

The General Solution of an Ordinary Differential Equation.

Evelyne Hubert*
LMC-IMAG Grenoble
E-mail: Evelyne.Hubert@imag.fr

Abstract

We consider in this paper an implicit non-linear ordinary differential equation $p(x, y, y') = 0$. There are several types of solutions. The singular solutions are characterized by the fact they make $\frac{\partial p}{\partial y'}$ vanish. No such characterization of the so called *general solution* can be found in classical treatises.

We propose here an algorithmic method to compute a similar characterisation of the general solution. We apply the result to give some insight on the local behaviour of the solutions in the neighbourhood of a singular solution.

Key words : General Solution, Singular Solutions, Differential algebra, Formal Power Series Solution.

1 Introduction

This paper is mainly concerned with ordinary differential equations of first order

$$p(x, y, y') = 0 \quad (1)$$

where p is a polynomial.

When the equation is linear, the set of its solutions has the structure of an affine vector space. Algorithms have been developed (see [14]) to compute formal power series solutions of these equations in the neighbourhood of singular points, where numerical analysis proves to be inefficient.

In the non-linear case, the structure of the solutions is not as clear. There might be several *types* of solution. We may first distinguish the singular solutions, which are the common solutions of (1) and

$$\frac{\partial p}{\partial y'}(x, y, y') = 0 \quad (2)$$

As for the general solution, it has not really gained a rigorous definition in classical treatises.

In section 2 we will briefly give the basic definitions and properties of the theory of differential algebra. It gives some insight on the structure of the solutions: each *type* of solution is defined by a *prime differential ideal*. In this context

*this work has been supported by European project CATHODE. Permission to make digital/hard copies of all or part of this material for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial advantage, the copyright notice, the title of the publication and its date appear, and notice is given that copyright is by permission of the ACM, Inc. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires specific permission and/or fee. ISSAC'96, Zurich, Switzerland. ©1996 ACM 0-89791-796-0/96/07 ... \$3.50

we can give a rigorous definition of the general solution which is due to Ritt. This is to be found in section 3.

In section 4 we propose an algorithmic method to compute a differential basis of the prime differential ideal defining the general solution. In other words, we will compute equations which, if satisfied by a solution of (1), will ensure that this solution is in the general solution.

Two applications of this result are then tackled. The first one, in section 5, called the *Ritt problem*, is to determine if a singular solution is a particular solution (of the general solution).

The second one, in section 6, is a study of when we can develop the general solution into formal power series. This is mainly interesting along the singular solution where numerical analysis can get into trouble: the existence of a singular solution results in the existence of infinitely many differentiable solutions through a point.

Basically, for a nice enough initial condition (x_o, y_o, y'_o) , we mean

$$p(x_o, y_o, y'_o) = 0 \quad \text{and} \quad \frac{\partial p}{\partial y'}(x_o, y_o, y'_o) \neq 0,$$

we are in a case which is tantamount to a Cauchy problem. Developing the (general) solution at this point into formal power series may be achieved, for instance, by successively differentiating p in order to obtain the higher derivatives of the solution at that point.

This process can obviously not be applied if (x_o, y_o) lies on the graph of a singular solution even if the general solution at that point generically have no singularity. The equations of the general solution we compute will enable us to determine the maximal set of initial conditions for which the general solution can be expanded into formal power series. We will then be able to compute this power series solution up to any order.

2 Differential algebra preliminaries

Differential algebra was introduced by Ritt in the 1930s to extend the theory of commutative polynomial algebra to differential equations. In the following we give the definitions and properties we need to speak about the general solution of an ordinary differential equation. For an exhaustive presentation of differential algebra, the reader is referred to [12] and [10]. An introduction to the subject may be found in [9].

2.1 Differential rings

We consider a differential ring $(A, +, \cdot, \delta)$. $(A, +, \cdot)$ is a commutative integral domain. δ is a derivation on A : it is an additive morphism such that $\delta(ab) = a\delta b + b\delta a$ for all elements a, b in A .

A *differential ideal* I of (A, δ) is an ideal of A that is stable under derivation : $a \in I \Rightarrow \delta a \in I$. As in a commutative ring, a differential ideal I is *radical* if for $a \in A$ such that $\exists \alpha \in \mathbb{N}^*$, $a^\alpha \in I$ then $a \in I$. It is *prime* if $ab \in I \Rightarrow a$ or $b \in I$.

EXAMPLE 2.1 Any commutative ring A can be considered as a differential ring with a trivial derivation mapping any element of A to zero. On $A[x]$, the ring of polynomials with coefficients in A , we can define a derivation δ that extends the derivation on A and satisfies $\delta x = 1$. Then $\delta(a_n x^n + a_{n-1} x^{n-1} + \dots + a_0) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1$. \circ

We will use the following notations. Let σ be a subset of the differential ring A . We define $\sqrt{\sigma} = \{a \in A \text{ such that } \exists \alpha \in \mathbb{N}^* \ a^\alpha \in \sigma\}$. Besides we will note respectively (σ) , $[\sigma]$ and $\{\sigma\}$ the (non-differential) ideal, the differential ideal and the radical differential ideal generated by σ .

The radical (non-differential) ideal generated by σ is $\sqrt{(\sigma)}$. $[\sigma]$ is actually the ideal generated by the elements of σ together with their derivatives up to any order. Besides $\{\sigma\} = \sqrt{[\sigma]}$ provided A contains a field isomorphic to \mathbb{Q} . We shall assume from now on that A contains \mathbb{Q} .

PROPERTY 2.1 Let σ be a subset of a differential ring A . For $a, b \in A$, $\{\sigma, ab\} = \{\sigma, a\} \cap \{\sigma, b\}$.

$(A\{y\}, \bar{\delta})$ denotes the ring of differential polynomials with coefficients in (A, δ) in one differential indeterminate.¹ $A\{y\}$ is the polynomial ring in infinitely many indeterminates $A[y_0, y_1, y_2, \dots]$. $\bar{\delta}$ is a derivation on $A\{y\}$ which extends s^2 the derivation δ of A and ratifies $\bar{\delta} y_i = y_{i+1}$.

EXAMPLE 2.2 We can associate to the ordinary differential equation

$$\frac{d^2 y}{dx^2} + xy \frac{dy}{dx} + x^2 = 0$$

the differential polynomial $p = y_2 + xy_0 y_1 + x^2$, with coefficients in $A = \mathbb{Q}[x]$. \circ

2.2 Essential components

In this section we shall show that each *type* of solution of a system of differential equations is defined by a prime differential ideal. We first make clear the connection between a solution and a prime differential ideal. Then we turn our attention to any system of differential polynomials.

Let $(B, \bar{\delta})$ be a differential over-ring of (A, δ) . The set of differential polynomials of $(A\{y\}, \bar{\delta})$ that vanish for an element $\mu \in B$ is a prime differential ideal provided B is an integral domain.

Conversely, consider a prime differential ideal in $(A\{y\}, \bar{\delta})$ that has no element in A , 0 excepted: $P \cap A^* = \emptyset$. $A\{y\}/P$ is an integral differential overing of A . The class of

¹This can of course be extended to several differential indeterminate-s

²For this reason, we shall shorten $\bar{\delta}$ in δ

y in $A\{y\}/P$ is a zero of P , called the generic zero of P . (For a detailed treatment of this the reader is invited to refer to [15, chapter I] or [7, section 1].)

If we consider any set σ of differential polynomials in $A\{y\}$, its set of zeroes is equal to the set of zeroes of (σ) and $\{\sigma\}$. These ideals are generically not prime.

To be able to handle the ideals in a differential polynomials ring, we would like to know about its noetherianity. We introduce a weaker notion that can be lifted from the ring of coefficients.

EXAMPLE 2.3 \mathbb{Q} is a field and is thus noetherian. Nonetheless $[y^2, (y')^2, (y'')^2, \dots] \in \mathbb{Q}\{y\}$ is not finitely generated. But $\{y^2, (y')^2, (y'')^2, \dots\} = \{y\}$ is. \circ

A differential ring (A, δ) is radically noetherian, if any radical differential ideal in it is finitely generated. In a radically noetherian differential ring, any radical differential ideal R is the intersection of a finite number of prime differential ideals.

$$R = \bigcap_{k=1}^r P_k$$

where the P_k are prime differential ideals. Furthermore, when we get rid of the P_k containing other ones, we get a minimal decomposition of R that is unique. The remaining P_k are the *essential components* of R .

The differential Hilbert basis theorem states that if (A, δ) is radically noetherian, so is $(A\{y\}, \bar{\delta})$. We assume from now on that it is the case. Therefore, any radical differential ideal in $(A\{y\}, \bar{\delta})$ has a unique minimal decomposition into essential components.

Consider a set σ of differential polynomials in $A\{y\}$. If a differential polynomial vanish on all the zeroes of σ , then it belongs to $\{\sigma\}$ (theorem of zeroes). Therefore the essential components of $\{\sigma\}$ describe completely the set of zeroes of σ . Each component defines a *type* of solution of σ as we have seen at the beginning of this section.

In section 3 we shall focus on one of the essential components when σ is made of a single polynomial : the component of the so called *general solution*. Let us look at an easy example (given in [12] and [9]) :

EXAMPLE 2.4 Consider the differential polynomial $p = y_1^2 - 4y_0 \in \mathbb{Q}\{y\}$ associated to the differential equation $y'^2 - 4y = 0$.

Thanks to property 2.1 we can write :

$$\begin{aligned} \{p\} &= \{p, \delta p\} = \{y_1^2 - 4y_0, 2y_1(y_2 - 2)\} \\ &= \{y_1^2 - 4y_0, y_2 - 2\} \cap \{y_1^2 - 4y_0, y_1\}. \end{aligned}$$

The decomposition in essential components of $\{p\}$ is actually $\{p\} = \{y_1^2 - 4y_0, y_2 - 2\} \cap \{y_1^2 - 4y_0, y_1\}$. The differential equation has thus two *types* of solution. The first is given by $\bar{y}(x) = 0$, the second is the solution of the system

$$\begin{cases} y'' - 2 = 0 \\ y'^2 - 4y = 0 \end{cases}$$

and thus can be given by $\bar{y}(x) = (x + a)^2$, where a is an arbitrary constant. Note that \bar{y} can not be obtained from \bar{y} by specializing a .

As seen in the introduction \bar{y} is a singular solution. The component $\{y_1^2 - 4y_0, y_2 - 2\}$ is the component of the *general solution*. \circ

The way we may compute the generators of the component defining the general solution is not always as trivial as in this example. It has been obtained by factorizing the separant, $\frac{\partial p}{\partial y_1}$, from the elements of $\{p\}$. The generalisation lies in the notion of quotient ideals we introduce in the next section.

2.3 Quotient ideals

The definition and properties given in what follows are of course suitable to commutative algebra. The reader is referred for instance to [7] for proofs and further details.

For a differential ideal I in A and an element $s \in A$ we define the saturation of I with respect to s

$$I : s^\infty = \{a \in A \mid \exists \alpha \in \mathbb{N} \ s^\alpha a \in I\}$$

which is a differential ideal containing I . For a radical differential ideal R in A and an element $s \in A$ we can define the quotient of R by s

$$R : s = \{a \in A \mid sa \in R\}$$

which is a radical differential ideal containing R . Note that $\sqrt{I : s^\infty} = \sqrt{I} : s$.

A generalisation of the property of decomposition 2.1 will be at the heart of the definition of the general solution :

PROPERTY 2.2 Let σ be a non-empty subset of A and s an element of A . Then $\{\sigma\} = \{\sigma\} : s \cap \{\sigma, s\}$.

Consider now a ring of differential polynomials $A\{y\}$. Let p be an element of $A\{y\}$, d its order. The separant s of p is $s = \frac{\partial p}{\partial y_d}$. p can be considered as a polynomial in $A[y_0, \dots, y_d]$. Note that in this ring $(p) : s^\infty$ is a radical ideal. Likewise, for $\alpha \in \mathbb{N}$, $\delta^\alpha p$ can be considered as a polynomial in $A[y_0, \dots, y_{d+\alpha}]$.

LEMMA 2.3 Let q be an element of $[p] : s^\infty$. If its order does not exceed $d + \alpha$, for some $\alpha \in \mathbb{N}$, then $q \in (p, \delta p, \dots, \delta^\alpha p) : s^\infty$.

This lemma, which is given in [10, I.11], entitles us to lift the algebraic properties of $(p) : s^\infty$ to the differential ideal $[p] : s^\infty$. For instance, as $(p) : s^\infty$ is a radical ideal in $A[y_0, \dots, y_d]$, $[p] : s^\infty$ is a radical differential ideal in $A\{y\}$ and is therefore equal to $\{p\} : s$. What we shall need in the next section is:

COROLLARY 2.4 If $(p) : s^\infty$ is a prime ideal of $A[y_0, \dots, y_d]$, $[p] : s^\infty$ is a prime differential ideal of $A\{y\}$.

The simplest case appears when p , considered as a polynomial in $A[y_0, \dots, y_d]$, is algebraically irreducible.

3 The general solution of a scalar differential equation

Following Ritt ([12], ch II) and Kolchin ([10], ch IV), we consider a differential polynomial p of $A\{y\}$. Let d be its order and s its separant. From property 2.2 we know that: $\{p\} = \{p\} : s \cap \{p, s\}$.

If we assume that p , considered as a polynomial of $A[y_0, \dots, y_d]$, is irreducible, $\{p\} : s = [p] : s^\infty$ is a prime differential ideal (corollary 2.4). It is thus the only essential component of $\{p\}$ that does not contain s .

DEFINITION 3.1 Let p be an irreducible differential polynomial of $A\{y\}$, s its separant. The general solution of p is the solution defined by the only essential component of $\{p\}$ that does not contain s : $\mathcal{G}_p = \{p\} : s$. \mathcal{G}_p is called the general component.

The other components of $\{p\}$ are to be taken among the components of $\{p, s\}$ which correspond to singular solutions. Assume the decomposition into essential components of this radical differential ideal is as follow:

$$\{p, s\} = \bigcap_{k=1}^{r_1} S_k.$$

Then $\{p\} = \mathcal{G}_p \cap S_1 \cap \dots \cap S_k$. But \mathcal{G}_p might be included in some of the S_i . This means that some of the S_i are not essential components of $\{p\}$. This corresponds to the notion of *particular solutions* in classical treatises (see [8] for instance). We will illustrate this in the example of the next section.

Determining whether a singular solution is in the general solution was called *the Ritt problem* by Kolchin. It was indeed first investigated by Ritt in [11]. The method proposed there has its foundation in the *low power theorem* and the *preparation process*. In section 5 we shall give another way to tackle this problem in the first order case. Actually, the following sections are devoted to first order differential polynomials.

4 Computing a basis of the general solution

p is a *characteristic set* of \mathcal{G}_p . This means in particular that we can test the membership to \mathcal{G}_p with a *Ritt reduction*. But this does not give a complete description of \mathcal{G}_p . For instance, p does not generate \mathcal{G}_p . As a consequence, the singular points of \mathcal{G}_p are contained in those of p but the inclusion can be strict.

What we undertake in this section is to compute a basis of the general component \mathcal{G}_p . We will achieve that by taking the problem to polynomial algebra. This is theoretically always possible. The decomposition into prime differential ideals of the radical differential ideal generated by a finite number of differential polynomials amounts to a similar problem in (non differential) polynomial algebra provided you consider enough derivatives of the given differential polynomials (see [12, chV.28]).

In the special case of a first order differential polynomial, a bound for the number of derivations to be made was brought by Ritt [12, ch VI.9] in the analytical case. Owing to the differential Lefschetz principle, due to Seidenberg [13], this result remains in abstract differential algebra. Cohn has nonetheless proved it directly in [4].

THEOREM 4.1 Let p be a first order irreducible differential polynomial of $A\{y\}$, where A is a field. Let s be its separant and m its degree in y_1 . Now, in the polynomial ring $A[y_0, \dots, y_m]$, let P_o be the unique essential component of the ideal $\sqrt{(p, \delta p, \dots, \delta^{m-1} p)}$ which does not contain s . Then

$$\mathcal{G}_p = \{P_o\}.$$

This means that if the set g_1, \dots, g_r is a basis of the polynomial ideal P_o , g_1, \dots, g_r is also a differential basis of

\mathcal{G}_p : for any $q \in \mathcal{G}_p$ there exists an $\alpha \in \mathbb{N}^*$ such that q^α is a linear combination of the g_i and their derivatives.

Thus, finding a basis of the general component amounts to computing the decomposition into prime ideals in polynomial algebra. This has been studied in [6]. But we claim that we know what P_0 is and that we can compute it directly.

For a given $k > 1$, we shall look more carefully at the ideal $\sqrt{(p, \delta p, \dots, \delta^{k-1} p)}$ in $A[y_0, \dots, y_k]$. We first note that, according to property 2.2,

$$\sqrt{(p, \dots, \delta^{k-1} p)} = \sqrt{(p, \dots, \delta^{k-1} p)} : s \cap \sqrt{(p, \dots, \delta^{k-1} p, s)}.$$

Besides lemma 2.3 implies that

$$\mathcal{G}_p^k = (p, \delta p, \dots, \delta^{k-1} p) : s^\infty = \mathcal{G}_p \cap A[y_0, \dots, y_k]$$

since $\mathcal{G}_p = [p] : s^\infty$. This ensures that $(p, \dots, \delta^{k-1} p) : s^\infty$ is prime and therefore equal to $\sqrt{(p, \delta p, \dots, \delta^{k-1} p)} : s$.

COROLLARY 4.2 $P_0 = (p, \delta p, \dots, \delta^{m-1} p) : s^\infty$.

For computational purpose we shall consider from now on the field of coefficients to be $A = \mathbb{Q}(x)$. We will actually lead our calculations in $\mathbb{Q}[x]$ but we shall be careful with the validity of our results over its fraction field.

We thus assume p is a first order irreducible differential polynomial p with coefficients in $\mathbb{Q}[x]^3$: p can be viewed as an irreducible polynomial in $\mathbb{Q}[x][y_0, y_1] = \mathbb{Q}[x, y_0, y_1]$. According to the Gaussian lemma, p remains irreducible in $\mathbb{Q}(x)[y_0, y_1]$.

Now, computing a basis of the saturation ideal $P_0 = (p, \delta p, \dots, \delta^{m-1} p) : s^\infty$ in $\mathbb{Q}[x, y_0, \dots, y_m]$ can be achieved using Grbner bases properties (see for instance [1]). First $(p, \delta p, \dots, \delta^{m-1} p) : s^\infty$ is the elimination ideal of $(sz - 1, p, \delta p, \dots, \delta^{m-1} p)$, living in $\mathbb{Q}[x, y_0, \dots, y_m, z]$, according to the dummy indeterminate z : $(p, \delta p, \dots, \delta^{m-1} p) : s^\infty = (sz - 1, p, \delta p, \dots, \delta^{m-1} p) \cap \mathbb{Q}[x, y_0, \dots, y_m]$.

On $\mathbb{Q}[x, y_0, \dots, y_m, z]$ a term order $>$ where z prevails satisfies the property: $\forall \alpha, \beta \in \mathbb{N}^*$ such that $\alpha > \beta$, for any monomials r and t of $\mathbb{Q}[x, y_0, \dots, y_m]$, $z^\alpha r > z^\beta t$. On the contrary x will be said to be reverse prevailing for $<$ if for any monomials r and t in $\mathbb{Q}[y_0, \dots, y_m, z]$, $x^\alpha r > x^\beta t$ iff $r > t$ or $(r = t$ and $\alpha > \beta)$.

If $G' = \{g_1, \dots, g_s\}$ is a Grbner basis of $(sz - 1, p, \delta p, \dots, \delta^{m-1} p)$ according to a term order where z prevails, then $G = G' \cap \mathbb{Q}[x, y_0, \dots, y_m]$ is a Grbner basis of the elimination ideal $(sz - 1, p, \delta p, \dots, \delta^{m-1} p) \cap \mathbb{Q}[x, y_0, \dots, y_m]$, which exactly is the saturation ideal $(p, \delta p, \dots, \delta^{m-1} p) : s^\infty$, according to the term order induced by $<$ on $\mathbb{Q}[x, y_0, \dots, y_m]$.

Moreover if we chose the order $<$ so that x is reverse prevailing, G is a Grbner basis of $(p, \delta p, \dots, \delta^{m-1} p) : s^\infty$ in $\mathbb{Q}(x)[y_0, \dots, y_m]$ with respect to the restriction of $<$ to the terms in the y_i .

EXAMPLE 4.1 Consider the differential polynomial $p = y_1^3 - 4xy_0y_1 + 8y_0^2 \in \mathbb{Q}(x)\{y\}$.

The singular solutions are the zeros of

$$\{p, s\} = \{p, 3y_1^2 - 4xy_0\} = \{27y_0 - 4x^3\} \cap \{y_0\}.$$

There are thus two of them: $\bar{y}_1(x) = 0$ and $\bar{y}_2(x) = \frac{4}{27}x^3$.

³Had p coefficients in $\mathbb{Q}(x)$, we could equivalently consider the principal part of the polynomial obtained by multiplying p by the least common multiple of the denominators of its coefficients.

To obtain a differential basis of the general solution, we first compute (with the help of Maple) in $\mathbb{Q}[x, y_0, \dots, y_3, z]$ a Grbner basis of $(p, \delta p, \delta^2 p, sz - 1)$ with a lexicographical order $x < y_0 < y_1 < y_3 < z$. Eliminating from this Grbner basis the polynomials where z appears, we obtain a Grbner basis of \mathcal{G}_p^3 , which lives in $\mathbb{Q}(x)[y_0, \dots, y_3]$. This is a differential basis of \mathcal{G}_p .

$$\mathcal{G}_p = \{y_3, y_2^2 - 2xy_2 + 2y_1, y_1y_2 - 2xy_1 + 4y_0, 2y_0y_2 - y_1^2, y_1^3 - 4xy_0y_1 + 8y_0^2\}.$$

As $y_3 \in \mathcal{G}_p$, the zero of \mathcal{G}_p is a polynomial of second order. We make its coefficients fulfill the other equations and we can write it as $\bar{y}(x) = a(x + a)^2$ where a is an arbitrary constant.

Each basis differential polynomial of \mathcal{G}_p is in $\{y_0\}$, thus $\mathcal{G}_p \subset \{y_0\}$. Therefore $\{y_0\}$ can not be an essential component. Meanwhile, 0 is a special case of $a(x + a)^2$ when $a = 0$. \bar{y}_1 is a particular solution.

Conversely, we can not find any a such that $\frac{4}{27}x^3$ equals $a(x + a)^2$. Meanwhile we can easily check that y_3 is not in $\{27y_0 - 4x^3\}$, which therefore does not contain \mathcal{G}_p . $\{27y_0 - 4x^3\}$ is an essential component of $\{p\}$.

$$\{p\} = \mathcal{G}_p \cap \{27y_0 - 4x^3\}.$$

◦

5 The Ritt problem

How to handle the Ritt problem in the first order case has been introduced in the previous example. On the one hand, we need to compute the singular components, by this we mean the essential components of $\{p, s\}$. As they are of order zero, this amounts to an algebraic problem. We can proceed as follow: Compute the decomposition into prime ideals in $\mathbb{Q}(x)[y_0, y_1]$ of the radical ideal $\sqrt{(p, s, \frac{\partial p}{\partial x} + y_1 \frac{\partial p}{\partial y_0})}$ using, for instance, the package presented in [6]. For each component obtained, the Rosenfeld-Grbner algorithm of Boulier (see [2] or [3]) can test if it defines a solution. If it does, the algorithm provides a membership test.

On the other hand, we have shown in the previous section how to obtain a differential basis of the general solution \mathcal{G}_p . Testing if \mathcal{G}_p is included into a singular component amounts to testing that each differential polynomial in the basis belongs to the singular component.

6 Developing the general solution into power series

This section shows how the basis of the general solution can help in giving some insight on the local behaviour of the general solution in the neighbourhood of a singular solution.

We consider a first order irreducible differential polynomial p in $\mathbb{Q}[x]\{y\}$. Let s be its separant. Both s and p can be seen as polynomials in $\mathbb{Q}[x, y_0, y_1]$. Likewise we will come across the rings of polynomials $\mathbb{Q}[x, y_0, y_1, \dots, y_r]$ for some $r \geq 1$. For some polynomials $p_1, \dots, p_l \in \mathbb{Q}[x, y_0, y_1, \dots, y_r]$, we will denote their affine variety in \mathbb{C}^{l+1} by $\mathcal{V}(p_1, \dots, p_l)$.

Suppose we are given the initial condition $(x^0, y_0^0) \in \mathbb{C}^2$. Provided (x^0, y_0^0) is not a singular point, that is (x^0, y_0^0) is not a root of the resultant of s and p in y_1^4 , we can develop

⁴The resultant determines the points where p and s have a common root in y_1 , that is the points where p has a multiple root in y_1 .

the general solution of p at this point into a formal power series :

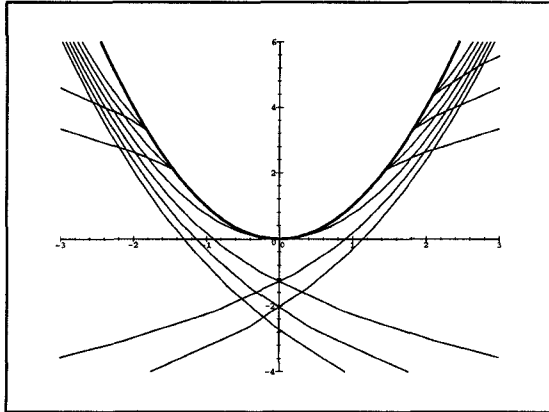
$$\bar{y} = y_0^o + (x - x^o)y_1^o + \frac{(x - x^o)^2}{2}y_2^o + \dots = \sum_{i \geq 0} \frac{(x - x^o)^i}{i!} y_i^o$$

where y_1^o is a simple root of $p(x^o, y_0^o, y_1)$ and the y_i^o for $i > 1$ are obtained by successively differentiating p . Indeed $\delta p = sy_2 + t_1$, $\delta^2 p = sy_3 + t_2, \dots$, where s, t_1 involve only x, y_0, y_1 and t_2 involves only x, y_0, y_1, y_2 . Therefore

$$y_2^o = \frac{t_1(x^o, y_0^o, y_1^o)}{s(x^o, y_0^o, y_1^o)}, y_3^o = \frac{t_2(x^o, y_0^o, y_1^o, y_2^o)}{s(x^o, y_0^o, y_1^o)}, \dots$$

At singular points, we should not expect to find such formal power series solutions. First we shall distinguish regular singular points, when $\frac{\partial p}{\partial x} + y_1 \frac{\partial p}{\partial y}$ does not vanish, from contact singular points. On the regular singular points, the underlying differential equation is generically equivalent to $y'^2 = x$. Solutions generically have a cusp at such points.

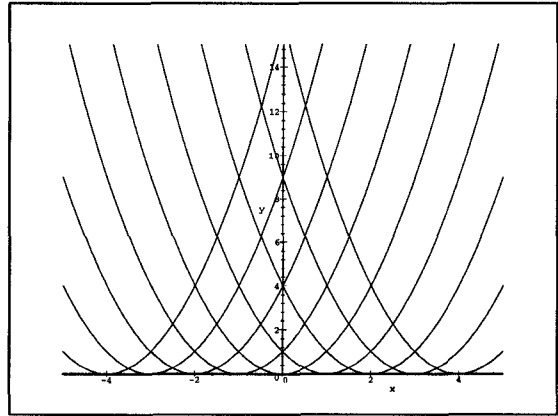
EXAMPLE 6.1 Consider the equation $y'^2 - 2xy' - y = 0$ associated to the differential polynomial $p = y_1^2 - 2xy_1 - y_0$. Then $s = \frac{\partial p}{\partial y_1} = 2y_1 - 2x$. Thus $\sqrt{(p, s)} = (y_1 - x, y_0 - x^2)$. The locus of singular points is the parabola $y_0 = x^2$. If we sketch the graphs of the solutions in the (x, y_0) plane we indeed see that they have a cusp on this parabola.



Note that the origin is a contact singular point. Two continuously differentiable solutions cross it. \circ

When the locus of singular points turns into a singular solution, it is made of contact singular points. The general solution does not, generically, have singularities then.

EXAMPLE 6.2 Recall example 2.4. If we sketch the graph of the solutions it looks like



The general solutions $\tilde{y}(x) = (x + a)^2$ have no singularities along the singular solution $\bar{y}(x) = 0$. \circ

We can thus expect to develop the general solution into formal power series along the singular solution. Note that we intrinsically look for infinitely differentiable solutions. In the example above, infinitely many differentiable solutions go through a point. More generally, when there is a singular solution, there may be infinitely many r -times differentiable solutions through a point. This r is bounded by the $m - 1$ in theorem 4.1.

Assume we have a formal power series that is a zero of $\mathcal{G}_p : \tilde{y} = \sum_{i \geq 0} \frac{(x - x^o)^i}{i!} y_i^o$. Then (x^o, y_1^o, y_2^o) is a zero of p . Likewise $(x^o, y_0^o, \dots, y_k^o)$ is a zero of the \mathcal{G}_p^k .

Conversely, we seek conditions under which (x^o, y_0^o) extends to a formal power series solution, that is, conditions under which we may find $y_1^o, y_2^o, y_3^o, \dots$. Part of the answer is given by the following *extension theorem* (see for instance [5]).

THEOREM 6.1 Let I be the ideal generated by some $g_1, \dots, g_l \in \mathbb{Q}[z_1, \dots, z_m, z]$. Let J be the elimination ideal of I according to $z : J = I \cap \mathbb{Q}[z_1, \dots, z_m]$. For each $1 \leq i \leq l$ write g_i in the form :

$$g_i = q_i(z_1, \dots, z_m)z^{N_i} + \text{terms of degree} < N_i \text{ in } z,$$

where $N_i \geq 0$ and q_i is non-zero.

Suppose $(a_1, \dots, a_m) \in \mathbb{C}^m$ is a zero of J (we call it a partial solution). If at least one of the q_i does not vanish for (a_1, \dots, a_m) then there exists $a \in \mathbb{C}$ such that (a_1, \dots, a_m, a) is a zero of I .

This theorem can be proved with resultants.

Note that we only have a sufficiency condition for the extension step to work : the partial solution must not be on the affine variety of the leading coefficients, $\mathcal{V}(q_1, \dots, q_l)$. Moreover the q_i depend on the given basis g_1, \dots, g_l of I .

But if g_1, \dots, g_l is a Grbner basis of I according to an order where z prevails the z -homogenisation of the g_i will give a basis of the z -homogenisation I^h of I . The projective variety of I^h is the projective closure of the affine variety of I . Therefore if a partial solution (a_1, \dots, a_m) makes all the leading coefficient q_i vanish, there is at least one way to extend this solution with an infinite value for z .

To put it in other words, if g_1, \dots, g_l is a Grbner basis of I according to an order where z prevail $\mathcal{V}(q_1, \dots, q_l)$ will be

the smallest set where we cannot make an extension step in \mathbb{C} .

Before giving the general algorithm, let us look at an example of how we can apply this theorem to decide when an initial condition extends to a formal power series solution.

EXAMPLE 6.3 Let p be the differential polynomial of $\mathbb{Q}[x]\{y\}$ given by $p = x^2y_1^2 + 2xy_0y_1 + y_0^2 - 4x^2y_0$. Thus $s = 2x(xy_1 + y_0)$ and the resultant of p and s is $r = 16x^6y_0$.

Therefore, for the initial conditions $(x^\circ, y_0^\circ) \in \mathbb{C}^2$ where $y_0^\circ \neq 0$ and $x \neq 0$, we can develop the general solution into formal power series by successively deriving p . We are going to show that the initial condition (x°, y_0°) can be extended into a formal power series solution under the less restrictive assumption that $x^\circ \neq 0$.

Note that the affine variety of (p, s) has two components

$$\sqrt{(p, s)} = (x, y_0) \cap (y_0, y_1)$$

$x, y_0 = 0$ is a contact singular point while $y_0, y_1 = 0$ corresponds to a singular solution $\tilde{y}(x) = 0$.

A differential basis of the general solution \mathcal{G}_p is given by a basis of $\mathcal{G}_p^2 = (p, \delta p) : s^\infty$. To be able to do the extension steps for a maximal set of initial condition we compute a Grbner basis of \mathcal{G}_p^2 according to the lexicographical order $y_2 > y_1 > y_0 > x$ (with the help of Maple) :

$$\begin{aligned} \mathcal{G}_p^2 = (p, \delta p) : s^\infty = & (2x^2y_2 + 3xy_1 - y_0 - 4x^2, \\ & \underline{2xy_0y_2 + xy_1^2 + 5y_0y_1 - 8xy_0}, \\ & (5xy_1 + y_0)y_2 + 8y_1^2 - 10xy_1 - 4y_0, \\ & \underline{2y_0^2y_2 - 5xy_1^3 - 9y_0y_1^2 + 20xy_0y_1 - 8y_0^2}, \\ & \underline{x^2y_1^2 + 2xy_0y_1 + y_0^2 - 4x^2y_0}). \end{aligned}$$

The underlined terms correspond to the leading coefficients (the q_i of the extension theorem).

In virtue of theorem 6.1, given the initial condition (x°, y_0°) , we may find $y_1^\circ \in \mathbb{C}$ a root of $p(x^\circ, y_0^\circ, y_1)$ provided $x^\circ \neq 0$. Now,

$$\sqrt{(p, 2y_0^2, 5xy_1 + y_0, 2xy_0, 2x^2)} = (x, y_0).$$

that corresponds to the contact singular point. According to the same theorem, for a given zero of p , $(x^\circ, y_0^\circ, y_1^\circ)$ such that $(x^\circ, y_0^\circ) \neq (0, 0)$ we may find $y_2^\circ \in \mathbb{C}$ such that $(x^\circ, y_0^\circ, y_1^\circ, y_2^\circ)$ is a zero of \mathcal{G}_p^2 . Furthermore y_2 appears, when it actually does, linearly in the polynomials of the basis of \mathcal{G}_p^2 . Considering them as differential polynomials, this implies that their separant is equal to their leading coefficient: y_3 will have the same coefficient in the derivated polynomials. We will thus be able to find y_3° . Similarly, we will successively get $y_4^\circ, y_5^\circ, \dots$

Let us take an initial condition on the singular solution: $y_0^\circ = 0$. We must chose $x^\circ \neq 0$ and $y_1^\circ = 0$. With such an initial condition there is only one polynomial in y_2 which does not vanish: $q = 2x^2y_2 + 3xy_1 - y_0 - 4x^2$. Thus $y_2^\circ = 2$. Differentiating q we will get y_3° : $\delta q = 2x^2y_3 + 7xy_2 + 2y_1 - 8x$. and consequently $y_3^\circ = -\frac{3}{x^\circ}$.

Carrying on that way we find the formal power series solution around the point $(x^\circ, 0)$:

$$\begin{aligned} \tilde{y}(x) = & (x - x^\circ)^2 - \frac{(x - x^\circ)^3}{x^\circ} + \frac{23(x - x^\circ)^4}{48(x^\circ)^2} \\ & - \frac{15(x - x^\circ)^5}{22(x^\circ)^3} + \frac{533(x - x^\circ)^6}{1152(x^\circ)^4} + \dots \end{aligned}$$

o

The first step of a general algorithm is thus to compute a Grbner basis of \mathcal{G}_p^m according to a lexicographical order $x < y_0 < y_1 < \dots < y_m$. We can read out of it the successive basis of the \mathcal{G}_p^k for all $1 \leq k \leq m$. This has the form :

$$\mathcal{G}_p^m \left\{ \begin{array}{l} \mathcal{G}_p^1 \left\{ \begin{array}{l} g_1^1 = q_1^1(x, y_0)y_1^{N_1} + \dots \\ \mathcal{G}_p^2 \left\{ \begin{array}{l} g_1^2 = q_1^2(x, y_0, y_1)y_2^{N_2} + \dots \\ \vdots \\ g_i^2 = q_i^2(x, y_0, y_1)y_2^{N_i} + \dots \end{array} \right. \\ \mathcal{G}_p^3 \left\{ \begin{array}{l} g_1^3 = q_1^3(x, y_0, y_1, y_2)y_3^{N_{i+1}} + \dots \\ \vdots \end{array} \right. \\ \dots \\ \vdots \\ g_k^m = q_k^m(x, y_0, \dots, y_{m-1})y_m^{N_r} + \dots \end{array} \right. \end{array} \right.$$

where $g_1^1 = p$.

We give the following notations: for some $1 \leq r \leq m$, \mathbf{g}^r will be the set of polynomials $\{g_i^r\}_i$, and \mathbf{q}^r the set of leading coefficients of the extension theorem:

$$\mathbf{q}^r = \left(\bigcup_{i=1, r-1} \mathbf{g}^i \right) \cup \{q_i^r\}_i.$$

We are going to look under which minimal conditions an initial condition (x°, y_0°) can be extended to a formal power series. The key point is that these conditions will be on x° , and the m first derivatives of $y, y_0^\circ, y_1^\circ, \dots, y_m^\circ$, only.

The first step is to find under which conditions (x°, y_0°) can be extended to a zero $(x^\circ, y_0^\circ, y_1^\circ, \dots, y_m^\circ)$ of \mathcal{G}_p^m . This is done by extending with one derivative at a time and applying at each step the extension theorem: provided (x°, y_0°) is not a root of q^1 , y_1° can be found in \mathbb{C} such that $(x^\circ, y_0^\circ, y_1^\circ)$ is a zero of p , that is a zero of \mathcal{G}_p^1 . $(x^\circ, y_0^\circ, y_1^\circ)$ extends to a zero $(x^\circ, y_0^\circ, y_1^\circ, y_2^\circ)$ of \mathcal{G}_p^2 if $(x^\circ, y_0^\circ, y_1^\circ) \notin \mathcal{V}(\mathbf{q}^2)$. Taking similar successive steps we will find the conditions under which (x°, y_0°) can be extended to a zero $(x^\circ, y_0^\circ, y_1^\circ, \dots, y_m^\circ)$ of \mathcal{G}_p^m .

Secondly, to extend this zero to higher orders, that is to determine when we can find $y_{m+1}^\circ, y_{m+2}^\circ, \dots$, a general process⁵ would be to compute successively the $\mathcal{G}_p^{m+1}, \mathcal{G}_p^{m+2}, \dots$. But in the case of a first order differential polynomial p we are considering here, we know that the $\{\mathbf{g}^r\}_{1 \leq r \leq m}$ is a differential basis of \mathcal{G}_p . Moreover, for $j < m$, $\delta g_i^j \in \mathcal{G}_p^{k+1}$. Therefore, adding the δg_i^m to the basis of \mathcal{G}_p^m will give a basis of \mathcal{G}_p^{m+1} . Similarly, adding all the derivatives up to order r of the polynomials in the set \mathbf{g}^m to the basis of \mathcal{G}_p^m will give a basis \mathcal{G}_p^{m+r} .

Let \mathbf{q}^{m+1} denote the set of separants of the polynomials in \mathbf{g}^m . This is the set of the leading coefficients in the derivatives of the polynomials in \mathbf{g}^m .

If the zero $(x, y_0^\circ, \dots, y_m^\circ)$ of \mathcal{G}_p^m we obtained earlier is not in the affine variety of \mathbf{q}^{m+1} , then it satisfies the condition of the extension theorem, and we can find a formal power series solution (up to any order).

We shall point out that if a partial solution $(x, y_0^\circ, \dots, y_k^\circ)$ is in $\mathcal{V}(\mathbf{q}^{k+1})$, it does not mean that there is no power eerie

⁵We mean a process that could be applied for a higher order differential polynomial.

solution extending it. It just means there is another type of solution (corresponding to a infinite y_{k+1}^o) which extends it.

EXAMPLE 6.4 In the last example, we have shown that when $x^o = 0$ the general solution could not be expanded into formal power series. But you can check that $\tilde{y}(x) = \frac{4}{9}x^2$ is a solution in the neighbourhood of $x^o = 0$. The point is that in the neighbourhood of $x^o = 0$ there are other solutions. Indeed the general solution is given by $\tilde{y}_b(x) = \frac{4}{9}x^2 + \frac{9}{16}\frac{b^2}{x} + b\sqrt{x}$, where b is an arbitrary constant. \circ

To put it in a nutshell, provided we can find a zero (x, y_0^o, \dots, y_m^o) of \mathcal{G}_p^m , by successive extension steps, which is not in the union of the affine varieties of the leading coefficient $\bigcup_{r=1}^{m+1} \mathcal{V}(\mathbf{q}^r) = \mathcal{V}(\bigcap_{r=1}^{m+1} (\mathbf{q}^r))$, we know we can develop the general solution into formal power series up to any order.

For higher order differential equation, we may find the formal power series of the general solution up to a given order k by similarly computing the \mathcal{G}_p^k . Nonetheless, we do not know whether it will extend any further.

7 Prospects

Points on the algebraic variety of the leading coefficients, which are the points where the general solution can not be developed into formal power series, require another approach. We shall certainly think about a more general class of formal series if we are tempted to develop the solution at these points.

It would be nice to extend the results to higher orders. As for a scalar differential equation of order higher than one, we have defined the general solution and computing its basis and developing it into formal power series can be done in quite the same way. What is left to determine is the bound for the number of derivations to be made.

When considering a system of differential equations, the first step is to find the right definition of the general solution. The keystone lies on a generalisation of the separant.

Acknowledgements : I am very grateful to Dr. F. Boulier for his numerous constructive comments and encouragements. I am also indebted to Pr. W. Sit for pointing out some problems in my paper.

References

- [1] BECKER, T., AND WEISPFENNING, V. *Grbner Bases - A Computational Approach to Commutative Algebra*. Springer-Verlag, 1993.
- [2] BOULIER, F. *Etude et Implantation de Quelques Algorithmes en algbre différentielle*. PhD thesis, Universit de Lille, 1994.
- [3] BOULIER, F., LAZARD, D., OLLIVIER, F., AND PETITOT, M. Representation for the radical of a finitely generated differential ideal. In *ISSAC'95* (1995), A. Levelt, Ed., ACM Press, 158–166.
- [4] COHN, R. The general solution of a first order differential polynomial. *Proceedings of the American Mathematical Society* 55, 1 (1976), 14–16.

- [5] COX, D., LITTLE, J., AND O'SHEA, D.. *Ideals, Varieties, and Algorithms*. Springer-Verlag, 1992.
- [6] GIANNI, P., TRAGER, B., AND ZACHARIAS, G. Grbner bases and primary decomposition of polynomial ideals. *Journal of Symbolic Computation* 6 (1988), 149–167.
- [7] HUBERT, E. Equations différentielles scalaires - solution gnrale et solutions singulires. Tech. rep., LMC - IMAG, 1995.
- [8] INCE, E. *Ordinary Differential Equations*. Dover Publications, Inc., 1956.
- [9] KAPLANSKY, I. *An Introduction to Differential Algebra*. Hermann, 1970.
- [10] KOLCHIN, E. *Differential Algebra and Algebraic Groups*, vol. 54 of *Pure and Applied Mathematics*. Academic Press, 1973.
- [11] RITT, J. On the singular solutions of algebraic differential equations. *Annals of Mathematics* 37, 3 (1936), 552–617.
- [12] RITT, J. *Differential Algebra*. Dover Publications, Inc, 1966.
- [13] SEIDENBERG, A. Abstract differential algebra and the analytic case. *Proceedings of the American Mathematical Society* 9 (1958), 159–164.
- [14] TOURNIER, E. *Solutions Formelles d'Equations Différentielles*. PhD thesis, IMAG, Grenoble, 1987.
- [15] WEIL, J.-A. *Constantes et Polynmes de Darboux en Algèbre Différentielle : Application aux Systèmes Différentiels Linéaires*. PhD thesis, GAGE-Ecole Polytechnique, 1995.

EVELYNE HUBERT is a final year Ph. D. student in the *Laboratoire de Modélisation et de Calcul, Grenoble*. She graduated from the Computer Science and Applied Mathematics College in Grenoble (the ENSIMAG) and obtained a Master's degree in Mathematics at Imperial College, London. She is now a member of the team of *Computer Algebra for Ordinary Differential Equations* where she investigates the non-linear equations from an algebraic standpoint.