



## Factorization-free Decomposition Algorithms in Differential Algebra

EVELYNE HUBERT<sup>†</sup>

*MSRI, 1000 centennial drive, Berkeley, CA 94720-5070, U.S.A.*

---

Insight on the structure of differential ideals defined by coherent autoreduced set allows one to uncouple the differential and algebraic computations in a decomposition algorithm. Original results as well as concise new proofs of already presented theorems are exposed. As a consequence, an effective version of Ritt's algorithm can be simply described.

© 2000 Academic Press

---

### 1. Introduction

This paper makes a contribution to differential elimination and more precisely to the problem of computing a representation of the radical differential ideal generated by a system of differential equations (ordinary or partial). The approach we use here involves characteristic set techniques;<sup>‡</sup> these were introduced by J. F. Ritt, the founder of differential algebra. The basic idea is to write the radical differential ideal generated by a finite set  $\Sigma$  of differential polynomials as an intersection of differential ideals that are uniquely defined by their characteristic sets. We will call these latter differential ideals components of  $\{\Sigma\}$  and we will call their intersection the *characteristic decomposition* of  $\{\Sigma\}$ .

With a characteristic decomposition of  $\{\Sigma\}$  we can determine whether  $\Sigma = 0$  has any solution, test membership to  $\{\Sigma\}$  and study the dimension properties of  $\{\Sigma\}$ . Similar to algebraic elimination methods, by choosing an appropriate *ranking*, an algorithm to compute a characteristic decomposition can also answer questions like: do the solutions of  $\Sigma = 0$  satisfy:

- An algebraic equation? Find all such constraints.
- An ordinary differential equation in one of the independent variables? Find these ordinary differential equations.
- A differential equation involving only a specific subset of the dependent variables? Find these differential equations.

Algorithms in differential elimination have been applied in symmetry analysis of partial differential equations (Clarkson and Mansfield, 1994; Mansfield *et al.*, 1998) and control theory (Diop, 1991, 1992; Fliess and Glad, 1993).

Ritt (1950) gave an algorithm to compute a characteristic decomposition of  $\{\Sigma\}$  where

<sup>†</sup>Current address: INRIA - BP93 - F-06902 Sophia Antipolis; E-mail: [Evelyne.Hubert@inria.fr](mailto:Evelyne.Hubert@inria.fr)

<sup>‡</sup>Differential analogues of Gröbner bases techniques were studied by Carra'Ferro (1987), Ollivier (1990) and Mansfield (1991).

the components are prime differential ideals. Seidenberg (1956) gave an effective algorithm to answer the question of the existence of a solution to an algebraic differential system. Inspired by this elimination theory, Boulier *et al.* (1995) pioneered an effective approach to the problem of the representation of a radical differential ideal generated by a finite set of differential polynomials. The extended algorithm presented in Boulier *et al.* (1997) computes a characteristic decomposition of  $\{\Sigma\}$ . In the ordinary case Maârouf *et al.* (1998) provided means to compute a characteristic decomposition in the spirit of Ritt's algorithm. All these methods work by interweaving differential reductions with algebraic operations. The algebraic operations are factorization over towers of algebraic extensions in Ritt (1950), Gröbner bases in Boulier *et al.* (1997) and computation of inverse polynomials in towers of algebraic extensions in Maârouf *et al.* (1998).

The main original contribution of this paper is to provide the tool that enables one to uncouple completely the typically differential operations from the purely algebraic operations in any of the above-mentioned decomposition algorithms. We also show that all the purely algebraic computations can be made in dimension zero, by enlarging the field of coefficients. More specifically, we show that the algorithms can be flattened out into two parts. The first part consist in computing a decomposition into *coherent components*. The second part consist in computing a characteristic decomposition for each coherent component. We show (Theorem 6.2) that a characteristic decomposition of a coherent component can be lifted directly from an irredundant characteristic decomposition of the associated polynomial ideal. We furthermore show (Theorem 3.10) that the latter characteristic decomposition can in turn be lifted directly from one computed in dimension zero, whatever the technique used for computing this latter decomposition.<sup>†</sup>

The two consecutive liftings are shown to be possible by clarifying the structure of the (differential) ideals defined by (coherent) autoreduced sets. We will give simple necessary and sufficient conditions for these ideals to be *characterizable* (Lemmas 3.5, 3.9 and 6.1).

Although there is practical evidence<sup>‡</sup> that Theorems 6.2, 3.10 and Lemma 3.5 seriously decrease the computation time, efficiency will not be an issue in this paper. We instead wish to acquire a wider audience by giving a complete but comparatively simple decomposition algorithm. For the differential part we will review Ritt's approach and make it factorization-free. The method used here for the purely algebraic part is based on Gröbner bases computations. More recent triangular set techniques by Lazard (1992) and Kalkbrenner (1993) would nonetheless provide an efficient and esthetically more consistent substitute.

In this article we will have to compute irredundant decomposition of *coherent components*. Nonetheless the complete decomposition of  $\{\Sigma\}$  computed is not generally minimal—neither are the previously cited decompositions. Only for the case where  $\Sigma$  consists of a single differential polynomial are there known algorithms to eliminate the redundancy in the decomposition (Ritt, 1936; Kolchin, 1973; Hubert, 1997, 1999).

In this paper, we adhere to the traditional mathematical objects of differential algebra, such as autoreduced sets and characteristic sets. The underlying reasons are, on the one hand, to highlight the basic scheme of a decomposition algorithm, and, on the other hand, keep the paper of reasonable size and self-contained in the sense that only refer-

<sup>†</sup>We thus go much beyond the use of dimension zero made by Boulier *et al.* (1997), whose claim was that the computations of the Gröbner bases involved in the Rosenfeld–Gröbner algorithm could be made in dimension zero.

<sup>‡</sup>See the comparison table on <http://daisy.uwaterloo.ca/~ehubert/Diffalg>.

ence to textbooks—mainly Kolchin (1973)—is required. Nonetheless, the generalizations of the definitions and consequences of *autoreduced sets*, *characteristic sets*, *coherence* investigated in more recent works both in algebra<sup>†</sup> and in differential algebra would entail a better efficiency. These generalizations can actually be smoothly incorporated in the framework of the present paper.

Readers interested in using an implementation of the algorithm presented in Boulier *et al.* (1997) modified according to the contributions of this paper are invited to visit the website <http://daisy.uwaterloo.ca/~ehubert/Diffalg> to download the MAPLE V package `diffalg99`, as well as examples of use and applications. The package `diffalg99` is a completion and improvement over the `diffalg` package by F. Boulier. The different versions of `diffalg` are part of the main library of MAPLE V.5 and the following releases. They have been developed at the Symbolic Computation Group, University of Waterloo, during the postdoctoral stays of F. Boulier and the author.

Given a finite set of differential polynomials  $\Sigma$ , in Section 5 we show how to compute a first decomposition of  $\{\Sigma\}$ , a decomposition into *coherent components*, with differential reductions. This is the differential part of the algorithm that is adapted from Ritt's algorithm. The rest of the algorithm requires no further differentiation. In Section 6, the properties and the *irredundant characteristic* decomposition of a coherent component are shown to be the lifting to the differential case of properties and decomposition of ideals defined by autoreduced sets in a finitely generated polynomial algebra. We thus start our investigation around the properties of such ideals; this is the purpose of Section 3. This section also details the purely algebraic part of the algorithm. Section 2 mainly recollects the definitions and basic results in differential algebra. Section 7 recapitulates the complete algorithm and gives two examples of applications.

## 2. Differential Ideal Theory

Differential algebra extends the concepts of polynomial algebra to differential equations. The purpose of this section is to give the basic information for reading this paper. We base our paper on the material found in Kolchin (1973). We will recall the definitions to ease the reading but we will omit the proofs to lighten the paper. More detailed presentation can be found in Ritt (1950), Kaplansky (1970), Kolchin (1973), Boulier (1994), Hubert (1997). The reader already familiar with Kolchin (1973)—more specifically with the characteristic zero version of it—needs only to look at the notation  $S^\infty$  and the definition of characteristic set<sup>‡</sup> and decomposition.

### 2.1. RING OF DIFFERENTIAL POLYNOMIALS

We consider *differential rings*  $(\mathcal{R}, \Theta)$ , where  $\mathcal{R}$  is a commutative integral domain that contains a field isomorphic to  $\mathbb{Q}$ , and  $\Theta$  is the free commutative monoid of derivation operators generated by a finite set of *derivations*  $\Delta$ . When  $\Delta$  consists of a single derivation  $\delta$  we shall speak of the ordinary differential ring  $\mathcal{R}$ . Let  $\Sigma$  be a subset of  $\mathcal{R}$ . We denote respectively  $[\Sigma]$  and  $\{\Sigma\}$  the differential ideal and the radical differential ideal generated by  $\Sigma$ .

<sup>†</sup>See the review of Aubry *et al.* (1999).

<sup>‡</sup>What is usually defined is a *characteristic set of a (differential) ideal*. We define furthermore *characteristic set* as a stand-alone term.

$(\mathcal{R}\{Y\}, \Theta)$  denotes the ring of differential polynomials with differential indeterminates  $Y = \{y_1, \dots, y_n\}$  and coefficients in  $(\mathcal{R}, \Theta)$ . In ring theoretic terms,  $\mathcal{R}\{Y\}$  is the polynomial ring in infinitely many indeterminates  $\mathcal{R}[\Theta Y] = \mathcal{R}[\{\theta y_i, y_i \in Y, \theta \in \Theta\}]$ . We will consider rings  $\mathcal{F}\{Y\}$  of differential polynomials the coefficients of which belong to a differential field  $\mathcal{F}$  of characteristic zero. For computational purposes we will typically choose a rational function field  $\mathcal{F} = \mathcal{K}(t_1, \dots, t_\mu)$  where  $\mathcal{K}$  is a finite extension of  $\mathbb{Q}$ .

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

Let  $S$  be a subset of  $\mathcal{F}\{Y\}$ . We denote by  $S^\infty$  the multiplicative-free monoid generated by 1 and the irreducible factors of the elements of  $S$ .<sup>†</sup> Let  $I$  be a differential ideal of  $\mathcal{F}\{Y\}$ . We define the saturation of  $I$  by a set  $S$  as  $I : S^\infty = \{q \in \mathcal{F}\{Y\} \mid \exists s \in S^\infty sq \in I\}$ .  $I : S^\infty$  is also a differential ideal and we have  $I \subset I : S^\infty$ . This practical way of defining the saturation of an ideal comes, to our knowledge, from Morrison (1999). When  $S$  is finite, we can match the usual definition by assigning  $s$  to the product of its elements. What we call  $I : S^\infty$  is in fact equal to  $\{q \in \mathcal{F}\{Y\} \mid \exists \alpha \in \mathbb{N} s^\alpha q \in I\}$  that is usually denoted  $I : s^\infty$ .

Consider a prime differential ideal  $P$  of  $\mathcal{F}\{Y\}$ .  $P : S^\infty$  is either equal to  $P$  or  $\mathcal{F}\{Y\}$  according to whether  $S \cap P$  is empty or not. As a consequence, if  $J$  is a radical differential ideal of  $\mathcal{F}\{Y\}$ ,  $J : S^\infty$  is the intersection of the essential components of  $J$  that have an empty intersection with  $S$ .

**PROPOSITION 2.1.** *Let  $\Sigma$  be a non-empty subset of  $\mathcal{R}$ . Let  $a_1, \dots, a_r \in \mathcal{R}$ ; we have  $\{\Sigma, \prod_{i=1}^r a_i\} = \bigcap_{i=1}^r \{\Sigma, a_i\}$ . Let  $S$  be a finite subset of  $\mathcal{R}$ ; we have  $\{\Sigma\} : S^\infty \cap (\bigcap_{s \in S} \{\Sigma, s\})$ .*

## 2.2. REDUCTION

A *ranking* over  $\mathcal{F}\{Y\}$  is a total order on  $\Theta Y = \{\theta y_i, i = 1, \dots, n, \theta \in \Theta\}$  such that for any derivative  $u \in \Theta Y$  we have  $\delta u \geq u, \forall \delta \in \Delta$  and for any pair of derivatives  $u, v \in \Theta Y$  with  $u \geq v$  we have  $\delta u \geq \delta v, \forall \delta \in \Delta$ . Any decreasing sequence of derivatives is finite (Kolchin, 1973, I.8). From now on  $\mathcal{F}\{Y\}$  will be understood to be endowed with a ranking.

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

$$p = i_p u_p^d + i_{d-1} u_p^{d-1} + \dots + i_0,$$

$$\theta p = s_p \theta u_p + q, \quad \text{where } q \text{ has no derivative equal to or higher than } \theta u_p.$$

The rank of  $p$  is  $u_p^d$ . An element  $q \in \mathcal{F}\{Y\}$  is said to have higher rank than  $p$  when its leader ranks higher than  $u_p$  or is equal but with a higher degree in  $q$ . The ranking on the derivatives thus induces a partial order on the differential polynomials of  $\mathcal{F}\{Y\}$ . A differential polynomial  $q$  is *partially reduced w.r.t. p* if no proper derivatives of  $u_p$  appears in  $q$ ;  $q$  is *reduced w.r.t. p* if  $q$  is partially reduced w.r.t. to  $p$  and the degree of  $q$  in  $u_p$  is strictly less than the degree of  $p$  in  $u_p$ .

<sup>†</sup>The complement of  $S^\infty$  in  $\mathcal{F}\{Y\}$  is therefore a prime ideal.

SPARSE PSEUDO-DIVISION

Let  $\mathcal{R}[x]$  be a ring of polynomials with coefficients in the ring  $\mathcal{R}$ . Let  $p, q \in \mathcal{R}[x]$ ,  $d, e$  the respective degrees of  $p, q$  in  $x$ ,  $c$  the coefficient of  $x^d$  in  $p$ . The pseudo-remainder of  $q$  w.r.t.  $p$  is defined as the polynomial  $\bar{q}$  such that  $\deg_x \bar{q} < \deg_x p$  and  $c^{e-d} q \equiv \bar{q} \pmod{p}$  when  $e \geq d$ . A sparse pseudo-remainder is usually defined by taking a power of  $c$  as small as possible. What we will call a sparse pseudo-remainder of  $q$  with respect to  $p$  is a polynomial  $\text{srem}(q, p, x)$  of degree in  $x$  strictly lower than that  $p$  such that  $\exists h \in c^\infty$   $h q \equiv \text{srem}(q, p) \pmod{p}$ ;  $h$  is taken as small as possible to limit the expressions swell.  $\mathcal{R}$  is usually a ring of polynomials over a field and we shall use gcd computations to find  $h$  and  $\text{srem}(q, p, x)$ .

DIFFERENTIAL REDUCTION

Let  $p$  and  $q$  be differential polynomials in  $\mathcal{F}\{Y\}$ ; with a finite number of differentiations and sparse pseudo divisions we can compute  $\text{d-prem}(q, p)$  and  $\text{d-rem}(q, p)$  respectively partially reduced and reduced with respect to  $p$  such that  $\exists s \in (s_p)^\infty$  and  $h \in (s_p i_p)^\infty$  such that  $s q \equiv \text{d-prem}(q, p) \pmod{[p]}$  and  $h q \equiv \text{d-rem}(q, p) \pmod{[p]}$ .

ALGORITHM 2.2. **d-rem ( or d-prem )**

Input:  $p, q \in \mathcal{F}\{Y\}$ .  
 Output:  $\bar{q}$  (partially) reduced w.r.t.  $p$  and such that  $\exists h \in (s_p i_p)^\infty$  (or  $s_p^\infty$ ),  $h q \equiv \bar{q} \pmod{[p]}$ .  
 $\bar{q} := q$ ;  
 While  $q$  is not (partially) reduced w.r.t.  $p$  do  
      $\theta u_p :=$  the highest ranking derivative of  $u_p$  in  $q$ .  
      $\bar{q} := \text{srem}(\bar{q}, \theta p, \theta u_p)$ ;  
 od;

2.3. AUTO-REDUCED SETS AND CHARACTERISTIC SETS

Let  $\mathcal{F}\{Y\}$  be endowed with a ranking. A subset  $A$  of  $\mathcal{F}\{y_1, \dots, y_n\}$  is called an autoreduced set if no element of  $A$  belongs to  $\mathcal{F}$  and each element of  $A$  is reduced w.r.t. all the others. Distinct elements of  $A$  have distinct leaders and  $A$  must be finite (Kolchin, 1973, I.9). We denote  $I_A$  the set of the initials of the elements of  $A$ ,  $S_A$  the set of the separants of the elements of  $A$ ,  $H_A = I_A \cup S_A$ ,  $\mathcal{L}(A)$  the set of the leaders of the elements of  $A$ ,  $\mathfrak{N}(A)$  the set of derivatives present in  $A$  that are not the leaders of elements of  $A$ . Thus  $\mathfrak{N}(A) \cup \mathcal{L}(A)$  is the finite subset of  $\Theta Y$  of the derivatives present in  $A$ .

For an autoreduced set  $A$ ,  $(A)$  denotes the ideal generated by  $A$  in the finitely generated polynomial algebra  $\mathcal{F}[\mathfrak{N}(A) \cup \mathcal{L}(A)]$ . Note that  $H_A \subset \mathcal{F}[\mathfrak{N}(A) \cup \mathcal{L}(A)]$  so that  $(A) : I_A^\infty, (A) : S_A^\infty, (A) : H_A^\infty$  are also understood to be ideals in this algebra.

A differential polynomial is said to be (partially) reduced w.r.t. an autoreduced set  $A$  when it is (partially) reduced w.r.t. each element of  $A$ . Given an element  $q \in \mathcal{F}\{Y\}$  we can compute  $s \in S_A^\infty$  and  $\text{d-prem}(q, A)$  that is partially reduced w.r.t.  $A$  such that  $s q \equiv \text{d-prem}(q, A) \pmod{[A]}$ . Similarly, we can compute  $h \in H_A^\infty$  and  $\text{d-rem}(q, A)$  that is reduced w.r.t.  $A$  such that  $h q \equiv \text{d-rem}(q, A) \pmod{[A]}$ .

**ALGORITHM 2.3. d-rem (or d-prem )**

**Input:**  $q \in \mathcal{F}\{Y\}$ ,  $A$  an autoreduced set of  $\mathcal{F}\{Y\}$ .  
**Output:**  $\bar{q}$  (partially) reduced w.r.t.  $A$  and such that  
 $\exists h \in H_A^\infty$  (or  $\in S_A^\infty$ ) such that  $hq \equiv \bar{q} \pmod{[A]}$ .  
 $\bar{q} := q$ ;  
**While**  $q$  is not (partially) reduced w.r.t.  $A$  **do**  
 $a :=$  an element of  $A$  s.t.  $\bar{q}$  is not reduced w.r.t.  $a$ ;  
 $\bar{q} := \text{d-rem}(\bar{q}, a)$  (or  $\text{d-prem}(\bar{q}, a)$ );  
**od**;

A ranking on  $\mathcal{F}\{Y\}$  induces a partial order on the autoreduced sets of  $\mathcal{F}\{Y\}$ . Let  $A = a_1, \dots, a_r$  and  $B = b_1, \dots, b_s$  be autoreduced sets arranged in order of increasing rank.  $A$  is said to be of lower rank than  $B$  when either:

- there exists  $1 \leq k \leq r, s$  such that the rank of  $a_i$  and  $b_i$  are the same for  $1 \leq i \leq k-1$  and the rank of  $a_k$  is less than the rank of  $b_k$ .
- $r > s$  and the rank of  $a_i$  is equal to the rank of  $b_i$ ,  $1 \leq i \leq s$ .

**DEFINITION 2.4.** An autoreduced set  $A$  in  $\mathcal{F}\{Y\}$  is a characteristic set of a differential ideal  $I$  if one of the following equivalent conditions holds:

- $A$  is of minimal rank among the autoreduced sets of  $I$ .
- $A \subset I$  and  $\forall q \in I$ ,  $\text{d-rem}(q, A) = 0$ .
- there is no non-zero element of  $I$  reduced w.r.t.  $A$ .

Thus, any two characteristic sets of a differential ideal have the same rank. Every differential ideal  $I$  admits a characteristic set (Kolchin, 1973, I.10, Proposition 3). If  $A$  is a characteristic set of the differential ideal  $I$  in  $\mathcal{F}\{Y\}$  then  $[A] \subset I \subset [A]:H_A^\infty$ .

**EXAMPLE 2.5.** Consider, in  $\mathcal{F}\{x, y\}$  endowed with a ranking such that  $x < y$ , the autoreduced set  $A = (x-1)y-1, x^2-1$ . Note that  $(x+1) \in [A]:H_A^\infty$  although it is reduced w.r.t.  $A$ . An autoreduced set  $A$  is not obviously a characteristic set of  $[A]:H_A^\infty$  nor of  $(A):H_A^\infty$ .

When  $A$  is a characteristic set of  $[A]:H_A^\infty$  then  $q \in [A]:H_A^\infty \Leftrightarrow \text{d-rem}(q, A) = 0$ . This fact will be central. We therefore extend the scope of the denomination *characteristic sets* and introduce some additional vocabulary to speak at ease of such autoreduced sets and of the ideals thus defined.

**DEFINITION 2.6.** An autoreduced set  $A$  of  $\mathcal{F}\{Y\}$  is a characteristic set if  $A$  is a characteristic set of  $[A]:H_A^\infty$ . A differential ideal  $I$  of  $\mathcal{F}\{Y\}$  is said to be characterizable if for a characteristic set  $A$  of  $I$  we have  $I = [A]:H_A^\infty$ . Then  $A$  is said to characterize  $I$ .

Prime differential ideals are characterizable for any ranking. This is the property that Ritt (1950) and Kolchin (1973) used in their work. Recent algorithmic improvements in differential algebra owes to the idea of using a wider class of differential ideals than prime differential ideals. And, indeed characterizable differential ideals that are not prime do exist; but, this then depends on the ranking (see Example 3.6). We will see that a characterizable differential ideal is radical (Theorem 4.4) and has specific dimension properties (Theorem 4.5).

2.4. CHARACTERISTIC DECOMPOSITION—DEFINITION

Let  $J$  be a radical differential ideal of  $\mathcal{F}\{Y\}$ . We call a *characteristic decomposition* of  $J$  a representation of  $J$  as an intersection of characterizable differential ideals, called *components* of  $J$ . Such a characteristic decomposition of  $J$  exists:  $J$  is the intersection of prime differential ideals and prime differential ideals are characterizable.

Given a finite set  $\Sigma$  of differential polynomials of  $\mathcal{F}\{Y\}$ , computing a characteristic decomposition of  $\{\Sigma\}$  means finding the characteristic sets of its components. In other words, given  $\Sigma$ , we want to compute characteristic sets  $C_1, \dots, C_r$  such that  $\{\Sigma\} = \bigcap_{i=1}^r [C_i] : H_{C_i}^\infty$ .

A characteristic decomposition of a radical differential ideal  $J$  will be said to be *irredundant* if associating each component in the decomposition with the set of its essential prime components yields a partition of the set of the essential prime components of  $J$ . In other words, consider a characteristic decomposition of  $J$ ,  $J = \bigcap_{i=1}^r [C_i] : H_{C_i}^\infty$ . This decomposition is irredundant if any prime differential ideal that contains two distinct components  $[C_i] : H_{C_i}^\infty$  is not an essential prime component of  $J$ .

**3. Results in Finitely Generated Polynomial Algebras**

This section contains all the purely algebraic material needed to achieve a decomposition algorithm in differential algebra. We work in a ring of polynomials in finitely many indeterminates  $x_1, \dots, x_n$  with coefficients in a field  $\mathcal{K}$  of characteristic zero:  $\mathcal{K}[X] = \mathcal{K}[x_1, \dots, x_n]$ . The underlying ranking is given by  $x_1 < \dots < x_n$ .

The first subsection presents the properties of (non-differential) ideals  $(A) : S_A^\infty$  and  $(A) : H_A^\infty$ , where  $A$  is an autoreduced set of  $\mathcal{K}[X]$ . The second and third subsections give an algorithm to compute an irredundant characteristic decomposition of an ideal defined by an autoreduced set. The decomposition of  $(A) : H_A^\infty$  is completed in dimension zero (Theorem 3.7, Algorithm 3.8) and then only lifted to positive dimension (Theorem 3.10). Theorem 3.10 is an original contribution of this paper.

We give a method to compute the decomposition in dimension zero (Algorithm 3.8) that relies on Gröbner bases computations. That way, we establish the connection between characteristic sets and Gröbner bases (Lemma 3.5).

We shall assume, without loss of generality, that the set of indeterminates is equal to  $\mathfrak{L}(A) \cup \mathfrak{N}(A)$  so that  $\mathcal{K}[X] = \mathcal{K}[x_1, \dots, x_n] = \mathcal{K}[\mathfrak{N}(A)][\mathfrak{L}(A)]$ . We will denote  $\mathcal{K}_A = \mathcal{K}(\mathfrak{N}(A))$  and we will also consider the ring of polynomials  $\mathcal{K}_A[\mathfrak{L}(A)]$ . In situations where there might be some confusion, the ideals taken in  $\mathcal{K}[\mathfrak{N}(A)][\mathfrak{L}(A)]$  or in  $\mathcal{K}_A[\mathfrak{L}(A)] = \mathcal{K}(\mathfrak{N}(A))[\mathfrak{L}(A)]$  will be subscripted with  $\mathcal{K}$  or  $\mathcal{K}_A$ .

3.1. IDEALS DEFINED BY AUTOREDUCE SETS

The definitions and properties presented in Section 2 are immediately transposed to polynomial algebra by setting the derivations to be the trivial one. In this section we give two fundamental properties of the ideals  $(A) : S_A^\infty$  and  $(A) : H_A^\infty$ , where  $A$  is an autoreduced set in  $\mathcal{K}[X] = \mathcal{K}[\mathfrak{N}(A)][\mathfrak{L}(A)]$ .

The first property, Theorem 3.2, is essential in differential algebra to compute effectively a decomposition in coherent components (see Section 5). This property was first presented in a differential algebra context by Boulier *et al.* (1995) under the name of *Lazard's lemma*. Its proof was criticized and Morrison (1999) proposed another proof.

We give here a new and concise proof which makes the result a direct application of the Jacobian criterion for regularity. The second property, Theorem 3.2, will be used to reduce the computation to dimension zero. We claim no special originality in the proof of this second result.

**THEOREM 3.1.** *Let  $A$  be an autoreduced set of  $\mathcal{K}[X]$ .  $(A):S_A^\infty$  is a radical ideal.*

**PROOF.** If  $Q$  is a primary ideal and  $S$  is a subset of  $\mathcal{K}[X]$ ,  $Q:S^\infty$  is either equal to  $Q$  or  $\mathcal{K}[X]$  according to whether  $S$  has an empty intersection with  $\sqrt{Q}$  or not. Thus, for any ideal  $I$  and any subset  $S$  in a polynomial ring  $\mathcal{K}[X]$ ,  $I:S^\infty$  is equal to the intersection of those primary components of  $I$  with radical having an empty intersection with  $S$ .

The product of the separants of  $A$ ,  $s_A$ , is the determinant of a maximal square submatrix of the Jacobian matrix of  $A$ . This is due to the triangular shape of  $A$ . Thus  $s_A$  belongs to the Jacobian ideal<sup>†</sup> of  $(A)$ .

If  $1 \in (A):S_A^\infty$  the result is trivial. Assume  $1 \notin (A):S_A^\infty$ . By the Jacobian criterion for regularity (Vasconcelos, 1998, Corollary 5.2.1, p. 127), the primary components of  $(A)$  with radical not containing the Jacobian ideal are prime. This is the case of all the primary components of  $(A)$  the intersection of which is equal to  $(A):s_A^\infty$ . We have  $(A):s_A^\infty = (A):S_A^\infty$ . Thus  $(A):S_A^\infty$  is an intersection of prime ideals; it is a radical ideal.  $\square$

In this latter theorem and the next one, we could replace  $S_A$  by any subset  $H$  of  $\mathcal{K}[X]$  containing  $S_A$ . Indeed the primary components of  $(A):H^\infty$  form a subset of the primary components of  $(A):S_A^\infty$ .

**THEOREM 3.2.** *Let  $A$  be an autoreduced set of  $\mathcal{K}[X]$ . If  $1 \notin (A):S_A^\infty$  then any minimal prime of  $(A):S_A^\infty$  admits the set of non-leaders of  $A$ ,  $\mathfrak{N}(A)$ , as a transcendence basis. More specifically, any characteristic set of a minimal prime of  $(A):S_A^\infty$  has the same set of leaders as  $A$ .*

**PROOF.** By Kolchin (1973, 0.16, Corollary 4), the minimal primes of  $(A):S_A^\infty$  admit the finite set of non-leaders of  $A$  as a transcendence basis. Assume  $A = a_1, \dots, a_r$  is arranged in order of increasing rank. We can apply the same result to subsets  $A_k = a_1, \dots, a_k$ ,  $1 \leq k \leq r$  of  $A$ .

If  $P$  is a minimal prime of  $(A):S_A^\infty$ ,  $P \cap \mathcal{F}[\mathfrak{N}(A_k), \mathfrak{L}(A_k)]$  is a prime ideal containing  $(A_k):S_{A_k}^\infty$  and therefore one of its minimal prime  $\bar{P}$ .  $P \cap \mathcal{F}[\mathfrak{N}(A_k), \mathfrak{L}(A_k)]$  and  $\bar{P}$  have the same dimension, and therefore are equal.  $P \cap \mathcal{F}[\mathfrak{N}(A_k), \mathfrak{L}(A_k)]$  is a minimal prime of  $(A_k):S_{A_k}^\infty$ . Thus,  $P$  admits a characteristic set having the same set of leaders as  $A$ .  $\square$

This theorem bears as immediate consequences the following facts. If  $A$  is an autoreduced set of  $\mathcal{K}[X]$  and  $H$  is a subset of  $\mathcal{K}[X]$  containing  $S_A$ , the extension of  $((A):H^\infty)_{\mathcal{K}}$  over  $\mathcal{K}_A$  is a zero-dimensional radical ideal of  $\mathcal{K}_A[\mathfrak{L}(A)]$ . Furthermore  $((A):H^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[X] = ((A):H^\infty)_{\mathcal{K}}$ .

We shall now make some comments on characteristic sets and characterizable ideals in a non-differential context. There are indeed slight differences due to the fact that no derivation occurs in the reduction process. If an autoreduced set  $A$  is a characteristic set

<sup>†</sup>For the definition and use of Jacobian ideals, see Eisenbud (1994) or Vasconcelos (1998).



of an ideal  $I$  then  $A \subset I \subset (A):I_A^\infty$ . It follows that if  $A$  is a characteristic set of  $(A):H_A^\infty$  then  $(A):H_A^\infty = (A):I_A^\infty$  and therefore  $(A):I_A^\infty$  is radical. We have, in fact, the following equivalence.

**PROPOSITION 3.3.** *Let  $A$  be an autoreduced set. Then  $(A):I_A^\infty$  is radical if and only if  $(A):I_A^\infty = (A):H_A^\infty$ .*

**PROOF.** By Theorem 3.1,  $(A):H_A^\infty$  is radical. Thus the implication  $(A):I_A^\infty = (A):H_A^\infty \Rightarrow (A):I_A^\infty$  is radical is immediate.

We shall first prove the other implication in dimension zero. Consider  $A$  as an autoreduced set of  $\mathcal{K}(\mathfrak{N}(A))[\mathfrak{L}(A)]$ . The Jacobian ideal of  $(A)$  is generated by  $s_A$ , the product of the separants of  $A$ . By Vasconcelos (1998, Theorem 5.4.2.),  $(A):s_A = \sqrt{(A)} = (A)$ . Thus  $(A):H_A^\infty = ((A):S_A^\infty):I_A^\infty = ((A):s_A^\infty):I_A^\infty = \sqrt{(A)}:I_A^\infty = (A):I_A^\infty$ .

It is now enough to prove that  $(A):I_A^\infty$  has no zero divisor in  $\mathcal{K}[\mathfrak{N}(A)]$ . We first prove that  $(A):I_A^\infty$  is unmixed dimensional. Then we prove that  $\mathfrak{N}(A)$  is algebraically independent modulo any minimal prime of  $(A):I_A^\infty$ . Let us note  $A = a_1, \dots, a_m$  and let  $u_i$  denote the leader of  $a_i$ . Each  $a_i$  introduces a new variable,  $u_i$ .

Consider the localization  $L_A = (I_A^\infty)^{-1}\mathcal{K}[X]$ .  $(A):I_A^\infty = (I_A^\infty)^{-1}(A) \cap \mathcal{K}[X]$  and  $L_A$  is Cohen–MacCaulay (Eisenbud, 1994, Proposition 18.9). Considered as a univariate polynomial in  $u_i$ ,  $a_i$  has one of its coefficient, its initial, invertible in  $L_A$ . Thus  $a_i$  can not divide zero modulo  $I_A^\infty^{-1}(a_1, \dots, a_{i-1})$  (Eisenbud, 1994, Gauss' lemma). It follows that  $a_1, \dots, a_n$  is a  $L_A$ -regular sequence. Thus  $(I_A^\infty)^{-1}(A)$  is unmixed dimensional of dimension the cardinal of  $\mathfrak{N}(A)$ . So is  $(A):I_A^\infty$  (Eisenbud, 1994, Exercise 9.4).

By hypothesis,  $(A):I_A^\infty$  is radical. We have proved that all its minimal primes have dimension the cardinal of  $\mathfrak{N}(A)$ . A minimal prime  $P$  of  $(A):I_A^\infty$  does not contain any initial of  $A$ . Therefore, for each  $1 \leq i \leq n$ , the image of  $a_i$  modulo  $P \cap \mathcal{K}[\mathfrak{N}(A), u_1, \dots, u_{i-1}]$  has a strictly positive degree in  $u_i$ . It follows that  $\mathfrak{L}(A)$  is algebraic over  $\mathcal{K}[\mathfrak{N}(A)]$  modulo  $P$ . Given the dimension of  $P$ , we conclude that  $\mathfrak{N}(A)$  is algebraically independent modulo  $P$ . It follows that  $((A):I_A^\infty)_{\mathcal{K}} = ((A):I_A^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[\mathfrak{N}(A), \mathfrak{L}(A)]$ .  $\square$

In the course of a decomposition algorithm in differential algebra, we will have to compute an irredundant characteristic decomposition of some  $(A):H_A^\infty$  where  $A$  is an autoreduced set. The components of the decomposition will also need to be radical ideals. We shall therefore specialize our vocabulary to radical ideals. We will say that *an ideal  $J$  is characterizable if it is radical and it admits a characteristic set  $A$  such that  $J = (A):I_A^\infty$* . Similarly, *an autoreduced set will be a characteristic set if  $A$  is a characteristic set of  $(A):I_A^\infty$  and this ideal is radical*, or, equivalently, if  $A$  is a characteristic set of  $(A):H_A^\infty$ .

### 3.2. CHARACTERISTIC DECOMPOSITION OF ZERO-DIMENSIONAL RADICAL IDEALS

In this section we will give a necessary and sufficient condition for a zero-dimensional radical ideal to be characterizable. Using this criterion we give a process to compute an irredundant characteristic decomposition of a zero-dimensional radical ideal.

We shall start with properties of zero-dimensional radical ideal that are easy consequences of the Chinese remainder theorem for which we did not find a reference.

**PROPOSITION 3.4.** *Let  $p$  be a polynomial and  $J$  be a zero-dimensional radical ideal of  $\mathcal{K}[x_1, \dots, x_n]$ .*

- (i) If  $p$  does not divide zero modulo  $J$ , then  $p$  is invertible modulo  $J$ . If furthermore  $p \in \mathcal{K}[x_1, \dots, x_k]$  there exists  $\bar{p} \in \mathcal{K}[x_1, \dots, x_k]$  such that  $\bar{p}p \equiv 1 \pmod{J \cap \mathcal{K}[x_1, \dots, x_k]}$ .
- (ii) If  $p$  divides zero modulo  $J$  there exists  $\bar{p} \in \mathcal{K}[X]$  such that  $\bar{p}p \in J$  and  $\bar{p} + p$  is invertible modulo  $J$ .

PROOF.  $J$  is the finite intersection of zero-dimensional prime ideals, say  $J = M_1 \cap \dots \cap M_r$ ; these  $M_i$  are maximal ideals of  $\mathcal{K}[X]$ . By the Chinese remainder theorem (Eisenbud, 1994, Exercise 2.6) there is an isomorphism  $\phi$  from  $\mathcal{K}[X]/J$  to the product of fields  $\mathcal{K}[X]/M_1 \times \dots \times \mathcal{K}[X]/M_r$ .

(i) Therefore, any element of  $\mathcal{K}[X]/J$  that is not a zero divisor admits an inverse. For  $1 \leq k \leq n$ , let  $J_k = J \cap \mathcal{K}[x_1, \dots, x_k]$ .  $J_k$  is also a zero-dimensional radical ideal. Let  $p \in \mathcal{K}[x_1, \dots, x_k]$ . If  $p$  does not divide zero modulo  $J$ , then  $p$  does not divide zero modulo  $J_k$ ; we can thus find  $\bar{p} \in \mathcal{K}[x_1, \dots, x_k]$  such that  $\bar{p}p \equiv 1 \pmod{J_k}$ .

(ii) Let  $p', p_1, \dots, p_r$  be the respective projections of  $p$  on  $\mathcal{K}[X]/J, \mathcal{K}[X]/M_1, \dots, \mathcal{K}[X]/M_r$ . For  $1 \leq i \leq r$ , let  $\bar{p}_i = 0$  if  $p_i \neq 0$  and  $\bar{p}_i = 1$  if  $p_i = 0$ . Let  $\bar{p}' \in \mathcal{K}[X]/J$  be the unique element such that  $\phi(\bar{p}') = (\bar{p}_1, \dots, \bar{p}_r)$ . We have  $\bar{p}'p' = 0$  and  $\phi(\bar{p}' + p') = (\bar{p}_1 + p_1, \dots, \bar{p}_r + p_r)$  where  $\bar{p}_i + p_i \neq 0$  is invertible in  $\mathcal{K}[X]/M_i$ . Let  $\bar{p}$  be a pre-image of  $\bar{p}'$  through the projection  $\mathcal{K}[X] \rightarrow \mathcal{K}[X]/J$ ; it satisfies the property enunciated in the proposition.  $\square$

We proceed by giving a necessary and sufficient condition for a zero-dimensional radical ideal to be characterizable. Our notion of characteristic sets and of characterizable ideals can be compared with the computationally dependent definition of *characteristic presentation* of Boulier *et al.* (1997). The criterion we obtain is actually much simpler than the sufficient condition obtained by Boulier *et al.* (1997) for the existence of a characteristic presentation. It furthermore makes precise the connection that exists between a Gröbner basis and a characteristic set.

LEMMA 3.5. *Let  $J$  be a zero-dimensional radical ideal of  $\mathcal{K}[x_1, \dots, x_n]$ .  $J$  is characterizable for the ranking  $x_1 < \dots < x_n$  iff its minimal Gröbner basis,  $G$ , according to the lexicographic order  $x_1 < \dots < x_n$ , has exactly  $n$  elements. Then  $G$  is a characteristic set characterizing  $J$ .*

Before proving this theorem, recall that if  $G$  has exactly  $n$  elements, then the leading terms are  $x_1^{d_1}, \dots, x_n^{d_n}$ , for some  $d_i \in \mathbb{N}^*$  (Becker and Weispfenning, 1993, Corollary 6.56).

PROOF. If  $G$  has  $n$  elements, then  $G$  is an autoreduced set and each of its elements has 1 as initial. It is furthermore of minimal rank and therefore is a characteristic set of  $J$ . We have  $(G):I_G^\infty = (G) = J$  so that  $J$  is characterizable and  $G$  is a characteristic set.

Assume that  $A = a_1, \dots, a_n$  is a characteristic set of  $J$  and  $J = (A):I_A^\infty$ . The initials  $i_1, \dots, i_n$  of the elements of  $A$  do not divide zero modulo  $J$ . Let  $J_k = J \cap \mathcal{K}[x_1, \dots, x_k]$ ,  $1 \leq k \leq n$ . We have  $i_1 \in \mathcal{K}$ ; let  $\bar{i}_1 = 1/i_1$ . Let  $c_1 = \bar{i}_1 a_1$ ;  $c_1 \in J_1$  is monic and has the same rank as  $a_1$ . For  $2 \leq k \leq n$  there exists  $\bar{i}_k \in \mathcal{K}[x_1, \dots, x_{k-1}]$  such that  $i_k \bar{i}_k = 1 + q_k$  where  $q_k \in J_{k-1}$ . Let  $c_k = \bar{i}_k a_k - q_k x_k^{d_k}$ . Each  $c_k$  belongs to  $J$ , has the same rank as  $a_k$  and has initial 1.  $C = c_1, \dots, c_n$  has the same rank as  $A$ . So does  $\bar{C}$  obtained from  $C$  by autoreduction. Thus  $\bar{C}$  is a characteristic set of  $J$ . It follows that  $(\bar{C}) \subset J \subset (\bar{C}):I_{\bar{C}}^\infty$ . The initials of  $\bar{C}$  being 1,  $J = (\bar{C}) = (\bar{C}):I_{\bar{C}}^\infty$  and  $\bar{C}$  is the minimal Gröbner basis of  $J$

according to the lexicographic order  $x_1 < \dots < x_n$  because the leading monomials have no common divisors.  $\square$

EXAMPLE 3.6. Some radical zero-dimensional ideals are not characterizable. Consider for instance  $J = (2x_1^2 + 3x_1 + 1, 2x_1x_2 + x_2, x_2^2 - 2x_1 - 2) \subset \mathbb{Q}[x_1, x_2]$ .  $J$  is a zero-dimensional radical ideal since  $J \cap \mathbb{Q}[x_1]$  and  $J \cap \mathbb{Q}[x_2]$  are generated by square-free polynomials, respectively  $2x_1^2 + 3x_1 + 1$  and  $x_2^3 - x_2$ .

The generators of  $J$  given above form a reduced Gröbner basis for the lexicographical order where  $x_1 < x_2$ . We see that this does not satisfy the condition of the previous proposition.  $J$  is not characterizable. Note nonetheless that  $J = (J, 2x_1 + 1) \cap J : (2x_1 + 1) = (2x_1 + 1, x_2^2 - 1) \cap (x_1 + 1, x_2)$ . The two components of this decomposition are characterizable zero-dimensional ideals that are comaximal since  $2(x_1 + 1) - (2x_1 + 1) = 1$ .

Note that the Gröbner basis of  $J$  for the lexicographical order  $x_2 < x_1$  is  $G' = x_2^3 - x_2, 2x_1 - x_2^2 + 2$ . Thus  $J$  is characterizable for the ranking  $x_2 < x_1$ .

PROPOSITION 3.7. *Every zero-dimensional radical ideal is the intersection of a finite number of pairwise comaximal characterizable zero-dimensional radical ideals. Algorithm 3.8 computes such an irredundant characteristic decomposition.*

The fact that a zero-dimensional radical ideal is the intersection of pairwise comaximal characterizable radical ideals is easily proved: every zero-dimensional radical ideal is the intersection of a finite number of zero-dimensional prime ideals. These are characterizable and maximal. This argument is nonetheless misleading in the sense that the components of an irredundant decomposition do not need to be prime. The constructive proof that we give shows the correctness of Algorithm 3.8. This latter is quite primitive compared with the already existing algorithms that could be used. Lazard (1992) showed that actually only one Gröbner basis computation is required to obtain the characteristic decomposition. See also Moreno-Maza (1997). Kalkbrener (1993), Szanto (1998), Wang (1999) and Aubry (1999) worked out Gröbner-free decomposition algorithms.

PROOF. Assume  $J$  is a zero-dimensional radical ideal of  $\mathcal{K}[X]$  that is not characterizable. Let  $G$  be a reduced Gröbner basis according to the lexicographical order. One of the elements  $g$  of  $G$  has its initial  $i_g$  which does belong to  $\mathcal{K}$ . We claim that  $i_g$  is a zero divisor modulo  $J$ . Let  $x_k$  be the leader of  $g$  and  $d = \deg_{x_k} g$ . Because  $G$  is reduced, there cannot be an element of  $G$  with leading monomial  $x_k^e$ , with  $e \leq d$ . If  $i_g$  were not a zero divisor modulo  $J$ , there would exist  $\bar{v}_g \in \mathcal{K}[x_1, \dots, x_{k-1}]$  such that  $\bar{v}_g i_g \equiv 1 \pmod J$ . Then  $\bar{v}_g g$  would be an element of  $J$  with leading monomial  $x_k^d$ . This cannot be since otherwise there would be an element of  $G$  with leading monomial dividing  $x_k^d$ . Thus, there exists  $\bar{v}_g, q \notin J$  such that  $i_g \bar{v}_g \in J$  and  $q(\bar{v}_g + i_g) \equiv 1 \pmod J$ . This entails first that  $J = J : i_g \cap J : \bar{v}_g$ . Indeed, if  $p \in J : i_g \cap J : \bar{v}_g$  then  $(\bar{v}_g + i_g)p \in J$  and therefore  $p \in J$ . Secondly  $J : \bar{v}_g$  and  $J : i_g$  are comaximal because  $i_g \in J : \bar{v}_g$  and  $\bar{v}_g \in J : i_g$ . For this same reason, the inclusion of  $J$  in both  $J : i_g$  and  $J : \bar{v}_g$  is strict. We can thus construct growing sequences of zero-dimensional radical ideals that cannot become stationary before we have obtained characterizable zero-dimensional radical ideals.

Furthermore  $(J, i_g) \subset J : \bar{v}_g$  and  $p \in J : \bar{v}_g \Rightarrow \bar{v}_g p + i_g p \in (J, i_g) \Rightarrow p \in (J, i_g)$ , so that  $J : \bar{v}_g = (J, i_g)$ . We do not need to actually compute  $\bar{v}_g$ .  $\square$

Each element of the characteristic sets  $T_i$  obtained by the following algorithm has 1 as

initial. It need not be the case to be in a position to lift the result to positive dimension (Theorem 3.10) nor to the differential case (Theorem 6.2). Also, this algorithm requires the input ideal  $J$  to be given in a way that a Gröbner basis of it can be computed. The fact is that this algorithm will need to be in a position to deal with ideals given as saturations  $(A):H_A^\infty$ , where  $A$  is an autoreduced set.

**ALGORITHM 3.8. 0D-Irredundant- $\chi$ -Decomposition**

**Input:**  $J$ , a zero-dimensional radical ideal in  $\mathcal{K}[X]$ .

**Output:**  $\mathfrak{T} = T_1, \dots, T_r$  a sequence of characteristic sets characterizing zero-dimensional radical ideals such that

$$J = (T_1):I_{T_1}^\infty \cap \dots \cap (T_r):I_{T_r}^\infty \text{ and, for } j \neq k, (T_j):I_{T_j}^\infty + (T_k):I_{T_k}^\infty = \mathcal{K}[X].$$

$G :=$  the minimal Gröbner basis of  $J$  w.r.t. to the lexicographical order;

if  $G \subset \mathcal{K}$  then

    return (Null-Sequence);

elif  $G$  has  $n$  elements then

    return ( $G$ );

else

$i :=$  the initial of an element of  $G$  such that  $i \notin \mathcal{K}$

$J_1 := (J, i); \quad J_2 := J:i;$

$\mathfrak{T} :=$  0D-Irredundant- $\chi$ -Decomposition ( $J_1, \mathcal{K}[X]$ ), 0D-Irredundant- $\chi$ -Decomposition ( $J_2, \mathcal{K}[X]$ );

fi;

3.3. LIFTING TO POSITIVE DIMENSION

This section shows how an irredundant characteristic decomposition of the ideal defined by an autoreduced set can be simply computed by the algorithm of the previous section, i.e. in dimension zero. This allows us to make the necessary intermediate step between the differential case and the computations in dimension zero. This is an original and very practical result. We start with an easy criterion to determine when an autoreduced set is a characteristic set in positive dimension.

**LEMMA 3.9.** *Let  $A$  be an autoreduced set.  $A$  is a characteristic set in  $\mathcal{K}[\mathfrak{N}(A), \mathfrak{L}(A)]$  if and only if  $A$  is a characteristic set in  $\mathcal{K}[\mathfrak{N}(A)][\mathfrak{L}(A)]$ .*

**PROOF.** Recall from Theorem 3.2 that  $((A):H_A^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[\mathfrak{N}(A), \mathfrak{L}(A)] = ((A):H_A^\infty)_{\mathcal{K}}$ .

Assume  $A$  is a characteristic set of  $((A):H_A^\infty)_{\mathcal{K}_A}$ . If  $((A):H_A^\infty)_{\mathcal{K}}$  contained a non-zero element reduced with respect to  $A$ , so would  $((A):H_A^\infty)_{\mathcal{K}_A}$ . Thus  $A$  is a characteristic set of  $((A):H_A^\infty)_{\mathcal{K}}$ .

Assume  $A$  is a characteristic set of  $((A):H_A^\infty)_{\mathcal{K}}$ . Assume, for contradiction, there is a non-zero element  $p$  of  $((A):H_A^\infty)_{\mathcal{K}_A}$  reduced with respect to  $A$ . Clearing out the denominators of  $p$  amounts to multiplying  $p$  by some element of  $\mathcal{K}[\mathfrak{N}(A)]$ . Let  $\bar{p}$  be the result of this operation. Obviously  $\bar{p}$  is non-zero and reduced with respect to  $A$  and belongs to  $((A):H_A^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[\mathfrak{N}(A), \mathfrak{L}(A)] = ((A):H_A^\infty)_{\mathcal{K}}$ . This contradicts the hypothesis.  $\square$

For this reason and Lemma 3.5,  $(A):H_A^\infty$  is characterizable iff its reduced Gröbner basis  $G$  with respect to the lexicographic ordering induced on  $\mathcal{K}_A[\mathfrak{L}(A)]$  has exactly as many elements as  $\mathfrak{L}(A)$ . If so,  $A$  is a characteristic set iff  $G$  and  $A$  have the same rank.

**THEOREM 3.10.** *Let  $A$  be an autoreduced set of  $\mathcal{K}[X]$ . Let  $((A):H_A^\infty)_{\mathcal{K}_A} = (T_1):I_{T_1}^\infty \cap \dots \cap (T_r):I_{T_r}^\infty$  be a (zero-dimensional) irredundant characteristic decomposition in  $\mathcal{K}_A[\mathfrak{L}(A)]$ . For  $1 \leq i \leq r$ , let  $C_i$  in  $\mathcal{K}[X]$  be obtained from  $T_i$  by clearing out the denominators. Then  $C_i$ ,  $1 \leq i \leq r$ , is an autoreduced set and  $((A):H_A^\infty)_{\mathcal{K}} = (C_1):I_{C_1}^\infty \cap \dots \cap (C_r):I_{C_r}^\infty$  is an irredundant characteristic decomposition in  $\mathcal{K}[X]$ .*

**PROOF.**  $C_i$  is a characteristic set of  $(T_i):I_{T_i}^\infty$  in  $\mathcal{K}_A[\mathfrak{L}(A)]$ . The  $I_{C_i}$  and  $S_{C_i}$  are simply obtained from  $I_{T_i}$  and  $S_{T_i}$  by multiplication by an element of  $\mathcal{K}[\mathfrak{N}(A)]$ . Thus, in  $\mathcal{K}_A[\mathfrak{L}(A)]$ ,  $((C_i):I_{C_i}^\infty)_{\mathcal{K}_A}$  and  $((C_i):I_{C_i}^\infty)_{\mathcal{K}_A}$  are respectively equal to  $(T_i):I_{T_i}^\infty$  and  $(T_i):H_{T_i}^\infty$ . Consequently, by Proposition 3.3 applied to  $(T_i):H_{T_i}^\infty$ ,  $((C_i):I_{C_i}^\infty)_{\mathcal{K}_A} = ((C_i):H_{C_i}^\infty)_{\mathcal{K}_A}$ .

Recall from Theorems 3.1 and 3.2 that  $((A):H_A^\infty)_{\mathcal{K}_A}$  is a zero-dimensional radical ideal in  $\mathcal{K}_A[\mathfrak{L}(A)]$  and  $((A):H_A^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[X] = ((A):H_A^\infty)_{\mathcal{K}}$ . We have

$$((A):H_A^\infty)_{\mathcal{K}} = (((C_1):I_{C_1}^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[X]) \bigcap \dots \bigcap (((C_r):I_{C_r}^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[X]).$$

The ideals  $((C_i):I_{C_i}^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[X]$  are radical. The  $((C_i):I_{C_i}^\infty)_{\mathcal{K}_A}$  being pairwise co-maximal in  $\mathcal{K}_A[\mathfrak{L}(A)]$  implies that a prime ideal  $P$  of  $\mathcal{K}[X]$  containing two distinct ideals  $((C_i):I_{C_i}^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[X]$  must contain an element of  $\mathcal{K}[\mathfrak{N}(A)]$ . Thus  $P$  cannot be an essential component of  $((C_i):I_{C_i}^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[X]$ . Therefore the minimal primes of the  $((C_i):I_{C_i}^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[X]$  give a partition of the set of minimal primes of  $(A):H_A^\infty$ .

Consider  $1 \leq i \leq r$ . Let  $P$  be a minimal prime of  $((C_i):I_{C_i}^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[X]$ . Both  $C_i$  and  $A$  are included in  $P$ . Assume  $C_i$  were not an autoreduced set. Then  $P$  would contain an autoreduced set lower than  $A$  and with a set of leaders different than  $\mathfrak{L}(A)$ . This would contradict Theorem 3.2.  $C_i$  is an autoreduced set in  $\mathcal{K}[X]$ .

$((C_i):I_{C_i}^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[X]$  contains no autoreduced set lower than  $C_i$  otherwise  $((C_i):I_{C_i}^\infty)_{\mathcal{K}_A} = (T_i):I_{T_i}^\infty$  would too; it follows that  $C_i$  is a characteristic set of  $((C_i):I_{C_i}^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[X]$ . Thus any element of  $((C_i):I_{C_i}^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[X]$  is reduced to zero by  $C$  and therefore belongs to  $((C_i):I_{C_i}^\infty)_{\mathcal{K}}$ . Since the extension-contraction process ensures that  $((C_i):I_{C_i}^\infty)_{\mathcal{K}} \subset ((C_i):I_{C_i}^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[X]$ , we are led to the equality  $((C_i):I_{C_i}^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[X] = ((C_i):I_{C_i}^\infty)_{\mathcal{K}}$ .  $C_i$  is thus a characteristic set and  $(A):H_A^\infty = (C_1):I_{C_1}^\infty \cap \dots \cap (C_r):I_{C_r}^\infty$  is an irredundant characteristic decomposition.  $\square$

#### 4. Coherence and its Consequences

Coherence is a concept similar to *formal integrability* or *involutivity* in some other algebraic formalisms for differential equations. It was introduced in differential ideal theory by Rosenfeld (1959). It answers the problem exposed in the following example.

**EXAMPLE 4.1.**  $A = u_{xy} - u, u_{xx}$  is an autoreduced set of  $\mathbb{Q}(x, y)\{u\}$ , endowed with derivations according to  $x$  and  $y$ . It is a characteristic set of  $(A):H_A^\infty$ . However  $\delta_x(u_{xy} - u) - \delta_y(u_{xx}) = u_x \in [A]:H_A^\infty$  is not reduced to zero by  $A$ . An autoreduced set  $A$  that is a characteristic set of  $(A):H_A^\infty$  is not obviously a characteristic set of  $[A]:H_A^\infty$  when dealing with partial differential polynomials.

Differential ideals defined by coherent autoreduced sets enjoy specific properties which make them the bridge between differential algebra and polynomial algebra. Neither Theorem 4.4 nor Theorem 4.5 appears in the work of Ritt and Kolchin. They are the liftings to the differential case of Theorem 3.1 and Theorem 3.2 through what Boulier (1994) named *Rosenfeld's lemma*. Theorem 4.4, which first appeared in Boulier *et al.* (1995), is

a direct lifting of Theorem 3.1. A special case of Theorem 4.5 appears in Hubert (1997, Proposition G.1.7). The present proof of Theorem 4.5 is not really different from the one presented in Boulier *et al.* (1997).

Let  $A$  be an autoreduced set of  $\mathcal{F}\{Y\}$ . For a derivative  $v$  of  $\mathcal{F}\{Y\}$  we define  $A_v^-$  to be the set of the elements of  $A$  and their derivatives that have a leader ranking strictly less than  $v$ .

**DEFINITION 4.2.** Let  $A$  be an autoreduced set in  $\mathcal{F}\{Y\}$ .  $A$  is said to be coherent if whenever  $a, b \in A$  are such that  $u_a$  and  $u_b$  have a common derivative, say  $v = \psi u_a = \phi u_b$ ,  $\phi, \psi \in \Theta$ , then  $s_b \psi a - s_a \phi b \in (A_v^-):H_A^\infty$ .

**DEFINITION 4.3.** Let  $a$  and  $b$  be differential polynomials in  $\mathcal{F}\{Y\}$ . If  $u_a$  and  $u_b$  have no common derivative, we define  $\mathbf{X}\text{-derivative}(a, b) = 0$ . Otherwise let  $\text{lcd}(u_a, u_b) = \bar{\psi}u_a = \bar{\phi}u_b$  be the lowest common derivative of  $u_a$  and  $u_b$ . We define then the cross-derivative of  $a$  and  $b$  to be

$$\mathbf{X}\text{-derivative}(a, b) = \frac{s_b}{\text{gcd}(s_b, s_a)} \bar{\psi}a - \frac{s_a}{\text{gcd}(s_b, s_a)} \bar{\phi}b.$$

We introduce the systematic division by  $\text{gcd}(s_b, s_a)$  in the cross-derivative to reduce the expression swell in an implementation. From Kolchin (1973, IV.9), it is easy to conclude that an autoreduced set  $A$  in  $\mathcal{F}\{Y\}$  is coherent if and only if  $\mathbf{X}\text{-derivative}(a, b) \in (A_{\text{lcd}(u_a, u_b)}^-):H_A^\infty, \forall a, b \in A$ . An autoreduced set  $A$  in  $\mathcal{F}\{Y\}$  is coherent if  $\mathbf{d}\text{-rem}(\mathbf{X}\text{-derivative}(a, b), A) = 0, \forall a, b \in A$ .

The key result here is a theorem by Rosenfeld (1959): if  $A$  is a coherent autoreduced set, a differential polynomial of  $\mathcal{F}\{Y\}$  that is partially reduced w.r.t.  $A$  belongs to  $[A]:H_A^\infty$  iff it belongs to  $((A):H_A^\infty)\mathcal{F}\{Y\}$ . A generalization to positive characteristic can be found in Kolchin (1973, III.8, Lemma 5). This bears as immediate corollaries that:

- (i)  $p \in [A]:H_A^\infty \Leftrightarrow \mathbf{d}\text{-prem}(p, A) \in ((A):H_A^\infty)\mathcal{F}\{Y\}$
- (ii)  $[A]:H_A^\infty \cap \mathcal{F}\mathfrak{N}(A), \mathfrak{L}(A) = (A):H_A^\infty$ .

Actually the proof of Rosenfeld’s result makes no use of the initials. The theorem could be stated for  $(A):S_A^\infty$  and  $[A]:S_A^\infty$ . Consequently, the statements made below for  $[A]:H_A^\infty$  could in fact be made for  $[A]:S_A^\infty$ . We did not feel it was worth reproducing a proof to make this clear because we will have to deal with the ideals  $[A]:H_A^\infty$  anyway in the decomposition algorithm.

The fundamental result to obtain a decomposition into *coherent components* is then the following.

**THEOREM 4.4.** *Let  $A$  be a coherent autoreduced set of  $\mathcal{F}\{Y\}$ . Then  $[A]:H_A^\infty$  is a radical differential ideal.*

**PROOF.** By Theorem 3.1  $(A):H_A^\infty$  is radical. It then follows from a corollary of Rosenfeld’s lemma (Kolchin, 1973, III.8, Lemma 6) that  $[A]:H_A^\infty$  is radical.  $\square$

Then, the computation of an irredundant characteristic decomposition of  $[A]:H_A^\infty$  can be reduced to polynomial algebra computations thanks to the following result.

**THEOREM 4.5.** *Let  $A$  be a coherent autoreduced set of  $\mathcal{F}\{Y\}$  such that  $1 \notin [A]:H_A^\infty$ .*

There is a one-to-one correspondence between the minimal primes of  $(A):H_A^\infty$  in  $\mathcal{F}[\mathfrak{N}(A), \mathfrak{L}(A)]$  and the essential prime components of  $[A]:H_A^\infty$  in  $\mathcal{F}\{Y\}$ . Assume  $C_i$  is a characteristic set of a minimal prime of  $(A):H_A^\infty$  then  $C_i$  is the characteristic set of a single essential prime component of  $[A]:H_A^\infty$  (and vice versa).

PROOF. We divide the proof into three steps.

(i) Let  $P$  be an essential prime component of  $[A]:H_A^\infty$ .  $P \cap \mathcal{F}[\mathfrak{N}(A), \mathfrak{L}(A)]$  is a minimal prime of  $(A):H_A^\infty$ .

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

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

(ii) Every minimal prime of  $(A):H_A^\infty$  is the intersection of an essential prime component of  $[A]:H_A^\infty$  with  $\mathcal{F}[\mathfrak{N}(A), \mathfrak{L}(A)]$

Assume the minimal prime decomposition of  $[A]:H_A^\infty$  is  $[A]:H_A^\infty = \bigcap_{i=1}^r P_i$ . By Kolchin (1973, III.8, Lemma 5),  $\bigcap_{i=1}^r (P_i \cap \mathcal{F}[\mathfrak{N}(A), \mathfrak{L}(A)]) = (A):H_A^\infty$ . Therefore, all the minimal primes of  $(A):H_A^\infty$  are the intersection of an essential prime component of  $[A]:H_A^\infty$  with  $\mathcal{F}[\mathfrak{N}(A), \mathfrak{L}(A)]$ .

(iii) If  $C_i$  is the characteristic set of a minimal prime  $P_i \cap \mathcal{F}[\mathfrak{N}(A), \mathfrak{L}(A)]$  of  $(A):H_A^\infty$  then  $C_i$  is a characteristic set of  $P_i$ .

Let  $p$  be an element of  $P_i$  and  $\bar{p} = \mathbf{d}\text{-prem}(p, C_i)$ . Then  $\bar{p} \in P_i \cap \mathcal{F}[\mathfrak{N}(A), \mathfrak{L}(A)]$ .  $C_i$  being a characteristic set of  $P_i \cap \mathcal{F}[\mathfrak{N}(A), \mathfrak{L}(A)]$ ,  $\bar{p}$  must be zero. Therefore  $C_i$  is a characteristic set of  $P_i$ . (In particular  $C_i$  must be coherent!) Since a characteristic set of a prime differential ideal determines uniquely this prime differential ideal, there is a unique essential prime component of  $[A]:H_A^\infty$  whose intersection with  $\mathcal{F}[\mathfrak{N}(A), \mathfrak{L}(A)]$  is equal to  $(C_i):H_{C_i}^\infty = P_i \cap \mathcal{F}[\mathfrak{N}(A), \mathfrak{L}(A)]$ .  $\square$

This theorem together with Theorem 3.2 bears the following consequence: a characteristic set of an essential prime component of  $[A]:H_A^\infty$  has the the same set of leaders as  $A$  iff  $(A):H_A^\infty \neq (1)$ .

### 5. Decomposition into Coherent Components

In the previous section we saw that the differential ideal  $[A]:H_A^\infty$ , where  $A$  is a coherent autoreduced set, bears pleasant properties that can be lifted from the algebraic properties of  $(A):H_A^\infty$ . For a given finite set  $\Sigma$  of  $\mathcal{F}\{Y\}$  it would thus be nice to find a coherent autoreduced set  $A$  such that  $\{\Sigma\} = [A]:H_A^\infty$ . This is obviously not the general case. We can nonetheless manage to represent  $\{\Sigma\}$  as an intersection of such differential ideals.

We will first show how to compute a coherent autoreduced set  $A$  that satisfies one of the

property of a characteristic set of  $[\Sigma]$ , namely that  $A \subset [\Sigma] \subset [A]:H_A^\infty$ . This is the first step of the Ritt algorithm (Kolchin, 1973, IV.9). We will then exhibit radical differential ideals that, when intersected with  $[A]:H_A^\infty$ , give  $\{\Sigma\}$ . The justification for this splitting step relies on Theorem 4.4. Note that neither Ritt nor Kolchin used the property that  $[A]:H_A^\infty$  is radical. The way they would proceed in their decomposition algorithm would rely on a process<sup>†</sup> to decide whether  $A$  is a characteristic set of a prime differential ideal. In the case where  $A$  is not a characteristic set of a prime differential ideal, the process would exhibit  $p, q \notin [A]:H_A^\infty$  reduced w.r.t.  $A$  such that  $pq \in [A]:H_A^\infty$  and operate the splitting  $\{\Sigma\} = \{\Sigma, p\} \cap \{\Sigma, q\}$ . In the case where  $A$  was finally a characteristic set of a prime differential ideal, the splitting on the separants could be done.

The Rosenfeld–Gröbner algorithm of Boulier *et al.* (1995) computes a decomposition into coherent components (called there regular components). The decomposition is obtained with a Seidenberg-like elimination scheme.

### 5.1. EXHIBITING A COHERENT AUTOREDUCE SET

Let  $\Sigma$  be a finite set of differential polynomials of  $\mathcal{F}\{Y\}$ . With a finite number of differentiations and arithmetic operations in  $\mathcal{F}\{Y\}$ , we can compute a coherent autoreduced set  $A$  such that  $A \subset [\Sigma]$  and  $\forall p \in \Sigma, \text{d-rem}(p, A) = 0$ . Thus  $A \subset [\Sigma] \subset [A]:H_A^\infty$ . Algorithm 5.1 is devoted to compute such a  $A$ . We have noted **Min-Autoreduced** a procedure which selects an autoreduced set of minimal rank among a finite set of differential polynomials of  $\mathcal{F}\{Y\}$ .

**ALGORITHM 5.1. Coherent-Autoreduced**

**Input:**  $\Sigma$  a set of differential polynomials in  $\mathcal{F}\{Y\}$

**Output:**  $A$  a coherent autoreduced set such that  $[A] \subset [\Sigma] \subset [A]:H_A^\infty$ .

$S := \emptyset; R := \Sigma \setminus \{0\}; D := \emptyset;$

**While**  $R \cup D \neq \emptyset$  and  $S \cap \mathcal{F} = \emptyset$  **do**

$S := S \cup R \cup D;$

$A := \text{Min-Autoreduced}(S);$

$R := \{\text{d-rem}(q, A) \neq 0 \mid q \in S \setminus A\};$

$D := \{\text{d-rem}(\text{X-derivative}(a, a'), A) \neq 0 \mid a, a' \in A\};$

**od;**

**if**  $S \cap \mathcal{F} \neq \emptyset$  **then**

**return** (1);

**else**

**return** ( $A$ );

**fi;**

At each iteration, a minimal autoreduced set of  $S \cup R \cup D$  has strictly lower rank than one of  $S$ . Any decreasing sequence of autoreduced sets is finite (Kolchin (1973, I.10, Proposition 3)). This algorithm thus terminates.

<sup>†</sup>Based on factorizations over towers of algebraic extension (Ritt, 1950).



5.2. SPLITTING

The crucial information here is that  $[A]:H_A^\infty$  is radical. Thus if  $A \subset [\Sigma] \subset [A]:H_A^\infty$  then  $[A] \subset \{\Sigma\} \subset [A]:H_A^\infty$  and therefore  $\{\Sigma\}:H_A^\infty = [A]:H_A^\infty$ . This, with Proposition 2.1, allows us to write:

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

**THEOREM 5.2.** *Given a finite set  $\Sigma$  of differential polynomials in  $\mathcal{F}\{Y\}$  we can compute a finite number of coherent autoreduced sets  $A_1, \dots, A_r$  such that*

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

*The differential ideals  $[A_i]:H_{A_i}^\infty$  are radical and we call them coherent components of  $\{\Sigma\}$ . Algorithm 5.3 computes such a decomposition into coherent components.*

**ALGORITHM 5.3. Coherent-Components**

**Input:**  $\Sigma$ , a finite set of differential polynomials of  $\mathcal{F}\{Y\}$ .

**Output:**  $\mathfrak{A} = A_1, \dots, A_r$ , a sequence of coherent autoreduced sets such that

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

$A := \text{Coherent-Autoreduced}(\Sigma, \mathcal{F}\{Y\})$  ;

if  $A=1$  then

return ( Null-Sequence );

else

$\mathfrak{A} = A, \text{Coherent-Components}(\{\Sigma, s_a\}, \mathcal{F}\{Y\})_{a \in A}, \text{Coherent-Components}(\{\Sigma, i_a\}, \mathcal{F}\{Y\})_{a \in A}$ ;

fi;

At each step,  $\{\Sigma, i_a\}$  and  $\{\Sigma, s_a\}$  admit autoreduced sets of lower rank than  $A$ . The algorithm thus terminates.

**6. Irredundant Characteristic Decomposition of a Coherent Component**

This section explains how an irredundant characteristic decomposition of  $(A):H_A^\infty$ , where  $A$  is a coherent autoreduced set of  $\mathcal{F}\{Y\}$ , can be readily used as an irredundant characteristic decomposition of  $[A]:H_A^\infty$ . This is a new result that can be applied in both the Ritt and Seidenberg approach. It allows us to uncouple the differential operations from the purely algebraic computations in a decomposition algorithm in differential algebra.

We start with a necessary and sufficient condition for an autoreduced set to be a characteristic set. Let us note that Ritt and Kolchin enunciated and made use only of the prime ideal case (Kolchin, 1973, IV.9, Lemma 2) of this following lemma.

**LEMMA 6.1.** *Let  $A$  be an autoreduced set of  $\mathcal{F}\{Y\}$ . A necessary and sufficient condition for  $A$  to be a characteristic set in  $\mathcal{F}\{Y\}$  is that  $A$  be coherent and a characteristic set in  $\mathcal{F}[\mathfrak{N}(A) \cup \mathfrak{L}(A)]$ .*

In other words,  $A$  is a characteristic set of  $[A]:H_A^\infty$  in  $\mathcal{F}\{Y\}$  if and only if  $A$  is coherent and  $A$  is a characteristic set of  $(A):H_A^\infty$  in  $\mathcal{K}[\mathfrak{N}(A) \cup \mathfrak{L}(A)]$ , or equivalently in  $\mathcal{K}_A[\mathfrak{L}(A)]$  (Lemma 3.9).

PROOF. We claim that if  $A$  is a characteristic set of  $[A]:H_A^\infty$  then  $A$  must be coherent. Indeed, for any  $a, b \in A$ ,  $\mathbf{X}\text{-derivative}(a, b) \in [A] \subset [A]:H_A^\infty$ . It must therefore be reduced to zero by  $A$ . The derivatives of the elements of  $A$  needed in the reduction have leaders that are not ranking higher than the lowest common derivative of  $u_a$  and  $u_b$ , say  $v$ . Thus  $\mathbf{X}\text{-derivative}(a, b) \in (A_v^-):H_A^\infty$ . Now, if  $A$  is a characteristic set of  $[A]:H_A^\infty$ ,  $[A]:H_A^\infty$  has no non-zero elements reduced w.r.t.  $A$ . It is then obviously also the case for  $(A):H_A^\infty$ .

Conversely, assume  $A$  is coherent and a characteristic set of  $(A):H_A^\infty$ . If there existed a non-zero differential polynomial  $p$  in  $[A]:H_A^\infty$  reduced w.r.t.  $A$ , then, by Rosenfeld's lemma (Kolchin, 1973, III.8, Lemma 5), it would belong to  $(A):H_A^\infty$ . This cannot be so since  $A$  is a characteristic set of  $(A):H_A^\infty$ . Thus  $A$  is a characteristic set of  $[A]:H_A^\infty$ .  $\square$

**THEOREM 6.2.** *If  $A$  is a coherent autoreduced set of  $\mathcal{F}\{Y\}$  and  $(A):H_A^\infty = \bigcap_{i=1}^r (C_i):I_{C_i}^\infty$  is a characteristic irredundant decomposition in  $\mathcal{F}[\mathfrak{N}(A), \mathfrak{L}(A)]$  then  $C_i$  is coherent,  $1 \leq i \leq r$ , and  $[A]:H_A^\infty = \bigcap_{i=1}^r [C_i]:H_{C_i}^\infty$  is a characteristic irredundant decomposition of  $[A]:H_A^\infty$  in  $\mathcal{F}\{Y\}$ .*

Recall here Proposition 3.3: since the components of  $(A):H_A^\infty$  are to be radical we have that  $(C_i):I_{C_i}^\infty = (C_i):H_{C_i}^\infty$ .

PROOF. Let  $B_{i,j}$ ,  $1 \leq j \leq r_i$ , be the characteristic sets of the minimal primes of  $(C_i):I_{C_i}^\infty$ ;  $(C_i):I_{C_i}^\infty = \bigcap_{j=1}^{r_i} (B_{i,j}):I_{B_{i,j}}^\infty$ . By Theorem 4.5,  $B_{i,j}$  is the characteristic set of  $[B_{i,j}]:H_{B_{i,j}}^\infty$ , an essential prime component of  $[A]:H_A^\infty$ .

Let  $a, b \in C_i$ ;  $\mathbf{X}\text{-derivative}(a, b)$  belongs to  $\bigcap_{j=1}^{r_i} [B_{i,j}]:H_{B_{i,j}}^\infty$ . Thus,  $\mathbf{d}\text{-rem}(\mathbf{X}\text{-derivative}(a, b), C_i)$  belongs to  $\bigcap_{j=1}^{r_i} ([B_{i,j}]:H_{B_{i,j}}^\infty \cap \mathcal{F}[\mathfrak{N}(A), \mathfrak{L}(A)])$ . As  $[B_{i,j}]:H_{B_{i,j}}^\infty \cap \mathcal{F}[\mathfrak{N}(A), \mathfrak{L}(A)] = (B_{i,j}):H_{B_{i,j}}^\infty = (B_{i,j}):I_{B_{i,j}}^\infty$  (Theorem 4.5) and  $\bigcap_{j=1}^{r_i} (B_{i,j}):I_{B_{i,j}}^\infty = (C_i):I_{C_i}^\infty$ , we deduce that  $\mathbf{d}\text{-rem}(\mathbf{X}\text{-derivative}(a, b), C_i) \in (C_i):I_{C_i}^\infty$ .  $C_i$  being a characteristic set of  $(C_i):I_{C_i}^\infty$ , we are led to the conclusion that  $\mathbf{d}\text{-rem}(\mathbf{X}\text{-derivative}(a, b), C_i) = 0$ . Therefore  $C_i$  is coherent. By Lemma 6.1,  $C_i$  is a characteristic set of  $[C_i]:H_{C_i}^\infty$ . By Theorem 4.5,  $[C_i]:H_{C_i}^\infty = \bigcap_{j=1}^{r_i} [B_{i,j}]:H_{B_{i,j}}^\infty$  and therefore  $[A]:H_A^\infty = \bigcap_{i=1}^r [C_i]:H_{C_i}^\infty$ . This decomposition is furthermore irredundant.  $\square$

In view of the note before Theorem 4.4, this theorem is still valid if we replace  $H_A$  by any subset of  $\mathcal{F}\{Y\}$  that contains  $S_A$ .

### 7. A Characteristic Decomposition Algorithm

We recapitulate in MAPLE pseudo-code the algorithm for which we have given all the mathematical justifications in this paper. It relies only on two elements: a decomposition into coherent components and an irredundant characteristic decomposition of a zero-dimensional radical ideal. Indeed Theorem 6.2 together with Theorem 3.10 show that a characteristic decomposition of a coherent component can be lifted from an irredundant characteristic decomposition of the corresponding zero-dimensional radical ideal.

We then illustrate with two examples the results one obtains with a characteristic

decomposition algorithm. The computations are performed with `difalg99`. These examples are representative of applications. The first one is the problem of reducing to zero or one the index of a differentio-algebraic equation. This is interesting for numerical integration for instance. The second example shows how to create new classes of ordinary differential equations that can be solved in closed form. This proves useful to write a symbolic solver of ordinary differential equations (Olver, 1986, Chapter 2.5). This latter type of application was presented to me by E. Chev-Terrab.

**ALGORITHM 7.1.  $\chi$ -Decomposition**

**Input:**  $\Sigma$ , a finite set of differential polynomials of  $\mathcal{F}\{Y\}$ .

**Output:**  $\mathfrak{C} = C_1, \dots, C_r$ , a sequence of characteristic sets such that

$$\{\Sigma\} = \bigcap_{i=1}^r [C_i]:H_{\mathcal{C}_i}^\infty.$$

$\mathfrak{A} := \text{Coherent-Components}(\Sigma, \mathcal{F}\{Y\})$  ;

$\mathfrak{C} := \text{Null-sequence}$ ;

For  $A$  in  $\mathfrak{A}$  do

$C := \text{0D-Irredundant-}\chi\text{-Decomposition}((A):H_A^\infty, \mathcal{F}(\mathfrak{N}(A))[\mathcal{L}(A)]);$

$C := \text{clear out the denominators in the elements of } C;$

$\mathfrak{C} := C, \mathfrak{C};$

od;

**EXAMPLE 7.2.** Consider a planar pendulum of constant mass  $m$ . Its equations of motion in Cartesian coordinates consist of two Newton equations plus a constraint

$$m \frac{d^2x}{dt^2} = -\lambda x, \quad m \frac{d^2y}{dt^2} = g - \lambda y, \quad x^2 + y^2 - l^2 = 0$$

where  $x, y, \lambda$ , the coordinates and the tension of the rod, are the unknown functions of time and  $g, l$  are the gravitational constant and the constant length of the rod. With the usual notation  $x' = \frac{dx}{dt}$ , this system corresponds to the set of differential polynomials  $\Sigma = \{m x'' + \lambda x, m y'' + \lambda y - g, x^2 + y^2 - l^2\}$ , in  $\mathbb{Q}(g, l)\{y, x\}$  endowed with a single derivation (according to time). We consider a ranking such that  $y < x < y' < x' < y'' < x'' < \dots < \lambda < \lambda' < \lambda''$ , that is a ranking that is *orderly* on  $x, y$  and that eliminates  $\lambda$ . A characteristic decomposition of  $\{\Sigma\}$  is  $\{\Sigma\} = [C_1]:H_{\mathcal{C}_1}^\infty \cap [C_2]:H_{\mathcal{C}_2}^\infty$  where  $C_1$  and  $C_2$  consist of

$C_1:$	$C_2:$
$\underline{x}^2 + y^2 - l^2,$	$\underline{y}^2 - l^2,$
$m l^2 (l^2 - y^2) \underline{y}'' + m l^2 y y'^2 - g (l^2 - y^2)^2,$	$\underline{x},$
$l^2 (l^2 - y^2) \underline{\lambda} + g (l^2 - y^2) y - m l^2 y'^2;$	$l^2 \underline{\lambda} + g y.$

In the above, the leaders are underlined.  $C_2$  represents the equilibria. The motion of the pendulum is described by  $C_1$ . Note that in the original system, direct integration was made difficult by the appearance of  $\lambda$  in the equations of  $x$  and  $y$ . This is no longer the case. The motion is completely described by the second-order ordinary differential equation in  $y$  of  $C_1$ .

**EXAMPLE 7.3.** Consider the following problem: find the conditions on  $F$  for the ordinary first-order differential equation

$$\frac{dy}{dx} = F(x, y) \tag{7.1}$$

to admit a group of symmetry the infinitesimal generator of which,  $\xi(x, y)\frac{\partial}{\partial x} + \phi(x, y)\frac{\partial}{\partial y}$ , have its coefficients satisfying

$$\xi_y + 1 = 0, \quad x\xi_x - y - \xi = 0, \quad \phi_x - 1 = 0, \quad y\phi_y - \phi + x = 0, \quad \phi_y - \xi_x = 0. \tag{7.2}$$

These latter equations state that  $\xi(x, y) = \alpha x - y, \phi = x + \alpha y$ , where  $\alpha$  is a constant. If  $F$  is as desired, (7.1) can thus be transformed to a quadrature  $\frac{dv}{du} = G(u)$  with the change of variables<sup>†</sup>  $u = \frac{1}{2} \ln(x^2 + y^2) - \alpha \arctan(\frac{y}{x}), v = \arctan(\frac{y}{x})$ .

The equations of the type (7.1) that admit a group of symmetry with infinitesimal generator  $\xi(x, y)\frac{\partial}{\partial x} + \phi(x, y)\frac{\partial}{\partial y}$  are the ones that satisfy

$$\phi_x + \phi_y F - \xi_x F - \xi_y F^2 - \xi F_x - \phi F_y = 0. \tag{7.3}$$

We therefore consider  $\mathbb{Q}(x, y)\{F, \phi, \xi\}$ , endowed with derivations according to  $x$  and  $y$ , and the set  $\Sigma$  of differential polynomials that correspond to equations (7.2) and (7.3). To find the conditions on  $F$  we must assign a ranking that eliminates  $\xi$  and  $\phi$ . We choose the elimination order  $F < F_y < F_x < F_{yy} < F_{xy} < F_{yy} < \dots < \xi < \xi_y < \xi_x < \dots < \phi < \phi_y < \phi_x < \dots$ . The characteristic decomposition computed is  $\{\Sigma\} = [C_1]: H_{C_1}^\infty \cap [C_2]: H_{C_2}^\infty$  where  $C_1$  consists of

$$\begin{aligned} & ((y^2 + x^2)F_y - x(F^2 + 1)) \underline{F_{xy}} - ((y^2 + x^2)F_x + y(F^2 + 1)) F_{yy} \\ & + 2 F_y F(F_y y + x F_x) - F_y (F^2 + 1) + x(F_x^2 + F_y^2), \end{aligned} \tag{7.4}$$

$$\begin{aligned} & ((y^2 + x^2)F_y - x(F^2 + 1))^2 \underline{F_{xx}} - ((y^2 + x^2)F_x + y(F^2 + 1))^2 F_{yy} \\ & + ((y^2 + x^2)(4xF - y)F_y - 2x(F^2 + 1)(xF - y)) F_x^2 \\ & + ((y^2 + x^2)(x + 4yF)F_x + 2y(F^2 + 1)(yF + x)) F_y^2 \\ & + (y^2 + x^2)(F_x^3 x - yF_y^3) \\ & - (F^2 + 1) (2(y^2 + x^2)F_x F_y + (F^2 + 1)(-xF_x + F_y y)), \end{aligned} \tag{7.5}$$

$$(F_y y + x F_x) \underline{\phi} - (y^2 + x^2) F_x - y(F^2 + 1), \tag{7.6}$$

$$(F_y y + x F_x) \underline{\xi} + (y^2 + x^2) F_y - x(F^2 + 1) \tag{7.7}$$

and  $C_2$  consists of

$$(x^2 + y^2) \underline{F_y} - x(1 + F^2), \quad (x^2 + y^2) \underline{F_x} + y(1 + F^2) \tag{7.8}$$

$$y \underline{\phi_y} - \phi + x, \quad \phi_x - 1, \quad y \underline{\xi} - x\phi + x^2 + y^2 \tag{7.9}$$

Practically, let us be given  $F$ . If  $F$  satisfies (7.4) and (7.5) or (7.8) we will be able to reduce the differential equation (7.1) to a quadrature with the change of variables given above.

In the case determined by  $C_2$ , (7.8) imply that  $F(x, y)$  is given by a formula of the type  $\frac{x+\alpha y}{\alpha x-y}$ . The solutions are directly given by the change of variables above, that is by  $\frac{1}{2} \ln(x^2 + y^2) + \alpha \arctan(\frac{y}{x}) = c$ ,  $c$  the constant of integration.

In the case determined by  $C_1$ , (7.6) or (7.7) allows us to determine the right pair  $\xi, \phi$ . For instance, one can check that the function<sup>†</sup>  $F(x, y) = \frac{y+xH(x^2+y^2)}{x-yH(x^2+y^2)}$ , where  $H$

<sup>†</sup>Olver (1986, Chapter 2.5) details how to find this change of variables from the knowledge of the infinitesimal generator.

<sup>†</sup>This defines in fact the generic first order differential equation that admits the rotation group  $SO(2)$  as a symmetry group (Olver, 1986, Example 2.47).

is an arbitrary function of one variable, satisfies (7.4) and (7.5) and entails  $\xi(x, y) = -y$ ,  $\phi(x, y) = x$ . The change of variables  $u = \frac{1}{2} \ln(x^2 + y^2)$ ,  $v = \arctan\left(\frac{y}{x}\right)$  then transforms (7.1) into the quadrature  $\frac{dv}{du} = H(e^{2u})$ .

## 8. Conclusion

We presented the basics of an effective decomposition algorithm in differential algebra. The key idea is to work with differential ideals that are not prime. This idea was first explored by Boulier (1994) with Seidenberg's elimination. Developments in the algorithm and in the theoretical background were exposed in Boulier *et al.* (1995) and then in Boulier *et al.* (1997). In this paper we reworked Ritt's elimination to make it factorization free. This gives an algorithm that, if not efficient, is easy to describe.

The main point of this paper was nonetheless to present new results that can be applied in both approaches. These results give insight into the central objects that are the (differential) ideals defined by a (coherent) autoreduced sets. They give a simple test for such ideals to be characterizable and they allow us to lift a decomposition obtained in polynomial algebra of dimension zero to a differential decomposition. This complete uncoupling of the algebraic and differential operations simplifies the algorithms.

## Acknowledgements

Research at MSRI is supported in part by NSF grant DMS-9701755.

## References

- Aubry, P. (1999). Ensembles triangulaires de polynômes et résolution des systèmes d'équations algébriques, Ph. D. Thesis, Paris 6.
- Aubry, P., Lazard, D., Moreno-Maza, M. (1999). On the theories of triangular sets. *J. Symb. Comput.*, **28**, 105–124.
- Becker, T., Weispfenning, V. (1993). In *Gröbner Bases—A Computational Approach to Commutative Algebra*, volume 141 of Graduate Texts in Mathematics. New York, Springer-Verlag.
- Boulier, F. (1994). Étude et implantation de quelques algorithmes en algèbre différentielle, Ph. D. Thesis. Université de Lille. New York, ACM Press.
- Boulier, F., Lazard, D., Ollivier, F., Petitot, M. (1995). Representation for the radical of a finitely generated differential ideal. In Levelt, A. ed., *ISSAC'95*. ACM Press.
- Boulier, F., Lazard, D., Ollivier, F., Petitot, M. (1997). Computing representations for radicals of finitely generated differential ideals. Technical Report IT-306, LIFL.
- Carra'Ferro, G. (1987). Gröbner bases and differential algebra. In *AAECC*, LNCS **356**. Berlin, Springer-Verlag.
- Clarkson, P., Mansfield, E. (1994). Symmetry reductions and exact solutions of a class of non-linear heat equations. *Physica*, **D70**, 250–288.
- Diop, S. (1991). Elimination in control theory. *Math. Control Signals Syst.*, **4**, 19–32.
- Diop, S. (1992). Differential algebraic decision methods and some applications to system theory. *Theor. Comput. Sci.*, **98**, 137–161.
- Eisenbud, D. (1994). In *Commutative Algebra with a view toward Algebraic Geometry*, volume 150 of Graduate Texts in Mathematics. Berlin, Springer-Verlag.
- Fliess, M., Glad, S. (1993). An algebraic approach to linear and nonlinear control. In Trentelman, H., Willems, J. eds, *Essays on Control: Perspectives in the Theory and its Applications*, PCST **14**, pp. 223–265. Boston, Birkhäuser.
- Hubert, E. (1997). Algebra and algorithms for singularities of implicit differential equations, Ph. D. Thesis, Institut national polytechnique de Grenoble. <ftp://ftp.imag.fr/pub/Mediatheque/IMAG/theses/97-Hubert.Evelyne/notice-anglais.html>.
- Hubert, E. (1999). Essential components of an algebraic differential equation. *J. Symb. Comput.*, **28**, 657–680.
- Kalkbrener, M. (1993). A generalized euclidean algorithm for computing triangular representations of algebraic varieties. *J. Symb. Comput.*, **15**, 143–167.

- Kaplansky, I. (1970). *An Introduction to Differential Algebra*. Paris, Hermann.
- Kolchin, E. (1973). In *Differential Algebra and Algebraic Groups*, volume 54 of Pure and Applied Mathematics. New York, London, Academic Press.
- Lazard, D. (1992). Solving zero dimensional algebraic systems. *J. Symb. Comput.*, **15**, 117–132.
- Maârouf, H. (1996). Étude de quelques problèmes effectifs en algèbre différentielle, Ph. D. Thesis. Université Cadi Ayyad, Faculté des sciences Semailia.
- Maârouf, H., Kandri Rody, A., Ssafini, M. (1998). Triviality and dimension of a system of algebraic differential equations. *J. Autom. Reasoning*, **20**, 365–385.
- Mansfield, E. (1991). Differential Gröbner bases, Ph. D. Thesis. University of Sydney.
- Mansfield, E., Reid, G., Clarkson, P. (1998). Nonclassical reductions of a 3+1-cubic nonlinear Schrödinger system. *Comput. Phys. Commun.*, **115**, 460–488.
- Moreno-Maza, M. (1997). Calculs de pgcd au-dessus des tours d’extensions simples et résolution des systèmes d’équations algébriques, Ph. D. Thesis. Université Paris 6.
- Morrison, S. (1999). The differential ideal  $[P] : M^\infty$ . *J. Symb. Comput.*, **28**, 631–656.
- Ollivier, F. (1990). Le problème de l’identifiabilité structurelle globale: approche théorique, méthodes effectives et bornes de complexité, Ph. D. Thesis. École polytechnique.
- Olver, P. (1986). In *Applications of Lie Groups to Differential Equations*, number 107 of Graduate Texts in Mathematics. New York, Berlin, Springer-Verlag.
- Ritt, J. (1936). On the singular solutions of algebraic differential equations. *Ann. Math.*, **37**, 552–617.
- Ritt, J. (1950). In *Differential Algebra*, volume XXXIII of Colloquium Publications. New York, American Mathematical Society. Reprinted by Dover Publications Inc, 1966.
- Rosenfeld, A. (1959). Specializations in differential algebra. *Trans. Am. Math. Soc.*, **90**, 394–407.
- Seidenberg, A. (1956). An elimination theory for differential algebra. *Univ. California Publ. Math.*, **3**, 31–66.
- Szanto, A. (1998). Computation with polynomial systems, Ph. D. Thesis. Cornell University.
- Vasconcelos, W. (1998). In *Computational Methods in Commutative Algebra and Algebraic Geometry*, volume 2 of Algorithms and Computation in Mathematics. Springer.
- Wang, D. (1999). *Elimination Methods*, Texts and Monographs in Symbolic Computations. Wien, Springer-Verlag.

Originally Received 1 February 1999

Accepted 1 June 1999