ESSENTIAL COMPONENTS OF AN ALGEBRAIC DIFFERENTIAL EQUATIOS

EVELYNE HUBERT

Abstract. We present an algorithm to determine the essential singular components of an algebraic differential equation. Geometrically, this corresponds to determining the singular solution that have enveloping properties. The algorithm is practical and efficient because it is factorization free, unlike the previous such algorithm.

1. Introduction

We present an algorithm to determine the set of *essential singular solutions* of a differential equation. Essential singular solutions can be informally described as follows: *the general solution of a differential equation is usually described as a solution depending on a number of arbitrary constants equal to the order of the differential equation. Then essential singular solutions are those that cannot be obtained by substituting numerical values to the arbitrary constants in the general solution. Adherence*, defined in (Ritt 1950, VI.2), is the correct concept: singular solutions that are not essential are adherent to the general solution or to one of the essential singular solutions.

For first order differential equations, Hamburger (1893) showed that the essential singular solutions were envelopes of the family of curves given by the *general solution*. Ritt gave a similar result for first order partial differential equations (Ritt 1945a) and for special cases of second order differential equations (Ritt 1946). These analytic and geometric properties may be seen as a first application for our algorithm. Nonetheless the concepts involved translate into algebraic definitions and properties. We shall thus work in the frame of differential algebra. Central there is the definition of the general solution due to Ritt (1930).

A system of algebraic differential equations can be seen as a set Σ of differential polynomials in an appropriate differential polynomial ring. The radical differential ideal generated by Σ can be written as the irredundant intersection of a finite number of prime differential ideals called the components of the radical differential ideal. In the case Σ consists of a single differential polynomial that is irreducible when considered as a polynomial, one of these components defines the general solution. The others are *essential singular components*.

Research at MSRI is supported in part by NSF grant DMS-9701755. Part of this paper has been written while the author's postdoctoral stay at the Symbolic Computation Group.

For our purpose, we will extend the definition of the general component to *regular* differential polynomials. Regular differential polynomials arise in practical algorithm dealing with differential algebraic systems. They form a wider class of differential polynomials than irreducible differential polynomials.

Ritt (1950) also developed an algorithm to decompose the radical differential ideal generated by a finite set Σ of differential polynomials into a finite intersection of prime differential ideals. This reduction-decomposition process allows us to test when a differential algebraic system admits no solution (the triviality of the system). Furthermore, the decomposition obtained provides a membership test to the radical differential ideal generated by Σ. Unfortunately the Ritt decomposition algorithm involves factorizations in towers of algebraic extensions. This algorithm is thus impractical and we know no implementation of it.

For a single differential polynomial Ritt (1936, 1945b) and Levi (1942, 1945) presented a process to discard the redundant components or, equivalently, determine the essential singular components from a Ritt decomposition. The keystones of the method are the component theorem and the low power theorem. The component theorem states that any essential singular component of a differential polynomial is the general component of an irreducible differential polynomial, even for partial differential polynomials. The low power theorem is a necessary and sufficient condition for the general component of an irreducible differential polynomial to be an essential singular component of another differential polynomial.

The low power theorem and the component theorem are among the most sophisticated theorems in differential algebra. Ritt (1936) first proved the low power theorem for ordinary differential equations in one differential indeterminate and with meromorphic coefficients. His proof involved complex analysis argumentation. Algebraization of the proofs allowed the extensions of the result to abstract differential fields and to partial differential equations. Levi (1942 and 1945) brought a purely algebraic proof of the sufficiency, the core of it being a lemma named after him. The necessity, as well as the component theorem, are shown to rely on the *leading coefficient theorem*, the most general form of which was given by Hillman (1943) and in (Hillman and Mead 1962).

In this paper we give a complete algorithm to compute a *minimal regular decomposition*. This type of minimal decomposition is more compact than the minimal prime decomposition but is not unique and depends on the ranking we chose. A minimal regular decomposition, nonetheless, contains all the information of the minimal prime decomposition; to recover the latter from the former, only factorization of squarefree polynomials are required. The process to compute a minimal regular decomposition that we propose here requires only Ritt reduction (differentiations and pseudo-divisions) and gcd computations. No factorization nor Groebner bases computations are needed. Our method provides thus an algorithmic practicality that the method of Ritt and Levi did not have. The process requires results in algebra[1] for which we will give concise proofs (Theorem 3.2, Theorem 4.8). Our process also

[1] also used in (Boulier *et al.* 1995)

requires extensions of the low power theorem and the component theorem to regular differential polynomials (Theorem 4.9, Theorem 6.2, Theorem 6.1). Our paper is self-contained in the sense it depends only on results present in textbooks, mainly (Kolchin 1973).

The second section of this paper is devoted to set the notations and recalls the background material in differential algebra required for the following sections. The third section discusses from a general point of view existing decomposition algorithms to represent the radical of a finitely generated differential ideal and establishes a less restrictive decomposition that proves sufficient for our purpose. In the fourth section we proceed to extend the definition of the general solution as well as the component theorem with regards to regular differential polynomials. Section 6 presents the extension of the low power theorem to regular differential polynomials. The necessary and sufficient conditions for a regular component to be essential are read on a preparation polynomial. The algorithm to compute this preparation polynomial is described in Section 5. It is an appropriate modification of the preparation process given by (Ritt 1936). The complete algorithm to compute a minimal regular decomposition of the radical differential ideal generated by a single differential polynomial will be found in Section 7 together with a series of examples.

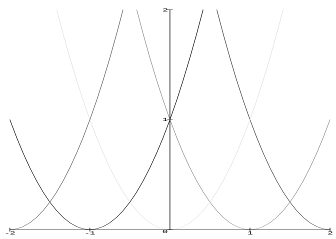
A note on the implementation: the algorithm presented in this paper is implemented in Maple V. It is part of the *diffalg* package developed by F.Boulier and the author during their postdoctoral stay at the Symbolic Computation Group[2] (Maple's lab). The package is available at *http://daisy.uwaterloo.ca/~ehubert/Diffalg*.

Illustration on first order ordinary differential equations

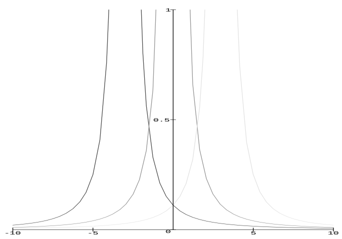
Consider the two similar differential equations $p_1 \equiv {y'}^2 - y = 0$ and $p_2 \equiv {y'}^2 - y^3 = 0$. If they admit a singular solution, it should satisfy $\dfrac{\partial p_i}{\partial y'} \equiv 2\,y' = 0,\ i = 1, 2.$

Actually, for both differential equations $y(t) = 0$ is the only singular solution. The general solutions of the differential equations can be given respectively as $\tilde{y_1}(t) = \frac{1}{4}(t-c)^2$ and $\tilde{y_2}(t) = \frac{4}{(t-c)^2}$, where c is an arbitrary constant.

Solutions of ${y'}^2 - y = 0$



Solutions of ${y'}^2 - y^3 = 0$



[2]I wish to express here my gratitude to Pr. G. Labahn and K.O. Geddes for their support

In the case of the first equation, $p_1 = 0$, the singular solution is essential: it is a an envelope of the graphs of the nonsingular solutions. On the contrary, for $p_2 = 0$ the singular solution is not essential and it can be seen as a limiting case of the non-singular solutions when c tends toward infinity.

In these two examples, would it be possible to forecast the behavior of the non-singular solutions in the vicinity of the singular solution without knowing a closed form of the general solution? In other words, how do we determine if $y(t) = 0$ is an essential singular solution or not? The answer is given by the low power theorem: p_1 has a unique term of lowest degree and this term involves no proper derivative of y, while this is not the case in p_2.

2. Differential algebra preliminaries and notations

Differential algebra extends the concepts of polynomial algebra to differential equations. The purpose of this section is to give a brief overview of the material we will need in the following sections and to specify the notations. We mostly use the definitions and properties which are given by Kolchin (1973).

We consider *differential rings* $(\mathcal{R}, \Theta)$, where $\mathcal{R}$ is a commutative integral domain that contains a field isomorphic to $\mathbb{Q}$, and Θ is the free commutative monoid of the derivation operators generated by a finite set of *derivations* Δ. When Δ consists of a single derivation δ we shall speak of the ordinary differential ring $\mathcal{R}$.

Let Σ be a subset of $\mathcal{R}$. We denote respectively (Σ), $[\Sigma]$ and $\{\Sigma\}$ the ideal, the differential ideal and the radical differential ideal generated by Σ.

Proposition 2.1. *Let Σ be a subset of the differential ring $\mathcal{R}$. Let a_i, $1 \leq i \leq r$, be elements of $\mathcal{R}$. Then*

$$\left\{\Sigma, \prod_{i=1}^{r} a_i\right\} = \bigcap_{i=1}^{r} \{\Sigma, a_i\}$$

For a subset I in $\mathcal{R}$ and an element $s \in \mathcal{R}$ we define the saturation and the quotient of I w.r.t. s by $I : s^\infty = \{a \in \mathcal{R} \mid \exists \alpha \in \mathbb{N}\ s^\alpha a \in I\}$ and $I : s = \{a \in \mathcal{R} |\ sa \in I\}$. We have $I \subset I : s \subset I : s^\infty$. If I is a differential ideal, $I : s^\infty$ is also a differential ideal. If I is a radical differential ideal, $I : s$ is a radical differential ideal and is equal to $I : s^\infty$.

Proposition 2.2. *Let Σ be a non-empty subset of $\mathcal{R}$ and s an element of $\mathcal{R}$. Then $\{\Sigma\} = \{\Sigma\} : s \cap \{\Sigma, s\}$.*

Proposition 2.3. *Let R_1 and R_2 be radical differential ideals and s an element of $\mathcal{R}$. Then $(R_1 \cap R_2) : s = R_1 : s \cap R_2 : s$.*

$(\mathcal{R}\{Y\}, \Theta)$ denotes the ring of differential polynomials with differential indeterminates $Y = \{y_1, \ldots, y_n\}$ and coefficients in $(\mathcal{R}, \Theta)$. Setwisely, $\mathcal{R}\{Y\}$ is the polynomial ring in infinitely many indeterminates $\mathcal{R}[\Theta Y] = \mathcal{R}[\{\theta y_i,\ y_i \in Y,\ \theta \in \Theta\}]$.

We will consider rings $\mathcal{F}\{Y\}$ of differential polynomials the coefficients of which belong to a differential field $\mathcal{F}$ of characteristic zero. For computational purposes we will typically choose a rational function field $\mathcal{F} = \mathcal{K}(t_1, \dots, t_\mu)$ where $\mathcal{K}$ is a finite extension of $\mathbb{Q}$.

In our examples, we will use the following notations. For an ordinary differential ring in one or two differential indeterminates we will mostly use $\mathbb{Q}(t)\{y\}$ or $\mathbb{Q}(t)\{x, y\}$. The derivation δ will be understood to be with respect to the independent variable t and we will use the standard notation $y' = \delta y,\ y'' = \delta^2 y,\ \dots,\ y^{(i)} = \delta^i y$. Partial differential rings will generally involve two independent variables s and t and the corresponding derivations will be noted δ_s and δ_t. Derivatives will be denoted with the usual subscript notation. For instance, in $\mathbb{Q}(s, t)\{y\}$, we will note $y_s = \delta_s y,\ y_{ss} = \delta_s^2 y,\ y_{st} = \delta_s \delta_t y, \dots$.

Any radical differential ideal R in $\mathcal{F}\{Y\}$ is the intersection of a finite set of prime differential ideals none of which contains another (Kolchin 1973, III.4, the basis theorem and 0.9 Theorem 1). This unique set is the set of *essential prime components* of R and forms the *minimal prime decomposition* of R.

A *zero* of a set Σ of differential polynomials in $\mathcal{F}\{Y\}$ is an $n-$tuple $\nu = (\nu_1, \dots, \nu_n)$ in a field extension $\mathcal{F}'$ of $\mathcal{F}$, such that the differential polynomials of Σ vanish when one replaces each y_i by ν_i. Such a zero exists if and only if $1 \notin \{\Sigma\}$ (Kolchin 1973, IV.2, the theorem of zero).

When A is a finite subset of $\mathcal{F}\{Y\}$, $\Theta_A Y$ will denote

- the set of derivatives occuring in A when we need a result about commutative polynomial algebra.
- the set of derivatives that are not proper derivatives of the leaders of the elements of A.

The ideal (A) will then denote the ideal generated by A in $\mathcal{F}[\Theta_A Y]$. The extension and contraction from one meaning of $\mathcal{F}[\Theta_A Y]$ to the other does not affect the ideal (A) (Kolchin 1973, IV.9, remark after lemma 2).

3. Decomposition algorithms

Describing a decomposition algorithm is a tremendous task and is out of the scope of this paper. The fact is that we do not need to complete such an algorithm in order to determine a minimal decomposition of the radical differential ideal generated by a single differential polynomial in $\mathcal{F}\{Y\}$. We shall therefore sketch the steps of a Ritt like algorithm in order to point out which computations are unnecessary and which type of decomposition and notions will prove to be sufficient for our purpose. We repeat only the definitions that are necessary for the reading of the rest of the paper. Though there has been some effort (Boulier *et al.* 1997) to generalize the definitions and results, we shall use here, for simplicity, the more traditional material to be found in (Kolchin 1973).

A ranking over $\mathcal{F}\{Y\}$ is a total order on $\Theta Y = \{\theta y_i,\ i = 1, \dots, n,\ \theta \in \Theta\}$ such that for any derivative $u \in \Theta Y$ we have $\delta u \geq u$, $\forall \delta \in \Delta$ and for any pair of derivatives $u, v \in \Theta Y$ with $u \geq v$ we have $\delta u \geq \delta v$, $\forall \delta \in \Delta$.

Let p be a differential polynomial of $\mathcal{F}\{Y\}$. The *leader* u_p and the *initial* i_p of p are respectively the highest ranking derivative appearing in p and the coefficient of its highest power in p. The *separant* of p is $s_p = \frac{\partial p}{\partial u_p}$. θu_p and s_p are respectively the leader and the initial of θp when θ is a proper derivation operator (i.e. not the identity):

$$\begin{aligned} p &= i_p\, u_p^d + i_{d-1}\, u_p^{d-1} + \cdots + i_0, \\ \theta p &= s_p \theta u_p + q, \quad \text{where } q \text{ has no derivative equal or higher than } \theta u_p. \end{aligned}$$

A differential polynomial q is *partially reduced w.r.t.* p if no proper derivatives of u_p appears in q; q is *reduced w.r.t.* p if q is partially reduced w.r.t. to p and the degree of q in u_p is strictly less then the degree of p in u_p.

A subset A of $\mathcal{F}\{y_1, \ldots, y_n\}$ is called autoreduced if no element of A belongs to $\mathcal{F}$ and each element of A is reduced w.r.t. all the others. Distinct elements of A have dinstinct leaders and A must be finite (Kolchin 1973, I.9). We denote by I_A and S_A respectively the product of the initials and the separants of the elements of A; We note $H_A = I_A\, S_A$.

Given an autoreduced set A of $\mathcal{F}\{y_1, \ldots, y_n\}$ and p there exist *reduction* algorithms[3] involving differentiation and pseudo-division to compute $\bar{p}$ partially reduced w.r.t. every element of A such that $\exists \alpha \in \mathbb{N}\ S_A^\alpha p \equiv \bar{p} \mod [A]$. Similarly we can compute $\bar{p}$ reduced w.r.t. every element of A such that $\exists \alpha, \beta \in \mathbb{N}\ S_A^\alpha I_A^\beta p \equiv \bar{p} \mod [A]$. We write $p \longrightarrow_A \bar{p}$.

Characteristic sets can be defined as follow: an autoreduced set A is a characteristic set of a differential ideal I if $A \subset I$ and $\forall p \in I,\ p \longrightarrow_A 0$. Note that

- an autoreduced set A is not obviously a characteristic set of $[A] : H_A^\infty$.
- if A, an autoreduced set, is a characteristic of a differential ideal of $\mathcal{F}\{Y\}$ then A is *coherent*[4] (Rosenfeld 1959, I.2), (Kolchin 1973, III.8).

What we mean by a complete decomposition algorithm can be specified as follows.

Proposition 3.1. *Let Σ be a finite set of differential polynomials in $\mathcal{F}\{Y\}$. There exist algorithms to compute a finite number of* autoreduced sets $C_1, \ldots, C_r$, *such that*

$$\{\Sigma\} = \bigcap_{i=1}^{r} [C_i] : H_{C_i}^\infty, \tag{1}$$

and where C_i is a characteristic set *of $[C_i] : H_{C_i}^\infty$. We shall call such a decomposition a* characteristic decomposition *of $\{\Sigma\}$.*

The first such decomposition algorithm for ordinary differential polynomials is due to Ritt (1950). The algorithm generalised to the partial differential case is presented in (Kolchin 1973, IV.9). The $[C_i] : H_{C_i}^\infty$ in the result are prime differential ideals.

[3] see for instance (Kolchin 1973, I.9, Proposition 1)

[4] Coherence corresponds to *formal integrability* or *involutivity* in other formalisms

It requires factorizations in towers of algebraic extensions. We do not know of any implementation of this algorithm.

Boulier *et al.* (1997) presents an effective characteristic decomposition algorithm using the Seidenberg (1956) elimination scheme. The algorithm is an improvement over the one presented in (Boulier *et al.* 1995).

None of these algorithm provide a minimal decomposition. Determining a minimal decomposition for Σ can be thought of as eliminating the redundancy in one these decomposition. It is the way Ritt did proceed for determining the minimal decomposition of the radical differential ideal generated by a single differential polynomial in $\mathcal{F}\{Y\}$.

The first and well known part of the Ritt algorithm is the following. Let Σ be a finite set of differential polynomials of $\mathcal{F}\{Y\}$. With a finite number of differentiations and arithmetic operations in $\mathcal{F}\{Y\}$, we can compute a coherent autoreduced set A such that $A \subset [\Sigma]$ and $\forall p \in \Sigma,\ p \longrightarrow_A 0$. Thus $A \subset [\Sigma] \subset [A] : H_A^\infty$. For a detailed treatment we invite the reader to refer to (Kolchin 1973, IV.9, page 168) or, for a presentation consistent with this section (Hubert 1997, part II).

To proceed in the algorithm, Ritt, in the ordinary case, and Kolchin (1973, IV.9) used a particular case (Kolchin 1973, IV.9, lemma 2) of a theorem by Rosenfeld (1959, I.2), (Kolchin 1973, III.8, lemma 5) which allows to decide when $[A]:H_A^\infty$ is prime and A is one of its characteristic set. Boulier (1995) was the first to use the following property which allows us to proceed in the algorithm without going down to prime differential ideals. Thanks to Rosenfeld's lemma and its corollaries, proving the property amounts to applying the Jacobian criterion for regularity. The form of this commutative algebra result that we will use here has been applied in direct algorithms for the computation of primary decomposition of ideals (Eisenbud *et al.* 1992), (Vasconcelos 1998).

Theorem 3.2. *Let A be a coherent autoreduced set of $\mathcal{F}\{Y\}$. $[A]:H_A^\infty$ is a radical differential ideal.*

Proof. Note first that for any finitely generated ideal I and any f in a polynomial ring $\mathcal{F}[X]$, $I:f^\infty$ is equal to the intersection of those primary components of I with radical not containing f (Eisenbud *et al.* 1992, lemma 2.4).

S_A, the product of the separants of A, is the determinant of a maximal square submatrix of the Jacobian matrix of the set of polynomials A in the polynomial ring $\mathcal{F}[\Theta_A Y]$. Thus S_A belongs to the Jacobian ideal of (A).

If $1 \in (A):H_A^\infty$ then $[A]:H_A^\infty = \mathcal{F}\{Y\}$ and the result is trivial. Assume $1 \notin (A):H_A^\infty$. By the Jacobian criterion for regularity (Vasconcelos 1998, corollay 5.2.1, page 127), the primary components of (A) with radical not containing the Jacobian ideal are prime. This is the case of all the primary components of (A) the intersection of which is equal to $(A):S_A^\infty$. Thus $(A):S_A^\infty$ is an intersection of prime ideals; it is radical and thus so is $((A):S_A^\infty):I_A^\infty = (A):H_A^\infty$. By Rosenfeld's lemma and its corollaries (Kolchin 1973, III.8, lemma 5 and lemma 6), $[A]:H_A^\infty$ is radical. $\square$

Thus $[A] \subset \{\Sigma\} \subset [A]:H_A^\infty$ and therefore $\{\Sigma\}:H_A \subset [A]:H_A^\infty$; by Proposition 2.1 and 2.2

$$\{\Sigma\} = [A]:H_A^\infty \cap \bigcap_{a\in A} \left(\{\Sigma, i_a\} \cap \{\Sigma, s_a\}\right).$$

We loop over the argument for $\{\Sigma, i_a\}$ and $\{\Sigma, s_a\}$. As these ideals contain autoreduced sets *lower* (Kolchin 1973, I.10) than A, we obtain a decomposition $\{\Sigma\} = \bigcap_{i=1}^r [A_i] : H_{A_i}^\infty$, where the A_i are coherent autoreduced sets, in a finite number of iterations[5]. We ennunciate this result for later reference in a defining proposition.

Proposition 3.3. *Given a finite set of differential polynomials in $\mathcal{F}\{Y\}$ we can compute a finite number of coherent autoreduced sets $A_1, \dots, A_r$ such that*

$$\{\Sigma\} = \bigcap_{i=1}^{r}[A_i]:H_{A_i}^\infty.$$

The ideals $[A_i]:H_{A_i}^\infty$ are radical and are called regular components[6] *of $\{\Sigma\}$. We will call such a decomposition a* regular decomposition *of $\{\Sigma\}$.*

To obtain a characteristic decomposition from a regular decomposition the following steps shall be undertaken.

- eliminate the components $[A_i] : H_{A_i}^\infty$ that contain 1. This can be tested by a purely algebraic procedure thanks to Rosenfeld's lemma (Kolchin 1973, III.8, lemma 5) and, for instance, a Groebner basis computation of $(A):H_A^\infty$.
- compute a characteristic decomposition for each regular component $[A_i]:H_{A_i}^\infty \neq \mathcal{F}\{Y\}$ i.e. compute a decomposition $[A_i] : H_{A_i}^\infty = \bigcap_{j=1}^{r_i}[C_{ij}] : H_{C_{ij}}^\infty$ whith the property that C_{ij} is a characteristic set of $[C_{ij}] : H_{C_{ij}}^\infty$. A procedure to do so, based on Groebner basis computations, is presented in (Boulier *et al.* 1997). This is, in some sense, an easier task then the work of Proposition 1 because regular components have properties very closed to prime ideals (Theorem 4.8).

Our goal in this paper is to determine a minimal decomposition of a radical differential ideal generated by a single differential polynomial of $\mathcal{F}\{Y\}$. We will see that to this end these latter computations are unnecessary. All we need to proceed is a regular decomposition as defined in Proposition 3.3.

4. Regular structure of a differential polynomial

We proceed to define singular and general solution from an algebraic point of view. The founding work in that direction is due to Ritt (1930) who defined the general solution of an irreducible differential polynomial. We extend here this definition and, what is more important, the component theorem to *regular* differential polynomials. The reason is that this type of differential polynomials naturally arises in effective

[5]because of (Kolchin 1973, I.10, proposition 3)
[6]this name was introduced by (Boulier *et al.* 1995)

algorithms in differential algebra. We will then proceed to define a minimal regular decomposition of a single differential polynomial.

4.1. **Singular and general components.** After the work of Darboux (1870), the singular zeros of a differential polynomial in a single differential indeterminate have been defined as the common zeros of p and the partial derivative of p according to its highest order derivative, what we call the separant, s_p. This is nonetheless not equivalent to the original idea that a singular solution cannot be obtained from the solution which contains a number of arbitrary constants equal to the order of the differential polynomial.

Example 4.1. *Consider the differential polynomial* $p = {y'}^3 - 4\,t\,y\,y' + 8\,y^2$ *in* $\mathbb{Q}(t)\{y\}$. *If there is any singular zero, it is a common zero of* p *and* $s_p = \frac{\partial p}{\partial y'} = 3\,{y'}^2 - 4\,t\,y$. *There are actually two singular zeros:* $\bar{y}(t) \equiv 0$ *and* $\hat{y}(t) = \frac{4}{27}t^3$.

The general zero *can be given by* $\tilde{y}(t) = a\,(t-a)^2$, *where* a *is an arbitrary constant. Contrary to* $\hat{y}$, *the singular zero* $\bar{y}(t) \equiv 0$ *is obtained from the general zero by replacing* a *by a numeric value, namely* $a = 0$.

For partial differential polynomials or differential polynomials in several differential indeterminates, the separant depends on the ranking. The work of Darboux (1873) suggests that the singular solutions should be defined as the common zero of p and all its possible separants. To simplify the wording we will nonetheless adopt the following definition, being aware it addresses a wider set of components than the ones suggested by Darboux. But our ultimate goal will be to find the essential singular components. These latter do not depend on the ranking.

Definition 4.2. *Let* p *be a differential polynomial in* $\mathcal{F}\{Y\}$, *endowed with a ranking. Let* s_p *be the separant of* p. *A prime differential ideal containing* $\{p, s_p\}$ *is a singular prime component of* p. *Similarly, a regular differential ideal containing* $\{p, s_p\}$ *is a singular regular component of* p.

The zeros of p for which s_p does not vanish, the *non-singular zeros*, are naturally part of the zeros of the so called *general component.* Recall from Property 2.2 that $\{p\} = \{p\} : s_p \cap \{p, s_p\}$. As $\{p\} : s_p$ does not contain s_p, the non-singular zeros must be zeros of $\{p\} : s_p$.

When p is an irreducible differential polynomial, Ritt (1945b) proved that there is a unique essential prime component of $\{p\}$ that contains no separant, whatever the ranking is. For a given ranking, this component is $\{p\} : s_p$ (Kolchin 1973, IV.6, Theorem 3).

We introduce here a more general class of differential polynomials that naturally arise in a regular decomposition. First note the following property that we will use extensively.

Proposition 4.3. *Let* p *be any differential polynomial in* $\mathcal{F}\{Y\}$. *Let* $\tilde{p}$ *be the product of all the simple factors of* p *involving* u_p. *We have* $\tilde{p} = \frac{p}{gcd(p, s_p^2)}$.

- *A differential polynomial q of $\mathcal{F}\{Y\}$ that is partially reduced w.r.t. p belongs to $[p]:s_p^\infty$ iff it is divisible by $\tilde{p}$.*
- *$[p]:s_p^\infty$ is a radical differential ideal and thus $\{p\}:s_p = [p]:s_p^\infty$.*

Proof. These properties can be seen as a particular case of Rosenfeld's lemma (Rosenfeld 1959) and of Theorem 3.2. Their proofs are nonetheless simpler.

- By (Kolchin 1973, I.11, corollary 2) $q \in (p):s_p^\infty$. We just observe that $(p):s_p^\infty = (\tilde{p})$.
- Consider $q \in \mathcal{F}\{Y\}$ such that $\exists n \in \mathbb{N},\ q^n \in [p]:s_p^\infty$. Let $q \longrightarrow_p \bar{q}$: there exists $\alpha \in \mathbb{N}$ $s_p^\alpha\, q \equiv \bar{q} \mod [p]$. Then, $s_p^{n\alpha}\, q^n \equiv \bar{q}^n \mod [p]$. Therefore, $\tilde{q}^n$ is divisible by $\tilde{p}$. As $\tilde{p}$ is squarefree, $\tilde{p}$ must divide $\bar{q}$. Thus $q \in [p]:s_p^\infty$.

Definition 4.4. *Let $\mathcal{F}\{Y\}$ be endowed with a ranking. A differential polynomial p of $\mathcal{F}\{Y\}$ is regular provided p does not belong to $\mathcal{F}$ and p has no common factors with its separant s_p. In other words, p is square free and has no factor independent of its leader.*

In the previous propostion, $\tilde{p}$, when not belonging to $\mathcal{F}$, is a regular differential polynomial. When p is itself regular, then $\tilde{p} = p$.

If p is a regular differential polynomial of $\mathcal{F}\{Y\}$, its decomposition into irreducible factors can be written $p = \prod_{k=1}^r p_k$ where the p_i are all distinct and have a common leader: $u_p = u_{p_1} = \cdots = u_{p_r}$. If s_{p_k} and i_{p_k} are the respective separant and initials of the irreducible factors p_k then

$$s_p = \sum_{k=1}^{r} s_{p_k} \prod_{j \neq k, j=1}^{r} p_j \quad \text{and} \quad i_p = \prod_{k=1}^{r} i_{p_k}$$

Irreducible differential polynomials over $\mathcal{F}$ are regular differential polynomials of $\mathcal{F}\{Y\}$. Consider $\mathcal{F}'$ a differential field extension of $\mathcal{F}$. If p is irreducible in $\mathcal{F}\{Y\}$, p might be reducible in $\mathcal{F}'\{Y\}$. It nonetheless remains regular in $\mathcal{F}'\{Y\}$. Regularity is a property that is conserved through extension of the field of coefficients. If we can work only with regular differential polynomials, we will not have to consider which field of coefficients we work with. Only the coefficients effectively involved in the differential polynomials will be of importance. But note that, contrary to irreducibility, regularity depends on the ranking defined on $\mathcal{F}\{Y\}$.

Example 4.5. *In the differential ring $\mathcal{F}\{u, v\}$, the differential polynomial $p = u^2 - u + u\,v - v = (u+v)\,(u-1)$ is regular if the ranking satisfies $u > v$. It is not so if the ranking is such that $v > u$.*

Definition 4.6. *Let A be an coherent autoreduced subset of $\mathcal{F}\{Y\}$ such that $p \in [A]:H_A^\infty$. $[A]:{}_A^\infty$ will be said to be a* redundant *regular component of p if none of its prime components are essential for $\{p\}$. $[A]:H_A^\infty$ will be said to be an* essential *regular component of p if each essential prime component of $[A]:H_A^\infty$ in $\mathcal{F}'\{Y\}$, is an essential prime components of $\{p\}$ in $\mathcal{F}'\{Y\}$, for any differential field extension $\mathcal{F}'$ of $\mathcal{F}$.*

Note that a regular component of $\{p\}$ can be neither essential nor redundant. In Example 7.5 we will encounter such a case where a regular component $[a]:h_a$ can be split into two regular components $[a]:h_a^\infty = [a_1]:h_{a_1}^\infty \cap [a_2]:h_{a_2}^\infty$ such that one of them is redundant and the other essential.

Theorem 4.7. *Let p be a regular differential polynomial in $\mathcal{F}\{Y\}$. $\{p\}:s_p$ is an essential regular component of p. Let $\mathcal{F}'$ be a differential field extension of $\mathcal{F}$. Then p is a regular differential polynomial in $\mathcal{F}'\{Y\}$. Furthermore, if $p = \prod_{i=1}^r p_i$ is the decomposition of p into irreducible factors over $\mathcal{F}'$, then $\{p\}:s_p = \bigcap_{i=1}^r \{p_i\}:s_i$ is the minimal prime decomposition of $\{p\}:s_p$ in $\mathcal{F}'\{Y\}$.*

Proof. As $\gcd(p, s_p) = 1$ in $\mathcal{F}\{Y\}$, we have the same equality in $\mathcal{F}'\{Y\}$ so that we can work indifferently over $\mathcal{F}$ or $\mathcal{F}'$.

For any pair p_i, p_j with $i \neq j$, p_j is partially reduced w.r.t. p_i and not divisible by p_i. Therefore, p_j does not belong to the prime differential ideal $\{p_i\}:s_i$ for $j \neq i$. Thus, none of the $\{p_i\}:s_i$ contains another one.

We proceed to prove that $\{p\}:s_p = \bigcap_{i=1}^r \{p_i\}:s_i$. Due to Property 2.1 and 2.3 $\{p\}:s_p = \{\prod_{i=1}^r p_i\}:s_p = \bigcap_{i=1}^r \{p_i\}:s_p$. It remains to show that $\{p_i\}:s_p = \{p_i\}:s_i$. Let $q \in \{p_i\}:s_p$. This means that $s_p\, q \in \{p_i\}$. The only term in $s_p\, q = \left(\sum_{k=1}^r s_k \prod_{j \neq k} p_j\right) q$ which is not trivially in $\{p_i\}$ is $s_i \left(\prod_{j \neq i} p_j\right) q$. Therefore $\left(\prod_{j \neq i} p_j\right) q \in \{p_i\}:s_i$ and since p_j, for $j \neq i$, does not belong to the prime differential ideal $\{p_i\}:s_i$, $q \in \{p_i\}:s_i$. We have shown that $\{p_i\}:s_p \subset \{p_i\}:s_i$. The converse inclusion is easy to see.

Recall from Proposition 2.2 that $\{p\} = \{p\}:s_p \cap \{p, s_p\}$. Any component of $\{p, s_p\}$ contains an element reduced w.r.t. u_p. By Proposition 4.3, no component of $\{p, s_p\}$ can be contained in $\{p_i\}:s_i$. Therefore each $\{p_i\}:s_i$ is an essential prime component of $\{p\}:s_p$. Thus $\{p\}:s_p$ is an essential regular component of $\{p\}:s_p$. $\square$

When p is a regular differential polynomial of $\mathcal{F}\{Y\}$, we call $\{p\}:s_p$ the *general component* of p. But we have to keep in mind that it depends on the ranking. In an ordinary differential field $\mathbb{Q}(t)\{y\}$, there is only one possible ranking. If the general zeros of the irreducible factors p_i can be given in the implicit form $f_i(t, y, c) = 0$, where c is a vector of arbitrary constants, then $\prod_{i=0}^r f_i(t, y, c) = 0$ is the general zero of p.

4.2. **Essential regular components.** The component theorem (Ritt 1945b) - see also (Kolchin 1973, IV.14) - asserts that any essential prime component of a differential polynomial is the general prime component of an irreducible differential polynomial. We extend this theorem to know what type of regular components are essential for p. This requires a very interesting result on the regular components that we give first. This result is also used for other purposes in (Boulier *et al.* 1997). After the component theorem we will then be in a position to define minimal regular decompositions of the radical differential ideal generated by a single differential polynomial.

Theorem 4.8. *Let A be an autoreduced coherent set of $\mathcal{F}\{Y\}$ such that $1 \notin [A]:H_A^\infty$. There is a one-to-one correspondence between the minimal primes of $(A):H_A^\infty$ and the essential prime components of $[A]:H_A^\infty$. Furthermore, assume C_i is a characteristic set of a minimal prime of $(A):H_A^\infty$. Then*

- *the set of leaders of C_i is equal to the set of leaders of A.*
- *C_i is the characteristic set of an essential prime component of $[A]:H_A^\infty$.*

Proof. Recall that $(A):H_A^\infty$ and $[A]:H_A^\infty$ are radical (Theorem 3.2).

∘ *A minimal prime of $(A):H_A^\infty$ has a characteristic set whose set of leaders is equal to the set of leaders of A:*

By (Kolchin 1973, 0.16, corollary 4), the minimal primes of $(A):H_A^\infty$ admit the set of non leaders of A as a transcendence basis. Assume $A = a_1, \dots, a_r$ so that the leader of a_i ranks less then the leader of a_{i+1}, $1 \leq i < r$. We can apply the same result to subsets $A_k = a_1, \dots, a_k$, $1 \leq k \leq r$ of A.

If P is a minimal prime of $(A):H_A^\infty$, $P \cap \mathcal{F}[\Theta_{A_k} Y]$ is a prime containing $(A_k):H_{A_k}^\infty$ and therefore one of its minimal prime $\bar{P}$. $P \cap \mathcal{F}[\Theta_{A_k} Y]$ and $\bar{P}$ have the same dimension, and therefore are equal. $P \cap \mathcal{F}[\Theta_{A_k} Y]$ is a minimal prime of $(A_k):H_{A_k}^\infty$.

Thus P admits a characteristic set having the same set of leaders than A.

∘ *Let P be an essential prime component of $[A]:H_A^\infty$. $P \cap \mathcal{F}[\Theta_A Y]$ is a minimal prime of $(A):H_A^\infty$.*

By Rosenfeld's lemma,(Kolchin 1973, III.8, lemma 5), $[A]:H_A^\infty \cap \mathcal{F}[\Theta_A Y] = (A):H_A^\infty$. $P \cap \mathcal{F}[\Theta_A Y]$ is a prime ideal that contains $(A):H_A^\infty$. It therefore contains a minimal prime $\bar{P}$ of $(A):H_A^\infty$.

Let p be an element of $P \cap \mathcal{F}[\Theta_A Y]$ that does not belong to $(A):H_A^\infty$ and therefore does not belong to $[A]:H_A^\infty$. There exists $q \in \mathcal{F}\{Y\}$, $q \notin P$ such that $q\,\bar{p} \in [A]:H_A^\infty$. Let $q \longrightarrow_A \bar{q}$ so that there exists $h \in H_A^\infty$ such that $h\,q \equiv \bar{q} \mod [A]$. We have that $\bar{q} \notin (A):H_A^\infty$ otherwise q would belong to $[A]:H_A^\infty$ and therefore to P. Nonetheless, $\bar{q}\,\bar{p}$ belongs to $[A]:H_A^\infty$ and thus to $(A):H_A^\infty$ since it is partially reduced w.r.t. A. This says that $\bar{p}$ belongs to a minimal prime of $(A):H_A^\infty$. Thus $P \cap \mathcal{F}[\Theta_A Y]$ belongs to a union of minimal primes of $(A):H_A^\infty$. By the prime avoidance theorem, (Eisenbud 1994, Lemma 3.3), $P \cap \mathcal{F}[\Theta_A Y]$ must be contained in one of the minimal primes, say $\bar{P}'$, of $(A):H_A^\infty$. Thus $\bar{P} \subset P \cap \mathcal{F}[\Theta_A Y] \subset \bar{P}'$. $\bar{P}'$. We must have $\bar{P}' = \bar{P}$ and therefore $P \cap \mathcal{F}[\Theta_A Y]$ is a minimal prime of $(A):H_A^\infty$.

∘ *Every minimal prime of $(A):H_A^\infty$ is the intersection of an essential prime component of $[A]:H_A^\infty$ with $\mathcal{F}[\Theta_A Y]$*

Assume the minimal prime decomposition of $[A]:H_A^\infty$ is $[A]:H_A^\infty = \bigcap_{i=1}^r P_i$. By (Kolchin 1973,), $\bigcap_{i=1}^r (P_i \cap \mathcal{F}[\Theta_A Y]) = (A):H_A^\infty$. Therefore, all the minimal prime of $(A):H_A^\infty$ are the intersection of an essential prime component of $[A]:H_A^\infty$ with $\mathcal{F}[\Theta_A Y]$.

∘ *If C_i is the characteristic set of a minimal prime $P_i \cap \mathcal{F}[\Theta_A Y]$ of $(A):H_A^\infty$ then C_i is a characteristic set of P_i.*

Let p be an element of P_i and $p \longrightarrow_{C_i} \bar{p}$. Then $\bar{p} \in P_i \cap \mathcal{F}[\Theta_A Y]$. C_i being a characteristic set of $P_i \cap \mathcal{F}[\Theta_A Y]$, $\bar{p}$ must be zero. Therefore C_i is a characteristic set of P_i. (In particular C_i must be coherent!).

Furthermore: since a characteristic set of a prime differential ideal determines uniquely this prime differential ideal, there is a unique essential prime component of $[A]:H_A^\infty$whose intersection with $\mathcal{F}[\Theta_A Y]$ is equal to $(C_i):H_{C_i}^\infty = P_i \cap \mathcal{F}[\Theta_A Y]$. □

Theorem 4.9. *Let p be a differential polynomial and A a coherent autoreduced set in $\mathcal{F}\{Y\}$ such that $p \in [A]:H_A^\infty$. If A has more than one element, then $[A]:H_A^\infty$ is a redundant regular component of $\{p\}$. In other words, any essential regular component of $\{p\}$ is the general component of a regular differential polynomial.*

Proof. Assume that A has more than one element. If $1 \in [A]:H_A^\infty$, the conclusion is trivial. We assume in the following that $1 \notin [A]:H_A^\infty$. Then the previous theorem tells us that a characteristic set of any minimal prime component of $[A]:H_A^\infty$ has the same number of elements as A. Therefore no essential prime component of $[A]:H_A^\infty$ is essential for $\{p\}$ (Kolchin 1973, IV.14, Theorem 5); $[A]:H_A^\infty$ is a redundant regular component of $\{p\}$. □

Proposition 4.10. *Let p be a differential polynomial in $\mathcal{F}\{Y\}$. From a regular decomposition (Proposition 3.3) of $\{p\}$ in $\mathcal{F}\{Y\}$ we can determine a decomposition*

$$\{p\} = \bigcap_{i=1}^{r} \{a_i\}:s_{a_i}$$

where a_i is a regular differential polynomial and is a characteristic set of $[a_i]:s_{a_i}^\infty$ for $1 \leq i \leq r$. We call such a decomposition a reduced regular decomposition *of $\{p\}$.*

Proof. From a regular decomposition of $\{p\}$, thanks to Theorem 4.9 we can eliminate the regular components defined by autoreduced set with more than one element. We are left with a decomposition

$$\{p\} = \bigcap_{i=1}^{k} [b_i]:b_{h_i}^\infty,$$

where h_{b_i} is the product of the initial and the separant of b_i. For each b_i in this decomposition we define $a_i = \frac{b_i}{\gcd(b_i, s_{b_i}^2)}$; a_i is the product of the simple factors of b_i that involve u_{b_i}. If $a_i \notin \mathcal{F}$ then it is a regular differential polynomial of $\mathcal{F}\{Y\}$.

By Proposition 4.3, $b_i \in \{a_i\}:s_{a_i}$ and $a_i \in \{b_i\}:s_{b_i}$. Thus $\{a_i\}:s_{b_i} \subset \{b_i\}:s_{b_i} \subset (\{a_i\}:s_{a_i}):s_{b_i}$.

By Proposition 4.3 and Proposition 4.7 an element $h \in \mathcal{F}\{Y\}$ partially reduced w.r.t a_i and relatively prime with a_i belongs to no essential prime component of $\{a_i\}:s_{a_i}$; then $(\{a_i\}:s_{a_i}):h = \{a_i\}:s_{a_i}$. The initial of b_i and $c_i = \frac{b_i}{a_i}$ are relatively prime with a_i.

$s_{b_i}\, q \in \{a_i\} \;\Leftrightarrow\; (a_i\, s_{c_i} + s_{a_i}\, c_i)\, q \in \{a_i\} \;\Leftrightarrow\; s_{a_i}\, c_i\, q \in \{a_i\} \;\Leftrightarrow\; q \in \{a_i\} : s_{a_i}$ because $(\{a_i\} : s_{a_i}) : c_i = \{a_i\} : s_{a_i}$ as seen in the previous remark. Thus $\{a_i\} : s_{b_i} = \{a_i\} : s_{a_i} = \{b_i\} : s_{b_i}$ and $\{b_i\} : h_{b_i} = (\{a_i\} : s_{a_i}) : i_{b_i} = \{a_i\} : s_{a_i}$.

If $a_i \in \mathcal{F}$ then $[b_i] : s_{b_i}^{\infty}$ can be discarded from the decomposition. Changing accordingly the indices, we obtain a decomposition as indicated in the proposition. $\square$

Definition 4.11. *Let p be a differential polynomial in $\mathcal{F}\{Y\}$. A reduced regular decomposition of $\{p\}$, $\{p\} = \bigcap_{i=1}^{r} \{a_i\} : s_{a_i}$, is a minimal regular decomposition if each $\{a_i\} : s_{a_i}$ is an essential regular component of $\{p\}$ and the a_i are pairwise relatively prime.*

The minimal prime decomposition of $\{p\}$ is a minimal regular decomposition. This settles the question of existence of minimal regular decomposition. There exists nonetheless minimal regular decomposition that are not prime minimal decomposition and we will present an algorithm to compute one of them. As for the uniqueness we have the following result which is a trivial consequence of the definitions and the previous properties.

Proposition 4.12. *Consider a minimal regular decomposition of $\{p\}$ in $\mathcal{F}\{Y\}$.*

$$\{p\} = \bigcap_{i=1}^{r} \{a_i\} : s_{a_i}. \tag{2}$$

Let $\mathcal{F}'$ be a differential field extension of $\mathcal{F}$. (2) is a minimal regular decomposition of $\{p\}$ in $\mathcal{F}'\{Y\}$. If $a_i = \prod_j^{r_i} b_{ij}$ is the factorization of a_i, $1 \le i \le r$ into irreducible factors, then

$$\{p\} = \bigcap_{1 \le i \le r,\ 1 \le j \le r_i} \{b_{ij}\} : s_{b_{ij}}.$$

is the minimal prime decomposition of $\{p\}$ in $\mathcal{F}'\{Y\}$.

The following sections are devoted to computing a minimal regular decomposition of any differential polynomial p in a differential polynomial ring $\mathcal{F}\{Y\}$.

5. Preparation polynomial

The low power theorem decides if the general component of a differential polynomial a is an essential component of a differential polynomial p. In the introduction we have seen a special case where $a = y$. In the other cases, the necessary and sufficient condition of the low power theorem relies on the way a makes itself visible in the algebraic structure of p. To see this structure we rewrite p as a differential polynomial in a. This is the purpose of the *preparation process*.

The preparation process was first introduced by Ritt (1936) for an ordinary irreducible differential polynomial a. An extension is defined in (Kolchin 1973, IV.13) where a is replaced by a characteristic set of a prime ideal. We extend here the definition of the preparation equation to a regular differential polynomial a.

If m is a differential monomial in a differential indeterminate z, $m = \prod_{i=1}^{r} (\theta_i\, z)^{\alpha_i}$, the degree of m is $\deg m = \sum_{i=1}^{d} \alpha_i$. Then, for a differential polynomial a in $\mathcal{F}\{Y\}$, $m(a)$ stands for $m\,(a) = \prod_{i=1}^{r} (\theta_i\, a)^{\alpha_i}$.

Definition 5.1. *Let p be any differential polynomial and a a regular differential polynomial in $\mathcal{F}\{Y\}$. A preparation polynomial of p w.r.t. a is an element of $\mathcal{F}\{Y\}\{z\}$*

$$\tilde{p} = \sum_{\gamma=0}^{l} c_\gamma m_\gamma$$

where $m_0, \ldots, m_l$ are distinct differential monomials in z and $c_0, \ldots, c_l$ are elements of $\mathcal{F}\{Y\}$ that do not belong to $\{a\} : s_a$, such that there exists a differential polynomial c_{-1} in $\mathcal{F}\{Y\}$ that does not divide zero modulo $\{a\} : s_a$ and satisfies

$$c_{-1}\, p = \sum_{\gamma=0}^{l} c_\gamma m_\gamma(a)$$

The above equation is a preparation equation of p w.r.t. a.

Proposition 5.2. *For any differential polynomial p and any regular differential polynomial a in $\mathcal{F}\{Y\}$, there exists a preparation polynomial of p w.r.t. a. Furthermore such a preparation polynomial can be computed by Algorithm 5.3.*

Algorithm 5.3. **Preparation-polynomial**

INPUT: *p and a differential polynomials of $\mathcal{F}\{Y\}$, a is regular.*

OUTPUT: *- A preparation polynomial of p w.r.t. a, $\tilde{p} = \sum_{\gamma=0}^{l} c_\gamma m_\gamma \in \mathcal{F}\{Y\}\{z\}$, where the c_γ are partially reduced w.r.t. a and not divisible by a.*
- The associated differential polynomial c_{-1}, partially reduced w.r.t. a and relatively prime with a.

$\tilde{p}$:= p; # $\tilde{p}$ is a polynomial in $\mathcal{F}\{Y\}\{z\}$

c_{-1} := 1;

while *$\tilde{p}$ is not partially reduced w.r.t. a* **do**

  θ := *the derivation operator s.t. θu_a is the highest ranking derivative of u_a in $\tilde{p}$;*

  e := *the degree of $\tilde{p}$ in θu_a.*

  # $s_a^e\, \tilde{p}$ is a polynomial in $s_a\, \theta u_a$

  # $\theta a = s_a\, \theta u_a + t$, where t is reduced w.r.t. to θu_a.

  c_{-1} := $c_{-1} \, . \, s_a^e$;

  $\tilde{p}'$:= *the polynomial obtained by replacing $s_a\, \theta u_a$ by $\theta z - t$ in $s_a^e\, \tilde{p}$;*

  # $\tilde{p}'$ involves only derivatives of u_a of strictly lower rank than θu_a.

  $\tilde{p}$:= $\tilde{p}'$;

od;

\# Now $\tilde{p}$ is of the form $\tilde{p} = \sum_{\gamma=0}^{l} c_\gamma \, m_\gamma$ where
\# - the m_γ are distinct monomials in z
\# - the c_γ belong to $\mathcal{F}\{Y\}$ and are partially reduced w.r.t. a

for γ **from** *0* **to** l **do**
e := *the biggest exponent* ϵ *such that* a^ϵ *divides* c_γ;
$c_\gamma := \frac{c_\gamma}{a^e}$;
$m_\gamma := z^e \, m_\gamma$;
od;

\# Now $\tilde{p} = \sum_{\gamma=0}^{l} c_\gamma \, m_\gamma$ is a preparation polynomial.

end;

PROOF. At each step of the while loop, the highest derivative of u_a in $\tilde{p}'$ ranks strictly less then the highest derivative of u_a in $\tilde{p}$. As any decreasing sequence of derivatives is finite (Kolchin 1973, I.8), the while loop ends in a finite number of steps.

The polynomial $\tilde{p}$ obtained after the while loop is partially reduced w.r.t. a. It can be written $\tilde{p} = \sum_{\gamma=0}^{l} c_\gamma \, m_\gamma$. We have $c_{-1}\, p = \sum_{\gamma=0}^{l} c_\gamma \, m_\gamma(a)$ where c_{-1} is a suitable power of s_a. s_a belongs to no essential component of $\{a\}:s_a$; therefore c_{-1} does not divide zero modulo $\{a\}:s_a$.

After the for loop, $\tilde{p} = \sum_{\gamma=0}^{l} c_\gamma \, m_\gamma$ is such that the c_γ are partially reduced w.r.t. a and not divisible by a. By Proposition 4.3 they do not belong to $\{a\}:s_a$. Moreover we still have $c_{-1}\, p = \sum_{\gamma=0}^{l} c_\gamma \, m_\gamma(a)$ and thus we have obtained a preparation polynomial of p w.r.t. a in a finite number of steps. □

The preparation equation of a differential polynomial p w.r.t. a regular differential polynomial a is not unique. First of all, it depends on the ranking chosen on $\mathcal{F}\{Y\}$ as shown in the example below.

Example 5.4. *Consider for instance the pair of differential polynomials in* $Q(s,t)\{y\}$*:*

$$p = y_{st}\, y_{ss} + y_{tt}^2 \quad \textit{and} \quad a = y_s + y_t$$

Choose a ranking on $\mathbb{Q}(s,t)\{y\}$ *such that* $y_{ss} > y_{st} > y_{tt} > y_s > y_t > y$*. Then the leader of* a *is* $u_a = y_s$ *and the highest ranking derivative of* u_a *in* $\tilde{p}$ *is* $\delta_s u_a = y_{ss}$*. We have* $\delta_s a = y_{ss} + y_{st}$*. We therefore substitute* y_{ss} *by* $z_s - y_{st}$ *in* p*;* $\tilde{p} = y_{st}\,(z_s - y_{st}) + y_{tt}^2$*. The highest ranking derivative of* u_a *in* $\tilde{p}$ *is now* $\delta_t u_a = y_{st}$*. We have* $\delta_t a = y_{st} + y_{tt}$ *and we substitute* y_{st} *in* $\tilde{p}$ *by* $z_t - y_{tt}$*. We obtain* $\tilde{p}' = -y_{tt}\, z_s + 2\, y_{tt}\, z_t - z_t^2 + z_t\, z_s$*. The coefficients of the monomials in* z *are partially reduced w.r.t.* a *and not divisible by* a*. This is therefore a preparation polynomial of* p *w.r.t.* a*. The corresponding preparation equation is* $p = -y_{tt}\,(\delta_s a) + 2\, y_{tt}\,(\delta_t a) - (\delta_t a)^2 + (\delta_t a)\,(\delta_s a)$*.*

If we had chosen a ranking such that $y_{tt} > y_{st} > y_{ss} > y_t > y_s > y$, we would have obtained the following preparation equation of p w.r.t. a $p = -y_{ss}(\delta_s a) + 2\, y_{ss}(\delta_t a) - 2\,(\delta_t a)\,(\delta_s a) + (\delta_t a)^2 + (\delta_s a)^2$.

The preparation equation depends also on the algorithm used to compute it. In the algorithm, we can first consider multiplying $\tilde{p}$, in the while loop by a tighter power of s_a or some of its factors. It suffices to substitute θu_a by $\frac{\theta z - t}{s_a}$ and to take $\tilde{p}'$ as the numerator of the expression obtained while multiplying c_{-1} by its denominator. We can also obtain a preparation polynomial $\tilde{p} = \sum_{\gamma=0}^{l} c_\gamma\, m_\gamma$ where the c_γ are reduced with respect to a. The corresponding c_{-1} would then be a power product of s_a and of the initial i_a of a, none of which is a divisor of zero modulo $\{a\}\!:\!s_a$.

Let ρ be the minimal degree of the monomials m_γ in the preparation polynomial $\tilde{p}$ of p w.r.t. a. It is no loss of generality to assume that the monomials of lowest degree in z are $m_0, \ldots, m_{l'}$, where $l' \leq l$. Then a *preparation congruence* of p w.r.t. a is

$$c_{-1}\, p \;\equiv\; \sum_{\gamma=0}^{l'} c_\gamma\, m_\gamma(a) \quad \bmod\, [a]^{\rho+1}.$$

It is proved in (Kolchin 1973, IV.15) that when a is irreducible, the degree ρ and the set of monomials $m_1, \ldots, m_{l'}$ in the preparation congruence are unique; they do not depend on the ranking. The argument relies on a result of Hillman (1943). It can be generalized when a is regular but this is not needed in this paper.

6. The low power theorem for regular differential polynomials

The sum of the terms of the lowest degree in z of a preparation polynomial of a differential polynomial p w.r.t. a regular differential polynomial a in $\mathcal{F}\{Y\}$ such that $p \in \{a\} : s_a$ can be of two types. Either it has a single term that does contain z but no proper derivatives of z or it involves proper derivatives of z. We will then be in a position to compute a divisor $\tilde{a} \notin \mathcal{F}$ of a such that, in the first case, $\{\tilde{a}\} : s_{\tilde{a}}$ is an essential regular component of $\{p\}$ and in the second case $\{\tilde{a}\}\!:\!s_{\tilde{a}}$ is a redundant component of $\{p\}$. This is the purpose of Theorem 6.1 and Theorem 6.2 that are extensions of the sufficiency and necessity conditions of the low power theorem (Kolchin 1973, IV).

The reader can then foresee what will be an algorithm to determine the maximal divisor b of a such that $\{b\}\!:\!s_b$ is an essential regular component of $\{p\}$, while the general component of $c = \frac{a}{b}$ is a redundant component. With the notation of the previous paragraph, if $\hat{a} = \frac{a}{\tilde{a}} \notin \mathcal{F}$, we iterate the process with $\hat{a}$ instead of a.

Theorem 6.1. *(Sufficiency)*
Let p be a non-zero differential polynomial and a a regular differential polynomial in $\mathcal{F}\{Y\}$. Assume a preparation congruence of p w.r.t. a is

$$c_{-1}\, p \;\equiv\; c\, a^\rho \quad \bmod\, [a]^{\rho+1},$$

where $\rho > 0$ and c is partially reduced w.r.t. a. Let $\hat{a} = \gcd(a, c)$ and $\tilde{a} = \frac{a}{\hat{a}}$. Then $\{\tilde{a}\}:s_{\tilde{a}}$ is an essential regular component of p.

Proof. Let b be an irreducible factor of a over $\mathcal{F}'$, a differential field extension of $\mathcal{F}$. By Proposition 4.7, $\{b\}:s_b$ is an essential prime component of $\{a\}:s_a$ in $\mathcal{F}'\{Y\}$.

As c is partially reduced w.r.t. b, by Proposition 4.3, c belongs to $\{b\}:s_b$ if and only if it is divisible by b. We shall show that if $\{b\}:s_b$ does not contain c then $\{b\}:s_b$ is an essential component of $\{p\}$. This will therefore be the case for any irreducible factors of $\tilde{a}$.

Assume $\{b\}:s_b$ is not an essential prime component of $\{p\}$ in $\mathcal{F}'\{Y\}$. There thus exists an essential prime component P of $\{p\}$ in $\mathcal{F}'\{Y\}$ that is strictly included in $\{b\}:s_b$. Such a P can not contain a, since otherwise it would contain an essential component of a.

According to Levi's lemma (Levi (1942), (1945) or Kolchin (1973), IV.11), there exists $\epsilon, d \in \mathbb{N}^*$ and $r \in [a]$ such that $a^\epsilon(c^d + r) \in \{p\} \subset P$. P being prime, $c^d + r \in P \subset \{b\}:s_b$.

As we have $r \in [a] \subset \{b\}:s_b$, we are brought to the conclusion that $c \in \{b\}:s_b$. □

Theorem 6.2. *(Necessity)*
Let p be a differential polynomial and a a regular differential polynomial in $\mathcal{F}\{Y\}$. Consider a preparation congruence of p w.r.t. a

$$c_{-1}\, p \;\equiv\; c_0\, a^\rho + \sum_{\gamma=1}^{l} c_\gamma\, m_\gamma(a) \mod [a]^{\rho+1}$$

where $\rho > 0$ and the c_γ, $0 < \gamma \leq r$, are partially reduced w.r.t. a; c_0 may be zero, but we assume that none of $c_1, \ldots, c_l$ is. Let $\tilde{a} = \gcd(a, c_1, \ldots, c_l)$ and $\hat{a} = \frac{a}{\tilde{a}}$. Then $\{\hat{a}\}:s_{\hat{a}}$ is a redundant component of p.

Proof. Let b be an irreducible factor of $\hat{a}$. Consider all the essential components of $\{p\}$ which are contained in $\{b\}:s_b$. By the component theorem (Kolchin 1973, IV.14), they are the general components of some irreducible differential polynomials $r_1, \ldots, r_\kappa$.

If $\{b\}:s_b$ were an essential component, κ would be equal to one and r_1 would be equal to b. We are in fact going to show that this cannot be so because one of the r_i involves a proper derivative of u_a and thus $\{r_i\}:s_{r_i}$ is strictly contained in $\{b\}:s_b$.

Let r_0 be a differential polynomial which does not belong to $\{b\}:s_b$ but which belongs to all the components of $\{p\}$ not contained in $\{b\}:s_b$. Thus $r_0\, r_1 \ldots r_\kappa \in \{p\}$.

Let ν be a generic zero (Kolchin 1973, IV.2) of $\{b\}:s_b$ in an extension field $\mathcal{F}'$ of $\mathcal{F}$. A differential polynomial q vanishes on ν if and only if it belongs to $\{b\}:s_b$. Thus $s_a(\nu) =\neq 0$.

For a differential polynomial q in $\mathcal{F}\{Y\}$ we denote $\bar{q}$, in $\mathcal{F}'\{Y\}$, to be the sum of the terms of lowest degree in $q(\nu+y)$. Note that $\overline{q\,r} = \bar{q}\,\bar{r}$, for any $q, r \in \mathcal{F}\{Y\}$. As

$$a(\nu+y) = s_a(\nu)\,u_a + \text{ first degree terms of lower rank } + \text{ higher degree terms }.$$

$\bar{a}$ has degree one and u_a as leader.

Now, if $q = c_0\,a^\rho + \sum_{\gamma=1}^{l} c_\gamma\,m_\gamma(a)$ then $\bar{q} = c_0(\nu)\,\bar{a}^\rho + \sum_{\gamma=1}^{l} c_\gamma(\nu)\,m_\gamma(\bar{a})$, where $c_\gamma(\nu) \neq 0$ for at least one γ, $1 \leq \gamma \leq l$. Among the derivatives of $\bar{a}$ effectively present in the monomials of the right hand side, let $\theta\bar{a}$ be such that θu_a has the highest rank. Let $\bar{q}_0$ be an irreducible factor of $\bar{q}$ which contains $\theta\bar{a}$.

We are now in a position to conclude thanks to the Leading coefficient theorem given in (Ritt 1950, III.30), (Hillman 1943), (Hillman and Mead 1962) or (Kolchin 1973, IV.10): $r_0\,r_1 \ldots r_\kappa \in \{p\} \Rightarrow \bar{r}_0\,\bar{r}_1 \ldots \bar{r}_\kappa \in \{\bar{p}\}$, where $\bar{r}_0 = r_0(\nu) \in \mathcal{F}'$ and for $i \geq 1$, $\bar{r}_i$ is of positive degree.

As $c_{-1}\,p \equiv q \mod [a]^{\rho+1}$, $\bar{c}_{-1}\,\bar{p} = \bar{q}$, where $\bar{c}_{-1} = c_{-1}(\nu)$ is a nonzero element of $\mathcal{F}'$. Thus $\{\bar{p}\} = \{\bar{q}\} \subset \{\bar{q}_0\} : s_{\bar{q}_0}$.

Consequently, $\{\bar{q}_0\} : s_{\bar{q}_0}$ being a prime differential ideal, there exists i, $1 \leq i \leq \kappa$ such that $r_i \in \{\bar{q}_0\} : s_{\bar{q}_0}$. Therefore, r_i cannot be reduced w.r.t. $\bar{q}_0$: it must contain a derivative of θu_a, and therefore a proper derivative of u_a. That is what we looked for. $\{b\} : s_b$, is not an essential prime component of $\{p\}$.

We have $p \in \{\tilde{a}\} : s_{\tilde{a}} \cap \{\hat{a}\} : s_{\hat{a}}$ and $\{\hat{a}\} : s_{\hat{a}}$ is a redundant regular component of $\{p\}$. □

7. Minimal regular decomposition algorithm

We present here a complete algorithm to compute a minimal regular decomposition of the radical differential ideal generated by a single differential polynomial $p \in \mathcal{F}\{Y\}$. We will then illustrate it with a series of examples.

The Ritt and Levi's method to determine the minimal prime decomposition of $\{p\}$ proceeds by eliminating the redundancy in a characteristic prime decomposition of $\{p\}$. Determining if a prime component $\{a\} : s_a$, a irreducible, of $\{p\}$, is essential or redundant is done with a single application of the low power theorem.

Our algorithm proceeds by eliminating the redundancy in a reduced regular decomposition (Proposition 4.10) of $\{p\}$. The crucial part of the algorithm lies in Algorithm 7.1 which splits a regular component $\{a\} : s_a$, where a is regular differential polynomial, into two regular components $\{b\} : s_b$ and $\{c\} : s_c$ such that $a = b\,c$ and $\{b\} : s_b$ is an essential regular component of $\{p\}$ while $\{c\} : s_c$ is a redundant regular component of $\{p\}$.

A reduced regular decomposition is obviously easier to obtain than a characteristic prime decomposition. Furthermore, we might be lucky and have several prime components treated at the same time.

In our process, only the coefficients effectively involved in p will be relevant to the determination of the minimal regular decomposition. Nonetheless, we can easily recover the minimal prime decomposition from a minimal regular decomposition; it suffices to factor the polynomials involved in it over the desired field of coefficients, as presented in Proposition 4.12.

7.1. **Algorithm.** We assume a differential polynomial p and a regular differential polynomial a given in $\mathcal{F}\{Y\}$ such that $p \in \{a\} : s_a$. We collect the results presented above in an algorithm that extracts a divisor b of a such that $\{b\} : s_b$ is an essential regular component of $\{p\}$ while $\frac{a}{b}$ defines a redundant regular component of $\{p\}$.

We call Low-powers a procedure that takes a preparation polynomial in $\mathcal{F}\{Y\}\{z\}$ and returns the sum of the terms of lowest degree in z.

Algorithm 7.1. Essential-part

INPUT: *p and a, differential polynomials in $\mathcal{F}\{Y\}$, a regular, such that $p \in \{a\} : s_a$*

OUTPUT: *b, the maximal divisor of a such that $\{b\} : s_b$ is an essential regular component of $\{p\}$.*

If $a \in \mathcal{F}$ then return 1; fi;

$\tilde{p} :=$ **Low-powers** *(* **Preparation-polynomial** $(p,\ a)$ *) ;*

If $\tilde{p} = c\, z^\rho$ *then*

  $\hat{a} :=$ *gcd* (c, a)*;*

  $\tilde{a} := \frac{a}{\hat{a}}$*;*

  # By Theorem 6.1, $\{\tilde{a}\} : s_{\tilde{a}}$ is an essential regular component for p

  $b := \tilde{a}$. **Essential-Part** $(p,\ \hat{a})$*;*

else # $\tilde{p} = c_0 z^\rho + \sum_{\gamma=1}^{l} c_\gamma m_\gamma$

  $\hat{a} :=$ *gcd* $(c_1, \ldots , c_l, a)$*;*

  $\tilde{a} := \frac{a}{\hat{a}}$

  # By Theorem 6.2, $\{\tilde{a}\} : s_{\tilde{a}}$ is a redundant regular component for p

  $b :=$ **Essential-Part** *$(p,\ \hat{a})$.*

fi;

end;

At each step, because a does not divide any c_γ, $\hat{a}$ is of strictly lower degree than a. The process finishes in a finite time.

Example 7.2. *In the ordinary differential ring $\mathbb{Q}\{y\}$, consider the differential polynomial $p = (y' - y)^2\, (y' + y) + 4\, (y'\, y'' - 2y'\, y)^2$ and the regular differential polynomial $a = y'^2 - y^2 = (y' - y)\, (y' + y)$.*

The preparation polynomial of p w.r.t. a computed by Algorithm 5.3 is $\tilde{p} = (y' - y)\, z + z'^2$. We are in the first case of the algorithm. The greatest common divisor *of a and the coefficient $c = y' - y$ is actually $\hat{a} = y' - y$. Let thus $\tilde{a} = y' + y$. By Theorem 6.1, $\{\tilde{a}\} : s_{\tilde{a}} = \{y' - y\}$ is an essential regular component of $\{p\}$.*

Now the preparation polynomial of p w.r.t. $\hat{a} = y' - y$ computed by Algorithm 5.3 is $\tilde{p} = (4\,{y'}^2 + y' + y)\,z^2 + 8\,{y'}^2\,z\,z' + 4\,{y'}^2\,{z'}^2$. We are in the second case of the algorithm. The greatest common divisor of $\hat{a}$, $8\,{y'}^2$ and $4\,{y'}^2$ is actually 1. By Theorem 6.2, $\{\hat{a}\} : s_{\hat{a}}$ is a redundant component of p.

We now proceed to give the complete algorithm to determine a minimal regular decomposition of any differential polynomial p in $\mathcal{F}\{Y\}$.

Let c_p and $\hat{p}$ be respectively the content and primitive part of p: $p = c_p\,\hat{p}$. Let $s_{\hat{p}}$ be the separant of $\hat{p}$ and $\bar{p} = \frac{\hat{p}}{\gcd(\hat{p}, s_{\hat{p}})}$. $\bar{p}$ has no multiple factor and, like $\hat{p}$, $\bar{p}$ has no factor independent of u_p: $\bar{p}$ is regular (in fact we also have $\bar{p} = \frac{p}{gcd(p, s_p)}$). Furthermore $\{p\} = \{c_p\,\hat{p}\} = \{c_p\,\bar{p}\}$. The essential components of p are therefore the essential components of $c_p\,\bar{p}$. In the case p has multiple factors, $c_p\,\bar{p}$ has a lower degree than p and thus simplifies the computations of the preparation equations involved in determining the minimal decomposition of p.

Note that there is one regular component that is obviously essential. With the notations introduced above, let $s_{\bar{p}}$ be the separant of $\bar{p}$. Then $\{\bar{p}\} : s_{\bar{p}}$ is an essential regular component of p. We indeed have $\{p\} = \{c_p\,\bar{p}\} = \{\bar{p}\} \cap \{c_p\} = \{\bar{p}\} : s_{\bar{p}} \cap \{\bar{p}, s_{\bar{p}}\} \cap \{c_p\}$. Any component of $\{\bar{p}, s_{\bar{p}}\}$ and $\{c_p\}$ contains an element reduced with respect to u_p and therefore can not be contained in any essential prime component of $\{\bar{p}\} : s_{\bar{p}}$ (Proposition 4.3, Theorem 4.7).

We call Regular-decomposition an algorithm which compute a regular decomposition as in Proposition 3.3 and Reduce an algorithm that applies a reduction of a regular decomposition as presented in Proposition 4.10 and returns the regular differential polynomials involved in this reduced regular decomposition. A complete algorithm to compute a minimal regular decomposition of $\{p\}$ can thus be written:

Algorithm 7.3. Minimal Regular Decomposition

INPUT: *p a differential polynomial in $\mathcal{F}\{Y\}$.*

OUTPUT: *$\mathcal{M} = a_1, \ldots, a_r$ a sequence of regular differential polynomials defining a minimal regular decomposition of $\{p\}$.*

$c_p :=$ *content* (p, u_p);

$\hat{p} :=$ *primitive-part* (p, u_p);

$\bar{p} := \frac{\hat{p}}{\gcd(\hat{p}, s_{\hat{p}})}$;

$\mathcal{D} :=$ *Reduce (Regular-decomposition* $(\{\bar{p}, s_{\bar{p}}\},\ \mathcal{F}\{Y\})$),
Reduce (Regular-decomposition $(\{c_p\},\ \mathcal{F}\{Y\})$);

For $1 < i < j \leq nops(\mathcal{D})$ *do* # we first make the $\mathcal{D}_i$ relatively prime
if leader $(\mathcal{D}_i,\ \mathcal{F}\{Y\})$ = *leader* $(\mathcal{D}_j,\ \mathcal{F}\{Y\})$ *then*

$$\mathcal{D}_j := \frac{\mathcal{D}_j}{\gcd(\mathcal{D}_i, \mathcal{D}_j)}$$

fi;

od;

$\mathcal{M} := \bar{p}$;

For each differential polynomial a in $\mathcal{D}$ do

$b :=$ **Essential-Part** $(c_p\,\bar{p},\ a)$;

If $b <> 1$ then $\mathcal{M} := \mathcal{M},\ b$; fi;

od;

end;

7.2. **Examples.**

Example 7.4. *Consider the partial differential ring $\mathbb{Q}\{y\}$ with two derivations, $\Delta = \{\delta_s, \delta_t\}$, and the differential polynomial $p = q + \delta_s q\, \delta_t q$ where $q = (y_s - y)\,(y_s - y_t)$.*

According to an order where $y_{ss} > y_{st} > y_{tt} > y_s > y_t > y$ a regular decomposition is $\{p\} = [p] : s_p^\infty \cap [q] : s_q^\infty \cap [y_s - y, y_t - y]$. By Theorem 4.9, we know that $[y_s - y, y_t - y]$ is a redundant component. We have $\mathcal{D} = p, q$. A preparation polynomial of p w.r.t. q is $\tilde{p} = z + z_s\, z_t$. The differential monomial in z of lowest degree does not involve any proper derivative of z and its coefficient is 1. By Theorem 6.1, $\{q\} : s_q = [q] : s_q^\infty$ is an essential regular component of p. Therefore, $\mathcal{M} = p, q$ and $\{p\} = \{p\} : s_p \cap \{q\} : s_q$ is a minimal regular decomposition according to the chosen ranking.

A minimal prime decomposition of p in $\mathbb{Q}\{y\}$ is obtained by simply factoring the differential polynomials involved in this decomposition over $\mathbb{Q}$. Since $q_1 = y_s - y$ and $q_2 = y_s - y_t$ are the two irreducible factors of q over $\mathbb{Q}$ and p is irreducible over $\mathbb{Q}$, we conclude that the minimal prime decomposition of $\{p\}$ in $\mathbb{Q}\{y\}$ is $\{p\} = \{p\} : s_p \cap \{y_s - y\} \cap \{y_s - y_t\}$.

Assume we choose a ranking where $y_{tt} > y_{ts} > y_{ss} > y_t > y_s > y$. The regular decomposition of $\{p\}$ is $\{p\} = \{p\} : s_p \cap [y_s - y] \cap [y_s - y_t]$. Thus $\mathcal{D} = p, y_s - y, y_s - y_t$. A preparation congruence of p w.r.t. $q_1 = (y_s - y)$ is $p \equiv (y_s - y_t)\, q_1 \mod [q_1]^2$. Since $y_s - y_t$ and q_1 have no common factor, by Theorem 6.1, $\{y_s - y\} = [y_s - y]$ is an essential regular component of $\{p\}$. It is furthermore an essential prime component of p in $\mathbb{Q}\{y\}$ since $y_s - y$ is irreducible over $\mathbb{Q}$. Similarly we determine that $q_2 = y_s - y_t$ is an essential regular component of p, which turns out to be an essential prime component in $\mathbb{Q}\{y\}$, since q_2 is irreducible over $\mathbb{Q}$.

What we have illustrated in this example is the fact that a minimal regular decomposition, as well as a regular decomposition, can depend on the ranking. Nonetheless, the underlying prime minimal decomposition, obtained from any minimal regular decomposition by simple factorization, is unique.

Example 7.5. *Consider the differential equation $(y')^2 - 4\,y^3 + g_2\,y + g_3 = 0$ where g_2, g_3 are constants in $\mathbb{Q}$. This is the reduced equation of the solitary wave $u(x, t) =$*

$2\,y(x-c\,t)-\frac{c}{6}$ *of the Korteg de Vries equation* $u_t - 6\,u\,u_x + u_{xxx} = 0$ *(Ablowitz and Clarkson 1991). We are mostly interested in its real solutions.*

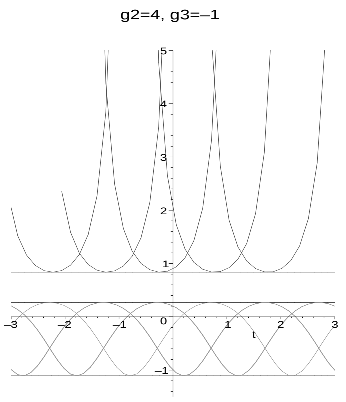
When $g_2^3 \neq 27\,g_3^2$*, i.e. when* $4\,y^3 - g_2\,y - g_3$ *has only simple roots, the equation admits the Weierstrass elliptic function, and its translations, as nonsingular solution (Whittaker and Watson 1927). We will see that the transition through* $g_2^3 = 27\,g_3^2$ *reflects a change of property of the singular solutions, from essential to non-essential.*

Consider $p = (y')^2 - 4\,y^3 + g_2\,y + g_3$ *in* $\mathbb{Q}\{y\}$ *with derivation* δ*. Let* $a = 4\,y^3 - g_2\,y - g_3$*.*

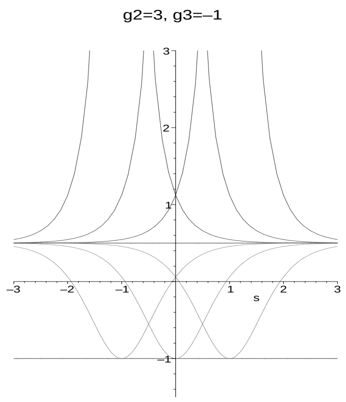
∘ *For* $g_2^3 \neq 27\,g_3^2$ *a regular decomposition of* $\{p\}$ *is given by* $\{p\} = \{p\} : s_p \,\cap\, \{a\}$*. A preparation polynomial of* p *w.r.t.* a *is* $\tilde{p} = (12\,y^2 - g_2)^2\,z + (\delta\,z)^2$ *so that* $(12\,y^2 - g_2)^2\,p = \tilde{p}(a)$*. Since the resultant of* a *and* $12\,y^2 - g_2$ *w.r.t.* y *is* $64\,(g_2^3 - 27\,g_3^2)$*,* $\{a\}$ *is an essential regular component in the case considered here. By (Hamburger 1893) the zeros of* a *are envelopes of the non singular zeros of* p*.*

If $g_2^3 > 27\,g_3^2$*,* $a(r) = 4\,r^3 - g_2\,r - g_3 = 0$ *has only real roots, say* $r_1 < r_2 < r_3$*. The singular solutions are given by* $y = r_i$*. Furthermore, there are real non-singular solutions for* $r_1 \leq y \leq r_2$ *and* $r_3 \leq y$*, that is when* $a(y) \geq 0$*. The fact that singular zeros are envelopes of the non-singular zeros can then be seen on the graph of these real solutions.*

$g_2^3 > 27\,g_3^2$



$g_2^3 = 27\,g_3^2$



∘ *Choose now* $g_2 = 3\,g^2, g_3 = g^3$*,* $g \neq 0$*. Then* $p = (y')^2 - 4\,y^3 + 3\,g^2\,y + g^3$*. Note that* $a = (y-g)(2\,y+g)^2$ *is no longer a regular differential polynomial. Let* $b = (y-g)(2\,y+g) = 2\,y^2 - g\,y - g^2$*. A regular decomposition of* $\{p\}$ *is* $\{p\} = \{p\} : s_p \cap \{b\} : s_b$*. A preparation polynomial of* p *w.r.t.* b *is* $\tilde{p} = (4\,y-g)^2\,(g+2\,y)\,z + (\delta\,z)^2$*, so that* $(4\,y-g)^2\,p = \tilde{p}(b)$*.*

Let $\tilde{b} = \gcd((4\,y-g)^2\,(g+2\,y), b) = (2\,y+g)$ *when* $g \neq 0$ *and* $\bar{b} = b/\tilde{b} = y - g$*. By Theorem 6.1* $\{\bar{b}\} : s_{\bar{b}}$ *is an essential regular component.*

A preparation polynomial of p *w.r.t.* $\tilde{b}$ *is* $\tilde{p} = 6\,g\,z^2 + (\delta\,z)^2 - 2\,z^3$*. By Theorem 6.2,* $\{\tilde{b}\} : s_{\tilde{b}}$ *is a redundant regular component. Thus a minimal regular decomposition,* *which turns out to be the minimal prime decomposition since* p *and* $\bar{b}$ *are irreducible, is* $\{p\} = \{p\}:s_p \cap \{y-g\}$. *The analytic interpretation is that* $y = g$ *is an envelope of nonsingular solutions while* $y = g/2$ *is* adherent *to the nonsingular solutions. This can be seen with the graph of the real solutions that exist for* $y > -g/2$ *when* $g > 0$.

∘ *When* $g_2 = g_3 = 0$, $p = (y')^2 - 4\,y^3$ *which is similar to the example shown in the introduction of this paper.*

Example 7.6. *The universal equation (Rubel 1981).*
Consider the following differential polynomial in the ordinary differential ring $\mathbb{Q}\{y\}$*:*

$$\begin{aligned} p \;=\; & 3\,y'^4\,y''\,y''''^2 - 4\,y'^4\,y'''^2\,y'''' + 6\,y'^3\,y''^2\,y'''\,y'''' + 24\,y'^2\,y''^4\,y'''' \\ & -12\,y'^3\,y''\,y'''^3 - 29\,y'^2\,y''^3\,y'''^2 + 12\,y''^7. \end{aligned}$$

The regular decomposition of $\{p\}$ *is* $\{p\} = \{p\}:s_p \cap \{q\}:s_q \cap \{y''\}$ *where* $q = y'^2\,y'''^2 + 3\,y''^4$. *The differential polynomial* p *has thus two singular regular components.* $\mathcal{D} = p, q, y''$.

A preparation polynomial of p *w.r.t* q *is* $\tilde{p} = 96\,(y''^7 + y'\,y'''\,y''^5)\,z - 32\,(y''\,y'''\,y' + y''^3)\,z^2 - 8\,y'^2\,y'''\,z'\,z + 3\,y''\,y'^2\,z'^2$. *The lowest degree monomial in* z *is free of any proper derivative of* z. *Its coefficient,* $96(y''^7 + y'\,y'''\,y''^5)$ *has no common factor with* q. *By Theorem 6.1,* $\{q\}:s_q$ *is an essential regular component of* $\{p\}$.

According to the extension of Hamburger (1893) of his own results, we know that the non-singular zeros of q *are envelopes of the zero of* p *since their respective orders differ only by* 1 *and* $\{q\}:s_q$ *is essential for* $\{p\}$ *- see also (Ritt 1950, III.36).*

Note that $\{q\}:s_q = \{q\} \subset \{y''\}$. *Indeed, the regular decomposition of* $\{q\}$ *is* $\{q\} = \{q\}:s_q \cap \{y''\}$. *This is in fact a prime decomposition in* $\mathbb{Q}\{y\}$ *since* q *and* y'' *are irreducible over* $\mathbb{Q}$. *A preparation polynomial of* q *w.r.t.* y'' *is* $\tilde{q} = y'^2\,z'^2 + 3\,z^4$. *By Theorem 6.2,* $\{y''\}$ *is a redundant component of* $\{q\}$. *Therefore it must contain* $\{q\}:s_q$. *As a consequence, we know that the zeros of* y'', *which are lines* $\tilde{y}(t) = c_1\,t + c_2$, *where* c_1 *and* c_2 *are arbitrary constants, are adherent (Ritt 1950, VI.2) to the non-singular zeros of* q.

This remark also tells us that $\{y''\}$ *is a redundant component of* $\{p\}$, *though we can check that directly by computing the preparation polynomial of* p *w.r.t.* y''. *We have* $\mathcal{M} = p, q$.

Nonetheless, to determine if the lines, zeros of y'', *are also adherent to the non-singular zeros of* p, *we need to determine if* $\{p\}:s_p \subset \{y''\}$. *This is in general an open problem, the Ritt problem. Nonetheless here, we can apply a criterion issued from the leading coefficient theorem.*

A preparation congruence of p *w.r.t* $a = y''$ *is* $p \equiv 3\,y'^4\,a\,(\delta^2 a)^2 - 4\,y'^4\,\delta a^2\,\delta^2 a$ mod $[a]^4$. *It involves* $\delta^2 a$. *By (Kolchin 1973, IV.15, Theorem 7.a), we conclude that* $\{p\}:s_p \subset \{y''\}$. *Consequently, the zeros of* y'' *are also adherent to the non-singular zeros of* p.

As q is irreducible over $\mathbb{Q}$, $\{p\} = \{p\} : s_p \cap \{q\} : s_q$ is a prime minimal decomposition in $\mathbb{Q}\{y\}$. If we work in $\mathbb{Q}(\alpha)\{y\}$, where α is a root of the polynomial $x^2 + 3$, we know, without extra heavy computations that the minimal prime decomposition of $\{p\}$ in $\mathbb{Q}(\alpha)\{y\}$ is $\{p\} = \{p\} : s_p \cap \{q_1\} : s_{q_1} \cap \{q_2\} : s_{q_2}$, where $q_1 = y'y''' - \alpha\, y''^2$ and $q_2 = y'y''' + \alpha\, y''^2$ are the irreducible factors of q over $\mathbb{Q}(\alpha)$.

More examples are treated on *http://daisy.uwaterloo.ca/˜ehubert/Diffalg*.

8. Conclusion

We have extended the definition of the general solution, the preparation process, the component theorem and the low power theorem to regular differential polynomials. These extensions allowed us to present a new algorithm to compute a minimal decomposition of the radical differential ideal generated by a single differential polynomial. The algorithm, contrary to its predecessor, involves no factorization, is efficient and is implemented in Maple V. We are thus in a position to determine automatically the essential singular solutions of any algebraic differential equation, ordinary or partial.

For first order differential equations, the essential singular solutions are envelopes of the non-singular solutions. We can determine the contact order and analyze the singularities of the non-singular solutions by computing a differential basis of the general component (Hubert 1996).

Similar investigations should be made for higher order ordinary differential equations. To this aim, attempts to compute the differential basis of the general component were started in (Hubert 1997) and will be pursued. We speculate that this basis is useful to determine further properties of the general solution.

Acknowledgments: I am very grateful to F. Boulier for his suggestions and his readiness to answer my questions. I appreciated the work and the comments of the referees. I would also like to thank G. Labahn and M. Singer for their sensible comments in the writing of this paper.

References

Ablowitz, M., Clarkson, P. (1991). *Solitons, Nonlinear Evolution Equations and Inverse Scattering.* Number 149 in London Mathematical Society Lecture Note Series. Cambridge University Press.

Boulier, F., Lazard, D., Ollivier, F., Petitot, M. (1995). Representation for the radical of a finitely generated differential ideal. In Levelt, A., editor, *ISSAC'95*. ACM Press.

Boulier, F., Lazard, D., Ollivier, F., Petitot, M. (1997). Computing representations for radicals of finitely generated differential ideals. Technical Report IT-306, LIFL. (Submitted).

Darboux, G. (1870). Sur les solutions singulière des équations au dérivées ordinaires du premier ordre. *Bulletin des Sciences Mathématiques et Astronomiques*, 4.

Darboux, G. (1873). Solutions singulière des équations au dérivées partielles du premier ordre. *Mémoires présentés par divers savants étrangers à l'Académie des Sciences*, 27:1–243.

Eisenbud, D. (1994). *Commutative Algebra with a view toward Algebraic Geometry.* Graduate Texts in Mathematics. Springer-Verlag.

Eisenbud, D., Huneke, C., Vasconcelos, W. (1992). Direct method for primary decomposition. *Inventiones Mathematicae*, 110:207–235.

Hamburger, M. (1893). Ueber die sigulären lösungen der algebraischen differenzialgleichnungen erster ordnung. *Journal für die reine und angewandte Mathematik*, 112:205–246.

Hillman, A. (1943). A note on differential polynomials. *Bulletin of the American Mathematical Society*, 49:711–712.

Hillman, A., Mead, D. (1962). On the Ritt polygon process. *American Journal of Mathematics*, 84:629–634.

Hubert, E. (1996). The general solution of an ordinary differential equation. In *ISSAC'96*. ACM Press.

Hubert, E. (Avril 1997). *Algebra and Algorithms for Singularities of Implicit Differential Equations*. PhD thesis, Institut National Polytechnique de Grenoble. http://www-mediatheque.imag.fr/Mediatheque.IMAG/collections-electroniques/publications/theses/.

Kolchin, E. (1973). *Differential Algebra and Algebraic Groups*, volume 54 of *Pure and Applied Mathematics*. Academic Press.

Levi, H. (1942). On the structure of differential polynomials and on their theory of ideals. *Transaction of the American Mathematical Society*, 51:532–568.

Levi, H. (1945). The low power theorem for partial differential equations. *Annals of the Mathematical Society*, 46:113–119.

Murphy, G. (1960). *Ordinary Differential Equations and Their Solutions*. Van Nostrand Reinhold Co.

Ritt, J. (1930). Manifolds of functions defined by systems of algebraic differential equations. *Transaction of the American Mathematical Society*, 32:569–598.

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

Ritt, J. (1945a). Analytical theory of singular solutions of partial differential equations of the first order. *Annals of Mathematics*, 46(1):120–143.

Ritt, J. (1945b). On the manifold of partial differential polynomials. *Annals of Mathematics*, 46(1):102–112.

Ritt, J. (1946). On the singular solutions of certain differential equation of second order. *Proceedings of the National Academy of Sciences of the U.S.A*, 32:255–258.

Ritt, J. (1950). *Differential Algebra*, volume XXXIII of *Colloquium publications*. American Mathematical Society. reprinted by Dover Publications, Inc (1966).

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

Rubel, L. (1981). A universal differential equation. *Bull. Amer. Math. Soc. (N.S.)*, 4(3):345–349.

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

Vasconcelos, W. (1998). *Computational Methods in Commutative Algebra and Algebraic Geometry*, volume 2 of *Algorithms and Computation in Mathematics.*. Springer.

Whittaker, E., Watson, G. (1927). *A course of modern analysis*. Cambridge Mathematical Library. Cambridge University Press.

Symbolic Computation Group University of Waterloo, Ontario, Canada, N2L 3G1

E-mail address: `ehubert@daisy.uwaterloo.ca`

Mathematical Science Research Institute, Berkeley, California, USA 94720-5070

E-mail address: `evelyne@mrsri.org`