A Differential Algebra Introduction For Tropical Differential Geometry

François Boulier

A Differential Algebra Introduction For Tropical Differential Geometry

François Boulier*†

November 24, 2019

These notes correspond to an introductory course to the workshop on tropical differential geometry, organized in December 2019 at the Queen Mary College of the University of London.

I would like to thank many colleagues for their feedback. In particular, François Lemaire, Adrien Poteaux, Julien Sebag, David Bourqui and Mercedes Haiech.

Contents

*Univ. Lille, CNRS, Centrale Lille, Inria, UMR 9189 - CRIStAL - Centre de Recherche en Informatique Signal et Automatique de Lille, F-59000 Lille, France.

†This work has been supported by the bilateral project ANR-17-CE40-0036 and DFG-391322026 SYMBIONT.

1 Formal Power Series Solutions of Differential Ideals

Twenty years ago I had the opportunity to teach differential elimination methods at Paris VI University (today Sorbonne University) in some Master course. The beginning of the course — up to differential ideals — is taught quite easily. But difficulties actually occur as soon as one writes a first equation: what do you mean by a solution of a differential equation whose left hand side is a general differential polynomial ? The approach followed by Ritt (a solution is a prime differential ideal which contains the equation) is very elegant but it is also terribly abstract for students. This time, I have decided to start with a more tedious but much more intuitive approach: we look for formal power series solutions. This approach actually perfectly suits the general context of the workshop.

The main issue of this section is: what about expansion points of formal power series ? They actually play an important role since the problem of the existence of formal power series solution of differential ideal is algorithmically decidable if the expansion point is unspecified while it is undecidable if it is fixed. The undecidability result is given in this section.

1.1 Differential Rings

Reference books are [17] and [12]. The following basic notions are introduced in [12, chap. I, 1].

An operator δ on a ring is called a *derivation operator* if $\delta(a+b) = \delta a + \delta b$ and $\delta(a\,b) = (\delta a)\,b + a\,\delta b$ for all elements a, b of the ring.

A *differential ring* $\mathscr{R}$ is defined as a ring with finitely many derivation operators which commute pairwise i.e. such that $\delta_1\delta_2 a = \delta_2\delta_1 a$ for all derivation operators δ_1, δ_2 and all $a \in \mathscr{R}$.

A *differential field* is a differential ring which is a field. If the number m of derivation operators is equal to 1 then the differential ring is said to be *ordinary*. If it is greater than 1, the differential ring is said to be *partial*.

The operator δ which maps every element of a ring to zero is a derivation so that every ring can be viewed as a trivial differential ring. If the ring is the field $\mathbb{Q}$ of the rational numbers, this derivation is the only possible one since

$$\begin{array}{rclcrcl} \delta(0) & = & \delta(0+0) & = & 2\,\delta(0) & = & 0\,, \\ \delta(1) & = & \delta(1\times 1) & = & 2\,\delta(1) & = & 0\,, \end{array}$$

hence the derivative of any rational number must be zero. More generally, it can be proved that the derivative of any complex number must be zero.

The equations we handle will have coefficients in some differential field $\mathscr{F}$ such that $\mathbb{Q} \subset \mathscr{F} \subset \mathbb{C}$. Since a *constant* is any element whose derivative is zero, we see that $\mathscr{F}$ is a field of constants and has characteristic zero.

In the context of tropical differential geometry, it may be useful to introduce "independent variables". We will see later how to handle them formally in differential algebra. For the moment, let us just say that the symbols $x_1, \ldots, x_m$ are supposed to be related to the derivation operators $\delta_1, \ldots, \delta_m$ by the relations: $\delta_i x_i = 1$ and $\delta_i x_j = 0$ for all $1 \leq i, j \leq m$ such that $i \neq j$. Thus we may interpret δ_i as the partial derivative $\partial/\partial x_i$. In the ordinary context, the derivation operator can thus be interpreted as $\mathrm{d}/\mathrm{d}x$. However let us stress that Ritt's theory and an important part of Kolchin's one do not require these assumptions and deal with an abstract differential field $\mathscr{F}$ of characteristic zero.

1.2 Differential Polynomials

From the differential algebra point of view, *differential indeterminates* are symbols such as u, v over which derivation operators may apply, giving an infinite set of *derivatives*. In the ordinary case, interpreting δ as $\mathrm{d}/\mathrm{d}x$, one may view differential indeterminates as representing unknown functions $u(x)$ and $v(x)$ and their derivatives

$$u, v, \dot{u}, \dot{v}, \ddot{u}, \ddot{v}, \ldots, u^{(r)}, v^{(r)}, \ldots$$

as representing the functions obtained by differentiation.

In the partial case, interpreting the derivation operators as $\delta_i = \partial/\partial x_i$ for $1 \leq i \leq m$, one may view differential indeterminates as representing unknown functions $u(x_1, \ldots, x_m)$ and $v(x_1, \ldots, x_m)$ and their derivatives as representing the functions obtained by partial differentiations.

In the general case it is convenient, following [12, chap. I, 1] to introduce the commutative semigroup (written multiplicatively) Θ generated by the derivation operators. Each *derivative operator* $\theta \in \Theta$ has the form

$$\theta \quad = \quad \delta_1^{e_1} \cdots \delta_m^{e_m}$$

where $e_1, \ldots, e_m \in \mathbb{N}$ (the set of the nonnegative integers). Then the corresponding derivative of the differential indeterminate (say) u will be denoted

$$\theta u \quad \text{or} \quad u_{x_1^{e_1} \cdots x_m^{e_m}} .$$

It represents the function

$$\frac{\partial^{e_1 + \cdots + e_m} u}{\partial x_1^{e_1} \cdots \partial x_m^{e_m}} (x_1, \ldots, x_m) .$$

The nonnegative integer $e_1 + \cdots + e_m$ is said to be the *order* of the derivative operator θ. A derivative operator θ is said to be *proper* if its order is strictly positive.

If $\mathscr{F}$ is a differential field and $U = \{u_1, \ldots, u_n\}$ is a set of n differential indeterminates then the polynomials in the derivatives in ΘU, with coefficients in $\mathscr{F}$ — the elements of $\mathscr{F}[\Theta U]$ — are called *differential polynomials*. All together, they form a *differential polynomial ring* denoted

$$\mathscr{F}\{u_1, \ldots, u_n\} .$$

1.2.1 An Example

Let us consider the ordinary differential polynomial ring $\mathscr{F}\{u\}$. Here is an example of a differential polynomial $p \in \mathscr{F}\{u\}$ and its first derivatives:

$$\begin{aligned} p &= \dot{u}^2 + u^3 , \\ \dot{p} &= 2\,\dot{u}\,\ddot{u} + 3\,u^2\,\dot{u} , \\ \ddot{p} &= 2\,\dot{u}\,u^{(3)} + 2\,\ddot{u}^2 + 3\,u^2\,\ddot{u} + 6\,u\,\dot{u}^2 . \end{aligned}$$

In the sequel, we will define *leading derivatives* through the general concept of *rankings*. For the moment, let us just claim that $\dot{u}, \ddot{u}, u^{(3)}$ are the leading derivatives of $p, \dot{p}, \ddot{p}$. Observe that: 1) each proper derivative of p has degree 1 in its leading derivative; and 2) these leading derivatives all have the same polynomial as coefficient. It is the so-called *separant* of p i.e. the partial derivative of the differential polynomial p w.r.t. its leading derivative

$$\text{separant of } p \quad = \quad \frac{\partial p}{\partial \dot{u}} \quad = \quad 2\,\dot{u} .$$

1.3 Differential Ideals

Let $\mathscr{R}$ denote the differential polynomial ring $\mathscr{F}\{u_1, \ldots, u_n\}$ with $m > 0$ derivation operators. The following definitions are borrowed from [17, chap. I, 7] in the ordinary case. They readily apply to the general case, as pointed out in [17, chap. IX].

A nonempty subset $\mathfrak{A}$ of $\mathscr{R}$ is said to be a *differential ideal* of $\mathscr{R}$ if:

1. it is an ideal of $\mathscr{R}$ and
2. it is stable under the action of the derivations i.e. if it is such that $p \in \mathfrak{A} \Rightarrow \theta p \in \mathfrak{A}$ for all derivation operator $\theta \in \Theta$.

A differential ideal contains an infinite number of differential polynomials unless it consists of the single differential polynomial 0. The intersection of any finite or infinite number of differential ideals is a differential ideal.

A differential ideal $\mathfrak{A}$ is said to be *perfect* if it is equal to its radical i.e. if $(\exists d \in \mathbb{N},\ p^d \in \mathfrak{A}) \Rightarrow p \in \mathfrak{A}$. The intersection of any finite or infinite number of perfect differential ideals is a perfect differential ideal.

A differential ideal $\mathfrak{A}$ is said to be *prime* if it is prime in the usual sense i.e. if $p\,q \in \mathfrak{A} \Rightarrow (p \in \mathfrak{A}$ or $q \in \mathfrak{A})$. Every prime differential ideal is perfect.

Let Σ be any subset of $\mathscr{R}$.

One denotes $[\Sigma]$ the *differential ideal of $\mathscr{R}$ generated by* Σ. It is defined as the intersection of all differential ideals of $\mathscr{R}$ containing Σ. It is the set of all finite linear combinations, with arbitrary elements of $\mathscr{R}$ for coefficients, of elements of Σ and their derivatives of any order.

One denotes $\{\Sigma\}$ the *perfect differential ideal of $\mathscr{R}$ generated by* Σ. It is defined as the intersection of all perfect differential ideals of $\mathscr{R}$ containing Σ.

It is clear that $[\Sigma] \subset \{\Sigma\}$. More precisely, we have the following

Proposition 1 *Let Σ be any subset of $\mathscr{R}$. Then $\{\Sigma\} = \sqrt{[\Sigma]}$. With words, $\{\Sigma\}$ is the set of all differential polynomials $p \in \mathscr{R}$ for which there exists some $r \in \mathbb{N}$ such that $p^r \in [\Sigma]$.*

The only part of the proof which is not immediate is given by the following Lemma, which essentially is [17, chap. I, 9, Lemma].

Lemma 1 *Let Σ be any subset and p be any element of $\mathscr{R}$. If there exists some positive integer r such that $p^r \in [\Sigma]$ then $\dot{p}^{2\,r-1} \in [\Sigma]$, where the dot indicates any derivation operator of $\mathscr{R}$.*

Proof Assume $p^r \in [\Sigma]$. Differentiating p^r and dividing by r we have $p^{r-1}\,\dot{p} \in [\Sigma]$. We thus have proved the Lemma in the case $r = 1$. For the general case $r \geq 2$, observe that we have proved (1) below for $k = 1$:

$$p^{r-k}\,\dot{p}^{2\,k-1} \quad \in \quad [\Sigma] \tag{1}$$

We need to establish that (1) holds for $k = r$. Assume thus (1) holds with $r \geq 2$ and $r > k \geq 1$. Differentiating (1) we get

$$(r-k)\,p^{r-k-1}\,\dot{p}^{2\,k} + (2\,k-1)\,p^{r-k}\,\dot{p}^{2\,k-2}\,\ddot{p} \quad \in \quad [\Sigma] \tag{2}$$

Multiply (2) by $\dot{p}$. Subtract (1) multiplied by $(2\,k-1)\,\ddot{p}$. Divide the result by $r-k$. One gets

$$p^{r-k-1}\,\dot{p}^{2\,k+1} \quad \in \quad [\Sigma] \tag{3}$$

Repeating the above computation (more rigorously, putting it some proof by induction on $r-k$), we see that the Lemma holds in general. □

1.4 Formal Power Series (Ordinary Case)

1.4.1 Informal Introduction

Consider the following ordinary differential polynomial equation

$$p \;=\; \dot{u}^2 + x\,u + 1\,. \tag{4}$$

Its coefficients depend on the "independent variable" x, which is an object that we have not formally introduced. For the moment, let us handle this example informally as if it were a differential polynomial of $\mathscr{F}\{u\}$. Its first derivatives are

$$\begin{aligned} p &= \dot{u}^2 + x\,u + 1\,,\\ \dot{p} &= 2\,\dot{u}\,\ddot{u} + x\,\dot{u} + u\,,\\ \ddot{p} &= 2\,\dot{u}\,u^{(3)} + 2\,\ddot{u}^2 + x\,\ddot{u} + 2\,\dot{u}\,,\\ &\vdots \end{aligned}$$

By analogy with the corresponding concept of algebraic geometry, define an *arc* as any infinite sequence of elements of $\mathscr{F}$

$$\underline{a} \;=\; (a_0, a_1, a_2, \ldots)$$

Let us fix some expansion point $x_0 \in \mathscr{F}$.

If p is any element of $\mathscr{F}\{u\}$, and $\underline{a}$ is any arc, one defines $p(\underline{a})$ as the result of the evaluation of a differential polynomial at an arc, over x_0. It is the element of $\mathscr{F}$ obtained by substituting x_0 to x and a_i to $u^{(i)}$ for each $i \geq 0$, in the differential polynomial p. Over (4), we have:

$$\begin{aligned} p(\underline{a}) &= a_1^2 + x_0\,a_0 + 1\,,\\ \dot{p}(\underline{a}) &= 2\,a_1\,a_2 + x_0\,a_1 + a_0\,,\\ \ddot{p}(\underline{a}) &= 2\,a_1\,a_3 + 2\,a_2^2 + x_0\,a_2 + 2\,a_1\,,\\ &\vdots \end{aligned}$$

Define now the mapping Ψ which associates a formal power series centered at x_0, to each arc, by the formula

$$\Psi(\underline{a}) \;=\; \sum_{i\geq 0} \frac{1}{i\,!}\,a_i\,(x - x_0)^i\,.$$

Then $p(\Psi(\underline{a}))$ denotes the formal power series of $\mathscr{F}[[x - x_0]]$ obtained by substituting the formal power series $\Psi(\underline{a})$ to the differential indeterminate u in p (evaluation of a differential polynomial at a formal power series). This being understood, according to [20, page 160], the following proposition is "nothing but a simple computational rule":

Proposition 2 *Let p be any element of the ordinary differential polynomial ring $\mathscr{F}\{u\}$ and $\underline{a}$ be any arc. Then*

$$p(\Psi(\underline{a})) \;=\; p(\underline{a}) + \dot{p}(\underline{a})\,(x - x_0) + \frac{1}{2}\,\ddot{p}(\underline{a})\,(x - x_0)^2 + \cdots \tag{5}$$

$$\;=\; \sum_{i\geq 0} \frac{1}{i\,!}\,p^{(i)}(\underline{a})\,(x - x_0)^i\,. \tag{6}$$

Over our example, taking the origin as expansion point, Proposition 2 gives

$$\begin{aligned} p(\Psi(\underline{a})) &= (a_1^2+1) + (2\,a_1\,a_2 + a_0)\,x + \frac{1}{2}\,(2\,a_1\,a_3 + 2\,a_2^2 + 2\,a_1)\,x^2 + \cdots\,, \\ \dot{p}(\Psi(\underline{a})) &= (2\,a_1\,a_2 + a_0) + (2\,a_1\,a_3 + 2\,a_2^2 + 2\,a_1)\,x + \cdots\,, \\ &\vdots \end{aligned}$$

Let us have a look to the left hand side of (5). A formal power series is zero if and only if all its coefficients are zero. From Proposition 2, we thus see that if the formal power series $\Psi(\underline{a})$ annihilates the differential polynomial p, it also annihilates all its derivatives and, more generally the whole differential ideal[1] $[p]$.

The coefficients of $\Psi(\underline{a})$ belong to a field i.e. to an integral domain. Thus if there exists some $r \in \mathbb{N}$ and some $q \in \mathscr{F}\{u\}$ such that $\Psi(\underline{a})$ annihilates q^r then $\Psi(\underline{a})$ annihilates q. Therefore, using Proposition 1, we see that if $\Psi(\underline{a})$ annihilates p then it annihilates the whole perfect differential ideal $\{p\}$.

Let us now have a look at the formal power series standing at the right hand side of (5). It is zero if and only if the differential polynomial p and all its derivatives are annihilated by the arc $\underline{a}$ over x_0. Argumenting as above, we see that the right hand side of (5) is zero if and only if the whole perfect differential ideal $\{p\}$ is annihilated by the arc $\underline{a}$ over x_0. In summary,

Corollary 1 *The formal power series $\Psi(\underline{a})$ annihilates the perfect differential ideal $\{p\}$ if and only if this perfect differential ideal evaluates to zero at the arc $\underline{a}$.*

1.4.2 On the Expansion Point

Many algebra books only deal with formal power series centered at the origin. Moreover, classical differential algebra books [17, 12] do not mention "non autonomous" differential polynomials i.e. differential polynomials whose coefficients depend on the "independent variables". In this section we show how formal power series centered at some $x_0 \in \mathscr{F}$ can be obtained from formal power series centered at the origin, on "autonomous" differential polynomials at the price of an extra differential indeterminate. We illustrate the process over our example (4).

We look for a formal power series solution of p centered at some $x_0 \in \mathscr{F}$. The "independent" variable x is encoded by an extra differential indeterminate. For legibility, the symbol x is kept for the differential indeterminate. The symbol used for the derivation is renamed as ξ which means that formal power series are sought in $\mathscr{F}[[\xi]]$ and that the derivation operator should be interpreted as $\mathrm{d}/\mathrm{d}\xi$. The differential equation $p = 0$ is thus equivalent to the following "autonomous" differential polynomial system of $\mathscr{F}\{u, x\}$

$$\dot{u}^2 + x\,u + 1 = 0\,, \tag{7}$$

$$\dot{x} - 1 = 0\,. \tag{8}$$

Since we are looking for a formal power series centered at x_0 i.e. such that $x(0) = x_0$, we fix the "initial condition" of the second equation to x_0 (the expansion point has been encoded as an initial condition), which means that we associate to the differential indeterminate x the following arc

$$\underline{x} = (x_0, 1, 0, 0, \ldots)\,, \tag{9}$$

so that the formal power series solution of (8) is

$$\Psi(\underline{x}) = x_0 + \xi\,. \tag{10}$$

[1] Notice that this generalization would not have made sense if we had put the "independent variable" in the field of coefficients since the coefficients of some elements of $[p]$ would then have vanishing denominators.

Let $\underline{a} = (a_0, a_1, \ldots)$ be any arc, associated to the differential indeterminate u. In order to evaluate (7) over the tuple of arcs $(\underline{x}, \underline{a})$ compute the derivatives of this differential polynomial

$$\begin{aligned} p &= \dot{u}^2 + x\,u + 1\,, \\ \dot{p} &= 2\,\dot{u}\,\ddot{u} + x\,\dot{u} + \dot{x}\,u\,, \\ \ddot{p} &= 2\,\dot{u}\,u^{(3)} + 2\,\ddot{u}^2 + x\,\ddot{u} + 2\,\dot{x}\,\dot{u} + u\,\ddot{x}\,, \\ &\vdots \end{aligned}$$

Evaluate them over the tuple of arcs

$$\begin{aligned} p(\underline{x}, \underline{a}) &= a_1^2 + x_0\,a_0 + 1\,, \\ \dot{p}(\underline{x}, \underline{a}) &= 2\,a_1\,a_2 + x_0\,a_1 + a_0\,, \\ \ddot{p}(\underline{x}, \underline{a}) &= 2\,a_1\,a_3 + 2\,a_2^2 + x_0\,a_2 + 2\,a_1\,, \\ &\vdots \end{aligned}$$

Fix the expansion point to the origin $\xi = 0$. One may now evaluate p over the tuple of formal power series $(\Psi(\underline{x}), \Psi(\underline{a}))$ by applying Proposition 2:

$$p(\Psi(\underline{x}), \Psi(\underline{a})) = (a_1^2 + x_0\,a_0 + 1) + (2\,a_1\,a_2 + x_0\,a_1 + a_0)\,\xi + \frac{1}{2}\,(2\,a_1\,a_3 + 2\,a_2^2 + x_0\,a_2 + 2\,a_1)\,\xi^2 + \cdots$$

Since $\xi = x - x_0$ by (10), one may now eliminate ξ from the above formula and get the sought formal power series, centered at x_0, for p:

$$\begin{aligned} p(\Psi(\underline{x}), \Psi(\underline{a})) = {} & (a_1^2 + x_0\,a_0 + 1) + (2\,a_1\,a_2 + x_0\,a_1 + a_0)\,(x - x_0) \\ & + \frac{1}{2}\,(2\,a_1\,a_3 + 2\,a_2^2 + x_0\,a_2 + 2\,a_1)\,(x - x_0)^2 + \cdots \end{aligned}$$

1.4.3 Summary

Given a differential polynomial (4), let us call *extended system* the system (7,8) obtained by encoding the "independent variable" as an extra differential indeterminate and renaming the derivation as $\delta = \mathrm{d}/\mathrm{d}\xi$.

In the sequel, when we will need to consider formal power series solutions or arc solutions of a differential polynomial, we will often tacitly assume that we consider solutions of the corresponding extended system, centered at, or over the origin. This actually justifies the fact that the notations $p(\underline{a})$ and $\Psi(\underline{a})$ do not feature the expansion point.

In the definition of the differential polynomial rings, the extra differential indeterminate used to encode the "independent variable" will always be omitted and we will write that the differential polynomial (4) belongs to $\mathscr{F}\{u\}$.

We will be more precise when there will be any risk of confusion.

Last notice that our encoding does not cover the case of differential polynomials with coefficients in the ring of formal power series of $\mathscr{F}[[x]]$ as in [1]. However, it covers the case of differential polynomials with coefficients in $\mathscr{F}[x]$.

1.5 Formal Power Series (Partial Case)

Let us now consider an example in the partial case. The differential polynomial ring is $\mathscr{F}\{u\}$ with two derivations, with respect to x and y. The left hand side of the following partial differential equation (PDE) is a differential polynomial p

$$u_y\,u_x^2 - 8\,u + 1 = 0\,. \tag{11}$$

The first derivatives of p are

$$\begin{aligned} p &= u_y\,u_x^2 - 8\,u + 1\,, \\ p_x &= u_x\,(2\,u_y\,u_{xx} + u_x\,u_{xy} + 24\,u^2)\,, \\ p_y &= 2\,u_x\,u_y\,u_{xy} + u_x^2\,u_{xy} - 24\,u^2\,u_y\,, \\ p_{xx} &= 2\,u_x\,u_y\,u_{xxx} + u_x^2\,u_{xxy} + 2\,u_y\,u_{xx}^2 + 4\,(u_x\,u_{xy} - 6\,u^2)\,u_{xx} - 48\,u\,u_x^2\,, \\ &\vdots \end{aligned}$$

Over this example, the two derivatives u_x and u_y could be considered as the leading derivative of p. Let us choose u_x. Then the leading derivatives of p_x, p_y, p_{xx} are u_{xx}, u_{xy}, u_{xxx}. As in the ordinary case, each proper derivative of p has degree 1 in its leading derivative; these leading derivatives all have the same polynomial as coefficient. It is the separant of the differential polynomial p

$$\text{separant of } p \;=\; \frac{\partial p}{\partial u_x} \;=\; 2\,u_y\,u_x\,.$$

The leading coefficient of p w.r.t. its leading derivative is called the *initial* of p. It is the differential polynomial u_y.

The definitions introduced in the ordinary differential case hold amost "as is" in the partial case.

An arc[2] is defined as an infinite sequence of elements of $\mathscr{F}$. Pairs $(i,j) \in \mathbb{N}^2$ are however used as indices:

$$\underline{a} \;=\; (a_{0,0}, a_{1,0}, a_{0,1}, a_{2,0}, a_{1,1}, a_{0,2}, a_{3,0}, a_{2,1}, a_{1,2}, a_{0,3}, a_{4,0}, \ldots)$$

Let us fix some expansion point $(x_0, y_0) \in \mathscr{F}^2$.

If p is any element of the partial differential ring $\mathscr{F}\{u\}$ and $\underline{a}$ is any arc, one defines $p(\underline{a})$ as the result of the evaluation of the differential polynomial p at an arc $\underline{a}$, over (x_0, y_0). It is the element of $\mathscr{F}$ obtained by substituting x_0 to x, y_0 to y and $a_{i,j}$ to $u_{x^i y^j}$ for all $i, j \geq 0$. Over our example we have:

$$\begin{aligned} p(\underline{a}) &= a_{0,1}\,a_{1,0}^2 - 8\,a_{0,0} + 1\,, \\ p_x(\underline{a}) &= a_{1,0}\,(2\,a_{0,1}\,a_{2,0} + a_{1,0}\,a_{1,1} + 24\,a_{0,0}^2)\,, \\ p_y(\underline{a}) &= 2\,a_{1,0}\,a_{0,1}\,a_{1,1} + a_{1,0}^2\,a_{1,1} - 24\,a_{0,0}^2\,a_{0,1}\,, \\ p_{xx}(\underline{a}) &= 2\,a_{1,0}\,a_{0,1}\,a_{3,0} + a_{1,0}^2\,a_{2,1} + 2\,a_{0,1}\,a_{2,0}^2 + 4\,(a_{1,0}\,a_{1,1} - 6\,a_{0,0}^2)\,a_{2,0} - 48\,a_{0,0}\,a_{1,0}^2\,, \\ &\vdots \end{aligned}$$

We may now generalize to the partial case, the mapping Ψ, which associates a formal power series centered at (x_0, y_0) to each arc:

$$\Psi(\underline{a}) \;=\; \sum_{i,j \geq 0} \frac{1}{i\,!}\,\frac{1}{j\,!}\,a_{i,j}\,(x - x_0)^i\,(y - y_0)^j\,. \tag{12}$$

Proposition 2 generalizes to

Proposition 3 *Let p be any element of the partial differential ring $\mathscr{F}\{u\}$ and $\underline{a}$ be any arc. Then*

$$\begin{aligned} p(\Psi(\underline{a})) &= p(\underline{a}) + p_x(\underline{a})\,(x - x_0) + p_y(\underline{a})\,(y - y_0) \\ &\quad + \frac{1}{2}\,p_{xx}(\underline{a})\,(x - x_0)\,(y - y_0) + \cdots \\ &= \sum_{i,j \geq 0} \frac{1}{i\,!}\,\frac{1}{j\,!}\,p_{x^i y^j}(\underline{a})\,(x - x_0)^i\,(y - y_0)^j\,. \end{aligned}$$

[2] In the multivariate case, a better terminology would be a "wedge".

Over our example, Proposition 3 gives:

$$\begin{aligned} p(\Psi(\underline{a})) &= (a_{0,1}\,a_{1,0}^2 - 8\,a_{0,0} + 1) + a_{1,0}\,(2\,a_{0,1}\,a_{2,0} + a_{1,0}\,a_{1,1} + 24\,a_{0,0}^2)\,x + \\ &\quad (2\,a_{1,0}\,a_{0,1}\,a_{1,1} + a_{1,0}^2\,a_{1,1} - 24\,a_{0,0}^2\,a_{0,1})\,y + \cdots \\ p_x(\Psi(\underline{a})) &= a_{1,0}\,(2\,a_{0,1}\,a_{2,0} + a_{1,0}\,a_{1,1} + 24\,a_{0,0}^2) + \\ &\quad (2\,a_{1,0}\,a_{0,1}\,a_{3,0} + a_{1,0}^2\,a_{2,1} + 2\,a_{0,1}\,a_{2,0}^2 + 4\,(a_{1,0}\,a_{1,1} - 6\,a_{0,0}^2)\,a_{2,0} - 48\,a_{0,0}\,a_{1,0}^2)\,x + \cdots \\ &\vdots \end{aligned}$$

The comments following Proposition 2 hold for Proposition 3. In particular, Corollary 1 holds in the partial case. The analysis conducted in Section 1.4.2 should be modified as follows. Consider the differential polynomial (11). The two independent variables are encoded by two extra differential indeterminates x and y. The symbols used for the two derivations are renamed as ξ and η. The extended system associated to (11), which belongs to $\mathscr{F}\{u, x, y\}$, is

$$u_\eta\,u_\xi^2 - 8\,u + 1 = 0\,, \quad x_\xi = 1\,, \quad x_\eta = 0\,, \quad y_\xi = 0\,, \quad y_\eta = 1\,.$$

The expansion point (x_0, y_0) is encoded via initial conditions. In particular, the following arcs are associated to the differential indeterminates x and y

$$\begin{aligned} \underline{x} &= (x_0, 1, 0, \ldots)\,, \\ \underline{y} &= (y_0, 0, 1, 0, \ldots)\,, \end{aligned}$$

so that x and y, viewed as functions of the independent variables ξ and η are

$$\begin{aligned} \Psi(\underline{x}) &= x_0 + \xi\,, \\ \Psi(\underline{y}) &= y_0 + \eta\,. \end{aligned}$$

The rest of the section as well as Section 1.4.3 are easily adapted.

1.6 Denef and Lipshitz Undecidability Result

The following analysis comes from [10, Theorem 4.11]. Let $f \in \mathscr{F}[z]$ be a polynomial in the usual sense. To fix ideas, take

$$f(z) = z^2 - 2\,. \tag{13}$$

Let $p \in \mathscr{F}\{u\}$ be the differential polynomial defined as follows, using f to form some differential operator and applying it to the differential indeterminate u

$$p = f\left(x\,\frac{\mathrm{d}}{\mathrm{d}x}\right) u\,. \tag{14}$$

Over our example, one obtains

$$p = \left(\left(x\,\frac{\mathrm{d}}{\mathrm{d}x}\right)^2 - 2\right) u\,, \quad = \quad x\,\frac{\mathrm{d}}{\mathrm{d}x}\left(x\,\frac{\mathrm{d}}{\mathrm{d}x}\,u\right) - 2\,u\,, \quad = \quad x^2\,\ddot{u} + x\,\dot{u} - 2\,u\,.$$

Fact 1. Fix the expansion point at the origin! If $\underline{a} = (a_0, a_1, \ldots)$ is any arc then

$$p(\Psi(\underline{a})) = \sum_{i \geq 0} a_i\,f(i)\,x^i\,. \tag{15}$$

Fact 2. The following identities hold:

$$\begin{aligned} \frac{1}{1-x} &= \sum_{i\geq 0} x^i\,, \quad \text{and more generally,} \\ \frac{1}{1-x_1}\cdots\frac{1}{1-x_m} &= \sum_{(i_1,\ldots,i_m)\in\mathbb{N}^m} x_1^{i_1}\cdots x_m^{i_m}\,. \end{aligned}$$

Combining the two above facts, we see that the differential polynomial equation

$$\begin{aligned} p &= \frac{1}{1-x}\,, \quad \text{which is equivalent to} \\ (1-x)\,p-1 &= 0 \end{aligned}$$

has a formal power series solution (which is convergent if it exists), centered at the origin, if and only if $a_i = 1/f(i)$ for each $i \in \mathbb{N}$. In particular, the formal power series solution exists if and only if the polynomial f has no positive integer root. This is the case over our example. Indeed, denoting $q = (1-x)\,p-1$ we have

$$\begin{aligned} q(\underline{a}) &= -2\,a_0 - 1\,, \\ \dot{q}(\underline{a}) &= 2\,a_0 - a_1\,, \\ \ddot{q}(\underline{a}) &= 2\,a_1 + 2\,a_2\,, \\ q^{(3)}(\underline{a}) &= -6\,a_2 + 7\,a_3\,, \\ &\vdots \end{aligned}$$

Solving, we get

$$\underline{a} = \left(-\frac{1}{2}, -1, 1, \frac{6}{7}, \ldots\right) = \left(\frac{0\,!}{f(0)}, \frac{1\,!}{f(1)}, \frac{2\,!}{f(2)}, \frac{3\,!}{f(3)}, \ldots\right)$$

This construct generalizes to the partial case. Take any $f \in \mathscr{F}[z_1,\ldots,z_m]$ and form the differential polynomials

$$\begin{aligned} p &= f\left(x_1\,\frac{\partial}{\partial x_1}, \ldots, x_m\,\frac{\partial}{\partial x_m}\right) u\,, \\ q &= (1-x_1)\cdots(1-x_m)\,p - 1\,. \end{aligned}$$

Then q has a formal power series (which is convergent if it exists), centered at the origin, if and only if the polynomial equation $f = 0$ has no positive integer solution. By the negative answer of Yuri Matiyasevich [14] to Hilbert's Tenth Problem, there does not exist any algorithm for determining whether this is the case of not, provided that m is large enough (Matiyasevich result holds at least for $m \geq 9$).

Observe that, in Fact 1, if an expansion point different from the origin is chosen then (15) is not valid anymore and the whole argument collapses.

Indeed, as we shall see, there does exist algorithms which decide the following problem: given a system of differential polynomials $p_1,\ldots,p_r$ of $\mathscr{F}\{u_1,\ldots,u_n\}$ with any number of derivation operators, does there exist an expansion point such that the system has formal power series solutions centered at this point ?

1.7 General Formulas

Let us come back to the general case of the differential polynomial ring $\mathscr{R} = \mathscr{F}\{u_1,\ldots,u_n\}$ endowed with m derivations.

The notion of arc, introduced in the former sections, generalizes in the following straightforward way. To each differential indeterminate u_i of $\mathscr{R}$, one associates an arc $\underline{a}_i$ which is an infinite sequence of elements of $\mathscr{F}$ whose coordinates $a_{i,(e_1,\ldots,e_m)}$ are indexed by multi-indices $(e_1,\ldots,e_m) \in \mathbb{N}^m$.

Formula (12) then generalizes to a formula which maps any tuple of arcs $(\underline{a}_1,\ldots,\underline{a}_n)$ (one arc per differential indeterminate) to a tuple of formal power series

$$\Psi(\underline{a}_i) \quad = \quad \sum_{(e_1,\ldots,e_m)\in\mathbb{N}^m} \frac{1}{e_1\,!\cdots e_m\,!}\, a_{i,(e_1,\ldots,e_m)}\,(x_1 - x_{1,0})^{e_1}\cdots(x_m - x_{m,0})^{e_m}\,, \quad 1 \leq i \leq n\,.$$

A straightforward generalization of Proposition 3 then follows. Corollary 1 may now be generalized as

Proposition 4 *Let $p_1,\ldots,p_r$ be differential polynomials of $\mathscr{F}\{u_1,\ldots,u_n\}$ and $\underline{a} = (\underline{a}_1,\ldots,\underline{a}_n)$ be any tuple of arcs.*

Then the tuple of formal power series $\Psi(\underline{a})$ annihilates the perfect differential ideal $\mathfrak{A} = \{p_1,\ldots,p_r\}$ if and only if this perfect differential ideal evaluates to zero at the tuple of arcs $\underline{a}$.

In the sequel, by a *zero* of a differential ideal $\mathfrak{A}$, we will mean a tuple of arcs $\underline{a}$ over some non specified expansion point or, equivalently, a tuple of formal power series of $\mathscr{F}[[x_1 - x_{1,0},\ldots,x_m - x_{m,0}]]$ where $(x_{1,0},\ldots,x_{m,0}) \in \mathscr{F}^m$. As pointed out in Section 1.4.3, one may also consider that the expansion point is part of the zero and that the expansion point is the origin, provided that $\mathfrak{A}$ contains the equations that encode "independent variables" as differential indeterminates.

If we consider a system of equations $p_1 = \cdots = p_r = 0$ where the p_i are differential polynomials, then, by a *solution* of the system, we will mean a zero of the perfect differential ideal $\{p_1,\ldots,p_r\}$.

2 A Differential Theorem of Zeros

This section is dedicated to the proof of the differential Theorem of Zeros, in terms of arcs, or of formal power series.

It is designed as follows: the approach is essentially the one of Ritt. However, some notions which were not fully designed when Ritt wrote his book (rankings) are modernized using Kolchin's book. Moreover, Ritt's theorems are presented in the general case of partial differential algebra while Ritt's presentation focuses on the ordinary differential case. I have also inserted a few propositions much inspired from papers of Seidenberg.

The title of the next section is a bit overstated: the classical definition of characteristic sets actually is constructive by many aspects. What the title actually tries to express is that, in this section, we only give the properties of characteristic sets which are needed to use them in some nonconstructive way, within the proof of the Ritt-Raudenbush Basis Theorem.

2.1 Characteristic Sets — The Nonconstructive Definition

A sequence of derivative operators

$$\theta_1, \theta_2, \theta_3, \ldots \tag{16}$$

is called a *Dickson sequence* if none of the θ_i divides any of its successors i.e. if, for all $k > i \geq 1$, there does not exist any derivative operator φ such that $\theta_k = \varphi\theta_i$. See Figure 1.

Proposition 5 *(Dickson's Lemma) Every Dickson sequence is finite.*

Proof By induction on the number m of derivation operators. The Proposition is clear if $m = 1$ since every strictly decreasing sequence of nonnegative integers is finite. Assume $m > 1$ and that the Lemma holds for every Dickson sequence built with less than m derivation operators. Denote $\theta_i = \delta_1^{e_i}\varphi_i$ for all $i \geq 1$ where the derivative operators φ_i are free of the derivation operator δ_1. Every infinite sequence of nonnegative integers

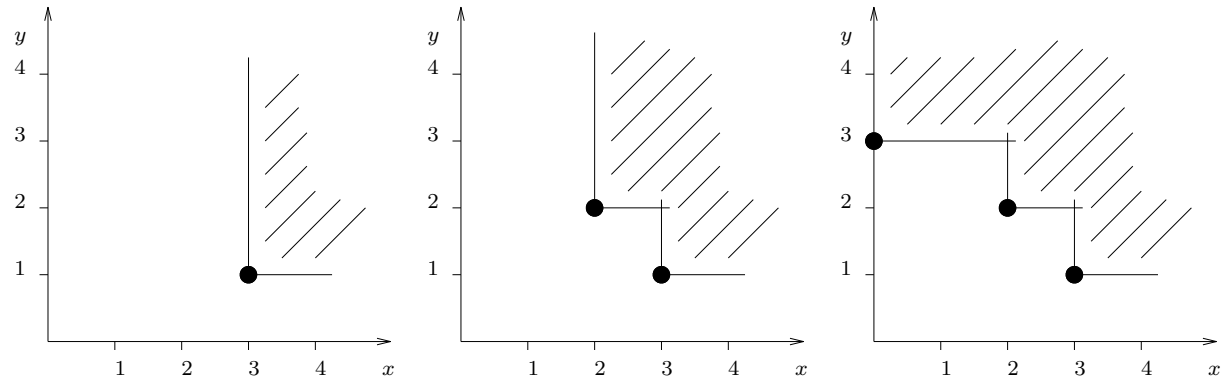

Figure 1: Graphical illustration of the beginning of a Dickson sequence in two derivations $\theta_1, \theta_2, \theta_3 = \delta_x^3\delta_y, \delta_x^2\delta_y^2, \delta_y^3$. Each time a derivative operator is introduced, the set of possible following operators, corresponding to the non shaded area, shrinks. It is clear that all possible prolongations are finite, though it is possible to build sequences of arbitrary length.

contains an infinite increasing subsequence. Thus if some Dickson sequence (16) were infinite, it would contain an infinite subsequence (θ_i) whose orders e_i would be increasing. The corresponding subsequence (φ_i) would then be an infinite Dickson sequence. This contradiction with the induction hypothesis concludes the proof of the Lemma. □

Let $U = \{u_1, \ldots, u_n\}$ be a set of differential indeterminates. A *ranking* [12, chap. I, 8] is a total order on the infinite set ΘU which satisfies the two following axioms, for all derivatives $v, w \in \Theta U$ and every derivative operator $\theta \in \Theta$:

1. $v \leq \theta v$ and
2. $v < w \Rightarrow \theta v < \theta w$.

Proposition 6 *Every ranking is a well-ordering (i.e. every strictly decreasing sequence of derivatives is finite).*

Proof If a strictly decreasing sequence of derivatives were infinite, it would contain an infinite subsequence $(\theta_i u)$ of derivatives of the same differential indeterminate u. The first axiom of rankings implies that the corresponding subsequence of derivative operators (θ_i) is a Dickson sequence. By Dickson's Lemma, such a sequence cannot be infinite. □

Let $\mathscr{R} = \mathscr{F}\{u_1, \ldots, u_n\}$ be a differential polynomial ring. Fix any ranking and consider some differential polynomial $p \in \mathscr{R} \setminus \mathscr{F}$.

The *leading derivative* (the *leader* in Kolchin's terminology) of p is the highest derivative v such that $\deg(p, v) > 0$.

Let v be the leading derivative of p and $d = \deg(p, v)$.

The *rank* of p is the monomial v^d.

The ranking induces a *total ordering on ranks* as follows. A rank v^d is said to be less than a rank w^e if $v < w$ with respect to the ranking or $v = w$ and $d < e$. It is convenient to extend the above definitions by introducing some artificial rank, common to all nonzero elements of $\mathscr{F}$ and considering that it is strictly less than the rank of any element of $\mathscr{R} \setminus \mathscr{F}$. If p, q are two nonzero differential polynomials, we will write $p < q$ to express the fact that the rank of p is strictly less than the one of q. Proposition 6 implies that any such ordering on ranks is a well-ordering.

The *initial* of p is the leading coefficient of p, viewed as a univariate polynomial in v. In general, the *initial* of p is a differential polynomial of $\mathscr{R}$. If A is a set of differential polynomials, we will write "the initials of A" instead of "the initials of the elements of A".

The *separant* of p is the differential polynomial $\partial p/\partial v$. If A is a set of differential polynomials, we will write "the separants of A" instead of "the separants of the elements of A".

Axioms of rankings imply:

1. the initial and the separant of p have ranks less than the rank v^d of p;
2. any proper derivative θp of p has rank θv; its initial is the separant of p.

Let $q \in \mathscr{R}$ and $p \in \mathscr{R} \setminus \mathscr{F}$ be two differential polynomials. Let p have rank v^d.

The differential polynomial q is said to be *partially reduced* with respect to p if it does not depend on any proper derivative of v i.e. if, for every proper derivative operator θ, we have $\deg(q, \theta v) = 0$.

The differential polynomial q is said to be *reduced* with respect to p if it is partially reduced with respect to p and $\deg(q, v) < d$.

Autoreduced Sets. A set of differential polynomials $A \subset \mathscr{R} \setminus \mathscr{F}$ is said to be *autoreduced* if its elements are pairwise reduced with respect to each other i.e. if, for every pair (p, q) of distinct elements of A, we have q reduced with respect to p.

Proposition 7 *Every autoreduced set is finite.*

Proof Let A be an autoreduced set. If A were infinite, it would contain an infinite subset of differential polynomials whose leading derivatives $\theta_i u$ would be derivatives of the same differential indeterminate u. Enumerating the corresponding derivative operators θ_i according to any order, one gets a Dickson sequence. By Dickson's Lemma, such a sequence cannot be infinite. Thus A is finite. □

Let A be an autoreduced set and $p \in \mathscr{R} \setminus \mathscr{F}$ be a differential polynomial reduced with respect to A (i.e. with respect to all elements of A). Then $B = A \cup \{p\}$ is not autoreduced but, if one removes from B any differential polynomial which is not reduced with respect to p, one gets another autoreduced set A'. This process can actually be viewed as an extremely simplified version of some "completion process". It plays an important role in the theory. The following definition actually permits us to say that A' is lower than A.

Ordering on Autoreduced Sets. Let $A = \{p_1, \ldots, p_r\}$ and $A' = \{p'_1, \ldots, p'_{r'}\}$ be two autoreduced sets such that $p_1 < \cdots < p_r$ and $p'_1 < \cdots < p'_{r'}$. The set A' is said to be *lower than* the set A if

1. there exists some index $j \in [1, \min(r, r')]$ such that $p'_j < p_j$ and the two subsets $\{p_1, \ldots, p_{j-1}\}$ and $\{p'_1, \ldots, p'_{j-1}\}$ have the same set of ranks ; or
2. no such j exists and $r < r'$ (longer sets are lower).

Observe that the above relation is transitive [17, chap. I, 4] and defines a total ordering on autoreduced sets of ranks. The proof of the following proposition comes from [12, chap. I, 10, Proposition 3].

Proposition 8 *Every nonempty set of autoreduced sets contains a minimal element.*

Proof Let $\mathscr{A}$ be a nonempty set of autoreduced sets. Define an infinite sequence

$$\mathscr{A} = \mathscr{A}_0 \supset \mathscr{A}_1 \supset \mathscr{A}_2 \supset \cdots$$

by defining $\mathscr{A}_i$ $(i > 0)$ as the set of all the autoreduced sets belonging to $\mathscr{A}_{i-1}$, which involve at least i elements, and whose ith element has lowest possible rank, $v_i^{d_i}$. If all the subsets $\mathscr{A}_i$ were nonempty then the set of all (v_i) would form an infinite autoreduced set: a condraction to Proposition 7. Thus there exists some $i \geq 0$ such that $\mathscr{A}_i$ is nonempty and $\mathscr{A}_j = \varnothing$ for $j > i$. Any element of $\mathscr{A}_i$ is a minimal element of $\mathscr{A}$. □

The next Proposition actually is nothing but a restatement of Proposition 8.

Proposition 9 *Every strictly decreasing sequence of autoreduced sets is finite.*

Proof By Proposition 7. □

If Σ is any subset of $\mathscr{R}$ then Σ contains autoreduced subsets (the empty set is an autoreduced set). Any minimal autoreduced subset of Σ is called a *characteristic set* of Σ.

The next proposition is emphasized in [17, chap. I, 5].

Proposition 10 *Let Σ be any subset of $\mathscr{R}$, A be a characteristic set of Σ and $p \in \mathscr{R} \setminus \mathscr{F}$ be a differential polynomial reduced with respect to A.*

Denote $\Sigma + p$ the set obtained by adjoining p to Σ.

The characteristic sets of $\Sigma + p$ are lower than A.

Corollary 2 *Let Σ be any subset of $\mathscr{R}$ and A be a characteristic set of Σ. Then Σ does not contain any differential polynomial of $\mathscr{R} \setminus \mathscr{F}$, reduced with respect to A.*

2.2 Ritt's Reduction Algorithms

Let f, g be two polynomials of $\mathscr{S}[x]$, where $\mathscr{S}$ is a ring and $\deg(g, x) > 0$, one denotes $\mathsf{prem}(f, g, x)$ the pseudoremainder of f by g (it is the polynomial $r(x)$ mentioned in [22, chap. I, 17, Theorem 9, page 30]).

Let now $A \subset \mathscr{R} \setminus \mathscr{F}$ be a finite set of differential polynomials and $f \in \mathscr{R}$ be a differential polynomial.

The *partial remainder* of f by A, denoted $\mathsf{partialrem}(f, A)$ is defined inductively as follows:

1. if f is partially reduced with respect to all elements of A then $\mathsf{partialrem}(f, A) = f$ else
2. there must exist some $p \in A$ with leading derivative v and some proper derivative operator θ such that $\deg(f, \theta v) > 0$. Among all such triples (p, v, θ), choose one such that θv is maximal with respect to the ranking. Then $\mathsf{partialrem}(f, A) = \mathsf{partialrem}(\mathsf{prem}(f, \theta p, \theta v), A)$.

The following example is useful in Section 3.4.1. Take $f = \ddot{u} + v$ and A made of a single differential polynomial $p = \dot{u}^2 + v$. The leading derivative of p is $\dot{u}$. The differential polynomial f is not partially reduced with respect to p. Differentiating, we get $\dot{p} = 2\,\dot{u}\,\ddot{u} + \dot{v}$. The pseudodivision of f by $\dot{p}$ computes the following relation. The differential polynomial g is the partial remainder of f by p.

$$\underbrace{2\,\dot{u}}_{h}\,\underbrace{(\ddot{u} + v)}_{f} \quad = \quad \underbrace{1}_{q} \times \underbrace{(2\,\dot{u}\,\ddot{u} + \dot{v})}_{\dot{p}} + \underbrace{(2\,v\,\dot{u} - \dot{v})}_{g}\,. \tag{17}$$

Proposition 11 *Let $A \subset \mathscr{R} \setminus \mathscr{F}$ be a finite set of differential polynomials, $f \in \mathscr{R}$ be a differential polynomial and $g = \mathsf{partialrem}(f, A)$. Then g is partially reduced with respect to A and there exists a power product h of the separants of A such that*

$$h\,f \quad = \quad g \mod [A]\,. \tag{18}$$

The *full remainder* of f by A, denoted $\mathsf{fullrem}(f, A)$, is defined as follows. Denote $A = \{p_1, \ldots, p_r\}$, assuming $p_1 < \cdots < p_r$.

1. if f is reduced with respect to all elements of A then $\mathsf{fullrem}(f, A) = f$ else
2. if f is not partially reduced with respect to A then $\mathsf{fullrem}(f, A) = \mathsf{fullrem}(\mathsf{partialrem}(f, A), A)$ else
3. there must exist some index $i \in [1, r]$ such that $\deg(f, v_i) \geq \deg(p_i, v_i)$ where v_i denotes the leading derivative of p_i. Among all such indices i, fix the maximal one. Then define $\mathsf{fullrem}(f, A)$ as $\mathsf{fullrem}(\mathsf{prem}(f, p_i, v_i), A)$.

The following example is useful in Section 3.4.2. Take $f = 2\,u\,u_y\,v_{xy} + 2\,u_y^2\,v_x - 4\,u_x$ and $A = p_1, p_2, p_3$ with $p_1 = u_y^2 - 4\,u$, $p_2 = u_x - v_x\,u$ and $p_3 = v_y$. The leading derivatives are u_y, u_x and v_y. The reduction of f is achieved by three pseudodivisions. The full remainder is g_3. The power product $h = h_1\,h_2\,h_3 = 1$.

$$\begin{aligned}
\underbrace{1}_{h_1} \times \underbrace{(2\,u\,u_y\,v_{xy} + 2\,u_y^2\,v_x - 4\,u_x)}_{f} &= \underbrace{2\,u\,u_y}_{q_1}\,\underbrace{v_{xy}}_{\delta_x p_3} + \underbrace{2\,u_y^2\,v_x - 4\,u_x}_{g_1}\,, \\
\underbrace{1}_{h_2} \times \underbrace{(2\,u_y^2\,v_x - 4\,u_x)}_{g_1} &= \underbrace{2\,v_x}_{q_2}\,\underbrace{(u_y^2 - 4\,u)}_{p_1} + \underbrace{8\,u\,v_x - 4\,u_x}_{g_2}\,, \\
\underbrace{1}_{h_3} \times \underbrace{(8\,u\,v_x - 4\,u_x)}_{g_2} &= \underbrace{-4}_{q_3} \times \underbrace{(u_x - v_x\,u)}_{p_2} + \underbrace{4\,u\,v_x}_{g_3}\,.
\end{aligned} \tag{19}$$

Proposition 12 *Let $A \subset \mathscr{R} \setminus \mathscr{F}$ be a finite set of differential polynomials, $f \in \mathscr{R}$ be a differential polynomial and $g = \mathsf{fullrem}(f, A)$. Then g is reduced with respect to A and there exists a power product h of the initials and the separants of A such that*

$$h\,f \quad = \quad g \mod [A]\,. \tag{20}$$

2.3 Characteristic Sets of Prime Differential Ideals

Consider a prime differential ideal $\mathfrak{P}$ different from $\mathscr{R}$. Assume a ranking is fixed and a characteristic set A of $\mathfrak{P}$ is known.

Proposition 13 *Let f be any differential polynomial of $\mathscr{R}$. Then $\mathsf{fullrem}(f, A) = 0$ if and only if $f \in \mathfrak{P}$.*

Proof Denote $g = \mathsf{fullrem}(f, A)$. The implication $\Leftarrow$ from right to left. Assume $f \in \mathfrak{P}$. Since $A \subset \mathfrak{P}$ we have $g \in \mathfrak{P}$ by the relation (20) of Proposition 12. The differential polynomial g cannot belong to $\mathscr{R} \setminus \mathscr{F}$ by Corollary 2, since it is reduced with respect to all elements of A. It cannot be a nonzero element of $\mathscr{F}$ because $\mathfrak{P} \neq \mathscr{R}$. Thus $g = 0$.

The implication $\Rightarrow$ from left to right. Assume $g = 0$. Then the product $h\,f \in \mathfrak{P}$. By Corollary 2, the initials and separants of A do not belong to $\mathfrak{P}$ since they are reduced with respect to all elements of A. Since h is a power product of these initials and separants and $\mathfrak{P}$ is prime, we have $f \in \mathfrak{P}$. □

The following notations are defined in [12, chap. 0, 1; and chap. I, 9]. In Kolchin's book, the notation $[A] : H_A^\infty$ seems to occur for the first time in [12, chap. IV, 9, Lemma 2].

If S is a subset and $\mathfrak{A}$ is an ideal of $\mathscr{R}$ then $\mathfrak{A} : S^\infty$ is the ideal of the elements $p \in \mathscr{R}$ such that, for some power product h of elements of S, we have $h\,p \in \mathfrak{A}$ (if $\mathfrak{A}$ is a differential ideal, so is $\mathfrak{A} : S^\infty$). An alternative definition is provided by means of a localization [13, chap. II, 3]: if M denotes the multiplicative family generated by S and $M^{-1}\mathfrak{A}$ denotes the ideal generated by $\mathfrak{A}$ in the localized ring $M^{-1}\mathscr{R}$, then $\mathfrak{A} : S^\infty = M^{-1}\mathfrak{A} \cap \mathscr{R}$.

Denote now H_A the set of the initials and separants of A. Proposition 13 implies that, if A is a characteristic set of a prime differential ideal $\mathfrak{P}$ then

$$\mathfrak{P} \quad = \quad [A] : H_A^\infty\,.$$

2.4 The Ritt-Raudenbush Basis Theorem

The differential polynomial ring is $\mathscr{R} = \mathscr{F}\{u_1, \ldots, u_n\}$. The two next propositions are slight adaptations of [17, chap. I, 10].

Proposition 14 *Let f, g be two differential polynomials and $\mathfrak{A}$ be a perfect differential ideal of $\mathscr{R}$ such that $f\,g \in \mathfrak{A}$. Then, for all derivative operators θ, φ, the product $(\theta f)\,(\varphi g) \in \mathfrak{A}$.*

Proof The proof is by induction on the sum of the orders of the derivative operators θ and φ. The basis of the induction (case of two operators of order zero) holds by assumption. Assume that the Proposition holds for all derivative operators θ, φ such that the sum of their orders is equal to some positive integer and consider any derivation operator δ. Then, differentiating $(\theta f)(\varphi g)$, we have $(\delta\theta f)(\varphi g) + (\theta f)(\delta\varphi g) \in \mathfrak{A}$ Multiply by θf and use the fact that $(\theta f)(\varphi g) \in \mathfrak{A}$ (induction hypothesis). Then $(\theta f)^2(\delta\varphi g) \in \mathfrak{A}$ and, since $\mathfrak{A}$ is perfect, $(\theta f)(\delta\varphi g) \in \mathfrak{A}$. The fact that $(\delta\theta f)(\varphi g) \in \mathfrak{A}$ is proved similarly. □

Following [17, chap. I, 9], in order to reduce possible confusion on the meaning of curly braces, if p is a differential polynomial and Σ is a set, we will often denote $\Sigma + p$ the set obtained by adjoining p to Σ.

Proposition 15 *Let f, g be two differential polynomials and Σ be a set of differential polynomials of $\mathscr{R}$. Then $\{\Sigma + f\,g\} = \{\Sigma + f\} \cap \{\Sigma + g\}$.*

Proof The inclusion $\subset$ is clear. Let us prove the converse one. Let $h \in \{\Sigma + f\} \cap \{\Sigma + g\}$. Then there exists differential polynomials $p, q \in [\Sigma]$, $\overline{f} \in [f]$, $\overline{g} \in [g]$ and, by Proposition 1, a positive integer t such that $h^t = p + \overline{f}$ and $h^t = q + \overline{g}$. Multiply these two equalities termwise. Then there exists a differential polynomial $r \in [\Sigma]$ such that $h^{2t} = r + \overline{f}\,\overline{g}$. Since $\overline{f} \in [f]$ and $\overline{g} \in [g]$, there exists finitely many differential polynomials $m_{\theta,\varphi}$ such that

$$\overline{f}\,\overline{g} \quad = \quad \sum_{\theta,\varphi \in \Theta} m_{\theta,\varphi}\,(\theta f)(\varphi g)\,.$$

The product $f\,g \in \{\Sigma + f\,g\}$. Thus, by Proposition 14, every product $(\theta f)(\varphi g) \in \{\Sigma + f\,g\}$. Thus we have $h \in \{\Sigma + f\,g\}$. □

The remaining part of this section comes from [17, chap. I, 12-16]. Let Σ be an infinite subset of $\mathscr{R}$. A subset Φ of Σ is said to be a *basis* of Σ if Φ is finite and $\Sigma \subset \{\Phi\}$.

Lemma 2 *Let Σ be an infinite subset of $\mathscr{R}$. If Σ contains a nonzero element of $\mathscr{F}$ then Σ has a basis.*

Proof Let a be any nonzero element of $\Sigma \cap \mathscr{F}$. Then the set $\{a\}$ is a basis of Σ. □

Theorem 1 *(Ritt-Raudenbush Basis Theorem) Every infinite subset of $\mathscr{R}$ has a basis.*

Proof We assume that there exists infinite subsets of $\mathscr{R}$ with no basis and seek a contradiction. Let Σ be such a subset and assume moreover that, among all infinite sets with no basis, Σ is such that its characteristic sets are minimal.

Let A be a characteristic set of Σ.

"Perform" Ritt's full reduction algorithm, with respect to A, over all $q \in \Sigma \setminus A$. For each $q \in \Sigma \setminus A$, there exists a power product h_q of initials and separants of A and a differential polynomial g_q, reduced with respect to A such that

$$h_q\,q \quad = \quad g_q \mod [A]\,. \tag{21}$$

Introduce the two following sets (the plus sign standing for "union"):

$$\begin{aligned} \Lambda &= \{h_q\,q \mid q \in \Sigma \setminus A\} + A\,, \\ \Omega &= \{g_q \mid q \in \Sigma \setminus A\} + A\,. \end{aligned}$$

The set Ω must have a basis. Indeed, if it contains any nonzero element of $\mathscr{F}$ it has a basis by Lemma 2. Otherwise, since the differential polynomials g_q are reduced with respect to A, its characteristic sets are lower than A by Proposition 10 thus it cannot lack a basis by the minimality assumption on Σ.

Thus there exists finitely many differential polynomials $q_1, \ldots, q_t \in \Sigma \setminus A$ such that the set $\Phi = \{g_{q_1}, \ldots, g_{q_t}\} + A$ is a basis of Ω (observe that is is always possible to enlarge a basis with finitely many further differential polynomials).

Claim: the set $\Psi = \{h_{q_1}\, q_1, \ldots, h_{q_t}\, q_t\} + A$ is a basis of Λ.

Each $h_{q_i}\, q_i - g_{q_i}$ $(1 \leq i \leq t)$, belongs to the perfect differential ideals $\{\Phi\}$ and $\{\Psi\}$ by Proposition 12 and the fact that A is a subset of both Φ and Ψ.

Thus, since each $g_{q_i} \in \Phi$ $(1 \leq i \leq t)$, we see that each $h_{q_i}\, q_i \in \{\Phi\}$ $(1 \leq i \leq t)$ and $\Psi \subset \{\Phi\}$. Conversely, since each $h_{q_i}\, q_i \in \Psi$, we see that each $g_{q_i} \in \{\Psi\}$ and $\Phi \subset \{\Psi\}$. Thus both perfect differential ideals $\{\Phi\}$ and $\{\Psi\}$ are equal.

Since Φ is a basis of Ω we have $\Omega \subset \{\Phi\}$. Since the full remainder g_q of each $q \in \Sigma$ belongs to Ω, we see that the corresponding product $h_q\, q$ of each $q \in \Sigma$ belongs to $\{\Omega\}$, which is included in $\{\Phi\} = \{\Psi\}$. Thus $\Lambda \subset \{\Psi\}$ and the claim is proved.

Let $f_1, \ldots, f_s$ denote the initials and separants of A. By Lemma 3, there exists an index $1 \leq i \leq s$ such that the set $\Sigma + f_i$ has no basis. The differential polynomial $f_i \notin \mathscr{F}$ by Lemma 2. Thus the set $\Sigma + f_i$ has a characteristic set lower than A by Proposition 10. This contradiction with the minimality assumption on Σ completes the proof of the Theorem. □

The next Lemma is involved in the proof of the Ritt-Raudenbush Basis Theorem. The differential polynomials f_i actually are the initials and separants of some characteristic set of Σ.

Lemma 3 *Let Σ be an infinite subset of $\mathscr{R}$ and $f_1, \ldots, f_s$ be differential polynomials of $\mathscr{R}$. Let*

$$\Lambda \quad = \quad \{h_q\, q \mid q \in \Sigma \text{ and } h_q \text{ is some power product of } f_1, \ldots, f_s\}\,.$$

If Σ has no basis and Λ has a basis then at least one of the sets $\Sigma + f_i$, for $1 \leq i \leq s$, has no basis.

Proof We assume that all sets $\Sigma + f_i$ $(1 \leq i \leq s)$ have a basis and seek a contradiction.

Let $\Psi = \{h_{q_1}\, q_1, \ldots, h_{q_t}\, q_t\}$ be a basis of Λ. Since a basis can always be enlarged as long as it remains finite, there exists some finite set $\Phi \subset \Sigma$ such that: 1) $\Phi + f_i$ is a basis of $\Sigma + f_i$ $(1 \leq i \leq s)$ and; 2) $q_1, \ldots, q_t \in \Phi$. Let g denote the product $f_1 \cdots f_s$.

By Proposition 15, the perfect differential ideal $\{\Sigma + g\}$ is the intersection of the perfect differential ideals $\{\Sigma + f_i\}$ $(1 \leq i \leq s)$; similarly, the perfect differential ideal $\{\Phi + g\}$ is the intersection of the perfect differential ideals $\{\Phi + f_i\}$. Since each $\Phi + f_i$ is a basis of $\Sigma + f_i$ we have

$$\{\Sigma + g\} \quad = \quad \bigcap_{i=1}^{s} \{\Sigma + f_i\} \quad \subset \quad \bigcap_{i=1}^{s} \{\Phi + f_i\} \quad = \quad \{\Phi + g\}\,.$$

Thus $\Phi + g$ is a basis of $\Sigma + g$.

Thus, for each differential polynomial $p \in \Sigma$, there exists a relation

$$p^d \quad = \quad r + m_1\, \theta_1 g + \cdots + m_e\, \theta_e g$$

where $d \geq 1$, $e \geq 0$, the m_i are differential polynomials of $\mathscr{R}$ and $r \in [\Phi]$. Multiplying by p we get

$$p^{d+1} \quad = \quad r\, p + m_1\, p\, \theta_1 g + \cdots + m_e\, p\, \theta_e g \tag{22}$$

Since $q_1, \ldots, q_t \in \Phi$ we have $\Psi \subset \{\Phi\}$. Since, moreover, $p \in \Sigma$ and g is the product of the f_i, we have $p\, g \in \{\Lambda\} \subset \{\Psi\} \subset \{\Phi\}$. Thus, by Proposition 15, we have $p\, \theta_i g \in \{\Phi\}$ for $1 \leq i \leq e$. Since $r \in [\Phi]$ we have $r\, p \in \{\Phi\}$. Thus, using (22), we have $p \in \{\Phi\}$, which means that Φ is a basis of Σ: the sought contradiction. □

Corollary 3 *Let $\mathfrak{A}$ be a perfect differential ideal of $\mathscr{R}$. Then there exists a finite $\Phi \subset \mathfrak{A}$ such that $\mathfrak{A} = \{\Phi\}$.*

Theorem 2 *Every perfect differential ideal $\mathfrak{A}$ is a finite intersection of prime differential ideals.*

Proof We assume that there exists some perfect differential ideal $\mathfrak{A}$ with no such presentation and seek a contradiction. The perfect differential ideal $\mathfrak{A}$ thus cannot be prime. Let f, g be two differential polynomials such that the product $f\,g \in \mathfrak{A}$ but $f, g \notin \mathfrak{A}$. By Proposition 14 we have $\mathfrak{A} = \{\mathfrak{A} + f\} \cap \{\mathfrak{A} + g\}$. At least one of these two perfect differential ideals — say $\mathfrak{A}_1 = \{\mathfrak{A} + f\}$ — is not a finite intersection of prime differential ideals; and we have $\mathfrak{A} \subsetneq \mathfrak{A}_1$. Repeating this argument, we see that there exists an infinite sequence of perfect differential ideals

$$\mathfrak{A} \subsetneq \mathfrak{A}_1 \subsetneq \mathfrak{A}_2 \subsetneq \cdots \tag{23}$$

Let Ω be the union of all these ideals. By the Ritt-Raudenbush Basis Theorem, there exists a finite set $\Phi \subset \Omega$ such that $\Omega \subset \{\Phi\}$. The set Φ must be a subset of some $\mathfrak{A}_t$ in (23). Thus $\mathfrak{A}_{t+1} \subset \{\Phi\} \subset \mathfrak{A}_t$. This contradiction with the fact that the inclusions of (23) are strict completes the proof of the Theorem. □

Let $\mathfrak{A}$ be a perfect differential ideal of $\mathscr{R}$. A representation

$$\mathfrak{A} \quad = \quad \mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_\varrho \tag{24}$$

of $\mathfrak{A}$ as an intersection of prime differential ideals $\mathfrak{P}_i$ is said to be *minimal* if, for all indices $1 \leq i, j \leq \varrho$ such that $i \neq j$ we have $\mathfrak{P}_i \not\subset \mathfrak{P}_j$. Anticipating on Theorem 3, these prime differential ideals are uniquely defined. Ritt calls them the *essential prime divisors* of $\mathfrak{A}$ [17, chap. I, 17]. We prefer to call them the *essential components* of $\mathfrak{A}$.

Theorem 3 *There exists a unique minimal representation of a perfect differential ideal $\mathfrak{A}$ as a finite intersection of prime differential ideals.*

Proof The existence comes from Theorem 2.

For the uniqueness, fix some representation (24). It suffices to prove that if $\mathfrak{P}$ is a prime differential ideal such that $\mathfrak{A} \subset \mathfrak{P}$ then there exists some index $1 \leq i \leq \varrho$ such that $\mathfrak{P}_i \subset \mathfrak{P}$. If this were not the case then each $\mathfrak{P}_i$ would contain some differential polynomial f_i such that $f_i \notin \mathfrak{P}$ $(1 \leq i \leq \varrho)$. Since $\mathfrak{P}$ is prime, the product $f = f_1 \cdots f_\varrho$ would not belong to $\mathfrak{P}$ either. However, it would belong to $\mathfrak{A}$. This contradiction with the hypothesis $\mathfrak{A} \subset \mathfrak{P}$ completes the proof of the Theorem. □

The following example comes from [17, chap. II, 8].

$$\{\dot{u}^2 - 4\,u\} \quad = \quad [\dot{u}^2 - 4\,u\,, \ddot{u} - 2] \cap [u]\,.$$

The differential polynomial $\dot{u}^2 - 4\,u$ is irreducible but its first derivative actually factors as $2\,\dot{u}\,(\ddot{u} - 2)$. The perfect differential ideal on the left hand side of (25) is not prime. It has two essential components, given on the right hand side of (25). The solution of the first component is the family of parabolas $(x + c)^2$ where c is an arbitrary constant. The solution of the second component is the zero function. The singleton $\dot{u}^2 - 4\,u$ is a characteristic set of the prime differential ideal $[\dot{u}^2 - 4\,u\,, \ddot{u} - 2]$.

A variant comes from [17, chap II, 19]. The perfect differential ideal generated by $\dot{u}^2 - 4\,u^3$ is actually prime. Its solution is the family of functions $(x + c)^{-2}$ where c is an arbitrary constant. The zero function also is a solution but (quoting Ritt) "we see, letting $|c|$ increase, that a differential polynomial which vanishes for every $(x+c)^{-2}$ vanishes for $u = 0$. Thus $u = 0$ is in the general solution". The prime differential ideal $[u]$ is not an essential component of $\{\dot{u}^2 - 4\,u^3\}$. See also [12, chap. IV, 15, Remark 1].

2.5 Zeros of a Prime Differential Ideal

This section is much inspired by papers of Seidenberg. See the proof of [19, Theorem 6].

The differential polynomial ring is $\mathscr{R} = \mathscr{F}\{u_1, \ldots, u_n\}$ endowed with m derivations. Since we are going to solve polynomial systems and look for solutions in $\mathscr{F}$, there are constraints on $\mathscr{F}$. The content of this section

is valid if $\mathscr{F}$ is a universal field extension of the field $\mathbb{Q}$ of the rational numbers (i.e. if $\mathscr{F}$ is algebraically closed and has an infinite transcendence degree over $\mathbb{Q}$) [22, chap. VI, 5bis]. To fix ideas, we may consider that $\mathscr{F}$ is the field $\mathbb{C}$ of the complex numbers.

Consider a prime differential ideal $\mathfrak{P}$ different from $\mathscr{R}$. Assume a ranking is fixed and a characteristic set A of $\mathfrak{P}$ is known. Denote $p_1, \ldots, p_r$ the elements of A and assume $p_1 < \cdots < p_r$.

Denote X the finite set of the derivatives A depends on, including the extra differential indeterminates used to encode the "independent variables" in the extended system associated to A, in the sense of Section 1.4.3.

Denote $V \subset X$ the set of leading derivatives of A. Then $\Theta U \setminus \Theta V$ denotes the possibly infinite set of the elements of ΘU which are not the derivative of any element of V. Let Θ^* denote the set of all proper derivative operators. Then $\Theta^* V$ denotes the set of all derivatives which are proper derivatives of some element of V. The three sets $V, \Theta U \setminus \Theta V$ and $\Theta^* V$ are pairwise disjoint. Their union is ΘU.

Process. The following process defines an expansion point and a tuple of arcs $\underline{a}$.

1. Solve the following system as a nondifferential polynomial system of $\mathscr{F}[X]$, where h denotes the product of the initial and separants of A
$$p_1 = \cdots = p_r = 0\,, \quad h \neq 0\,.$$

2. Assign any value from $\mathscr{F}$ to the derivatives of $\Theta U \setminus \Theta V$ and to the "independent variables" encoding differential indeterminates which were not already assigned values at Step 1.

3. Let v be any element of $\Theta^* V$. By Ritt's partial reduction process, compute a power product h of separants of A and a differential polynomial g such that
$$h\, v \quad = \quad g \mod [A]\,. \tag{25}$$
Then assign to v the value of g/h.

A few remarks:

- the polynomial system to be solved at Step 1 is triangular in the sense that each equation $p_i = 0$ introduces at least one indeterminate;
- if the field $\mathscr{F}$ is the field of the complex numbers, which is algebraically closed, the polynomial system to be solved has solutions;
- since the differential indeterminates which encode the "independent variables" belong to X, the constraint $h \neq 0$ may forbid some expansion points;
- at the end of Step 2, the expansion point is fixed;
- at Step 3, the differential polynomials h and g depend on derivatives which were assigned values at Steps 1 and 2.

As an example, let us consider the differential polynomial $p = x^2\,\ddot{u} + x\,\dot{u} - 2\,u$ from Section 1.6, formula (14). We have $X = \{x, u, \dot{u}, \ddot{u}\}$ and $V = \{\ddot{u}\}$ and $\Theta U \setminus \Theta V = \varnothing$. The system of $\mathscr{F}[x, u, \dot{u}, \ddot{u}]$ to be solved at Step 1 is
$$x^2\,\ddot{u} + x\,\dot{u} - 2\,u = 0\,, \quad x \neq 0\,.$$
The constraint thus imposes that the first coordinate x_0 of the arc $\underline{x} = (x_0, 1, 0, \ldots)$ assigned to x is different from zero. With other words, the origin is not allowed as an expansion point by the process. However, (14) comes from the polynomial (13) which has no positive integer solution. Thus, as seen in Section 1.6, the differential polynomial p has a formal power series for $x_0 = 0$. In summary, the system to be solved at Step 1 may forbid more expansion points than necessary.

Proposition 16 *The tuple of arcs $\underline{a}$ or equivalently the formal power series $\Psi(\underline{a})$ defined by the above process provides a zero of the prime differential ideal $\mathfrak{P}$.*

Proof The proof is by induction on the leading derivative v of the differential polynomials $f \in \mathfrak{P}$, ordered by the ranking. This transfinite induction [21, chap. 9, 4] is allowed by Proposition 6.

Basis. Thanks to Proposition 13, the elements $f \in \mathfrak{P}$ with lowest leading derivative satisfy $h\,f = q\,p_1$ where h is a power of the initial of p_1 (the lowest element of A) and q is some differential polynomial. Since p_1 is annihilated by $\underline{a}$ and h is not, the differential polynomial f must vanish.

General case. Let v be the leading derivative of some $f \in \mathfrak{P}$. Assume (induction hypothesis) that every element of $\mathfrak{P}$ with leading derivative less than v is annihilated by $\underline{a}$. We may assume, without loss of generality, that the initial of f does not belong to $\mathfrak{P}$. Thus, thanks to Proposition 13, we must have $v \in \Theta V$.

Subcase 1. Assume $v \in V$. Perform Ritt's full reduction algorithm over f. Then there exists a power product h of initials and separants of A such that $h\,f \in [A]$ by Propositions 12 and 13. Observe now that, in this reduction process, the first pseudodivision is performed with respect to the differential polynomial $p_i \in A$ with leading derivative v. The following pseudodivisions are performed with respect to differential polynomials of ΘA with leading derivatives strictly less than v; and the differential polynomial h does not depend either on any derivative greater than or equal to v. Removing all the elements of ΘA which are annihilated according to the induction hypothesis, we see that there exists a differential polynomial q such that $h\,f = q\,p_i$. Since p_i is annihilated by $\underline{a}$ and h is not, the differential polynomial f must vanish.

Subcase 2. Assume $v \in \Theta^* V$ and that there is a single differential polynomial $p_i \in A$, with leading derivative v_i such that, for some $\theta \in \Theta^*$, we have $v = \theta v_i$.

Consider Ritt's partial reduction (25) which yielded the value of v. In this reduction process, the first pseudodivision is performed with respect to θp_i and since the differential polynomial to be reduced is a mere derivative, the first pseudoquotient is 1. Then, argumenting as in Subcase 1 and removing all the elements of ΘA which are annihilated according to the induction hypothesis, we see that $h\,v = g + \theta p_i$. Since the value assigned to v is g/h, we see that θp_i vanishes at $\underline{a}$.

Perform now Ritt's full reduction algorithm over f. Then there exists a power product h of initials and separants of A such that $h\,f \in [A]$ by Proposition 12. Argumenting as in Subcase 1 and removing all the elements of ΘA which are annihilated according to the induction hypothesis, we see that there exists a differential polynomial q such that $h\,f = q\,\theta p_i$. Since θp_i is annihilated by $\underline{a}$ and h is not, the differential polynomial f must vanish.

Subcase 3. Assume $v \in \Theta^* V$ and that there exist many different (say two) differential polynomials $p_i, p_j \in A$, with leading derivatives v_i, v_j such that, for some $\theta_i, \theta_j \in \Theta^*$, we have $v = \theta_i v_i = \theta_j v_j$.

One of these two differential polynomials (say p_i) was used to assign a value to v. As proved in Subcase 2, the differential polynomial $\theta_i p_i$ is annihilated by $\underline{a}$.

Denote s_i and s_j the separants of p_i and p_j. The cross derivative $s_j\,\theta_i p_i - s_i\,\theta_j p_j$ belongs to $\mathfrak{P}$ and either is zero or has a leading derivative strictly less than v. Thus it is annihilated by $\underline{a}$, according to the induction hypothesis. Since $\theta_i p_i$ is annihilated and the separants are not, the differential polynomial $\theta_j p_j$ must vanish also.

Perform now Ritt's full reduction algorithm over f. Argumenting as in Subcase 2, we see that f must vanish at $\underline{a}$ also. □

In the proof of the next Proposition, some field $\mathscr{D}$ is introduced. This field seems to be a *field of definition*, which is a notion introduced in [12, chap. III, 3].

Proposition 17 *Let f be a differential polynomial and $\mathfrak{P}$ be a prime differential ideal of $\mathscr{R}$.*
If $f \notin \mathfrak{P}$ then $\mathfrak{P}$ has a zero which does not annihilate f.

Proof The idea of the proof consists in proving that $\mathfrak{P}$ has a *generic* (or *general*) zero i.e. a zero which only annihilates the elements of $\mathfrak{P}$. A zero $\underline{a}$ is generic if $\mathscr{F}(\underline{a})$ is isomorphic to the field of fractions of $\mathscr{R}/\mathfrak{P}$. See [21, chap. 16].

In the field of fractions of $\mathscr{R}/\mathfrak{P}$, the derivatives in $\Theta U \setminus \Theta V$ are transcendental over $\mathscr{F}$. This is an easy corollary to Proposition 13. Moreover, the process described at the beginning of this section for building a

zero of $\mathfrak{P}$ shows that, for every derivative $v \in \Theta V$, the set $(\Theta U \setminus \Theta V) + v$ is algebraically dependent over $\mathscr{F}$ in $\mathscr{R}/\mathfrak{P}$. Thus $\Theta U \setminus \Theta V$ provides a transcendence basis of the field of fractions of $\mathscr{R}/\mathfrak{P}$ over $\mathscr{F}$.

In order to obtain a zero $\underline{a}$ of $\mathfrak{P}$ which does not annihilate f, it is thus sufficient to assign to the derivatives in $\Theta U \setminus \Theta V$, values which are transcendental over $\mathscr{F}$.

The issue (solved below) is that the coordinates of $\underline{a}$ belong to $\mathscr{F}$ thus cannot be transcendental over $\mathscr{F}$.

Perform Ritt's full reduction algorithm over f using some characteristic set A of $\mathfrak{P}$. Then, by Proposition 12, there exists a power product h of initials and separants of A and differential polynomials $g, m_{i,\theta}$ such that

$$h\, f \;=\; g + \sum_{\substack{1 \leq i \leq r,\\ \theta \in \Theta}} m_{i,\theta}\, \theta p_i\,.$$

Since Ritt's reduction algorithm is "rational", the above formula holds in any differential polynomial ring $\mathscr{D}\{u_1, \ldots, u_n\}$ such that $\mathscr{D}$ contains the rational numbers plus the finitely many coefficients of f and the elements of the characteristic set A. We can thus choose for $\mathscr{D}$ a finite extension of the field of the rational numbers, over which the field $\mathscr{F}$ has an infinite degree of transcendency.

Thus, assigning values in $\mathscr{F}$ which are transcendental over $\mathscr{D}$ to the derivatives in $\Theta U \setminus \Theta V$, we obtain a generic zero $\underline{a}$ of the prime differential ideal $\mathfrak{P} \cap \mathscr{D}\{u_1, \ldots, u_n\}$. Since $f, g \notin \mathfrak{P}$, they do not belong to $\mathfrak{P} \cap \mathscr{D}\{u_1, \ldots, u_n\}$ either so that they are not annihilated by $\underline{a}$. In the differential polynomial ring $\mathscr{R}$, the zero $\underline{a}$ is no more generic but it still does not annihilate f, which is the result we are looking for. □

2.6 A Differential Theorem of Zeros

Let $\mathscr{F}$ be a universal extension of the field of the rational numbers. To fix ideas, one may let $\mathscr{F}$ be the field $\mathbb{C}$ of the complex numbers. Let $\mathscr{R} = \mathscr{F}\{u_1, \ldots, u_n\}$ endowed with m derivations. Let us stress that, in the statement of the next Theorem, the expansion points of the solutions depend on the solutions. With other words, we are looking for solutions in the ring of formal power series $\mathscr{F}[[x_1 - x_{1,0}, \ldots, x_m - x_{m,0}]]$ for unspecified $x_{1,0}, \ldots, x_{m,0} \in \mathscr{F}$. As pointed out in Section 1.4.3, we may also consider that the expansion point is the origin, provided that the differential system under consideration is assumed to be "extended".

Theorem 4 *(Differential Theorem of Zeros) Let $p_1 = \cdots = p_r = 0$ be a system of polynomial differential equations and f be a differential polynomial of $\mathscr{R}$. Let $\mathfrak{A} = \{p_1, \ldots, p_r\}$ be the perfect differential ideal of $\mathscr{R}$ generated by the left hand sides of the equations.*

If $f \in \mathfrak{A}$ then f annihilates over every solution of the system of equations.

Conversely, if every solution of the system of equations annihilates f then $f \in \mathfrak{A}$.

Proof The first statement is clear and is valid for any field $\mathscr{F}$. For the second statement, we assume $f \notin \mathfrak{A}$ and prove that the system of equations has a solution which does not annihilate f. By Theorem 3, there exists a prime differential ideal $\mathfrak{P}$ such that $\mathfrak{A} \subset \mathfrak{P}$ and $f \notin \mathfrak{P}$. By Proposition 17, the prime differential ideal $\mathfrak{P}$ has a zero which does not annihilate f. This zero is a solution of the system of equations. □

The Theorem implies that a system has no solution if and only if $1 \in \mathfrak{A}$ where $\mathfrak{A}$ denotes the perfect differential ideal that generated by the system. As we shall see in the next section, there exists an algorithm which decides if $1 \in \mathfrak{A}$. Thus the Theorem would be false if the expansion point were fixed to (say) the origin since, otherwise, we would have a contradiction with Denef and Lipshitz undecidability result.

3 Differential Elimination Methods

This section is dedicated to the question: given a set of differential polynomials Σ, how can we proceed to implement (24) ? Given a ranking, is it possible to compute, from the input system, one characteristic set for each essential prime component of the perfect differential ideal $\{\Sigma\}$ generated by Σ ?

The answer to the last question is no.

What we can do is this: from Σ, compute finitely many autoreduced sets A. Each of these sets defines a differential ideal $\mathfrak{A} = [A] : H_A^\infty$ and provides, through Ritt's reduction technique, a decision algorithm for membership testing in $\mathfrak{A}$. Moreover, the intersection of the differential ideals defined by the sets A is equal to the perfect differential ideal $\{\Sigma\}$.

The differential ideals $\mathfrak{A}$ are actually perfect but not necessarily prime. However, there exists algorithms to decompose them as intersections of prime differential ideals, presented by characteristic sets.

We thus can compute a finite decomposition (24) but it is not necessarily minimal. Surprisingly, there is no known algorithm to make the computed decomposition minimal. In particular, there is no known general algorithm to decide the inclusion of two prime differential ideals presented by characteristic sets.

It should be noticed that, in the case of a perfect differential ideal generated by a single differential polynomial, the minimal decomposition (24) can be computed, thanks to the Low Power Theorem. Ritt proves it in the ordinary case in [17, chap. III]. A general version is available in [12, chap. IV, 15, Theorem 6].

This section is structured as follows. Section 3.1 actually provides a new definition of characteristic sets, starting from the question: what can prevent an autoreduced set A to be a characteristic set of the differential ideal that it defines ? The new definition relies on some test. Section 3.2 shows that this test can be made algorithmic by means of resultant computations. As a byproduct we get, in Section 3.3, an algorithm for computing normal forms of differential polynomials modulo the differential ideals defined by characteristic sets. This normal form algorithm permits us to compute solutions (arcs, formal power series) of these (non necessarily prime) differential ideals. Last, in Section 3.4, we sketch an algorithm for computing the decomposition of a perfect differential ideal as an intersection of perfect differential ideals defined by characteristic sets.

This section aims at explaining the ideas but we will not give proofs, which are too long. Two key ideas (the unmixedness property of ideals defined by triangular sets and the fact that the ideals of the form $(A) : S_A^\infty$ are radical) are recent, in the sense that they do not appear in Kolchin's book. We will almost not address historical considerations in these notes. We refer interested readers to [7, sect. 8].

3.1 Characteristic Sets — The Constructive Definition

As stated in Proposition 13, if A is a characteristic set of a prime differential ideal $\mathfrak{P}$ then, it provides a membership decision algorithm to $\mathfrak{P}$: for any differential polynomial $p \in \mathscr{R}$ we have $p \in \mathfrak{P}$ if and only if $\mathsf{fullrem}(p, A) = 0$. In turn, the decision algorithm implies that $\mathfrak{P}$ is equal to $[A] : H_A^\infty$, which is the differential ideal generated by $[A]$, saturated by the multiplicative family generated by the initials and separants of A.

During the computations of an elimination process, it is easy to determine if a set A of differential polynomials is autoreduced. But is it the characteristic set of some differential ideal $\mathfrak{A}$? is it necessary for $\mathfrak{A}$ to be prime in order to have the membership decision algorithm stated above ?

The answer to both questions is no. There are actually two obstacles which may prevent an autoreduced set A to be a characteristic set of the differential ideal $\mathfrak{A} = [A] : H_A^\infty$ that it *defines* (let us use this term rather than "generate" since A does not generate $\mathfrak{A}$): a nondifferential obstacle and a differential one, which only occurs in the partial case.

3.1.1 The Nondifferential Obstacle

Let us denote (A) the nondifferential ideal generated by A, I_A the set of the initials, and S_A the set of the separants of A. Consider the following set

$$A \quad = \quad p_1, p_2 \quad = \quad u^2 - 1,\ (u+1)\, v - 1\,.$$

It is an autoreduced set of $\mathscr{F}\{u, v\}$ provided that the ranking imposes $u < v$. The ideal $(A) : I_A^\infty$ is equal to $(2\, v - 1, u - 1)$ (the saturation by the initial $u + 1$ of p_2 permits to remove one factor of p_1), which actually is a prime ideal. This ideal contains the polynomial $u - 1$, which is reduced with respect to A, proving

that A is not a characteristic set of $(A) : I_A^\infty$. Since $(A) : I_A^\infty \subset \mathfrak{A}$, we see that A is not a characteristic set of the differential ideal $\mathfrak{A}$ either. The same argument proves that A does not provide a membership decision algorithm to $\mathfrak{A}$ since $\mathsf{fullrem}(u-1, A) = u-1$ though $u-1 \in \mathfrak{A}$.

The above problem comes from the fact that the initial of some differential polynomial $p_i \in A$ is a *zero divisor* modulo the ideal defined by the differential polynomials $p_1, \ldots, p_{i-1}$ i.e. the differential polynomials of A with ranks lower than p_i.

Beware to the fact that the technical aspect of the above statement is necessary, since the initials of A *never* are zero divisors modulo the ideal $(A) : I_A^\infty$, for the obvious reason that they then belong to the multiplicative family by which the ideal is saturated.

Informally speaking, we are heading towards a definition of characteristic sets based on the requirement that the initials are not zero divisors, i.e. are *regular*, in some quotient ring. We may thus relax the degree condition which occurs in the definition of autoreduced sets. Instead of considering sets A which are autoreduced, we consider, more generally, sets A which are: 1) *triangular* i.e. which have pairwise distinct leading derivatives; and 2) *partially autoreduced* i.e. whose elements are pairwise partially reduced with respect to each other.

Regular Chains. Let $A = p_1, \ldots, p_r$ be a partially autoreduced triangular set of differential polynomials of $\mathscr{R}$. For each index $i \in [1, r]$, denote $A_i = p_1, \ldots, p_i$ and $\mathfrak{a}_i = (A_i) : I_{A_i}^\infty$ the ideal of $\mathscr{R}$ defined by A_i. Then A is said to be a *regular chain*[3] if, for each $i \in [2, r]$, the initial of p_i is regular in the ring $\mathscr{R}/\mathfrak{a}_{i-1}$. One may also use the following inductive definition

Definition 1 *A partially autoreduced triangular set of differential polynomials $A = p_1, \ldots, p_r$ is a* regular chain *if $r = 1$ or $r > 1$, A_{r-1} is a regular chain and the initial of p_r is regular in $\mathscr{R}/\mathfrak{a}_{r-1}$.*

It can be proved (but the proof is long) that a regular chain A provides a membership decision algorithm to $\mathfrak{a} = \mathfrak{a}_r$. Indeed, to avoid any differentiation in the reduction process, consider a differential polynomial f, partially reduced with respect to a regular chain A. Then $f \in \mathfrak{a}$ if and only if $\mathsf{fullrem}(f, A) = 0$.

Thus, up to the relaxed degree condition, a regular chain A is a characteristic set of $\mathfrak{a}$. More precisely, we can say that: 1) an autoreduced regular chain A is a characteristic set of $\mathfrak{a}$; and 2) a regular chain A has the same rank as the characteristic sets of $\mathfrak{a}$.

Notice that the ideal $\mathfrak{a}$ is not necessarily prime.

Notice also that $\mathfrak{a}$ may have characteristic sets which are not regular chains. Indeed, consider the following set

$$A \quad = \quad p_1, p_2 \quad = \quad u^2 - 1,\ v - 1\,.$$

Assume $u < v$. Then A is an autoreduced regular chain thus a characteristisc set of $\mathfrak{a} = (A)$. Multiply p_2 by $u - 1$. The result is autoreduced and has the same rank as A. It is thus also a characteristic set of $\mathfrak{a}$. However, the initial $u - 1$ of $(u-1)\,p_2$ is a zero divisor in $\mathscr{R}/\mathfrak{a}_1$, which implies that the characteristic set is not a regular chain.

Regular Differential Chains. As mentioned above, the differential obstacle only concerns the partial case. Let us thus assume that $\mathscr{R}$ is an ordinary differential polynomial ring and A is a regular chain of $\mathscr{R}$. Let us moreover assume A is autoreduced. Is A a characteristic set of $\mathfrak{A} = [A] : H_A^\infty$ in general ? The answer is no. Consider the following autoreduced regular chain made of a single differential polynomial, featuring a multiple factor

$$A \quad = \quad p \quad = \quad (u-1)\,(u+1)^2\,.$$

Differentiating p we get

$$\dot{p} \quad = \quad (u+1)\,(3\,u-1)\,\dot{u}\,.$$

[3] The concept of regular chain was introduced in the context or usual polynomials, where the notion of a partially autoreduced set is irrelevant. The definition we give in these lecture notes are specifically tuned for the context of differential algebra.

The separant $(u+1)\,(3\,u-1)$ of p has a common factor[4] with p. Thus, because of the saturation process, the differential polynomial $u-1$, which is reduced with respect to A, belongs to $\mathfrak{A}$ and A is not a characteristic set of A. We thus need to impose an extra condition on regular chains.

Let $A = p_1, \ldots, p_r$ be a regular chain of $\mathscr{R}$. For each index $i \in [1, r]$, denote $A_i = p_1, \ldots, p_i$ and $\mathfrak{a}_i = (A_i) : I_{A_i}^{\infty}$ the ideal of $\mathscr{R}$ defined by A_i.

Definition 2 *A regular chain A is said to be* squarefree *if, for each $i \in [1, r]$, the separant of p_i is not a zero divisor in the ring $\mathscr{R}/\mathfrak{a}_i$.*

In the ordinary differential case, a squarefree regular chain is called a *regular differential chain* (there is an extra condition in the partial case).

It can be proved (but the proof is long) that a regular differential chain A provides a membership decision algorithm to $\mathfrak{A}$. Indeed, let f be a differential polynomial and A be a regular differential chain of $\mathscr{R}$. Then $f \in \mathfrak{A}$ if and only if $\mathsf{fullrem}(f, A) = 0$.

Thus, up to the relaxed degree condition, a regular differential chain A is a characteristic set of $\mathfrak{A}$. More precisely, we can say that: 1) an autoreduced regular differential chain is a characteristic set of $\mathfrak{A}$; and 2) a regular differential chain A has the same rank as the characteristic sets of $\mathfrak{A}$.

Moreover, it can be proved that if A is a regular differential chain then the ideal $\mathfrak{a}$ is equal to $(A) : H_A^{\infty}$ (the proof is easy) and that both ideals $\mathfrak{a}$ and $\mathfrak{A}$ are radical ideals (the proof is long). In particular, $\mathfrak{A}$ is perfect. The fact that $\mathfrak{a}$ is radical is a consequence of a result known as Lazard's Lemma.

3.1.2 The Differential Obstacle

Consider the following set

$$A \;=\; p_1,\, p_2 \;=\; v_x - u,\, v_y\,.$$

It is an autoreduced set of the differential polynomial ring $\mathscr{F}\{u, v\}$, endowed with derivations δ_x and δ_y, provided that the ranking imposes that u is less than v_x and v_y. Its initials and separants are equal to 1. It is thus a squarefree regular chain of $\mathscr{F}\{u, v\}$, defining (and generating) a differential ideal $\mathfrak{A} = [A]$. The differential polynomial $\delta_y p_1 - \delta_x p_2 = u_y$ belongs to $\mathfrak{A}$ and is reduced with respect to A, proving that A is not a characteristic set of $\mathfrak{A}$. This differential polynomial is a particular case of a Δ-polynomial, defined below.

Let $A = p_1, \ldots, p_r$ be a partially autoreduced triangular subset of a differential polynomial ring $\mathscr{R}$ endowed with $m > 1$ derivations. Since $m > 1$, it may happen that the leading derivatives $\theta_i u$ and $\theta_j u$ of two elements p_i and p_j of A are derivatives of the same differential indeterminate u. Such a pair of differential polynomials is called a *critical pair* of A. Denote θ_{ij} the least common multiple of θ_i and θ_j so that $\theta_{ij} u$ is the least common derivative of the two leading derivatives $\theta_i u$ and $\theta_j u$. Then, denoting s_i and s_j the separants of p_i and p_j, the Δ-polynomial $\Delta_{ij} = \Delta(p_i, p_j)$ is defined as

$$\Delta(p_i, p_j) \;=\; s_j\,\frac{\theta_{ij}}{\theta_i}\,p_i - s_i\,\frac{\theta_{ij}}{\theta_j}\,p_j\,. \tag{26}$$

It is either an element of $\mathscr{F}$ or a differential polynomial with leading derivative *strictly less* than $\theta_{ij} u$. Indeed, in (26), the leading derivatives of both differential polynomials $(\theta_{ij}/\theta_i)p_i$ and $(\theta_{ij}/\theta_j)p_j$ are both equal to $\theta_{ij} u$ but a cancellation occurs (by design) so that $\deg(\Delta_{ij}, \theta_{ij} u) = 0$.

Denote $A_{ij} \subset \Theta A$ the set of the derivatives of the elements of A with leading derivatives *strictly less* than $\theta_{ij} u$. The critical pair (p_i, p_j) of A is said to be *solved* if the Δ-polynomial Δ_{ij} belongs to the nondifferential ideal defined by A_{ij} i.e. if $\Delta_{ij} \in (A_{ij}) : H_{A_{ij}}^{\infty}$. Remarks:

1. if we denote $\mathscr{R}_{ij}$ the ring of all differential polynomials of $\mathscr{R}$ with leading derivatives strictly less than $\theta_{ij} u$. We have $(A_{ij}) : H_{A_{ij}}^{\infty} \subset \mathfrak{A} \cap \mathscr{R}_{ij}$ but the equality does not hold in general ; in particular, if the critical pair is not solved, the inclusion is strict ;

[4] This is not a surprise since the separant of a differential polynomial is the derivative of this polynomial in the usual sense thus every irreducible factor of p with multiplicity $d \geq 2$ is a factor of its separant with multiplicity $d - 1$.

2. if $\mathsf{fullrem}(\Delta_{ij}, A) = 0$ then the critical pair is solved ;

3. for a given finite set A, there are only finitely many critical pairs.

Definition 3 *A partially autoreduced triangular set A of differential polynomials is said to be* coherent *if all its critical pairs are solved.*

Since a partially autoreduced triangular set has no critical pair in the ordinary differential case, the following definition holds in both the ordinary and the partial differential context.

Definition 4 *A* regular differential chain *is a coherent squarefree regular chain of partially autoreduced differential polynomials.*

All the comments following the definition of regular differential chains in the ordinary case apply "as is" in the partial case, to the new definition. In particular, an autoreduced regular differential chain is a characteristic set of the differential ideal that it defines. The part of the proof (which is long) which addresses the consequences of the coherence property is known as Rosenfeld's Lemma [18]. A close version was proved by Seidenberg [19, Theorem 6].

3.2 Identifying Zero Divisors

The idea of using resultants to identify zero divisors modulo ideals defined by regular chains comes from [9]. It was generalized to the differential case in [8].

The differential polynomial ring is $\mathscr{R} = \mathscr{F}\{u_1, \ldots, u_n\}$ with m derivations. Let $A = p_1, \ldots, p_r$ be a partially autoreduced triangular set of differential polynomials of $\mathscr{R}$. Let $V = v_1, \ldots, v_r$ be the set of the leading derivatives of A and $\mathscr{R}_0 = \mathscr{F}[\Theta U \setminus \Theta^* V]$ denote the ring of the differential polynomials of $\mathscr{R}$ which are partially reduced with respect to A. Denote $\mathfrak{A} = [A] : H_A^\infty$ the differential ideal defined by A.

In the next Proposition, A needs not be a regular chain and the two ideals $\mathfrak{A}$ and $(A) : H_A^\infty$ may contain 1. For a proof, see [18, Lemma].

Proposition 18 *(Rosenfeld's Lemma)*
If A is a coherent, partially autoreduced triangular set of differential polynomials of $\mathscr{R}$ then

$$\mathfrak{A} \cap \mathscr{R}_0 \quad = \quad (A) : H_A^\infty \, .$$

Let A be a partially autoreduced triangular set (not necessarily coherent), $f, \overline{f}$ be two differential polynomials of $\mathscr{R}$ and $g, \overline{g}$ be their partial remainders by A. We have $f \in \mathfrak{A}$ if and only if $g \in \mathfrak{A}$. Similar statements hold for the pair $(\overline{f}, \overline{g})$ and the pair of products $(f\,\overline{f}, g\,\overline{g})$. Thus f is a zerodivisor in $\mathscr{R}/\mathfrak{A}$ if and only if g, which belongs to $\mathscr{R}_0$, is a zerodivisor in $\mathscr{R}/\mathfrak{A}$; moreover, if g is a zerodivisor in $\mathscr{R}/\mathfrak{A}$ then there exists $\overline{g} \in \mathscr{R}_0$ with $\overline{g} \notin \mathfrak{A}$, such that the product $g\,\overline{g} \in \mathfrak{A}$.

In summary, in our study of zero divisors in $\mathscr{R}/\mathfrak{A}$, we may restrict ourselves, with no loss of generality, to differential polynomials partially reduced with respect to A i.e. to the ring $\mathscr{R}_0/(\mathfrak{A} \cap \mathscr{R}_0)$.

Assume now that A is moreover coherent. Then Rosenfeld's Lemma applies and we may restrict our study of zero divisors, with no loss of generality, to the ring $\mathscr{R}_0/(A) : H_A^\infty$.

In general, the polynomial ring $\mathscr{R}_0$ is not finitely generated since there may exist infinitely many derivatives in $\Theta U \setminus \Theta V$. However, only finitely many derivatives occur in a given differential polynomial g and the elements of A. Let $w_1, \ldots, w_t \in \Theta U \setminus \Theta V$ denote the finitely many derivatives needed to form a finitely generated subring $\mathscr{R}_1 = \mathscr{F}[v_1, \ldots, v_r, w_1, \ldots, w_t]$ of $\mathscr{R}_0$ containing the differential polynomials under consideration. We see that we may restrict our study of zero divisors, with no loss of generality, to the ring $\mathscr{R}_1/(A) : H_A^\infty$.

The restriction to $\mathscr{R}_1$ is important because it is a Nötherian ring [22, chap. IV] and the Lasker-Nöther Theorem characterizes the zero divisors of $\mathscr{R}_1/(A) : H_A^\infty$. According to [22, chap. IV, 6, Corollary 3 to Theorem 11], the set of all zero divisors is the union of the associated prime ideals (isolated and embedded) of $(A) : H_A^\infty$.

Let $\mathfrak{a}$ denote any of the ideals $(A) : H_A^\infty$, $(A) : I_A^\infty$ or $(A) : S_A^\infty$.

Then $\mathfrak{a}$ is either equal to $\mathscr{R}_1$ (if $1 \in \mathfrak{a}$) or unmixed dimensional [22, chap. VII, 7], which implies that all its associated prime ideals are isolated and have the same dimension (the proof is long and ultimately relies on Macaulay's unmixedness Theorem [22, chap. VII, 8, Theorem 26]). Then it is not difficult to see that, if $\mathfrak{p}$ is an associated prime ideal of $\mathfrak{a}$ (assuming it is different from $\mathscr{R}_1$) then $\mathfrak{p} \cap \mathscr{F}[w_1, \ldots, w_t] = (0)$, proving that any nonzero element of $\mathscr{F}[w_1, \ldots, w_t]$ is a regular element (i.e. a non zero divisor) in $\mathscr{R}_1/\mathfrak{a}$.

This property is important because a differential polynomial $g \in \mathscr{R}_1$ is a zero divisor in $\mathscr{R}_1/\mathfrak{a}$ if and only if it a zero divisor in the *total ring of fractions* (called *total quotient ring* in [22, chap. I, 19]) of $\mathscr{R}_1/\mathfrak{a}$, which is the ring obtained by inverting all the regular elements of $\mathscr{R}_1/\mathfrak{a}$. Define $\mathscr{R}_2 = \mathscr{F}(w_1, \ldots, w_t)[v_1, \ldots, v_r]$. By the unmixedness property of $\mathfrak{a}$, the rings $\mathscr{R}_1/\mathfrak{a}$ and $\mathscr{R}_2/\mathfrak{a}$ have the same total ring of fractions. We thus see that a differential polynomial g is a zero divisor in $\mathscr{R}_1/\mathfrak{a}$ if and only if it is a zero divisor, in the ring $\mathscr{R}_2/\mathfrak{a}$.

In the case of $\mathfrak{a} = (A) : S_A^\infty$, it can be proved that $\mathscr{R}_2/\mathfrak{a}$ is isomorphic to a direct product of fields (the proof essentially relies on the basic properties of the separants mentioned in the former section and the Chinese Remainder Theorem [13, chap. II, 2]). This implies that $\mathscr{R}_2/\mathfrak{a}$ does not involve any nilpotent element i.e. any zero divisor, a power of which is zero which, in turn, implies the following Proposition. An incomplete proof first appears in [4]. It was fixed in [15, 16].

Proposition 19 *(Lazard's Lemma)*
The ideal $(A) : S_A^\infty$ is radical.

Since 1) an ideal is radical if and only if it is the intersection of its associated prime ideals ; and 2) $(A) : H_A^\infty$ is the intersection of the associated prime ideals of $(A) : S_A^\infty$ which do not contain any element of I_A, we see that $(A) : H_A^\infty$ also is a radical ideal.

Then, it is easy to see that, if A is coherent, then 1) the differential ideal $\mathfrak{A}$ is radical hence admits a representation (24) (page 18) as an intersection of essential components $\mathfrak{P}_i$ for $i \in [1, \varrho]$; and 2) there is a bijection between these essential components and the associated prime ideals $\mathfrak{p}_i$ of $(A) : H_A^\infty$ given by $\mathfrak{P}_i \cap \mathscr{R}_0 = \mathfrak{p}_i$ for $i \in [1, \varrho]$.

3.2.1 Decision Algorithms Available With Regular Chains

So far, we have not assumed that A is a regular chain. For simplicity, let us place ourselves in the ring $\mathscr{R}_0$ of the differential polynomials partially reduced with respect to A and denote $\mathfrak{a} = (A) : I_A^\infty$ in $\mathscr{R}_0$.

Let us introduce two algorithms: the pseudoremainder $\mathsf{prem}(g, A)$ and the resultant $\mathsf{res}(g, A)$ of a differential polynomial $g \in \mathscr{R}_0$ by A.

The Pseudoremainder. The pseudoremainder of a differential polynomial by a set A is defined inductively using the pseudoremainder of a differential polynomial by another one, with respect to some derivative:

1. $\mathsf{prem}(g, \varnothing) = g$ and
2. $\mathsf{prem}(g, \{p_1, \ldots, p_r\}) = \mathsf{prem}(\mathsf{prem}(g, p_r, v_r), \{p_1, \ldots, p_{r-1}\})$ if $r \geq 1$.

The Resultant. Similarly, the resultant of a differential polynomial by a set A is defined inductively using the resultant of two differential polynomials with respect to some derivative [13, chap. IV, 10]:

1. $\mathsf{res}(g, \varnothing) = g$ and
2. $\mathsf{res}(g, \{p_1, \ldots, p_r\}) = \mathsf{res}(\mathsf{res}(g, p_r, v_r), \{p_1, \ldots, p_{r-1}\})$ if $r \geq 1$.

If A is a regular chain then the unmixedness property of $\mathfrak{a}$ permits to prove that this ideal is necessarily different from $\mathscr{R}_0$. The following Proposition can be proved:

Proposition 20 *Let A be a partially autoreduced triangular set and g be a differential polynomial of $\mathscr{R}_0$. Then the following properties are equivalent:*

1. *A is a regular chain,*

2. *$g \in \mathfrak{a}$ if and only if* $\mathsf{prem}(g, A) = 0$,

3. *g is a zerodivisor in $\mathscr{R}_1/\mathfrak{a}$ if and only if* $\mathsf{res}(g, A) = 0$.

An Example. Observe that the resultant computation hides subtleties and must be performed from top to bottom. Consider the following regular differential chain (assuming $v > u$) and the differential polynomial $f = u + v - 31$,

$$A \;=\; p_1,\, p_2 \;=\; (u-1)\,(u-3),\, v - 10\,u\,.$$

The resultant of f by A is the differential polynomial g_2. This proves that f is regular in $\mathscr{R}/\mathfrak{A}$.

$$\begin{array}{rcrcl} \mathsf{res}(f, p_2, v) & = & -11\,u + 31 & = & g_1\,, \\ \mathsf{res}(g_1, p_1, u) & = & -40 & = & g_2\,. \end{array}$$

Let us now consider $\overline{f} = \mathsf{res}(f, p_1, u) = (30 - v)\,(28 - v)$. The resultant of $\overline{f}$ by A is the differential polynomial $g_4 = 0$. This proves that $\overline{f}$ is a zero divisor in $\mathscr{R}/\mathfrak{A}$.

$$\begin{array}{rcrcl} \mathsf{res}(\overline{f}, p_2, v) & = & (30 - 10\,u)\,(28 - 10\,u) & = & g_3\,, \\ \mathsf{res}(g_3, p_1, u) & = & 0 & = & g_4\,. \end{array}$$

The last property of Proposition 20 permits to determine if a given partially autoreduced triangular set A is a regular chain. Indeed, denoting i_k the initial of any $p_k \in A$, for $k \in [1, r]$, the set A is seen to be a regular chain if and only if $\mathsf{res}(i_k, \{p_1, \ldots, p_{k-1}) \neq 0$ for $k = 2, 3, \ldots, r$.

It also permits to determine if a given regular chain is squarefree. Indeed, denoting s_k the separant of any $p_k \in A$, for $k \in [1, r]$, the regular chain A is seen to be squarefree if and only if $\mathsf{res}(s_k, \{p_1, \ldots, p_k) \neq 0$ for $k \in [1, r]$.

Noticing that $\mathsf{fullrem}(f, A) = \mathsf{prem}(\mathsf{partialrem}(f, A))$ for any differential polynomial $f \in \mathscr{R}$, we thus see that the following Proposition holds

Proposition 21 *Let A be a coherent, partially autoreduced triangular set and f be a differential polynomial of $\mathscr{R}$. Then the following properties are equivalent:*

1. *A is a regular differential chain,*

2. *$f \in \mathfrak{A}$ if and only if* $\mathsf{fullrem}(f, A) = 0$,

3. *f is a zerodivisor in $\mathscr{R}/\mathfrak{A}$ if and only if* $\mathsf{res}(\mathsf{partialrem}(f, A), A) = 0$.

3.2.2 Testing the Inclusion of Differential Ideals

Let A and B be two regular differential chains, defining differential ideals $\mathfrak{A}$ and $\mathfrak{B}$ in $\mathscr{R}$. If $A \not\subset \mathfrak{B}$ then $\mathfrak{A} \not\subset \mathfrak{B}$. If $A \subset \mathfrak{B}$ and all elements of H_A are regular in $\mathscr{R}/\mathfrak{B}$ then $\mathfrak{A} \subset \mathfrak{B}$. However, if $A \subset \mathfrak{B}$ and there exists some $h \in H_A$ which is either zero or a zero divisor in $\mathscr{R}/\mathfrak{B}$ then we cannot conclude.

The problem comes from the fact that A is not a basis of $\mathfrak{A}$. In the nondifferential case, the inclusion problem can be decided since, thanks to Gröbner bases and the Rabinowitsch trick, it is possible to compute a basis of $(A) : H_A^\infty$.

3.3 Normal Forms and Formal Power Series Solutions

The content of this section comes from [3, 6]. By a differential fraction, we mean a fraction f/g of two differential polynomials of $\mathscr{R}$, with $g \neq 0$.

Proposition 22 *(and Definition of Normal Forms)*
Let $A = p_1, \ldots, p_r$ be a regular differential chain, $\mathfrak{A}$ the differential ideal that it defines and f/g be a differential fraction of $\mathscr{R}$. The normal form *of f/g modulo A exists: it is the unique differential fraction p/q such that*

1. *p is fully reduced with respect to A,*
2. *$q \in \mathscr{F}[\Theta U \setminus \Theta V]$,*
3. *f/g and p/q are equal in the total ring of fractions of $\mathscr{R}/\mathfrak{A}$.*

3.3.1 Computation of Normal Forms

Normal forms can be computed by Algorithm 1, which relies on Algorithms 2 and 3 which, in turn, rely on inverse/resultant computations.

Algorithm 1: $\mathtt{NF}\,(f/g, A)$ the normal form of a general differential fraction

input : a differential fraction f/g and a differential regular chain A with g regular in $R/\mathfrak{A}$
output: the normal form of f/g modulo A

1 compute $h_f\, f = \overline{f} \pmod{[A]}$ where h_f denotes a power product of separants of A ; /* by computing $\overline{f} = \mathsf{partialrem}(f, A)$ */
2 compute $h_g\, g = \overline{g} \pmod{[A]}$ where h_g denotes a power product of separants of A ; /* by computing $\overline{g} = \mathsf{partialrem}(g, A)$ */
3 **return** $\mathtt{NFfrac}\left(\dfrac{h_g\,\overline{f}}{h_f\,\overline{g}}, A\right)$

The resultant of two polynomials can be computed by means of subresultant sequences. Moreover, there exists extended versions of the algorithms for computing subresultant sequences [11] which permit to express the resultant of two polynomials as a linear combination of these two polynomials, with polynomial coefficients. These algorithms imply the following algorithmic Proposition

Proposition 23 *Let $A = p_1, \ldots, p_r$ be a regular differential chain and $g \in \mathscr{R}_0$ be a differential polynomial partially reduced with respect to A. Then there exist differential polynomials $q, q_1, q_2, \ldots, q_r$ of $\mathscr{R}_0$ such that*

$$q\, g \quad = \quad \mathsf{res}(g, A) + q_1\, p_1 + q_2\, p_2 + \cdots + q_r\, p_r\,. \tag{27}$$

The differential polynomial $\mathsf{res}(g, A) \in \mathscr{F}[\Theta U \setminus \Theta V]$.

Let $g \in \mathscr{R}_0$ be a differential polynomial partially reduced with respect to a regular differential chain A. If $\mathsf{res}(g, A) \neq 0$ then g and $\mathsf{res}(g, A)$ are both regular elements of $\mathscr{R}/\mathfrak{A}$ and the fraction $q/\,\mathsf{res}(g, A)$ (where q comes from (27)) is said to be an *inverse* of g modulo A. It actually is an inverse of g in the total ring of fractions of $\mathscr{R}/\mathfrak{A}$.

For simplicity, it is assumed that A is a regular differential chain in Algorithm 2. Strictly speaking, this assumption actually makes the recursive call at line 7 incorrect since a subset of a coherent set is not necessarily coherent (but a subset of squarefree regular chain is a squarefree regular chain).

3.3.2 Application to the Computation of Formal Power Series Solutions

In Section 2.5, a process is described for computing a zero of differential prime ideal, presented by a characteristic set. First of all, notice that this process holds "as is" for the radical differential ideals defined by regular differential chains. Now, normal forms provide a variant of this process, which is convenient but

Algorithm 2: `NFpoly`(f, A) the normal form of a partially reduced differential polynomial

input : a differential polynomial $f \in \mathscr{R}_0$ and $A = p_1, \ldots, p_r$ a regular differential chain
output: the normal form of f modulo A

if *A is empty* **then**
  return f
else
  denote i_r and v_r the initial and the leading derivative of p_r ;
  compute $i_r^\alpha\, f = g + q\, p_r$; `/* by computing` $g = \mathsf{prem}(f, p_r, v_r)$ `*/`
  compute u/s an inverse of i_r modulo A ;
  return $(1/s^\alpha) \times$ `NFpoly`$(u^\alpha g, \{p_1, \ldots, p_{r-1}\})$
end

Algorithm 3: `NFfrac`$(f/g, A)$ the normal form of a partially reduced differential fraction

input : a fraction f/g and a regular differential chain A with $f, g \in \mathscr{R}_0$ and g regular in $R/\mathfrak{A}$
output: the normal form of f/g modulo A

compute u/s an inverse of g modulo A ;
return $(1/s) \times$ `NFpoly`$(u\, f, A)$

slightly less general than the one of Section 2.5 since the set of forbidden expansion points and initial values may increase.

Let $A = p_1, \ldots, p_r$ be a regular differential chain, defining a perfect differential ideal $\mathfrak{A} = [A] : H_A^\infty$ of $\mathscr{R}$. Denote X the finite set of the derivatives A depends on, including the extra derivatives used to encode the "independent variables" in the extended system associated to A, in the sense of Section 1.4.3.

Denote $V \subset X$ the set of leading derivatives of A. Then $\Theta U \setminus \Theta V$ denotes the possibly infinite set of the elements of ΘU which are not the derivative of any element of V. Let Θ^* denote the set of all proper derivative operators. Then $\Theta^* V$ denotes the set of all derivatives which are proper derivatives of some element of V.

The following process defines an expansion point and a tuple of arcs $\underline{a}$ such that $\underline{a}$ or equivalently, the formal power series $\Psi(\underline{a})$, is a zero of $\mathfrak{A}$.

Process.

1. Let h denote the product of the initials and separants of A and f/g the normal form of $1/h$ modulo A. Solve the following system as a nondifferential system of $\mathscr{F}[X]$
$$p_1 = \cdots = p_r = 0\,, \quad g \neq 0\,.$$
2. Assign any value from $\mathscr{F}$ to the derivatives of $\Theta U \setminus \Theta V$ and to the "independent variables" encoding differential indeterminates which were not already assigned values at Step 1.
3. Let $v \in \Theta^* V$ be a proper derivative of some leading derivative of A. Assign to v the value of its normal form modulo A.

A few remarks:

- the idea of the above Process is that, among the zeros which annihilate $p_1 = \cdots = p_r = 0$, we should only forbid the ones which prevent us to compute normal forms i.e. the ones which annihilate their denominators;
- the irreducible factors of the denominators of all normal forms considered at Step 3 are factors of the differential polynomial g defined at Step 1.

- Every tuple of values which annihilates h is forbidden by $g \neq 0$ since we have the identity $h\,f/g = 1$ in the total ring of fractions of $\mathscr{R}/\mathfrak{A}$ so that the system to be solved at Step 1 in this section cannot have more solutions than that of Section 2.5.

- In some cases, the system to be solved at Step 1 has strictly less solutions than that of Section 2.5. Consider the set

$$A \;=\; p_1,\, p_2 \;=\; v^2 - 1,\, (v - w)\,u - z\,.$$

  It is a regular differential chain for any ranking such that u is the leading derivative of p_2. We have $h = v - w$. The normal form of $1/h$ modulo A is $(v + w)/(1 - w^2)$ so that the system to be solved at Step 1 involves the constraint $w^2 \neq 1$. However, the constraint $h \neq 0$ allows $w = \pm 1$, provided that v has the opposite sign.

- As well in this section as in Section 2.5, the constraints $h \neq 0$ or $g \neq 0$ may forbid values for which solutions actually exist. This phenomenon may be "easier to observe" when using the normal form algorithm. Consider the differential polynomial

$$p \;=\; \dot{u}^2 - u^3 + 8$$

  in the ordinary differential polynomial ring $\mathscr{F}\{u\}$. Let A be the regular differential chain involving p as single element. It can be proved that

$$\{p\} \;=\; [A] : H_A^\infty \cap [u^3 - 8,\, \dot{u}]\,.$$

  The differential ideal $[u^3 - 8,\, \dot{u}]$ obviously admits a single solution which is the arc $\underline{a} = (2, 0, \ldots)$ leading to the formal power series $\Psi(\underline{a}) = 2$. Let us now consider the regular differential chain A. Dropping the numerical constant, we have $h = \dot{u}$. The normal form of $1/h$ modulo A is $\dot{u}/(u^3 - 8)$ which implies that any arc whose first coordinate is 2 is forbidden thus that any formal power series $u(x)$ with initial condition $u(0) = 2$ is forbidden. However, the computation of the normal forms of the first derivatives of u suggests that this constraint is pointless:

$$\begin{aligned}
a_2 &= (3/2)\,u^2,\\
a_3 &= 3\,\dot{u}\,u,\\
a_4 &= (15/2)\,u^3 - 24,\\
a_5 &= (45/2)\,\dot{u}\,u^2,\\
a_6 &= (315/4)\,u^4 - 360\,u,\\
&\vdots
\end{aligned}$$

  Indeed, it is quite easy to prove that if the differential polynomial p has the form $\dot{u}^2 + q$ with $q \in \mathscr{F}[u]$ (no "independent variable" among the coefficients) then the normal form of any derivative of $\ddot{u}$ is a differential polynomial of $\mathscr{F}[u, \dot{u}]$.

  Let us come back to our example and choose the forbidden value $a_0 = 2$. Then necessarily $a_1 = 0$ (since $a_1^2 - a_0^3 + 8 = 0$) and, evaluating the normal forms above over this beginning of arc we get the solution

$$\begin{aligned}
\underline{a} &= (2, 0, 6, 0, 36, 0, 540, 0, 12960, 0, 486000, \ldots)\\
\Psi(\underline{a}) &= 2 + 3\,x^2 + \frac{3}{2}\,x^4 + \frac{3}{4}\,x^6 + \frac{9}{28}\,x^8 + \frac{15}{112}\,x^{10} + \cdots
\end{aligned}$$

3.4 A Sketched Elimination Algorithm

The content of this section is much inspired from the descriptions of the *RosenfeldGroebner* algorithm given in [5, 2].

There exists an algorithm which gathers as input any finite system Σ of differential polynomials (and a ranking) and outputs finitely many regular differential chains $A_1, \ldots, A_t$ such that

$$\{\Sigma\} \quad = \quad [A_1] : H_{A_1}^\infty \cap \cdots \cap [A_t] : H_{A_t}^\infty .$$

If $1 \in \{\Sigma\}$ then $t = 0$. Thus, thanks to the differential Theorem of Zeros, this algorithm permits to decide whether Σ has solutions over some unspecified expansion point.

This algorithm proceeds in two main steps. In the first step, it computes finitely many *regular differential systems* of the form $A = 0$, $S \neq 0$ where A is a coherent, partially autoreduced triangular set of differential polynomials and S is a set of differential polynomials partially reduced with respect to A. A regular differential system defines the perfect differential ideal $[A] : S^\infty$ which is the ideal of the differential polynomials which annihilate over all the solutions of the system. A regular differential system may have no solution. In that case, $[A] : S^\infty = \mathscr{R}$. The perfect differential ideal $\{\Sigma\}$ is the intersection of the perfect differential ideals defined by the regular differential systems produced at the first step.

In the second step, the algorithm transforms each regular differential system $A = 0$, $S \neq 0$ into finitely many regular differential chains (none if the regular differential system has no solution). The intersection of the perfect differential ideals defined by the regular differential chains is equal to the perfect differential ideal $[A] : S^\infty$.

Let us sketch the algorithm, called *regCharacteristic*, for the second step. Its principle consists in testing whether A is a squarefree regular chain by testing the regularity of the initials and separants of A, processing the elements of A from bottom up and implementing the ideas explained in Section 3.2. This being done, A is proved to be a regular differential chain and the regularity of all the elements of S can be verified. Every regular element of S which is proved regular is discarded. Of course, it may happen that some differential polynomial is proved to be a zero divisor at some stage. In that case, a factorization of some $p_i \in A$ is discovered. This exhibited factorization permits to split the current system into two branches. If one of the factors of p_i divides an element of S then the corresponding branch is discarded. The regularity test can be achieved by means of the resultant computations explained in Section 3.2 however this test "as is" does not provide the factorization. A possibility consists in using a recursive variant of the extended Euclidean algorithm such as the one provided in [3, Appendix].

The main ideas underlying a complete elimination algorithm are explained through two examples, in the following sections.

3.4.1 An Ordinary Differential Example

See Figure 2. The differential polynomial ring is $\mathscr{F}\{u, v\}$.

$$(\Sigma_1) \qquad \ddot{u} + v = 0, \quad \dot{u}^2 + v = 0.$$

The ranking is such that every derivative of u is greater than any derivative of v (the differential indeterminate u is eliminated). The leading derivatives of the two differential polynomials are $\ddot{u}$ and $\dot{u}$. The first differential polynomial is not partially reduced with respect to the first one. The partial remainder computation is carried out in (17), page 14. This computation amounts to differentiate the second equation, giving

$$2\,\dot{u}\,\ddot{u} + \dot{v} = 0$$

then replace $\ddot{u}$ by $-\dot{v}/(2\,\dot{u})$ in the first one, giving

$$-\frac{\dot{v}}{2\,\dot{u}} + v = 0.$$

Then replace the first equation by the numerator of the reduced equation, which is the partial remainder g, provided that the separant $2\,\dot{u}$, which is the differential polynomial h of (17), is different from zero. The solutions of (Σ_1) which annihilate the separant are considered separately. We obtain a splitting[5] of (Σ_1) into

$$(\Sigma_2) \qquad \ddot{u} + v = 0, \quad \dot{u}^2 + v = 0, \quad \dot{u} = 0$$

[5]It is actually not the same type of splitting as in *regCharacteristic* because it does not correspond to a factorization.

and

$$(\Sigma_3) \qquad 2\,v\,\dot{u} - \dot{v} = 0, \quad \dot{u}^2 + v = 0, \quad \dot{u} \neq 0.$$

Consider (Σ_2). Simplify the second equation using the third one. One gets $v = 0$. This system thus simplifies as a regular differential system

$$(\Sigma_4) \qquad \dot{u} = 0, \quad v = 0$$

whose solutions are $u(x) = c$ and $v(x) = 0$ where c is an arbitrary constant. This system is a regular differential chain. Consider now (Σ_3) (Σ_3). The two first equations have the same leading derivative: it is nottriangular. To get a triangular set, apply Ritt's reduction algorithm which informally amounts to proceed as follows: replace $\dot{u}$ by $\dot{v}/(2\,v)$ in the second equation, giving

$$\left(\frac{\dot{v}}{2\,v}\right)^2 + v = 0.$$

Replace the second equation by the numerator of the reduced equation, provided that $v \neq 0$ and consider separately the solutions of (Σ_3) which annihilate v. One obtains a splitting of (Σ_3) into two systems

$$(\Sigma_5) \qquad 2\,v\,\dot{u} - \dot{v} = 0, \quad \dot{u}^2 + v = 0, \quad v = 0, \quad \dot{u} \neq 0$$

and

$$(\Sigma_6) \qquad 2\,v\,\dot{u} - \dot{v} = 0, \quad \dot{v}^2 + 4\,v^3 = 0, \quad \dot{u} \neq 0, \quad v \neq 0.$$

Consider (Σ_5). The equation $v = 0$ reduces to zero the first one, by Ritt's reduction algorithm. It also permits to simplify the second equation. We then get a system

$$(\Sigma_7) \qquad \dot{u}^2 = 0, \quad v = 0, \quad \dot{u} \neq 0$$

which is a regular differential system. The *regCharacteristic* algorithm may then be applied over it. By a gcd computation between the equation $\dot{u}^2 = 0$ and the inequation $\dot{u} \neq 0$, it concludes that this system has no solution. Let us discard it and come back to (Σ_6). It is not yet a regular differential system because the separant $2\,\dot{v}$ of the second equation does not belong to the inequation set. This is solved by splitting (Σ_6) into two systems which separate the solutions of (Σ_6) which satisfy $\dot{v} = 0$ from the ones which satisfy $\dot{v} \neq 0$. One gets two systems

$$(\Sigma_8) \qquad 2\,v\,\dot{u} - \dot{v} = 0, \quad \dot{v}^2 + 4\,v^3 = 0, \quad \dot{v} = 0, \quad \dot{u} \neq 0, \quad v \neq 0.$$

$$(\Sigma_9) \qquad 2\,v\,\dot{u} - \dot{v} = 0, \quad \dot{v}^2 + 4\,v^3 = 0, \quad \dot{v} \neq 0, \quad \dot{u} \neq 0, \quad v \neq 0.$$

Argumenting as for (Σ_7), we see that (Σ_8) has no solution. The system (Σ_9) (Σ_9) is a regular differential system. Its set of equations actually form a regular differential chain. We may then discard the inequation $\dot{u} \neq 0$ which is not an initial or a separant of the chain. The solutions of (Σ_9) actually are $u(x) = c_1 - \ln(x + c_2)$ and $v(x) = -1/(x + c_2)^2$ where c_1 and c_2 are arbitrary constants.

Summary. Every solution of (Σ_1) is either a solution of (Σ_4) or of (Σ_9). Conversely, the solutions of (Σ_4) and (Σ_9) are solutions of (Σ_1). Therefore,

$$\{\ddot{u} + v,\, \dot{u}^2 + v\} \quad = \quad [\dot{u},\, v] \cap [2\,v\,\dot{u} - \dot{v},\ \dot{v}^2 + 4\,v^3] : (v\,\dot{v})^\infty\,. \tag{28}$$

This decomposition permits to decide membership to the perfect differential ideal $\mathfrak{A}$ generated by Σ_1. Indeed, a differential polynomial $p \in \mathfrak{A}$ if and only if its normal form with respect to both regular differential chains is zero. This is actually the case for $v_{xx} + 6\,v^2$.

Let us assume that the two differential ideals on the right hand side of (28) are prime. It is not clear if the second one is included or not in the first one since the separants v and $\dot{v}$ belong to $[\dot{u},\, v]$. Performing the

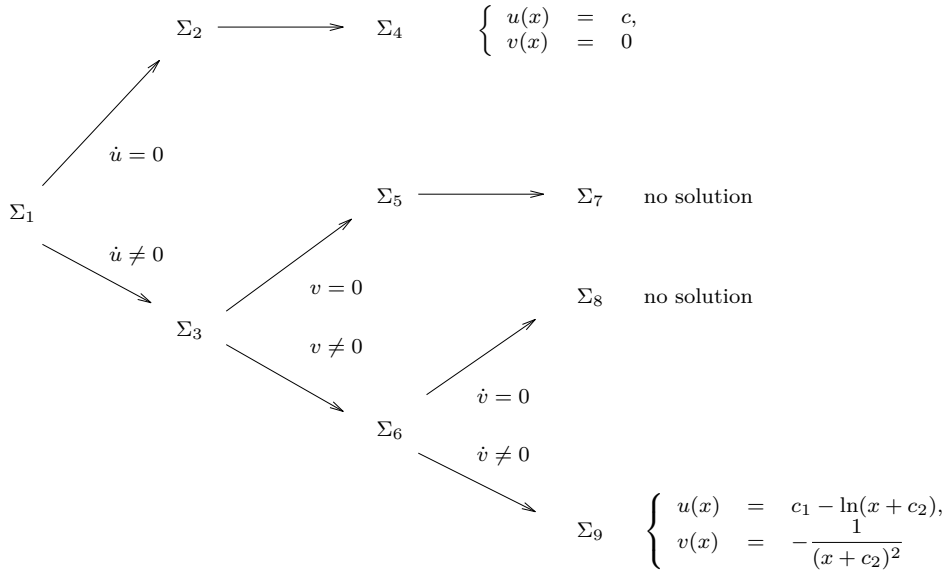

Figure 2: The splitting tree of Section 3.4.1.

elimination process over the same system, with respect to a ranking which eliminates v, one actually gets the following single regular differential chain

$$\{\ddot{u} + v,\, \dot{u}^2 + v\} \quad = \quad [v + \dot{u}^2,\, \ddot{u} - \dot{u}^2] \tag{29}$$

Its leading derivatives are v and $\ddot{u}$. The differential ideal defined by the chain is thus prime (if it were not prime, one of its equations would factor, which is impossible since their leading degrees are 1). We can then conclude that, in (28), the component $[\dot{u},\, v]$ is redundant.

On this case, we have been able to compute the minimal decomposition but this is not always possible. For this reason, we cannot, in general decide whether a differential polynomial p is a zero divisor in $\mathscr{R}/\mathfrak{A}$. Indeed, if $[\dot{u},\, v]$ had been an essential component, the differential polynomial v would have been a zero divisor in $\mathscr{R}/\mathfrak{A}$.

3.4.2 A Partial Differential Example

See Figure 3. The differential polynomial ring is $\mathscr{F}\{u, v\}$ endowed with two derivations δ_x and δ_y. The three differential polynomials of Σ_1 are denoted f_1, f_2 and f_3.

$$(\Sigma_1) \qquad u_y^2 - 4\,u = 0, \quad u_x - v_x\,u = 0, \quad v_y = 0.$$

The ranking is

$$\cdots > u_{xx} > u_{xy} > u_{yy} > v_{xx} > v_{xy} > v_{yy} > u_x > u_y > v_x > v_y > u > v.$$

The leading derivatives are thus u_y, u_x and v_y. The system is partially autoreduced and triangular. Is it coherent ? The two first equations form a critical pair $\{f_1,\, f_2\}$. To form the Δ-polynomial, differentiate the first equation by δ_x

$$\delta_x\, f_1 = 2\,u_y\,u_{xy} - 4\,u_x.$$

Differentiate the second equation by δ_y and multiply it by the separant $2\,u_y$ of the first equation, giving

$$2\,u_y\,\delta_y\,f_2 = 2\,u_y(u_{xy} - v_{xy}\,u - v_x\,u_y).$$

Subtract,

$$\Delta(f_1,\, f_2) = 2\, u\, u_y\, v_{xy} + 2\, u_y^2\, v_x - 4\, u_x.$$

The full reduction of this Δ-polynomial by (Σ_1) is detailed in (19), page 15. One gets a fourth equation $f_4 = u\, v_x = 0$ (the full remainder) which is inserted in the system

$$(\Sigma_2) \qquad u_y^2 - 4\, u = 0, \quad u_x - v_x\, u = 0, \quad v_y = 0, \quad u\, v_x = 0.$$

The insertion of f_4 implies that the critical pair $\{f_1,\, f_2\}$ is now solved. However, a new critical pair $\{f_3,\, f_4\}$ is generated. Before forming the new Δ-polynomial, the system is split on the initial of f_4. One then considers separately the solutions of (Σ_2) which annihilate u from the ones which do not. One gets

$$(\Sigma_3) \qquad u_y^2 - 4\, u = 0, \quad u_x - v_x\, u = 0, \quad v_y = 0, \quad u\, v_x = 0, \quad u = 0$$

and

$$(\Sigma_4) \qquad u_y^2 - 4\, u = 0, \quad u_x = 0, \quad v_y = 0, \quad v_x = 0, \quad u \neq 0.$$

The system (Σ_3) simplifies to

$$(\Sigma_5) \qquad v_y = 0, \quad u = 0$$

which actually is a regular differential chain. Its solutions are $u(x,\, y) = 0$ and $v(x,\, y) = \varphi(x)$ where $\varphi(x)$ is an arbitrary function of x.

Consider (Σ_4). The critical pair $\{f_1,\, f_2\}$ is solved. The critical pair $\{f_3,\, f_4\}$ is solved also since $\Delta(f_3,\, f_4) = 0$. This system is thus coherent. It is not yet a regular differential system because the separant u_y of f_1 does not belong to the inequation set. One then splits (Σ_4) into

$$(\Sigma_5) \qquad u_y^2 - 4\, u = 0, \quad u_x = 0, \quad v_y = 0, \quad v_x = 0, \quad u_y = 0, \quad u \neq 0$$

and

$$(\Sigma_6) \qquad u_y^2 - 4\, u = 0, \quad u_x = 0, \quad v_y = 0, \quad v_x = 0, \quad u_y \neq 0, \quad u \neq 0.$$

System (Σ_5) has no solution: the new equation $u_y = 0$ permits to simplify the first one and obtain $u = 0$, which is incompatible with the inequation $u \neq 0$. System (Σ_6) is a regular differential system. Its set of equations even for a regular differential chain. The *regCharacteristic* algorithm permits to prove that the inequation $u \neq 0$, which is not an initial or a separant of the chain, is regular modulo the differential ideal defined by the chain. It is thus discarded. The solutions of (Σ_6) are $u(x,\, y) = (y + c_1)^2$ and $v(x,\, y) = c_2$ where c_1 and c_2 are arbitrary constants.

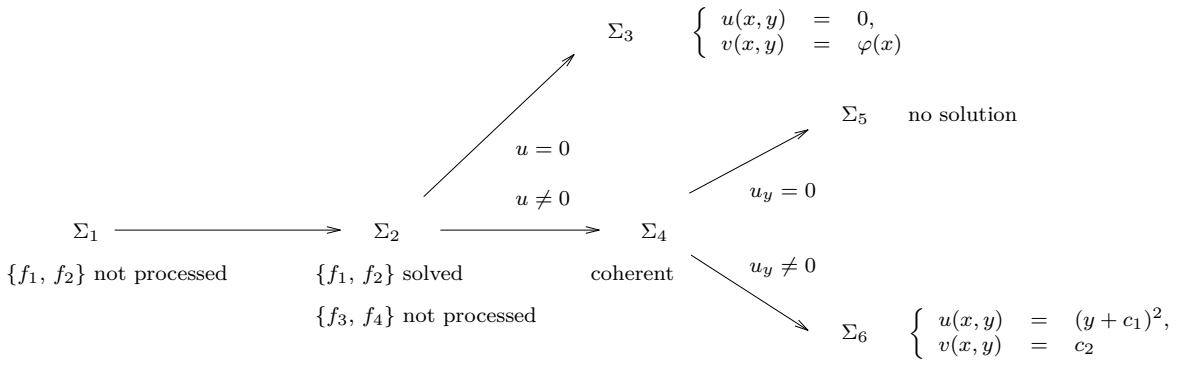

Figure 3: The splitting tree of Section 3.4.2.

Summary. Every solution of (Σ_1) is a solution of (Σ_3) or (Σ_6), and conversely. Thus

$$\{u_y^2 - 4\,u,\, u_x - v_x\,u,\, v_y\} \quad = \quad [u,\, v_y] \cap [u_y^2 - 4\,u,\, u_x,\, v_y,\, v_x] : (u_y)^\infty\,. \tag{30}$$

By normal form computations, it is easy to see that u and v_x do not belong to the perfect differential ideal $\mathfrak{A}$ generated by Σ_1. However, the product $u\,v_x$ belongs to $\mathfrak{A}$ (its normal form modulo each regular differential chain on the right hande side of (30) is zero). Thus $\mathfrak{A}$ is thus not a prime differential ideal.

References

[1] Fuensanta Aroca, Cristhian Garay, and Zeinab Toghani. The Fundamental Theorem of Tropical Differential Algebraic Geometry. *Pacific J. Math.*, (283):257–270, 2016. `arXiv:1510.01000v3`.

[2] François Boulier. Réécriture algébrique dans les systèmes d'équations différentielles polynomiales en vue d'applications dans les Sciences du Vivant, May 2006. Mémoire d'habilitation à diriger des recherches. Université Lille I, LIFL, 59655 Villeneuve d'Ascq, France. `http://tel.archives-ouvertes.fr/tel-00137153`.

[3] François Boulier and François Lemaire. A Normal Form Algorithm for Regular Differential Chains. *Mathematics in Computer Science*, 4(2):185–201, 2010. 10.1007/s11786-010-0060-3.

[4] François Boulier, Daniel Lazard, François Ollivier, and Michel Petitot. Representation for the radical of a finitely generated differential ideal. In *ISSAC'95: Proceedings of the 1995 international symposium on Symbolic and algebraic computation*, pages 158–166, New York, NY, USA, 1995. ACM Press. `http://hal.archives-ouvertes.fr/hal-00138020`.

[5] François Boulier, Daniel Lazard, François Ollivier, and Michel Petitot. Computing representations for radicals of finitely generated differential ideals. *Applicable Algebra in Engineering, Communication and Computing*, 20(1):73–121, 2009. (1997 Techrep. IT306 of the LIFL).

[6] François Boulier, François Lemaire, Marc Moreno Maza, and Adrien Poteaux. A Short Contribution to the Theory of Regular Chains. *Mathematics in Computer Science (submitted)*, 2019. Presented at CASC 2019. Available at `http://hal.archives-ouvertes.fr/hal-02189197`.

[7] François Boulier, François Lemaire, Marc Moreno Maza, and Adrien Poteaux. An Equivalence Theorem For Regular Differential Chains. *Journal of Symbolic Computation*, 93:34–55, 2019. doi:`10.1016/j.jsc.2018.04.011`.

[8] François Boulier, François Lemaire, Adrien Poteaux, and Marc Moreno Maza. An Equivalence Theorem for Regular Differential Chains. *Journal of Symbolic Computation*, 93:34–55, 2019. `hal.archives-ouvertes.fr/hal-01391768`.

[9] Changbo Chen, Oleg Golubitsky, François Lemaire, Marc Moreno Maza, and Wei Pan. Comprehensive Triangular Decompositions. In *Proceedings of CASC'07*, pages 73–101, 2007.

[10] Jan Denef and Leonard Lipshitz. Power Series Solutions of Algebraic Differential Equations. *Mathematische Annalen*, 267:213–238, 1984.

[11] Lionel Ducos. source of the axiom package `prs.spad`, 1999. `http://www-math.sp2mi.univ-poitiers.fr/~ducos/src/travaux.html`.

[12] Ellis Robert Kolchin. *Differential Algebra and Algebraic Groups*. Academic Press, New York, 1973.

[13] Serge Lang. *Algebra*. Addison-Wesley, 1965. Second printing (1967).

[14] Youri Matiiassevitch. Enumerable sets are diophantine. *Sov. Math. Dokl.*, 11:354–357, 1970.

[15] Sally Morrison. Pseudo–Reduction, Second Preliminary Draft. private communication, december 1995.

[16] Sally Morrison. The Differential Ideal $[P] : M^{\infty}$. *Journal of Symbolic Computation*, 28:631–656, 1999.

[17] Joseph Fels Ritt. *Differential Algebra*, volume 33 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, New York, 1950.

[18] Azriel Rosenfeld. Specializations in differential algebra. *Trans. Amer. Math. Soc.*, 90:394–407, 1959.

[19] Abraham Seidenberg. An elimination theory for differential algebra. *Univ. California Publ. Math. (New Series)*, 3:31–65, 1956.

[20] Abraham Seidenberg. Abstract differential algebra and the analytic case. *Proc. Amer. Math. Soc.*, 9:159–164, 1958.

[21] Bruno Louis van der Waerden. *Algebra*. Springer Verlag, Berlin, seventh edition, 1966.

[22] Oscar Zariski and Pierre Samuel. *Commutative Algebra*. Van Nostrand, New York, 1958. Also volumes 28 and 29 of the *Graduate Texts in Mathematics*, Springer Verlag.

Index