Computing representations for radicals of finitely generated differential ideals

François Boulier, Daniel Lazard, François Ollivier, Michel Petitot

J. Symbolic Computation (2001) **11**, 1–000

Computing representations for radicals of finitely generated differential ideals

François Boulier[†], Daniel Lazard, François Ollivier and Michel Petitot

Université Lille I, LIFL, 59655 Villeneuve d'Ascq CEDEX, France
Université Paris VI, LIP6, 75252 Paris CEDEX 05, France
École Polytechnique, GAGE, 91128 Palaiseau CEDEX, France
Université Lille I, LIFL, 59655 Villeneuve d'Ascq CEDEX, France

boulier@lifl.fr, lazard@posso.lip6.fr, ollivier@gage.polytechnique.fr, petitot@lifl.fr

Technical report IT306 of the LIFL. Unpublished.

(Received July 1997 (revised February 1999))

This paper deals with systems of polynomial differential equations, ordinary or with partial derivatives. The embedding theory is the differential algebra of Ritt and Kolchin. We describe an algorithm, named Rosenfeld–Gröbner, which computes a representation for the radical $\mathfrak{p}$ of the differential ideal generated by any such system Σ. The computed representation constitutes a normal simplifier for the equivalence relation modulo $\mathfrak{p}$ (it permits to test membership in $\mathfrak{p}$). It permits also to compute Taylor expansions of solutions of Σ. The algorithm is implemented within a package[†] in MAPLE V.

Introduction

The following system Σ (which has no physical significance) is a system of three polynomial differential equations with partial derivatives.

$$\Sigma \begin{cases} \left(\dfrac{\partial}{\partial x}\, u(x,y)\right)^2 - 4\, u(x,y) = 0, \\ \left(\dfrac{\partial^2}{\partial x\, \partial y}\, u(x,y)\right)\left(\dfrac{\partial}{\partial y}\, v(x,y)\right) - u(x,y) + 1 = 0, \\ \dfrac{\partial^2}{\partial x^2}\, v(x,y) - \dfrac{\partial}{\partial x}\, u(x,y) = 0. \end{cases}$$

In the following, we denote (for short) derivations using indices. The system Σ becomes

$$\Sigma \begin{cases} u_x^2 - 4\, u = 0, \\ u_{xy}\, v_y - u + 1 = 0, \\ v_{xx} - u_x = 0. \end{cases}$$

[†] A part of this work (in particular the MAPLE package) was realized while the first author was a postdoctoral fellow at the Symbolic Computation Group of the University of Waterloo, N2L 3G6 Ontario, Canada.

[†] The package is available for MAPLE VR3 and R4. It is going to enter the main library of MAPLE VR5.

0747–7171/90/000000 + 00 $03.00/0

The Rosenfeld–Gröbner algorithm that we present in this paper computes a representation of the radical $\mathfrak{p}$ of the differential ideal[‡] generated by Σ. This representation tells us in particular that the solutions of Σ (which turn out to be polynomials) depend on three arbitrary constants and permits us to compute Taylor expansions of these solutions. If we expand them in the neighborhood of the origin then the arbitrary constants are $u(0,0)$, $v(0,0)$ and $v_x(0,0)$. For $u(0,0) = 5$, $v(0,0) = 421$ and $v_x(0,0) = \pi$ our algorithm gives us (computations are detailed in section 8)

$$u(x,\, y) = 5 + x\,\sqrt{10}\,\sqrt{2} + y\,\sqrt{10} + x^2 + x\,y\,\sqrt{2} + \frac{1}{2}\,y^2,$$

$$v(x,\, y) = 421 + x\,\pi + 2\,y\,\sqrt{2} + \frac{1}{2}\,x^2\,\sqrt{10}\,\sqrt{2} + x\,y\,\sqrt{10} + \frac{1}{4}\,y^2\,\sqrt{10}\,\sqrt{2} + \frac{1}{3}\,x^3 + \frac{1}{2}\,x^2\,y\,\sqrt{2} + \frac{1}{2}\,x\,y^2 + \frac{1}{12}\,y^3\,\sqrt{2}.$$

The applied mathematical theory is called *differential algebra*. It was initiated mostly by French and American researchers at the early twentieth century (Riquier (1910), Janet (1920) and (1929) and Ritt (1932)) and really developed by the American teams of Ritt (1950) and Kolchin (1973). Differential algebra aims at studying differential equations from a purely algebraic point of view. It is much closer to ordinary commutative algebra than to analysis.

The Rosenfeld–Gröbner algorithm represents the radical of the differential ideal generated by any finite system Σ of polynomial differential equations as a finite intersection of differential ideals $\mathfrak{r}$'s (that we call *regular*).

$$\mathfrak{p} = \sqrt{[\Sigma]} = \mathfrak{r}_1 \cap \cdots \cap \mathfrak{r}_n.$$

Each regular differential ideal $\mathfrak{r}_i$ is presented by a set of differential polynomial equations C_i which satisfies:

1 C_i is a canonical representative of $\mathfrak{r}_i$,
2 C_i reduces to zero a differential polynomial p if and only if $p \in \mathfrak{r}_i$.

Therefore, the set of the C's constitutes a normal simplifier for the equivalence relation modulo $\mathfrak{p}$ (i.e. an algorithm which decides membership in $\mathfrak{p}$). The simplifier is not canonical for the representation may contain redundant components: every differential prime ideal which is minimal over $\mathfrak{p}$ is minimal over at least one of the regular differential ideals produced but the converse is not true.

Assume the solutions of $\mathfrak{p}$ depend on finitely many arbitrary constants. The algorithm separates the solutions which do not depend on the same number of arbitrary constants. In our introductory example, only one regular differential ideal was produced. This proves that all the solutions of $\mathfrak{p}$ depend on three arbitrary constants.

An implementation of this algorithm was realized for the MAPLE V computer algebra software. It is embedded in a package named `diffalg`.

‡ We make precise in further sections some of the notations and the terminology used in this introduction

Used theorems

The Rosenfeld–Gröbner algorithm relies mainly on three theorems:

1 a theorem of zeros (Hilbert's Nullstellensatz), which states that a polynomial p belongs to the radical of an ideal presented by a basis Σ if and only if every solution of Σ is a solution of p ; we apply this theorem in the algebraic and in the differential case,

2 a lemma of Rosenfeld, which gives a sufficient condition so that a system of polynomial differential equations admits a solution if and only if this same system, considered as a purely algebraic system admits a solution,

3 a lemma of Lazard, which establishes that each regular ideal $\mathfrak{r}$ is radical and that all its prime components have a same parametric set (this property is stronger than "defining an unmixed algebraic variety").

It utilizes only the operations and the equality test with zero in the base field of the equations: we refer to Ritt's reduction algorithms, computations of Gröbner bases and splittings similar to those in the elimination methods of Seidenberg (1956). In particular, it does not need any factorization.

New results

The Rosenfeld–Gröbner algorithm was first described by Boulier (1994) and improved by Boulier *et al.* (1995). This paper contains new results.

We give in section 2 a proof of Lazard's lemma which is more precise than the one we gave in Boulier *et al.* (1995), lemma 2, page 161.

We give an original presentation of the fundamental Rosenfeld's lemma. We present it as a property of some class of systems of polynomial differential equations and inequations instead of a property of some class of sets of differential polynomials.

We give a version of Rosenfeld's lemma more general than the one of Rosenfeld (this was already proven by Boulier (1997)) and not contained in Kolchin's version. Briefly, our version only imposes to the ideals to be saturated by the separants of the differential polynomials (and no more by the initials). It also only imposes to the set of equations to be triangular instead of autoreduced (but this is anecdotic). Since Lazard's lemma also holds in such a situation, we formulate our theorems without considering the initials of differential polynomials (though we do it in our implementation for efficiency reasons). This is an improvement w.r.t. Kolchin's theory.

We prove new results for regular ideals: theorems 4.2 and 6.1. The former permits to compute the minimal differential prime components of regular ideals and provides also informations about these prime ideals without having to compute them ; the latter gives us an original presentation of a well known proof about formal power series.

The algorithm presented is much more efficient than the one of 1995. It applies for polynomial differential equations an analogue of the second criterion proven by Buchberger (1979) for Gröbner bases. Our implementation of this criterion was designed after the method of Gebauer and Möller (1988).

Comparison with other methods

There is a strong relationship between our algorithm and Seidenberg's work. Anton Seidenberg (1956) designed elimination algorithms for systems of ODE and PDE in characteristic zero and non zero. His PDE elimination algorithm in characteristic zero actually solves the same problem we are solving: deciding membership in the radical of a finitely generated differential ideal. He proved (theorem 6, page 51) an analogue of Rosenfeld's lemma which is a bit weaker (restriction to orderly rankings on the derivatives of a single differential indeterminate) and more technical (note Rosenfeld (1959) presents his lemma as a new version of Seidenberg's theorem). In his theorem 11, page 59 he shows that, if Σ is a system which satisfies the hypotheses of his theorem 6 then every algebraic solution of Σ furnishes a unique differential solution. He showed later (Seidenberg, 1969) how differential solutions can be converted as formal power series.

There are differences between Seidenberg's algorithm and ours. The most important is the following: the Rosenfeld–Gröbner algorithm computes a representation of radical differential ideals which can be used afterwards for testing membership in the ideal many times afterwards while Seidenberg's decides if a differential polynomial p belongs to the radical of the differential ideal generated by a finite family Σ by eliminating successively all the differential indeterminates which occur in the system $\Sigma = 0,\ p \neq 0$ in order to test if this system admits solutions (Hilbert's theorem of zeros). The answer of his algorithm is a boolean.

Another important difference: Seidenberg's elimination algorithms are restricted to elimination rankings between differential indeterminates which induce very explosive computations, while orderly rankings are handled by the Rosenfeld–Gröbner algorithm (this is the case for instance in our introductory example).

Ritt (1950) gave a method to decompose the radical of an ordinary differential ideal as an intersection of prime differential ideals, providing a characteristic set for each of these ideals. This decomposition is not the minimal one because of the redundancy problem (still open). That algorithm is inconvenient because it is only partially effective: it proceeds by factorization over a tower of algebraic field extensions of the field of coefficients. To our knowledge, it has not been implemented. It only applies for ODE.

Wu Wen Tsün (1987) designed a variant of Ritt's algorithm for ordinary differential equations, with a notion of characteristic set weaker than Ritt's (e.g. a characteristic set in the sense of Wu may have no solution). Other authors (e.g. Wang (1994)) developed later Wu's and Seidenberg's ideas. These algorithms only apply for ODE.

Ollivier (1990) and Carra-Ferro (1987) have independently tried to generalize Gröbner bases to systems of ordinary polynomial differential equations. These differential Gröbner bases are in general infinite, even for ODE systems.

Another definition of differential Gröbner bases was attempted by Mansfield (1991). The algorithm DIFFGBASIS, implemented in MAPLE, utilizes Ritt's algorithm of reduction and then always terminates. It handles PDE systems. In general however, it cannot guarantee its output to be a differential Gröbner basis. Note that the membership problem in an arbitrary differential ideal is undecidable (Gallo *et al.*, 1991), and the membership problem of a finitely generated differential ideal is still open.

Bouziane *et al.* (1996) and Maârouf (1996) designed recently a variant of the Rosenfeld–Gröbner algorithm. They started from the algorithm of Kalkbrener (1993) which compute decompositions of radicals of ideals in non differential polynomial algebras. They describe

a method for computing characteristic sets of prime differential ideals different from our methods given in Ollivier (1990), Boulier (1994) and Boulier *et al.* (1995), section 5, page 164.

Reid *et al.* (1994) and Reid *et al.* (1996) developed algorithms for studying systems of PDE and computing Taylor expansions of their solutions. These methods are based more on differential geometry than on algebra. They do not claim to be as general as the Rosenfeld–Gröbner algorithm.

Organization of the paper

Sections 1 and 2 deal with commutative algebra. The former contains preliminaries; in the latter, we prove Lazard's lemma and show how some computations can be performed in dimension zero. Section 3 contains differential algebra preliminaries. In section 4 we prove our version of Rosenfeld's lemma and some technical results which will be used for efficiently testing the coherence hypothesis of this lemma (in particular, we show there our analogue of Buchberger's second criterion). Section 5 shows how to represents radical differential ideals as intersections of regular differential ideals. This is the core of the Rosenfeld–Gröbner algorithm. In the next section, we show how to compute canonical representatives for regular differential ideals and we state the Rosenfeld–Gröbner algorithm as a theorem (theorem 6.4) with an effective proof. The algorithm is obtained by translating the proof in any programming language. In section 7 we explain how algebraic solutions of regular differential ideals can be expanded as formal power series. A few examples are developed in the last section.

1. Commutative algebra preliminaries

Let $R = K[X]$ be a polynomial ring where K is a field and X is an alphabet (possibly infinite) endowed with an ordering $\mathcal{R}$. Let $p \in R \setminus K$ be a polynomial. The *leader* of p is the greatest indeterminate $x \in X$ w.r.t. $\mathcal{R}$ which appears in p. It is denoted $\mathrm{ld}\, p$. Let $d = \deg(p, x)$ be the degree of p in x. The *initial* i_p of p is the coefficient of x^d in p. The *separant* s_p of p is the polynomial $\partial p/\partial x$. The *rank* of p is the monomial x^d. It is denoted $\mathrm{rank}\, p$. The rank of a set of polynomials is the set of ranks of the elements of the set.

If $A \subset R \setminus K$ is a set of polynomials then I_A (respectively S_A) denotes the set of the initials (respectively separants) of the elements of A and $H_A = I_A \cup S_A$.

If p and q are two polynomials with ranks x^d and y^e then $q < p$ if $y < x$ or $y = x$ and $e < d$.

Let $A = \{p_1, \ldots, p_n\}$ and $A' = \{p'_1, \ldots, p'_{n'}\}$ be two nonempty subsets of $R \setminus K$. Renaming the polynomials if needed, assume $\mathrm{rank}\, p_i \leq \mathrm{rank}\, p_{i+1}$ and $\mathrm{rank}\, p'_j \leq \mathrm{rank}\, p'_{j+1}$ for all $i < n$, $j < n'$. The set A is said to be *less than* A' if there exists some $i \leq \min(n, n')$ such that $p_i < p'_i$ and $\mathrm{rank}\, p_j = \mathrm{rank}\, p'_j$ for $1 \leq j < i$ else if $n > n'$ and $\mathrm{rank}\, p_j = \mathrm{rank}\, p'_j$ for $1 \leq j \leq n'$. Two sets of polynomials such that none of them is less than the other one are said to have the same rank.

A subset A of $R \setminus K$ is said to be *triangular* if the leaders of its elements are pairwise different.

If $A \subset R$ then (A) denotes the smallest ideal of R containing A. If $\mathfrak{a}$ is an ideal of R then the *radical* $\sqrt{\mathfrak{a}}$ of $\mathfrak{a}$ is the ideal of all the elements of R, a power of which lies in $\mathfrak{a}$. An ideal equal to its radical is said to be radical. Any radical ideal $\mathfrak{r}$ of a polynomial

ring $R = K[X]$ (X finite) is a finite intersection of prime ideals which is unique when minimal.

A component (say $\mathfrak{p}_1$) of an intersection $\mathfrak{r} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ is said to be *redundant* w.r.t. $\mathfrak{r}$ if $\mathfrak{r} = \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_n$. An element p of a ring R is said to be a *divisor of zero* if $p \neq 0$ and there exists in R an element $q \neq 0$ such that the product $p\,q = 0$.

If $\mathfrak{r}$ is an ideal and S is a finite subset of a ring R then the *saturation* $\mathfrak{r} : S^\infty$ of $\mathfrak{r}$ by S is the ideal of all the polynomials $p \in R$ such that there exists a power product h of elements of S such that $h\,p \in \mathfrak{r}$.

1.1. Gröbner bases

In this section $R = K[X]$ denotes a polynomial ring over a field. We only recall some properties of Gröbner bases. The books of Cox *et al.* (1992) and Becker and Weispfenning (1991) provide a real presentation.

If B is a Gröbner basis of an ideal $\mathfrak{r}$ of a polynomial ring $R = K[X]$ for an ordering $\mathcal{R}$. The reduction by B, denoted $\xrightarrow[B]{*}$ preserves the equivalence relation mod $\mathfrak{r}$ and we have

1 $\mathfrak{r} = (B)$,
2 when it is *reduced*, a Gröbner basis is a canonical representative of $\mathfrak{r}$ (it only depends on the ideal and on the ordering),
3 the ideal $\mathfrak{r}$ is equal to R if and only if $1 \in B$ (Becker and Weispfenning, 1991, corollary 6.16, page 257),
4 given any $p \in R$, there exists a unique polynomial $\bar{p}$ irreducible by B such that $p \xrightarrow[B]{*} \bar{p}$. This polynomial is a canonical representative of the residue class of p modulo $\mathfrak{r}$ (it only depends on the ideal and the ordering). In particular, if $p \in \mathfrak{r}$ then $\bar{p} = 0$,

Even if X is infinite, one can compute Gröbner bases of finitely generated ideals of $K[X]$. This remark is important since we are going to compute Gröbner bases of (non differential) ideals in differential polynomial rings. The theoretical justification is given by the following lemma.

Lemma 1.1. *Let $\mathfrak{r}$ be an ideal of a ring R and x be transcendental over R. If ϕ denotes the canonical ring homomorphism $\phi : R \to R[x]$ then $\phi^{-1}(\phi\mathfrak{r}) = \mathfrak{r}$.*

Let $A = \{p_1, \ldots, p_n\}$ and $S = \{s_1, \ldots, s_m\}$ be finite sets of polynomials of R. Let $\{z_1, \ldots, z_m\}$ be a finite set of indeterminates over R. One gets a Gröbner basis B_0 of the ideal $S^{-1}(A)$ of $S^{-1}R$ by computing a Gröbner basis of the set

$$\{p_1, \ldots, p_n, s_1\,z_1 - 1, \ldots, s_m\,z_m - 1\}$$

for any ordering (Eisenbud, 1995, exercise 2.2, page 79). Each z_i stands for $1/s_i$. To get a Gröbner basis B_1 of $(A) : S^\infty$, compute first B_0 for any ordering which eliminates the z's. Then $B_1 = B_0 \cap R$ (Becker and Weispfenning, 1991, proposition 6.15, page 257).

2. Lazard's lemma

Lazard's lemma (theorem 2.1) is a result of commutative algebra, interesting in itself. It was first published in (Boulier *et al.*, 1995, lemma 2, page 161) with a proof relying on

basic arguments. During the *Special Year in Differential Algebra and Algebraic Geometry* organized in 1995 at the City College of New York by Prof. Hoobler and Sit, a weakness in the proof was pointed out[†]: there was a claim which was true but not proven. Morrison (1995) proved then a generalized version of the lemma which is presented in Morrison (1997). Another proof was written later by Schicho and Li (1995). The one we give here only relies on elementary commutative algebra (say van der Waerden (1966), chapter 15). In this sense, it is simpler than the other ones. The knowledge of Morrison's proof helped us to fix ours. Section 2.2 contains the argument (Ollivier, 1998) missing in (Boulier *et al.*, 1995).

DEFINITION 2.1. *(regular algebraic systems)*
A system $A = 0,\ S \neq 0$ of a polynomial ring R is said to be a regular algebraic system *(for an ordering $\mathcal{R}$) if*

1 A is triangular,
2 S contains the separants of the elements of A.

The ideal $(A) : S^\infty$ is called the regular algebraic ideal *defined by the system. The system is said to be* inconsistent *if $(A) : S^\infty = R$. It is said to be* consistent *otherwise.*

THEOREM 2.1. *(Lazard's lemma)*
Let $A = 0,\ S \neq 0$ be a consistent regular algebraic system of a polynomial ring $R = K[X]$. Denote L the set of the leaders of the elements of A and $N = X \setminus L$. Then

1 the regular algebraic ideal $(A) : S^\infty$ is radical,
2 if $\mathfrak{p}$ is a prime ideal minimal over $(A) : S^\infty$ then $\dim \mathfrak{p} = |N|$ and $\mathfrak{p} \cap K[N] = (0)$.

PROOF. Notice it is enough to prove the theorem in the case $S = S_A$ for, if $(A) : S_A^\infty$ is radical, the ideal $(A) : S^\infty$ is the intersection of the prime ideals which are minimal over $(A) : S_A^\infty$ and which do not meet S (van der Waerden, 1966, section 15.6).

Propositions 2.2 and 2.3 imply that if $\mathfrak{p}$ is an associated prime of $(A) : S_A^\infty$ then $\dim \mathfrak{p} = |N|$ and $\mathfrak{p} \cap K[N] = (0)$. This proves the point 2.

The nonzero elements of $K[N]$ are thus different from zero and do not divide zero in $R/(A) : S_A^\infty$. The elements of S_A are not zero and do not divide zero either in $R/(A) : S_A^\infty$. We have thus the ring isomorphism[†]

$$\mathbf{Fr}(R/(A) : S_A^\infty) \simeq \mathbf{Fr}(S_{\bar{A}}^{-1}\bar{R}/S_{\bar{A}}^{-1}(\bar{A}))$$

where $\bar{R} = K(N)[L]$ and $\bar{A}$ denotes the image of A by the canonical ring homorphism $R \to \bar{R}$. A product of fields is isomorphic to its total ring of fractions thus the ring $\mathbf{Fr}(R/(A) : S_A^\infty)$ is isomorphic to a product of fields by proposition 2.1. According to the axioms of products, $\mathbf{Fr}(R/(A) : S_A^\infty)$ contains no nilpotent[‡] element thus $R/(A) : S_A^\infty$ does not either whence $(A) : S_A^\infty$ is radical. □

[†] The first author would like to thank Prof. Hoobler, Sit and in particular Prof. Sally Morrison for many fruitful comments and email communications.

[†] If R is a ring then $\mathbf{Fr}(R)$ denotes the total ring of fractions of R, obtained by making invertible all the non divisors of zero of R.

[‡] An element g of a ring R is said to be nilpotent if $g \neq 0$ and $g^n = 0$ for some $n \in \mathbb{N}$.

In the sequel, we consider the ideal $(A) : S_A^\infty$. We denote L the set of leaders of the triangular set A and N the remaining indeterminates. Thus $(A) : S_A^\infty \subset R = K[N, L]$. We assume $(A) : S_A^\infty \neq R$.

2.1. Lazard's lemma in dimension zero

In this section we consider the case $|N| = 0$.

We denote $S_A^{-1}R$ the ring localized at S_A and $S_A^{-1}(A)$ the ideal generated by the image of (A) in $S_A^{-1}R$ (van der Waerden, 1966, section 15.9) or (Eisenbud, 1995, section 2).

Lemma 2.1. *Let $K[x]$ be a polynomial ring in one indeterminate over a field. Let $p \in K[x]$ be a polynomial and s be its separant. The ideal $s^{-1}K[x]/s^{-1}(p)$ is isomorphic to a product of algebraic field extensions of K.*

Proof. The ideal $s^{-1}(p)$ is generated by the product of the irreducible simple factors of p. These factors generate comaximal ideals in $K[x]$. The lemma comes from the Chinese remainders theorem (Eisenbud, 1995, section 2, exercise page 79). □

Lemma 2.2. *If R_0 is a ring isomorphic to a product of algebraic field extensions of K and x is a new inderminate, $p \in R_0[x]$ is a polynomial and $s = \partial p/\partial x$ is its separant then $s^{-1}R_0[x]/s^{-1}(p)$ is isomorphic to a product of algebraic field extensions of K.*

Proof. Let $R_0 \simeq K_1 \times \cdots \times K_h$. We have $R_0[x] \simeq K_1[x] \times \cdots \times K_h[x]$. Denote π_i the canonical ring homomorphism $R_0[x] \to K_i[x]$ $(1 \leq i \leq h)$. We have

$$s^{-1}R_0[x]/s^{-1}(p) \simeq \prod_{i=1}^{h} (\pi_i s)^{-1} K_i[x]/(\pi_i s)^{-1}(\pi_i p).$$

Since $\pi_i s = \partial \pi_i p/\partial x$ $(1 \leq i \leq h)$, lemma 2.1 applies: each $(\pi_i s)^{-1}K_i[x]/(\pi_i s)^{-1}(\pi_i p)$ is isomorphic to a product of algebraic field extensions of K thus so is $s^{-1}R_0[x]/s^{-1}(p)$. □

Proposition 2.1. *The ring $S_A^{-1}R/S_A^{-1}(A)$ is isomorphic to a product of algebraic field extensions of K.*

Proof. Apply lemma 2.2 inductively on $|A|$. □

2.2. Non leaders form a parametric set

If $\mathfrak{i}$ and $\mathfrak{j}$ are two ideals of R then the *quotient* $\mathfrak{i} : \mathfrak{j}$ of $\mathfrak{i}$ by $\mathfrak{j}$ (van der Waerden, 1966, section 15.2) is defined by $\mathfrak{i} : \mathfrak{j} = \{p \in R \mid \forall q \in \mathfrak{j},\ p\,q \in \mathfrak{i}\}$

Lemma 2.3. *Denote $\mathfrak{i} = (A) : S_A^\infty$. If $h \in R$ then for every $q \in \mathfrak{i} : (h)$ we have*

$$\forall x \in L,\ \frac{\partial q}{\partial x} = 0 \quad \Rightarrow \quad \forall x \in N,\ \frac{\partial q}{\partial x} \in \mathfrak{i} : (h).$$

Proof. Denote D the determinant of the jacobian matrix J of A, which is the product of the elements of S_A since A is triangular.

$$J = \left(\frac{\partial p}{\partial x}\right)_{p \in A,\, x \in L}$$

Assume $q \in \mathfrak{i} : (h)$. Then there exists some $\alpha \geq 0$ and some $m_p \in R$ $(p \in A)$ such that

$$D^\alpha \, h \, q \quad = \quad \sum_{p \in A} m_p \, p.$$

Assume $x \in L$. Differentiating w.r.t. x, multiplying by D and h and applying the fact that $\partial q / \partial x = 0$ we conclude

$$D \, h \sum_{p \in A} m_p \, \frac{\partial p}{\partial x} \quad \in \quad (A).$$

Denote $\tilde{J}$ the cofactors matrix of J and I the identity matrix. Using the fact that $J \, \tilde{J} = D \, I$ we find that $D^2 \, h \, m_p \in (A)$ for each $p \in A$ which implies $m_p \in \mathfrak{i} : (h)$ for each $p \in A$ whence $\partial q / \partial x \in \mathfrak{i} : (h)$ for any $x \in N$. □

COROLLARY 2.1. *Denote* $\mathfrak{i} = (A) : S_A^\infty$. *If* $h \in R$ *is a polynomial such that* $\mathfrak{i} : (h) \neq R$ *then* $\mathfrak{i} : (h) \cap K[N] = (0)$.

PROOF. If $q \in \mathfrak{i} : (h) \cap K[N]$ then for any $x \in L$ we have $\partial q / \partial x = 0$. Using lemma 2.3 we see $\mathfrak{i} : (h) \cap K[N]$ is stable under the action of the partial derivations w.r.t. all the indeterminates. This ideal is therefore either equal to $K[N]$ (in which case $\mathfrak{i} : (h) = R$) or to (0). □

PROPOSITION 2.2. *If* $\mathfrak{q}$ *is an isolated primary component of* $(A) : S_A^\infty$ *then* $\dim \mathfrak{q} = |N|$ *and* $\mathfrak{q} \cap K[N] = (0)$.

PROOF. Let $h \in R$ be a polynomial belonging to all the associated primes of $\mathfrak{i} = (A) : S_A^\infty$ but not to the associated prime of $\mathfrak{q}$. This polynomial exists for $\mathfrak{q}$ is isolated (van der Waerden, 1966, section 15.6). For $\beta \geq 0$ great enough, h^β belongs to all the primary components of $\mathfrak{i}$ but not to $\mathfrak{q}$ and we have $\mathfrak{i} : (h^\beta) = \mathfrak{q}$. Corollary 2.1 implies $\mathfrak{q} \cap K[N] = (0)$ whence $\dim \mathfrak{q} \geq |N|$.

Now, denote $\bar{R} = K(N)[L]$ and denote $\bar{A}$ the image of A by the canonical ring homorphism $\phi : R \to \bar{R}$. If $\mathfrak{p}$ is a prime ideal minimal over $\mathfrak{i}$ then $\bar{\mathfrak{p}} = (\phi \mathfrak{p})$ is minimal over the ideal $\mathfrak{j} = (\bar{A}) : S_{\bar{A}}^\infty$ (van der Waerden, 1966, section 15.9). The proposition 2.1 implies that $\dim \bar{\mathfrak{p}} = 0$ whence $\dim \mathfrak{p} = |N|$. □

PROPOSITION 2.3. *If* $\mathfrak{q}$ *is a primary component of* $(A) : S_A^\infty$ *then* $\mathfrak{q}$ *is isolated.*

PROOF. Assume $\mathfrak{i} = (A) : S_A^\infty$ admits an imbedded primary component $\mathfrak{q}$. By proposition 2.2 we have $\dim \mathfrak{q} < |N|$ whence $\mathfrak{q} \cap K[N] \neq (0)$. There exists some polynomial h (taken in all the isolated components of $\mathfrak{i}$ but not in $\mathfrak{q}$) such that $\mathfrak{i} : (h) \neq R$. Since $\mathfrak{i} : (h)$ contains an intersection of imbedded primary components of $\mathfrak{i}$ we have $\mathfrak{i} : (h) \cap K[N] \neq (0)$. This contradicts corollary 2.1. □

DEFINITION 2.2. *(associated Gröbner basis)*

Let $A = 0$, $S \neq 0$ *be a consistent regular algebraic system of a ring* $R = K[X]$. *Denote* L *the set of the leaders of the elements of* A *and* $N = X \setminus L$. *The reduced Gröbner basis of the ideal* $(A) : S^\infty$, *computed in the ring* $K(N)[L]$ *for the elimination ordering given by the ordering over* X *is called the* Gröbner basis associated to $A = 0$, $S \neq 0$.

COROLLARY 2.2. *If $A = 0,\ S \neq 0$ is a consistent regular algebraic system of a polynomial ring $R = K[X]$ and $x_i \in X$ is an indeterminate then the following conditions are equivalent*

1 *x_i is the leader of some element of A,*
2 *x_i is the leader of some element of the Gröbner basis associated to $A = 0,\ S \neq 0$,*
3 *x_i is the leader of a characteristic set (for the ordering defined over X) of any prime ideal minimal over $(A) : S^\infty$.*

2.3. COMPUTING IN DIMENSION ZERO

Let $A = 0,\ S \neq 0$ be a regular algebraic system of a polynomial ring $R_0 = K[X]$ for an ordering $\mathcal{R}$. Let $L \subset X$ be the set of the leaders of the elements of A and $N = X \setminus L$. Denote $\mathfrak{r}_0 = (A) : S^\infty$ and B_0 the reduced Gröbner basis of $\mathfrak{r}_0$ w.r.t. the elimination ordering given by $\mathcal{R}$.

Let $R_1 = K(N)[L]$ be the polynomial ring obtained by extending the ground field K with N and φ the canonical ring homomorphism $R_0 \longrightarrow R_1$. Denote $\mathfrak{r}_1 = (\varphi A) : (\varphi S)^\infty$ and B_1 the Gröbner basis associated to $A = 0,\ S \neq 0$. The basis B_1 is a Gröbner basis of $\mathfrak{r}_1$.

Because of theorem 2.1 the ring homomorphism $R_0/\mathfrak{r}_0 \longrightarrow R_1/\mathfrak{r}_1$ is injective and there is a one–to–one correspondence between the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ which are minimal over $\mathfrak{r}_0$ and the prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ which are minimal of $\mathfrak{r}_1$. The $\mathfrak{q}$'s are dimension zero ideals thus so is $\mathfrak{r}_1$.

Therefore, though B_1 is not a Gröbner basis of $\mathfrak{r}_0$, many computations can be performed using the latter since

1 for any $p \in R_0$ we have $p \in \mathfrak{r}_0$ if and only if $\varphi p \xrightarrow[B_1]{*} 0$,
2 a polynomial $p \in R_0$ is a divisor of zero modulo $\mathfrak{r}_0$ if and only if φp is a divisor of zero modulo $\mathfrak{r}_1$,
3 minimal triangular subsets of B_0 have the same rank as minimal triangular subsets of B_1.

The basis B_1 turns out to be much smaller and faster to compute than B_0. It is sometimes faster to compute Gröbner bases of regular algebraic ideals in dimension zero in MAPLE than to compute the Gröbner bases in dimension $d > 0$ using the GB software of Faugère (which runs usually one thousand times faster than the MAPLE's implementation of the Buchberger's algorithm).

3. Differential algebra preliminaries

The reference book is the one of Kolchin (1973), chapters I–IV. Readers who discover the theory had probably better however to start with the book of Ritt (1950).

A differential ring is a ring endowed with finitely many derivations $\delta_1, \ldots, \delta_m$ which commute pairwise. Derivation operators are denoted multiplicatively $\theta = \delta_1^{a_1} \cdots \delta_m^{a_m}$ where the a's are nonnegative integers. The sum of the exponents a's is the *order* of θ, denoted $\operatorname{ord}\theta$. The identity operator has order 0. All other operators are said to be *proper*. If $\theta = \delta_1^{a_1} \cdots \delta_m^{a_m}$ and $\phi = \delta_1^{b_1} \cdots \delta_m^{b_m}$ then $\theta\phi = \delta_1^{a_1+b_1} \cdots \delta_m^{a_m+b_m}$. If $a_i \geq b_i$

for $i = 1, \ldots, m$ then $(\theta/\phi) = \delta_1^{a_1-b_1} \cdots \delta_m^{a_m-b_m}$. The monoid of derivation operators is denoted Θ.

If R is a differential ring and $S \subset R$ then ΘS denotes the smallest subset of R containing S and stable under derivation. If $R_0 \subset R_1$ are two differential rings and $S \subset R_1$ then $R_0\{S\}$ denotes the smallest differential ring containing R_0 and S i.e. $R_0[\Theta S]$.

We deal with a differential polynomial ring $R = K\{u_1, \ldots, u_n\}$ where K is a differential field of characteristic zero. The u's are called *differential indeterminates* and the θu's are called *derivatives*. The set of the derivatives is denoted ΘU.

The differential ring R can be viewed as a non differential polynomial ring $K[\Theta U]$ whose indeterminates are the derivatives of R. The definitions given for non differential polynomial rings hold therefore for differential ones.

If θu and ϕu are derivatives of some same differential indeterminate u, we denote $\operatorname{lcd}(\theta u, \phi u)$ the *least common derivative* between θu and ϕu. It is equal to $\operatorname{lcm}(\theta, \phi)u$.

A *ranking* $\mathcal{R}$ is an ordering over ΘU compatible with the action of the derivations over ΘU (Kolchin, 1973, page 75):

1 $\delta v > v$ (for all derivation δ and $v \in \Theta U$),
2 $v > w \Rightarrow \delta v > \delta w$ (for all derivation δ and $v, w \in \Theta U$).

Rankings such that $\operatorname{ord}\theta > \operatorname{ord}\phi \Rightarrow \theta v > \phi w$ (for all derivations operators θ, ϕ and all differential indeterminates v, w) are said to be *orderly*. Rankings such that $v > w \Rightarrow \theta v > \phi w$ (for all derivations operators θ, ϕ and all differential indeterminates v, w) are said to be *elimination* rankings. Any ranking is a well–ordering (Kolchin, 1973, page 75).

Properties of rankings imply that the separant of a differential polynomial $p \in R \setminus K$ is also the initial of all the proper derivatives of p.

If $A \subset R \setminus K$ is a set of differential polynomials and v is any derivative then A_v denotes the set of the derivatives of the elements of A whose leaders are less than or equal to v:

$$A_v = \{\theta p \mid p \in A,\ \theta \in \Theta \text{ and } \operatorname{ld}\theta p \leq v\}.$$

According to this notation, R_v denotes the ring of the differential polynomials whose leaders are less than or equal to v. Therefore

$$A \cap R_v = \{p \in A \mid \operatorname{ld} p \leq v\}.$$

Let $p \in R \setminus K$ and $q \in R$ be differential polynomials. Denote $\operatorname{rank} p = v^d$. The differential polynomial q is said to be *partially reduced* w.r.t. p if no proper derivative of v appears in q; it is said to be *reduced* w.r.t. p if q is partially reduced w.r.t. p and $\deg(q, v) < d$.

A set $A \subset R \setminus K$ is said to be *autoreduced* if any element of A is reduced w.r.t. any other element of the set.

DEFINITION 3.1. *A set $A \subset R \setminus K$ is said to be* differentially triangular *if it is triangular and if its elements are pairwise partially reduced.*

Every autoreduced set is finite (Kolchin, 1973, page 77). The proof holds also for differentially triangular sets. A *characteristic set* of a set† $S \subset R$ is an autoreduced

† This definition corresponds to Ritt's one (Ritt, 1950, I, 5, page 5) and coincides with Kolchin's when S is a differential ideal. Kolchin only defined characteristic sets for ideals (Kolchin, 1973, I 10, page 81 and III, 2, page 124).

subset of S which has lowest rank among the autoreduced subsets of S. It is also a minimal (according to our definition) element in the set of the autoreduced subsets of S. If $S \subset R$ admits autoreduced subsets then S admits a characteristic set.

A *differential ideal* of a differential ring R is an ideal of R stable under derivation. If $A \subset R$ then $[A] = (\Theta A)$ denotes the smallest differential ideal of R containing A. Since R has characteristic zero, the radical of a differential ideal is a differential ideal. Any radical differential ideal $\mathfrak{r}$ of a differential polynomial ring R is a finite intersection of differential prime ideals which is unique when minimal (Kolchin, 1973, III, Theorem 1, page 126) or (Ritt, 1950, I, Theorem, page 10). The following is a differential analogue of Hilbert's theorem of zeros (Seidenberg, 1952, Nullstellensatz, weak form) or (Kolchin, 1973, chapter IV, section 2).

THEOREM 3.1. *(theorem of zeros)*
Let $R = K\{U\}$ be a differential polynomial ring over a differential field of characteristic zero and $\mathfrak{r}$ be a differential ideal of R. A differential polynomial p vanishes on every solution of $\mathfrak{r}$, in any differential field extension of K, if and only if $p \in \sqrt{\mathfrak{r}}$.

PROOF. The implication from right to left is immediate. The implication from left to right: if $p \notin \sqrt{\mathfrak{r}}$ then p does not belong to at least one differential prime ideal $\mathfrak{p}$ minimal over $\sqrt{\mathfrak{r}}$. The canonical ring homorphism which maps R to the field of fractions of $R/\mathfrak{p}$ furnishes a solution of $\mathfrak{r}$ which is not a solution of p. □

COROLLARY 3.1. *A differential polynomial p vanishes on every solution of a system of polynomial differential equations and inequations $A = 0,\ S \neq 0$ iff $p \in \sqrt{[A] : S^\infty}$.*

PROOF. Using the definitions of the radical and of the saturation of an ideal, we see that $p \in \sqrt{[A] : S^\infty}$ if and only if there exists a product h of elements of S such that $hp \in \sqrt{[A]}$. According to the theorem of zeros, $hp \in \sqrt{[A]}$ if and only if hp vanishes on every solution of the system $A = 0$ i.e. if and only if p vanishes on every solution of the system $A = 0,\ S \neq 0$. □

The following technical lemma is classical. See Ritt (1950), page 30 for instance. We are going to use it many times.

LEMMA 3.1. *Let A be a finite subset of some differential polynomial ring R. Let $q = s\,v + r$ be a differential polynomial with leader v, such that* $\deg(q, v) = 1$ *and v does not appear in s, r nor any element of A. For any $p \in R$, if $p \in (A, q)$ and v does not appear in p then $p \in (A) : s^\infty$.*

PROOF. Since $p \in (A, q)$ there exists a formula (f) such that

$$p = \underbrace{\sum_{p_i \in A} B_i\, p_i + C\, q}_{(f)}$$

where B_i, $C \in R$. Apply on the terms of (f) the substitution

$$v \longrightarrow \frac{q - r}{s}$$

and multiply by some power of s to erase denominators. Since v does not appear in p and the p_i one gets another formula (f') such that

$$s^\alpha\, p = \underbrace{\sum_{p_i \in A} D_i\, p_i + E\, q}_{(f')}$$

where $D_i, E \in R$ and v only appears in q. Therefore $E = 0$ and $p \in (A) : s^\infty$. □

3.1. Ritt's reduction algorithms

Ritt's reduction algorithms are pseudo–division (Knuth, 1966, vol. 2, page 407) algorithms, extended to differential algebra. Many such algorithms exist (Kolchin, 1973, page 77) (Ritt, 1950, I, 6, page 5) which may produce different results. We fix one of them.

Let q be a differential polynomial and A be any finite subset of $R \setminus K$. Denote $v = \mathrm{ld}\, q$. Let $\bar{A} = \{p \in A \mid \mathrm{rank}\, p \leq \mathrm{rank}\, q\}$. We distinguish the *Ritt's partial reduction* (purely differential, denoted partial–rem) from *Ritt's full reduction* (denoted full–rem).

Specification of the partial reduction algorithm.

If $\bar{q} = q$ partial–rem A denotes the *partial remainder* of q by A then

1 $\bar{q}$ is partially reduced w.r.t. all the elements of A,
2 there exists a power product h of elements of $S_{\bar{A}}$ such that $h\, q \equiv \bar{q} \pmod{(\bar{A}_v)}$.

The following instructions provide an algorithm to compute h and $\bar{q}$ from q. Build a sequence of pairs (h_i, q_i). Initially, set $h_0 = 1$ and $q_0 = q$ and stop at the first index n such that q_n is partially reduced w.r.t. A (then take $h = h_n$ and $\bar{q} = q_n$). If i is an index such that q_i is not partially reduced w.r.t. A then let w be the highest derivative which occurs in q_i which is also a proper derivative of the leader of some $p \in A$. If there are many different possibilities for p, take which one you want. Now, let θ be the derivation operator such that $\mathrm{ld}\, \theta p = w$. Take for q_{i+1} the pseudo–remainder of q_i by θp. There exists then some $\alpha \in \mathbb{N}$ such that $s_p^\alpha\, q_i = q_{i+1} \pmod{(\theta p)}$. Take $h_{i+1} = s_p^\alpha\, h$.

Specification of the full reduction algorithm.

If $\bar{q} = q$ full–rem A denotes the *full remainder* of q by A then

1 $\bar{q}$ is reduced w.r.t. all the elements of A,
2 there exists a power product h of elements of $H_{\bar{A}}$ such that $h\, q \equiv \bar{q} \pmod{(\bar{A}_v)}$.

The following instructions provide an algorithm to compute h and $\bar{q}$ from q. Build a sequence of pairs (h_i, q_i). Initially, set $h_0 = 1$ and $q_0 = q$ and stop at the first index n such that q_n is reduced w.r.t. A (then take $h = h_n$ and $\bar{q} = q_n$). If i is an index such that q_i is not reduced w.r.t. A then let w be the highest derivative which occurs in q_i such that one of the following conditions holds:

1 w is a proper derivative of the leader of some $p \in A$,
2 w is the leader of some $p \in A$ and $\deg(q_i, w) \geq \deg(p, w)$.

If the first case arises then proceed as for the partial reduction algorithm else if the second case arises then take for q_{i+1} the pseudo–remainder of q_i by p There exists then some $\alpha \in \mathbb{N}$ such that $i_p^\alpha\, q_i = q_{i+1} \pmod{(p)}$. Take $h_{i+1} = i_p^\alpha\, h$.

We have $q \in [A] : H_A^\infty$ if and only if (q full–rem A) $\in [A] : H_A^\infty$. In particular, q full–rem $A = 0 \Rightarrow q \in [A] : H_A^\infty$. We have $q \in [A] : S_A^\infty$ if and only if (q partial–rem A) $\in [A] : S_A^\infty$.

4. Regular differential systems

All the definitions given in this section are new (e.g. the definitions of "pairs" and "solved pairs"). We define the coherence as a property of systems of differential polynomial equations and inequations (condition **C3** of definition 4.4) instead of the traditional property of systems of differential polynomials. This important change turns out to be very convenient and permits us to formulate Rosenfeld's lemma for regular systems instead of coherent autoreduced sets. Though this lemma only needs Δ–polynomials to be defined between elements of differentially triangular sets, we give a more general definition because we want to prove an analogue of Buchberger's second criterion in non triangular situations.

DEFINITION 4.1. *(pairs)*
A set $\{p_1, p_2\}$ of differential polynomials is said to be a pair *if the leaders of p_1 and p_2 have common derivatives. If A is a set of differential polynomials then* pairs(A) *denotes the set of all the pairs which can be formed between any two elements of A.*

We do not distinguish a pair $\{p_1, p_2\}$ from the pair $\{p_2, p_1\}$.

Let $\{p_1, p_2\}$ be a pair. It may happen that the leader of (say) p_2 is a (non necessarily proper) derivative of the leader of p_1. In that case, the pair $\{p_1, p_2\}$ is called a *reduction pair*.

Note however we will never consider a pair $\{p_1, p_2\}$ such that $\operatorname{rank} p_1 = \operatorname{rank} p_2$.

DEFINITION 4.2. *(Δ–polynomials)*
Let $\{p_1, p_2\}$ be a pair. Assume $\operatorname{rank} p_1 < \operatorname{rank} p_2$. *Denote $\theta_1 u = \operatorname{ld} p_1$, $\theta_2 u = \operatorname{ld} p_2$ and $\theta_{12} u = \operatorname{lcd}(\theta_1 u, \theta_2 u)$. The* Δ–polynomial *$\Delta(p_1, p_2)$ between p_1 and p_2 is defined as follows. If $\{p_1, p_2\}$ is a reduction pair then*

$$\Delta(p_1, p_2) = p_2 \text{ full–rem } \frac{\theta_2}{\theta_1} p_1,$$

else

$$\Delta(p_1, p_2) = s_1 \frac{\theta_{12}}{\theta_2} p_2 - s_2 \frac{\theta_{12}}{\theta_1} p_1.$$

If D is a set of pairs then $\Delta(D)$ denotes the set of all the Δ–polynomials of its elements.

With the same notations, if $\theta_1 u < \theta_2 u$ then $\operatorname{ld} \Delta(p_1, p_2) < \theta_{12} u$ and there exist some $\alpha \in \mathbb{N}$ and a differential polynomial $q \in R$ such that

$$\Delta(p_1, p_2) = s_1^\alpha \frac{\theta_{12}}{\theta_2} p_2 - q \frac{\theta_{12}}{\theta_1} p_1.$$

The notation Δ for Δ–polynomials comes from Rosenfeld's paper†. Seidenberg, Rosenfeld and Kolchin never considered reduction pairs. Our definition coincides with theirs in the other case.

4.1. Solved pairs

Definition 4.3. *(solved pairs)*
A pair $\{p_1, p_2\}$ *is said to be* solved by *a differential system of equations and inequations* $A = 0,\ S \neq 0$ *if there exists a derivative* $v < \operatorname{lcd}(\operatorname{ld} p_1, \operatorname{ld} p_2)$ *such that*

$$\Delta(p_1, p_2) \in (A_v) : (S \cap R_v)^\infty.$$

In our algorithm, we shall apply the following criterion to test whether a pair is solved by a differential system.

Lemma 4.1. *Let* $\{p_1, p_2\}$ *be a pair such that* $\operatorname{ld} p_1 \neq \operatorname{ld} p_2$. *Let* $A = 0,\ S \neq 0$ *be a differential system such that* $H_A \subset S$. *If* $\Delta(p_1, p_2)$ full–rem $A = 0$ *then the pair* $\{p_1, p_2\}$ *is solved by* $A = 0,\ S \neq 0$.

Proof. Denote $v = \operatorname{ld} \Delta(p_1, p_2)$. Since $\operatorname{ld} p_1 \neq \operatorname{ld} p_2$ we have $v < \operatorname{lcd}(\operatorname{ld} p_1, \operatorname{ld} p_2)$. Denote $\bar{A} = \{p \in A \mid \operatorname{rank} p \leq \operatorname{rank} \Delta(p_1, p_2)\}$. According to the specifications of Ritt's algorithms of reduction, there exist then $h_1, \ldots, h_n \in H_{\bar{A}}$ such that, for some positive integers $\alpha_1, \ldots, \alpha_n$ we have $h_1^{\alpha_1} \cdots h_n^{\alpha_n} \Delta(p_1, p_2) \in (\bar{A}_v)$. Since $H_{\bar{A}} \subset H_A \cap R_v$ and $\bar{A}_v \subset A_v$ we have $\Delta(p_1, p_2) \in (A_v) : (S \cap R_v)^\infty$ and the pair is solved by the differential system $A = 0,\ S \neq 0$. □

The next lemma is a generalization to a non triangular situation of a lemma already proven by Seidenberg (1956), inside theorem 6, page 51, Rosenfeld (1959), inside the lemma page 397 and Kolchin (1973), page 167.

Lemma 4.2. *Let* p_1 *and* p_2 *be two differential polynomials whose leaders* $\theta_1 u$ *and* $\theta_2 u$ *have common derivatives. Denote* s_1 *and* s_2 *their separants. Let* (Σ) *denote a differential system* $A = 0,\ S \neq 0$. *If* **(H1)** $\theta_1 u$ *and* $\theta_2 u$ *are different,* **(H2)** *the pair* $\{p_1, p_2\}$ *is solved by* (Σ) *and* **(H3)** $s_1, s_2 \in S$ *then for each derivation operator* $\gamma \in \Theta$, *the pair* $\{\gamma p_1, \gamma p_2\}$ *is solved by* (Σ).

Proof. Denote $\theta_{12} = \operatorname{lcm}(\theta_1, \theta_2)$ and $\Delta_\gamma = \Delta(\gamma p_1, \gamma p_2)$. Denote also $\theta u = \gamma \theta_{12} u = \operatorname{lcd}(\operatorname{ld} \gamma p_1, \operatorname{ld} \gamma p_2)$.

The proof is done by induction on the order of γ. If the order is zero then the lemma is satisfied because of **H2** else, decompose $\gamma = \delta\lambda$ where δ is a mere derivation and denote $\phi = \lambda \theta_{12}$. Assume (induction hypothesis) that the pair $\{\lambda p_1, \lambda p_2\}$ is solved by (Σ). There exists then a derivative $v < \phi u$ and a power product h of elements of $S \cap R_v$ such that $h\, \Delta_\lambda \in (A_v)$. By **H1** (assuming $p_1 < p_2$) there exist some $\alpha \in \mathbb{N}$ and a differential polynomial q such that $\Delta_\lambda = s_1^\alpha\, (\phi/\theta_2) p_2 - q\, (\phi/\theta_1) p_1$.

Consider the differential polynomial $\delta(h\, \Delta_\lambda)$. The second axiom of rankings implies that it belongs to $(A_{\delta v})$ and that $\delta v < \theta u$. Multiply it by h. One gets a sum $(\delta h)\, h\, \Delta_\lambda +$

† Note the symbol Δ has a different meaning in Kolchin's text: it denotes the set of derivations.

$h^2\,\delta\Delta_\lambda$ whose first term is in (A_v) by induction hypothesis. Since $(A_v) \subset (A_{\delta v})$ we conclude $h^2\,\delta\Delta_\lambda$ belongs to this latter ideal. Expand this polynomial

$$\begin{aligned} h^2(\delta\Delta_\lambda) &= h^2\delta\Big\{s_1^\alpha\,\frac{\phi}{\theta_2}p_2 - q\,\frac{\phi}{\theta_1}p_1\Big\} && (4.1)\\ &= h^2\Big\{(\delta(s_1^\alpha))\frac{\phi}{\theta_2}p_2 - (\delta q)\frac{\phi}{\theta_1}p_1\Big\} && (4.2)\\ &+ h^2\Big\{s_1^\alpha\,\frac{\theta}{\theta_2}p_2 - q\,\frac{\theta}{\theta_1}p_1\Big\}. && (4.3) \end{aligned}$$

The polynomials $(\phi/\theta_i)p_i$ $(i = 1, 2)$ have both $\phi u < \theta u$ for leaders. If $w = \max(\phi u, \delta v)$ then $w < \theta u$ and the term (4.2) is in (A_w). Thus so is the term (4.3). Since θ/θ_2 and θ/θ_1 are proper derivation operators, we have $\Delta_\gamma = s_1\,(\theta/\theta_2)p_2 - s_2\,(\theta/\theta_1)p_1$. The term (4.3) is equal to $h^2\,s_1^{\alpha-1}\,\Delta_\gamma + C\,(\theta/\theta_1)p_1$ where C is a differential polynomial. Using **H3**, the fact that $R_v \subset R_w$ and $\operatorname{ld} s_1 \leq \operatorname{ld} p_1 \leq \phi u \leq w$, for some power product h' of elements of $S \cap R_w$ we have $h'\,\Delta_\gamma \in (A_w,\, (\theta/\theta_1)p_1)$. The differential polynomial $h'\,\Delta_\gamma$ and the elements of A_w are free of θu. Lemma 3.1 applies, $\Delta_\gamma \in (A_w) : (S \cap R_w)^\infty$ and the pair $\{\gamma p_1,\, \gamma p_2\}$ is solved by (Σ). □

4.2. Rosenfeld's lemma

Definition 4.4. *(regular differential systems)*
A differential system $A = 0,\ S \neq 0$ of a differential polynomial ring R is said to be a regular differential system *(for a ranking $\mathcal{R}$) if*

C1 *A is differentially triangular,*

C2 *S contains the separants of the elements of A and is partially reduced w.r.t. A,*

C3 *all the pairs $\{p, p'\} \in \operatorname{pairs}(A)$ are solved by $A = 0,\ S \neq 0$ (coherence property).*

The differential ideal $[A] : S^\infty$ is called the regular differential ideal *defined by the system.*

The following lemma is a generalization of Rosenfeld (1959), lemma, page 397. which was already proven by Boulier (1997). The first version is due to Seidenberg (1956), theorem 6, page 51. Another version was proven in Kolchin (1973), lemma 5, page 137 but the part of Kolchin's lemma which is not in Rosenfeld's is not proven algorithmic. Kolchin's proof consists in a very nice transfinite induction (van der Waerden, 1966, chapter 9). We apply the idea in the proof of theorem 4.1.

Theorem 4.1. *(Rosenfeld's lemma)*
If $A = 0,\ S \neq 0$ is a regular differential system of a differential polynomial ring R for a ranking $\mathcal{R}$ then every differential polynomial in $[A] : S^\infty$ which is partially reduced w.r.t. A belongs to $(A) : S^\infty$.

Proof. Let $A = \{p_1, \ldots, p_n\}$. Let $q \in [A] : S^\infty$ be a differential polynomial partially reduced w.r.t. A. Denote $F(q)$ the set of all the formulæ (f) such that, for some power

product h of elements of S we have a finite sum

$$h\,q = \underbrace{\sum_{\phi\in\Theta}\sum_{j=1}^{n} B_{j,\phi}\ \phi p_j}_{(f)}\,.$$

Assume $q \notin (A) : S^\infty$. In each formula $(f) \in F(q)$ appears therefore some (at least one) proper derivatives of some leaders of elements of A. Denote $v(f)$ the greatest of them according to the ranking $\mathcal{R}$. Among all the formulæ $(f) \in F(q)$ let us consider one such that $v(f)$ is minimal w.r.t. $\mathcal{R}$. Such a formula exists for all rankings are well–orderings. We claim there exists another formula $(f') \in F(q)$ such that $v(f') < v(f)$. This contradiction will prove the lemma.

By lemma 1.1 and the minimality hypothesis, $v(f)$ is the derivative of the leader of at least one element of A. Let $v(f) = \theta u$ be a proper derivative of the leaders $\theta_1 u, \ldots, \theta_i u$ of the differential polynomials $p_1, \ldots, p_i \in A$, renaming the p's if needed.

Denote $\dfrac{\theta}{\theta_i} p_i = s_i\,\theta u + r$. Apply on the terms of the formula (f) the substitution

$$v(f) \to \frac{(\theta/\theta_i)p_i - r}{s_i}$$

(as in lemma 3.1) and multiply by some power s_i^α to erase denominators. Denoting $\gamma_j = (\theta/\mathrm{lcm}(\theta_i, \theta_j))$ we get a formula

$$\begin{aligned} s_i^\alpha\, h\, q &= D\ \frac{\theta}{\theta_i} p_i && (4.4)\\ &+ \sum_{j=1}^{i-1} E_j\ \ \Delta(\gamma_j p_i, \gamma_j p_j) && (4.5)\\ &+ \sum_{\phi\in\Theta}\sum_{j=1}^{n} C_{j,\phi}\ \phi p_j && (4.6) \end{aligned}$$

such that only derivatives less than $v(f)$ appear in the terms of the sums (4.5) and (4.6). Since the elements of S and q are partially reduced w.r.t. A, the derivative $v(f)$ only appears in the differential polynomial $(\theta/\theta_i)p_i$. Therefore $D = 0$.

If A is a system of ODE the sum (4.5) is empty and there exists a derivative $w < v(f)$ such that $q \in (A_w) : S^\infty$. Contradiction.

Assume $A = 0,\ S \neq 0$ is a PDE system. Since it is regular, condition **C3** of definition 4.4 holds and lemma 4.2 applies: all the pairs $\{\gamma_j p_i,\ \gamma_j p_j\}$ are solved. There exists thus a derivative $w < v(f)$ such that $q \in (A_w) : S^\infty$. Contradiction. □

Corollary 4.1. *If $A = 0,\ S \neq 0$ is a regular differential system of a differential polynomial ring R then*

1. *we have $[A] : S^\infty = R$ if and only if $(A) : S^\infty = R$,*
2. *for any $p \in R$ we have $p \in [A] : S^\infty$ iff (p partial–rem A) $\in (A) : S^\infty$,*
3. *a differential polynomial $p \in R$ is a divisor of zero modulo $[A] : S^\infty$ if and only if (p partial–rem A) is a divisor of zero modulo $(A) : S^\infty$.*

Proof. The first point. By Rosenfeld's lemma, $1 \in [A] : S^\infty$ if and only if $1 \in (A) : S^\infty$.

Let $p \in R$ be a differential polynomial. The second point relies on the two following facts: because of condition **C2**, $p \in [A] : S^\infty$ if and only if (p partial–rem A) $\in [A] : S^\infty$; the differential polynomial (p partial–rem A) is partially reduced w.r.t. A.

The third point. Let p, $q \in R$ be differential polynomials. Denote $\bar{p} = p$ partial–rem A and $\bar{q} = q$ partial–rem A. According to the second point above, we have

$$p \in [A] : S^\infty \;\Leftrightarrow\; \bar{p} \in (A) : S^\infty \quad \text{and} \quad q \in [A] : S^\infty \;\Leftrightarrow\; \bar{q} \in (A) : S^\infty.$$

We also have $pq \in [A] : S^\infty$ if and only if $\bar{p}\,\bar{q} \in (A) : S^\infty$. Therefore, $pq \in [A] : S^\infty$, p, $q \notin [A] : S^\infty$ (i.e. p is a divisor of zero modulo $[A] : S^\infty$) if and only if $\bar{p}\,\bar{q} \in (A) : S^\infty$, $\bar{p}$, $\bar{q} \notin (A) : S^\infty$ (i.e. $\bar{p}$ is a divisor of zero modulo $(A) : S^\infty$). □

THEOREM 4.2. *(lifting of Lazard's lemma)*
If $A = 0,\ S \neq 0$ is a consistent regular differential system of a differential polynomial ring R and $R_0 \subset R$ denotes the ring of the differential polynomials partially reduced w.r.t. A then

1. *the regular differential ideal $[A] : S^\infty$ is radical,*
2. *there is a bijection between the minimal differential prime components $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of $[A] : S^\infty$ and the minimal prime components $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ of $(A) : S^\infty$ given by $\mathfrak{b}_i = (\mathfrak{p}_i \cap R_0)$; moreover, if C_i is a characteristic set of $\mathfrak{b}_i$ then C_i is also a characteristic set of $\mathfrak{p}_i$ and $\mathfrak{p}_i = [C_i] : H_{C_i}^\infty$.*

PROOF. Assume $p^k \in [A] : S^\infty$ for some $k \in \mathbb{N}$. Denote $\bar{p} = (p$ partial–rem $A)$. By Rosenfeld's lemma $\bar{p}^k \in (A) : S^\infty$. By Lazard's lemma $\bar{p} \in (A) : S^\infty$. By the corollary below Rosenfeld's lemma (point 2), $p \in [A] : S^\infty$ thus $[A] : S^\infty$ is radical.

The ideals $\mathfrak{b}$'s are prime and their intersection is equal to $(A) : S^\infty$. Let's assume **(H1)** that $\mathfrak{b}_1$ is redundant w.r.t. $(A) : S^\infty$ and seek a contradiction. Let $f \in \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_n$ be a differential polynomial and $g = f$ partial–rem A. Since $A \subset \mathfrak{p}_i$ we have $g \in \mathfrak{p}_i$ for every $2 \leq i \leq n$. Since $g \in R_0$ we have $g \in \mathfrak{b}_2 \cap \cdots \cap \mathfrak{b}_n$. Using **H1** we conclude $g \in (A) : S^\infty$. Let's summarize: (f partial–rem A) $\in (A) : S^\infty$. By the corollary (point 2) below Rosenfeld's lemma $f \in [A] : S^\infty$ thus $\mathfrak{p}_1$ is redundant w.r.t. $[A] : S^\infty$. Contradiction.

Assume C_i is a characteristic set of $(\mathfrak{p}_i \cap R_0)$. Let $p \in \mathfrak{p}_i$ and denote $q = p$ full–rem C_i. We have $q \in \mathfrak{p}_i$. By Lazard's lemma, $\mathrm{ld}\, A = \mathrm{ld}\, C_i$ thus $q \in R_0$. Since $q \in \mathfrak{p}_i \cap R_0$ is reduced w.r.t. C_i we have $q = 0$. Therefore C_i is a characteristic set of $\mathfrak{p}_i$ and $\mathfrak{p}_i = [C_i] : H_{C_i}^\infty$. □

If $A = 0,\ S \neq 0$ is a regular differential system then the set of leaders of the elements of A is equal to the set of leaders of each of the differential prime ideals which are minimal over $[A] : S^\infty$. All these differential prime ideals have therefore the same differential Hilbert's function. The computation of this function is then a purely combinatorial problem (Kolchin, 1973, chapter II, section 12).

Moreover, by applying a primary decomposition algorithm over $(A) : S^\infty$ we get the differential prime decomposition of the differential ideal $[A] : S^\infty$. Characteristic sets for the minimal differential prime components of $[A] : S^\infty$ can then be computed using the method given by Boulier *et al.* (1995), Theorem 6, page 164.

4.3. Testing the coherence

Let $A = 0,\ S \neq 0$ be a differential system of R which satisfies conditions **C1** and **C2** of definition 4.4. If A is differentially triangular, $H_A \subset S$ and $\Delta(p, p')$ full–rem $A = 0$ for all pairs $\{p,\, p'\} \in \text{pairs}(A)$ then the differential system $A = 0,\ S \neq 0$ is regular (lemma 4.1).

This criterion is useful for practical purposes but only gives a sufficient condition. Consider the next differential system $A = 0,\ S_A \neq 0$ for any elimination ranking such that $u > v$. It generates only one Δ–polynomial $\Delta(p_1, p_2) = v_y$. Now, $\Delta(p_1, p_2)\,(v_y+1)^2 \in (A_\alpha)$ for some derivative $\alpha < u_{xy}$. Since (v_y+1) is a multiple factor of p_3, it is also a factor of the separant of p_3 whence $\Delta(p_1, p_2) \in (A_\alpha) : (S \cap R_\alpha)^\infty$. Therefore $A = 0,\ S_A \neq 0$ is a regular differential system. However, the Δ–polynomial v_y is reduced w.r.t. A.

$$A \left\{ \begin{array}{lcl} p_1 & = & u_x + v, \\ p_2 & = & u_y, \\ p_3 & = & v_y(v_y+1)^2. \end{array} \right.$$

Given a differential system and a ranking, one may decide whether the system is regular or not. The decision algorithm is quite expensive and not very useful: the following example (borrowed from Boulier (1997)) shows that the coherence property is only a sufficient condition for Rosenfeld's lemma.

Consider the following system A of $\mathbb{Q}\{t,\, u,\, v,\, w\}$ endowed with derivations w.r.t. x and y, for any ranking such that t_x, u_x, u_y and v_y are the leaders of p_1, p_2, p_3 and p_4 respectively. It generates only one pair $\{p_2,\, p_3\}$. The associated Δ–polynomial is $\Delta(p_2, p_3) = v_y - w_x$.

$$A \left\{ \begin{array}{lcl} p_1 & = & t_x^2 + v_y, \\ p_2 & = & u_x + v, \\ p_3 & = & u_y + w, \\ p_4 & = & (v_y - w_x)v_y. \end{array} \right.$$

If the ranking is orderly, then there exists a derivative α such that $t_x,\, u_x,\, u_y,\, v_y \leq \alpha < u_{xy}$. Then $A \subset A_\alpha$ and $t_x \in S_A \cap R_\alpha$. Using p_1 and p_4 it is clear that $\Delta(p_2, p_3)\, t_x^2 \in (A_\alpha)$. Since $t_x \in S_A \cap R_\alpha$ it follows that $\Delta(p_2, p_3) \in (A_\alpha) : (S_A \cap R_\alpha)^\infty$ i.e. the pair $\{p_2,\, p_3\}$ is solved by $A = 0,\ S \neq 0$. This differential system is thus regular and Rosenfeld's lemma applies.

If the ranking is an elimination ranking such that $t > u$ then for each derivative $\alpha < u_{xy}$ we have $p_1 \notin A_\alpha$ and $t_x \notin S_A \cap R_\alpha$. It can be proven (Boulier, 1997, lemma 6) — but this is quite obvious — that $\Delta(p_2, p_3) \notin (A_\alpha) : (S \cap R_\alpha)^\infty$ i.e. the pair $\{p_2,\, p_3\}$ is not solved by $A = 0,\ S \neq 0$. This differential system is not regular w.r.t. this latter ranking. However, since the leaders and the families S_A are the same for both rankings, the conclusion of Rosenfeld's lemma still holds.

4.3.1. Buchberger's criteria

Most of the results of this section are borrowed from Boulier (1997). Buchberger (1979) established a few criteria which predict that some S–polynomials (Becker and Weispfenning, 1991, def. 5.46, page 211) are reduced to zero without having to actually reduce them. They turn out to be very important in practice since most of the CPU time is spent in S–polynomials reductions. Remark however they do not change the theoretical

complexity of Gröbner bases since this complexity expresses the size of the Gröbner basis (which does not depend on the algorithm) in terms of the size of the input system.

Buchberger's first criterion (Becker and Weispfenning, 1991, lemma 5.66, page 222) states that if the leading terms of two polynomials p and q are disjoint (i.e. their least common multiple is equal to their product) then the S–polynomial $S(p,q) \xrightarrow[\{p,q\}]{*} 0$.

In differential algebra, we might conjecture that if p and q are two differential polynomials with leaders θu and ϕu respectively and if θ and ϕ are disjoint then the Δ–polynomial $\Delta(p,q)$ full–rem $\{p, q\} = 0$. This conjecture is false in general but true in the next case.

PROPOSITION 4.1. *(analogue of Buchberger's first criterion)*
If p and q are two differential polynomials which are linear, homogeneous, in one differential indeterminate, with constant coefficients and if (denoting $\operatorname{ld} p = \theta u$ and $\operatorname{ld} q = \phi u$) we have $\operatorname{lcd}(\theta u, \phi u) = \theta\phi u$ then $\Delta(p,q)$ full–rem $\{p, q\} = 0$.

PROOF. Let $R = K\{u\}$ be a differential polynomial ring endowed with a ranking and a set of derivations $\{\delta_1, \ldots, \delta_m\}$. Let $\bar{R} = K[x_1, \ldots, x_m]$ be a non differential polynomial ring.

To each differential polynomial $f = \theta_1 u + \cdots + \theta_s u$ which is linear, homogeneous and with constant coefficients we may associate a polynomial $\gamma f \in \bar{R}$ defined by $\gamma f = \gamma\theta_1 u + \cdots + \gamma\theta_s u$ and $\gamma c = c$ for every $c \in K$ and $\gamma(\delta_1^{\alpha_1} \cdots \delta_m^{\alpha_m} u) = x_1^{\alpha_1} \cdots x_m^{\alpha_m}$. The monoid of terms over the alphabet $\{x_1, \ldots, x_m\}$ is endowed with the admissible ordering (Becker and Weispfenning, 1991, def. 4.59, page 167) given by the ranking.

Let $p, q, r \in R$ satisfying the hypotheses of the proposition. On one hand, $\Delta(p,q) = \gamma^{-1} S(\gamma p, \gamma q)$; on another hand r full–rem $\{p, q\} = \bar{r}$ if and only if $\gamma r \xrightarrow[\{\gamma p, \gamma q\}]{*} \gamma\bar{r}$.

By Buchberger's first criterion, $S(\gamma p, \gamma q) \xrightarrow[\{\gamma p, \gamma q\}]{*} 0$ so $\Delta(p,q)$ full–rem $\{p, q\} = 0$. □

The following example shows that the conjecture is false if the equations are not homogeneous: take $p = u_x + 1$ and $q = u_y + u$. The Δ–polynomial $\Delta(p,q) = u_x$ is reduced to 1 by the set $\{p, q\}$.

This one shows that the conjecture is false if the coefficients of the equations are not constants: assume the coefficient c is such that $c_y = 1$ and take $p = u_x + cu$ and $q = u_y$. The Δ–polynomial $\Delta(p,q) = cu_y + u$ is reduced to u by $\{p, q\}$.

In proposition 4.2, we prove an analogue of Buchberger's second criterion. However we impose restrictions on the differential polynomials which have no counterpart in the Gröbner bases theory. This makes the proof of its implementation in the Rosenfeld–Gröbner algorithm more painful than in the non differential case.

PROPOSITION 4.2. *(analogue of Buchberger's second criterion)*
Let $\langle p_1, p_2, p_3\rangle$ be a triple of differential polynomials such that **(H1)** *the leaders $\theta_1 u$, $\theta_2 u$ and $\theta_3 u$ of the p's have common derivatives and are pairwise different,* **(H2)** $\operatorname{lcd}(\theta_1 u, \theta_3 u)$ *is a derivative of $\theta_2 u$ and* **(H3)** *one of the following conditions holds:*

1. $\operatorname{ld} p_i$ *is not a derivative of* $\operatorname{ld} p_j$ $(1 \leq i, j \leq 3$ *and* $i \neq j)$,
2. $p_1 < p_2 < p_3$ *or* $p_3 < p_2 < p_1$,
3. $p_2 < p_1 < p_3$ *and* $\deg(p_1, \theta_1 u) = 1$,
4. $p_1 < p_3 < p_2$ *and* $\deg(p_3, \theta_3 u) = 1$.

Let $A = 0,\ S \neq 0$ be a differential system. If **(H4)** *the pairs $\{p_1, p_2\}$ and $\{p_2, p_3\}$ are solved by $A = 0,\ S \neq 0$ and* **(H5)** *$s_1, s_2, s_3 \in S$ then the pair $\{p_1, p_3\}$ is solved by $A = 0,\ S \neq 0$.*

PROOF. Denote $\theta_{ij}u = \mathrm{lcd}(\theta_i u, \theta_j u)$. Because of **H2** the derivation operators $(\theta_{13}/\theta_{12})$ and $(\theta_{13}/\theta_{23})$ exist. Denote

$$\begin{aligned}\Delta_3 &= \Delta\left(\frac{\theta_{13}}{\theta_{12}}p_1, \frac{\theta_{13}}{\theta_{12}}p_2\right),\\ \Delta_1 &= \Delta\left(\frac{\theta_{13}}{\theta_{23}}p_2, \frac{\theta_{13}}{\theta_{23}}p_3\right).\end{aligned}$$

Lemma: if there exist differential polynomials B, C and D and a power product h of elements of S such that $\mathrm{ld}\, h < \theta_{13}u$ and

$$h\,\Delta(p_1, p_3) = B\,\Delta_3 + C\,\Delta_1 + D\,\frac{\theta_{13}}{\theta_1}p_1 \tag{4.7}$$

then the pair $\{p_1, p_3\}$ is solved by $A = 0,\ S \neq 0$. Proof: by **H4** and lemma 4.2 there exists a derivative $v < \theta_{13}u$ such that $\Delta_3, \Delta_1 \in (A_v) : (S \cap R_v)^\infty$. By **H5** there exists a power product h' of elements of S such that $h'\Delta(p_1, p_3) \in (A_v, (\theta_{13}/\theta_1)p_1)$ and $\mathrm{ld}\, h' = \max(\mathrm{ld}\, h, v) < \theta_{13}u$. Denote $w = \max(\theta_1 u, \mathrm{ld}\, h')$. Because of **H1** we have $w < \theta_{13}u$. By **H5** and lemma 3.1, $\Delta(p_1, p_3) \in (A_w) : (S \cap R_w)^\infty$ and the pair $\{p_1, p_3\}$ is solved by $A = 0,\ S \neq 0$. □

If $\mathrm{ld}\, p_i$ is not a derivative of $\mathrm{ld}\, p_j$ $(1 \leq i, j \leq 3$ and $i \neq j)$ then $s_2\,\Delta(p_1, p_3) = s_1\Delta_1 + s_3\Delta_3$. Because of **H1** we have $\mathrm{ld}\, s_2 < \theta_{13}u$. By **H5** our lemma above applies and the pair $\{p_1, p_3\}$ is solved by $A = 0,\ S \neq 0$.

If $p_1 < p_2 < p_3$ then there exist some $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{N}$ and some differential polynomials q_1, q_2 and q_3 such that

$$\begin{aligned}\Delta_3 &= s_1^{\alpha_3}\frac{\theta_{13}}{\theta_2}p_2 - q_3\,\frac{\theta_{13}}{\theta_1}p_1,\\ \Delta_1 &= s_2^{\alpha_1}\frac{\theta_{13}}{\theta_3}p_3 - q_1\,\frac{\theta_{13}}{\theta_2}p_2,\\ \Delta(p_1, p_3) &= s_1^{\alpha_2}\frac{\theta_{13}}{\theta_3}p_3 - q_2\,\frac{\theta_{13}}{\theta_1}p_1.\end{aligned}$$

Denoting $\beta = \max(\alpha_2, \alpha_3)$, there exists a differential polynomial C such that

$$s_1^{\beta-\alpha_2}s_2^{\alpha_1}\Delta(p_1, p_3) = s_1^{\beta}\Delta_1 + q_1\,s_1^{\beta-\alpha_3}\Delta_3 + C\,\frac{\theta_{13}}{\theta_1}p_1.$$

Because of **H1** we have $\mathrm{ld}(s_1^{\beta-\alpha_2}s_2^{\alpha_1}) < \theta_{13}u$. By **H5** our lemma applies and the pair $\{p_1, p_3\}$ is solved by $A = 0,\ S \neq 0$.

If $p_2 < p_1 < p_3$ then

$$\Delta_3 = s_2^{\alpha_3}\frac{\theta_{13}}{\theta_1}p_1 - q_3\frac{\theta_{13}}{\theta_2}p_2.$$

Computing as above we find a relation

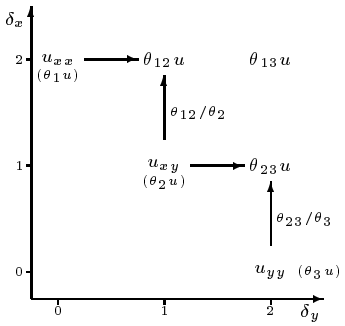
$$q_3\,s_2^{\alpha_1}\Delta(p_1, p_3) = q_1\,s_1^{\alpha_2}\Delta_3 - q_3\,s_1^{\alpha_2}\Delta_1 + C\,\frac{\theta_{13}}{\theta_1}p_1.$$

In the general case, one cannot apply our lemma for $q_3 \notin S$. Assume $\deg(p_1, \theta_1 u) = 1$.

By **H5** we have $q_3 = s_1 \in S$. Because of **H1**, we have $\mathrm{ld}(q_3\, s_2^{\alpha_1}) < \theta_{13}u$. Our lemma applies and the pair $\{p_1, p_3\}$ is solved by $A = 0,\ S \neq 0$.

The last case is similar to the former one. □

$$
\begin{array}{lcl}
p_1 & = & v u_{xx}^3 + u_{xx}^2 + u_x, \\
p_2 & = & u_{xy}, \\
p_3 & = & u_{yy} + u_y^2, \\
p_4 & = & v_y, \\
p_5 & = & v_{xxx} + u_{xx}^3, \\
 & & \\
\Delta(p_1, p_2) & = & v_y u_{xx}^3 + u_{xy}, \\
\Delta(p_2, p_3) & = & u_y u_{xy}.
\end{array}
$$



The picture illustrates proposition 4.2 in the triangular case. Both $\Delta(p_1, p_2)$ and $\Delta(p_2, p_3)$ are reduced to zero by A. Therefore the pairs $\{p_1, p_2\}$ and $\{p_2, p_3\}$ are solved by the system $A = 0,\ H_A \neq 0$. The least common derivative between the leaders of p_1 and p_3 is a derivative of the leader of p_2. Thus the pair $\{p_1, p_3\}$ is solved by the system.

5. Computing a regular decomposition

This section aims at proving the theorem 5.1 which constitutes the core of the Rosenfeld–Gröbner algorithm. Our implementation of the algorithm can be viewed as a mere translation in the MAPLE programming language of the effective proof of this theorem.

Our implementation carries the analogue of Buchberger's second criterion out. It is a lifting for the differential algebra of the version of Buchberger's algorithm by Gebauer and Möller (1988). The book of Becker and Weispfenning (1991), pages 230–232 furnished us many important informations on that subject. It is much more efficient than the ones given by Boulier (1994) or Boulier *et al.* (1995).

THEOREM 5.1. *(computing a regular decomposition)*
If $P_0 = 0,\ S_0 \neq 0$ is a differential system of a differential polynomial ring R then it is possible to compute finitely many consistent regular differential systems $A_i = 0,\ S_i \neq 0$ $(1 \leq i \leq n)$ such that

$$\mathfrak{p} = \sqrt{[P_0] : S_0^\infty} \quad = \quad [A_1] : S_1^\infty \cap \cdots \cap [A_n] : S_n^\infty. \tag{5.1}$$

This decomposition may contain components redundant w.r.t. $\mathfrak{p}$. Operations needed are addition, multiplication, differentiation and equality test with zero in the base field of R.

A *quadruple* $G = \langle A, D, P, S \rangle$ is a data structure which contains a differential system being processed until it is regular. The set $A \subset R$ contains equations already processed. The set $P \subset R$ contains the equations which are not yet processed. The set D contains pairs which have to be solved and $S \subset R$ contains the inequations.

Initially, $P = P_0$, $S = S_0$ and $A = D = \emptyset$. If $P \neq \emptyset$ or $D \neq \emptyset$ then the current quadruple is rewritten as finitely many quadruples by a completion and splitting process. If $P = D = \emptyset$ then an autoreduction process transforms the differential system $A = 0,\ S \neq 0$

as an equivalent regular differential system $\bar{A} = 0,\ \bar{S} \neq 0$. The autoreduction process decides if the system is consistent or not. In the former case, the regular differential ideal $[\bar{A}] : \bar{S}^\infty$ becomes one of the components of intersection 5.1; in the latter, the system is discarded.

Let $G = \langle A, D, P, S \rangle$ be a quadruple. We denote $\mathcal{P}(D)$ the set of all the differential polynomials p such that there exists a reduction pair[†] $\{p, p'\} \in D$ with $\operatorname{rank} p > \operatorname{rank} p'$. We denote $\mathcal{F}(G) = A \cup \mathcal{P}(D) \cup P$ and $\mathcal{I}(G) = \sqrt{[\mathcal{F}(G)] : S^\infty}$. The solutions of a quadruple G are defined as the solutions of the differential system $\mathcal{F}(G) = 0,\ S \neq 0$. A pair is said to be solved by G if it is solved by the system $\mathcal{F}(G) = 0,\ S \neq 0$. The following axioms give the definition of pairs *nearly solved* by G.

A1 Every pair which is solved by G is nearly solved by G.
A2 Every pair which belongs to D is nearly solved by G.
A3 If $\{p_1, p_2\}$ and $\{p_2, p_3\}$ are pairs nearly solved by G and if the triple $\langle p_1, p_2, p_3 \rangle$ satisfies the hypotheses **H1**, **H2** and **H3** of proposition 4.2 then the pair $\{p_1, p_3\}$ is nearly solved by G.

We are now ready to state some properties which will become loop invariants of our implementation of the Rosenfeld–Gröbner algorithm. Let $G = \langle A, D, P, S \rangle$ be a quadruple.

I1 The rank of the set A is autoreduced.
I2 If $\{p, p'\} \in D$ is a reduction pair with $\operatorname{rank} p > \operatorname{rank} p' = v^d$ and $F = \{f \in \mathcal{F}(G) \mid \operatorname{rank} f \leq v^d\}$ then $p' \in (F_v) : (S \cap R_v)^\infty$.
I3 Every pair $\{p, p'\} \in \operatorname{pairs}(A)$ is nearly solved by G.
I4 If $p \in A$ or p belongs to some pair of D then $i_p,\ s_p \in S$.
I5 If $\{p, p'\} \in D$ is not a reduction pair then $\Delta(p, p') \in \mathcal{I}(G)$.
I6 If $\{p, p'\} \in D$ is a pair then $\operatorname{rank} p \neq \operatorname{rank} p'$.

5.1. The final autoreduction process

Let $G = \langle A, D, P, S \rangle$ be a quadruple satisfying the invariants and s.t. $D = P = \emptyset$. The differential system is not necessarily regular. We present here one possible way to transform it as an equivalent regular differential system. This process may show that $\mathcal{I}(G) = R$. In that case, the quadruple G is discarded. We build a sequence of differential systems. Let

$$A_0 = A, \quad S_0 = S.$$

Let $k \geq 0$ be an index. If A_k is not differentially triangular then let θu be the greatest derivative occuring in some $p \in A_k$ being also a proper derivative of the leader $\theta' u$ of some $p' \in A_k$. Denoting $\phi = \theta/\theta'$, compute $\bar{p} = p$ full–rem $\phi p'$ and

$$\begin{aligned} A_{k+1} &= A_k \setminus \{p\} \cup \{\bar{p}\}, \\ S_{k+1} &= S_k \cup \{i_{\bar{p}},\ s_{\bar{p}}\}. \end{aligned}$$

If $\operatorname{rank} A_k \neq \operatorname{rank} A_{k+1}$ then $\mathcal{I}(G) = R$ (proved below) and the quadruple is discarded. Let's assume $\operatorname{rank} A_k = \operatorname{rank} A_{k+1}$. If A_k is differentially triangular then take

$$\bar{A} = A_k, \quad \bar{S} = S_k \text{ partial–rem } \bar{A}.$$

[†] Recall we don't distinguish $\{p, p'\}$ from $\{p', p\}$.

PROPOSITION 5.1. *The autoreduction process terminates.*

PROOF. The sequence of the rewritten derivatives θu is strictly decreasing and rankings are well orderings. □

PROPOSITION 5.2. *For each index* $k \geq 0$ *we have* $H_{A_k} \subset S_k$. *Moreover,* $H_{\bar{A}} \subset \bar{S}$.

PROOF. The first statement is clear. The second one is due to the fact that, since $\bar{A}$ is differentially triangular, the initials and the separants of its elements are partially reduced w.r.t. it, and are thus left inchanged by the final partial reduction. □

PROPOSITION 5.3. *For each index* $k \geq 0$, *if* $\operatorname{rank} A_k \neq \operatorname{rank} A_{k+1}$ *then* $[A_k] : S_k^\infty = R$.

PROOF. If $\operatorname{rank} A_k \neq \operatorname{rank} A_{k+1}$ then some initial i_p of some element of A_k has been reduced to zero. By proposition 5.2 we have $i_p \in [A_k] : S_k^\infty$. Since $i_p \in S_k$ (by proposition 5.2 again) $[A_k] : S_k^\infty = R$. □

Let us now explicit the values of $\bar{p}$, its initial and its separant. Let $k \geq 0$ be an index. Since $\operatorname{rank} A_k$ is autoreduced, $\operatorname{ld} \phi p' = \theta u < \operatorname{ld} p$ and there exist some $\alpha \in \mathbb{N}$ and differential polynomials q_0, q_1, $q_2 \in R_{\theta u}$ such that

$$\bar{p} = s_{p'}^\alpha\, p - q_0\, \phi p', \tag{5.2}$$

$$s_{\bar{p}} = s_{p'}^\alpha\, s_p - q_1\, \phi p', \tag{5.3}$$

$$i_{\bar{p}} = s_{p'}^\alpha\, i_p - q_2\, \phi p'. \tag{5.4}$$

LEMMA 5.1. *If* $\operatorname{rank} A_k = \operatorname{rank} A_{k+1}$ *then for every derivative* v *we have*†

$$(A_{k,v}) : (S_k \cap R_v)^\infty \subset (A_{k+1,v}) : (S_{k+1} \cap R_v)^\infty.$$

PROOF. First observe $S_k \subset S_{k+1}$. If $v < \operatorname{ld} p$ then $A_{k,v} = A_{k+1,v}$. If $v \geq \operatorname{ld} p$, it suffices to prove $p \in (A_{k+1,v}) : (S_{k+1} \cap R_v)^\infty$. Since $\operatorname{ld} p = \operatorname{ld} \bar{p}$ we have $\bar{p} \in A_{k+1,v}$. Since $\operatorname{ld} \phi p' = \theta u < \operatorname{ld} p$ we have $\phi p' \in A_{k+1,v}$ and $s_{p'} \in R_v$. Using proposition 5.2 and relation (5.2) we conclude $p \in (A_{k+1,v}) : (S_{k+1} \cap R_v)^\infty$. □

PROPOSITION 5.4. *For each index* $k \geq 0$, *we have* $[A_k] : S_k^\infty = [A_{k+1}] : S_{k+1}^\infty$.

PROOF. The inclusion $[A_k] : S_k^\infty \subset [A_{k+1}] : S_{k+1}^\infty$ comes from lemma 5.1. The converse one. Assume f is a differential polynomial such that, for some β, $\gamma \in \mathbb{N}$ we have $i_{\bar{p}}^\beta s_{\bar{p}}^\gamma f \in [A_{k+1}]$. By relation (5.2) we have $\bar{p} \in [A_k] : S_k^\infty$ hence $[A_{k+1}] \subset [A_k] : S_k^\infty$. By relations (5.3) and (5.4) and the fact that s_p, $s_{p'}$, $i_p \in S_k$ (proposition 5.2) $f \in [A_k] : S_k^\infty$. □

LEMMA 5.2. *Assume all the sets* A_k *have the same rank. All pairs in* $\operatorname{pairs}(A_k)$ *are solved by* $A_k = 0,\ S_k \neq 0$.

† By $A_{k,v}$ we mean E_v where $E = A_k$.

PROOF. The proof is an induction on k. Basis of the induction. Because of **I3**, the fact that $D = \emptyset$ and proposition 4.2 every pair $\{p, p'\} \in \text{pairs}(A_0)$ is solved by the differential system $A_0 = 0,\ S_0 \neq 0$.

The general case. Let $k \geq 0$ be an index. We assume (induction hypothesis) that all pairs in $\text{pairs}(A_k)$ are solved by $A_k = 0,\ S_k \neq 0$ and we prove that, if $\{p_1, p_2\} \in \text{pairs}(A_{k+1})$ then $\{p_1, p_2\}$ is solved by $A_{k+1} = 0,\ S_{k+1} \neq 0$.

First subcase: $p_1 \neq \bar{p}$ and $p_2 \neq \bar{p}$. Then $\{p_1, p_2\} \in \text{pairs}(A_k)$ is solved by the system $A_k = 0,\ S_k \neq 0$ i.e. there exists some $v < \text{lcd}(\text{ld}\, p_1, \text{ld}\, p_2)$ such that $\Delta(p_1, p_2) \in (A_{k,v}) : (S_k \cap R_v)^\infty$. By lemma 5.1 $\Delta(p_1, p_2) \in (A_{k+1,v}) : (S_{k+1} \cap R_v)^\infty$ and the pair is solved by $A_{k+1} = 0,\ S_{k+1} \neq 0$.

Second subcase: $p_1 = \bar{p}$. Since $\text{rank}\, A_k = \text{rank}\, A_{k+1}$ we have $\text{ld}\, p = \text{ld}\, \bar{p} = \text{ld}\, p_1 = \theta_1 u$ and (assuming with no loss of generality that $\bar{p} < p_2$)

$$\Delta(\bar{p}, p_2) \quad = \quad s_{\bar{p}} \frac{\theta_{12}}{\theta_2} p_2 - s_{p_2} \frac{\theta_{12}}{\theta_1} \bar{p}.$$

Expanding the value of $\Delta(\bar{p}, p_2)$ using formulæ (5.2) and (5.3) and recalling $\text{ld}\, \phi p' < \text{ld}\, p_1$ we see there exists a derivative $v < \theta_{12} u$ such that $s^\alpha_{p'} \Delta(p, p_2) \equiv \Delta(\bar{p}, p_2) \pmod{(A_{k,v})}$. By the fact that the pair $\{p, p_2\}$ is solved by $A_k = 0,\ S_k \neq 0$ (induction hypothesis) and lemma 5.1 the pair $\{\bar{p}, p_2\}$ is solved by $A_{k+1} = 0,\ S_{k+1} \neq 0$. □

PROPOSITION 5.5. *Every pair in* $\text{pairs}(\bar{A})$ *is solved by* $\bar{A} = 0,\ \bar{S} \neq 0$.

PROOF. By lemma 5.2 every pair in $\text{pairs}(\bar{A})$ is solved by $\bar{A} = 0,\ S_k \neq 0$, where k is the index such that $\bar{A} = A_k$ is differentially triangular.

It suffices to prove that for any derivative v we have $(\bar{A}_v) : (S_k \cap R_v)^\infty \subset (\bar{A}_v) : (\bar{S} \cap R_v)^\infty$. Let $s \in S_k \cap R_v$ be not partially reduced w.r.t. A and $\bar{s} = s$ partial–rem A. There exists a power product h of elements of $S_A \cap R_v$ such that $h\, s \equiv \bar{s} \pmod{(A_v)}$. By proposition 5.2 we have $S_A \subset \bar{S}$ and the proposition is proved. □

By propositions 5.3 and 5.4, if the rank of the set A_k changes during the autoreduction process then the differential system $A = 0,\ S \neq 0$ is proved to be inconsistent and can be discarded. Let's assume this is not the case. The system $\bar{A} = 0,\ \bar{S} \neq 0$ is a regular differential system. Indeed $\bar{A}$ is differentially triangular (condition **C1** is satisfied); $\bar{S}$ contains $H_{\bar{A}}$ (proposition 5.2) and is partially reduced w.r.t. $\bar{A}$ (condition **C2** is satisfied); proposition 5.5 proves condition **C3** holds for $\bar{A} = 0,\ \bar{S} \neq 0$. Computing a Gröbner basis of the ideal $(\bar{A}) : \bar{S}^\infty$ in dimension zero, one decides whether the regular differential system $\bar{A} = 0,\ \bar{S} \neq 0$ is consistent (corollary below Rosenfeld's lemma, point 1). If it is inconsistent, it is discarded. Otherwise, $\mathcal{I}(G) = [\bar{A}] : \bar{S}^\infty$ by theorem 4.2 (point 1).

5.2. The completion process

We consider a quadruple $G = \langle A, D, P, S \rangle$ satisfying the invariants and such that $D \neq \emptyset$ or $P \neq \emptyset$. Roughly, we pick a new equation $q = 0$ from these sets, reduce it by A and enlarge A with it (if non zero of course). Applying the analogues of Buchberger's criteria, we do not only try to generate as few pairs as possible but also to remove as many pairs as possible from D. The method is not optimal. Gebauer and Möller's version of the Buchberger algorithm is not either.

Pick either a differential polynomial $q_0 \in P$ or a pair $\{p_0, p'_0\} \in D$. In the former

case, let $P^* = P \setminus \{q_0\}$ let $D^* = D$ and $q = q_0$ full–rem A. In the latter let $P^* = P$, let $D^* = D \setminus \{\{p_0, p_0'\}\}$ and $q = \Delta(p_0, p_0')$ full–rem A. Assume $q \neq 0$ and denote $G' = \langle A', D', P', S' \rangle$ any quadruple satisfying:

$A' = \{q\} \cup \{p \in A \mid \mathrm{ld}\, p$ is not a derivative of $\mathrm{ld}\, q\}$.
$D' = D_1 \cup D_2$ where
$D_1 \subset D_0 = \{\{p, q\} \mid p \in A$ and $\mathrm{ld}\, p$ has common derivatives with $\mathrm{ld}\, q\}$
A pair $\{p, q\} \in D_0$ is not kept in D_1 only if condition (a) or (b) holds:
(a) p and q are linear homogeneous differential polynomials in one differential indeterminate with constant coefficients and $\mathrm{lcm}(\theta, \phi) = \theta\phi$ (where $\mathrm{ld}\, q = \theta u$ and $\mathrm{ld}\, p = \phi u$),
(b) there exists a pair $\{p', q\} \in D_1$ such that the triple $\langle q, p', p \rangle$ satisfies the hypotheses **H1**, **H2** and **H3** of proposition 4.2.
$D_2 \subset D^*$.
A pair $\{p, p'\} \in D^*$ is not kept in D_2 only if the triple $\langle p, q, p' \rangle$ satisfies the hypotheses **H1**, **H2** and **H3** of proposition 4.2 and $\mathrm{lcd}(\mathrm{ld}\, p, \mathrm{ld}\, p')$ is different from both $\mathrm{lcd}(\mathrm{ld}\, p, \mathrm{ld}\, q)$ and $\mathrm{lcd}(\mathrm{ld}\, p', \mathrm{ld}\, q)$.
$P' = P^*$.
$S' = S \cup \{i_q, s_q\}$.

LEMMA 5.3. $A \subset A' \cup \mathcal{P}(D')$.

PROOF. It suffices to show that if $p \in A$ is such that $\mathrm{ld}\, p$ is a derivative of $\mathrm{ld}\, q$ then the reduction pair $\{p, q\}$ is kept† in D_1. By the hypothesis **H2** of proposition 4.2, if $\{p, q\}$ is not kept in D_1, there exists a differential polynomial $p' \in A$ such that $\mathrm{lcd}(\mathrm{ld}\, p, \mathrm{ld}\, q) = \mathrm{ld}\, p$ is a derivative of $\mathrm{ld}\, p'$. This is impossible for $p, p' \in A$ and $\mathrm{rank}\, A$ is autoreduced. □

LEMMA 5.4. *If $\{p, p'\} \in D^*$ is a reduction pair then $\{p, p'\} \in D_2$.*

PROOF. Assume $\mathrm{rank}\, p > \mathrm{rank}\, p'$. Since $\{p, p'\}$ is a reduction pair we have $\mathrm{lcd}(\mathrm{ld}\, p, \mathrm{ld}\, p') = \mathrm{ld}\, p$. Thus, if the triple $\langle p, q, p' \rangle$ satisfies the hypothesis **H2** of proposition 4.2 then $\mathrm{ld}\, p$ is a derivative of $\mathrm{ld}\, q$ hence $\mathrm{lcd}(\mathrm{ld}\, p, \mathrm{ld}\, q) = \mathrm{ld}\, p = \mathrm{lcd}(\mathrm{ld}\, p, \mathrm{ld}\, p')$ and the pair is kept in D_2. □

LEMMA 5.5. *If v^d is any rank, $F = \{p \in \mathcal{F}(G) \mid \mathrm{rank}\, p \leq v^d\}$ and $F' = \{p \in \mathcal{F}(G') \mid \mathrm{rank}\, p \leq v^d\}$ then $(F_v) : (S \cap R_v)^\infty \subset (F'_v) : (S' \cap R_v)^\infty$.*

PROOF. Denote $F^* = \{p \in A \cup \mathcal{P}(D^*) \cup P^* \mid \mathrm{rank}\, p \leq v^d\}$. By lemmas 5.3 and 5.4 we have $F^* \subset F'$. We thus have two cases to consider.

First case: $P^* \neq P$. More precisely, we assume $q = q_0$ full–rem A with $q_0 \in P$ and we prove that, if $\mathrm{rank}\, q_0 \leq v^d$ then $q_0 \in (F'_v) : (S' \cap R_v)^\infty$.

This comes from lemma 5.3, the fact that the elements of A involved in the reduction process of q_0 have rank lower than or equal to that of q_0 that $H_A \subset S \subset S'$ that $q \in A'$ and $\mathrm{rank}\, q \leq \mathrm{rank}\, q_0$.

† Actually, the lemma is false when p, q are linear homogeneous differential polynomials, in one differential indeterminate u, with constant coefficients and when $\mathrm{ld}\, q = u$. In that case, the equation p is lost. However, this does not matter for $q := u = 0$ makes superfluous all other linear homogeneous differential polynomials in u alone and with constant coefficients.

Second case: $\mathcal{P}(D^*) \neq \mathcal{P}(D)$. More precisely, we assume $q = \Delta(p_0, p_0')$ full–rem A and $\{p_0, p_0'\}$ is a reduction pair with $\operatorname{rank} p_0 > \operatorname{rank} p_0'$. We prove that, if $\operatorname{rank} p_0 \leq v^d$ then $p_0 \in (F_v') : (S' \cap R_v)^\infty$.

Claim: there exists a power product h of elements of $S' \cap R_v$ such that $h\, p_0 \equiv \Delta(p_0, p_0') \pmod{(F_v')}$. Since $\{p_0, p_0'\}$ is a reduction pair, there exists some derivation operator ϕ such that $\Delta(p_0, p_0') = p_0$ full–rem $\phi p_0'$. Thus there exist α, $\beta \in \mathbb{N}$ such that $i_{p_0'}^{\alpha}\, s_{p_0'}^{\beta}\, p_0 \equiv \Delta(p_0, p_0') \pmod{(\phi p_0')}$.

Using lemmas 5.3 and 5.4, the fact that G satisfies **I2** and $\operatorname{rank} p_0' < \operatorname{rank} p_0 \leq v^d$ we see $p_0' \in (F_v') : (S' \cap R_v)^\infty$. Since $\operatorname{ld} \phi p_0' = \operatorname{ld} p_0 \leq v$, we have $\phi p_0' \in (F_v') : (S' \cap R_v)^\infty$. Since $i_{p_0'}$, $s_{p_0'} \in S' \cap R_v$ by **I4** the claim is proved. □

Now $\operatorname{ld} \Delta(p_0, p_0') \leq v$ thus, according to the specifications of Ritt's algorithms of reduction, there exists a power product h of elements of $S' \cap R_v$ such that $h\, \Delta(p_0, p_0') \equiv q \pmod{(F_v')}$. Since $\operatorname{rank} q \leq \operatorname{rank} \Delta(p_0, p_0') < v^d$ we have $q \in F_v'$. Using the claim above, the lemma is proved. □

PROPOSITION 5.6. *$\mathcal{I}(G) : \{i_q, s_q\}^\infty = \mathcal{I}(G')$.*

PROOF. The inclusion $\mathcal{I}(G) : \{i_q, s_q\}^\infty \subset \mathcal{I}(G')$ is a corollary of lemma 5.5. Let's prove the converse inclusion and first that $q \in \mathcal{I}(G)$. For this, we consider three cases:

First case: $q = q_0$ full–rem A with $q_0 \in P$. It is clear for $q_0 \in \mathcal{I}(G)$, $A \subset \mathcal{I}(G)$ and $H_A \subset S$.

Second case: $q = \Delta(p_0, p_0')$ full–rem A when $\{p_0, p_0'\}$ is not a reduction pair. It comes from **I5** and the fact that $A \subset \mathcal{I}(G)$ and $H_A \subset S$.

Third case: $q = \Delta(p_0, p_0')$ full–rem A when $\{p_0, p_0'\}$ is a reduction pair (with $\operatorname{rank} p_0 > \operatorname{rank} p_0'$). It comes from the fact that $p_0' \in \mathcal{I}(G)$ by **I2** (applied to G), $p_0 \in \mathcal{P}(D) \subset \mathcal{I}(G)$, $A \subset \mathcal{I}(G)$ and $H_A \subset S$.

Since $q \in \mathcal{I}(G)$, we have $A' \subset \mathcal{I}(G)$. If $p \in \mathcal{P}(D')$ does not belong to $\mathcal{P}(D)$ then p belongs to a reduction pair $\{p, q\} \in D'$ with $p \in A$; thus $\mathcal{P}(D') \subset \mathcal{I}(G)$. The lemma comes now from the fact that $P' \subset P$ and $S' = S \cup \{i_q, s_q\}$. □

PROPOSITION 5.7. *G' satisfies invariants* **I1**, **I4** *and* **I6**.

PROPOSITION 5.8. *G' satisfies invariant* **I5**.

PROOF. This comes from the fact that all the pairs in D' which are not reduction pairs have the form $\{p, q\}$ with p, $q \in A' \subset \mathcal{I}(G')$, that $\mathcal{I}(G) \subset \mathcal{I}(G')$ and G satisfies **I5**. □

PROPOSITION 5.9. *G' satisfies invariant* **I2**.

PROOF. Invariant **I2** is satisfied for all reduction pairs in D' which are not in D since those pairs have the form $\{p, q\}$ with $\operatorname{rank} p > \operatorname{rank} q$ and $q \in A'$. Invariant **I2** is satisfied for all reduction pairs in D' which belong also to D by lemma 5.5. □

LEMMA 5.6. *If v is any derivative then every $\{p, p'\} \in \operatorname{pairs}(A \cup \{q\})$ which is such that $\operatorname{lcd}(\operatorname{ld} p, \operatorname{ld} p') < v$ is nearly solved by G'.*

PROOF. By induction on v. Basis of the induction: if v is less than or equal to the

minimum v_0 of $\mathrm{lcd}(\mathrm{ld}\,p, \mathrm{ld}\,p')$ for all $\{p, p'\} \in \mathrm{pairs}(A \cup \{q\})$ then the lemma is trivially satisfied. In the general case, let us assume that $v > v_0$ and (induction hypothesis) that every $\{p, p'\} \in \mathrm{pairs}(A \cup \{q\})$ such that $\mathrm{lcd}(\mathrm{ld}\,p, \mathrm{ld}\,p') < v$ is nearly solved by G'.

First case: $p \neq q$ and $p' \neq q$.

First subcase: if $\{p, p'\}$ is solved by G then, by lemma 5.5, the pair $\{p, p'\}$ is solved by G'. It is thus nearly solved by G' according to **A1**.

Second subcase: if $\{p, p'\} \in D^*$ then either it belongs to D' or it does not. In the former case, it is nearly solved by G' according to **A2**. In the latter, the triple $\langle p, q, p' \rangle$ satisfies the hypotheses **H1** to **H3** of proposition 4.2 and $\mathrm{lcd}(\mathrm{ld}\,p, \mathrm{ld}\,p')$ is a *proper* derivative of both $\mathrm{lcd}(\mathrm{ld}\,p, \mathrm{ld}\,q)$ and $\mathrm{lcd}(\mathrm{ld}\,p', \mathrm{ld}\,q)$. By the induction hypothesis and **A3**, the pair $\{p, p'\}$ is nearly solved by G'.

Third subcase: if $\{p, p'\} = \{p_0, p'_0\} \in D$ and $q = \Delta(p_0, p'_0)$ full–rem A then $\{p, p'\}$ is solved by the differential system $A \cup \{q\} = 0,\ S' \neq 0$ (specifications of Ritt's reduction algorithms). By lemma 5.3 and the fact that $q \in A'$, the pair $\{p, p'\}$ is solved by G'. It is thus nearly solved by G' according to **A1**.

Second case: the pair is formed by q and some $p \in A$.

First subcase: If $\{p, q\} \in D_1 \subset D'$ then $\{p, q\}$ is nearly solved by G' according to **A2**.

Second subcase: If $\{p, q\} \notin D'$ then either it is solved by G' according to proposition 4.1 or there exists a pair $\{p', q\} \in D_1 \subset D'$ such that the triple $\langle q, p', p \rangle$ satisfies the hypotheses **H1** to **H3** of proposition 4.2. In this latter case, $\mathrm{lcd}(\mathrm{ld}\,p, \mathrm{ld}\,q)$ is a derivative of $\mathrm{lcd}(\mathrm{ld}\,p, \mathrm{ld}\,p')$ and, according to the first case considered above, the pair $\{p, p'\} \in \mathrm{pairs}(A)$ is solved by G'. According to **A3** the pair $\{p, q\}$ is nearly solved by G'. □

PROPOSITION 5.10. *G' satisfies* **I3**.

PROOF. This is a consequence of lemma 5.6 and of the fact that $A' \subset A \cup \{q\}$. □

5.3. SPLITTINGS

When the completion process enlarges A with a new equation $q = 0$, the set S is also enlarged with two inequations $i_q \neq 0$, $s_q \neq 0$. In order not to loose solutions of the current quadruple, we must also consider its solutions which cancel the initial or the separant of q. This we do by splitting cases as in Seidenberg's elimination algorithms. The argument relies on the differential analogue of Hilbert's theorem of zeros (theorem 3.1).

LEMMA 5.7. *If $A = 0,\ S \neq 0$ is a differential system and h is a differential polynomial then every solution of $A = 0,\ S \neq 0$ is a solution of $A \cup \{h\} = 0,\ S \neq 0$ or a solution of $A = 0,\ S \cup \{h\} \neq 0$ and conversely.*

COROLLARY 5.1. $\sqrt{[A] : S^\infty} = \sqrt{[A, h] : S^\infty} \cap \sqrt{[A] : (S \cup \{h\})^\infty}$.

PROOF. The corollary comes from lemma 5.7 and the corollary 3.1 of the theorem of zeros. □

Let's come back to the quadruples G, G' and to the differential polynomial q of section 5.2. Denote $\mathrm{rank}\,q = v^d$. Let $q_i = q - i_q\, v^d$ and $q_s = d\,q - v\, s_q$. Denote

$$\begin{aligned} G_i &= \langle A, D^*, P^* \cup \{i_q, q_i\}, S \rangle, \\ G_s &= \langle A, D^*, P^* \cup \{s_q, q_s\}, S \cup \{i_q\} \rangle. \end{aligned}$$

PROPOSITION 5.11. $\mathcal{I}(G) = \mathcal{I}(G_i) \cap \mathcal{I}(G_s) \cap \mathcal{I}(G')$.

PROOF. Using lemma 5.7, every solution of $\mathcal{F}(G) = 0,\ S \neq 0$ is a solution of $\mathcal{F}(G) \cup \{i_q\} = 0,\ S \neq 0$ (denoted Σ_i) or a solution of $\mathcal{F}(G) = 0,\ S \cup \{i_q\} \neq 0$ and conversely. Using lemma 5.7 again, every solution of the latter system is a solution of $\mathcal{F}(G) \cup \{s_q\} = 0,\ S \cup \{i_q\} \neq 0$ (denoted Σ_s) or a solution of $\mathcal{F}(G) = 0,\ S \cup \{i_q, s_q\} \neq 0$ (denoted Σ') and conversely.

The system Σ_i (respectively Σ_s) has the same solutions as the quadruple G_i (respectively G_s). By proposition 5.6, the system Σ' has the same solutions as the quadruple G'.

The proposition follows now from corollary 5.1. □

Observe that if a differential polynomial h does not divide zero modulo $\sqrt{[\Sigma]}$ then there is no need of splitting on h since in that case $\sqrt{[\Sigma]} = \sqrt{[\Sigma] : h^\infty}$. This is the case for instance if $h \in K$ $(h \neq 0)$.

5.3.1. THE SYSTEM G_i SATISFIES ALL THE INVARIANTS

Note: the proofs are simpler variants of the ones given for G' in section 5.2. They rely on the fact that $q \in (i_q, q_i)$ and $\operatorname{rank} i_q, q_i < \operatorname{rank} q$. *Therefore, since* $q \in (s_q, q_s)$ *and* $\operatorname{rank} s_q, q_s < \operatorname{rank} q$ *the same proofs hold for* G_s *; if* $q = 0$ *then they hold for the quadruple* $G^* = \langle A, D^*, P^*, S \rangle$ *too.*

LEMMA 5.8. *If* v^d *is any rank,* $F = \{p \in \mathcal{F}(G) \mid \operatorname{rank} p \leq v^d\}$ *and* $F_i = \{p \in \mathcal{F}(G_i) \mid \operatorname{rank} p \leq v^d\}$ *then* $(F_v) : (S \cap R_v)^\infty \subset (F_{i,v}) : (S_i \cap R_v)^\infty$.

PROOF. We only have to consider two cases.

First case: $P^* \neq P$. More precisely, we assume $q = q_0$ full–rem A with $q_0 \in P$ and we prove that, if $\operatorname{rank} q_0 \leq v^d$ then $q_0 \in (F_{i,v}) : (S_i \cap R_v)^\infty$.

This comes from the fact that the elements of A involved in the reduction process of q_0 have rank lower than or equal to that of q_0, the fact that $H_A \subset S \subset S'$ and the fact that $q \in (i_q, q_i) \subset (F_{i,v})$.

Second case: $\mathcal{P}(D^*) \neq \mathcal{P}(D)$. More precisely, we assume $q = \Delta(p_0, p_0')$ full–rem A and $\{p_0, p_0'\}$ is a reduction pair with $\operatorname{rank} p_0 > \operatorname{rank} p_0'$. We prove that, if $\operatorname{rank} p_0 \leq v^d$ then $p_0 \in (F_{i,v}) : (S_i \cap R_v)^\infty$.

Claim: there exists a power product h of elements of $S_i \cap R_v$ such that $h\, p_0 \equiv \Delta(p_0, p_0')$ (mod $(F_{i,v})$). Since $\{p_0, p_0'\}$ is a reduction pair, there exists some derivation operator ϕ such that $\Delta(p_0, p_0') = p_0$ full–rem $\phi p_0'$. Thus there exist $\alpha, \beta \in \mathbb{N}$ such that $i_{p_0'}^\alpha\, s_{p_0'}^\beta\, p_0 \equiv \Delta(p_0, p_0')$ (mod $(\phi p_0')$).

Using the fact that G satisfies **I2** and $\operatorname{rank} p_0' < \operatorname{rank} p_0 \leq v^d$ we see $p_0' \in (F_{i,v}) : (S_i \cap R_v)^\infty$. Since $\operatorname{ld} \phi p_0' = \operatorname{ld} p_0 \leq v$, we have $\phi p_0' \in (F_{i,v}) : (S_i \cap R_v)^\infty$. Since $i_{p_0'}, s_{p_0'} \in S_i \cap R_v$ by **I4** the claim is proved. □

Now $\operatorname{ld} \Delta(p_0, p_0') \leq v$ thus, according to the specifications of Ritt's algorithms of reduction, there exists a power product h of elements of $S_i \cap R_v$ such that $h\, \Delta(p_0, p_0') \equiv q$ (mod $(F_{i,v})$). Since $\operatorname{rank} i_q, q_i < \operatorname{rank} \Delta(p_0, p_0') < v^d$ and $q \in (i_q, q_i)$ we have $q \in (F_{i,v})$. Using the claim above, the lemma is proved. □

PROPOSITION 5.12. G_i *satisfies invariants* **I1**, **I4** *and* **I6**.

PROPOSITION 5.13. *G_i satisfies invariant* **I5**.

PROOF. This comes from the fact that $\mathcal{I}(G) \subset \mathcal{I}(G_i)$ and G satisfies invariant **I5**. □

PROPOSITION 5.14. *G_i satisfies invariant* **I2**.

PROOF. This proposition is a corollary of lemma 5.8. □

PROPOSITION 5.15. *G_i satisfies invariant* **I3**.

PROOF. Because of lemma 5.8, all the pairs in D solved by G which still belong to D^* are also solved by G_i.

It suffices thus to show that if $q = \Delta(p_0, p_0')$ full–rem A then $\{p_0, p_0'\}$ is solved by G_i. This pair is solved by the differential system $A \cup \{q\} = 0,\ S_i \neq 0$. Since $q \in (i_q, q_i) \subset \mathcal{F}(G_i)$ and $\operatorname{rank} i_q, q_i < \operatorname{rank} q$ the pair $\{p_0, p_0'\}$ is solved by G_i. □

5.4. PROOF OF THEOREM 5.1

The axioms below define a partial ordering among quadruples. Let $G = \langle A', D', P', S' \rangle$ and $G = \langle A, D, P, S \rangle$ be two quadruples such that $\operatorname{rank} A$ and $\operatorname{rank} A'$ are autoreduced.

O1 If $A' < A$ then G' is said to be less than G.
O2 If $A' = A$ and D' has fewer elements than D then G' is said to be less than G.
O3 Assume $A' = A$ and $D' = D$. If there exists a differential polynomial $p \in P$ and a finite set E (possibly empty) of differential polynomials all less than p such that $P' = P \setminus \{p\} \cup E$ then G' is said to be less than G.

LEMMA 5.9. *The ordering defined above is artinian (i.e. every strictly decreasing sequence of quadruples is finite).*

PROOF. We assume there exists an infinite strictly decreasing sequence (G_n) of quadruples and seek a contradiction. Denote $G_n = \langle A_n, D_n, P_n, S_n \rangle$. Since the ordering on autoreduced sets of differential polynomials is artinian, (G_n) contains an infinite subsequence (G_{i_n}) of quadruples such that all A_i's have the same rank. By a similar argument, (G_{i_n}) contains itself an infinite subsequence (G_{j_n}) of quadruples such that all A_j's have the same rank and all D_j have the same number of elements. By an argument of graph theory (König, 1950, Satz 6.6) (i.e. every infinite locally finite† tree contains a branch of infinite length) there exists (taken from the P_j) an infinite strictly decreasing sequence of differential polynomials. This cannot be for rankings are well–orderings. This final contradiction proves the lemma. □

PROOF OF THEOREM 5.1. Differential systems are represented using quadruples. Let $G = \langle A, D, P, S \rangle$ be a quadruple of R satisfying the invariant properties **I1** up to **I6**. The initial system, coded $\langle \emptyset, \emptyset, P_0, S_0 \rangle$ satisfies them. We assume inductively that the theorem holds for any quadruple $G' < G$ satisfying the invariants. The induction is transfinite (lemma 5.9).

† A tree is said to be locally finite if only finitely many branches start from each of its nodes.

Assume D and P are empty (basis of the induction). Applying the method described in section 5.1, one decides whether the differential system $A = 0,\ S \neq 0$ is consistent or not. It is discarded if it is inconsistent else one gets a regular differential system $\bar{A} = 0,\ \bar{S} \neq 0$ such that $\mathcal{I}(G) = [\bar{A}] : \bar{S}^{\infty}$.

Assume D or P not empty (general case). Pick either a differential polynomial $q_0 \in P$ or a pair $\{p_0, p_0'\} \in D$. In the former case, let $P^* = P \setminus \{q_0\}$ let $D^* = D$ and $q = q_0$ full–rem A. In the latter let $P^* = P$, let $D^* = D \setminus \{\{p_0, p_0'\}\}$ and $q = \Delta(p_0, p_0')$ full–rem A.

Assume $q = 0$ and denote $G^* = \langle A, D^*, P^*, S\rangle$. The quadruple G^* satisfies the invariants (cf. the note in section 5.3.1). Since $\mathcal{I}(G) = \mathcal{I}(G^*)$ and $G^* < G$ by **O2** or **O3** the quadruple G^* can be disposed of by induction.

Assume $q \neq 0$. Let G' be any quadruple obtained following section 5.2. The quadruple G' satisfies the invariants and is less than G according to **O1**. It can be disposed of by induction.

Denote $\operatorname{rank} q = v^d$. Let $q_i = q - i_q\, v^d$ and $q_s = d\, q - v\, s_q$. Form two quadruples G_i and G_s as in section 5.3. Since $q_i,\ q_s,\ i_q,\ s_q < q$ the quadruples G_i and G_s are both less than G according to **O2** or **O3**. They satisfy the invariants. They can be disposed of by induction.

The proof of the theorem is now completed by proposition 5.11. □

5.5. About the implementation

The following pseudo–code furnishes the method carried out by implementation of the Rosenfeld–Gröbner algorithm for constructing D' from D_0 and D^*. Note the first loop keeps the pairs which could be discarded using the analogue of Buchberger's first criterion (proposition 4.1). Let's pseudo–quote Becker and Weispfenning (1991), page 231: if two or more pairs have the same least common derivative of leaders, so that there is a choice as to which one(s) should be deleted, then it is advantageous to try and keep one which will be discarded later by the analogue of Buchberger's first criterion. That way, one eventually gets rid of all of them.

$D_1 := \emptyset$
while $D_0 \neq \emptyset$ **do**
  pick a pair $\{p, q\} \in D_0$
  $D_0 := D_0 \setminus \{\{p, q\}\}$
  if p, q are linear homogeneous differential polynomials in one differential indeterminate and with constant coefficients or if there does not exist any pair $\{p', q\} \in D_0 \cup D_1$ such that the triple $\langle q, p', p\rangle$ satisfies the hypotheses **H1** to **H3** of proposition 4.2 **then**
    $D_1 := D_1 \cup \{\{p, q\}\}$
  fi
od
Remove from D_1 all pairs $\{p, q\}$ such that p, q are linear homogeneous differential polynomials in one differential indeterminate and with constant coefficients
Let D_2 be the subset of all the pairs $\{p, p'\} \in D^*$ such that $\langle p, q, p'\rangle$ does not satisfy the hypotheses **H1**, **H2** and **H3** of proposition 4.2 or $\operatorname{lcd}(\operatorname{ld} p, \operatorname{ld} p')$ is equal to $\operatorname{lcd}(\operatorname{ld} p, \operatorname{ld} q)$ or $\operatorname{lcd}(\operatorname{ld} p', \operatorname{ld} q)$.
$D' := D_1 \cup D_2$.

5.5.1. Avoiding splittings

As stated in section 5.3, if a differential polynomial h does not divide zero modulo $\mathfrak{p} = \sqrt{[P_0] : S_0^\infty}$ then there is nod need of splitting on h.

Here is a way to apply this idea: before computing a decomposition of $\mathfrak{p}$ w.r.t. to some desired ranking $\mathcal{R}$ first compute a decomposition of $\mathfrak{p}$ w.r.t. another ranking $\mathcal{R}'$ chosen heuristically so that the representation involves only few components. Afterwards, use it while computing the decomposition of $\mathfrak{p}$ w.r.t. $\mathcal{R}$: each time the algorithm is about to split computations between (say) $h = 0$ and $h \neq 0$, test whether h is a divisor of zero modulo $\mathfrak{p}$. If h is proven not to be a divisor of zero, the splitting can be avoided and the branch $h = 0$ discarded. The differential polynomial $h \in \mathfrak{p}$ if and only if the branch $h \neq 0$ only leads to inconsistent regular differential systems. Such branches can therefore always be detected and discarded. If h is proven to be a divisor of zero or if nothing can be proven then the splitting must be generated.

The method above is particularly interesting when $\mathfrak{p}$ can be represented by a unique regular differential system $C = 0$ which is orthonomic (i.e. all the initials and separants of C belong to the base field of R). In that case (which turns out to happen quite often) $\mathfrak{p} = [C]$ is prime. No differential polynomial can divide zero modulo a prime ideal.

The implementation of the Rosenfeld–Gröbner algorithm in the `diffalg` package applies this improvement.

5.5.2. Reducing the inequations

It is interesting to keep S partially reduced w.r.t. A for inequations are usually small differential polynomials (for problems which can be handled): reducing them is not very CPU expensive and can point out inconsistencies. Note invariant **I4** must then be changed and proofs modified.

5.5.3. Linear equations

If our implementation is given linear differential polynomials then the analogue of Buchberger's second criterion always applies ; moreover, no splittings are generated. In particular, if the given system is a set of non differential polynomials, coded as differential polynomials linear, homogeneous, in one differential indeterminate with constant coefficients then this implementation behaves exactly (up to the implementation overhead) as a good implementation of the Buchberger's algorithm (the one of Gebauer and Möller (1988)).

6. Computing canonical representatives

According to the results of the previous sections any regular differential ideal may be presented by a regular differential system and by its associated Gröbner basis. This was the choice in (Boulier *et al.*, 1995). This representation is not only heavy but also non canonical for different regular differential systems may define the same regular differential ideal. In this section, we define better representatives of regular differential ideals that we call *characteristic presentations*. Theorem 6.3 then shows how to compute *characteristic presentations* from regular differential systems. The Rosenfeld–Gröbner algorithm (theorem 6.4) can then be stated.

6.1. Characteristic presentations

The implication from left to right in the proof of the following theorem was already proven in Boulier *et al.* (1995), lemma 5, page 162.

Theorem 6.1. *(canonicity theorem)*
If $A_1 = 0,\ S_1 \neq 0$ *and* $A_2 = 0,\ S_2 \neq 0$ *are two regular differential systems of some differential polynomial ring* R *then* $[A_1] : S_1^\infty = [A_2] : S_2^\infty$ *iff* $(A_1) : S_1^\infty = (A_2) : S_2^\infty$.

Proof. The implication from left to right. We assume (**H1**) that $[A_1] : S_1^\infty = [A_2] : S_2^\infty$ and (**H2**) that $(A_1) : S_1^\infty \neq (A_2) : S_2^\infty$. We seek a contradiction. Denote $B_1 = p_1 < \cdots < p_n$ and $B_2 = q_1 < \cdots < q_m$ the Gröbner bases associated to the algebraic regular ideals. Apply **H2** and assume $B_1 < B_2$. There exists an index $i \leq n$ such that p_i is not reduced to zero by B_2 and $p_j = q_j$ $(1 \leq j < i)$. By **H1** we have $p_i \in [A_2] : S_2^\infty$. By the corollary below Lazard's lemma and the fact that $p_j = q_j$ $(1 \leq j < i)$, the differential polynomial p_i is partially reduced w.r.t. $q_1, \ldots, q_{i-1}$. It is also partially reduced w.r.t. $q_i, \ldots, q_m$ for $\mathrm{ld}\, p_i \leq \mathrm{ld}\, q_i, \ldots, \mathrm{ld}\, q_m$ and B_2 is a Gröbner basis w.r.t. an elimination ordering defined by a ranking. By the corollary of Lazard's lemma, p_i is partially reduced w.r.t. A_2. By Rosenfeld's lemma $p_i \in (A_2) : S_2^\infty$. Contradiction.

The implication from right to left now. We assume (**H1**) that $(A_1) : S_1^\infty = (A_2) : S_2^\infty$ and (**H2**) that $p \in [A_1] : S_1^\infty$. We claim $p \in [A_2] : S_2^\infty$. Let $q = (p \text{ partial–rem } A_2)$. There exists thus a power product h of elements of S_2 such that $h\, p \equiv q$ modulo $[A_2]$. According to **H1** we have $A_2 \subset [A_1] : S_1^\infty$ thus $h\, p \equiv q$ modulo this latter ideal. Because of **H2** we have $q \in [A_1] : S_1^\infty$. By the corollary below Lazard's lemma and **H1** again q is partially reduced w.r.t. A_1. By Rosenfeld's lemma, it belongs to $(A_1) : S_1^\infty = (A_2) : S_2^\infty$. Let's summarize: $(p \text{ partial–rem } A_2) \in (A_2) : S_2^\infty$. By the corollary (point 2) below Rosenfeld's lemma, $p \in [A_2] : S_2^\infty$. □

In the next definition, the only purpose of conditions **C2** and **C3** is to ensure the canonicity property of characteristic presentations.

Definition 6.1. *(characteristic presentations)*
Let $A = 0,\ S \neq 0$ *be a consistent regular differential system of a differential polynomial ring* R *for a ranking* $\mathcal{R}$ *and* B *be the Gröbner basis associated to the regular algebraic ideal* $(A) : S^\infty$*, computed in dimension zero.*

A differentially triangular set $C = p_1 < \cdots < p_n$ *is called a* characteristic presentation *of the regular differential ideal* $[A] : S^\infty$ *if it satisfies the following conditions:*

C1 *for any* $p \in R$ *we have* $p \in [A] : S^\infty$ *if and only if* $(p \text{ full–rem } C) = 0$,
C2 *the set* C *is a minimal differentially triangular subset of* B,
C3 *if* $C' = p'_1 < \cdots < p'_n$ *is another set which satisfies* **C1** *and* **C2** *and* $i \leq n$ *is the smallest index such that* $p_i \neq p'_i$ *then the leading term*† *of* p_i *is less than the one of* p'_i.

A characteristic presentation C of a regular differential ideal $[A] : S^\infty$ is not exactly a characteristic set in the sense of Ritt of the ideal since it is not autoreduced. However,

† The term ordering used is the elimination one given by the ranking.

it has the same rank as the characteristic sets of the ideal and it could easily be made autoreduced by performing a few reductions. We have $[A] : S^\infty = [C] : H_C^\infty$. Remark also that a characteristic set of $[A] : S^\infty$ is not necessarily a characteristic presentation of this ideal since it may reduce to zero more than the ideal.

THEOREM 6.2. *(canonicity of characteristic presentations)*
If it exists, the characteristic presentation of a regular differential ideal is a canonical representative of this ideal (it only depends on the ideal and on the ranking).

PROOF. It is an easy consequence of theorem 6.1, conditions **C2** and **C3** and the canonicity property of reduced Gröbner bases. □

Here is an algorithm to extract a minimal differential triangular subset C from the associated Gröbner basis B of a consistent regular differential system $A = 0,\ S \neq 0$: for each derivative v which is the leader of some element of A, pick from B a differential polynomial with leader v and with minimal degree in v (among the elements of B whose leader is v).

If C is such a set of differential polynomials then C is a triangular subset of B. By Lazard's lemma, a derivative v is the leader of some element of B if and only if it is the leader of some element of A. Thus C is a minimal triangular subset of B. Since A is differentially triangular, so is C.

LEMMA 6.1. *(algorithmic test for condition* **C1***)*
Let $A = 0,\ S \neq 0$ be a consistent regular differential system of a differential polynomial ring R for a ranking $\mathcal{R}$ and B be its associated Gröbner basis.
If C is a minimal differentially triangular subset of B and no element of H_C is a divisor of zero modulo $(A) : S^\infty$ then C satisfies **C1**.

PROOF. By the hypothesis and the corollary (point 3) below Rosenfeld's lemma, no element of H_C is a divisor of zero modulo $[A] : S^\infty$. Since $C \subset [A] : S^\infty$, the set C only reduces to zero elements of this differential ideal.

By the corollary of Lazard's lemma, a derivative v is the leader of some element of C if and only if it is the leader of some element of B. Thus if p is a non zero differential polynomial reduced in the sense of Ritt w.r.t. C then p is partially reduced w.r.t. A on one hand; on the other hand, the terms of p are not divisible by the leading terms of the elements of B thus p is irreducible by the Gröbner basis B and $p \notin (B) = (A) : S^\infty$. By Rosenfeld's lemma, $p \notin [A] : S^\infty$. Therefore, every element of $[A] : S^\infty$ is reduced to zero by C. □

LEMMA 6.2. *Let $A = 0,\ S \neq 0$ be a consistent regular differential system of a differential polynomial ring R for a ranking $\mathcal{R}$, B be its associated Gröbner basis and C be a minimal differentially triangular subset of B.*
An element $h \in H_C$ is a divisor of zero modulo (B) if and only if the reduced Gröbner basis of $(B) : h^\infty$ (computed in dimension zero) is different from B.

PROOF. First note $h \notin (B)$ for h is irreducible by B. Now, the ideal (B) is radical by Lazard's lemma; the prime ideals which are minimal over $(B) : h^\infty$ are the minimal prime ideals of (B) which do not contain h; a polynomial h is a divisor of zero modulo a radical

ideal $\mathfrak{r}$ if and only if it belongs to some but not all of the prime ideals which are minimal over $\mathfrak{r}$; reduced Gröbner bases are canonical representatives of the ideals they generate. □

THEOREM 6.3. *(computing characteristic presentations)*
If $A = 0,\ S \neq 0$ is a consistent regular differential system for a ranking $\mathcal{R}$ of a differential polynomial ring R then it is possible to compute finitely many regular differential ideals given by characteristic presentations C_i $(i = 1, \ldots, n)$ such that

$$[A] : S^\infty \quad = \quad [C_1] : H_{C_1}^\infty \cap \cdots \cap [C_n] : H_{C_n}^\infty. \tag{6.1}$$

This decomposition does not contain redundant components w.r.t. $[A] : S^\infty$. Operations needed are addition, multiplication and equality test with zero in the base field of R.

PROOF. Denote $\mathfrak{r} = [A] : S^\infty$ and B the Gröbner basis associated to $(A) : S^\infty$. The paragraph above lemma 6.1 shows how to extract minimal differentially triangular subsets C from B. Lemmas 6.1 and 6.2 show how to test if one of them is a characteristic presentation of $\mathfrak{r}$.

The proof is an induction on the number of prime components of (B). If (B) is prime and C is a minimal differentially triangular subset of B then no element of H_C divides zero modulo (B) hence C satisfies **C1**.

Assume $(A) : S^\infty$ admits no characteristic presentation. Let C be a minimal differentially triangular subset of B and $p \in H_C$ be a divisor of zero modulo (B). We have $\mathfrak{r} = \mathfrak{r}_1 \cap \mathfrak{r}_2$ where $\mathfrak{r}_1 = \sqrt{[A \cup \{p\}] : S^\infty}$ and $\mathfrak{r}_2 = \mathfrak{r} : p^\infty$.

Both $\mathfrak{r}_1$ and $\mathfrak{r}_2$ have fewer components than $\mathfrak{r}$. The latter ideal is a regular differential system whence is disposed of by induction. Using theorem 5.1, one can compute a representation of $\mathfrak{r}_1$ as an intersection of regular differential ideals. Moreover, one can manage to compute an irredundant intersection by using the technique described in paragraph 5.5.1 □

The method described in the proof above is the one applied in the `diffalg` package. It is not very efficient. The `Lextriangular` algorithm of Lazard (1992) (see also Moreno Maza (1997)) would be much more efficient and would even permit us to completely avoid the use of Gröbner bases.

6.1.1. AN EXAMPLE

Some regular differential ideals (quite unusual in practice) have no characteristic presentation. An example is given by the following triangular set A, for the elimination ordering $x_5 > \cdots > x_1$. The example is purely algebraic but can be easily transformed into a differential one.

$$A \begin{cases} p_3 &= ((x_2^2 + x_1)x_5 + x_4^2 + x_3)(x_2x_5 + x_4), \\ p_2 &= x_4(x_4^2 + x_3), \\ p_1 &= x_2(x_2^2 + x_1). \end{cases}$$

Below is the reduced Gröbner basis B (computed over $\mathbb{Q}$) of the ideal $(A) : S_A^\infty$ for the elimination ordering $x_5 > \cdots > x_1$.

$$B \left\{ \begin{array}{lcl} b_5 & = & x_5, \\ b_4 & = & x_4(x_4^2 + x_3), \\ b_3 & = & x_1 x_4^2 + (x_2^2 + x_1)x_3, \\ b_2 & = & x_2 x_4, \\ b_1 & = & x_2(x_2^2 + x_1). \end{array} \right.$$

It contains only one minimal triangular subset $\{b_1, b_2, b_5\}$, which is not a characteristic presentation of $\mathfrak{r} = (A) : S_A^\infty$ since the initial x_2 of b_2 is a divisor of zero modulo $\mathfrak{r}$.

Moreover, $\mathfrak{r}$ contains no differentially triangular subset satisfying **C1**. Let us assume the existence of such a set C and seek a contradiction. This set reduces b_2 to zero. So it contains either a polynomial $p \in \mathfrak{r} \cap K[x_1, x_2]$ of degree 1 in x_2 (impossible) or a polynomial $p \in \mathfrak{r} \cap K[x_1, \ldots, x_4]$ of degree 1 in x_4, say $p = a_1\, x_4 + a_0$. In this latter case, $p \in (b_1, b_2)$ is a multiple of x_2 and so is a_1 which is thus a divisor of zero modulo $\mathfrak{r}$ (contradiction).

According to theorem 6.3, the regular ideal can be decomposed as an intersection of regular ideals which admit characteristic presentations. The ideal $\mathfrak{r} = (A) : S_A^\infty$ is decomposed as the intersection $\mathfrak{r} = \mathfrak{r}_1 \cap \mathfrak{r}_2$ where $\mathfrak{r}_1 = \mathfrak{r} : x_2^\infty$ and $\mathfrak{r}_2 = \mathfrak{r} + (x_2)$. Here are characteristic presentations of these two ideals.

$$\mathfrak{r}_1 \left\{ \begin{array}{l} x_5, \\ x_4, \\ x_2^2 + x_1\ ; \end{array} \right. \qquad \mathfrak{r}_2 \left\{ \begin{array}{l} x_5, \\ x_4^2 + x_3, \\ x_2. \end{array} \right.$$

6.2. The main theorem

Theorem 6.4. *(the Rosenfeld–Gröbner algorithm)*

If $P_0 = 0$, $S_0 \neq 0$ is a differential system of a differential polynomial ring R then it is possible to compute finitely many regular differential systems given by characteristic presentations C_i $(i = 1, \ldots, n)$ such that

$$\mathfrak{p} = \sqrt{[P_0] : S_0^\infty} \quad = \quad [C_1] : H_{C_1}^\infty \cap \cdots \cap [C_n] : H_{C_n}^\infty. \tag{6.2}$$

Operations needed are addition, multiplication, differentiation and equality test with zero in the base field of R. This decomposition may contain components redundant w.r.t. $\mathfrak{p}$. It provides a normal simplifier for the equivalence relation modulo this ideal i.e.

$$p \in \mathfrak{p} \iff p \text{ full–rem } C_i = 0 \quad (1 \leq i \leq n).$$

Proof. The first claim is proven by theorems 5.1 and 6.3. The property of being a normal simplifier is an immediate consequence of condition **C1** of definition 6.1. □

By applying a primary decomposition algorithm over the regular decomposition of $\mathfrak{p}$, one would get a (redundant) differential prime decomposition of $\mathfrak{p}$ (see a remark below theorem 4.2). This algorithm would probably be much more efficient than the characteristic sets algorithm of Ritt (1950) and would provide the same result.

Remark that decomposition of radical differential ideals in regular differential ideals does not depend on the base field whereas the decomposition in prime differential ideals does.

The computed representation of a radical differential ideal $\mathfrak{p}$ is not canonical because of the regular components which may be redundant w.r.t. $\mathfrak{p}$. Moreover, even if $\mathfrak{r}$ is a regular differential ideal which is not redundant w.r.t. $\mathfrak{p}$, there may exist among the minimal differential prime components of $\mathfrak{r}$ some differential ideals redundant w.r.t. $\mathfrak{p}$.

Deciding whether a regular differential ideal is redundant or not w.r.t. a decomposition of type (6.2) is related to a famous open problem in differential algebra (Kolchin, 1973, page 166).

The computed representation of $\mathfrak{p}$ is therefore not a canonical simplifier for the equivalence relation modulo $\mathfrak{p}$. However, being a normal simplifier is enough for deciding whether two given differential polynomials p and q are equivalent modulo $\mathfrak{p}$ for $p \equiv q$ if and only if $p - q \equiv 0$ modulo $\mathfrak{p}$.

In the case of differential ideals generated by only one differential polynomial, the problem of the computation of the minimal prime decomposition is solved by the Low Power Theorem (Kolchin, 1973, chapter IV, section 15), much studied by Ritt (1950) and Levi (1945). See also Hubert (1997) for an implementation of this theorem based on the Rosenfeld–Gröbner algorithm and a generalization of it to regular differential decompositions.

7. Formal power series solutions of regular differential ideals

The content of this section is a variant of Seidenberg's results (Seidenberg, 1956, theorem 11, page 59) (Seidenberg, 1958, Embedding theorem) and (Seidenberg, 1969). We give proofs for the sake of completeness and because the hypotheses of Seidenberg's theorems are slightly different from ours. This section was also partly inspired by (Péladan-Germa, 1997).

Let $A = 0,\ S \neq 0$ be a differential system of a differential polynomial ring $R = K\{u_1, \ldots, u_n\}$ and R_0 be the ring of the differential polynomials partially reduced w.r.t. A.

Let ϕ_0 be any algebraic solution of $A = 0,\ S \neq 0$, viewed as a non differential system of R_0. The solution ϕ_0 defines a K–algebra homomorphism $\phi_0 : R_0 \to G$ where G is some field extension of K. Note ϕ_0 maps the elements of S to nonzero elements of G.

We prove first (proposition 7.1) that ϕ_0 extends to a unique solution ϕ of the differential ideal $[A] : S^\infty$. Then we prove ϕ is uniquely defined (proposition 7.2) and provides the coefficients of a formal power series solution of $[A] : S^\infty$ (proposition 7.3).

Let $v \in \Theta U$ be a derivative and let $p = v$ partial–rem A. There exist then a power product h of elements of S and a differential polynomial $p \in R_0$ such that

$$h\, v \quad \equiv \quad p \ (\mathrm{mod}\ [A]). \tag{7.1}$$

We define $\phi(v) = \phi_0(p)/\phi_0(h)$.

LEMMA 7.1. *The map ϕ is well defined (i.e. the definition does not depend on the differential polynomials h and p).*

PROOF. Let h, p be the differential polynomials defined in congruence (7.1). Assume there exists another power product h' of elements of S and another differential polynomial $p' \in R_0$ such that $h'\, v \equiv p'$ (mod $[A]$). We have $hp' - h'p \in [A] : S^\infty \cap R_0$. Since $A = 0,\ S \neq 0$ is a regular differential system, Rosenfeld's lemma applies and $hp' - h'p \in (A) : S^\infty$ whence $\phi_0(p)/\phi_0(h) = \phi_0(p')/\phi_0(h')$. □

The map ϕ extends to a unique K–algebra homomorphism $K[\Theta U] \to G$ that we denote ϕ also.

PROPOSITION 7.1. *If $p \in [A] : S^\infty$ then $\phi(p) = 0$.*

PROOF. First observe that if p is a proper derivative of some element of A then there exists a possible partial reduction such that p partial–rem $A = 0$; according to lemma 7.1 we have $\phi(p) = 0$.

Now, if $p \in [A] : S^\infty$ then $\bar{p} = (p \text{ partial–rem } A) \in (A) : S^\infty$ by Rosenfeld's lemma whence $\phi(\bar{p}) = 0$. Moreover, there exists a power product h of elements of S such that $h\,p - \bar{p}$ is equal to a linear combination of proper derivatives of elements of A ; thus $\phi(p) = \phi(\bar{p})/\phi(h) = 0$. □

PROPOSITION 7.2. *The homomorphism ϕ is the unique K–algebra homomorphism extending ϕ_0 which maps $[A] : S^\infty$ to zero.*

PROOF. Assume there exists another homomorphism ϕ' extending ϕ_0 which maps $[A]:S^\infty$ to zero. Let $v \in \Theta U$ be a derivative and h, p be the differential polynomials defined in congruence (7.1). We have $\phi'(v) = \phi_0(p)/\phi_0(h) = \phi(v)$. □

If $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m$ is a multi–index, and $\eta = (\eta_1, \ldots, \eta_m) \in G^m$ then we denote $\alpha\,! = \prod_{i=1}^m \alpha_i\,!$ and $(x-\eta)^\alpha = (x_1 - \eta_1)^{\alpha_1} \cdots (x_m - \eta_m)^{\alpha_m}$ and $\delta^\alpha = \delta_1^{\alpha_1} \cdots \delta_m^{\alpha_m}$. To each differential indeterminate $u \in U$ we can associate a formal power series (η is the point of expansion of the series):

$$\bar{u} = \sum_{\alpha \in \mathbb{N}^m} \frac{\phi(\delta^\alpha u)}{\alpha!}(x-\eta)^\alpha.$$

The derivations defined over R act over such a formal power series according to the rules:

$$\delta_i x_i = 1, \quad \delta_i x_j = 0, \quad (i \neq j).$$

LEMMA 7.2. *The substitution $u \to \bar{u}$ defines a differential homomorphism of K–algebra $R \to G[[x-\eta]]$.*

We omit the proof which is purely computational.

PROPOSITION 7.3. *The n–uple $(\bar{u}_1, \ldots, \bar{u}_n)$ is a differential solution of $[A] : S^\infty$.*

PROOF. Using lemma 7.2, for any differential polynomial $p \in R$ we have

$$p(\bar{u}_1, \ldots, \bar{u}_n) = \sum_{\alpha \in \mathbb{N}^m} \frac{\phi(\delta^\alpha p)}{\alpha!}(x-\eta)^\alpha$$

hence $p(\bar{u}_1, \ldots, \bar{u}_n) = 0$ if and only if $\phi(\delta^\alpha p) = 0$ for each $\alpha \in \mathbb{N}^m$. Since ϕ maps $[A]:S^\infty$ to zero and $[A] : S^\infty$ is a differential ideal, for every $p \in [A] : S^\infty$ and every $\alpha \in \mathbb{N}^m$ we have $\phi(\delta^\alpha p) = 0$ whence $p(\bar{u}_1, \ldots, \bar{u}_n) = 0$. □

A regular differential ideal may have a formal power series solution for initial conditions

which annihilate some elements of S. The simplest example is probably $u_x^2 - 4u = 0$ with $u_x \neq 0$ and $\phi_0(u_x) = 0$ (the solution being $u(x) = x^2$).

The formal power series defined here do not belong to $G[[x]]$ but to $G[[x - \eta]]$. Fixing the ring of formal power series where we seek solutions would fix the expansion point. Denef and Lipshitz (1984) showed that there does not exist any algorithm which decides whether systems of polynomial differential equations have solutions in a given ring of formal power series (see however their article for exact statements).

8. Examples

We detail the resolution of the system presented in the introduction with the help of the `diffalg` package of MAPLE V.

$$\Sigma \begin{cases} u_x^2 - 4u & = & 0, \\ u_{xy}\, v_y - u + 1 & = & 0, \\ v_{xx} - u_x & = & 0. \end{cases}$$

The following instructions load the package and store in R the differential polynomial ring $\mathbb{Q}(x, y)\{u, v\}$ endowed with derivations w.r.t. x and y and an orderly ranking over $\Theta\{u,\, v\}$ such that

1 if $\mathrm{ord}(\theta) = \mathrm{ord}(\varphi)$ then $\theta u > \varphi v$
2 if $\mathrm{ord}(\theta) = \mathrm{ord}(\varphi)$ and $\theta > \varphi$ for the lexical order $x > y$ then $\theta u > \varphi u$ (idem for v).

```
> with ( diffalg ):
> R := differential_ring ( derivations = [x,y], ranking = [[u,v]] ):
```

The Rosenfeld–Gröbner algorithm is called and returns a list (understand "intersection") of regular differential ideals presented by characteristic sets. The ideals are stored in MAPLE tables. Only the names of the tables (i.e. "regular") get printed. Over this example, the list only involves one table.

```
> Sigma := [ u[x]^2 - 4*u[], u[x,y]*v[y] - u[] + 1, v[x,x] - u[x] ]:
> ideal := Rosenfeld_Groebner ( Sigma, R );
bytes used=1002848, alloc=851812, time=1.48
                              ideal := [regular]
```

The following instruction displays the characteristic presentation of the regular ideal as rewrite rules for Ritt's reduction algorithms: let p be a differential polynomial with rank v^d ; then $p = a_d v^d + a_{d-1} v^{d-1} + \cdots + a_0$ for some differential polynomials a's (the initial of p is a_d). the differential polynomial p is displayed as

$$v^d = -\frac{a_{d-1} v^{d-1} + \cdots + a_0}{a_d}.$$

```
> rewrite_rules ( ideal [1] );
```

$$[v_{x,\,x} = 2\,\frac{u_y\, v_y}{-1+u},\ u_x = 2\,\frac{u_y\, v_y}{-1+u},\ {u_y}^2 = 2\,u,\ {v_y}^2 = \frac{1}{2}\,u^2 - u + \frac{1}{2}]$$

Looking at the leaders of the differential polynomials we see that there are only three derivatives (i.e. u, v and v_x) which are not derivatives of the leader of any equation of the characteristic presentation. The solutions of Σ depend therefore on three arbitrary constants (the symbols starting with underscores denote initial conditions).

```
> initial_conditions ( ideal [1] );
```

$$[\_Cu,\ \_Cv,\ \_Cv\_x]$$

The following function call computes two objects from the computed representation which give us formal power series solutions of Σ.

1. a "generic" formal power series solution of Σ expanded at the origin and up to order 100 (the series turn out to be a polynomial) ; this is the returned value of the function call,
2. a triangular system of non differential polynomial equations and inequations over the initial conditions (this is returned in the output parameter `syst`).

```
> generic_series := power_series_solution ([x=0,y=0],100,ideal[1],'syst');
```

$$\begin{aligned}
generic_series := [u(x,\ y) &= _Cu + 2\,\frac{x\,_Cu_y\,_Cv_y}{-1+_Cu} + y\,_Cu_y \\
&- \frac{1}{2}\,\frac{x^2\,(-128\,_Cv_y\,_Cu^3 + 384\,_Cv_y\,_Cu^2 - 384\,_Cv_y\,_Cu + 128\,_Cv_y)}{64\,_Cv_y\,_Cu^3 - 192\,_Cv_y\,_Cu^2 + 192\,_Cv_y\,_Cu - 64\,_Cv_y} \\
&- \frac{x\,y\,(48\,_Cu^2 - 48\,_Cu - 16\,_Cu^3 + 16)}{16\,_Cv_y - 32\,_Cv_y\,_Cu + 16\,_Cv_y\,_Cu^2} + \frac{1}{2}\,y^2, \quad v(x,\ y) = _Cv + x\,_Cv_x \\
&+ y\,_Cv_y + \frac{x^2\,_Cu_y\,_Cv_y}{-1+_Cu} + x\,y\,_Cu_y - \frac{1}{8}\,\frac{y^2\,(-2\,_Cu\,_Cu_y + 2\,_Cu_y)}{_Cv_y} \\
&- \frac{1}{6}\,\frac{x^3\,(-128\,_Cv_y\,_Cu^3 + 384\,_Cv_y\,_Cu^2 - 384\,_Cv_y\,_Cu + 128\,_Cv_y)}{64\,_Cv_y\,_Cu^3 - 192\,_Cv_y\,_Cu^2 + 192\,_Cv_y\,_Cu - 64\,_Cv_y} \\
&- \frac{1}{2}\,\frac{x^2\,y\,(48\,_Cu^2 - 48\,_Cu - 16\,_Cu^3 + 16)}{16\,_Cv_y - 32\,_Cv_y\,_Cu + 16\,_Cv_y\,_Cu^2} \\
&- \frac{1}{2}\,\frac{x\,y^2\,(-128\,_Cv_y\,_Cu^2 + 256\,_Cv_y\,_Cu - 128\,_Cv_y)}{128\,_Cv_y\,_Cu^2 - 256\,_Cv_y\,_Cu + 128\,_Cv_y} \\
&- \frac{1}{6}\,\frac{y^3\,(-128\,_Cu^3 + 384\,_Cu^2 - 384\,_Cu + 128)}{256\,_Cv_y\,_Cu^2 - 512\,_Cv_y\,_Cu + 256\,_Cv_y}]
\end{aligned}$$

```
> syst;
```

$$\begin{aligned}
[&-_Cv_xx + _Cv_xx\,_Cu - 2\,_Cu_y\,_Cv_y = 0, \\
&-_Cu_x + _Cu_x\,_Cu - 2\,_Cu_y\,_Cv_y = 0,\ -2\,_Cu + _Cu_y^2 = 0, \\
&-_Cu^2 + 2\,_Cu + 2\,_Cv_y^2 - 1 = 0,\ _Cv_y \neq 0,\ _Cu_y \neq 0,\ -1 + _Cu \neq 0]
\end{aligned}$$

According to section 7, every solution of `syst` furnishes a unique formal power series solution of Σ. According to Lazard's lemma $\_Cu$, $\_Cv$ and $\_Cv\_x$ furnish a family of

abitrary parameters. Let's take $\_Cu = 5$, $\_Cv = 421$ and $\_Cv\_x = \pi$. The specialized system has now only finitely many solutions. Here is one of them, computed from bottom up.

$$algebraic\_solution := \_Cv\_xx = \sqrt{10}\sqrt{2},\ \_Cu\_x = \sqrt{10}\sqrt{2},\ \_Cu\_y = \sqrt{10},\ \_Cv\_y = 2\sqrt{2},$$
$$\_Cu = 5,\ \_Cv = 421,\ \_Cv\_x = \pi$$

The corresponding solutions of Σ are obtained by specializing the formal power series of `generic_series` at `algebraic_solution`.

```
> subs ( algebraic_solution, generic_series );
```

$$[u(x,\,y) = 5 + x\sqrt{10}\sqrt{2} + y\sqrt{10} + x^2 + x\,y\sqrt{2} + \frac{1}{2}\,y^2, v(x,\,y) = 421 + x\,\pi + 2\,y\sqrt{2}$$
$$+ \frac{1}{2}\,x^2\sqrt{10}\sqrt{2} + x\,y\sqrt{10} + \frac{1}{4}\,y^2\sqrt{10}\sqrt{2} + \frac{1}{3}\,x^3 + \frac{1}{2}\,x^2\,y\sqrt{2} + \frac{1}{2}\,x\,y^2 + \frac{1}{12}\,y^3\sqrt{2}]$$

8.1. Lie symmetries with automatic discussion

This example consists in solving a system of linear partial differential equations depending on a parameter. By splitting cases, the Rosenfeld–Gröbner algorithm actually discusses the solutions w.r.t. the parameter. The example and a part of its analysis are borrowed from Reid (1991). It deals with Lie symmetries of differential equations. See Olver (1993) and (1995) for the mathematical theory. The following differential equation is a variant of the wave equation. The symbol H denotes an arbitrary function of $u(x, y)$ (i.e. a parameter of the differential equation).

$$\mathrm{E}_H : \qquad \frac{\partial^2}{\partial x^2}\,u(x,\,y) \;=\; \frac{\partial^2}{\partial y^2}\,u(x,\,y) + H(u(x,\,y))\,\frac{\partial}{\partial y}\,u(x,\,y)$$

We are concerned with the Lie symmetries of the equation (E_H). Indeed, the graph of a solution of the equation (E_H) is a set of points $(x, y, u) \in \mathbb{R}^3$; a Lie symmetry of this equation is a transformation (a local diffeomorphism) which maps the graphs of solutions to the graphs of other solutions:

$$\left\{\begin{array}{lcl} X & = & \varphi_1(x, y, u), \\ Y & = & \varphi_2(x, y, u), \\ U & = & \varphi_3(x, y, u). \end{array}\right.$$

We are looking for vector fields

$$V = V^1(x, y, u)\,\frac{\partial}{\partial x} + V^2(x, y, u)\,\frac{\partial}{\partial y} + V^3(x, y, u)\,\frac{\partial}{\partial u}$$

whose flows are the desired symmetries. The set of these vector fields form a Lie algebra i.e. a vector space endowed with a Lie bracket.

With the help of the `liesymm` package of MAPLE, we build a system Σ_H of linear partial derivatives equations in the three differential indeterminates V^1, V^2 and V^3 and derivations w.r.t. x, y and u.

$$\Sigma_H = [V^1_{xx} - H\,V^1_y - 2\,V^3_{xu} - V^1_{yy},\ V^2_{xx} - V^2_{yy} + H\,V^2_y + V^3\,H_u + 2\,V^3_{yu},$$
$$V^3_{xx} - H\,V^3_y - V^3_{yy},\ V^1_{uu},\ V^2_{uu},\ -2\,V^1_{xu} + V^3_{uu},\ V^2_u,\ V^1_u,\ V^1_x - V^2_y,\ V^2_{yu} - V^1_{xu},$$
$$V^2_x - V^1_y,\ V^2_{xu} - V^1_{yu}]$$

Derivatives of the parameter H appear in the coefficients of the linear differential equations. We enlarge the system with the two following equations, to express the fact that H only depends on u.

$$H_x = 0,\ H_y = 0.$$

We want to discuss w.r.t. H the structure of the Lie algebra (in particular, its dimension as a vector space). For this reason, we consider Σ_H as a system of polynomial differential equations in four differential indeterminates V^1, V^2, V^3 and H and we call the Rosenfeld–Gröbner algorithm with a ranking which eliminates the V's. By splitting cases, the Rosenfeld–Gröbner algorithm discusses the structure of the Lie algebra w.r.t. H. Four regular systems are generated.

In the paragraphs below, computations of regular differential systems and Taylor expansions of solutions are performed using the `diffalg` package. Outputs are pretty printed. Taylors expansions are computed in the neighborhoud of $x = 0$, $y = 0$, $u = 0$. The symbols starting with a C denote the constants appearing in these developments (e.g. $CH = H(0,0,0)$, $CH_u = H_u(0,0,0)$, ...).

8.1.1. First system

Here is the characteristic presentation of the first system.

$$V^1_x = 0,\ V^1_y = 0,\ V^1_u = 0,\ V^2_x = 0,\ V^2_y = 0,\ V^2_u = 0,\ V^3 = 0,\ H_x = 0,\ H_y = 0$$

There is no differential equation in H alone (except the two ones we have introduced above). This case corresponds to the general case. The solutions of the V's are

$$\begin{aligned} V^1(x,y,u) &= CV^1, \\ V^2(x,y,u) &= CV^2, \\ V^3(x,y,u) &= 0. \end{aligned}$$

The allowed transformations are translations in the $(x,\ y)$ plane ($\lambda,\ \mu$ denote constants):

$$X = x + \lambda, \quad Y = y + \mu, \quad U = u.$$

8.1.2. Second system

Here is the characteristic presentation of the second system.

$$V^1_x = -\frac{V^3\, H_u}{H},\ V^1_y = 0,\ V^1_u = 0,\ V^2_x = 0,\ V^2_y = -\frac{V^3\, H_u}{H},\ V^2_u = 0,\ V^3_x = 0,\ V^3_y = 0,$$

$$V^3_u = -\frac{-V^3\, {H_u}^2 + H_{uu}\, H\, V^3}{H_u\, H},\ H_{uuu} = -\frac{-2\, H\, {H_{uu}}^2 + {H_u}^2\, H_{uu}}{H_u\, H},\ H_x = 0,\ H_y = 0.$$

This case corresponds to any function H which satisfies the third order differential equation above. Computing Taylor expansions of solutions we get

$$\begin{aligned} V^1(x,y,u) &= CV^1 - \frac{x\ CV^3\ CH_u}{CH}, \\ V^2(x,y,u) &= CV^2 - \frac{y\ CV^3\ CH_u}{CH}, \end{aligned}$$

$$V^3(x,y,u) \quad = \quad CV^3 - \frac{u\ (-CV^3\ {CH_u}^2 + CH_{uu}\ CH\ CV^3)}{CH_u\ CH}$$

The Lie algebra has dimension three i.e. the solutions depend on the three arbitrary constants CV^1, CV^2 and CV^3 (the constants which appear in the Taylor expansion of H are supposed to be known).

$$V = CV^1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + CV^2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + CV^3 \begin{pmatrix} -\dfrac{x\ CH_u}{CH} \\ -\dfrac{y\ CH_u}{CH} \\ CH_u\ CH + u\,({CH_u}^2 - CH_{uu}\ CH) \end{pmatrix}$$

Remark we find again (setting $CV^3 = 0$) the Lie symmetries of section 8.1.1. Some other symmetries exist however in this particular case. A class of functions H which satisfy the third order differential equation above is given by

$$H(u) = \alpha\, u + \beta$$

where α, β are constants (actually $\alpha = CH_u$ and $\beta = CH$ here since solutions have been expanded at the origin). Setting $CH_u = CH = 1$ we find the symmetry group

$$V = CV^1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + CV^2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + CV^3 \begin{pmatrix} -x \\ -y \\ u+1 \end{pmatrix}$$

The flows generated by the two first vector fields are translations in the (x,y) plane. The third vector field generates the group of dilatations (where λ denotes a constant)

$$X = \frac{x}{\lambda}, \quad Y = \frac{y}{\lambda}, \quad U + 1 = \lambda\,(u+1).$$

8.1.3. Third system

The third regular differential system correspond to the case $H(u) =$ constant.

$$V^2_{xx} = 0,\ V^3_{xx} = H\,V^3_y + V^3_{yy},\ V^3_{xu} = -\frac{1}{2}\,V^2_x\,H,\ V^3_{yu} = 0,\ V^3_{uu} = 0,\ V^1_x = 0,$$

$$V^1_y = V^2_x,\ V^1_u = 0,\ V^2_y = 0,\ V^2_u = 0,\ H_x = 0,\ H_y = 0,\ H_u = 0.$$

The solutions of the V's are

$$\begin{aligned} V^1(x,y,u) &= CV^1 + y\ CV^2_x, \\ V^2(x,y,u) &= CV^2 + x\ CV^2_x, \\ V^3(x,y,u) &= CV^3 + x\ CV^3_x + y\ CV^3_y + u\ CV^3_u + \frac{1}{2}\,x^2(CH\ CV^3_y + CV^3_{yy}) \\ &\quad + x\,y\ CV^3_{xy} - \frac{1}{2}\,x\,u\ CV^2_x\ CH + \frac{1}{2}\,y^2\ CV^3_{yy} + \cdots \end{aligned}$$

The vector fields associated to CV^1 and CV^2 generate the translations we already met in the general case. The vector field associated to CV^2_x generates an hyperbolic rotation

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \quad U = u\,e^{-\frac{1}{2}(Y-y)}$$

where $a^2 - b^2 = 1$. The vector field associated to CV_u^3 generates the group of dilatations $U = \lambda\, u$. The other symmetries depend on an arbitrary solution $\alpha(x, y)$ of the equation E_H since it is linear in this case (see Olver (1993), page 124):

$$V = \alpha(x, y)\, \frac{\partial}{\partial u}.$$

8.1.4. Fourth system

The fourth system corresponds to the wave equation ($H(u) = 0$). There are still more symmetries than in the third case. See Olver (1993), page 124 for their descriptions.

$$V_{xx}^2 = V_{yy}^2,\ V_{xx}^3 = V_{yy}^3,\ V_{xu}^3 = 0,\ V_{yu}^3 = 0,\ V_{uu}^3 = 0,\ V_x^1 = V_y^2,\ V_y^1 = V_x^2,$$
$$V_u^1 = 0,\ V_u^2 = 0,\ H = 0.$$

Conclusion

We have described an algorithm which computes a representation of the radical $\mathfrak{p}$ of any finitely generated differential ideal as an intersection of radical differential ideals. The representation separates the minimal differential prime components of $\mathfrak{p}$ which do not have the same dimension. It permits to compute Taylor expansions of solutions of $\mathfrak{p}$ and the Hilbert's polynomials associated to its minimal differential prime components. The algorithm is implemented in MAPLE within a package. Its implementation is quite tricky: it applies an analogue of Buchberger's second criterion, it manages to perform Gröbner bases computations in dimension zero and is able to reuse a representation of $\mathfrak{p}$ for a ranking to simplify the computation of a representation of $\mathfrak{p}$ for another ranking. Quite surprisingly, the algebraic computations turn out to be much easier to handle than one might fear.

In order to prove and present our algorithm, we had to improve some of Kolchin's theorems. Our results (e.g. Lazard's lemma) do not only apply in differential algebra but also for the non differential commutative algebra. Remark this phenomenon is not new: Ritt's characteristic sets theory, first developed for differential equations, has become later very popular for systems of usual polynomials.

References

Becker, T., Weispfenning, V. (1991). *Gröbner Bases: a computational approach to commutative algebra*, volume 141 of *Graduate Texts in Mathematics*. Springer Verlag.

Boulier, F. (1994). *Étude et implantation de quelques algorithmes en algèbre différentielle*. PhD thesis, Université Lille I, 59655, Villeneuve d'Ascq, France.

Boulier, F. (1997). Some improvements of a lemma of Rosenfeld. *Journal of AAECC*. (submitted).

Boulier, F., Lazard, D., Ollivier, F., Petitot, M. (1995). Representation for the radical of a finitely generated differential ideal. In *proceedings of ISSAC'95*, pages 158–166, Montréal, Canada.

Bouziane, D., Kandri Rody, A., Maârouf, H. (1996). Unmixed–Dimensional Decomposition of a Finitely Generated Perfect Differential Ideal. *Journal of Symbolic Computation*. (submitted).

Buchberger, B. (1979). *A criterion for detecting unnecessary reductions in the construction of Gröbner bases*, volume 72 of *LNCS*, pages 3–21. Springer Verlag.

Carra-Ferro, G. (1987). Gröbner bases and differential ideals. In *Notes of AAECC 5*, pages 129–140, Menorca, Spain. Springer Verlag.

Cox, D., Little, J., O'Shea, D. (1992). *Ideals, Varieties and Algorithms. An introduction to computational algebraic geometry and commutative algebra*. Undergraduate Texts in Mathematics. Springer Verlag, New York.

Denef, J., Lipshitz, L. (1984). Power Series Solutions of Algebraic Differential Equations. *Mathematische Annalen*, **267**:213–238.
Eisenbud, D. (1995). *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer Verlag.
Gallo, G., Mishra, B., Ollivier, F. (1991). *Some constructions in rings of differential polynomials*, volume 539 of *Lecture Notes in Computer Science*, pages 171–182. , Montréal, Canada.
Gebauer, R., Möller, H. M. (1988). On an Installation of Buchberger's Algorithm. *Journal of Symbolic Computation*, **6**(2&3):275–286.
Hubert, E. (1997). *Étude Algébrique et Algorithmique des Singularités des Équations Différentielles Implicites*. PhD thesis, Institut National Polytechnique de Grenoble, France.
Janet, M. (1920). *Systèmes d'équations aux dérivées partielles*, volume 3 of *Journal de Mathématiques, 8^e série*. Gauthier–Villars, Paris.
Janet, M. (1929). *Leçons sur les systèmes d'équations aux dérivées partielles*, volume IV of *Cahiers Scientifiques*. Gauthier–Villars, Paris.
Kalkbrener, M. (1993). A Generalized Euclidean Algorithm for Computing Triangular Representations of Algebraic Varieties. *Journal of Symbolic Computation*, **15**:143–167.
Knuth, D. E. (1966). *The art of computer programming*. Addison–Wesley.
Kolchin, E. R. (1973). *Differential Algebra and Algebraic Groups*. Academic Press, New York.
König, D. (1950). *Theorie der endlichen und unendlichen Graphen*. Chelsea publ. Co., New York.
Lazard, D. (1992). Solving Zero–dimensional Algebraic Systems. *Journal of Symbolic Computation*, **13**:117–131.
Levi, H. (1945). The low power theorem for partial differential equations. *Annals of the Mathematical Society*, **46**:113–119.
Maârouf, H. (1996). *Étude de Quelques Problèmes Effectifs en Algèbre Différentielle*. PhD thesis, Université Cadi Ayyad, Morocco.
Mansfield, E. (1991). *Differential Gröbner Bases*. PhD thesis, University of Sydney, Australia.
Moreno Maza, M. (1997). *Calculs de Pgcd au–dessus des Tours d'Extensions Simples et Résolution des Systèmes d'Équations Algébriques*. PhD thesis, Université Paris VI, France.
Morrison, S. (1995). Yet another proof of Lazard's lemma. private communication.
Morrison, S. (1997). The Differential Ideal $[P] : M^\infty$. *Journal of Symbolic Computation (submitted)*.
Ollivier, F. (1990). *Le problème de l'identifiabilité structurelle globale : approche théorique, méthodes effectives et bornes de complexité*. PhD thesis, École Polytechnique, 91128, Palaiseau, France.
Ollivier, F. (1998). A proof of Lazard's lemma. private communication.
Olver, P. J. (1993). *Applications of Lie groups to differential equations*, volume 107 of *Graduate Texts in Mathematics*. Springer Verlag, second edition.
Olver, P. J. (1995). *Equivalence, Invariants and Symmetry*. Cambridge University Press, New York.
Péladan-Germa, A. (1997). *Tests effectifs de Nullité dans des extensions d'anneaux différentiels*. PhD thesis, École Polytechnique, Palaiseau, France.
Reid, G. J. (1991). Algorithms for reducing a system of PDEs to standard form determining the dimension of its solution space and calculating its Taylor series solution. *Eur. J. of Applied Math.*, **2**:293–318.
Reid, G. J., Lin, P., Wittkopf, A. D. (1996). Differential Elimination–Completion Algorithms for DAE and PDAE. Technical report, Dept. of Maths of the University of British Columbia, Vancouver, Canada.
Reid, G. J., Wittkopf, A. D., Boulton, A. (1994). Reduction of systems of nonlinear partial differential equations to simplified involutive forms. *Eur. J. of Applied Math.*. (to appear).
Riquier, C. (1910). *Les systèmes d'équations aux dérivées partielles*. Gauthier–Villars, Paris.
Ritt, J. F. (1932). *Differential equations from the algebraic standpoint*, volume 14 of *American Mathematical Society Colloquium Publications*. AMS, New York.
Ritt, J. F. (1950). *Differential Algebra*. Dover Publications Inc., New York.
Rosenfeld, A. (1959). Specializations in differential algebra. *Trans. Amer. Math. Soc.*, **90**:394–407.
Schicho, J., Li, Z. (1995). A construction of radical ideals in polynomial algebra. Technical report, RISC, Johannes Kepler University, Linz, Austria.
Seidenberg, A. (1952). Some basic theorems in differential algebra (characteristic p arbitrary). *Trans. Amer. Math. Soc.*, **73**:174–190.
Seidenberg, A. (1956). An elimination theory for differential algebra. *Univ. California Publ. Math. (New Series)*, **3**:31–65.
Seidenberg, A. (1958). Abstract differential algebra and the analytic case. *Proc. Amer. Math. Soc.*, **9**:159–164.
Seidenberg, A. (1969). Abstract differential algebra and the analytic case II. *Proc. Amer. Math. Soc.*, **23**:689–691.
van der Waerden, B. L. (1966). *Algebra*. Springer Verlag, Berlin, seventh edition.
Wang, D. (1994). An elimination method for differential polynomial systems I. Technical report, LIFIA–IMAG, Grenoble, France.
Wu Wen Tsün (1987). On the foundation of algebraic differential geometry. *Mechanization of Mathematics, research preprints*, **3**.