = y_s^2 + y_t^2 - 1$. An analytic solution of the system is a common *zero*[1] A common zero of p and q must be a zero of any derivative of p or q and of any linear combination of those. For instance it is a zero of $r = p + q + \delta_s(q) = y_{ss}^2 + 2\, y_s y_{ss} + y_s^2$, where δ_s indicates the derivation according to s. Note that $r = (y_{ss} + y_s)^2$. Therefore a common zero of p and q is a zero of $y_{ss} + y_s$. The set of all the *differential and algebraic consequences* of p and q is the *radical differential ideal* generated by p and q. It has the same zero set as p and q and is in fact the biggest set having this property.

We start by giving the formal definitions and properties of differential rings and differential ideals. We then introduce the ring of differential polynomials together with the fundamental results.

2.1 Differential rings and ideals

All rings $\mathcal{R}$ that we consider are commutative and contain the field $\mathbb{Q}$ of rational numbers. A derivation δ on $\mathcal{R}$ is a map from $\mathcal{R}$ to $\mathcal{R}$ such that for all $a, b \in \mathcal{R}$

$$\delta(a+b) = \delta(a) + \delta(b) \qquad \delta(a\, b) = a\, \delta(b) + \delta(a)\, b$$

Example 2.1. *On the polynomial ring $\mathbb{Q}[s,t]$ we can define the usual derivations $\delta_s = \frac{\partial}{\partial s}$ and $\delta_t = \frac{\partial}{\partial t}$ so that $\delta_s(s) = 1$ and $\delta_s(t) = 0$ and similarly for δ_t. These two derivations commute: $\delta_s\, \delta_t = \delta_t\, \delta_s$. We could also consider the Euler derivations $\bar{\delta}_s = s\, \frac{\partial}{\partial s}$ and $\bar{\delta}_t = t\, \frac{\partial}{\partial t}$ so that $\bar{\delta}_s(s) = s$, $\bar{\delta}_s(t) = 0$ and similarly for $\bar{\delta}_t$. For all examples in this paper we consider the usual derivations δ_s and δ_t. They extend uniquely to $\mathbb{Q}(s,t)$.*

Let $\Delta = \{\delta_1, \ldots, \delta_m\}$ be a set of pairwise commuting derivations on a ring $\mathcal{R}$ that are linearly independent over $\mathcal{R}$. We note Θ the free commutative monoid with a unit generated by Δ. An element θ of Θ is a *derivation operator*. It can be written $\theta = \delta_1^{e_1} \ldots \delta_m^{e_m}$ for some $(e_1, \ldots, e_m) \in \mathbb{N}^m$. Its *order* is then $\mathrm{ord}(\theta) = e_1 + \ldots + e_m$. The only derivation operator of order zero is the identity. We note Θ_r, $r \in \mathbb{N}$, the set of derivation operators of order r or lower and Θ^+ the set of derivation operators of positive order.

Endowed with a set Δ of commuting derivations, a ring (or a field) $\mathcal{R}$ becomes a *differential ring* (or a *differential field*). An element c of $\mathcal{R}$ is a *constant* if $\delta c = 0$ for all $\delta \in \Delta$. When Δ consists of a single derivation δ we speak of an ordinary differential ring. If Δ has more than one element we have a partial differential ring. From now on we shall speak of differential ring assuming that the set $\Delta = \{\delta_1, \ldots, \delta_m\}$ of derivations has been fixed.

In a differential ring $\mathcal{R}$, an ideal I of $\mathcal{R}$ is a *differential ideal* if it is stable under derivation, that is $\delta(a) \in I$, for all $a \in I$ and $\delta \in \Delta$. A differential ideal I is radical if $a^e \in I$, for $e \in \mathbb{N} \setminus \{0\}$, implies $a \in I$. It is prime if whenever a product ab belongs to I at least one of the factor, a or b, belongs to I.

[1] A precise definition of zero will appear later. It is nonetheless appropriate to think analytic or meromorphic solution of the associated system when one reads zero of a set of polynomial.

Given a set of elements Σ in a differential ring $\mathcal{R}$, we note $[\Sigma]$ the differential ideal generated by Σ i.e. the intersection of all the differential ideals containing Σ. $[\Sigma]$ is in fact the ideal generated by the elements of Σ together with all their derivatives: $[\Sigma] = (\Theta\Sigma)$. $\llbracket\Sigma\rrbracket$ denotes the radical differential ideal generated by Σ, i.e. the intersection of all radical differential ideals containing Σ. Because we assumed that $\mathbb{Q} \subset \mathcal{R}$, $\llbracket\Sigma\rrbracket$ is the radical of $[\Sigma]$ i.e. the set $\{q \in \mathcal{R} \mid \exists e \in \mathbb{N},\ q^e \in [\Sigma]\}$.

Let H be a subset of $\mathcal{R}$. We denote by H^∞ the minimal subset of $\mathcal{R}$ that contains 1 and H and is stable by multiplication and division i.e. $a, b \in H^\infty \Leftrightarrow ab \in H^\infty$. When H consists of a unique element h we write h^∞ instead of $\{h\}^\infty$. For a differential ideal I we define the *saturation* of I by a subset H of $\mathcal{R}$ as $I : H^\infty = \{q \in \mathcal{R} \mid \exists\, h \in H^\infty \text{ s.t. } h\, q \in I\}$. $I \subset I : H^\infty$ and $I : H^\infty$ is easily seen to be a differential ideal with Proposition 2.2 below. If I is a prime differential ideal $I : H^\infty$ is either equal to I or $\mathcal{F}\llbracket Y\rrbracket$ according to whether $H \cap I$ is empty or not.

PROPOSITION 2.2. *Let a, b be elements of the differential ring $\mathcal{R}$. For any $\theta \in \Theta_e$, $a^{e+1}\,\theta b$ belongs to the ideal generated by the set $\{\psi(a\,b) | \psi \in \Theta, \psi$ divides $\theta\}$.*

Thus $a^{e+1}\,\theta(b) \in [a\,b]$, for all $\theta \in \Theta_e$ and $\phi(a)\psi(b) \in \llbracket ab\rrbracket$, for all $\phi, \psi \in \Theta$.

Proof. This is trivially true if $\mathrm{ord}(\theta) = 0$. Assume the property is true for all θ of order e or less. Let θ be a derivation operator of order $e+1$. We can write $\theta = \delta\bar{\theta}$ for some $\delta \in \Delta$ and $\bar{\theta} \in \Theta_e$. By induction hypothesis $a^{e+1}\bar{\theta}(b) = \sum_{\psi|\bar{\theta}} \alpha_\psi \psi(a\,b)$ for some $\alpha_\psi \in \mathcal{R}$. Thus

$$\begin{aligned} a^{e+2}\delta\bar{\theta}(b) &= a\left(\delta\left(a^{e+1}\bar{\theta}(b)\right) - (e+1)a^e\delta(a)\bar{\theta}(b)\right) \\ &= a\sum_{\psi|\bar{\theta}} \left(\delta(\alpha_\psi)\psi(a\,b) + \alpha_\psi\delta\psi(ab)\right) - (e+1)\delta(a)\sum_{\psi|\bar{\theta}} \alpha_\psi\psi(a\,b). \end{aligned}$$

The conclusion follows.

2.2 Differential polynomial rings

Let $\mathcal{F}$ be a differential field for the derivations $\Delta = \{\delta_1, \ldots, \delta_m\}$. It is assumed that $\mathcal{F}$ contains $\mathbb{Q}$. Given a set of *differential indeterminates* $Y = \{y_1, \ldots, y_n\}$, we construct the ring of *differential polynomials*, $\mathcal{F}\llbracket Y\rrbracket$ that is a ring in the infinitely many variables $\Theta Y = \{\theta y,\ y \in Y,\ \theta \in \Theta\}$ called the *derivatives*. This is naturally a differential ring for Δ. A differential polynomial p corresponds to a differential equation $p = 0$.

EXAMPLE 2.3. *The ordinary differential equation $y'^2 - t\,y' + y = 0$ is modeled by the differential polynomial $q = (\delta_t y)^2 - t\,\delta_t y + y$ in the ordinary differential polynomial ring $\mathbb{Q}(t)\llbracket y\rrbracket$ where the derivation on $\mathbb{Q}(t)$ is the usual one, i.e. $\delta_t = \frac{\mathrm{d}}{\mathrm{d}t}$.*

Let us now look at a partial differential ring. Consider $\mathcal{F} = \mathbb{Q}(s,t)$ endowed with the derivations δ_s and δ_t of the previous example and $Y = \{y\}$. The differential polynomial $p = \delta_s y\,\delta_t y + s\,\delta_s y + t\,\delta_t y - y$ represent the differential equation

$y_s\, y_t + s\, y_s + t\, y_s - y = 0$ where we took the standard notation $y_s = \frac{\partial y}{\partial s}$, $y_t = \frac{\partial y}{\partial t}$. In the examples we shall in fact use this notation for differential polynomials so that p shall be written $y_s\, y_t + s\, y_s + t\, y_s - y$.

The analogue of the Hilbert basis theorem for polynomial rings is given by the basis or Ritt-Raudenbush theorem. The most general proof is given in [40]. The proof for ordinary differential ring is given in [60, 38].

Theorem 2.4. *If J is any radical differential ideal in $\mathcal{F}\,[\![Y]\!]$ there exists a finite subset Σ of $\mathcal{F}\,[\![Y]\!]$ s.t. $J = [\![\Sigma]\!]$.*

This is equivalent to the fact that any increasing sequence of radical differential ideals is stationary. The result does not hold for differential ideals.

Theorem 2.5. *Any radical differential ideal J in $\mathcal{F}\,[\![Y]\!]$ is the intersection of a finite number of prime differential ideals. When minimal, this decomposition is unique.*

The decomposition is minimal if none of the components contains another one. The prime differential ideals coming into the minimal decomposition are called the *essential prime components* of J.

A n-tuple $\xi = (\xi_1, \ldots, \xi_n)$ with components in a differential field extension $\mathcal{F}'$ of $\mathcal{F}$ is a zero of a differential polynomial $p \in \mathcal{F}\,[\![y_1, \ldots, y_n]\!]$ if p vanishes when we replace the y_i by the ξ_i.

Example 2.6. *We considered in Example 2.3 the differential polynomial $p = {y_t}^2 - t\, y_t + y$ in $\mathbb{Q}(t)\,[\![y]\!]$. The elements $\frac{1}{4}t^2$ and $a(t-a)$ of $\mathbb{Q}(a,t)$, where a is any constant (it could be transcendental), are zeros of p. In a matching way, the minimal prime decomposition of $[\![p]\!]$ is given by*

$$[\![p]\!] = [\![p, y_{tt}]\!] \cap [\![4\, y - t^2]\!]\,.$$

The zero of the second component has to be $\frac{1}{4}\, t^2$. The other zero, $a\,(t-a)$, is a zero of the first component.

A zero of a differential polynomial is also a zero of any of its derivatives. If ξ is a common zero to a set of differential polynomials Σ, it is a zero of any linear combination over $\mathcal{F}\,[\![Y]\!]$ of the elements of Σ and their derivatives. This amounts to say that ξ is a zero of $[\Sigma]$. One can see it is also a zero of $[\![\Sigma]\!]$ since any element q of $[\![\Sigma]\!]$ is such that $q^e \in [\Sigma]$ for some $e \in \mathbb{N} \setminus \{0\}$. One can inquire if there is a bigger set in $\mathcal{F}\,[\![Y]\!]$ that admits the same zeros as Σ. The answer is given by the differential Nullstellensatz.

To any prime differential ideal P we can associate the differential field that is the quotient field of the integral differential ring $\mathcal{F}\,[\![Y]\!]\,/P$. The canonical image of $(y_1, \ldots, y_n)$ on that field is a zero of P. It is in fact a *generic zero*, i.e. every differential polynomial that vanishes on that zero belongs to P. If P contains $[\![\Sigma]\!]$, that image is also a zero of $[\![\Sigma]\!]$. That abstract construction of zeros allows us to state the differential Nullstellensatz, known also as the theorem of zeros.

THEOREM 2.7. *Let Σ be a subset of $\mathcal{F}[\![Y]\!]$.*

- *Σ admits a zero iff $1 \notin [\![\Sigma]\!]$*
- *a differential polynomial of $\mathcal{F}[\![Y]\!]$ vanishes on all the zeros of Σ iff it belongs to $[\![\Sigma]\!]$.*

Indeed, if $g \in \mathcal{F}[\![Y]\!]$ vanishes on all zeros of Σ it must vanish in particular on the generic zeros of the essential prime components of $[\![\Sigma]\!]$ and therefore it belongs to $[\![\Sigma]\!]$. In addition to this abstract setting, Ritt details the *analytic case*, i.e. the case where $\mathcal{F}$ is a field of meromorphic functions in a region. If g does not belong to a prime differential ideal P, an analytic zero of P can be constructed so that it does not make g vanish. In the partial differential case, this relies on the Riquier's existence theorem [57].

Instead of trying to study directly the solutions of the differential system $\Sigma = 0$ we shall inspect $[\![\Sigma]\!]$. Our goal is to give an adequate representation of $[\![\Sigma]\!]$. This representation shall allow us to test membership to $[\![\Sigma]\!]$ and to answer question about the zero set of Σ.

We shall discuss now systems of equations and inequations like $\Sigma = 0, H \neq 0$ where Σ and H are two finite but non empty set of differential polynomials. Its best differential ideal representation is $[\![\Sigma]\!]:H^\infty$. Let us note $\mathcal{Z}(\Sigma/H)$ the subset of the zeros of Σ that are not zeros of any element of H. A differential polynomial p vanishes on $\mathcal{Z}(\Sigma/H)$ iff $p \in [\![\Sigma]\!]:H^\infty$. Indeed, if h is the product the element of H then $h\,p$ vanishes on all the zeros of Σ so that $h\,p \in [\![\Sigma]\!]$. Note that if J is a radical differential ideal of $\mathcal{F}[\![Y]\!]$, $J:H^\infty$ is the intersection of the essential prime components of J that have an empty intersection with H. The generic zeros of the essential components of $[\![\Sigma]\!]:H^\infty$ are elements of $\mathcal{Z}(\Sigma/H)$. Note nonetheless that a zero of $[\![\Sigma]\!]:H^\infty$ can make a zero of an element of H. In the ordinary and analytic case, Ritt proves that those zeros are *adherent* to $\mathcal{Z}(\Sigma/H)$ [60].

EXAMPLE 2.8. *In the ordinary differential polynomial ring $\mathbb{Q}(t)[\![y]\!]$, consider the differential polynomial $p = y_t^2 - 4\,y^3$. The common zero to p and $h = y_t$ is $\xi = 0$. You can nonetheless show [59] that $[\![p]\!]:h^\infty = [\![p]\!]$ so that $\xi = 0$ is a zero of $[\![p]\!]:h^\infty$.* A general zero *of p is given by $\frac{c^2}{(c\,t-1)^2}$ so that 0 is analytically embedded in a family of zeros of p for which h does not vanish.*

3 The tools for algorithms

This section defines the objects we manipulate for algorithms. We introduce differential rankings that are orders on the derivatives that are compatible with derivations. They provide well orders. Then it is possible to define consistently leaders and differential triangular sets in an analogous way to what is done in the polynomial case [34]. We give a reduction algorithm by differential triangular sets. A differential ranking induces a pre-order on differential triangular set and this allows to define differential characteristic set and prove their existence. We introduce all these concepts to set up algorithms. These tools are nonetheless fundamental in showing the Ritt-Raudenbush theorem of previous section.

In polynomial algebra, ideals defined by triangular sets have good structural properties. In differential algebra this happens if we add a condition, namely *coherence*. This is studied in next section.

In this section, and the following, we have a fixed differential polynomial ring $\mathcal{F}[\![Y]\!] = \mathcal{F}[\![y_1, \ldots, y_n]\!]$ with derivations $\Delta = \{\delta_1, \ldots, \delta_m\}$. The set of derivation operators is denoted Θ.

3.1 Differential ranking

DEFINITION 3.1. *A* differential ranking*, or d-ranking, on a set of differential indeterminates Y is a total order on the set of derivatives ΘY that satisfies for all $u, v \in \Theta Y$ and all $\delta \in \Delta$ the two conditions*

$$u \leq \delta u, \qquad u \leq v \;\Rightarrow\; \delta u \leq \delta v$$

This of course implies that for any $\theta \in \Theta$ we have $u \leq \theta u$ and $u \leq v \;\Rightarrow\; \theta u \leq \theta v$. If $Y = \{y_1, \ldots, y_n\}$ and the derivations are $\Delta = \{\delta_1, \ldots, \delta_m\}$, any derivative of ΘY can be written as $\delta_1^{e_1} \ldots \delta_m^{e_m} y_i$ and is thus determined by a $(m+1)$-tuple $(i, e_1, \ldots, e_m)$ in $\mathbb{N}_n \times \mathbb{N}^m$, where $\mathbb{N}_n = \{1, \ldots, n\}$. Consequently, a d-ranking is a total order on $\mathbb{N}_n \times \mathbb{N}^m$ that satisfies for any $i, j \in \mathbb{N}_n$ and $e, f, g \in \mathbb{N}^m$ $(i, e) \leq (i, e+g)$ and $(i, e) \leq (j, f) \;\Rightarrow\; (i, e+g) \leq (j, f+g)$. The restriction of this order to $\{i\} \times \mathbb{N}^m$, for some $i \in \mathbb{N}_n$, is an extension of the direct product order on $\mathbb{N}^m$. Conversely, if there is a single differential indeterminate y, any order on $\mathbb{N}^m$ that is an extension of the direct product order of $\mathbb{N}^m$, noted $\preceq_{\mathbb{N}^m}$, provides a d-ranking in a natural way. Recall that a relation on a set M is well founded if every non empty subset of M has a minimal element for this relation. This is equivalent to the fact that there is no infinite decreasing sequence in M. See for instance [5, Chapter 4]. A well founded order is a well-order.

PROPOSITION 3.2. *A d-ranking is a well order.*

The essential ingredients for that is the first defining property of a d-ranking and Dickson's lemma.

Proof. Assume we have an infinite decreasing sequence of derivatives in ΘY. Since Y is finite, we can extract from it an infinite subsequence of derivatives $\{\theta_k y\}_{k \in \mathbb{N}}$ of a single differential indeterminate $y \in Y$ that is strictly decreasing. The infinite sequence $\{\theta_k y\}_{k \in \mathbb{N}}$ can be viewed as an infinite sequence of $\mathbb{N}^m$. By Dickson's lemma [5, Corollary 4.48], there exists a subsequence $\{\theta_{k_i} y\}_{i \in \mathbb{N}}$ such that $\theta_{k_i} y \preceq_{\mathbb{N}^m} \theta_{k_j} y$ for all $i < j$. This implies that $\theta_{k_i} y \leq \theta_{k_j} y$ for all $i < j$. This contradicts our assumption that the original sequence is strictly decreasing.

Study and classification of d-rankings are examined in [17, 62]. We introduce here only the most commonly used d-rankings. In Section 8 we shall see that a d-ranking is chosen according to the kind of properties on the solution set of a differential system we want to exhibit. A d-ranking is *orderly* if it satisfies $\psi y < \phi x$, for $x, y \in Y$ and $\phi, \psi \in \Theta$, as soon as the order of ϕ is greater that the order of ψ. Let Z be a subset of Y. A d-ranking on Y *eliminates* Z if $\phi y < \psi z$ for any $y \in Y \setminus Z$, $z \in Z$, $\psi, \phi \in \Theta$. We write $Y \setminus Z \ll Z$. A pure elimination d-ranking is such that $y_{\sigma(1)} \ll y_{\sigma(2)} \ll \ldots \ll y_{\sigma(n)}$ for some permutation σ of $\mathbb{N}_n$.

EXAMPLE 3.3. *Consider an ordinary differential polynomial ring* $\mathbb{Q}(t)\,[\![Y]\!]$, *with derivation* δ_t. *If there is a single differential indeterminate,* $Y = \{y\}$, *there is only one possible d-ranking:* $y < y_t < y_{tt} < \ldots$. *If* $Y = \{y, z\}$, *an orderly d-ranking is given by* $y < z < y_t < z_t < y_{tt} < \ldots$. *An elimination d-ranking is given by* $y < y_t < y_{tt} < \ldots < z < z_t < z_{tt} < \ldots$.

EXAMPLE 3.4. *Assume we have two derivations,* δ_s *and* δ_t, *and a single differential indeterminate* $Y = \{y\}$. *The lexicographic order on* $\mathbb{N}^2$ *induces the d-ranking* $y < y_s < y_{ss} < \ldots < y_t < y_{st} < y_{sst} < \ldots$. *An example of orderly d-ranking is:* $y < y_s < y_t < y_{ss} < y_{st} < y_{tt} < \ldots$.

From now on, when we speak of the differential polynomial ring $\mathcal{F}\,[\![Y]\!]$ we assume that we are given a differential ranking on Y. For $u \in \Theta Y$, we note $\Theta Y_{<u}$ the set of derivatives that rank lower than u. Similarly $\Theta Y_{\leq u}$ denotes the set of derivatives that are equal to or lower than u. These sets are finite when we have an orderly ranking but this needs not be the case for other d-rankings.

Let p be a differential polynomial of $\mathcal{F}\,[\![Y]\!]$ that is not in $\mathcal{F}$. The *leader* and the *initial* of p are respectively the highest ranking derivative appearing in p and the coefficient of its highest power in p. We shall denote them as $\mathsf{lead}(p)$ and $\mathsf{init}(p)$ respectively. The *separant* of p is the formal derivative of p w.r.t. its leader, i.e. $\frac{\partial p}{\partial \mathsf{lead}(p)}$. It is denoted by $\mathsf{sep}(p)$.

If we take here $u = \mathsf{lead}(p)$ we can write

$$p = a_d\, u^d + a_{d-1}\, u^{d-1} + \cdots + a_0,$$

where $a_i \in \mathcal{F}[\Theta Y_{<u}]$, $a_d \neq 0$. Then $\mathsf{init}(p) = a_d$ and $\mathsf{sep}(p) = d\, a_d\, u^{d-1} + (d-1)\, a_{d-1} u^{d-2} + \cdots + a_1$. We define furthermore the *rank* of p, $\mathsf{rank}(p)$, to be the term u^d and $\mathsf{tail}(p) = p - \mathsf{init}(p)\mathsf{rank}(p)$ that is $a_{d-1}\, u^{d-1} + \cdots + a_0$ in the above write up.

For $\delta \in \Delta$, the derivatives appearing in $\delta(p)$ consists of derivatives v appearing in p and of their derivatives δv. The second defining property of d-ranking allows us thus to state that $\delta \mathsf{lead}(p) = \mathsf{lead}(\delta p)$ for any $\delta \in \Delta$. Furthermore, from the definition of the separant, we can write

$$\delta(p) = \mathsf{sep}(p)\, \delta(\mathsf{lead}(p)) + \sum_{v \in \Theta Y} \frac{\partial p}{\partial v}\, \delta v.$$

Thus $\delta(p)$ has degree one in its leader, $\delta(\mathsf{lead}(p))$ and $\mathsf{sep}(p)$ is the initial of $\delta(p)$. By induction, for any $\theta \in \Theta^+$, $\theta \mathsf{lead}(p)$ and $\mathsf{sep}(p)$ are respectively the leader and the initial of θp and θp has degree one in $\theta \mathsf{lead}(p)$.

For two elements $p, q \in \mathcal{F}\,[\![Y]\!]$, we say that p has higher rank (or ranks higher) than q, and write $\mathsf{rank}(q) < \mathsf{rank}(p)$, if either

- $q \in \mathcal{F}$ and $p \notin \mathcal{F}$
- $\mathsf{lead}(q)$ ranks lower than $\mathsf{lead}(p)$
- $\mathsf{lead}(q) = \mathsf{lead}(p) = u$ and $\deg(q, u) < \deg(p, u)$.

The d-ranking on the differential indeterminates thus induces a pre-order[2] on $\mathcal{F}[\![Y]\!]$.

A differential polynomial q is *partially reduced* w.r.t. p if no proper derivative of $\mathsf{lead}(p)$ appears in q; q is *reduced w.r.t.* p if q is partially reduced w.r.t. to p and the degree of q in $\mathsf{lead}(p)$ is strictly less than the degree of p in $\mathsf{lead}(p)$.

EXAMPLE 3.5. *In $\mathbb{Q}(s,t)\{y\}$ endowed with a d-ranking such that $y < y_s < y_t < y_{ss} < y_{st} < y_{tt}$,*

- *$q = y_{ss} - y_t$ is partially reduced with respect to $p = y_{tt} + y_s$ but not w.r.t. $p_2 = y_s + y$*
- *$q = (y_t)^3 + y_s$ is partially reduced w.r.t. $p = y_t^2 + y_s^2$ but not reduced.*

Let F be a finite subset of $\mathcal{F}[\![Y]\!]$ and u a derivative of ΘY. We note ΘF the set of differential polynomials consisting of the element of F together with all their derivatives. $\Theta F_{<u}$ (respectively $\Theta F_{\leq u}$) denotes the set consisting of all elements of F together with all their derivatives the leaders of which are of lower (respectively lower or equal) rank than u. In other words $\Theta F_{<u} = \Theta F \cap \mathcal{F}[\Theta Y_{<u}]$ and $\Theta F_{\leq u} = \Theta F \cap \mathcal{F}[\Theta Y_{\leq u}]$. $\Theta F_{<u}$ and $\Theta F_{\leq u}$ need not be finite. The following property follows directly from Proposition 2.2.

PROPOSITION 3.6. *Let F and H be finite subsets of $\mathcal{F}[\![Y]\!]$ and $u \in \Theta Y$. If $p \in (\Theta F_{<u}) : H^\infty$ then $\theta p \in (\Theta F_{<\theta u}) : H^\infty$ for any $\theta \in \Theta$.*

3.2 Differential triangular sets and differential reduction

In the ordinary differential case and w.r.t to an elimination ranking, the *chains* of [60] coincide with the *autoreduced set* of [40]. The *differential chains* defined here are slightly less restrictive but still allow to give the Ritt-Kolchin definition and properties of *characteristic set* of differential ideals. An intermediate step in defining differential chains is the notion of *differential triangular sets* from [9] and reduction by these. In the algorithm of Section 6 the additional notion of *weak differential triangular set* arises.

DEFINITION 3.7. *A subset A of $\mathcal{F}[\![Y]\!]$ is a* weak differential triangular set, *if*

- *no element of A belongs to $\mathcal{F}$*
- *for any two distinct elements a, b of A $\mathsf{lead}(a)$ is not a derivative of $\mathsf{lead}(b)$.*

It is a differential triangular set, *or d-triangular set for short, if furthermore any element of A is partially reduced w.r.t. the other ones.*

It is an autoreduced set *if no element of A belongs to $\mathcal{F}$ and each element of A is reduced w.r.t. all the others.*

[2] We take the convention that a pre-order is a relation that is reflexive, transitive and connex. Therefore the difference with an order is that $a \leq b$ and $b \leq a$ does not imply $a = b$.

An autoreduced set is a (weak) d-triangular set.

EXAMPLE 3.8. *With the d-ranking* $y < y_s < y_t < y_{ss} < y_{st} < y_{tt} < \ldots$ *the subset* $\{y_{tt} - y_{ss}^2, y_s - y\}$ *is a weak d-triangular,* $\{y_{tt} - y_s^2, y_s - y\}$ *is a d-triangular set and* $\{y_{tt}, y_s\}$ *is an autoreduced set.*

PROPOSITION 3.9. *A weak d-triangular set is finite.*

Proof. This is of course another application of Dickson's lemma. Assume for contradiction that a weak d-triangular set is infinite. Take $\{u_l\}_{l\in\mathbb{N}}$ the sequence of the leaders of this infinite weak d-triangular set. Since Y is finite, there must be an infinite subsequence $\{u_{l_k}\}_{k\in\mathbb{N}}$ such that $u_{l_k} = \theta_k y$ for a $y \in Y$. $\{\theta_k y\}_{k\in\mathbb{N}}$ can be viewed as an infinite sequence of $\mathbb{N}^m$. By Dickson's lemma, there exists a subsequence $\{\theta_{k_i} y\}_{i\in\mathbb{N}}$ such that $\theta_{k_i} y \preceq_{\mathbb{N}^m} \theta_{k_j} y$ for all $i < j$. This means that $\theta_{k_j} y$ is a derivative of $\theta_{k_i} y$. This contradicts the definition.

Let $a_1, a_2, \ldots, a_r$ be the elements of a weak d-triangular set A indexed such that $\mathsf{lead}(a_1) < \mathsf{lead}(a_2) < \ldots < \mathsf{lead}(a_r)$. We write $A = a_1 \vartriangle a_2 \vartriangle \ldots \vartriangle a_r$. We can also use the $\vartriangle$ notation to construct weak d-triangular sets by mixing differential polynomials a and weak d-triangular sets A, B in the following ways: $a \vartriangle A$ (respectively $A \vartriangle a$) denotes the weak d-triangular set $A \cup \{a\}$ if the leader of a ranks lower (respectively higher) than the leader of any element of A; $A \vartriangle B$ denotes the weak d-triangular set $A \cup B$ if the leader of any element of A ranks lower than the leader of any element of B and $A \cup B$ forms a weak d-triangular set.

We denote $\mathfrak{L}(A) = \mathsf{lead}(A)$, $I_A = \mathsf{init}(A)$ and $S_A = \mathsf{sep}(A)$ the sets of leaders, initials and separants of the elements of A. Also $H_A = I_A \cup S_A$ is the set of the initials and the separants of A.

For $u \in \mathfrak{L}(A)$, A_u denotes the element of A having u as leader. For $u \in \Theta Y$, $A_{<u}$ (respectively $A_{\leq u}$) denotes the elements of A with leader ranking lower than u (respectively lower or equal to u). $A_{>u}$ denotes the elements of A with leader ranking higher than u. $A_{<u}$ and $A_{\leq u}$ do not include any derivative of the elements of A contrary to $\Theta A_{<u} = \Theta A \cap \mathcal{F}[\Theta Y_{<u}]$ and $\Theta A_{\leq u} = \Theta A \cap \mathcal{F}[\Theta Y_{\leq u}]$. Note that $\Theta A_{<u}$ and $\Theta A_{\leq u}$ need not be finite nor triangular.

EXAMPLE 3.10. *In* $\mathbb{Q}(s,t)\llbracket y \rrbracket$ *endowed with the d-ranking s.t.* $y < y_s < y_t < y_{ss} < y_{tt} < \ldots$ *consider the d-triangular set* $A = y_s - sy \vartriangle y_t + y$. *Then* $\Theta A_{\leq y_{tt}} = \{y_s - sy, y_t + y, y_{ss} - sy_s - y, y_{st} - sy_t, y_{st} + y_s, y_{tt} + y_t\}$.

When A is the empty set we take the convention that $[A] = \llbracket A \rrbracket = [0]$.

A differential polynomial is said to be (partially) reduced w.r.t. a weak d-triangular set A when it is (partially) reduced w.r.t. each element of A. Given an element $q \in \mathcal{F}\llbracket Y \rrbracket$ we can compute $s \in S_A^\infty$ and $\mathsf{pd\text{-}red}(q, A)$ that is partially reduced w.r.t. A such that $s\,q \equiv \mathsf{pd\text{-}red}(q, A) \mod [A]$. Similarly, we can compute $h \in H_A^\infty$ and $\mathsf{d\text{-}red}(q, A)$ that is reduced w.r.t. A such that $h\,q \equiv \mathsf{d\text{-}red}(q, A)$ mod $[A]$. We give examples of algorithms for differential reduction and partial differential reduction. In the partial differential case, it is neither enough to reduce successively by the elements of A starting with the highest ranking one nor starting with the lowest ranking one. This is illustrated in the next example.

EXAMPLE 3.11. *In $\mathbb{Q}(s,t)\{y\}$ endowed with the ranking $y < y_s < y_t < y_{ss} < y_{st} < y_{tt} < \ldots$ consider the differential polynomials $a_1 = y_{ss} - y_t$, $a_2 = y_t^2 - y_s$, $p = y_{st}$ and $q = y_{sss}$. $A = a_1 \vartriangle a_2$ is an autoreduced set. On the one hand $\mathsf{d\text{-}red}(p, a_2) = p$ and $\mathsf{d\text{-}red}(p, a_1) = y_{ss}$ that is not reduced w.r.t. A. On the other hand $\mathsf{d\text{-}red}(q, a_1) = q$ and $\mathsf{d\text{-}red}(q, a_2) = y_{st}$ that is not reduced w.r.t. A.*

ALGORITHM 3.12. **pd-red** .
INPUT: *$q \in \mathcal{F}[\![Y]\!]$, A a weak d-triangular set of $\mathcal{F}[\![Y]\!]$.*
OUTPUT: *$\bar{q} \in \mathcal{F}[\![Y]\!]$ s.t.*
- *$\bar{q}$ is partially reduced w.r.t. A*
- *$\exists s \in S_A^\infty$ s.t. $s\,q \equiv \bar{q} \mod (\Theta A_{\leq u})$ where $u = \mathsf{lead}(q)$*
- *$\mathsf{rank}(\bar{q}) \leq \mathsf{rank}(q)$*

$\bar{q} := q$;
while $\bar{q}$ is not partially reduced w.r.t. A do
  $v :=$ the highest ranking element of $\Theta^+\mathfrak{L}(A)$ that appears in $\bar{q}$.
  $a :=$ any element of $\{b \in A \mid v$ is a derivative of $\mathsf{lead}(b)\}$;
  $\theta :=$ the element of Θ s.t. $\theta\,\mathsf{lead}(a) = v$;
  $\tilde{q} := \mathsf{srem}(\bar{q}, \theta a, v)$;
  $\bar{q} := \tilde{q}$;
od;
return($\bar{q}$);

Contrary to the algorithm proposed in [40, I.9], this algorithm taken from [10] is not completely deterministic in the sense that at each step there may be a choice among the elements of A by which one can reduce. This freedom is an advantage in the sense we can make criteria to choose elements with lower degree or smaller coefficients in order to limit expression swell.

By definition of weak d-triangular sets, $\Theta^+\mathfrak{L}(A) \cap \mathfrak{L}(A) = \emptyset$. Therefore θ needs to be in Θ^+. Consequently θa is of degree one in v with initial $\mathsf{sep}(a)$. The pseudo-division relationship obtained is $\tilde{s}\bar{q} \equiv \tilde{q} \mod (\theta a)$ for some $\tilde{s} \in \mathsf{sep}(a)^\infty$. Furthermore $\tilde{q}$ is free of v, and the derivatives appearing in $\tilde{q}$ consist of derivatives that were in $\bar{q}$ or derivatives lower than v. The highest ranking element of $\Theta^+\mathsf{lead}(A)$ that appears in $\tilde{q}$ is of lower rank than v. The sequence of the v's appearing in the while loop is thus strictly decreasing. In virtue of Proposition 3.2, the algorithm terminates. Note that the first v to be selected has to rank lower than $u = \mathsf{lead}(p)$. Thus the differential polynomials used for pseudo-division belong to $\Theta A_{\leq u}$. The final relationship $s\,q \equiv \bar{q} \mod (\Theta A_{\leq u})$, for some $s \in S_A^\infty$, follows from the intermediate pseudo-division relationships.

The algorithm to compute a full reduction is no different. For a derivative $u \in \Theta Y$ occurring in $\bar{q}$, we shall say that the differential polynomial $\bar{q} \in \mathcal{F}[\![Y]\!]$ is reduced w.r.t. A at u if u is not a proper derivative of an element of $\mathfrak{L}(A)$ or, if u belongs to $\mathfrak{L}(A)$, the degree of q in u is lower than the degree of A_u in u.

ALGORITHM 3.13. **d-red** .
INPUT: *$q \in \mathcal{F}[\![Y]\!]$, A a weak d-triangular set of $\mathcal{F}[\![Y]\!]$.*
OUTPUT: *$\bar{q} \in \mathcal{F}[\![Y]\!]$ s.t.*

– $\bar{q}$ *reduced w.r.t.* A
– $\exists h \in H_A^\infty$ *s.t.* $h\, q \equiv \bar{q} \mod (\Theta A_{\leq u})$ *where* $u = \mathit{lead}(q)$
– $\mathit{rank}(\bar{q}) \leq \mathit{rank}(q)$

$\bar{q}$:= q;
while $\bar{q}$ *is not reduced w.r.t.* A *do*
  v := *the highest ranking derivative* $u \in \Theta\mathfrak{L}(A)$ *in* $\bar{q}$ *s.t.* $\bar{q}$ *is not reduced w.r.t.* A *at* u;
  a := *any element of* $\{b \in A \mid v$ *is a derivative of* $\mathit{lead}(b)\}$;
  θ := *the element of* Θ *s.t.* $\theta\, \mathit{lead}(a) = v$;
  $\tilde{q} := \mathit{srem}(\bar{q}, \theta a, v)$;
  $\bar{q} := \tilde{q}$;
od;
return($\bar{q}$*);*

The full reduction algorithm of [40, I.9] by an autoreduced set first proceed by a partial reduction then an algebraic reduction. That strategy is not possible when we reduce by a weak d-triangular set.

Note that $\tilde{q}$ is reduced w.r.t. to A at v and that the other derivatives appearing in $\tilde{q}$ consist of derivatives that were in $\bar{q}$ or derivatives lower than v. The sequence of the v's appearing in the while loop is therefore strictly decreasing and thus the algorithm terminates (Proposition 3.2). According to whether $v \in \mathsf{lead}(A)$ or $v \in \Theta^+\mathsf{lead}(A)$, we have a pseudo-division relationship $\tilde{h}\bar{q} \equiv \tilde{q} \mod (\theta a)$, where $h \in \mathsf{sep}(a)^\infty$ or $h \in \mathsf{init}(a)^\infty$. The final relationship $h\, q \equiv \bar{q} \mod [A]$, for some $h \in H_A^\infty$ follows from these intermediate pseudo-division relationships.

3.3 Differential characteristic sets

In order to introduce and show the existence of differential characteristic sets we define a pre-order on d-triangular sets. This pre-order is also of use in proving the termination of algorithms.

Definition 3.14. *Let* $A = a_0 \vartriangle \ldots \vartriangle a_r$ *and* $B = b_0 \vartriangle \ldots \vartriangle b_s$ *be two weak d-triangular sets. We say that* A *has lower rank than* B *and write* $\mathit{rank}(A) < \mathit{rank}(B)$ *if there exists* k, $0 \leq k \leq r, s$, *such that* $\mathit{rank}(a_i) = \mathit{rank}(b_i)$ *for all* $1 \leq i \leq k$ *and either* $k = s < r$ *or* $\mathit{rank}(a_k) < \mathit{rank}(b_k)$.

If $A = B \vartriangle C$ then $\mathsf{rank}(A) < \mathsf{rank}(B)$ reflecting the inclusion of differential ideals $[B] \subset [A]$. In particular, if B is the empty set and A is not then $\mathsf{rank}(A) < \mathsf{rank}(B)$.

Proposition 3.15. *The pre-order on weak d-triangular set is well-founded.*

Proof. Assume we have an infinite sequence of weak d-triangular sets $\{A_j\}_{j\in\mathbb{N}}$ that is strictly decreasing. We shall construct from it an infinite autoreduced set of derivatives. Since this is not possible by Proposition 3.9, the result is proved by contradiction.

Let $a_j^{(1)}$ be the element of lowest rank in A_j. The sequence $\{\mathsf{rank}(a_j^{(1)})\}_{j\in\mathbb{N}}$ is decreasing and thus must be stationary after a certain $j_1 \in \mathbb{N}$. Let $u_1 = \mathsf{lead}(a_j^{(1)}) = u_1$ for $j \geq j_1$. For $j > j_1$, A_j must have at least two elements. Let $a_j^{(2)}$ be the second lowest ranked element in A_j, for $j > j_1$. The sequence $\{\mathsf{rank}(a_j^{(2)})\}_{j>j_1}$ is decreasing and therefore must become stationary after a $j_2 > j_1$. Let $u_2 = \mathsf{lead}(a_j^{(2)})$ for $j \geq j_2$. Because u_1 and u_2 are the leaders of the two lowest elements of A_{j_2} they form an autoreduced set. Continuing this way, we construct an infinite autoreduced set of derivatives $\{u_n\}_{n\in\mathbb{N}}$.

For the same reason as in the polynomial case we need to introduce specific d-triangular sets in order to define differential characteristic sets.

Definition 3.16. *A differential triangular set A is a* differential chain *if for all $x \in \mathfrak{L}(A)$ $\mathsf{red}(A_x, A_{<x})$ has the same rank as A_x.*

Note that owing to the definition of d-triangular sets, A_x is partially reduced w.r.t. A and therefore only algebraic reduction is needed to reduce A_x by $A_{<x}$. Basically this definition says that we can associate an autoreduced set to a differential chain and the same discussion than in the polynomial case applies.

The definition of a differential characteristic set of a differential ideal is no different than the definition of a characteristic set of an ideal in the polynomial case and the equivalence between the different definitions is shown similarly.

Definition 3.17. *Let I be a differential ideal in $\mathcal{F}[\![Y]\!]$. A differential chain A contained in I is a* differential characteristic set *of I if one of the following equivalent conditions holds:*

1. *A is of minimal rank among the differential chains contained in I.*
2. *there is no non zero element of I reduced w.r.t. A.*
3. *$\forall q \in I,\ \mathsf{d\text{-}red}(q, A) = 0$.*

The existence of a differential characteristic set for any differential ideal is secured by the first definition and by Proposition 3.15. The first definition also secures that any two characteristic sets of a differential ideal have the same rank.

Note that if $\mathsf{d\text{-}red}(p, A) = 0$, for $p \in \mathcal{F}[\![Y]\!]$ and A a weak d-triangular set, then $p \in [A]\!:\!H_A^\infty$. If A is a differential characteristic set of a differential ideal I we thus have $A \subset I \subset [A]\!:\!H_A^\infty$.

Proposition 3.18. *If C is a differential characteristic set of a prime differential ideal P then $P = [C]\!:\!H_C^\infty = [C]\!:\!S_C^\infty$.*

To prove that $P = [C] : H_C^\infty$ it is sufficient to note that no initial and no separant of C can belong to P and therefore if $\mathsf{d\text{-}red}(p, C) = 0$ then $p \in P$. The fact that $P = [C]\!:\!S_C^\infty$ will be proved more generally in Section 5. Indeed, recent algorithmic improvement in differential algebra owes to the idea of using a wider class of differential ideals than prime differential ideals. We define in Section 5 a less restrictive class of differential ideals that have those properties of prime differential ideals exhibited in the proposition above.

4 Regular differential systems

A necessary and sufficient condition for the existence of a solution to a system of differential equations such as

$$\frac{\partial y}{\partial s} = f(s,t), \quad \frac{\partial y}{\partial t} = g(s,t)$$

is that $\frac{\partial f}{\partial t} = \frac{\partial g}{\partial s}$. Coherence is a property that generalizes this condition for systems given by d-triangular sets. Coherence implies *formal integrability* and is a cousin concept of Riquier's *passivity* [57, 36]. Riquier-Janet approach is discussed in [2]. Informally speaking, the approach through coherence is to the approach through passivity what Gröbner bases are to *involutive* or *Riquier bases*.

The theorem that F. Boulier named Rosenfeld's lemma [6], appeared in [61]. A generalization of use for specialization in positive characteristic appears in [40, III.8]. As for algorithms, in characteristic zero, Kolchin applied this theorem only in the special case of prime differential ideals [40, IV-9] to compute prime characteristic decompositions.

F. Boulier and coauthors [9] showed the fundamental relevance of this theorem for effective algorithms to compute representation of radical differential ideals that allow a membership test. Since then, several generalization were shown. The original theorem applies to ideals $[A] : H_A^\infty$ defined by a coherent autoreduced set A. We give the version of [10] that applies to differential ideals $[A]:H^\infty$ defined by a *regular differential system* (A, H). The proof is nonetheless no different than the original one. The approach of E. Mansfield [46] does not go through d-triangular sets explicitly. [51] gives a generalization of Rosenfeld's lemma that applies in this context.

As a general principle Rosenfeld's lemma makes the bridge between differential algebras and polynomial algebras through ideals that are defined by coherent sets of differential polynomials. In virtue of this principle, many a property of ideals defined by d-triangular sets can be *lifted* to differential ideals defined by coherent d-triangular sets.

In this section we first define the coherence of a d-triangular set and give a finite test for it. We then prove Rosenfeld lemma and give the structure theorem for differential ideals defined by regular differential systems.

4.1 Coherence

We define *coherence of a d-triangular set A away from a set H*. Classically coherence of A is away from H_A. In Section 6, H will be the set of differential polynomials by which it has been allowed to premultiply for reduction and therefore are intrinsically assumed not to vanish identically. H can thus involve separants or initials of elements that are no longer in A.

Testing coherence from its definition is an impossible task since it imposes infinitely many conditions. We give the usual finite test that is analogous to the construction of S-polynomials in the Gröbner bases theory. These analogues to the S-polynomial we call the Δ-polynomials[3]. Inspired by the Gröbner bases theory, an analogue to the second Buchberger criterion was given in [10]. We present this criterion but the real difficulty of it is in its implementation.

The ideals $(A):H^\infty$, where A is a weak d-triangular set and H is a finite set, we shall encounter can be understood as living in the polynomial ring $\mathcal{F}[\Theta Y]$ but also as living in $\mathcal{F}[X]$ where X is a subset of derivatives that include all the ones present in the differential polynomials of A and H. If V is a finite set of derivatives such that $A, H \subset \mathcal{F}[V]$ and I is the ideal $(A):H^\infty$ considered in $\mathcal{F}[V]$ then, since $\mathcal{F}[V]$ is Noehterian,

- I is finitely generated: there exists a finite set $G \subset \mathcal{F}[V]$ such that $I = (G)$
- I admits a primary decomposition in $\mathcal{F}[V]$ say $I = Q_1 \cap \ldots \cap Q_r$.

If X is any set of derivatives such that $V \subset X$ and $I^e, Q_1^e, \ldots, Q_2^e$ are the extension of $I, Q_1, \ldots Q_r$ to $\mathcal{F}[X]$, then $I^e \cap \mathcal{F}[V] = I$ and $Q_1^e \cap \mathcal{F}[V] = Q_1, \ldots, Q_r^e \cap \mathcal{F}[V] = Q_r$. The point is that the polynomial ring in which $(A):H^\infty$ is considered is not very relevant. Since A and H are finite sets, $(A) : H^\infty$ is finitely generated, admits a primary decomposition and any computations on $(A):H^\infty$ can be made in a polynomial ring with finitely many variables.

Two derivatives u and v have a *common derivative* if there exist $\psi, \phi \in \Theta$ such that $\psi u = \phi v$. This happens when u and v are the derivative of the same differential indeterminate. Assume $u = \delta_1^{e_1} \ldots \delta_m^{e_m} y$ and $v = \delta_1^{f_1} \ldots \delta_m^{f_m} y$. Then any $\delta_1^{g_1} \ldots \delta_m^{g_m} y$ with $g_i \geq \max(e_i, f_i)$ is a common derivative of u and v. If we take $g_i = \max(e_i, f_i)$ we obtain the *lowest common derivative* of u and v and that is noted $\mathsf{lcd}(u, v)$.

Definition 4.1. *Let A be a weak d-triangular set in $\mathcal{F}\llbracket Y \rrbracket$ and H a subset of $\mathcal{F}\llbracket Y \rrbracket$. A is said to be coherent away from H (or H-coherent for short) if:*

- $S_A \subset H^\infty$
- *whenever $a, b \in A$ are such that $\mathsf{lead}(a)$ and $\mathsf{lead}(b)$ have a common derivative, say $v = \psi(\mathsf{lead}(a)) = \phi(\mathsf{lead}(b))$, $\phi, \psi \in \Theta$, then*

$$\mathsf{sep}(b)\, \psi(a) - \mathsf{sep}(a)\, \phi(b) \in (\Theta A_{<v}):H^\infty.$$

Note that the leader of $\mathsf{sep}(b)\, \psi(a) - \mathsf{sep}(a)\, \phi(b)$ is lower than v and obviously $\mathsf{sep}(b)\, \psi(a) - \mathsf{sep}(a)\, \phi(b) \in [A]:H^\infty$. What is required here is that $\mathsf{sep}(b)\, \psi(a) - \mathsf{sep}(a)\, \phi(b)$ can be obtained algebraically over the derivatives of the element of A with leader lower than v.

Testing coherence can be done in fact with finitely many tests. For each pair of differential polynomial a and b in the weak d-triangular set it is sufficient to look at the differential polynomial corresponding to the lowest common derivative between $\mathsf{lead}(a)$ and $\mathsf{lead}(b)$.

---

[3] Though the analogy goes this way today, it is worth recalling that this construction of Δ-polynomial dates from 1959's paper of Rosenfeld.

Definition 4.2. *Let a and b be differential polynomials in $\mathcal{F}[\![Y]\!]$. We note $\Delta(a,b)$ the Δ-polynomial of a and b that is defined as follow. If $\mathsf{lead}(a)$ and $\mathsf{lead}(b)$ have no common derivative, then $\Delta(a,b)=0$. Otherwise let $\psi,\phi\in\Theta$ be s.t. $\mathsf{lcd}(\mathsf{lead}(a),\mathsf{lead}(b))=\psi(\mathsf{lead}(a))=\phi(\mathsf{lead}(b))$. Then*

$$\Delta(a,b)=\mathsf{sep}(b)\,\psi(a)-\mathsf{sep}(a)\,\phi(b)$$

We could in fact replace $\mathsf{sep}(a)$ and $\mathsf{sep}(b)$ by their respective quotients with $\gcd(\mathsf{sep}(a),\mathsf{sep}(b))$ to limit expression swell when we compute the Δ-polynomials.

Proposition 4.3. *Let A be a weak d-triangular set and H a subset of $\mathcal{F}[\![Y]\!]$, $S_A\subset H$. If for all $a,b\in A$ we have $\Delta(a,b)\in(\Theta A_{<v}):H^\infty$, where $v=\mathsf{lcd}(\mathsf{lead}(a),\mathsf{lead}(b))$, then A is H-coherent.*

Proof. Note first that for any $h,p\in\mathcal{F}[\![Y]\!]$ and $\theta\in\Theta$, $\theta(hp)\equiv h\theta(p) \mod (\gamma(p)\mid\gamma \text{ divides } \theta,\ \gamma\neq\theta)$. Assume that $v=\mathsf{lcd}(\mathsf{lead}(a),\mathsf{lead}(b))=\psi(\mathsf{lead}(a))=\phi(\mathsf{lead}(b))$ for some $\psi,\phi\in\Theta$. Then $\Delta(a,b)=\mathsf{sep}(b)\,\psi(a)-\mathsf{sep}(a)\,\phi(b)$. Any other common derivative of $\mathsf{lead}(a)$ and $\mathsf{lead}(b)$ can be written θv for some $\theta\in\Theta$. By the first remark $\theta\,(\Delta(a,b))\equiv\mathsf{sep}(b)\,\theta\psi(a)-\mathsf{sep}(a)\,\theta\phi(b) \mod (\gamma\psi(a),\gamma\phi(b)\mid\gamma \text{ divides } \theta,\ \gamma\neq\theta)$. According to the hypotheses and Proposition 3.6, $\theta\,(\Delta(a,b))\in(\Theta A_{<\theta v}):H^\infty$. It follows that $\mathsf{sep}(b)\,\theta\psi(a)-\mathsf{sep}(a)\,\theta\phi(b)\in(\Theta A_{<\theta v}):H^\infty$.

The simplest test for coherence is thus the following. It gives only a sufficient condition as shows the example.

Proposition 4.4. *A weak d-triangular set A in $\mathcal{F}[\![Y]\!]$ is H_A-coherent if $\mathsf{d\text{-}red}(\Delta(a,b),A)=0$, for all $a,b\in A$.*

Example 4.5. *With the orderly d-ranking $y<y_t<y_s<\ldots$ consider the d-triangular set $A=a\,\Delta\,b$ where $a=y_t^2-t^2$ and $b=(y_t-t)\,y_s-2\,t+t\,s$. Then $\Delta(b,a)=2\,y_t\delta_t(b)-(y_t-t)\delta_s(a)=2\,y_t\,(y_s\,y_{tt}-y_s+s-2)$ is such that $\mathsf{d\text{-}red}(\Delta(a,b),A)=(2-s)(y_t+t)$. Nonetheless, $\Delta(a,b)\in\left(\Theta A_{<y_{st}}\right):H_A^\infty=(\delta_t b,a,b):(y_t(y_t-t))^\infty$ since $y_t+t\in(A):H_A^\infty$.*

Note that a differential characteristic set C of a differential ideal I must be H_C-coherent. Indeed $\Delta(a,b)\in[C]\subset I$ for all $a,b\in C$. Thus $\Delta(a,b)$ is reduced to zero by C as prescribed by Definition 3.17.

We proceed to give the analogue of the second Buchberger criterion introduced in [10]. This allows to check coherence by forming less Δ-polynomials. To that end, let us introduce a notation for lowest common derivation operators. Assume $\phi,\psi\in\Theta$ can be written $\phi=\delta_1^{e_1}\ldots\delta_m^{e_m}$ and $\psi=\delta_1^{f_1}\ldots\delta_m^{f_m}$. We define the lowest common derivation operator of ϕ and ψ to be $\phi\diamond\psi=\delta_1^{g_1}\ldots\delta_m^{g_m}$ where $g_i=\max(e_i,f_i)$. In order to get familiar with that notation in use for the rest of the section, note that if $\mathsf{lead}(a)=\phi y$ and $\mathsf{lead}(b)=\psi y$ for some $y\in Y$ and $\phi,\psi\in\Theta$ then

$$\Delta(a,b)=\mathsf{sep}(b)\frac{\phi\diamond\psi}{\phi}(a)-\mathsf{sep}(a)\frac{\phi\diamond\psi}{\psi}(b)$$

and the coherence condition is that

$$\Delta(a,b)\in\left(\Theta A_{<\phi\diamond\psi y}\right):H^\infty.$$

THEOREM 4.6. *Let A be a weak d-triangular set and H a subset of $\mathcal{F}[\![Y]\!]$ that contains the separants of A. Let $p,q,r \in A$ be s.t. $\mathsf{lead}(p) = \phi y$, $\mathsf{lead}(q) = \psi y$ and $\mathsf{lead}(r) = \theta y$ for some $y \in Y$ and $\phi, \psi, \theta \in \Theta$. If the three following conditions are satisfied*

1. *θ divides $\phi\diamond\psi$*
2. *$\Delta(r,p) \in (\Theta A_{<\theta\diamond\phi y}) : H^\infty$*
3. *$\Delta(r,q) \in (\Theta A_{<\theta\diamond\psi y}) : H^\infty$*

then $\Delta(p,q) \in (\Theta A_{<\phi\diamond\psi y}) : H^\infty$

Proof. Note first the easy equivalence $\phi\diamond\theta$ divides $\phi\diamond\psi$ $\Leftrightarrow$ θ divides $\phi\diamond\psi$ $\Leftrightarrow$ $\psi\diamond\theta$ divides $\phi\diamond\psi$. By application of Proposition 3.6 to the hypotheses we obtain:

$$\frac{\phi\diamond\psi}{\phi\diamond\theta}(\Delta(r,p)) \in (\Theta A_{<\phi\diamond\psi\, y}) : H^\infty, \quad \frac{\phi\diamond\psi}{\psi\diamond\theta}(\Delta(r,p)) \in (\Theta A_{<\phi\diamond\psi\, y}) : H^\infty.$$

Since for all $\gamma \in \Theta$ we have $\gamma(hp) \equiv h\gamma(p) \mod (\beta(p) \mid \beta \text{ divides } \gamma,\ \beta \neq \gamma)$ we can write from the above memberships

$$s_p\, \frac{\phi\diamond\psi}{\theta}\,(r) - s_r\, \frac{\phi\diamond\psi}{\phi}\,(p) \in (\Theta A_{<\phi\diamond\psi\, y}) : H^\infty,$$
$$s_p\, \frac{\phi\diamond\psi}{\theta}\,(r) - s_r\, \frac{\phi\diamond\psi}{\psi}\,(q) \in (\Theta A_{<\phi\diamond\psi\, y}) : H^\infty.$$

Multiplying the differential polynomials by s_q and s_p respectively and subtracting one to the other, we get $s_r\Delta(p,q) \in (\Theta A_{<\phi\diamond\psi\, y}) : H^\infty$. As $s_r \in H$, the conclusion follows.

4.2 Rosenfeld's lemma

To apply Rosenfeld lemma to H-coherent d-triangular sets we need some additional reduction hypothesis on the pair (A,H). These properties were encapsulated in the name *regular differential systems* in [9, 10].

DEFINITION 4.7. *A pair (A,H) is a* regular differential system *if*

- *A is a d-triangular set*
- *H is a set of nonzero differential polynomials partially reduced w.r.t. A*
- *$S_A \subset H^\infty$*
- *for all $a,b \in A$, $\Delta(a,b) \in (\Theta A_{<v}) : H^\infty$ where $v = \mathsf{lcd}(\mathsf{lead}(a), \mathsf{lead}(b))$.*

Note that the fact that A is a d-triangular set implies that the separants of A are partially reduced w.r.t. A.

It is practical to define *regular differential ideals* as differential ideals of the type $[A] : H^\infty$ where (A,H) is a regular differential system.

THEOREM 4.8. *Let (A,H) be a regular differential system in $\mathcal{F}[\![Y]\!]$. A differential polynomial that is partially reduced w.r.t. A belongs to $[A] : H^\infty$ if and only if it belongs to $(A) : H^\infty$.*

Proof. For $a \in A$ we note u_a and s_a respectively the leader and the separant of a. Let us consider $p \in [A]:H^\infty$. There thus exists a finite subset D of $\Theta^+ \times A$ s.t. for some $h \in H^\infty$ we can write

$$h\,p = \sum_{(\theta,a)\in D\subset\Theta^+\times A} \alpha_{\theta,a}\,\theta(a) + \sum_{a\in A}\alpha_a\,a \tag{1}$$

for some $\alpha_a, \alpha_{\theta,a} \in \mathcal{F}[\![Y]\!]$. For each equation of type (1) we consider v to be the highest ranking derivative of $\Theta^+\mathfrak{L}(A)$ that appears effectively in the right hand side.

Assume that p is partially reduced w.r.t. A. If the set D is empty then $p \in (A):H^\infty$. Assume, for contradiction, that there is no relation of type (1) with an empty D for p. Among all the possible relationships (1) that can be written, we consider one for which v is minimal.

Consider $E = \{(\theta,a) \in D \mid \theta(u_a) = v\}$ and single out any $(\bar\theta,\bar a)$ of E. As A is H-coherent, for all (θ,a) of E we have $s_{\bar a}\,\theta(a) \equiv s_a\,\bar\theta(\bar a) \mod (\Theta A_{<v}):H^\infty$. Thus

$$s_{\bar a}\,h\,p \equiv \left(\sum_{(\theta,a)\in E} s_a\,\alpha_{\theta,a}\right)\bar\theta(\bar a) + \sum_{(\theta,a)\in D\setminus E} s_{\bar a}\alpha_{\theta,a}\,\theta a + \sum_{a\in A} s_{\bar a}\alpha_a\,a \mod (\Theta A_{<v}):H^\infty \tag{2}$$

so that we can find $k \in H^\infty$ s.t.

$$s_{\bar a} k\,p = \beta_{\bar\theta,\bar a}\,\bar\theta(\bar a) + \sum_{\substack{(\theta,a)\,\in\,\Theta\,\times\,A,\\ \theta(u_a)\,<\,v}} \beta_{\theta,a}\,\theta a + \sum_{a\in A}\beta_a\,a \tag{3}$$

for some $\beta_a, \beta_{\theta,a} \in \mathcal{F}[\![Y]\!]$.

We proceed now to eliminate v from the coefficients $\beta_{\bar\theta,\bar a}$. We make use of the fact that $s_{\bar a}\,v = \bar\theta(\bar a) - \mathsf{tail}(\theta(\bar a))$. Recall that $\mathsf{tail}(\theta(\bar a))$ contains only derivatives lower than v. Multiplying both sides of (3) by $s_{\bar a}^d$, where d is the degree of v in the right hand side, and replacing $s_{\bar a}\,v$ by $\bar\theta(\bar a) - \mathsf{tail}(\theta(\bar a))$ we can rewrite the relationship obtained as

$${s_{\bar a}}^{d+1} k\,p = \gamma_d\,\bar\theta(\bar a)^d + \ldots + \gamma_1\,\bar\theta(\bar a) + \gamma_0 \tag{4}$$

where $\gamma_0, \gamma_1, \ldots, \gamma_d$ no longer contain v and $\gamma_0 \in (\Theta A_{<v})$. The only occurrences of v in that right hand side is through $\bar\theta(\bar a)$. Because p and the elements of H are partially reduced w.r.t. A, v does not appear in the left hand side. The coefficients γ_i, for $1 \le i \le d$ must be zero. We have thus exhibited a relationship like (1) with a v lower than what we started from. This contradicts our hypotheses.

In Section 6.4 we will see that for a weak d-triangular set B that is K-coherent, we can compute a regular differential system (A,H) such that $\mathfrak{L}(A) = \mathfrak{L}(B)$ and $[B]:K^\infty = [A]:H^\infty$. Some of the consequences of Rosenfeld lemma we shall see can therefore be applied to coherent weak d-triangular sets. But Rosenfeld lemma does not, as shows this example.

EXAMPLE 4.9. *In* $\mathbb{Q}(s,t)\,[\![y]\!]$ *endowed with the d-ranking* $y < y_s < y_t < y_{ss} < y_{st} < y_{tt} < \dots$ *consider the weak d-triangular set* $A = y_s \,\Delta\, y_{tt} - y_{ss}$ *that is 1-coherent.* y_{tt} *is partially reduced w.r.t.* A *and belongs to* $[A]$*. Nonetheless* y_{tt} *does not belong to* (A)*.*

There is a number of corollaries that immediately derives from Rosenfeld's lemma. The first one provides a membership test to regular differential ideals. The second one conveys the fact that a regular differential system is formally integrable (outside the union of the zeros of the elements of H). These corollaries are in fact simple consequences of the property: *A differential polynomial that is partially reduced w.r.t. A belongs to* $[A]\!:\!H^\infty$ *if and only if it belongs to* $(A)\!:\!H^\infty$*.* We saw that coherence, i.e. the fact that (A,H) is a regular differential system, is a sufficient condition to get that property. It is not a necessary condition as discussed in [68].

COROLLARY 4.10. *Let* (A,H) *be a regular differential system. Then* $p \in [A]:H^\infty$ *iff* pd-red$(p,A) \in (A)\!:\!H^\infty$*.*

COROLLARY 4.11. *Let* (A,H) *be a regular differential system and* $u \in \Theta Y$ *ranking higher than all the leaders of the elements of* A*. Then* $[A]\!:\!H^\infty \cap \mathcal{F}[\Theta Y_{\leq u}] = (\Theta A_{\leq u})\!:\!H^\infty$*.*

This trivially implies that if $v > u$, $(\Theta A_{\leq v})\!:\!H^\infty \cap \mathcal{F}[\Theta Y_{\leq u}] = (\Theta A_{\leq u})\!:\!H^\infty$. If we have an orderly d-ranking and $v(n)$ is the highest derivative of order n, then $\Theta A_{\leq v(n)}$ is the *prolongation* of A at order n. The property implies that *projection* of the prolongation does not introduce new conditions: $(\Theta A_{\leq v(n+r)}): H^\infty \cap \mathcal{F}[\Theta_n Y] = (\Theta A_{<v(n)})\!:\!H^\infty$. A procedure to compute a power series solution according to any d-ranking is described in [63, 42].

4.3 Regular differential ideals

Rosenfeld lemma allows us to lift the properties of the polynomial ideal $(A)\!:\!H^\infty$ to the differential ideal $[A]:H^\infty$ when (A,H) is a regular differential system. The first result in this line, Theorem 4.12, states that $[A]\!:\!H^\infty$ is radical. This is the key to effective algorithm. Theorem 4.13 shows that we can inspect on the d-triangular set some properties of the essential prime components of the regular differential ideal defined. Theorem 4.12 is the direct lift of Lazard lemma and was first given in [9]. Theorem 4.13 appeared in [10] and we give the proof of [33].

THEOREM 4.12. *Let* (A,H) *be a regular differential system of* $\mathcal{F}\,[\![Y]\!]$*. Then* $[A]\!:\!H^\infty$ *is a radical differential ideal.*

Proof. Assume p^e belongs to $[A]:H^\infty$ and let $\bar{p} =$ pd-red(p,A). $\bar{p}^e$ belongs to $[A]:H^\infty$ and is partially reduced w.r.t. A so that it belongs to $(A):H^\infty$. By [34, Theorem 7.5] $(A):S_A^\infty$ is radical. So is $(A):H^\infty$ since $S_A \subset H^\infty$. Thus $\bar{p}$ belongs to $(A)\!:\!H^\infty$ and therefore p belongs to $[A]\!:\!H^\infty$. It follows that $[A]\!:\!H^\infty$ is radical.

THEOREM 4.13. *Let (A, H) be a regular differential system of $\mathcal{F}[\![Y]\!]$ such that $1 \notin (A):H^\infty$. C is a characteristic set of an associated prime of $(A):H^\infty$ iff C is a differential characteristic set of an essential prime component of $[A]:H^\infty$. Then $\mathfrak{L}(C) = \mathfrak{L}(A)$.*

There is therefore a one-to-one correspondence between the minimal primes of $(A):H^\infty$ and the essential prime components of $[A]:H^\infty$.

Proof. Since we assume $1 \notin (A):H^\infty$, $1 \notin [A]:H^\infty$ by Theorem 4.8 and $[A]:H^\infty$ is radical by Theorem 4.12.

Let X to be the set of the derivatives that are partially reduced w.r.t. A. Then $A, H \subset \mathcal{F}[X]$. Assume the minimal prime decomposition of $[A]:H^\infty$ is $[A]:H^\infty = \bigcap_{i=1}^r P_i$. By Theorem 4.8, $[A]:H^\infty \cap \mathcal{F}[X] = \bigcap_{i=1}^r (P_i \cap \mathcal{F}[X]) = (A):H^\infty$. All the $\tilde{P}_i = P_i \cap \mathcal{F}[X]$ are prime ideals in $\mathcal{F}[X]$ and therefore the minimal primes of $(A):H^\infty$ are to be taken among these $\tilde{P}_i$. We shall show first that all the $\tilde{P}_i$ are minimal primes of $(A):H^\infty$.

$\tilde{P}_i$ must contain at least one minimal prime $\bar{P}_i$ of $(A):H^\infty$. Let $\bar{p}$ be an element of $\mathcal{F}[X]$ that belongs to $\tilde{P}_i$ but does not belong to $(A):H^\infty$ and therefore does not belong to $[A]:H^\infty$ by Theorem 4.8. There exists $q \in \mathcal{F}[\![Y]\!]$, $q \notin P_i$ such that $q\,\bar{p} \in [A]:H^\infty$. Let $\bar{q} = \mathsf{pd\text{-}red}(q, A)$ so that there exists $s \in S_A^\infty$ such that $s\,q \equiv \bar{q} \mod [A]$. We have that $\bar{q} \notin (A):H^\infty$ otherwise q would belong to $[A]:H^\infty$ and therefore to P_i. Nonetheless, $\bar{q}\,\bar{p}$ belongs to $[A]:H^\infty$ and thus to $(A):H^\infty$ since it is partially reduced w.r.t. A. This says that $\bar{p}$ belongs to a minimal prime of $(A):H^\infty$. Thus $\tilde{P}_i$ is contained in the union of minimal primes of $(A):H^\infty$. By the prime avoidance theorem [28, Lemma 3.3] $\tilde{P}_i$ must be contained in one of the minimal primes, say $\bar{P}_i'$, of $(A):H^\infty$. Thus $\bar{P}_i \subset \tilde{P}_i \subset \bar{P}_i'$. We must have $\bar{P}_i' = \bar{P}_i$ and therefore $\tilde{P}_i$ is a minimal prime of $(A):H^\infty$.

If $\tilde{C}_i$ is the characteristic set of a minimal prime $\tilde{P}_i = P_i \cap \mathcal{F}[X]$ of $(A):H^\infty$, we saw in [34, Theorem 7.5] that $\mathfrak{L}(C_i) = \mathfrak{L}(A)$. Thus $\tilde{C}_i$ is a d-triangular set. Let p be an element of P_i and $\bar{p} = \mathsf{d\text{-}red}(p, \tilde{C}_i)$. Then $\bar{p} \in P_i \cap \mathcal{F}[X] = \tilde{P}_i$. C_i being a characteristic set of $\tilde{P}_i$, $\bar{p}$ must be zero. Therefore $\tilde{C}_i$ is a differential characteristic set of P_i.

As all differential characteristic sets of P_i have the same rank, if C_i is another differential characteristic set of P_i, it is included in $\mathcal{F}[X]$. P_i does not contain any non-zero element reduced w.r.t. C_i and so neither does $\tilde{P}_i = P_i \cap \mathcal{F}[X]$. C_i is a characteristic set of $\tilde{P}_i$.

5 Characterizable differential ideals

If A is a d-triangular set and p is a differential polynomial s.t. $\mathsf{d\text{-}red}(p, A) = 0$ then $p \in [A]:H_A^\infty$. What Ritt and Kolchin used in their developments is the fact that if A is the characteristic of a prime differential ideal P then $P = [A]:H_A^\infty = [A]:S_A^\infty$ and $\mathsf{d\text{-}red}(p, A) = 0 \;\Leftrightarrow\; p \in [A]:H_A^\infty$. Recent algorithmic improvement in differential algebra owes to the idea of using a wider class of differential ideals and d-triangular set. We shall introduce *differential regular chains* [42] and show that they are the d-triangular sets A for which $p \in [A]:H_A^\infty \;\Leftrightarrow\; \mathsf{d\text{-}red}(p, A) = 0$

and then $[A]:H_A^\infty = [A]:S_A^\infty$. They define *characterizable differential ideals* that are particular cases of regular differential ideals. Contrary to regular differential ideals though, characterizable differential ideals can be defined intrinsically. They are the best thing after prime differential ideals.

We proceed to define the *characteristic decomposition* of a radical differential ideal as the representation of this ideal into an intersection of characterizable differential ideals.

We finally show that the characteristic decomposition of a regular differential ideal can be trivially lifted from a characteristic decomposition in polynomial algebra [33]. The remarkable thing is that it is independent of the algorithm used to compute the algebraic characteristic decomposition. That is the last main theorem on which is based the complete algorithm to compute characteristic decompositions for finitely generated radical differential ideals.

5.1 Differential regular chains

Definition 5.1. *A differential ideal I is characterizable if for a differential characteristic set C of I we have $I = [C]:H_C^\infty$. C is said to characterize I.*

Membership to a characterizable differential ideal can thus be tested by a simple differential reduction: if I is characterized by C then $p \in I \Leftrightarrow \mathsf{d\text{-}red}(p, C) = 0$. Prime differential ideals are characterizable for any d-ranking. Characterizable differential ideals that are not prime do exist, but that depends on the d-ranking.

We need nonetheless to determine when a d-triangular set A characterizes $[A]:H_A^\infty$. The criterion was provided in [33].

Theorem 5.2. *Let A be a d-triangular set of $\mathcal{F}[\![Y]\!]$. A is a differential characteristic set of $[A]:H_A^\infty$ if and only if A is H_A-coherent and A is a characteristic set of $(A):H_A^\infty$.*

Proof. We claim that if A is a differential characteristic set of $[A]:H_A^\infty$ then A must be H_A-coherent. For any $a, b \in A$, $\Delta(a,b) \in [A] \subset [A]:H_A^\infty$. Therefore $\mathsf{d\text{-}red}(\Delta(a,b), A) = 0$ so that $\Delta(a,b) \in (\Theta A_{<v}):H_A^\infty$, where $v = \mathsf{lcd}(\mathsf{lead}(a), \mathsf{lead}(b))$. Now if A is a differential characteristic set of $[A]:H_A^\infty$, $[A]:H_A^\infty$ has no non-zero element reduced w.r.t. A. It is then obviously also the case for $(A):H_A^\infty$.

Conversely, assume A is H_A-coherent and a characteristic set of $(A):H_A^\infty$. If there would exist a non-zero differential polynomial p in $[A]:H_A^\infty$ reduced w.r.t. A then, by Rosenfeld's lemma (Theorem 4.8) it would belong to $(A):H_A^\infty$. It cannot be so since A is a characteristic set of $(A):H_A^\infty$. Thus A is a differential characteristic set of $[A]:H_A^\infty$.

By application of Theorem 4.12 and Theorem 4.13, a characterizable differential ideal $[C]:H_C^\infty$ is radical and the characteristic sets of its essential prime components have the same set of leaders as C.

Together with the results seen in [34, Section 5 and 7], we can give now a characterization of practical use in terms of regular chains.

COROLLARY 5.3. *Let A be a d-triangular set of $\mathcal{F}\llbracket Y\rrbracket$. A is a differential characteristic set of $[A]:H_A^\infty$ iff the two following conditions are satisfied:*

- *A is H_A-coherent*
- *A is a squarefree regular chain.*

Proof. If A is a squarefree regular chain then A is a characteristic set of $(A):I_A^\infty$ and $(A):H_A^\infty = (A):I_A^\infty$ [34, Theorem 5.13 and Theorem 7.1]. Conversely, if A is a characteristic set of $(A):H_A^\infty$ then any element of $p \in (A):H_A^\infty$ is such that $\mathsf{red}(p, A) = 0$ and therefore $p \in (A):I_A^\infty$. Thus $(A):H_A^\infty = (A):I_A^\infty$ so that A is a squarefree regular chain.We can conclude thanks to Theorem 5.2.

It is reasonable to call a d-triangular set satisfying the two conditions of the preceding corollary a *differential regular chain* so that we can state the previous corollary in an analogous way to the polynomial counterpart seen in [34, Theorem 5.13]: A differential triangular set A is a differential characteristic set of $[A]:H_A^\infty$ iff it is a differential regular chain.

We saw in [34] that when A is a squarefree regular chain then $(A):I_A^\infty = (A):H_A^\infty = (A):S_A^\infty$. This has the following implication which is used in [13].

COROLLARY 5.4. *If A is a differential regular chain then $[A]:H_A^\infty = [A]:S_A^\infty$.*

Proof. Let $p \in [A]:H_A^\infty$. Then $\mathsf{pd\text{-}red}(p, A)$ belongs to $(A):H_A^\infty$. Since $(A):H_A^\infty = (A):S_A^\infty$, $\mathsf{pd\text{-}red}(p, A)$ belongs to $(A):S_A^\infty$ and therefore $p \in [A]:S_A^\infty$.

5.2 Characteristic decomposition

Let J be a radical differential ideal of $\mathcal{F}\llbracket Y\rrbracket$. We call a *characteristic decomposition* of J a representation of J as an intersection of characterizable differential ideals, called *components* of J. Such a characteristic decomposition of J exists: J is the intersection of prime differential ideals and prime differential ideals are characterizable.

Given a finite set Σ of differential polynomials of $\mathcal{F}\llbracket Y\rrbracket$, computing a characteristic decomposition of $\llbracket\Sigma\rrbracket$ means finding the characteristic sets of its components. In other words, given Σ, we want to compute differential regular chains $C_1, \ldots, C_r$ such that $\llbracket\Sigma\rrbracket = \cap_{i=1}^r [C_i]:S_{C_i}^\infty$. This provides naturally a membership test to $\llbracket\Sigma\rrbracket$:

$$p \in \llbracket\Sigma\rrbracket \;\Leftrightarrow\; \mathsf{d\text{-}red}(p, C_i) = 0 \;\forall i,\; 1 \leq i \leq r.$$

According to the d-ranking chosen this allows also to exhibit diverse properties of $\llbracket\Sigma\rrbracket$ or equivalently of the zeros of Σ. As an example, assume we want to know if the zeros of Σ are zeros of differential polynomials in only a subset Z of the differential indeterminates Y. Compute a characteristic decomposition according to an elimination ranking $Z \ll Y \setminus Z$. If there exists such a differential polynomial in Z, it must reduce to zero by the differential regular chains in the decomposition. That is possible only if there is a differential polynomial in all the differential regular chains that has a leader in ΘZ. In view of the d-ranking, all the derivatives of this differential polynomial must be in ΘZ. We can thus read on the differential regular chains the answer.

A characteristic decomposition of a radical differential ideal J is *irredundant* if associating each component in the decomposition with the set of its essential prime components yields a partition of the set of the essential prime components of J. In other words, consider a characteristic decomposition of J, $J = \cap_{i=1}^{r} [C_i] : S_{C_i}^\infty$. This decomposition is irredundant if any prime differential ideal that contains two distinct components $[C_i] : S_{C_i}^\infty$ is not an essential prime component of J.

5.3 Characteristic decomposition of regular differential ideals

We present now the theorem on which is based the last step of the characteristic decomposition algorithm. It shows that the characteristic decomposition of a regular differential ideal can be achieved algebraically, i.e. without performing any derivations. The result was presented in [33].

THEOREM 5.5. *If (A, H) is a regular differential system and $(A) : H^\infty = \cap_{i=1}^{r} (C_i) : I_{C_i}^\infty$ is an irredundant characteristic decomposition then each C_i is a differential regular chain and $[A] : H^\infty = \cap_{i=1}^{r} [C_i] : S_{C_i}^\infty$ is an irredundant characteristic decomposition.*

Proof. From [34, Theorem 7.5], $(A) : H^\infty$ is radical as $S_A \subset H$ and therefore all the components $(C_i) : I_{C_i}^\infty$ in the irredundant decomposition are radical ideals. It follows that each C_i is a squarefree regular chains and $(C_i) : I_{C_i}^\infty = (C_i) : H_{C_i}^\infty$.

Let $B_{i,j}$, $1 \leq j \leq r_i$, be characteristic sets for the minimal primes of $(C_i) : I_{C_i}^\infty$ so that $(C_i) : I_{C_i}^\infty = \cap_{j=1}^{r_i} (B_{ij}) : I_{B_{ij}}^\infty$ is an irredundant prime characteristic decomposition. Thus $(A) : H^\infty = \bigcap_{i,j} (B_{ij}) : I_{B_{ij}}^\infty$ is an irredundant prime characteristic decomposition. By Theorem 4.13, $[A] : H^\infty = \bigcap_{i,j} [B_{ij}] : H_{B_{ij}}^\infty$ is an irredundant prime characteristic decomposition and $\mathfrak{L}(B_{ij}) = \mathfrak{L}(A) = \mathfrak{L}(C_i)$. In particular C_i is a d-triangular set.

We prove now that C_i is H_{C_i}-coherent. Let $a, b \in C_i$. Since a and b belong to $\cap_{j=1}^{r_i} [B_{ij}] : H_{B_{ij}}^\infty$, so does $\Delta(a, b)$ and $\mathsf{d\text{-}red}(\Delta(a, b), C_i)$. Since $\mathsf{d\text{-}red}(\Delta(a, b), C_i)$ is partially reduced w.r.t. all the B_{ij} it must belong to $\cap_{j=1}^{r_i} (B_{ij}) : H_{B_{ij}}^\infty = (C_i) : H_{C_i}^\infty$ in virtue of Theorem 4.8. Now, C_i is a characteristic set of $(C_i) : H_{C_i}^\infty$ so that $\mathsf{d\text{-}red}(\Delta(a, b), C_i)$, that is reduced w.r.t. C_i, must be zero. C_i is thus H_{C_i}-coherent.

We thus have proved that C_i is a differential regular chain. By Theorem 4.13 and Corollary 5.4 $[C_i] : S_{C_i}^\infty = [C_i] : H_{C_i}^\infty = \cap_{j=1}^{r_i} [B_{ij}] : H_{B_{ij}}^\infty$ is an irredundant prime decomposition. We can conclude that $[A] : H^\infty = \cap_{i=1}^{r} [C_i] : S_{C_i}^\infty$ is an irredundant characteristic decomposition.

6 The Rosenfeld Gröbner algorithm

We saw that Rosenfeld's lemma was a link between differential algebra and polynomial algebra and is therefore the key to effective algorithms in differential algebra. Boulier *et al.* gave a first algorithm called Rosenfeld-Gröbner in [9]. For a finite set of differential polynomials, the algorithm computes in a factorization free way a representation of the radical differential ideal generated that allows to test membership. The radical differential ideal is represented as an intersection of regular differential ideals. Each regular differential ideal was given by a *regular differential system* (A, H) together with a Gröbner basis of the polynomial ideal $(A):H^\infty$, hence the Gröbner part of the name. The membership test was thus into two parts: first a differential reduction by A and a membership test to $(A):H^\infty$ by mean of the computed Gröbner basis.

The algorithm for the decomposition into regular differential ideals was greatly improved in [10]. That is the algorithm we reproduce here less the application of the differential analogue of Buchberger second criterion. The full algorithm was implemented by F. Boulier in the *diffalg* package of MAPLE [8].

The splitting strategy of the Rosenfeld-Gröbner algorithm owes to the differential elimination scheme of Seidenberg [66]. Alternative effective algorithms evolving from the Ritt and Kolchin algorithm [40, IV.9] were presented in [33] and [13]. The algorithm of [33] was the first to implement the present strategy that is, first compute a decomposition into regular differential ideals then refine it into a characteristic decomposition by purely algebraic means. The algorithm of [13] is closer to Ritt and Kolchin's algorithm. It intertwines purely algebraic and differential computations recursively to compute a characteristic decomposition. Doing so one is able to compute a *zero decomposition* and that is finer than the radical differential ideal decomposition under study here.

6.1 Philosophy and data representation

The input to the algorithm are two finite sets F and S of differential polynomials. The output is a finite set of regular differential systems, $\{(A_1, H_1), \ldots, (A_r, H_r)\}$, such that

$$[\![F]\!]:S^\infty = [A_1]:H_1^\infty \cap \ldots \cap [A_r]:H_r^\infty$$

Before we obtain regular differential systems we work with *RG-quadruples* that we process towards being regular differential systems.

DEFINITION 6.1. *A RG-quadruple T is defined by a sequence of four finite subsets G, D, A, H of $\mathcal{F}[\![Y]\!]$ such that*

- *A is a weak d-triangular set*
- *$H_A \subset H$.*
- *D is a set of Δ-polynomials*
- *for all $a, b \in A$ either $\Delta(a, b) = 0$ or $\Delta(a, b) \in D$ or $\Delta(a, b) \in \left(\Theta(A \cup G)_{<u}\right):H_u^\infty$, where $u = \mathsf{lcd}(\mathsf{lead}(a), \mathsf{lead}(b))$ and $H_u = H_{A_{<u}} \cup (H \setminus H_A) \cap \mathcal{F}[\Theta Y_{<u}]$.*

To a RG-quadruple noted $T = (G, D, A, H)$ we associate the radical differential ideal $\mathcal{J}(T) = [\![G \cup D \cup A]\!]:H^\infty$.

The weak d-triangular set A consists of the *processed* differential polynomials, while G is the set of differential polynomials to be processed. Rosenfeld-Gröbner starts with only one RG-quadruple, namely $(F, \emptyset, \emptyset, S)$. Each step of the Rosenfeld-Gröbner algorithm consists in processing one step further a RG-quadruple (G, D, A, H). An element of $G \cup D$ is taken out and reduced w.r.t. A. If the element does not reduce to an element of $\mathcal{F}$, we *insert* it into A. This is the role of the algorithm update presented in Section 6.5. New Δ-polynomials are added to D and the separant and the initial of the new element are added to H. To keep the decomposition correct, we need to introduce new RG-quadruples containing the separant and the initial of the new element.

A RG-quadruple is nearly processed when it is of the type $(\emptyset, \emptyset, A, H)$. It is the role of auto-partial-reduce in Section 6.4. to make the final step of taking (A, H) to a regular system (B, K) so that $[\![A]\!] : H^\infty = [B] : K^\infty$. A regular differential system (A, H) can be considered as a RG-quadruple $(\emptyset, \emptyset, A, H)$. At all time the intersection of the differential ideals defined by the present RG-quadruples is equal to $[\![F]\!] : S^\infty$.

The *coherence condition* in the definition of a RG-quadruple is seemingly difficult and the reason for that precision is dictated by the proof of the last part of the algorithm auto-partial-reduce. Basically, the Δ-polynomial between two elements of A is either awaiting treatment, and it belongs to D, or it has been reduced to zero by A. It could also have been discarded by some criterion.

First are presented the lemmas that allow to show the termination of the algorithm, then the lemmas that allow the splittings. The algorithm is afterwards divided in three parts.

6.2 Finiteness lemmas

We shall introduce a partial order on RG-quadruples that is a refinement of the pre-order on d-triangular sets. This order is used to prove the termination of the algorithm.

DEFINITION 6.2. *Let E and F be two finite subsets of $\mathcal{F}[\![Y]\!]$. We say that F precedes E w.r.t. $\prec_s$ if F is obtained from E by replacing only one of its element by a finite number of elements of strictly lower rank. In other words*

$$F \prec_s E \;\Leftrightarrow\; \exists p \in E \text{ s.t. } F = \begin{cases} E \setminus \{p\} \cup \{p_1, \dots p_k\}, & \text{where } \mathsf{rank}(p_i) < \mathsf{rank}(p) \\ \text{or } E \setminus \{p\} \end{cases}$$

PROPOSITION 6.3. *The partial order $\prec_s$ on finite sets of $\mathcal{F}[\![Y]\!]$ is well founded.*

Proof. Let $\{E_i\}_{i\in\mathbb{N}}$ be a strictly decreasing sequence of subsets of $\mathcal{F}[\![Y]\!]$. It can be represented by a finite number of trees. The roots of these trees are the elements of E_1. At each i, we transform one leaf, i.e. one element p of E_i, into a node. The descendants of this node are the differential polynomials of lower ranks $p_1, \dots, p_k$, $k \in \mathbb{N}$, by which p is replaced. A final leaf correspond to the sheer elimination of a polynomial. Therefore, the paths in the trees consist of strictly decreasing sequences of differential polynomials. The trees must have finite depth and thus the sequence $\{E_i\}_{i\in\mathbb{N}}$ must be finite.

Definition 6.4. *Let $T = (G, D, A, H)$ and $\bar{T} = (\bar{G}, \bar{D}, \bar{A}, \bar{H})$ be quadruples. We say that $T \prec_t \bar{T}$ if either*

- $\mathsf{rank}(A) < \mathsf{rank}(\bar{A})$
- $\mathsf{rank}(A) = \mathsf{rank}(\bar{A})$ *and* $G \cup D \prec_s \bar{G} \cup \bar{D}$

Proposition 6.5. *The partial order $\prec_t$ on RG-quadruple is well founded.*

Proof. It follows immediately from Proposition 3.15 and Proposition 6.3.

6.3 Splitting

At each step of the algorithm we want to replace a differential polynomial by its reduction by a weak d-triangular set. This implies premultiplying by initials and separants and intrinsically assuming that we are seeking zeros where those do not vanish. We need to look for the zeros where the separants and the initials vanish, by introducing a branch split.

Let Σ and H be finite subset of differential polynomials. The first type of split expresses that the zero set of Σ can be decomposed into the union of the set of zeros of Σ that make no element of H vanish with the set of zeros common to Σ and an element of H. This split is used in Ritt-Kolchin style of algorithm [40, 33, 13]. The second kind of split introduced in [66] and used in Rosenfeld-Gröbner algorithm [9, 10] is somewhat finer.

Proposition 6.6. *Let Σ be a non-empty subset of a differential ring $\mathcal{R}$.*

- $[\![\Sigma \cup \{ab\}]\!] = [\![\Sigma \cup \{a\}]\!] \cap [\![\Sigma \cup \{b\}]\!]$ *for all* $a, b \in \mathcal{R}$.
- $[\![\Sigma]\!] = [\![\Sigma]\!] : H^\infty \cap \left[\!\left[\Sigma \cup \left\{\prod_{h \in H} h\right\}\right]\!\right]$ *for all finite subset H of $\mathcal{R}$.*

Proof. As $[\![\Sigma \cup \{ab\}]\!] \subset [\![\Sigma \cup \{a\}]\!], [\![\Sigma \cup \{b\}]\!]$, the first inclusion is trivial. Let $p \in [\![\Sigma \cup \{a\}]\!] \cap [\![\Sigma \cup \{b\}]\!]$. There exist $e, f \in \mathbb{N}^*$ s.t. $p^e = q + \alpha$ and $p^f = r + \beta$ where $q, r \in [\Sigma]$ while $\alpha \in [a]$ and $\beta \in [b]$. Thus $p^{e+f} = (q+\alpha)r + \beta q + \alpha\beta$. By Proposition 2.2, $\alpha\beta \in [\![ab]\!]$ so that $p \in [\![\Sigma \cup \{ab\}]\!]$.

Consider $\bar{h}$ the product of the elements of H. We have $[\![\Sigma]\!] : H^\infty = [\![\Sigma]\!] : \bar{h}^\infty$. Let $p \in [\![\Sigma]\!] : \bar{h}^\infty \cap [\![\Sigma \cup \{\bar{h}\}]\!]$. On the one hand there exists $e \in \mathbb{N}^*$ s.t. $p^e = q + \sum_{\theta \in \Theta} \alpha_\theta \theta(\bar{h})$ where $q \in [\Sigma]$ and $\{\alpha_\theta\}_\theta$ is a family of elements of $\mathcal{F}[\![Y]\!]$ with finite support. Then $p^{e+1} = qp + \sum_{\theta \in \Theta} \alpha_\theta p\, \theta(\bar{h})$ so that $p^{e+1} - qp \in [\![\bar{h}p]\!]$ by Proposition 2.2. On the other hand $[\![\bar{h}p]\!] \subset [\![\Sigma]\!]$. It follows that p^{e+1} and therefore p belongs to $[\![\Sigma]\!]$.

If $H = \{h_1, h_2\}$ we can thus write $[\![\Sigma]\!] = [\![\Sigma]\!] : H^\infty \cap [\![\Sigma \cup \{h_1\}]\!] \cap [\![\Sigma \cup \{h_2\}]\!]$. Informally speaking, if we note $\mathcal{Z}(\Sigma)$ the set of zeros of Σ and $\mathcal{Z}(\Sigma/H)$ the subset of zeros of Σ that do not make any element of H vanish, we can write $\mathcal{Z}(\Sigma) = \mathcal{Z}(\Sigma/\{h_1, h_2\}) \cup \mathcal{Z}(\Sigma \cup \{h_1\}) \cup \mathcal{Z}(\Sigma \cup \{h_2\})$. We could also make the following decomposition that introduces less redundancies: $\mathcal{Z}(\Sigma) = \mathcal{Z}(\Sigma/\{h_1, h_2\}) \cup \mathcal{Z}(\Sigma \cup \{h_1\}/\{h_2\}) \cup \mathcal{Z}(\Sigma \cup \{h_2\})$. In terms of radical differential ideals it translates into $[\![\Sigma]\!] = [\![\Sigma]\!] : \{h_1, h_2\}^\infty \cap [\![\Sigma \cup \{h_1\}]\!] : {h_2}^\infty \cap [\![\Sigma \cup \{h_2\}]\!]$. We give and prove the formal and general property that is used in Rosenfeld-Gröbner algorithm.

Proposition 6.7. *Let Σ be a non-empty subset of $\mathcal{R}$.*

- $[\![\Sigma \cup \{\prod_{i=1}^{r} a_i\}]\!] = \bigcap_{i=1}^{r-1} [\![\Sigma \cup \{a_i\}]\!] : \{a_{i+1}, \ldots, a_r\}^\infty \;\cap\; [\![\Sigma \cup \{a_r\}]\!]$ *for any* $a_1, \ldots, a_r \in \mathcal{R}$.
- $[\![\Sigma]\!] = [\![\Sigma]\!] : H^\infty \cap \bigcap_{1 \leq i < r} [\![\Sigma \cup \{h_i\}]\!] : \{h_{i+1}, \ldots, h_r\}^\infty \cap [\![\Sigma \cup \{h_1, \ldots, h_r\}]\!]$ *for any* $H = \{h_1, \ldots, h_r\} \subset \mathcal{F}[\![Y]\!]$.

Proof. The result is trivial for $r = 1$. Assume this is true up to $r-1$, for $r \geq 2$. We have

$$\begin{aligned}
&[\![\Sigma \cup \{a_1 \ldots a_r\}]\!] = [\![\Sigma \cup \{a_1\}]\!] \cap [\![\Sigma \cup \{a_2 \ldots a_r\}]\!] \\
&= [\![\Sigma \cup \{a_1\}]\!] : \{a_2, \ldots, a_r\}^\infty \cap [\![\Sigma \cup \{a_1\} \cup \{a_2 \ldots a_r\}]\!] \cap [\![\Sigma \cup \{a_2 \ldots a_r\}]\!] .
\end{aligned}$$

by application of Proposition 6.6. Noting that the last component is included in the middle component, we can remove this latter so that $[\![\Sigma \cup \{a_1 \ldots a_r\}]\!] = [\![\Sigma \cup \{a_1\}]\!] : \{a_2, \ldots, a_r\}^\infty \cap [\![\Sigma \cup \{a_2 \ldots a_r\}]\!]$. We obtain the result by applying the induction hypothesis on $[\![\Sigma \cup \{a_2 \ldots a_r\}]\!]$. The second point follows immediately since $[\![\Sigma]\!] = [\![\Sigma]\!] : H^\infty \cap [\![\Sigma \cup \{h_1 \ldots h_r\}]\!]$ by Proposition 6.6.

6.4 Computing regular systems equivalent to weak coherent d-triangular sets

We are going to give the last bit of the algorithm. For a pair (A, H) s.t. $(\emptyset, \emptyset, A, H)$ is a RG-quadruple we compute a pair (B, K) that is a regular differential system with the property that $[A] : H^\infty = [B] : K^\infty$. The algorithm consists simply in making partial reductions of the elements of A and H, but the proof is quite involved.

Algorithm 6.8. **auto-partial-reduce**
Input: *Two finite subsets A and H s.t. $(\emptyset, \emptyset, A, H)$ is a RG-quadruple*
Output:

- *the empty set if it is detected that $1 \in [A] : H^\infty$.*
- *a set with a single regular differential system (B, K) with $\mathfrak{L}(A) = \mathfrak{L}(B)$, $H_B \subset K$ and $[A] : H^\infty = [B] : K^\infty$*

```
B := ∅;
for u ∈ 𝔏(A) increasingly do
   b := pd-red(A_u, B);
   if rank(b) = rank(A_u) then
      B := B △ b;
   else
      return(∅);
   fi;
od;
K := H_B ∪ {pd-red(h, B) | h ∈ H \ H_A};
```

if $0 \in K$ *then*
  return($\emptyset$);
else
  return($\{(B,K)\}$);
fi;

Correctness

In the proof we use implicitly the following lemma that is immediate to establish.

LEMMA 6.9. *Let H and K be two subsets and I a (differential) ideal in a (differential) ring $\mathcal{R}$. If $H^\infty K \subset H^\infty + I$ then $I : H^\infty = I : (H \cup K)^\infty$*

The condition $H^\infty K \subset H^\infty + I$ means that for all $k \in K$ there exists h and $\bar{h}$ in H^∞ s.t. $h\,k = \bar{h} + p$ for some $p \in I$.

We shall prove first that after the for loop, either $1 \in [A] : S_A^\infty$ or for any $u \in \mathfrak{L}(A)$ we have:

I0 $\mathsf{rank}(A_{\leq u}) = \mathsf{rank}(B_{\leq u})$ and B_u is partially reduced w.r.t. $B_{<u}$.
I1 $S_{B_{<u}}^\infty H_{A_{\leq u}} \subset H_{B_{\leq u}}^\infty + (\Theta B_{<u})$
I2 $H_{B_{\leq u}} \subset H_{A_{\leq u}}^\infty + (\Theta B_{<u})$
I3 $(\Theta A_{\leq u}) : H_{A_{\leq u}}^\infty = (\Theta B_{\leq u}) : H_{B_{\leq u}}^\infty$

The properties are true for the lowest $u \in \mathfrak{L}(A)$ since then $A_u = B_u$. Let us assume that the properties I0, I1, I2, I3 hold for all $v \in \mathfrak{L}(A)$ with $v < u$, that is as we start a new iteration for u.

Note that induction hypothesis I3 implies that $(\Theta A_{<u}) : H_{A_{<u}}^\infty = (\Theta B_{<u}) : H_{B_{<u}}^\infty$ in virtue of Proposition 3.6 and induction hypothesis I1 and I2.

By induction hypothesis I0, $\mathfrak{L}(B_{<u}) = \mathfrak{L}(A_{<u})$ and thus $u \notin \Theta\mathfrak{L}(B_{<u})$ as A is a weak d-triangular set. The reduction of A_u by $B_{<u}$ is in fact a reduction on the coefficients of A_u seen as a polynomial in u. If $\mathsf{rank}(b) \neq \mathsf{rank}(A_u)$ then $\mathsf{init}(A_u)$ belongs to $(\Theta B_{<u}) : S_{B_{<u}}^\infty$ and thus to $(\Theta A_{\leq u}) : H_{A_{\leq u}}^\infty$ by I3 so that $1 \in [A] : H_A^\infty$. Otherwise $\mathsf{rank}(b) = \mathsf{rank}(A_u)$, so that I0 is preserved, and there exists $s \in S_{B_{<u}}^\infty$ such that

$$\begin{aligned} s\,A_u &\equiv B_u \mod (\Theta B_{<u}) \\ s\,\mathsf{sep}(A_u) &\equiv \mathsf{sep}(B_u) \mod (\Theta B_{<u}) \\ s\,\mathsf{init}(A_u) &\equiv \mathsf{init}(B_u) \mod (\Theta B_{<u}) \end{aligned}$$

From the latter equations, we see immediately that I1 and I2 are kept true.

From the pseudo-division relationship $s\,A_u \equiv B_u \mod (\Theta B_{<u})$ and the induction hypothesis I3 we see that $(\Theta A_{<u}) : H_{A_{<u}}^\infty + (A_u) \subset \left((B_u) + (\Theta B_{<u}) : H_{B_{<u}}^\infty\right) : H_{B_{<u}}^\infty$ so that, by Lemma 6.9 and what we just have seen (property I1) $(\Theta A_{\leq u}) : H_{A_{\leq u}}^\infty \subset (\Theta B_{\leq u}) : H_{B_{\leq u}}^\infty$. Similarly the pseudo-division relationship, induction hypothesis I3 and property I2 just shown give the converse inclusion. Thus $(\Theta A_{\leq u}) : H_{A_{\leq u}}^\infty = (\Theta B_{\leq u}) : H_{B_{\leq u}}^\infty$ so that I3 is preserved.

I0, I1, I2 and I3 are thus proved for all $u \in \mathfrak{L}(A)$ unless we found that $1 \in [A]:H^\infty$. They imply that B is a d-triangular set and $(\Theta A_{<v}):H^\infty_{A_{<v}} = (\Theta B_{<v}):H^\infty_{B_{<v}}$ for all $v \in \Theta Y$ and $[A]:H^\infty_A = [B]:H^\infty_B$.

Consider $\bar{H} = H \setminus H_A$ and for $v \in \Theta Y$, write $\bar{H}_v = \bar{H} \cap \mathcal{F}[\Theta Y_{<v}]$. We shall show now first that $(\Theta A_{<v}):(H_{A_{<v}} \cup \bar{H}_v)^\infty \subset (\Theta B_{<v}):K^\infty$ for all $v \in \Theta Y$ and $[A]:H^\infty = [B]:K^\infty$. We shall prove then that (B, K) is a regular system.

By construction $S^\infty_{B_{<v}} \bar{H}_v \subset K^\infty + (\Theta B_{<v})$ thus $(\Theta A_{<v}):(H_{A_{<v}} \cup \bar{H}_v)^\infty = (\Theta B_{<v}):(H_{B_{<v}} \cup \bar{H}_v)^\infty \subset (\Theta B_{<v}):K^\infty$.

The latter inclusion implies that $[A]:H^\infty \subset [B]:K^\infty$. For the converse inclusion, we saw that $H_B \subset H^\infty_A + [B]$ and thus $K \subset H^\infty + [A]:H^\infty_A$ so that $[B]:K^\infty = [A]:(H_A \cup K \setminus H_B)^\infty \subset [A]:H^\infty$. We thus have the desired equality $[A]:H^\infty = [B]:K^\infty$.

Let $u, v \in \mathfrak{L}(B)$ have common derivatives. We want to show that $\Delta(B_u, B_v) \in (\Theta B_{<w}):K^\infty$, where $w = \mathsf{lcd}(u, v)$. By construction there exists $s_u \in S^\infty_{B_{<u}}$ s.t. $B_u \equiv s_u\, A_u \mod (\Theta B_{<u})$ and $\mathsf{sep}(B_u) \equiv s_u\, \mathsf{sep}(A_u) \mod (\Theta B_{<u})$. Thus $B_u \equiv s_u\, A_u \mod (\Theta A_{<u}) : H^\infty_{A_{<u}}$ and $\mathsf{sep}(B_u) \equiv s_u\, \mathsf{sep}(A_u) \mod (\Theta A_{<u}) : H^\infty_{A_{<u}}$. Similarly there exists $s_v \in S^\infty_{B_{<v}}$ s.t. $B_v \equiv s_v\, A_v \mod (\Theta A_{<v}) : H^\infty_{A_{<v}}$ and $\mathsf{sep}(B_v) \equiv s_v\, \mathsf{sep}(A_v) \mod (\Theta A_{<v}):H^\infty_{A_{<v}}$.

Take $\psi, \phi \in \Theta$ s.t. $w = \mathsf{lcd}(u, v) = \phi u = \psi v$. Since $\phi(s_u A_u) \equiv s_u \phi(A_u) \mod (\Theta A_{<\phi u})$ and similarly for $\psi(s_v A_v)$ we can write:

$$
\begin{aligned}
\Delta(B_u, B_v) &= \mathsf{sep}(B_v)\phi(B_u) - \mathsf{sep}(B_u)\psi(B_v) \\
&\equiv s_v \mathsf{sep}(A_v)\phi(s_u A_u) - s_u \mathsf{sep}(A_u)\psi(s_v A_v) \mod (\Theta A_{<w}):H^\infty_{A_{<w}} \\
&\equiv s_u s_v \Delta(A_u, A_v) \mod (\Theta A_{<w}):H^\infty_{A_{<w}}
\end{aligned}
$$

From the hypothesis on (A, H), $\Delta(A_u, A_v) \in (\Theta A_{<w}):(H_{A_{<w}} \cup \bar{H}_w)^\infty$. Thus $\Delta(B_u, B_v) \in (\Theta B_{<w}):K^\infty$ so that (B, K) is a regular differential system.

Let us note here the difficulty encountered with a lighter coherence condition for RG-quadruples. Assume that the hypothesis on (A, H) had been $\Delta(A_u, A_v) \in (\Theta A_{<w}):H^\infty$ for all $u, v \in \mathfrak{L}(A)$. We could then not conclude that $\Delta(B_u, B_v) \in (\Theta B_{<w}):K^\infty$ as the element of H could have required reduction by some element of ΘB with leader bigger than w.

6.5 A simple updating of RG-quadruple

At each step we need to augment the weak d-triangular set of a RG-quadruple with a new differential polynomial. We need to do it so as to preserve a RG-quadruple structure. The sub-algorithm `update` we present in this section is meant for that. It is in this procedure that the analogue of second Buchberger criterion (Theorem 4.6) should be applied to prune the set of Δ-polynomials. As in the polynomial case, this is a rather delicate matter [5, 10, 7] and only a simple version of the `update` algorithm is given.

Algorithm 6.10. **update**
Input:

- *a 4-tuple* (G, D, A, H) *of finite sets of* $\mathcal{F}[\![Y]\!]$
- $p \in \mathcal{F}[\![Y]\!]$ *reduced w.r.t.* A *s.t.* $(G \cup \{p\}, D, A, H)$ *is a RG-quadruple*

OUTPUT: $\bar{T} = (\bar{G}, \bar{D}, \bar{A}, \bar{H})$ *a RG-quadruple such that*
- $\bar{A} \prec A$
- $\mathcal{J}\left(\bar{G}, \bar{D}, \bar{A}, \bar{H}\right) = \mathcal{J}\left(G \cup \{p\}, D, A, H\right) : \{\mathsf{sep}(p), \mathsf{init}(p)\}^{\infty}$

$u := \mathsf{lead}(p)$;
$G_A := \{a \in A \mid \mathsf{lead}(a) \in \Theta u\}$;
$\bar{A} := A \setminus G_A$;
$\bar{G} := G \cup G_A$;
$\bar{D} := D \cup \{\Delta(p, a) \mid a \in \bar{A}\} \setminus \{0\}$;
$\bar{H} = H \cup \{\mathsf{sep}(p), \mathsf{init}(p)\}$;
return($(\bar{G},\, \bar{D},\, \bar{A}_{<u} \vartriangle p \vartriangle \bar{A}_{>u},\, \bar{H})$ *);*

$(\bar{G},\, \bar{D},\, \bar{A}_{<u} \vartriangle p \vartriangle \bar{A}_{>u},\, \bar{H})$ is a RG-quadruple since:
- p is reduced w.r.t. A and therefore w.r.t. $\bar{A}$ so that $\bar{A}_{<u} \vartriangle p \vartriangle \bar{A}_{>u}$ is a weak d-triangular set.
- $\bar{H}$ contains all the initials and separants of $\bar{A}_{<u} \vartriangle p \vartriangle \bar{A}_{>u}$
- $\bar{A} \cup \bar{G} = A \cup G$. Thus if a, b are elements of $\bar{A}$, they are elements of A so that, by hypothesis on the input, either $\Delta(a, b) = 0$ or $\Delta(a, b) \in D$ or $\Delta(a, b) \in \left(\Theta(A \cup G \cup \{p\})_{<v}\right) : H_v^{\infty}$ where $v = \mathsf{lcd}(\mathsf{lead}(a), \mathsf{lead}(b))$ and $H_v = H_{A_{<v}} \cup (H \setminus H_A) \cap \mathcal{F}[\Theta Y_{<v}]$. Now $D \subset \bar{D}$ and $H_v \subset H_{\bar{A}_{<v}} \cup (H \setminus H_{\bar{A}} \cap \mathcal{F}[\Theta Y_{<v}])$.
- the Δ-polynomials of elements of $\bar{A}$ with p are added to $\bar{D}$.

Because p is reduced w.r.t. A, $\mathsf{rank}(\bar{A}_{<u} \vartriangle p) < \mathsf{rank}(A_{\leq u})$ so that $\mathsf{rank}(A_{<u} \vartriangle p \vartriangle \bar{A}_{>u}) < \mathsf{rank}(A)$.

Furthermore the equality of differential ideals requested is immediate from the facts that $G \cup A = \bar{G} \cup \bar{A}$ and all the $\Delta(p, a)$ introduced in $\bar{D}$ belong to $[\bar{A}]$.

As it stands in this presentation, we could remove from $\bar{D}$ the Δ-polynomials involving elements of G_A.

6.6 Core of the algorithm

After giving the algorithm we shall write down the invariants of the while loop that help understanding the algorithm. In the algorithm description, the set $\mathcal{S}$ contains the RG-quadruples that are still to be processed while $\mathcal{A}$ contains the regular differential systems already obtained.

ALGORITHM 6.11. **Rosenfeld-Gröbner**
INPUT: F, K *finite subsets of* $\mathcal{F}[\![Y]\!]$
OUTPUT: *A set* $\mathcal{A}$ *of regular differential systems s.t.*

- $\mathcal{A}$ *is empty if it has been detected that* $1 \in [\![F]\!] : K^{\infty}$
- $[\![F]\!] : K^{\infty} = \bigcap_{(A,H) \in \mathcal{A}} [A] : H^{\infty}$ *otherwise*
- $H_A \subset H$ *for all* $(A, H) \in \mathcal{A}$

$\mathcal{S} := \{(F, \emptyset, \emptyset, K)\}$;
$\mathcal{A} := \emptyset$;
while $\mathcal{S} \neq \emptyset$ *do*
  (G, D, A, H) := *an element of* $\mathcal{S}$;
  $\bar{\mathcal{S}} := \mathcal{S} \setminus \{(G, D, A, K)\}$
  if $G \cup D = \emptyset$ *then*
    $\bar{\mathcal{A}} := \bar{\mathcal{A}} \cup$ *auto-partial-reduce* (A, H);
  else
    p := *an element of* $G \cup D$;
    $\bar{G},\ \bar{D} := G \setminus \{p\},\ D \setminus \{p\}$;
    $\bar{p}$:= d-red(p, A) ;
    if $\bar{p}$=0 *then*
      $\bar{\mathcal{S}} := \bar{\mathcal{S}} \cup \{(\bar{G}, \bar{D}, A, K)\}$;
    elif $\bar{p} \notin \mathcal{F}$ *then*
      $\bar{p}_i := \bar{p} - \mathit{init}(\bar{p})\ \mathit{rank}(\bar{p})$;
      $\bar{p}_s := \deg(\bar{p}, \mathit{lead}(\bar{p}))\ \bar{p} - \mathit{lead}(\bar{p})\ \mathit{sep}(\bar{p})$;
      $\bar{\mathcal{S}} := \bar{\mathcal{S}} \cup \{$ update $(\bar{G},\ \bar{D},\ A,\ H,\ \bar{p})$,
        $(G \cup \{\bar{p}_s,\ \mathit{sep}(\bar{p})\},\ \bar{D},\ A,\ H \cup \{\mathit{init}(\bar{p})\})$,
        $(\bar{G} \cup \{\bar{p}_i,\ \mathit{init}(\bar{p})\},\ \bar{D},\ A,\ H)\}$;
    fi;
  fi;
  $\mathcal{S} := \bar{\mathcal{S}}$
od;
return($\mathcal{A}$ *);*

Correctness

We shall prove that the following properties are invariants of the while loop.

I0 All elements of $\mathcal{S}$ are RG-quadruple
I1 All elements of $\mathcal{A}$ are regular differential systems
I2 $[\![F]\!]:K^\infty = \bigcap_{T \in \mathcal{S}} \mathcal{J}(T) \cap \bigcap_{(A,H) \in \mathcal{A}} [A]:H^\infty$

These properties are trivially satisfied before the while loop. Assume they are true at the beginning of a new iteration. A RG-quadruple $T = (G, D, A, H)$ is selected.

<u>When $G \cup D = \emptyset$</u>

I0 is trivially preserved. The output of auto-partial-reduce is the empty set only if $1 \in [\![A]\!] : H^\infty$. Otherwise, the output of auto-partial-reduce is the set $\{(B, K)\}$ where (B, K) is a regular differential system s.t. $[A]:H^\infty = [B]:K^\infty$. By Theorem 4.12, $[B]:K^\infty$ is radical and therefore $\mathcal{J}(T) = [\![A]\!]:H^\infty = [B]:K^\infty$. I1 and I2 are thus preserved.

<u>If $G \cup D$ is not empty</u>

I1 is trivially preserved. There exists $h \in H^{\infty}_{A_{\leq u}}$ s.t. $h\,p \equiv \bar{p} \mod (\Theta A_{\leq u})$ where $u = \mathsf{lead}(p)$. Consequently $\mathcal{J}(T) = [\![\bar{G} \cup \bar{D} \cup \{\bar{p}\} \cup A]\!] : H^{\infty}$ since $H_A \subset H$.

We check that for all $a, b \in A$ we have that either $\Delta(a,b) = 0$ or $\Delta(a,b) \in \bar{D}$ or $\Delta(a,b) \in \left(\Theta(A \cup \bar{G} \cup \{\bar{p}\})_{<v}\right) : H_v^{\infty}$, where $v = \mathsf{lcd}(\mathsf{lead}(a), \mathsf{lead}(b))$ and $H_v = H_{A_{<v}} \cup (H \setminus H_A) \cap \mathcal{F}[\Theta Y_{<v}]$. If p was taken in D and $p = \Delta(a,b)$ then $u = \mathsf{lead}(p)$ is lower than $v = \mathsf{lcd}(\mathsf{lead}(a), \mathsf{lead}(b))$ and thus $\Delta(a,b) \in (\Theta A_{<v} \cup \{\bar{p}\}) : H^{\infty}_{A_{<v}}$. Nothing changes for other elements of D. If p was taken in G, we have to note that $\theta p \in \left(\Theta(A \cup \{\bar{p}\})_{\leq \theta u}\right) : H^{\infty}_{A_{\leq u}}$ so that $\left(\Theta(A \cup G)_{<v}\right) : H_v^{\infty} \subset \left(\Theta(A \cup \bar{G} \cup \{\bar{p}\})_{<v}\right) : H_v^{\infty}$ for all $v \in \Theta Y$.

If $\bar{p} = 0$, $(\bar{G}, \bar{D}, A, H)$ is thus a RG-quadruple by induction hypothesis on I0 and we have $\mathcal{J}(T) = \mathcal{J}\left(\bar{G}, \bar{D}, A, H\right)$. Therefore I0 and I3 are preserved. If $\bar{p} \in \mathcal{F}$, $\bar{p} \neq 0$, then $1 \in \mathcal{J}(T)$ so that this component can be dropped. Otherwise, let us write $\bar{s} = \mathsf{sep}(\bar{p})$ and $\bar{\imath} = \mathsf{init}(\bar{p})$. By Proposition 6.7

$$\begin{aligned}\mathcal{J}(T) &= [\![\bar{G} \cup \bar{D} \cup \{\bar{p}\} \cup A]\!] : H^{\infty} \\ &= [\![\bar{G} \cup \bar{D} \cup \{\bar{p}\} \cup A]\!] : (H \cup \{\bar{\imath}, \bar{s}\})^{\infty} \\ &\quad \cap [\![\bar{G} \cup \bar{D} \cup \{\bar{p}, \bar{s}\} \cup A]\!] : (H \cup \{\bar{\imath}\})^{\infty} \cap [\![\bar{G} \cup \bar{D} \cup \{\bar{p}, \bar{\imath}\} \cup A]\!] : H^{\infty}\end{aligned}$$

$(\bar{G}, \bar{D}, A, H)$ and $\bar{p}$ satisfy the input specifications of update (Algorithm 6.10). Then, by the output properties of that latter, $[\![\bar{G} \cup \bar{D} \cup \{\bar{p}\} \cup A]\!] : (H \cup \{\bar{\imath}, \bar{s}\})^{\infty} = \mathcal{J}\left(\mathsf{update}(\bar{G}, \bar{D}, A, H, \bar{p})\right)$ and $\mathsf{update}(\bar{G}, \bar{D}, A, H, \bar{p})$ is a RG-quadruple. Since $[\bar{p}, \bar{s}] = [\bar{p}_s, \bar{s}]$ and $[\bar{p}, \bar{\imath}] = [\bar{p}_i, \bar{\imath}]$ we can replace $\bar{p}$ by respectively $\bar{p}_s$ and $\bar{p}_i$ in the last two components of the above decomposition. We do that to ensure that the corresponding RG-quadruples, $(\bar{G} \cup \{\bar{p}_i, \bar{\imath}\}, \bar{D}, A, H)$ and $(G \cup \{\bar{p}_s, \bar{s}\}, \bar{D}, A, H \cup \{\mathsf{init}(\bar{p})\})$, are lower than (G, D, A, H) for the partial order of Definition 6.4. I0 is preserved and so is I3 since we proved that

$$\begin{aligned}\mathcal{J}(G, D, A, H) &= \mathcal{J}\left(\mathsf{update}(\bar{G}, \bar{D}, A, H, \bar{p})\right) \\ &\quad \cap \mathcal{J}\left(\bar{G} \cup \{\bar{p}_s, \bar{s}\}, \bar{D}, A, H \cup \{\bar{\imath}\}\right) \cap \mathcal{J}\left(\bar{G} \cup \{\bar{p}_i, \bar{\imath}\}, \bar{D}, A, H\right)\end{aligned}$$

Termination

The algorithm proceeds by constructing a tree where the nodes are RG-quadruples, the root being $(F, \emptyset, \emptyset, K)$. The final leafs are RG-quadruples of the type $(\emptyset, \emptyset, A, H)$ or RG-quadruples that define differential ideals containing 1. At each iteration, we give to a RG-quadruple $T = (G, D, A, H)$ in $\mathcal{S}$ that is not a final leaf one or three descendants according to whether $\bar{p} = 0$ or not. These descendant are RG-quadruples that precede T w.r.t. $\prec_q$ (Definition 6.4) so that each path in the tree describes a decreasing sequence of RG-quadruples. By Proposition 6.5 it must be finite.

Improvements

In order to detect earlier inconsistencies, it is recommended to partially reduce the sets H in a RG-quadruple by the weak d-triangular set A. Also, it is worth noting that there is no theoretical need for the initials to appear in the output regular differential systems. One can consider adding them to the sets H and splitting according to them only when they are used for premultiplication in a reduction.

If the differential polynomial $\bar{p}$ has multiple factors, it has common factors with its separant and then inconsistencies and redundancies will appear in the computations. In the implementation it is worth making a partial factorization of the differential polynomial $\bar{p}$ and split according to its *regular* factors. A differential polynomial is said *regular* if it has no common factor with its separant. We can simplify a squarefree factorization scheme to produce the regular differential polynomials $p_1, p_2 \ldots, p_r$ s.t. $\bar{p} = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$ for some $e_i \in \mathbb{N}$. Then

$$\llbracket \bar{G} \cup \bar{D} \cup \{\bar{p}\} \rrbracket : H^\infty = \llbracket \bar{G} \cup \bar{D} \cup \{p_1\} \rrbracket : (H \cup \{p_2, \ldots, p_r\})^\infty \\ \cap \llbracket \bar{G} \cup \bar{D} \cup \{p_2\} \rrbracket : (H \cup \{p_3, \ldots, p_r\})^\infty \cap \ldots \cap \llbracket \bar{G} \cup \bar{D} \cup \{p_r\} \rrbracket : H^\infty$$

in virtue of Proposition 6.7. The related RG-quadruples can then be added to $\mathcal{S}$.

7 Characteristic decomposition algorithm

In this section we give first an algorithm to compute the irredundant characteristic decomposition of a regular differential ideal. We showed in Theorem 5.5 that an irredundant characteristic decomposition of a regular differential ideal $[A] : H^\infty$ could be trivially lifted from an irredundant characteristic decomposition of $(A) : H^\infty$ taken in $\mathcal{F}[X]$ where X is the set of derivatives appearing in A and H. Together with the Rosenfeld-Gröbner algorithm that provides a full algorithm to compute a characteristic decomposition of any finitely generated radical differential ideal. The whole decomposition might nonetheless be redundant. If one furthermore wants a prime characteristic decomposition, it is just a matter of computing prime characteristic decomposition of some zero dimensional radical ideals in some polynomial algebra. It is an open problem to make that prime characteristic decomposition minimal.

7.1 Characteristic decomposition for regular differential ideals

This part is purely algebraic. We describe an algorithm based on Kalkbrener's pseudo-gcd algorithm[4] to compute the irredundant characteristic decomposition of the an ideal defined by a triangular set saturated by at least its initial and separants. Alternative algorithms are given in [33] and in [11]. The algorithm in [33] is based on the computation of Gröbner bases. The algorithm in [11] evolves on the ideas of [41, 50]. The outputs of both these algorithms consist of Gröbner chains. They work by first reducing the problem to dimension 0 by extending the coefficient field with the non leading variables and compute an irredundant

[4] Late in the preparation of these notes the author was pointed out to [4] where the same idea has been developed independently

decomposition according to the ranking induced on the leading variables. In those approaches it needs to be proved additionally that the decomposition obtained in dimension zero can be lifted back to positive dimension. A crucial point is to prove that the triangular sets obtained by considering the non leading variables in the coefficient field are triangular sets for the original ranking on all the variables. This was shown to be true independently of the algorithm used in [33, Theorem 3.10]. The three algorithms have been implemented by their respective authors.

ALGORITHM 7.1. **Irredundant-Characteristic-Decomposition**
INPUT:

- *$\mathcal{F}[X]$ a ring of polynomials.*
- *A a triangular set of $\mathcal{F}[X]$*
- *H a finite subset of $\mathcal{F}[X]$ such that $S_A, I_A \subset H^\infty$*

OUTPUT: *A set $\mathcal{C}$ of squarefree regular chains such that*

- *$\mathcal{C}$ is empty iff $(A):H^\infty = (1)$.*
- *Otherwise $(A):H^\infty = \bigcap_{C\in\mathcal{C}} (C):I_C^\infty$ is an irredundant decomposition.*

$\mathcal{C} := \{\emptyset\}$
for x in X increasingly do
  $H_x := \{h \mid h \in H,\ \mathsf{lead}(h) = x\}$;
  if $x \notin \mathfrak{L}(A)$ then
    for h in H_x do
      $\mathcal{C} := \bigcup_{C\in\mathcal{C}} \mathcal{U}_C$ *where $(\mathcal{Z}_C, \mathcal{U}_C)$ is the output of* *Ksplit*$(\mathcal{F}[X_{\leq x}], C, h)$;
    od;
  else
    for h in H_x do
      $\mathcal{C} := \bigcup_{C\in\mathcal{C}}$ *Krelatively-prime* $(\mathcal{F}[X_{\leq x}][x], C, A_x, h)$
    od;
  fi;
od;
return($\mathcal{C}$);

Termination is not an issue here since Ksplit and Krelatively-prime are called a finite number of time.

Correctness

We show that the outer for loop has the following invariants.

I1 C is a squarefree regular chain, for all $C \in \mathcal{C}$.
I2 $(A_{\leq x}):H_{\leq x}^\infty = \bigcap_{C\in\mathcal{C}} (C):I_C^\infty$ is an irredundant characteristic decomposition.

The invariants are satisfied before the outer for loop when $\mathcal{C} = \{\emptyset\}$ and $A_{<x} = \emptyset$. Let $x \in X$ and assume the invariants are satisfied for all $y \in X_{<x}$.

If $x \notin \mathfrak{L}(A)$

By induction hypothesis on I1, any C in $\mathcal{C}$ is a squarefree regular chain so that the output of $\mathsf{Ksplit}(\mathcal{F}[X_{\leq x}], C, *)$ consists of squarefree regular chains. I1 is preserved.

If $(\mathcal{Z}_C, \mathcal{U}_C)$ is the output of $\mathsf{Ksplit}(\mathcal{F}[X_{\leq x}], C, h)$, where C is a squarefree regular chain, then $(C) : I_C^\infty : h^\infty = \cap_{B \in \mathcal{U}_C} (B) : I_B^\infty$. The inner for loop thus computes an irredundant characteristic decomposition of $(C) : I_C^\infty : H_x^\infty$. I2 is preserved.

If $x \in \mathfrak{L}(A)$

By induction hypothesis on I2 and because $H_A \subset H$, $\mathsf{init}(A_x) \in H_{<x}$ is not a zero divisor modulo any $(C) : I_C^\infty$ for any $C \in \mathcal{C}$. Thus $C \vartriangle A_x$ is a regular chain, for any $C \in \mathcal{C}$. The inputs of $\mathsf{Krelatively\text{-}prime}$ are therefore correct. The output of $\mathsf{Krelatively\text{-}prime}(\mathcal{F}[X_{\leq x}][x], C, A_x, h)$ is an irredundant characteristic decomposition $\langle C \vartriangle A_x \rangle : I_{C \vartriangle A_x}^\infty : h^\infty = \langle B_1 \rangle : I_{B_1}^\infty \cap \ldots \cap \langle B_r \rangle : I_{B_r}^\infty$ so that $(C \vartriangle A_x) : I_{C \vartriangle A_x}^\infty : h^\infty \subset (B_i) : I_{B_i}^\infty$. The inner loop thus computes an irredundant characteristic decompositions of $\langle C \vartriangle A_x \rangle : I_{C \vartriangle A_x}^\infty : H_x^\infty = \langle C_1 \rangle : I_{C_1}^\infty \cap \ldots \cap \langle C_r \rangle : I_{C_r}^\infty$ so that $(C \vartriangle A_x) : I_{C \vartriangle A_x}^\infty : H_x^\infty \subset (C_i) : I_{C_i}^\infty$. If $\deg(A_x, x) = 1$ then $C \vartriangle A_x$ is a squarefree regular chain and so are the C_i. If $\deg(A_x, x) > 1$ then $\mathsf{sep}(A_x)$ belongs to H_x so that $(C \vartriangle A_x) : I_{C \vartriangle A_x}^\infty : H_x^\infty$ is radical. It follows that all the $(C_i) : I_{C_i}^\infty$ are radical and therefore the C_i are squarefree regular chains. I1 and I2 are preserved.

7.2 The complete algorithm

We now have all the material to present an algorithm to compute a characteristic decomposition of the radical differential ideal $[\![F]\!] : K^\infty$ given by two finite set F and K of differential polynomials in $\mathcal{F}[\![Y]\!]$.

For a regular differential system (A, H) we define $X_{A,H}$ to be the finite set of derivatives appearing in A or H. They are ordered according to the underlying d-ranking on $\mathcal{F}[\![Y]\!]$.

Algorithm 7.2. **Differential-Characteristic-Decomposition**

Input: *F, K finite subsets of $\mathcal{F}[\![Y]\!]$*

Output: *A set $\mathcal{C}$ of regular differential chains s.t.*

- *$\mathcal{C}$ is empty iff $1 \in [\![F]\!] : K^\infty$*
- *$[\![F]\!] : K^\infty = \bigcup_{C \in \mathcal{C}} [C] : S_C^\infty$ otherwise*

$\mathcal{A}$:= *Rosenfeld-Gröbner* (F, K);

$\mathcal{C} := \bigcap_{(A,H) \in \mathcal{A}}$ *Irredundant-Characteristic-Decomposition* $(\mathcal{F}[X_{A,H}], A, H)$

return($\mathcal{C}$);

If $\mathcal{A}$ is not the empty set, the output properties of Rosenfeld-Gröbner imply that $[\![F]\!] : K^\infty = \bigcap_{(A,H)\in\mathcal{A}} [A] : H^\infty$ where all $(A,H) \in \mathcal{A}$ are regular differential systems. If $\mathcal{C}_{A,H}$ is the output of Irredundant-Characteristic-Decomposition $(\mathcal{F}[X_{A,H}], A, H)$, $(A) : H^\infty = \bigcap_{C\in\mathcal{C}_{A,H}} (C) : I_C^\infty$ is an irredundant characteristic decomposition. By Theorem 5.5 $[A] : H^\infty = \bigcap_{C\in\mathcal{C}_{A,H}} [C] : S_C^\infty$ is an irredundant characteristic decomposition. Thus $[\![F]\!] : K^\infty = \bigcap_{C\in\mathcal{C}} [C] : S_C^\infty$ is a characteristic decomposition.

In virtue of Theorem 4.13 or Theorem 5.5, the decomposition could be refined to a prime characteristic decomposition by purely algebraic means. By [34, Proposition 5.18] it is in fact a matter of decomposing the radical zero dimensional ideals (C) in $\mathcal{F}(\mathfrak{T}(C))[\mathfrak{L}(C)]$ into prime ideals. That can be achieved by factorizations in towers of extensions as described in [60]. One can alternatively use Gröbner bases techniques and factorization of univariate polynomials [5].

Note that in general the characteristic decomposition computed is not irredundant. In the case we have computed a prime characteristic decomposition, it is possible that one component contains another one.

The *generalized Ritt problem* is the following: given B and C differential characteristic sets of prime differential ideals, can we algorithmically decide whether $[B] : S_B^\infty \subset [C] : S_C^\infty$. This problem is equivalent to be able to compute a basis for a prime differential ideal defined by its differential characteristic set. Already in the case where B and C consist each of a single differential polynomial the problem has remained unsolved.

If one can solve the Ritt problem one can for sure eliminate the redundancy in the characteristic decomposition obtained by the presented algorithm. But this might not be necessary. Indeed, in the case of the radical differential ideal generated by a single polynomial p we can remove the redundancy in a characteristic decomposition. The process is described in [40, Chapter IV] and a factorization free algorithm starting from a decomposition into regular differential ideals is given in [32]. It is based on the *component theorem* and the *low power theorem*, which are among Ritt's deeper results in differential algebra [59]. The link between this algebraic theorem and the analysis of singular solution is extremely interesting and still bears many open problems. For lack of space we had to discard the discussion from the present paper.

8 Examples of applications

In this section we give examples of typical problems where the questions mentioned in the introduction arise. They are answered by computing a characteristic decomposition. We treat here small examples with *diffalg*, a MAPLE package. The *diffalg* package was developed by F. Boulier for the main library of MAPLE V.5. The author has contributed extensions and improvements to the package for MAPLE V.5.1, 6 and 7. We provide a MAPLE worksheet online to demonstrate how to use the package on the presented examples and more space demanding examples [8].

The different questions in the introduction require different d-rankings. Assume we want to know if the solution of a differential system $F = 0$ satisfy some algebraic constraints. That translates into determining if the radical differential ideal $[\![F]\!]$ contains a differential polynomial of order 0. Take an orderly ranking and compute a characteristic decomposition of $[\![F]\!]$. If there exists a differential polynomial of order 0 in $[\![F]\!]$ it must reduce to zero by the differential regular chains defining the decomposition. This is possible only if there are differential polynomials of order 0 in all differential regular chains. We can thus read on the output differential regular chains the answer.

Similarly, assume we want to know if there is an ordinary differential polynomial in one of the independent variables in $[\![F]\!]$. That translates into determining if there is a differential polynomials where all the derivatives are given by a power of a single derivation, say δ_1. We introduce a d-ranking s.t. $e_1 < f_1$ implies $\delta_1^{e_1} \ldots \delta_m^{e_m} y < \delta_1^{f_1} \ldots \delta_m^{e_m} z$ for any $y, z \in Y$. If the radical differential ideal $[\![F]\!]$ contains a differential polynomial with only δ_1 in the derivatives, it must reduce to zero by the regular differential chains defining the characteristic decomposition. These regular differential chains must thus contain such a differential polynomial.

Unfortunately, no example of application to mechanical theorem proving in differential geometry is given. The reader can refer to [74, 23, 43, 4].

8.1 Solving systems of ordinary differential equations

The abilities of the non linear differential system solver, *dsolve*, were enhanced in MAPLE 6 by using the *diffalg* package. For a single differential equation, a characteristic decomposition exhibits the differential equations for the *singular solution*. If they are solved, the complete set of solutions is now returned by *dsolve*.

The simple idea for solving ordinary differential systems is to take advantage of the solver for single non linear differential equation [21, 22, 20]. The input system is thus decomposed with respect to an elimination ranking. We attempt then to solve the system in close form by solving iteratively single differential equations in a unique indeterminate. These applications were developed by E. Cheb Terrab in collaboration with the author. We give an example for each problem.

EXAMPLE 8.1. *Consider the differential equation $(y'' + y^3 y')^2 = (y y')^2(4\,y' + y^4)$. That differential equation came up in Chazy's work to extend the Painlevé analysis to 3rd order differential equations [19, 35]. The particularity of this equation is that the* general *solution has no movable singularity whereas one of the singular solution has.*

Let p be the differential polynomial $(y_{tt}+y^3 y_t)^2-(y y_t)^2(4\,y_t+y^4)$ in $\mathbb{Q}(t)\,[\![y]\!]$. The characteristic decomposition obtained for $[\![p]\!]$ is $[\![p]\!] = [p]:s_p^\infty \cap [q]:s_q^\infty \cap [y]$ where $q = y_t(4\,y_t+y^4)$ and s_p and s_q are the respective separants of p and q. The complete set of solutions is now found by MAPLE *6 or 7. Given semi-explicitely* *they are*

$$y(t) = 0, \quad y(t) = a, \quad y(t)^3 = \frac{4}{3\,(x+a)}, \quad y(t) = a\,\tan(a^3\,x + b).$$

EXAMPLE 8.2. *Let us consider the differential system*

$$x' = y - x^2, \qquad y' = 4\,yx - 4\,x^3, \qquad z' = z^2 - 2\,x^2 + y$$

to which we associate the set of differential polynomials $F = \{x_t - y + x^2, y_t - 4\,yx + 4\,x^3, z_t - z^2 + 2\,x^2 - y\}$ *in the differential ring* $\mathbb{Q}(t)\,[\![x, y, z]\!]$. *We use the elimination ranking such that* $x \ll y \ll z$. *The characteristic decomposition computed is* $[\![F]\!] = [C]\!:\!H_C^\infty$ *where* $C = x_{tt} - 2\,xx_t \vartriangle y - x_t - x^2 \vartriangle z_t - z^2 + x^2 - x_t$. *The solution of the original system is thus given by the solutions of the differential system below that is amenable, by a chain resolution, for a solver of differential equations.*

$$x'' = 2\,xx', \qquad y = x' + x^2, \qquad z' = z^2 - x^2 + x'.$$

The solutions are $(x(t), y(t), z(t)) = \big(a\tan(at+b), a^2 + 2\,a^2\tan(at+b)^2, a\tan(at+c)\big)$ *where* a, b, c *are arbitrary constants.*

Another way of solving regular differential systems is to use the results of [26]. It is shown there that any regular differential system is equivalent to a single differential equation. A method to compute that differential equation is given.

8.2 New classes of ordinary differential equations

Another application of characteristic decomposition algorithms in the line of solving ODE was explored by E. Cheb Terrab. The idea is to create new classes of ordinary differential equations, say of first order, that can be solved together with a way of recognizing whether a given ordinary differential equation is in the class.

EXAMPLE 8.3. *We look for the condition on the function* f *for the ordinary first order differential equation* $\frac{dy}{dx} = f(x,y)$ *to admit a group of symmetry the infinitesimal generator of which,* $\xi(x,y)\frac{\partial}{\partial x} + \phi(x,y)\frac{\partial}{\partial y}$, *have its coefficient satisfying*

$$\xi_y + 1 = 0,\ x\xi_x - y - \xi = 0,\ \phi_x - 1 = 0,\ y\phi_y - \phi + x = 0,\ \phi_y - \xi_x = 0. \quad (5)$$

Those equations say that $\xi(x,y) = \alpha\,x - y,\ \ \phi = x + \alpha\,y$, *where* α *is an arbitrary constant. If* f *is as desired,* $\frac{dy}{dx} = f(x,y)$ *can be transformed to a quadrature* $\frac{dv}{du} = g(u)$ *with the change of variables*[5] $u = \frac{1}{2}\ln(x^2+y^2) - \alpha\,\arctan\left(\frac{y}{x}\right),\ \ v = \arctan\left(\frac{y}{x}\right)$.

[5] [53, Chapter 2.5] details how to find this change of variables from the knowledge of the infinitesimal generator.

The equations $\frac{dy}{dx} = f(x,y)$ *that admit a group of symmetry with infinitesimal generator* $\xi(x,y)\frac{\partial}{\partial x} + \phi(x,y)\frac{\partial}{\partial y}$ *are the ones that satisfy*

$$\phi_x + \phi_y\, f - \xi_x\, f - \xi_y\, f^2 - \xi\, f_x - \phi\, f_y = 0 \tag{6}$$

We therefore consider $\mathbb{Q}(x,y)\,[\![f,\phi,\xi]\!]$, *endowed with derivations according to* x *and* y, *and the set* F *of differential polynomials that correspond to equations (5) and (6). To find the conditions on* f *we must assign a d-ranking that eliminates* ξ *and* ϕ. *We choose* $f < f_y < f_x < f_{yy} < f_{xy} < f_{yy} < \ldots < \xi < \xi_y < \xi_x < \ldots < \phi < \phi_y < \phi_x < \ldots$. *The characteristic decomposition computed is* $\{\Sigma\} = [C_1]\!:\!H_{C_1}^{\infty} \cap [C_2]\!:\!H_{C_2}^{\infty}$ *where* C_1 *is*

$$\begin{array}{ll}
& \left((y^2+x^2)f_y - x(f^2+1)\right)\underline{f_{xy}} - \left((y^2+x^2)f_x + y(f^2+1)\right)f_{yy} \\
& +2\,f_y f(f_y y + x f_x) - f_y(f^2+1) + x({f_x}^2 + {f_y}^2) \\
\triangle & \left((y^2+x^2)f_y - x(f^2+1)\right)^2 \underline{f_{xx}} - \left((y^2+x^2)f_x + y(f^2+1)\right)^2 f_{yy} \\
& + \left((y^2+x^2)(4\,xf-y)f_y - 2\,x(f^2+1)(xf-y)\right) f_x^2 \\
& + \left((y^2+x^2)(x+4\,yf)f_x + 2\,y(f^2+1)(yf+x)\right) f_y^2 \\
& +(y^2+x^2)(x{f_x}^3 - y{f_y}^3) \\
& -(f^2+1)\left(2\,(y^2+x^2)f_x f_y + (f^2+1)(yf_y - xf_x)\right) \\
\triangle & (f_y y + x f_x)\,\underline{\phi} - \left(y^2+x^2\right) f_x - y(f^2+1) \\
\triangle & (f_y y + x f_x)\,\underline{\xi} + \left(y^2+x^2\right) f_y - x\left(f^2+1\right).
\end{array}$$

and C_2 *is*

$$\begin{array}{llll}
& (x^2+y^2)\,\underline{f_y} - x(1+f^2) & \triangle & (x^2+y^2)\,\underline{f_y} + y(1+f^2) \\
\triangle & y\underline{\phi_y} - \phi + x, \quad \triangle \quad \phi_x - 1, & \triangle & y\,\underline{\xi} - x\phi + x^2 + y^2.
\end{array}$$

The leaders have been underlined.

Let us be given f. *If the two first differential polynomials of either* C_1 *or* C_2 *vanish on* f, *we are able to reduce the differential equation* $\frac{dy}{dx} = f(x,y)$ *to a quadrature with the change of variables given above.*

In the case determined by C_2, *the zero of the two first differential polynomials is given by a formula of the type* $\frac{x+\alpha\,y}{\alpha\,x-y}$. *The solutions are given implicitly as* $\frac{1}{2}\,\ln(x^2+y^2) + \alpha\,\arctan\left(\frac{y}{x}\right) = c$, *where* c *is an arbitrary constant.*

In the case determined by C_1, *the two last differential polynomials allow us to determine the right pair* ξ, ϕ. *For instance, one can check that the function* $f(x,y) = \frac{y+x\,H(x^2+y^2)}{x-y\,H(x^2+y^2)}$, *where* H *is an arbitrary function of one variable, makes the two first differential polynomials of* C_1 *vanish and entails* $\xi(x,y) = -y$, $\phi(x,y) = x$. *The change of variables* $u = \frac{1}{2}\,\ln(x^2+y^2)$, $v = \arctan\left(\frac{y}{x}\right)$ *then transforms* $\frac{dy}{dx} = f(x,y)$ *to the quadrature* $\frac{dv}{du} = H(e^{2u})$.

8.3 Differential algebraic systems

Consider implicit differential systems $F(t,Y,Y') = 0$, where $Y = (y_1,\ldots,y_n)$ and $F = (f_1,\ldots,f_n)$ is a polynomial map. When the Jacobian w.r.t. Y', is identically zero, it indicates that there are algebraic constraints on the components of Y and classical schemes of numerical integration fail. The difficulty of numerical integration has been measured by the differential index and specific numerical schemes can handle low index cases [14, 31, 3].

Algorithms specifically designed to reduce a quasi-linear differential-algebraic system to a system a priori amenable to numerical computations were given in [69, 71]. The difficulty is that the expressions can become really big and one is faced with their numerical evaluation. A successful study of a sample of high order index systems was carried out in [71] and the related software and test set are available [70]. We give here only one common example. Interestingly, the computation could not be completed before the results of [33] were implemented.

EXAMPLE 8.4. *We consider the set of differential polynomials in* $\mathbb{Q}(t)\,[\![\lambda, x, y, \nu, u, v]\!]$

$$\begin{aligned} F = \{\, & x_{tt} - 2\,\lambda x + 2\,\nu u,\ y_{tt} - 2\,\lambda y + 2\,\nu v, \quad x^2 + y^2 - 1, \\ & u_{tt} + x_{tt} - 2\,\nu u, \quad v_{tt} + y_{tt} - 2\,\nu v + 1,\ u^2 + v^2 - 1\,\}. \end{aligned}$$

The defined system of ordinary differential equations describes the motion of a double pendulum in Cartesian coordinates. The indeterminates λ, ν are the Lagrangian multipliers used to obtain the equations. It is of course possible to transform it into a set of differential polynomials of order one or less by introducing new differential indeterminates, but in the present approach it is better not to. If we are interested in knowing the trajectory of the two masses only, we choose a d-ranking s.t. $\{x, y, u, v\} \ll \{\lambda, \nu\}$ and the d-ranking on $\{x, y, u, v\}$ is orderly. The characteristic decomposition obtained is $[\![F]\!] = [C_1]\!:\!S_{C_1}^{\infty} \cap [C_2]\!:\!S_{C_2}^{\infty}$ where

$$\begin{aligned} C_1 = \quad & \underline{x}^2 + y^2 - 1 \ \vartriangle\ \underline{u}^2 + v^2 - 1 \\ \vartriangle\ & x^2u^2(2\,yv(yv - xu) - y^2 - v^2 - 1)\,\underline{y_{tt}} \\ & -(yu - xv)(x^3v_t^2 + u^3y_t^2 - x^3u^2v) + yu^2y_t^2 + x^4u^2 \\ \vartriangle\ & x^3u^2\,\underline{v_{tt}} - x^2u^3(xu + yv)y_{tt} + x^3vv_t^2 - u^3vy_t^2 - x^3u^4 \\ \vartriangle\ & 2u^2x^3y\,\underline{\lambda} - x^2u^2(v(xv - yu) + x)y_{tt} + x^3vv_t^2 + u^3vy_t^2 - x^3u^2(v^2 + 1) \\ \vartriangle\ & 2\,v\,\underline{\nu} - y_{tt} - v_{tt} - 1 \end{aligned}$$

and

$$C_2 = \underline{y}^2 - 1 \ \vartriangle\ \underline{x} \ \vartriangle\ \underline{v}^2 - 1 \ \vartriangle\ \underline{u} \ \vartriangle\ \underline{\lambda} - y \ \vartriangle\ 2\underline{\nu} - v.$$

The leaders have been underlined. C_2 represent the equilibrium, while C_1 represent the motion. It is described by two second order differential polynomials together with two constraints. The solutions thus depends on only four arbitrary constants (initial conditions) only.

8.4 Observability of control systems

The work of M. Fliess, T. Glad and coworkers showed the relevance of constructive differential algebra in control theory [29]. We consider systems of the type

$$X' = F(X, U, \Lambda), \quad Y = G(X, U, \Lambda),$$

where $X = (x_1, \ldots, x_n)$ are the state variables, $U = (u_1, \ldots, u_k)$ are the control variables, $\Lambda = (\lambda_1, \ldots, \lambda_p)$ are parameters and $Y = (y_1, \ldots, y_d)$ are the output variables. The questions that one can answer with a characteristic decomposition, when F and G are rational maps, are

- what are the differential equations giving Y in terms of U (the input-output representation).
- can the sate variables be deduced from the knowledge of the output Y and the controls U. In which case the system is observable.
- can the parameters be deduced uniquely from the knowledge of the output Y and the controls U. In which case the system is identifiable.

The first step is to consider the set of differential polynomials C obtained from the above equations together with the additional differential polynomials $\lambda_{1t}, \ldots, \lambda_{pt}$ and the set S of numerators coming into F and G. The answer to the previous questions can be read from a characteristic decomposition of $[\![F]\!]:S^\infty$ w.r.t. a d-ranking s.t. $U \ll Y \ll X \cup \Lambda$.

Example 8.5. *Consider the following system with one control and one parameter:*

$$x_1' = x_1 - \lambda u, \quad x_2' = x_2(1 - x_1), \quad y = \lambda x_1.$$

We compute the characteristic decomposition of $F = \{x_{1t} - x_1 + \lambda u, x_{2t} - x_2(1 - x_1), y - \lambda x_1, \lambda_t\}$ *in* $\mathbb{Q}[\![x_1, x_2, y, \lambda]\!]$ *endowed with a d-ranking s.t.* $u \ll y \ll \lambda \ll \{x_1, x_2\}$. *We obtain* $[\![F]\!] = [C_1]:S_{C_1}^\infty \cap [C_2]:H_{C_2}^\infty \cap [C_3]:H_{C_3}^\infty$ *where*

$$\begin{aligned} C_1 = \; & u\underline{y_{tt}} - uy_t - u_t y_t + u_t y \vartriangle u\underline{\lambda}^2 - y_t + y \vartriangle (y_t - y)\,\underline{x_1} - \lambda u y \\ & \vartriangle (y_t - y)\,\underline{x_{2t}} - x_2(y_t + y + \lambda y u) \end{aligned}$$

$$C_2 = \underline{u} \vartriangle \underline{y_t} - y \vartriangle \lambda \underline{x_1} - y \vartriangle \lambda \underline{x_{2t}} - x_2(\lambda + y)$$

$$C_3 = \underline{y} \vartriangle \underline{\lambda} \vartriangle \underline{x_{2t}} - x_2(1 - x_1) \vartriangle \underline{x_{1t}} - x_1$$

We read from C_1 *that* generically, *the parameter* λ *is algebraically identifiable and* x_1 *is algebraically observable: for a given input and output there are only a finite number of possibilities for their values. On the contrary* x_2 *is not observable. From* C_2 *we see that when* $u = 0$ *the parameter* λ *is no longer identifiable.*

A number of biological models arising in the literature are examined under variants of the characteristic decomposition algorithms in [49]. Another approach is to note that C is a characteristic set for a d-ranking $U \cup \Lambda \ll X \cup Y$ with an orderly ranking on $X \cup Y$ and that $[C]:S^\infty$ is a prime differential ideal. We can take advantage of this fact to avoid splitting when computing a characteristic decomposition for the d-ranking $U \cup Y \ll X \cup \Lambda$. This approach is brought to a very efficient algorithm in [12]. Also, A. Sedoglavic developed an algorithm specific to the question of observability and identifiability [65]. The probabilistic aspect of it brings it to a polynomial time algorithm.

8.5 Symmetry analysis of partial differential equations

A source of over-determined systems of partial differential equations comes from symmetry analysis. The determining equations of the infinitesimal generators of the Lie symmetry group of a differential equation form a set of linear partial differential equations. *Reducing* this set allows to determine if there is a symmetry, to analyze the structure of the group and apply that knowledge to classification problems or to find a reduction of the original equation [53]. Because the system is linear, there is a number of alternative algorithms that can be applied. For a bibliography on the subject, the reader is invited to check [1, 64]. We just give an example that will illustrate a way to solve systems of partial differential systems.

EXAMPLE 8.6. *The determining equations for the infinitesimal generators of the Lie symmetry group of the Burgers' equation $u_t = u_{ss} - u u_s$ are given by the set F of differential polynomials below.*

$$F = \{ -\tau_u - \xi_{s,u}, \xi_{s,s} + 2\,\tau_s - \xi_t, -u\phi_s + \phi_{s,s} - \phi_t, 2\,\tau_{s,u} + 2\,u\tau_u - \phi_{u,u},$$
$$\phi - \tau_t + u\tau_s - 2\,\phi_{s,u} + \tau_{s,s}, -\xi_{u,u}, -\xi_s, -\xi_u, -\tau_{u,u} \}$$

We shall use a d-ranking that is induced by a lexicographical order on the derivation variables s, t, u, i.e. a d-ranking such that

$$\xi < \tau < \phi, \xi_u < \tau_u < \phi_u < \xi_{uu} < \tau_{uu} < \phi_{uu} < \dots$$
$$< \xi_t < \tau_t < \phi_t < \xi_{tu} < \tau_{tu} < \phi_{tu} < \xi_{tuu} < \dots$$

in order to exhibit the ordinary differential equations in u satisfied by the zeros of F. The characteristic decomposition for $[\![F]\!]$ has a single component as the differential polynomials of F are linear. It corresponds to the differential system:

$$\xi_u = 0,\ \tau_u = 0,\ \phi_{uu} = 0,$$
$$\xi_t = -2\,\phi_u,\ \tau_t = \phi - u\phi_u,\ \phi_{tu} = \frac{\phi_t}{u},\ \phi_{tt} = 0,$$
$$\xi_s = 0,\ \tau_s = -\phi_u,\ \phi_s = \frac{\phi_t}{u}.$$

Form this differential characteristic set we can determine that the symmetry group is of dimension 5. We can even solve *the determining equations, starting with solving the ordinary differential polynomials in the above set. We find the solution $(\phi(t,s,u), \tau(t,s,u), \xi(t,s,u)) = (a + bs - 1/2\,cu - btu, d + at + 1/2\,cs + bst, e + ct + bt^2)$ where a, b, c, d, e are arbitrary constants.*

When we look for classes of differential equations [54] or when we search non-classical symmetry reduction [24], the determining equation are non-linear. The work of E.L. Mansfield and coauthors lead, after some monster computations with the competitor MAPLE packages *rif* [56, 73] and *diffgrob2* [46, 47] to new closed form solutions to physically relevant partial differential equations [25, 48].

References

[1] R. L. Anderson, V. A. Baikov, R. K. Gazizov, W. Hereman, N. H. Ibragimov, F. M. Mahomed, S. V. Meleshko, M. C. Nucci, P. J. Olver, M. B. Sheftel, A. V. Turbiner, and E. M. Vorob'ev. *CRC handbook of Lie group analysis of differential equations. Vol. 3.* CRC Press, Boca Raton, FL, 1996. New trends in theoretical developments and computational methods.

[2] J. Apel. *Passive Complete Orthonormal Systems of PDEs and Riquier Bases of Polynomial Modules*, chapter In this volume. 2002.

[3] U. M. Ascher and L. R. Petzold. *Computer methods for ordinary differential equations and differential-algebraic equations.* Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1998.

[4] P. Aubry and D. Wang. Reasonning about surfaces using differential zero and ideal decomposition. In J. Richet-Gebert and D. Wang, editors, *ADG 2000*, number 2061 in LNAI, pages 154–174, 2001.

[5] T. Becker and V. Weispfenning. *Gröbner Bases - A Computational Approach to Commutative Algebra.* Springer-Verlag, New York, 1993.

[6] F. Boulier. *Étude et Implantation de Quelques Algorithmes en Algèbre Différentielle.* PhD thesis, Université de Lille, 1994.

[7] F. Boulier. A new criterion to avoid useless critical pairs in buchberger's algorithm. Technical Report 2001-07, LIFL, Université de Lille, `ftp://ftp.lifl.fr/pub/reports/internal/2001-07.ps`, 2001.

[8] F. Boulier and E. Hubert. *DIFFALG: description, help pages and examples of use.* Symbolic Computation Group, University of Waterloo, Ontario, Canada, 1998. Now available at `http://www.inria.fr/cafe/Evelyne.Hubert/webdiffalg`.

[9] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Representation for the radical of a finitely generated differential ideal. In A. H. M. Levelt, editor, *ISSAC'95.* ACM Press, New York, 1995.

[10] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Computing representations for radicals of finitely generated differential ideals. Technical Report IT-306, LIFL, 1997.

[11] F. Boulier and F. Lemaire. Computing canonical representatives of regular differential ideals. In C. Traverso, editor, *ISSAC.* ACM-SIGSAM, ACM, 2000.

[12] F. Boulier, F. Lemaire, and M. Moreno-Maza. Pardi! In *ISSAC 2001*, 2001. To appear.

[13] D. Bouziane, A. Kandri Rody, and H. Maârouf. Unmixed-dimensional decomposition of a finitely generated perfect differential ideal. *Journal of Symbolic Computation*, 31(6):631–649, 2001.

[14] K. E. Brenan, S. L. Campbell, and L. R. Petzold. *Numerical solution of initial value problems in differential-algebraic equations.* North-Holland, 1989.

[15] A. Buium and P. J. Cassidy. Differential algebraic geometry and differential algebraic groups: from algebraic differential equations to diophantine geometry. In Bass et al. [39].

[16] G. Carra Ferro. Gröbner bases and differential algebra. In *AAECC*, volume 356 of *Lecture Notes in Computer Science.* Springer-Verlag Berlin, 1987.

[17] G. Carrà Ferro and W. Y. Sit. On term-orderings and rankings. In *Computational algebra (Fairfax, VA, 1993)*, number 151 in Lecture Notes in Pure and Applied Mathematics, pages 31–77. Dekker, New York, 1994.

[18] E. Cartan. *Les systèmes Différentiels Extérieurs et leurs Applications Géométrique.* Hermann, 1945.

[19] J. Chazy. Sur les équations différentielles du troisième ordre et d'ordre supérieur dont l'intgrale générale a ses points critiques fixes. *Acta Mathematica*, 34:317–385, 1911.

[20] E. S. Cheb-Terrab. Odetools: A maple package for studying and solving ordinary differential equations. `http://lie.uwaterloo.ca/description/odetools`, 1998. presented for the incoming update of "Handbook of Computer Algebra".

[21] E. S. Cheb-Terrab, L. G. S. Duarte, and L. A. C. P. da Mota. Computer algebra solving of first order ODEs using symmetry methods. *Computer Physics Communications. An International Journal and Program Library for Computational Physics and Physical Chemistry*, 101(3):254–268, 1997.

[22] E. S. Cheb-Terrab, L. G. S. Duarte, and L. A. C. P. da Mota. Computer algebra solving of second order ODEs using symmetry methods. *Computer Physics Communications. An International Journal and Program Library for Computational Physics and Physical Chemistry*, 108(1):90–114, 1998.

[23] S-C. Chou and X-S. Gao. Automated reasonning in differential geometry and mechanics using the characteristic set method. part II. mechanical theorem proving. *Journal of Automated Reasonning*, 10:173–189, 1993.

[24] P. A. Clarkson, D. K. Ludlow, and T. J. Priestley. The classical, direct, and nonclassical methods for symmetry reductions of nonlinear partial differential equations. *Methods and Applications of Analysis*, 4(2):173–195, 1997. Dedicated to Martin David Kruskal.

[25] P. A. Clarkson and E. L. Mansfield. Symmetry reductions and exact solutions of a class of non-linear heat equations. *Physica*, D70:250–288, 1994.

[26] T. Cluzeau and E. Hubert. Resolvent representation for regular differential ideals. *Applicable Algebra in Engineering, Communication and Computing*, to appear.

[27] S. Diop. Differential-algebraic decision methods and some applications to system theory. *Theoretical Computer Science*, 98(1):137–161, 1992. Second Workshop on Algebraic and Computer-theoretic Aspects of Formal Power Series (Paris, 1990).

[28] D. Eisenbud. *Commutative Algebra with a View toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer-Verlag New York, 1994.

[29] M. Fliess and S.T. Glad. An algebraic approach to linear and nonlinear control. In H.L. Trentelman and J.C. Willems, editors, *Essays on control: Perspectives in the theory and its applications*, volume 14 of *PCST*, pages 223–265. Birkhäuser, Boston, 1993.

[30] L. Guo, W. F. Keigher, P. J. Cassidy, and W. Y. Sit, editors. *Differential Algebra and Related Topics*. World Scientific Publishing Co., 2002.

[31] E. Hairer and G. Wanner. *Solving Ordinary Differential Equations II - Stiff and Differential- Algebraic Problems - Second Revised Edition*. Springer, 1996.

[32] E. Hubert. Essential components of an algebraic differential equation. *Journal of Symbolic Computation*, 28(4-5):657–680, 1999.

[33] E. Hubert. Factorisation free decomposition algorithms in differential algebra. *Journal of Symbolic Computation*, 29(4-5):641–662, 2000.

[34] E. Hubert. Notes on triangular sets and triangulation-decomposition algorithms. I Polynomial systems. In this volume, 2002.

[35] E. L. Ince. *Ordinary Differential Equations*. Dover Publications, Inc., 1956.

[36] M. Janet. *Sur les systèmes d'équations aux dérivées paritelles*. Gauthier-Villars, 1929.

[37] M. Kalkbrener. A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. *Journal of Symbolic Computation*, 15(2):143–167, 1993.

[38] I. Kaplansky. *An Introduction to Differential Algebra.* Hermann, Paris, 1970.

[39] E. Kolchin. *Selected works of Ellis Kolchin with commentary.* Commentaries by Armand Borel, Michael F. Singer, Bruno Poizat, Alexandru Buium and Phyllis J. Cassidy, Edited and with a preface by Hyman Bass, Buium and Cassidy. American Mathematical Society, Providence, RI, 1999.

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

[41] D. Lazard. Solving zero dimensional algebraic systems. *Journal of Symbolic Computation*, 15:117–132, 1992.

[42] F. Lemaire. *Contribution à l'algorithmique en algèbre différentielle.* PhD thesis, Université des Sciences et Technoligies de Lille, `http://www.lifl.fr/ lemaire/pub`, 2002.

[43] Z. Li. Mechanical theorem proving in the local theory of surfaces. *Annals of Mathematics and Artificial Intelligence*, 13(1-2):25–46, 1995.

[44] Z. Li and D. Wang. Coherent, regular and simple system in zero decompositions of partial differential systems. *Systems Sciences and Mathematical Sciences*, 12 suppl, 1999.

[45] B. Malgrange. Differential algebra and differential geometry. In *Differential Geometry - Kyoto Nara 2000*, 2000. to appear.

[46] E. L. Mansfield. *Differential Gröbner Bases.* PhD thesis, University of Sydney, 1991.

[47] E. L. Mansfield. *DIFFGROB2: a symbolic algebra package for analysing systems of PDE using MAPLE.* University of Exeter, 1994. Preprint M/94/4.

[48] E. L. Mansfield, G. J. Reid, and P. A. Clarkson. Nonclassical reductions of a 3+1-cubic nonlinear Schrödinger system. *Computer Physics Communications*, 115:460–488, 1998.

[49] G. Margaria, E. Riccomagno, M. J. Chappell, and H. P. Wynn. Differential algebra methods for the study of the structural identifiability of rational function state-space models in the biosciences. *Mathematical Biosciences*, 174(1):1–26, 2001.

[50] M. Moreno Maza and R. Rioboo. Polynomial gcd computations over towers of algebraic extensions. In *Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995)*, pages 365–382. Springer, Berlin, 1995.

[51] S. Morrison. The differential ideal $[P]:M^\infty$. *Journal of Symbolic Computation*, 28(4-5):631–656, 1999.

[52] F. Ollivier. Canonical bases : Relations with standard bases, finiteness conditions and application to tame automorphisms. In Costiglioncello, editor, *MEGA'90.* Birkhauser, August 1990.

[53] P. Olver. *Applications of Lie Groups to Differential Equations.* Number 107 in Graduate texts in Mathematics. Springer-Verlag, New York, 1986.

[54] G. J. Reid. Algorithms for reducing a system of pde to standard form, determining the dimension of its solution space and calculating its taylor series solution. *European Journal Of Applied Mathematics*, 2:293–318, 1991.

[55] G. J. Reid. Finding abstract Lie symmetry algebras of differential equations without integrating determining equations. *European Journal of Applied Mathematics*, 2(4):319–340, 1991.

[56] G. J. Reid, A. D. Wittkopf, and A. Boulton. Reduction of systems of nonlinear partial differential equations to simplified involutive forms. *Eur. J. of Appl. Math.*, 7:604 – 635, 1996.

[57] C. Riquier. *Les systèmes d'q́uations aux dérivés partielles.* Gauthier-Villars, Paris, 1910.

[58] J. F. Ritt. *Differential Equations from the Algebraic Standpoint.* Amer. Math. Soc. Colloq. Publ., 1932.

[59] J. F. Ritt. On the singular solutions of algebraic differential equations. *Annals of Mathematics*, 37(3):552–617, 1936.

[60] J. F. Ritt. *Differential Algebra*, volume XXXIII of *Colloquium publications.* American Mathematical Society, 1950. Reprinted by Dover Publications, Inc (1966).

[61] A. Rosenfeld. Specializations in differential algebra. *Transaction of the American Mathematical Society*, 90:394–407, 1959.

[62] C. J. Rust and G. J. Reid. Rankings of partial derivatives. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI)*, pages 9–16, New York, 1997. ACM.

[63] C. J. Rust, G. J. Reid, and A. D. Wittkopf. Existence and uniqueness theorems for formal power series solutions of analytic differential systems. In *Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC)*, pages 105–112, New York, 1999. ACM.

[64] F. Schwarz. In F. Winkler, editor, *SNCS.* Springer Heidelberg, 2002. In this volume.

[65] A. Sedoglavic. A probabilistic algorithm to test local algebraic observability in polynomial time. In B. Mourrain, editor, *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation (London, Canada, July 22–25 2001)*, pages 309–316, 2001.

[66] A. Seidenberg. An elimination theory for differential algebra. *University of California Publications in Mathematics*, 3(2):31–66, 1956.

[67] W. Seiler. Computer algebra and differential equations - an overview. *mathPAD 7*, 7:34–49, 1997.

[68] W. Sit. The Ritt-Kolchin theory for differential polynomials. In Guo et al. [30].

[69] G. Thomas. *Contributions Théoriques et Algorithmiques à l'Étude des Équations Différentielles-Algébriques. Approche par le Calcul Formel.* PhD thesis, Institut National Polytechnique de Grenoble, Juillet 1997.

[70] J. Visconti. HIDAES (Higher Index Differential Algebraic Equations Solver). Software and test set. Technical report, LMC-IMAG, `http://www-lmc.imag.fr/CF/LOGICIELS/page_dae.html`, 1999.

[71] J. Visconti. *Résolution numérique des équations algébro-différentielles, Estimation de l'erreur globale et réduction formel de l'indice.* PhD thesis, Institut National Polytechnique de Grenoble, 1999. `http://www-lmc.imag.fr/CF/publi/theses/visconti.ps.gz`.

[72] D. Wang. An elimination method for differential polynomial systems. I. *Systems Science and Mathematical Sciences*, 9(3):216–228, 1996.

[73] A. Witkopf and G. Reid. *The RIF package.* CECM - Simon Fraser University - Vancouver, `http://www.cecm.sfu.ca/ wittkopf/rif.html`.

[74] W. T. Wu. Mechanical theorem proving of differential geometries and some of its applications in mechanics. *Journal of Automated Reasoning*, 7(2):171–191, 1991.