Representation for the radical of a finitely generated differential ideal*

F. Boulier
LIFL – Université Lille I
F–59655 Villeneuve d'Ascq CEDEX
e-mail: *boulier@lifl.fr*

D. Lazard†
LITP – Institut Blaise Pascal
Université Paris VI
F–75252 Paris CEDEX 05
e-mail: *lazard@posso.ibp.fr*

F. Ollivier
GAGE – École Polytechnique
F–91128 Palaiseau CEDEX
e-mail: *ollivier@marie.polytechnique.fr*

M. Petitot
LSS – École SUPELEC
F–91192 Gif-Sur-Yvette CEDEX
e-mail: *petitot@lss.supelec.fr*

Abstract

We give an algorithm which represents the radical $\mathcal{J}$ of a finitely generated differential ideal as an intersection of radical differential ideals. The computed representation provides an algorithm for testing membership in $\mathcal{J}$. This algorithm works over either an ordinary or a partial differential polynomial ring of characteristic zero. It has been programmed. We also give a method to obtain a characteristic set of $\mathcal{J}$, if the ideal is prime.

Keywords. Differential Algebra. Radical differential ideals. Characteristic sets.

1 Introduction

Let Σ be a finite subset of a differential polynomial ring[1] $K\{y_1, \ldots, y_n\}$, where K denotes a differential field, ordinary or with partial derivatives, of characteristic zero. Let $\mathcal{R}$ be a ranking of the set of derivatives of these y_i.

We present an algorithm, called Rosenfeld–Gröbner, which represents the least radical differential ideal containing Σ as a finite intersection of radical differential ideals $\mathcal{J}_i$:

$$\{\Sigma\} = \mathcal{J}_1 \cap \cdots \cap \mathcal{J}_s.$$

Each radical differential ideal $\mathcal{J}_i$ is described by a differential system of polynomial equations and inequations Ω_i and a (non-differential) Gröbner basis B_i satisfying:

1) Ω_i and B_i provide an algorithm for testing membership in $\mathcal{J}_i$, through simple reductions,

2) B_i depends only on the differential ideal $\mathcal{J}_i$ and the ranking $\mathcal{R}$.

Thus, the set of tuples (Ω_i, B_i) allows to decide the membership in the differential ideal $\{\Sigma\}$ by simple reductions.

The intersection computed may not be minimal. Unfortunately, we do not know how to test redundancy, which is a problem close to the open problem related in [Ko], page 166. However, when we know that the differential ideal $\{\Sigma\}$ is prime, the formula mentioned above may be simplified to:

$$\{\Sigma\} = \mathcal{J}_1,$$

and we give a method for calculating, starting with the Gröbner basis B_1, a characteristic set of the differential ideal $\{\Sigma\}$, in the sense of Ritt, relative to the ranking $\mathcal{R}$.

The Rosenfeld–Gröbner algorithm relies essentially on three theorems:

1) the theorem of zeros of Hilbert, which states that a polynomial p belongs to the radical of an ideal given by a finite family of generators Σ if and only if the system of equations and inequations $\Sigma = 0,\ p \neq 0$ has no solutions; we use this theorem, in the algebraic case, and in the differential case.

2) a lemma of Rosenfeld [Ro], which gives a sufficient condition so that a system of polynomial equations and inequation admits a differential solution if and only if it admits a purely algebraic solution; the systems Ω_i described above satisfy the condition of Rosenfeld,

3) a lemma of D. Lazard, which establishes in particular that the ideals $\mathcal{J}_i$ described above are radical.

The algorithm which we describe utilizes only the operations and equality test with zero in the base field K: we refer to the reduction algorithm of Ritt, the computations of Gröbner bases, and splittings similar to those in the elimination methods of Seidenberg [Se1]. It does not need any factorization. An implementation of Rosenfeld–Gröbner has been realized [Bo], in the language C. It makes calls to the big number library of PARI and the software GB [FGLM] for the calculus of Gröbner bases.

In order to place the interest of this algorithm,

*The authors would like to thank the participants of the *Special Year in Differential Algebra and Algebraic Geometry* for their help and their comments, in particular Pr. William Sit and Raymond T. Hoobler.

†This research was partially supported by EC contract ESPRIT B.R.A. n° 6846 POSSO.

[1] We make precise in the following sections some of the notations and definitions used in this introduction.

let us describe in a few words the principals of existing methods.

Ritt gave [Ri] a method to decompose the radical of a differential ideal as an intersection of prime differential ideals, providing a characteristic set for each of these ideals. 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.

Ollivier [Ol] and Carrà–Ferro [Ca] have independently tried to generalize to differential algebra the Gröbner bases invented by Buchberger [Bu] for the study of polynomial ideals in commutative algebra. These differential Gröbner bases are in general however infinite.

Another attempt to define differential Gröbner bases has been done by E. Mansfield [Ma]. The algorithm DIFFGBASIS, implemented in MAPLE, utilizes Ritt's algorithm of reduction and then always terminates. In general however, it cannot guarantee its output to be a differential Gröbner basis.

We may remark that the membership problem in an arbitrary differential ideal is undecidable [GMO], and the membership problem of a finitely generated differential ideal is still open.

The elimination algorithms of Seidenberg [Se1] are more general. Rosenfeld–Gröbner borrows from them the idea to combine Hilbert's theorem of zeros and Ritt's algorithm of reduction. They decide the membership problem in the radical $\{\Sigma\}$ of a finitely generated differential ideal by successively eliminating all the unknowns appearing in the polynomials of Σ. They use only the operations of the base field K, but present two inconveniences: first, the description of the differential ideal $\{\Sigma\}$ they give is not usable to test the membership in the ideal afterwards; second, their behavior is a lot more explosive in practice than that of Rosenfeld–Gröbner, because they are restricted to the elimination rankings. This phenomenon is particularly striking in the case of systems with partial derivatives.

2 Preliminaries

Differential algebra. In this paper, K denotes a differential field of characteristic zero endowed with a certain number of derivations denoted $\delta_1, \ldots, \delta_m$. Let u be an element of K. We denote by θ the derivation operators ($\theta = \delta_1^{a_1} \cdots \delta_m^{a_m}$, $a_i \in \mathbb{N}$) and by θu the element of K obtained by differentiating u a_1 times by δ_1, ..., a_m times by δ_m. The sum of the exponents a_i is called the *order* of the operator θ. The identity operator is of order 0. The other operators are said to be *proper*.

Let S be a subset of a differential ring R which contains K. We denote respectively by $K[S]$ and $K\{S\}$ the smallest subring and the smallest differential subring of R containing K and S (denoting by ΘS the smallest subset of R containing S and stable under differentiation, we have $K[\Theta S] = K\{S\}$).

Let S be a subset of a differential ring R. We denote by (S) and $[S]$ the smallest ideal and the smallest differential ideal of R which contains S (we have $(\Theta S) = [S]$). The smallest radical differential ideal containing S, denoted by $\{S\}$, coincides with the radical of $[S]$.

Let I be an ideal and T be a multiplicatively stable family of R. We denote $I:T$ the ideal of all the elements p of R such that, for some $t \in T$, the element tp belongs to I. If the ideal I is differential or radical, then so is $I:T$. If $T \subset R$ is any set, then T^∞ denotes the smallest multiplicative family of R which contains T.

We work with differential polynomials in the ring $K\{y_1, \ldots, y_n\}$. We call the y_j *letters* and the θy_j *derivatives*.

An order $\mathcal{R}$ over the set of the derivatives (θy_j) is said to be a *ranking* ([Ko], page 75) if it is total and if it is compatible with the differentiations over the alphabet:

1) $\delta_i \theta y_j > \theta y_j$ (for all derivation δ_i, all operator θ and all letter y_j)

2) $\theta_1 y_i > \theta_2 y_j \Rightarrow \delta_\ell \theta_1 y_i > \delta_\ell \theta_2 y_j$ (for all derivations δ_ℓ, all operators θ_1, θ_2 and all letters y_i, y_j).

Let p be a polynomial[2] of $K\{y_1, \ldots, y_n\}$ and $\mathcal{R}$ a ranking on the θy_j. The *leader* u of p is the largest derivative with respect to the ranking $\mathcal{R}$ which appears in p. The two conditions mentioned above imply that the leader of θp is θu for all derivation operators θ. Let d be the degree of u in p. The initial I_p of p is the coefficient of u^d in p. The separant S_p of p is the initial of all the proper derivatives of p ($S_p = \partial p / \partial u$). The *rank* of a polynomial $p = I_p \cdot u^d + R_p$ is the polynomial u^d. The rank of a set E is the set of ranks of the elements of E.

Let p and q be two polynomials and let u^d be the rank of p. The polynomial q is said to be *partially reduced* with respect to p if no proper derivative of u appears in q. The polynomial q is said to be *reduced* with respect to p if q is partially reduced with respect to p and its degree in u is less than d.

A set of polynomials A is said to be *triangular* if its elements have different leaders. A set of polynomials A is said to be *autoreduced* if each element of A is reduced with respect to every other element of the set. Every autoreduced set is triangular. Every autoreduced set is finite ([Ko], page 77).

Let A be an autoreduced set. We denote H_A the set of all the initials and the separants of A. Hence H_A^∞ denotes the set of all the products of powers of the initials and separants of the elements of A.

Let p be a polynomial and $A = p_1, \ldots, p_s$ be an autoreduced set. There exists ([Ko], page 77) an algorithm, called *Ritt's algorithm of reduction*, which rewrites p as a polynomial $r = p \textit{ rem } A$, reduced with respect to A (i.e. with respect to all the elements of A), satisfying the relation: $r \equiv I_1^{a_1} \cdots I_s^{a_s} S_1^{b_1} \cdots S_s^{b_s} p \pmod{[A]}$, for some integers a_i and b_i (where I_ℓ and S_ℓ denote respectively the initial and the separant of p_ℓ).

The algorithm begins by producing a partial remainder $q = p \textit{ partial-rem } A$. The polynomial q is partially reduced with respect to A and satisfies for some integers $b_1, \ldots, b_s$ the relation: $q \equiv S_1^{b_1} \cdots S_s^{b_s} p \pmod{[A]}$. The algorithm then calcu-

[2] The definitions which we give are only valid for polynomials $p \notin K$. In this paper, we don't need to bother with the exceptions $p \in K$.

lates $r = p\ rem\ A$ by applying to q a simple algebraic reduction.

If $p \in [A] : H_A^\infty$ then $(p\ rem\ A) \in [A] : H_A^\infty$.

Many such algorithms exist. We fix one of them.

An autoreduced subset C of a set E of polynomials is called a *characteristic set*[3] of E if E does not contain any non-zero element reduced with respect to C. All the characteristic sets of E have the same rank. A characteristic set C of an ideal $\mathcal{J}$ reduces to zero all elements of $\mathcal{J}$. If the ideal is prime, C reduces to zero only the elements of $\mathcal{J}$ and we have $\mathcal{J} = [C] : H_C^\infty$ ([Ko], lemma 2, page 167).

Let p_i and p_j be two polynomials in an autoreduced subset A of $K\{y_1, \dots, y_n\}$, whose leaders $\theta_i y_\ell$ and $\theta_j y_\ell$ are derivatives of some same letter y_ℓ (this can only happen for partial differential systems). We denote θ the operator of minimal order and ϕ_i and ϕ_j the two derivation operators such that $\phi_i \theta_i = \phi_j \theta_j = \theta$. We define the Δ–polynomial between p_i and p_j as the polynomial $\Delta_{ij} = S_{p_j} \phi_i p_i - S_{p_i} \phi_j p_j$. Its leader is strictly less than θy_ℓ.

Denote Δ–polynomial (A) the set of all possible Δ–polynomials which can be formed between any two elements of A. The set A is said to be *coherent*[4] if it reduces to zero all its Δ–polynomials: Δ–polynomial (A) $rem\ A = \{0\}$ (or $= \emptyset$).

Gröbner Bases. We shall have to calculate (non-differential) Gröbner bases of (non-differential) ideals of $K\{y_1, \dots, y_n\}$. Let A be a finite subset of $K\{y_1, \dots, y_n\}$ and let $\mathcal{R}_1$ be a ranking of the derivatives θy_i. We order following $\mathcal{R}_1$ the derivatives $w_1 < \cdots < w_t$ which appear in the elements of A. The order $\mathcal{R}_1$ *induces* an order of elimination $\mathcal{R}_2$ on the monomials of the ring $K[w_1, \dots, w_t]$. Let $m_1 = w_1^{a_1} \cdots w_t^{a_t}$ and $m_2 = w_1^{b_1} \cdots w_t^{b_t}$. The order $\mathcal{R}_2$ is defined by: $m_1 < m_2$ if for the largest index i such that a_i and b_i are different, we have $a_i < b_i$.

The largest monomial for the order $\mathcal{R}_2$ which appears in a polynomial p is called the *head monomial* of p. Also, if u^d is the rank of a polynomial p for the order $\mathcal{R}_1$, then u^d appears as a factor in the head monomial of p.

If A is a subset of $K[w_1, \dots, w_t] \subset K\{y_1, \dots, y_n\}$, then the non-differential ideal generated by A in the ring $K[w_1, \dots, w_t]$ coincides with the intersection between the non-differential ideal generated by A in $K\{y_1, \dots, y_n\}$ and the polynomial ring $K[w_1, \dots, w_t]$. Thus for the non-differential ideal (A), the property to be *prime* of *radical* is independent of the polynomial ring.

3 Theorems Used

3.1 The theorem of zeros

Let Σ be a polynomial system of equations and inequations. A model of Σ is a solution of Σ in a field extension of the base field of the system. More formally,

Definition 1 *Let Σ be a differential polynomial system of equations and inequations of $K\{y_1, \dots, y_n\}$. A* differential model *of Σ is a morphism of differential K–algebras $K\{y_1, \dots, y_n\} \to L$ into a differential field L that annuls the equations but not the inequations of Σ.*

Let $w_1, \dots, w_t$ denote the derivatives which appear in the equations and inequations of Σ. An algebraic model *of Σ is a morphism of K–algebras $K[w_1, \dots, w_t] \to L$ into a field L which annuls the equations but not the inequations of Σ.*

Every differential model provides an algebraic model, but the converse is not true. Take the example of a partial differential system of $\mathbb{Q}\{u, v\}$, equipped with two derivations δ_x and δ_y which we denote by subscripts:

$$u_x = 0,\ u_y = v,\ v_x \neq 0.$$

The system does not admit a differential model since the equation $\delta_y u_x - \delta_x(u_y - v) = v_x = 0$ contradicts the inequation. It admits however an obvious algebraic model: $u_x = u_y = v = 0$ and $v_x = 1$.

Theorem 1 (theorem of zeros, Hilbert). *Let Σ be a differential polynomial system of equations and inequations: $p_1 = 0, \dots, p_m = 0$; $q \neq 0$ in the ring $K\{y_1, \dots, y_n\}$.*

The system Σ has no differential model if and only if some power of q belongs to the differential ideal $[p_1, \dots, p_m]$.

The system Σ has no algebraic model if and only if some power of q belongs to the ideal $(p_1, \dots, p_m)$.

Proof. See [Se2], page 178. We give the proof in the differential case. The proof in the algebraic case is similar.

The implication from left to right. The radical of a differential ideal is a radical differential ideal and every radical differential ideal is an intersection of prime differential ideals. Suppose that q does not belong to the radical of the ideal $[p_1, \dots, p_m]$. There exists then a prime differential ideal P which contains $[p_1, \dots, p_m]$ but not q. This ideal provides a differential model: the canonical morphism of the ring $K\{y_1, \dots, y_n\}$ into the field of quotients of the ring $K\{y_1, \dots, y_n\}/P$.

The reverse implication is immediate. □

3.2 Regular systems

A rapid computation shows that $\dot{x}^3 \in [x\dot{x}]$ but that $\dot{x}^3 \notin (x\dot{x})$. More generally, if A denotes a finite set of polynomials, the set of the elements of $[A]$ partially reduced w.r.t. A may also contain polynomials which are not in (A). This phenomenon demonstrates well the importance of the following lemma.

Lemma 1 (Rosenfeld). *If A is an autoreduced and coherent subset of the ring $K\{y_1, \dots, y_n\}$ then every differential polynomial which belongs to $[A] : H_A^\infty$ and which is partially reduced with respect to A belongs also to $(A) : H_A^\infty$.*

[3] This definition corresponds to Ritt's one (see [Ri], page 5) and coincides with Kolchin's when E is a differential ideal. Kolchin only defined characteristic sets for ideals (see [Ko], page 81 and 124).

[4] This definition is stronger than that of Rosenfeld [Ro] or Kolchin [Ko], page 136. Any autoreduced set which is coherent in our sense is also coherent in the classical sense (so theorems still apply). We adopt it because it corresponds to an algorithmic test.

Proof. See [Ro], page 397 or [Ko], lemma 5, page 135. □

The regular systems are differential polynomial systems of equations and inequations for which Rosenfeld's lemma applies.

Definition 2 *A system of differential equations and inequations is said to be* regular *with respect to a ranking $\mathcal{R}_1$, if the set of its equations is autoreduced and coherent, the initial and separant of each equation appear among the inequations and if its other inequations are partially reduced with respect to the equations:*

$$\Omega \left\{ \begin{array}{lcll} p_1 & = & 0 & \\ & \vdots & & A = p_1, \ldots, p_s \textit{ is autoreduced} \\ p_s & = & 0 & \qquad\qquad\qquad \textit{and coherent} \\ I_1 & \neq & 0 & \\ & \vdots & & \textit{the initial and separant of each } p_i \\ S_s & \neq & 0 & \\ q & \neq & 0 & q \textit{ is partially reduced w.r.t. } A \end{array} \right.$$

Notation. We use the letter Ω to denote regular systems (for instance: Ω, Ω_s etc ...). We use the letter A to denote the set of the equations of Ω (for instance, A_1 and A_s, stand for the set of the equations of Ω_1 and Ω_s). We use H_Ω^∞ to denote the set of all the power products of the inequations of Ω (for instance, $H_{\Omega_1}^\infty$ and $H_{\Omega_s}^\infty$ correspond to Ω_1 and Ω_s). We have $H_A^\infty \subset H_\Omega^\infty$.

Theorem 2 (Rosenfeld). *A regular system Ω admits a differential model if and only if it admits an algebraic model.*

Proof. See [Ro], page 398. Suppose that Ω does not admit a differential model and we show that it then does not admit an algebraic model. By the theorem of zeros, $1 \in [A] : H_\Omega^\infty$. By Rosenfeld's lemma, $1 \in (A) : H_\Omega^\infty$, and Ω does not admit an algebraic model. The other implication is immediate. □

The lemma 1 and the theorem 2 are extensions of two results of Seidenberg ([Se1], theorems 6 and 7 pages 51 and 52) which provide his elimination algorithm for partial differential systems.

3.3 Regular ideals

We establish in this section some important properties of the ideals $[A] : H_\Omega^\infty$ and $(A) : H_\Omega^\infty$. In particular, we show that they are always radical and that there exists an algorithm which decides if a given polynomial belongs to them.

The following lemma is interesting by itself. In particular, it generalizes a result of Kolchin (see [Ko], lemma 13, page 36).

The total ring of fractions of a ring R is obtained by making invertible all the elements of R which do not divide zero. We denote it $Q(R)$.

Lemma 2 (Lazard). *Let $A = p_1, \ldots, p_s$ be a triangular set of a polynomial ring $K[w_1, \ldots, w_t]$, for the ranking $w_1 < \cdots < w_t$. Let $u_1 < \cdots < u_s$ be the leaders of the elements of A and S_A denote the set of the separants of the elements of A. If the ideal $(A) : S_A^\infty$ is non trivial, then the total ring of fractions $\mathcal{Q}$ of the ring $K[w_1, \ldots, w_t]/(A) : S_A^\infty$ verifies the two following properties:*

(P1) it is isomorphic to a product of fields.

(P2) denoting $\bar{w}_i$ the image of w_i, we have: $\bar{w}_i$ satisfies an algebraic relation over $Q(K[\bar{w}_1, \ldots, \bar{w}_{i-1}])$ if and only if w_i is some u_j.

Moreover, the properties above remain true if S_A^∞ is replaced by any multiplicative family S which contains it, provided that the ideal $(A) : S$ is non trivial.

The following small lemmas are used in the proof.

a. Let R be a ring. Let I be an ideal and S be a multiplicative family of R. Let X be an indeterminate. The ring homomorphisms $R \xrightarrow{i_s} S^{-1}R$, $R \xrightarrow{p} R/I$ and $R \rightarrow R[X]$ commute together. Moreover, if S and S' are two multiplicative families, the morphisms i_s and $i_{s'}$ commute also. If $I \subset J$, then $R/J \simeq (R/I)/p(J)$.

b. We retain the notations of (a). Since $I : S = i_s^{-1}(i_s(I))$ and the image of S in $R/I : S$ contains no zero divisor, by (a), we have the isomorphisms $Q(R/I : S) \simeq Q(S^{-1}R/S^{-1}I) \simeq Q(p(S)^{-1}(R/I))$.

c. Let R be a ring. If $a \in R$ is nilpotent, then $a^{-1}R$ is the zero ring. $R/(1)$ is also the zero ring.

d. If $R = R_1 \times \cdots \times R_n$ is a product of rings and if $a = (a_1, \ldots, a_n)$ is one of its elements, we have:

$R/(a) = R_1/(a_1) \times \cdots \times R_n/(a_n)$,

$a^{-1}R = a_1^{-1}R_1 \times \cdots \times a_n^{-1}R_n$,

$R[X] = R_1[X] \times \cdots \times R_n[X]$.

e. Let $R \xrightarrow{f} S$ be a ring homomorphism. Let $p \in R[X]$ be a polynomial and S_p be its separant. Then $f(S_p) = S_{f(p)}$.

f. Let $p \in K[X]$ be a polynomial over a field. Let $p_1^{a_1} \cdots p_n^{a_n}$ be the decomposition of p into irreducible factors. Since the separant S_p of p contains as factors the multiple factors $(a_i > 1)$ of p, the ideal $(p) : S_p^\infty$ is generated by the product of the simple factors of p. The ring $K[X]/(p) : S_p^\infty$ is hence either the zero ring (by (c), if p has no simple factors), either a product of fields, according to the Chinese Remainders theorem.

Proof. We define a sequence of rings as follows:

$R_0 = K$,

$R_{i+1} = Q(R_i[w_{i+1}])$ if $w_{i+1} \neq u_j$ for each u_j,

$R_{i+1} = R_i[u_j]/(\bar{p}_j) : \bar{S}_j^\infty$ if $w_{i+1} = u_j$.

where $\bar{p}_j$ and $\bar{S}_j$ denote the images of p_j and S_j in the ring $R_i[u_j]$.

To prove the lemma 2 we are going to establish, first that R_t verifies (P1) and (P2), second that R_t is isomorphic to $\mathcal{Q}$. Last, we consider the case of multiplicative families which contain S_A^∞.

1. We show by induction on i that R_t verifies (P1) and (P2). Clearly, R_0 satisfies them. Assume that $R_i \simeq K_1 \times \cdots \times K_m$ verifies these two properties and let us show that R_{i+1} verifies (P1) and (P2) also.

If w_i is not a leader u_j, using (d), R_{i+1} is isomorphic to $\prod_{k=1}^m K_k(w_{i+1})$. It verifies (P1) and (P2).

Now, let us consider the case $w_i = u_j$. Let $\bar{p}_j = (\bar{p}_{j1}, \ldots, \bar{p}_{jm})$ and $\bar{S}_j = (\bar{S}_{j1}, \ldots, \bar{S}_{jm})$. By (d) we have, $R_i[u_j]/(\bar{p}_j) : \bar{S}_j^\infty \simeq \prod_{k=1}^m K_k[u_j]/(\bar{p}_{jk}) : \bar{S}_{jk}^\infty$.

Let $1 \leq k \leq m$.

If $\bar{p}_{jk} \in K_k$, then $\bar{S}_{jk} = 0$ and the k^{th} factor of the product above is the zero ring, by (e) and (c).

If $\bar{p}_{jk} \notin K_k$, then by (f), $K_k[u_j]/(\bar{p}_{jk}) : \bar{S}_{jk}^{\infty}$ is either the zero ring, either isomorphic to some product of algebraic field extensions of K_k.

Thus R_{i+1} verifies (P1) and (P2).

2. We show by induction on i that $R_t \simeq \mathcal{Q}$. The main point to check is that the inversion of the non zero divisors commute with the other ring homomorphisms. Let us denote $T_i = K[w_1, \ldots, w_i]/(p_1, \ldots, p_{j-1}) : (S_1, \ldots, S_{j-1})^{\infty}$, where $u_{j-1} \leq w_i < u_j$. We have $\mathcal{Q} = Q(T_t)$. Clearly, $R_0 \simeq Q(T_0)$. Assume that $R_i \simeq Q(T_i)$ and let us prove that $R_{i+1} \simeq Q(T_{i+1})$.

If $w_{i+1} \neq u_j$ then $R_{i+1} = Q(R_i[w_{i+1}])$. Every non zero divisor in T_i is still a non zero divisor in $T_i[w_{i+1}]$, so $R_{i+1} \simeq Q(T_i[w_{i+1}])$ and by (a), $R_{i+1} \simeq Q(T_{i+1})$.

If $w_{i+1} = u_j$ then $R_{i+1} = R_i[u_j]/(\bar{p}_j) : \bar{S}_j^{\infty}$. Since R_{i+1} verifies (P2), every non zero divisor in T_i is still a non zero divisor in $T_i[u_j]/(\bar{p}_j) : \bar{S}_j^{\infty}$. Since R_{i+1} verifies (P1) we have $R_{i+1} \simeq Q(T_i[u_j]/(\bar{p}_j) : \bar{S}_j^{\infty})$. Then by (a) and (b) $R_{i+1} \simeq Q(T_{i+1})$.

3. By (c) and (d), the inversion of an element p of a product of fields only suppresses the fields of the product for which p has a zero component. □

Definition 3 *A differential ideal $\mathcal{J}$ is said to be* regular *if there exists a regular system Ω such that $\mathcal{J} = [A] : H_{\Omega}^{\infty}$. An algebraic ideal $\mathcal{J}$ is said to be regular if there exists a regular system Ω such that $\mathcal{J} = (A) : H_{\Omega}^{\infty}$.*

Theorem 3 *Every regular ideal is radical.*

Proof. Let Ω be a regular system. Let p be a polynomial for which a power p^n belongs to $(A) : H_{\Omega}^{\infty}$. The image of p^n in $K[w_1, \ldots, w_t]/(A) : H_{\Omega}^{\infty}$ is zero. That ring has no nilpotent element, since its total ring of fractions is a product of fields, according to the lemma 2. Hence the image of p is zero, p belongs to $(A) : H_{\Omega}^{\infty}$ and that ideal is radical.

Let us show that the regular differential ideal $[A] : H_{\Omega}^{\infty}$ is also radical. Let p be a polynomial for which a power p^n belongs to $[A] : H_{\Omega}^{\infty}$. The polynomial $\bar{p} = p \; rem \; A$ is equivalent to some $S_1^{a_1} \cdots S_s^{a_s} p$ modulo $[A] : H_A^{\infty}$. By Rosenfeld's lemma and the first part of the proof, $\bar{p} \in (A) : H_{\Omega}^{\infty}$ whence p is in $[A] : H_{\Omega}^{\infty}$. This ideal is thus radical. □

The following lemma is a consequence of lemma 2 (property (P2)), the proof of which is left to the reader. It is used in the proof of the lemma 5 and shows that we may read the transcendance degree of a system without calculating the Gröbner basis of $(A) : H_{\Omega}^{\infty}$, except the condition to ascertain that the ideal is non trivial.

Lemma 3 *Let Ω be a regular system for a ranking $\mathcal{R}_1$. Let $u_1 < \cdots < u_s$ be the leaders of the equations of the system. Let B be a Gröbner basis of $(A) : H_{\Omega}^{\infty}$ for the order $\mathcal{R}_2$ induced by $\mathcal{R}_1$.*

If $(A) : H_{\Omega}^{\infty}$ is not the unit ideal, then the leaders of the polynomials of B are the derivatives $u_1, \ldots, u_s$.

Let Ω be a regular system and A be the set of its equations. We give in section 4 a method to calculate a Gröbner basis B of $(A) : H_{\Omega}^{\infty}$, and in section 6 an example of a regular system without models.

The following lemma shows how to decide the membership problem in a regular differential ideal. Its proof is an easy consequence of Rosenfeld's lemma.

Lemma 4 *Let Ω be a regular system, A be the set of its equations, and B be a Gröbner basis of $(A) : H_{\Omega}^{\infty}$. For each polynomial p of $K\{y_1, \ldots, y_n\}$ we have:*

$$p \in [A] : H_{\Omega}^{\infty} \iff (p \text{ partial-rem } A) \in (B).$$

We would like to clarify the correspondance between systems of regular algebraic ideals and regular differential ideals. An example suffices to show that two different regular systems may define the same regular ideals:

$$x + 1 = 0, \quad \text{and}$$
$$(x+1)(x+2)^2 = 0, \; (x+2)(3x+4) \neq 0.$$

Question: Is the correspondance between regular algebraic ideals and regular differential ideals bijective ? In other words, do two regular differential systems define the same regular algebraic ideal if and only if they define the same regular differential ideal ? The following lemma, which shows the implication from right to left, is a step in the proof of theorem 6. The converse implication, which we have not established, seems to be in keeping with the open problem: to decide the inclusion of two prime differential ideals each given by a characteristic set (see [Ko], page 166).

Lemma 5 *Two regular systems which define the same regular differential ideal define also the same regular algebraic ideal.*

Proof. Let Ω and Ω' be two regular systems defining the same regular differential ideal $[A] : H_{\Omega}^{\infty} = [A'] : H_{\Omega'}^{\infty}$. Let B and B' be the Gröbner bases respectively of the ideals $(A) : H_{\Omega}^{\infty}$ and $(A') : H_{\Omega'}^{\infty}$ for the order $\mathcal{R}_2$ induced by $\mathcal{R}_1$. We suppose B is different from B' and we seek a contradiction.

We order the polynomials of $B = b_0, b_1, \ldots, b_m$ and of $B' = b'_0, b'_1, \ldots, b'_{m'}$ by increasing order. Let i be the least index such that the head monomials of the polynomials b_i and b'_i are different and suppose $b'_i < b_i$. Since b'_i belongs to the differential ideal $[A] : H_{\Omega}^{\infty}$, by lemma 4 ($b'_i$ *partial-rem* A) $\in (B)$.

Let u_ℓ and u'_ℓ be the leaders of the polynomials in the basis B and B' and let u'_j be the leader of b'_i. We have $u_1 = u'_1, \ldots, u_{j-1} = u'_{j-1}$.

By the lemma 3, each polynomial of the basis B (respectively B') is partially reduced w.r.t. each other. Since $u_1 = u'_1, \ldots, u_{j-1} = u'_{j-1}$ and since $b'_i < b_i$, the partial reduction of b'_i by A does not modify b'_i and we have $b'_i \in (B)$. In view of the hypothesis made on i, the head monomial of b'_i can not be reduced by any rule from B.

This contradiction proves the lemma. □

While the basis B is "canonical", it does not permit easy computation in $K\{y_1, \ldots, y_n\}/[A] : H_{\Omega}^{\infty}$. In fact, the partial reduction algorithm does not transform a polynomial into a polynomial which is equivalent modulo the ideal:

$$p \not\equiv (p \; partial\text{-}rem \; A) \pmod{[A] : H_{\Omega}^{\infty}}.$$

4 The Rosenfeld–Gröbner Algorithm

The program Rosenfeld–Gröbner gathers at entry a differential system of equations and inequations Σ and a ranking $\mathcal{R}_1$. It produces by splittings a finite family (Ω_i) of consistent (with models) regular systems whose differential models form a partition of the differential models of Σ.

The Greek letters Λ, Ω, Γ_i, denote systems of equations and inequations. Λ_{eq} and Λ_{in} stand respectively for the set of the equations and for the set of the inequations of the system Λ.

The function *obviouslyInconsistent* returns *true* if a non-zero element of K appears among the equations, or if 0 appears among the inequations of the system.

program Rosenfeld–Gröbner $(\Lambda, \mathcal{R}_1)$
begin
  if not obviouslyInconsistent (Λ) **then**
    $A :=$ a characteristic set of the finite set Λ_{eq}
    Let $\{h_1, \dots, h_r\}$ denote the set of the initials and of the separants of the elements of A such that $h_i \notin K$.
    $R := (\Lambda_{\text{eq}} \setminus A \cup \Delta\text{–pols}(A))$ *rem* A
    if $R = \emptyset$ **or** $R = \{0\}$ **then**
      $\Omega_{\text{eq}} := A$
      $\Omega_{\text{in}} := (\Lambda_{\text{in}}$ *partial-rem* $A) \cup \{h_1 \neq 0, \dots, h_r \neq 0\}$
      $B :=$ a Gröbner basis of $(A) : H_\Omega^\infty$
      if $B \neq \{1\}$ **then**
        produce on output Ω and B
      endif
    else
      $\Gamma_{r+1,\text{eq}} := A \cup R$
      $\Gamma_{r+1,\text{in}} := \Lambda_{\text{in}} \cup \{h_1 \neq 0, \dots, h_r \neq 0\}$
      Rosenfeld–Gröbner $(\Gamma_{r+1}, \mathcal{R}_1)$
    endif
    for $i := r$ **downto** 1 **do**
      $\Gamma_{i,\text{eq}} := \Lambda_{\text{eq}} \cup \{h_i = 0\}$
      $\Gamma_{i,\text{in}} := \Lambda_{\text{in}} \cup \{h_{i-1} \neq 0, \dots, h_1 \neq 0\}$
      Rosenfeld–Gröbner $(\Gamma_i, \mathcal{R}_1)$
    end
  endif
end

Some other ways exist to do the splitting of Λ into the Γ_i (see [Bo]). This one was used by Seidenberg in [Se1].

The Gröbner basis B of the ideal $(A) : H_\Omega^\infty$ is computed by the method below. It is classical [Tr]. It detects regular systems without models: those with basis $\{1\}$.

1. The system Ω is transformed into a system of equations: the algorithm introduces a new unknown z_i for each inequation $h_i \neq 0$ of the system and rewrites $h_i \neq 0$ as $h_i z_i = 1$.

2. A basis B_0 is computed following any elimination order $\mathcal{R}_2$ satisfying: $\theta y_i < z_j$ (for all derivatives θy_i and all unknowns z_j),

3. The desired basis B is obtained by truncating B_0. Only those polynomials of B_0 which do not involve z_i are retained.

4.1 Proofs

Lemma 6 *The Rosenfeld–Gröbner algorithm stops.*

Proof. The set of the equations of each system Γ_i not obviously inconsistent, produced from Λ, contains A and at least one polynomial $p \notin K$ reduced w.r.t. A.

Thus, the characteristic sets of the sets of the equations of the systems Γ_i not obviously inconsistent are lower than A, for the usual ranking over autoreduced sets ([Ko], page 81).

This ranking is a well ordering ([Ko], proposition 3, page 81). Since the algorithm discards obviously inconsistent systems, Rosenfeld–Gröbner stops. □

The two lemmas below deal with the correction of the algorithm. Since Ω corresponds to a particular case of Γ_{r+1}, we do not distinguish it from Γ_{r+1}, in order to simplify the statements.

Lemma 7 *ϕ is a differential model of Λ if and only if ϕ is a differential model of some Γ_i $(1 \leq i \leq r+1)$. Moreover, the differential models of the systems Γ_i are disjoint.*

We only give the main argument of the proof.

Let ϕ be a differential model of some system $A = 0, h_1 \neq 0, \dots, h_r \neq 0$. Let p be any polynomial and let $\bar{p} = p$ *rem* A. According to the definition of the models and to the specifications of Ritt's algorithm of reduction, we have $\phi(p) = 0 \Leftrightarrow \phi(\bar{p}) = 0$.

We need the notations below for the lemma 8, which is used for the calculus of characteristic sets in section 5.

Let Σ be a system of equations and inequations, $\{\Sigma_{\text{eq}}\}$ be the radical differential ideal generated by the equations of the system, and H_Σ^∞ be the multiplicative family generated by its inequations. We denote $\mathcal{J}(\Sigma)$ the radical differential ideal $\{\Sigma_{\text{eq}}\} : H_\Sigma^\infty$.

Lemma 8 *If $\mathcal{J}(\Lambda)$ is prime and if ℓ is the greatest index such that Γ_ℓ has a differential model, then*

$$\mathcal{J}(\Lambda) = \mathcal{J}(\Gamma_\ell).$$

Proof. According to the lemma 7 above and to the theorem of zeros,

$$\mathcal{J}(\Lambda) = \mathcal{J}(\Gamma_{r+1}) \cap \cdots \cap \mathcal{J}(\Gamma_1),$$

so the index ℓ exists. We consider thus two cases.

1. No polynomial h_i $(1 \leq i \leq r)$ belongs to $\mathcal{J}(\Lambda)$. We prove that $\mathcal{J}(\Gamma_{r+1}) \subset \mathcal{J}(\Lambda)$ and the equality follows from the formula above $(\ell = r+1)$.

We have $\Gamma_{r+1,\text{eq}} \subset [\Lambda_{\text{eq}}] \subset \mathcal{J}(\Lambda)$. Since the ideal is prime and since no polynomial h_i belongs to it, we have $H_{\Gamma_{r+1}}^\infty \cap \mathcal{J}(\Lambda) = \emptyset$. Now, assume that $p \in \mathcal{J}(\Gamma_{r+1})$ i.e. that for some $h \in H_{\Gamma_{r+1}}^\infty$, we have $hp \in \{\Gamma_{r+1,\text{eq}}\} \subset \mathcal{J}(\Lambda)$. Since $h \notin \mathcal{J}(\Lambda)$ and that ideal is prime, we have $p \in \mathcal{J}(\Lambda)$.

2. Let $t \leq r$ be the smallest index such that $h_t \in \mathcal{J}(\Lambda)$. We prove that all the ideals $\mathcal{J}(\Gamma_i)$ $(t < i \leq r+1)$ are trivial and that $\mathcal{J}(\Gamma_t) \subset \mathcal{J}(\Lambda)$. The equality follows from the formula above $(\ell = t)$.

By the formula above, for $t < i \leq r+1$ we have $h_t \in \mathcal{J}(\Lambda) \subset \mathcal{J}(\Gamma_i)$ but, according to the way the Γ_i are computed, we have also $h_t \in H_{\Gamma_i}^\infty$. These ideals $\mathcal{J}(\Gamma_i)$ are hence trivial and the corresponding systems Ω_i are not produced on the output of the program.

According to the hypothesis $\Gamma_{t,\text{eq}} \subset \mathcal{J}(\Lambda)$. Since this ideal is prime and no polynomial h_i $(1 \le i < t)$ belongs to it, we have $H_{\Gamma_t}^\infty \cap \mathcal{J}(\Lambda) = \emptyset$ whence as in **1.** above, $\mathcal{J}(\Gamma_t) = \mathcal{J}(\Lambda)$. □

4.2 Properties of the computed representation

A *basis in the sense of Ritt and Raudenbush* of a radical differential ideal $\mathcal{J}$ is any finite family Σ such that $\mathcal{J} = \{\Sigma\}$. Ritt and Raudenbush established [Ri], page 10 that every radical differential ideal admitted a basis.

The Rosenfeld–Gröbner algorithm decomposes a differential ideal $\{\Sigma\}$ given by a finite basis as an intersection of regular differential ideals each described by a regular system. This decomposition is also an algorithm for membership testing in $\{\Sigma\}$.

Consider a system $\Sigma : p_1 = 0, \ldots, p_m = 0$ of differential polynomial equations of $K\{y_1, \ldots, y_n\}$. Let $\Omega_1, \ldots, \Omega_s$ be the successive regular systems produced by the Rosenfeld–Gröbner algorithm applied to Σ for some ranking $\mathcal{R}_1$.

For each system Ω_i, we denote A_i the set of its equations and $H_{\Omega_i}^\infty$ the multiplicative family generated by its inequations.

Theorem 4 *With notations as above, we have:*

1) ϕ is a differential model of Σ if and only if ϕ is a differential model of some Ω_i $(1 \le i \le s)$. Moreover, the differential models of the regular systems Ω_i are disjoint.

2) the radical differential ideal $\{\Sigma\}$ is the intersection of the regular differential ideals $[A_i] : H_{\Omega_i}^\infty$.

$$\{\Sigma\} = \sqrt{[\Sigma]} = [A_1] : H_{\Omega_1}^\infty \cap \cdots \cap [A_s] : H_{\Omega_s}^\infty.$$

Proof.

1) It is an easy consequence of the lemma 7.

2) By 1) and the theorem of zeros, a polynomial p belongs to $\{\Sigma\}$ if and only if, for each $i \in [1, s]$, the system obtained by adjoining the inequation $p \ne 0$ to Ω_i has no differential models. By the theorem of zeros and the theorem 3, these systems have no differential models if and only if $p \in [A_i] : H_{\Omega_i}^\infty$. □

The description of the ideal $\{\Sigma\}$ computed by Rosenfeld–Gröbner allows us to decide the membership problem in $\{\Sigma\}$, using a few reductions. This is expressed in the following theorem, whose proof is an immediate consequence of the theorem 4 and the lemma 4.

Theorem 5 *With notations as above, we have:*

$$p \in \{\Sigma\} \;\Leftrightarrow\; \forall i \in [1, s],\; (p \text{ partial-rem } A_i) \in (B_i).$$

5 Computation of characteristic sets

We give a method to compute the characteristic set of a prime differential ideal given by a basis in the sense of Ritt and Raudenbush. We generalize here the result [Ol], page 89, of Ollivier.

We retain the notations of the preceding section.

Lemma 9 *If the differential ideal $\{\Sigma\}$ is prime then*

$$\{\Sigma\} = [A_1] : H_{\Omega_1}^\infty.$$

Proof. The inclusion from left to right comes from the theorem 4. The other one is a consequence of the lemma 8. □

To our knowledge, there does not exist any algorithm which decides if a differential ideal given by a basis (either in the classical sense or in the sense of Ritt and Raudenbush) is prime.

The coherent and autoreduced set A_1 satisfies a property of characteristic sets of the ideal: if C is a characteristic set of a prime differential ideal $\{\Sigma\}$, then we have $\{\Sigma\} = [C] : H_C^\infty$. However, A_1 is not necessarily a characteristic set of the ideal. Consider the (algebraic) example below:

$$A_1 : (x+1)(x+2) = 0,\; (x+1)y + 2 = 0.$$

A_1 is autoreduced with respect to the order $x < y$, the ideal $(A_1) : H_{A_1}^\infty$ is prime but its characteristic set is

$$C : x + 2 = 0,\; y - 2 = 0.$$

The basis B of $(A_1) : H_{\Omega_1}^\infty$, computed with respect to the order $\mathcal{R}_2$ induced by $\mathcal{R}_1$ is almost a characteristic set of $\{\Sigma\}$, but not quite. We give in the following section an example which shows that this is not necessarily the case.

The theorem below indicates how to compute C from B.

Theorem 6 *Let $\{\Sigma\}$ be a prime differential ideal and Ω be a regular system with respect to a ranking $\mathcal{R}_1$ such that $\{\Sigma\} = [A] : H_\Omega^\infty$. Let B be a Gröbner basis of $(A) : H_\Omega^\infty$ computed with respect to the order $\mathcal{R}_2$ induced by $\mathcal{R}_1$.*

The following algorithm calculates a characteristic set C of the ideal $\{\Sigma\}$, with respect to the ranking $\mathcal{R}_1$, from the basis B.

begin
    Assume that the elements of $B = b_1 < \cdots < b_m$
      are arranged in increasing order.
    $C := \{b_1\}$
    for $i := 2, \ldots, m$ **do**
        let u_i and u_{i-1} be the leaders of b_i and b_{i-1}
        if $u_i \ne u_{i-1}$ **then**
            $C := C \cup \{b_i \operatorname{rem} C\}$
        endif
    end
end

Proof. We are going to successively establish the following points:

1. To determine C amounts to determining a characteristic set of the prime ideal $(C) : H_C^\infty$, with respect to the order $\mathcal{R}_1$.

2. B is a Gröbner basis of $(C) : H_C^\infty$.

3. Let $p = I_p \cdot u^{d_p} + R_p$ be a polynomial of $(B) = (C) : H_C^\infty$, whose initial I_p is not in the ideal. There exists then in B a polynomial $b = I_b \cdot u^{d_b} + R_b$ with $d_b \le d_p$ and there exists in C a polynomial $c = I_c \cdot u^{d_c} + R_c$ with $d_c \le d_p$.

Since neither I_b, nor I_c, appear in $(B) = (C) : H_C^\infty$, and since B and C are two subsets of the ideal, the algorithm described in the theorem extracts from B a set of polynomials of the same rank as C, but which is not necessarily autoreduced in the sense of Ritt. The proof of the theorem is completed by:

4. The reductions carried out by the algorithm may not reduce the rank of the polynomials extracted from the basis. □

Proof of 1. See [Ro]. The characteristic set of a differential ideal, autoreduced by definition, is coherent since it reduces to zero every polynomial (in particular the Δ–polynomials) of the ideal. We apply the lemma of Rosenfeld. $(C):H_C^\infty$ is the intersection of the prime differential ideal $[C]:H_C^\infty$ and the ring of partially reduced polynomials with respect to C. The ideal $(C):H_C^\infty$ is then prime.

To say that a coherent and autoreduced set C is not a characteristic set of $[C]:H_C^\infty$, is to say that there exists in that ideal a non-zero polynomial p, reduced with respect to C. By the lemma of Rosenfeld, this is to say that p belongs to $(C):H_C^\infty$ and hence C is not a characteristic set of $(C):H_C^\infty$. □

Proof of 2. Since $\{\Sigma\} = [C]:H_C^\infty$ (see [Ko], lemma 2, page 167) and $\{\Sigma\} = [A]:H_\Omega^\infty$, by lemma 5, we have $(B) = (C):H_C^\infty$. □

Proof of 3. Let $p = I_p \cdot u^{d_p} + R_p$ be a polynomial of $(B) = (C):H_C^\infty$, whose initial I_p is not in the ideal. Suppose the head monomial m_i of I_p under normal form modulo B. Since p is reduced to zero by B, there exists a polynomial b of B whose head monomial divides the head monomial $m_p = m_i \cdot u^{d_p}$ of p, but does not divide m_i. The rank of b is then u^{d_b} with $0 < d_b \leq d_p$.

Since $(B) = (C):H_C^\infty$ is prime and since I_p does not belong to the ideal, C does not reduce I_p to zero. There exists then in the characteristic set a polynomial $c = I_c \cdot u^{d_c} + R_c$ with $0 < d_c \leq d_p$. □

Proof of 4. This is immediate since the initials of the polynomials of B do not belong to $(B) = (C):H_C^\infty$, the ideal is prime and the characteristic set of a prime ideal reduces to zero only the elements of the ideal. □

6 Examples

The algorithms described in the preceding sections have been programmed (see [Bo], VI) in the language C. The manipulations of big numbers are effected by the library of PARI. The Gröbner bases computations are by the software GB (see [FGLM]).

The computations are done on the IBM RS/6000 station cosme.polytechnique.fr. The timing of computation are given by the UNIX command *time*.

6.1 Membership testing

We first give a very simple example to illustrate splittings and to show how to test membership in radical differential ideals. We deal with

$$\Sigma \left\{ \begin{array}{l} (2\ddot{x}+1)\dot{y}+y=0 \\ \dot{x}^2+x=0. \end{array} \right.$$

For the ranking $\theta x < \phi y$ (for all derivation operators θ and ϕ), the first equation may be reduced by the second one. Its remainder is $\dot{x}y$. Σ is thus split into two systems:

$$\Gamma_2 \left\{ \begin{array}{l} \dot{x}y=0 \\ \dot{x}^2+x=0 \\ \dot{x}\neq 0 \end{array} \right. \quad \text{and } \Gamma_1 \left\{ \begin{array}{l} (2\ddot{x}+1)\dot{y}+y=0 \\ \dot{x}^2+x=0 \\ \dot{x}=0. \end{array} \right.$$

The system Γ_2 gives immediately a regular system $\Omega_2 = \Gamma_2$. The Gröbner basis computation only simplifies the factor $\dot{x}$ in the first equation: $B_2 = \{y, \dot{x}^2+x\}$. The system Γ_1 leads with no splittings to the regular system below. The Gröbner basis computation is useless.

$$\Omega_1 \left\{ \begin{array}{l} \dot{y}+y=0 \\ x=0 \end{array} \right.$$

Now, we may verify that $(2\ddot{x}+1) \notin \{\Sigma\}$. We apply the theorem 5: $(2\ddot{x}+1)$ is reduced to zero by $(\dot{x}^2+x)$ in Ω_1, but reduced to 1 in Ω_2.

We may also verify that $\dot{x}(2\ddot{x}+1)$, which is the first derivative of $(\dot{x}^2+x)$, belongs to $\{\Sigma\}$. This polynomial is reduced to zero by both systems Ω_2 and Ω_1.

6.2 Hidden algebraic contradictions

The following example does not have any physical significance. It shows the necessity to assure that the regular systems have models.

Consider the following system in $\mathbb{Q}\{u, v\}$ equiped with three derivations δ_x, δ_y and δ_z. The derivation operators are denoted by subscripts.

$$u_y^2 u_x^2 = 2u_y u_x - 1, \quad u_{xy} = v, \quad v_x = u_x v_z, \\ v_y = u_y v_z, \quad u_z^3 = u_x u_y.$$

The ranking $\mathcal{R}_1$ used for the calculations is the following:

1) $\theta u > \phi v$ for all derivation operators θ, ϕ,

2) $\theta u > \phi u$ if $\theta > \phi$ for the lexicographic order given by $\delta_x > \delta_y > \delta_z$ (same choice for v).

The Rosenfeld–Gröbner algorithm computes two regular systems in a little more than 6 seconds:

$$\left\{ \begin{array}{l} v_z v_{yz} - v_{zz} v_y = 0, \\ (v_z^2 v_y v_{yy} + (-v_{zz} + v v_z) v_y^3) v_x - v_z^4 v_{yy} \\ \qquad\qquad + (v_z^2 v_{zz} - v v_z^3) v_y^2 = 0, \\ u_z^3 - 1 = 0, \quad v_z u_y - v_y = 0, \\ (v_z^2 v_y v_{yy} + (-v_{zz} + v v_z) v_y^3) u_x - v_z^3 v_{yy} \\ \qquad\qquad + (v_z v_{zz} - v v_z^2) v_y^2 = 0, \\ v_z \neq 0, \quad v_z v_y v_{yy} - v_y^2 v_{yz} + v v_y^3 \neq 0, \quad v_y \neq 0 \\ u_z \neq 0, \quad v_y^2 v_x - v_z^2 v_y \neq 0, \\ v_z^2 v_y v_{yy} + (-v_{zz} + v v_z) v_y^3 \neq 0 \end{array} \right.$$

$$\left\{ \begin{array}{l} v=0 \\ u_z^3 - 1 = 0 \\ u_{yy} = 0 \\ u_y u_x - 1 = 0 \\ u_z \neq 0 \\ u_y \neq 0 \end{array} \right.$$

The first is inconsistent. Remark that it is not detected before the Gröbner bases computation, although our implementation of the splitting process looks for simple contradictions: the final algebraic treatment is necessary. Here is the Gröbner basis associated with the second system:

$$v, \quad u_z^3 - 1, \quad u_{yy}, \quad u_x u_y - 1.$$

6.3 Computing a characteristic set

The example below, which has no physical significance, shows the necessity to proceed with the described reductions in theorem 6 to obtain a characteristic set of a differential ideal that (we know) is prime.

Let Σ be the following system of ordinary differential equations:

$$\begin{cases} \ddot{x} = y\dot{x} + \dot{y} + 1 \\ \ddot{y} = 2\dot{y}x + 2\dot{x}yx + y + 2x \\ z = y \end{cases}$$

The differential ideal $[\Sigma]$ is prime, since the system is orthonomic ($H_A^\infty = \{1\}$) and autoreduced[5] with the ranking:

1) $\theta z > \phi y$ and $\theta z > \psi x$ for all derivation operators θ, ϕ and ψ,

2) $\phi y > \psi x$ if the order of ϕ is larger or equal to that of ψ,

3) $\psi x > \phi y$ if the order of ψ is strictly larger than that of ϕ.

We now apply the Rosenfeld–Gröbner algorithm to Σ with the elimination order:

1) $\theta z > \phi y > \psi x$ for all operators θ, ϕ and ψ.

We obtain (in a bit more than 3 seconds) a unique regular system Ω_1. The Gröbner basis B_1 that is associated to it is:

$$\begin{aligned} p_1 &= ((\ddot{x} - \dot{x}^2 + 1)x^{(4)} - {x^{(3)}}^2 + (3\dot{x}\ddot{x} + 2x\dot{x}^2 - \dot{x} \\ &\quad - 2x)x^{(3)} - 2\ddot{x}^3 + ((-6x - 2)\dot{x} - 1)\ddot{x}^2 + ((2x \\ &\quad + 2)\dot{x}^3 + \dot{x}^2 + (-2x - 2)\dot{x} + 2)\ddot{x} - \dot{x}^2 + 1) \\ p_2 &= ((\ddot{x} - \dot{x}^2 + 1)y - x^{(3)} + (\dot{x} + 2x)\ddot{x} - \dot{x}) \\ p_3 &= ((x^{(3)} - 2\dot{x}^3 + 2\dot{x})y - x^{(4)} + (-2\dot{x} + 2x)x^{(3)} \\ &\quad + 2\ddot{x}^2 + (2\dot{x}^2 + (6x + 2)\dot{x} - 1)\ddot{x} - 2\dot{x}^2 - 1) \\ p_4 &= (z - y). \end{aligned}$$

If we extract a characteristic set from B_1, without effecting the described reduction in theorem 6, we obtain an autoreduced set $A = p_1, p_2$, which is not a characteristic set of the ideal $[\Sigma]$ (the polynomial p_4 in fact does not leave since it is not reduced with respect to p_2). Apply the theorem 6 by reducing p_4 by p_2. We obtain then a characteristic set C of $[\Sigma]$:

$$p_1, \; p_2, \; ((\ddot{x} - \dot{x}^2 + 1)z - x^{(3)} + (\dot{x} + 2x)\ddot{x} - \dot{x}).$$

Remark. In practice, we may often do without Rosenfeld–Gröbner for generating the system Ω_1: the majority of the time, we know that an ideal $[\Sigma]$ is prime by showing a ranking $\mathcal{R}$ for which Σ is orthonomic, autoreduced and coherent (cf. the example above). The ranking $\mathcal{R}$ furnishes a characteristic set, hence a membership testing algorithm of the ideal $[\Sigma]$, which permits avoiding the splittings.

[5] It is necessarily coherent, since it only involves ordinary differential equations.

7 Conclusion

Although the models of the regular systems produced by the Rosenfeld-Gröbner algorithm are disjoint, the regular differential ideals which are defined by them may be redundant. In particular, the algorithm may produce many systems, even when the differential ideal $\{\Sigma\}$ is prime.

We do not know how to decide the inclusion of two regular differential ideals. It is a problem very close to the problem of Ritt: to decide the inclusion of two prime differential ideals each given by a characteristic set, which *"seems very far from solution"* ([Ko], page 166). Its solution would allow us to decide if a differential ideal given by a finite family of generators is prime.

References

[Bo] F. Boulier.– *Étude et implantation de quelques algorithmes en algèbre différentielle* (Thèse de l'Université des Sciences et Technologies de Lille, (1994))

[Bu] B. Buchberger.– *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero–Dimensional Polynomial Ideal (German)* (Ph. D. Thesis. Math. Inst. Univ. of Innsbruck, Austria 1965, and Aequationes Math. **4/3** (1970), 374–383)

[Ca] G. Carrà–Ferro.– *Gröbner bases and differential ideals* (notes de AAECC5, Menorca, Spain, Springer Verlag (1987), 129–140)

[F] M. Fliess.– *Automatique et corps différentiels* (Forum Math. I, 227–238)

[FGLM] J. C. Faugère, P. Gianni, D. Lazard, T. Mora.– *Efficient computation of Gröbner bases by change of orderings* (Journal of Symb. Comp. **16** (1993), 329–344)

[GMO] G. Gallo, B. Mishra, F. Ollivier.– *Some Constructions in Rings of Differential Polynomials* (Lecture Notes in C. Sc. Vol. 539 (AAECC–9), 171–182)

[Ko] E. R. Kolchin.– *Differential Algebra and Algebraic Groups* (Academic Press, New York (1973))

[Ma] E. Mansfield.– *Differential Gröbner bases* (PhD thesis, University of Sydney, (1991))

[Ol] F. Ollivier.– *Le problème de l'identifiabilité structurelle globale : approche théorique, méthodes effectives et bornes de complexité* (Thèse de doctorat, École Polytechnique (1990))

[Ri] J. F. Ritt.– *Differential Algebra* (Amer. Math. Soc, New York (1950))

[Ro] A. Rosenfeld.– *Specializations in differential algebra* (Trans. Amer. Math. Soc. **90** (1959), 394–407)

[Se1] A. Seidenberg.– *An elimination theory for differential algebra* (Univ. California Publ. Math. (N.S.) (1956), 31–38)

[Se2] A. Seidenberg.– *Some basic theorems in differential algebra (characteristic p arbitrary)* (Trans. Amer. Math. Soc. **73** (1952), 174–190)

[Tr] W. L. Trinks.– *Über B. Buchbergers Verfahren Systeme algebraischer Gleichungen zu lösen* (J. Number Theory **10** (1978), 475–488)