FACTORIZATION FREE DECOMPOSITION ALGORITHMS IN DIFFERENTIAL ALGEBRA

EVELYNE HUBERT

Abstract. We present an effective version of Ritt's algorithm. We apply material of (Boulier *et al.* 1995) for which we give new concise proofs. We present original results in constructive algebra that makes the algorithm flexible and simple.

1. Introduction

We present an algorithm to compute a representation of the radical differential ideal generated by a system of differential equations (ordinary or partial). The method we use here involves characteristic set techniques[1]; 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 Σ of differential polynomials as an intersection of (radical) 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 decide membership to $\{\Sigma\}$ and study the dimension properties of $\{\Sigma\}$. 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 dependent variable? Find these differential equations.

Ritt (1950) gave an algorithm to compute a characteristic decomposition of $\{\Sigma\}$ where the components are prime differential ideals. Boulier (1994, 1995) pioneered an effective approach to the problem of the representation of a radical differential ideal generated by a finite set of differential polynomial. Evolving from Seidenberg's elimination theory, the version of the *Rosenfeld-Groebner* algorithm presented in (Boulier *et al.* 1997) does compute a characteristic decomposition of $\{\Sigma\}$. In the ordinary case Maârouf *et al.* (1998) provided means to compute a characteristic decomposition. All these methods work by interweaving differential reductions with algebraic operations. The algebraic operations are factorization over towers of algebraic extensions in (Ritt 1950), Groebner bases in (Boulier *et al.* 1997) and computation of inverse polynomials in towers of algebraic extensions in (Maârouf *et al.* 1998).

In this paper we rework Ritt's approach to establish that the same algebraic results as the ones uncovered by Boulier *et al.* (1995, 1997) can be applied to make this approach effective. We furthermore present some new and concise proofs of these results (Theorem 3.1, Theorem 3.2, Theorem 4.3, Theorem 4.4).

The main original contribution of this paper is to provide the tool (Theorem 6.2) that enables one to decouple completely the typically differential operations from the purely algebraic operations. We also show that all the purely algebraic operations can be done in dimension zero (Theorem 3.10). In our opinion, this paper clarifies and simplifies the essence of the algorithms in differential algebra and sets the framework for improving independently the separated pieces, differential reductions on the one hand and the algebraic operations in dimension zero on the other hand.

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

[1] differential analogues of Groebner bases techniques were studied by Carra'Ferro (1987), Mansfield (1991) and Ollivier (1990)

In the course of the paper, the notion of *characteristic presentation* is quite central. This notion was introduced in (Boulier *et al.* 1997). We will give in this paper a necessary and sufficient conditions for the existence of a characteristic presentation in different contexts (Lemma 3.5, Lemma 3.9, Lemma 6.1). The basic condition of Lemma 3.5 is in fact much simpler and more efficient than the sufficient condition obtained in (Boulier *et al.* 1997) and establishes the connection there is between a characteristic presentation and a Groebner basis.

The purely algebraic method proposed here is based on Groebner bases computations of zero dimensional radical ideals. These are widely known and well studied. Using a simple heuristic preprocessing - as the ones presented in the appendix - the Groebner bases computations are in fact no longer the bottleneck of our implementation. We nonetheless expect that triangular set techniques, as in (Kalkbrener 1993) and (Lazard 1992), will provide an efficient and aesthetically more consistent substitute to Algorithm 3.8. The description of the output reflects such a concern: we dictate the properties that should be achieved to carry on in the algorithm.

Though we shall, in this article, compute irredundant decomposition of *coherent components*, the complete decomposition computed are not generally minimal - neither is the decomposition of Ritt, Boulier or Rody. Only for the case where Σ consists of a single differential polynomial are there known algorithms to eliminate the redundancy in the decomposition (Ritt 1936), (Kolchin 1973), (Hubert 1998).

In this paper, we adhere to the traditional mathematical objects of differential algebra, such as autoreduced sets and characteristic sets. The underlying reason is, 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 reference to textbooks - mainly (Kolchin 1973) - is required. There is no question, nonetheless, that we benefitted of the recent work of (Boulier *et al.* 1997), (Maârouf *et al.* 1998). The readers should also be aware that generalizations of the definitions and consequences of *coherence*, *autoreduced sets*, *characteristic sets* have been studied by Boulier *et al.* (1997) and Morrison (1999). These generalizations can actually be smoothly incorporated in the framework of the present paper.

Readers interested in using a simple interfaced implementation of the Rosenfeld-Groebner algorithm, modified according to the contributions of this paper, are invited to visit the web site *http://daisy.uwaterloo.ca/~ehubert/Diffalg*. From there they can load the MAPLE V package *diffalg(2)* developed by F. Boulier and the author during their postdoctoral stays at the Symbolic Computation Group, University of Waterloo. Examples of use and applications will also be found there.

Given a finite set of differential polynomials Σ, we show in Section 5 how to compute a first decomposition of $\{\Sigma\}$, a decomposition into *coherent components*, with differential reductions. This is the differential part of the 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 investigations 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.

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 definition of characteristic presentation and decomposition and the notation S^∞.

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 Θ is the free commutative monoid of derivation operators generated by a finite set of *derivations* Δ. When Δ consists of a single derivation δ we shall speak of the ordinary differential ring $\mathcal{R}$.

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

$(\mathcal{R}\{Y\}, \Theta)$ denotes the ring of differential polynomials with differential indeterminates $Y = \{y_1, \ldots, y_n\}$ and coefficients in $(\mathcal{R}, \Theta)$. 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 $\mathcal{F} = \mathcal{K}(t_1, \ldots, t_\mu)$ where $\mathcal{K}$ is a finite extension of $\mathbb{Q}$.

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

Let S be a subset of $\mathcal{F}\{Y\}$. We denote by S^∞ the multiplicative free monoid generated by 1 and the irreducible factors of the element of S. Let I be a differential ideal of $\mathcal{F}\{Y\}$. We define the saturation of I by a set S as $I : S^\infty = \{q \in \mathcal{F}\{Y\} \mid \exists\, s \in S^\infty\ s\, q \in I\}$. $I : S^\infty$ is also a differential ideal and we have $I \subset I : S^\infty$. This practical way of defining the saturation of an ideal originates in the work of 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 R is a radical differential ideal of $\mathcal{F}\{Y\}$, $R : S^\infty$ is the intersection of the essential components of R that have an empty intersection with S.

Proposition 2.1. *Let Σ be a non-empty subset of $\mathcal{R}$.*

- *Let $a_1, \ldots, a_r \in \mathcal{R}$. 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 $\{\Sigma\} = \{\Sigma\} : S^\infty \cap \left(\bigcap_{s \in S} \{\Sigma, s\}\right)$.*

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

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

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

Any decreasing sequence of derivatives is finite (Kolchin 1973, I.8).

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 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 then the degree of p in u_p.

SPARSE PSEUDO-DIVISION: Let $\mathcal{R}[x]$ be a ring of polynomials with coefficients in the ring $\mathcal{R}$. Let $p, q \in R[x]$, 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 $c^{e-d}\, q \equiv \bar{q} \mod p$ 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 $\mathsf{srem}(q,p,x)$ of degree in x strictly lower than that p such that $\exists h \in c^\infty$ such that $h\,q \equiv \mathsf{srem}(q,p) \mod p$; h is taken as small as possible to limit the expressions swell. R is usually a ring of polynomials over a field and we shall use gcd computations to find $\mathsf{srem}(q,p,x)$ and h.

DIFFERENTIAL REDUCTION: Let p and q be differential polynomial in $\mathcal{F}\{Y\}$; With differentiation and sparse pseudo division we can compute $\mathsf{d\text{-}prem}(q,p)$ and $\mathsf{d\text{-}rem}(q,p)$ 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 $s\,q \equiv \mathsf{d\text{-}prem}(q,p) \mod [p]$ and $h\,q \equiv \mathsf{d\text{-}rem}(q,p) \mod [p]$.

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^∞*),* $h\,q \equiv \bar{q} \mod [p]$.
$\bar{q} := q$;
While q *is not (partially) reduced w.r.t.* p *do*
  $\theta u_p :=$ *the highest ranking derivative of* u_p *in* q.
  $\bar{q} := \mathsf{srem}(\bar{q}, \theta p, \theta u_p)$;
od;

2.3. **Auto-reduced sets and characteristic presentations.** Let $\mathcal{F}\{Y\}$ be endowed with a ranking. A subset A of $\mathcal{F}\{y_1, \dots, y_n\}$ is called 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[2]. 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;
- $H_A = I_A \cup S_A$.
- $\mathfrak{L}(A)$ 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 $\mathfrak{L}(A) \cup \mathfrak{N}(A)$ is the finite subset of ΘY of the derivatives present in A.

For an autoreduced set A, (A) denotes the ideal generated by A in the finitely generated polynomial algebra $\mathcal{F}[\mathfrak{L}(A) \cup \mathfrak{N}(A)]$. Note that $H_A \subset \mathcal{F}[\mathfrak{L}(A) \cup \mathfrak{N}(A)]$ 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 $h \in H_A^\infty$ and $\mathsf{d\text{-}rem}(q,A)$ that is reduced w.r.t. A such that $h\,q \equiv \mathsf{d\text{-}rem}(q,A)$. Similarly, we can compute $s \in S_A^\infty$ and $\mathsf{d\text{-}prem}(q,A)$ that is partially reduced w.r.t. A such that $s\,q \equiv \mathsf{d\text{-}prem}(q,A)$.

Algorithm 2.3. d-rem (or d-prem) .

INPUT: $q \in \mathcal{F}\{Y\}$, $A \subset \mathcal{F}\{Y\}$ *an autoreduced set , a ranking on* $\mathcal{F}\{Y\}$.
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* $h\,q \equiv \bar{q} \mod [A]$.
$\bar{q} := q$;
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.
  $\bar{q} := \mathsf{d\text{-}rem}(\bar{q}, a)$ *(or* $\mathsf{d\text{-}prem}(\bar{q}, a)$*)*;
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

[2](Kolchin 1973, I.9)

- there exists $1 \le k \le r, s$ such that the rank of a_i and b_i are the same for $1 \le i \le k-1$ 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, $1 \le i \le s$.

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 an autoreduced set of minimal rank among the autoreduced sets of I.*
- *$A \subset I$ and $\forall q \in I$, $\mathsf{d\text{-}rem}(p, A) = 0$.*
- *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[3]. If A is a characteristic set of the differential ideal I in $\mathcal{F}\{Y\}$ then $[A] \subset I \subset [A]:H_A^\infty$. When A is a characteristic set of $[A]:H_A^\infty$ then $q \in [A]:H_A^\infty \;\Leftrightarrow\; \mathsf{d\text{-}rem}(q, A) = 0$.

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 $(x+1) \in [A]:H_A^\infty$ though it is not reduced w.r.t. A. An autoreduced set A is not obviously a characteristic set of $[A]:H_A^\infty$ nor of $(A):H_A^\infty$.*

Example 2.6. *$A = u_{xy} - u, u_{xx}$ is an autoreduced set of $\mathbb{Q}(x, y)\{u\}$, endowed with derivation according to x and y. It is a characteristic set of $(A):H_A^\infty$. But $\delta_x(u_{xy} - u) - \delta_y(u_{xx}) = u_x \in [A]:H_A^\infty$ is not reduced to 0 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.*

Definition 2.7. *Let $\mathcal{F}\{Y\}$ be endowed with a ranking. An autoreduced set is a characteristic presentation if A is a characteristic set of $[A]:H_A^\infty$. A differential ideal is said to be characterizable if for a characteristic set A of I we have $I = [A]:H_A^\infty$. We say that A is a characteristic presentation of I.*

Prime differential ideals are characterizable for any ranking. Furthermore, any characteristic set of a prime differential ideal is a characteristic presentation of it. These are the properties that Ritt (1950) and Kolchin (1973) used in their work. Recent algorithmic improvement in differential algebra owes to the idea of using a wider class of differential ideals than prime differential ideals. And, indeed characterizable differential ideal 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 4.3) and has specific dimension properties (Theorem 4.4).

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

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

A characteristic decomposition of a radical differential ideal R 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 R. In other words, consider a characteristic decomposition of R, $R = \cap_{i=1}^r [C_i]:H_{C_i}^\infty$. 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 R.

3. Results in finitely generated polynomial algebras

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

[3](Kolchin 1973, I.10, Proposition 3)

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 completely done 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. It relies on Groebner bases computations in dimension 0 (Algorithm 3.8). But this can easily be replaced without preturbing the rest of the results. In the development of this method, we nonetheless establish the connection there is between characteristic sets and Groebner 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 $\mathcal{K}[X] = \mathcal{K}[x_1, \ldots, x_n] = \mathcal{K}[\mathfrak{N}(A)][\mathfrak{L}(A)]$. We will denote $\mathcal{K}_A = \mathcal{K}(\mathfrak{N}(A))$ and we will also consider the ring of polynomials $\mathcal{K}_A[\mathfrak{L}(A)]$. When 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 autoreduced sets.** The definitions and properties presented in Section 2 are immediately transposed to polynomial algebra by setting the derivation 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.* Morrison (1999) proposes 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 in dimension zero. We claim no special originality in the proof of this result in comparison with the previous mentioned papers.

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 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, corollay 5.2.1, page 127), the primary components of (A) with radical not containing the Jacobian ideal are prime. This is the case of all the primary components of (A) the intersection of which is equal to $(A):s_A^\infty$. 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. $\square$

Note that we can state the same result when considering a subset H of $\mathcal{K}[X]$ containing S_A. The primary components of $(A):H^\infty$ is a subset of the primary components of $(A):S_A^\infty$. Thus $(A):H^\infty$ is also radical.

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 $A = a_1, \ldots, a_r$ is arranged in order of increasing rank. We can apply the same result to subsets $A_k = a_1, \ldots, a_k$, $1 \le k \le r$ of A.

If P is a minimal prime of $(A):H_A^\infty$, $P \cap \mathcal{F}[\mathfrak{N}(A_k), \mathfrak{L}(A_k)]$ is a prime ideal containing $(A_k):H_{A_k}^\infty$ 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 $(A_k):H_{A_k}^\infty$.

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

Here again, we could replace S_A in the theorem by a set of polynomials containing S_A.

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 make now some comments on characteristic sets and presentations 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 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 such that A is a characteristic set of $(A):I_A^\infty$. Then $(A):I_A^\infty$ is radical if and only if $(A):I_A^\infty = (A):H_A^\infty$.*

We will in fact use only this result in dimension zero to prove Theorem 3.10.

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

We shall prove first the other implication in dimension 0. 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 $(A):I_A^\infty$.

$(A):I_A^\infty$ is the pull back of the image of (A) through the localization $\mathcal{K}[X] \longrightarrow L_A = I_A^{-1}\,\mathcal{K}[X]$. Let us note $A = a_1, \dots, a_n$ and let u_i denote the leader of a_i. Each a_i introduces a new variable, u_i, and, considered as a univariate polynomial in u_i, it has one of its coefficient, its initial, invertible in L_A. Thus a_i can not divide zero modulo $I_A^{-1}\,(a_1, \dots, a_{i-1})$ (Eisenbud 1994, Gauss' lemma). It follows that $a_1, \dots, a_n$ is a L_A-regular sequence. Thus $I_A^{-1}\,(A)$ is unmixed dimensional of dimension the cardinal of $\mathfrak{N}(A)$ (Eisenbud 1994).

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 $1 \le i \le n$, 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 $((A):I_A^\infty)_\mathcal{K} = ((A):I_A^\infty)_{\mathcal{K}_A} \cap \mathcal{K}[\mathfrak{N}(A), \mathfrak{L}(A)]$. □

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 specialized our vocabulary to radical ideals. We will say that *an ideal R is characterizable if it is radical and it admits a characteristic set A such that $R = (A):I_A^\infty$*. Similarly, *an autoreduced set will be a characteristic presentation if A is a characteristic set of $(A):I_A^\infty$ and this ideal is radical*, or, equivalently A is a characteristic set of $(A):H_A^\infty$.

3.2. **Characteristic decomposition of 0-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.

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

- *if p does not divide zero modulo R, then p is invertible modulo R. 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 $\bar{p}p \equiv 1 \mod R \cap \mathcal{K}[x_1, \dots, x_k]$.*
- *if p divides zero modulo R there exists $\bar{p} \in \mathcal{K}[X]$ such that $\bar{p}p \in R$ and $\bar{p} + p$ is invertible modulo R.*

Proof. R is the finite intersection of zero dimensional prime ideals, say $R = M_1 \cap \ldots \cap M_r$; these M_i are maximal ideals of $\mathcal{K}[X]$. By the Chinese remainder theorem (Eisenbud 1994, exercise 2.6) there is an isomorphisms ϕ from $\mathcal{K}[X]/R$ to the product of fields $\mathcal{K}[X]/M_1 \times \ldots \times \mathcal{K}[X]/M_r$.

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

Let $p', p_1, \ldots, p_r$ be the respective projections of p on $\mathcal{K}[X]/R, \mathcal{K}[X]/M_1, \ldots, \mathcal{K}[X]/M_r$. 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 $\bar{p}' \in \mathcal{K}[X]/R$ be the unique element such that $\phi(\bar{p}') = (\bar{p}_1, \ldots, \bar{p}_r)$. We have $\bar{p}'\, p' = 0$ and $\phi(\bar{p}' + p') = (\bar{p}_1 + p_1, \ldots, \bar{p}_r + p_r)$ where $\bar{p}_i + p_i \neq 0$ is invertible in $\mathcal{K}[X]/M_i$. Let $\bar{p}$ be a preimage of $\bar{p}'$ through the projection $\mathcal{K}[X] \longrightarrow \mathcal{K}[X]/R$; it satisfies the property enunciated in the proposition. □

We proceed by giving a necessary and sufficient condition for a zero dimensional radical ideal to be characterizable. The idea of extracting a characteristic presentation from a Groebner basis originates in (Boulier *et al.* 1997). There only a sufficient condition was used. Our criterion is nonetheless much simpler and, together with its proof, makes precise the connection there exists between a Groebner basis and a characteristic presentation. The idea of inverting the initials, which we use to go from a characteristic set to the Groebner basis, owes to some extent to (Maârouf *et al.* 1998).

Lemma 3.5. *Let R be a zero dimensional radical ideal of $\mathcal{K}[x_1, \ldots, x_n]$. R is characterizable for the ranking $x_1 < \ldots < x_n$ iff its reduced Groebner basis, G, according to the lexicographic order $x_1 < \ldots < x_n$, has exactly n element. Then G is a characteristic presentation of R.*

Before proving this theorem, it should be reminded that if G has exactly n elements this implies that the leading terms are $x_1^{d_1}, \ldots, x_n^{d_n}$, 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 its elements have 1 as initial. It is furthermore of minimal rank and therefore is a characteristic set of R. We have $(G) : I_G^\infty = (G) = R$ so that G is a characteristic presentation of R.

Assume $A = a_1, \ldots, a_n$ is a characteristic set of R and $R = (A) : I_A^\infty$. The initials $i_1, \ldots, i_n$ of the elements of A do not divide zero modulo R. Let $R_k = R \cap \mathcal{K}[x_1, \ldots, x_k]$, $1 \leq k \leq n$. We have $i_1 \in \mathcal{K}$; let $\bar{\imath}_1 = 1/i_1$. Let $c_1 = \bar{\imath}_1\, a_1$; $c_1 \in R_1$ is monic and has the same rank as a_1. For $2 \leq k \leq n$ there exists $\bar{\imath}_k \in \mathcal{K}[x_1, \ldots, x_{k-1}]$ such that $i_k\, \bar{\imath}_k = 1 + q_k$ where $q_k \in R_{k-1}$. Let $c_k = \bar{\imath}_k a_k - q_k\, x_k^{d_k}$. Each c_k belongs to R, has the same rank as a_k and is monic in x_k. $C = c_1, \ldots, c_n$ is therefore a triangular set R of minimal rank. Thus C is a characteristic set of R. It follows that $(C) \subset R \subset (C) : I_C^\infty$. The initials of C being 1, $R = (C) = (C) : I_C^\infty$ and C is a Groebner basis of R according to the lexicographic order $x_1 < \ldots < x_n$ because the leading monomials have no common divisors. By autoreducing the element of C (note that here Ritt reduction is equivalent to Hironaka division), we obtain the unique reduced Groebner basis of R that is also a characteristic presentation of R. □

Example 3.6. *Some radical zero dimensional ideals are not characterizable. Consider for instance $R = (2\,x_1^2 + 3\,x_1 + 1, 2\,x_1\,x_2 + x_2, x_2^2 - 2\,x_1 - 2) \in \mathbb{Q}[x_1, x_2]$. R is a zero dimensional radical ideal since $R \cap \mathbb{Q}[x_1]$ and $R \cap \mathbb{Q}[x_2]$ are generated by squarefree polynomials, respectively $2\,x_1^2 + 3\,x_1 + 1$ and $x_2^3 - x_2$.*

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

Note furthermore that the Groebner basis for the lexicographical order $x_2 < x_1$ is $G' = x_2^3 - x_2, 2\,x_1 - x_2^2 + 2$. Thus R 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 radical ideals is easily proved: every zero-dimensional radical ideal is the intersection of a finite number of zero dimensional prime ideals. These admit a characteristic presentation and are maximal. This argument is nonetheless misleading in the sense that the components of an irredundant decomposition do not need to be prime. We give a constructive proof which justifies Algorithm 3.8.

PROOF. Assume R is a zero dimensional radical ideal of $\mathcal{K}[X]$ that does not admit a characteristic presentation. Let G be the reduced Groebner basis according to the lexicographical order. One of the element g of G has its initial i_g which does belong to $\mathcal{K}$. We claim that i_g is a zero divisor modulo R. 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 R, there would exist $\bar{\imath}_g \in \mathcal{K}[x_1, \ldots, x_{k-1}]$ such that $\bar{\imath}_g \, i_g \equiv 1 \mod R$. Then $\bar{\imath}_g \, g$ would be an element of R 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 $\bar{\imath}_g, q \notin R$ such that $i_g \, \bar{\imath}_g \in R$ and $q\,(\bar{\imath}_g + i_g) \equiv 1 \mod R$. Thus

- $R = R{:}i_g \cap R{:}\bar{\imath}_g$. Indeed, if $p \in R{:}i_g \cap R{:}\bar{\imath}_g$ then $(\bar{\imath}_g + i_g)\, p \in R$ and therefore $p \in R$.
- $R{:}\bar{\imath}_g$ and $R{:}i_g$ are comaximal because $i \in R{:}\bar{\imath}_g$ and $\bar{\imath}_g \in R{:}i_g$. For this same reason, the inclusion of R in both $R{:}i_g$ and $R{:}\bar{\imath}_g$ is strict.

We can thus construct growing sequences of zero dimensional radical ideals that cannot become stationary before we have obtained zero dimensional radical ideals that admit a characteristic presentation.

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

Algorithm 3.8. 0D-Irredundant-χ-Decomposition

INPUT: *R a zero dimensional radical ideal in $\mathcal{K}[X]$.*
OUTPUT: *$\mathcal{T} = T_1, \ldots, T_r$ a sequence of characteristic presentations of zero dimensional radical ideals such that $R = (T_1){:}I_{T_1}^\infty \cap \ldots \cap (T_r){:}H_{T_r}^\infty$ and $(T_j){:}I_{T_j}^\infty + (T_k){:}I_{T_k}^\infty = \mathcal{K}[X]$, $j \neq k$.*
$G :=$ the reduced Groebner basis of R w.r.t. to the lexicographical order.
if $G = \{1\}$ then
return (Null-Sequence)
elif G has n elements then
return (G)
else
$i :=$ the initial of an element of G such that $i \neq 1$
$R_1 := (R, i)$; $R_2 := R{:}i$;
$\mathcal{T} :=$ 0D-irredundant-χ-decomposition $(R_1, \mathcal{K}[X])$, 0D-irredundant-χ-decomposition $(R_2, \mathcal{K}[X])$;
fi;

We invite the reader to refer to (Moreno-Maza 1997) and (Szanto 1998) to establish constructions that do not involve Groebner basis computations. The elements of the characteristic presentation T_i obtained by the above algorithm all have 1 as initial. It needs not be the case to be in a position to lift the result to positive dimension nor to the differential case. Also, this algorithm requires the input ideal R to be given in a way that a Groebner basis of it can be computed. The fact is that this algorithm needs to be in a position to deal with ideals given as saturations $(A){:}H_A^\infty$, where A is an autoreduced set.

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 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 by an easy criterion to determine when an autoreduced set is a characteristic presentation in positive dimension.

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

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

Assume A is a characteristic set of $((A):H_A^\infty)_{K_A}$. If $((A):H_A^\infty)_K$ contained a nonzero element reduced with respect to A, so would $((A):H_A^\infty)_{K_A}$. Thus A is a characteristic set of $((A):H_A^\infty)_K$

Assume A is a characteristic set of $((A):H_A^\infty)_K$. Assume, for contradiction, there is a nonzero element p of $((A):H_A^\infty)_{K_A}$ reduced with respect to A. Clearing out the denominators of p amounts to multiply p with some element of $\mathcal{K}[\mathfrak{N}(A)]$. Let $\bar{p}$ be the result of this operation. Obviously $\bar{p}$ is nonzero and reduced with respect to A and belongs to $((A):H_A^\infty)_{K_A} \cap \mathcal{K}[\mathfrak{N}(A),\mathfrak{L}(A)] = ((A):H_A^\infty)_K$. This contradict the hypothesis. □

For this reason and Lemma 3.5, $(A):H_A^\infty$ is characterizable iff its reduced Groebner basis with respect to the lexicographic ordering on $\mathcal{K}_A[\mathfrak{L}(A)]$ induced by the ranking has exactly as many elements as $\mathfrak{L}(A)$.

Theorem 3.10. *Let A be an autoreduced set of $\mathcal{K}[X]$. Let $((A):H_A^\infty)_{\mathcal{K}_A} = (T_1):I_{T_1}^\infty \cap \ldots \cap (T_r):I_{T_r}^\infty$ be a (zero dimensional) irredundant characteristic decomposition in $\mathcal{K}_A[\mathfrak{L}(A)]$. For $1 \le i \le r$, let C_i in $\mathcal{K}[X]$ be obtained from T_i by clearing out the denominators. Then $((A):H_A^\infty)_{\mathcal{K}} = (C_1):I_{C_1}^\infty \cap \ldots \cap (C_r):I_{C_r}^\infty$ 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 $\mathcal{K}_A[\mathfrak{L}(A)]$, $\left((C_i):I_{C_i}^\infty\right)_{\mathcal{K}_A}$ and $\left((C_i):I_{C_i}^\infty\right)_{\mathcal{K}_A}$ are respectively equal to $(T_i):I_{T_i}^\infty$ and $(T_i):H_{T_i}^\infty$. Consequently, by Proposition 3.3 applied to $(T_i):H_{T_i}^\infty$, $\left((C_i):I_{C_i}^\infty\right)_{\mathcal{K}_A} = \left((C_i):H_{C_i}^\infty\right)_{\mathcal{K}_A}$.

Recall from Theorem 3.1 and Theorem 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

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

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

Consider $1 \le i \le r$. Let P be a minimal prime of $\left((C_i):I_{C_i}^\infty\right)_{\mathcal{K}_A} \cap \mathcal{K}[X]$. 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 $\mathcal{K}[X]$. $\left((C_i):I_{C_i}^\infty\right)_{\mathcal{K}_A} \cap \mathcal{K}[X]$ contains no autoreduced set lower than C_i otherwise $\left((C_i):I_{C_i}^\infty\right)_{\mathcal{K}_A} = (T_i):I_{T_i}^\infty$ would too; It follows that C_i is a characteristic set of $\left((C_i):I_{C_i}^\infty\right)_{\mathcal{K}_A} \cap \mathcal{K}[X]$ and thus $C_i \subset \left((C_i):I_{C_i}^\infty\right)_{\mathcal{K}_A} \cap \mathcal{K}[X] \subset \left((C_i):I_{C_i}^\infty\right)_{\mathcal{K}}$. Taking the saturation by I_{C_i} on each member of this inclusion we are lead to $\left((C_i):I_{C_i}^\infty\right)_{\mathcal{K}_A} \cap \mathcal{K}[X] = \left((C_i):I_{C_i}^\infty\right)_{\mathcal{K}}$. C_i is thus a characteristic presentation and we have $(A):H_A^\infty = (C_1):I_{C_1}^\infty \cap \ldots \cap (C_r):I_{C_r}^\infty$, which is an irredundant decomposition. □

4. Coherence and its consequences

Coherence is a concept similar to *formal integrability* or *involutivity* in some other algebraic formalism for differential equations. It was introduced in differential ideal theory by (Rosenfeld 1959). It answers the problem exposed in Example 2.6.

Differential ideals defined by coherent autoreduced sets enjoy specific properties which make them the bridge between differential algebra and polynomial algebra. Neither Theorem 4.3 nor Theorem 4.4 appears in the work of Ritt and Kolchin; they did use only particular cases of these theorems related to prime ideals. The first occurrences of these theorem is in (Boulier *et al.* 1995). They are the lifting of Theorem 3.1 and Theorem 3.2 through what Boulier (1994) named the *Rosenfeld lemma*.

Theorem 4.3 is a direct lifting of Theorem 3.1. Our proof of Theorem 4.4 is somewhat different than the one presented in (Boulier *et al.* 1997). From now on, we assume that $\mathcal{F}\{Y\}$ is endowed with a ranking.

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

Definition 4.1. *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 $s_b\, \psi a - s_a \phi b \in (\Theta_v A) : H_A^\infty$.*

Definition 4.2. *Let a and b be differential polynomials in $\mathcal{F}\{Y\}$. If u_a and u_b have a common derivative, let $lcd(u_a, u_b) = \bar\psi u_a = \bar\phi u_b$ be the lowest such derivative. We define the cross-derivative of a and b to be*

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

When u_a and u_b have no common derivative, we define $\textsf{X-derivative}(a,b) = 0$.

We introduce the systematic division by $\gcd(s_b, s_a)$ 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 $\textsf{X-derivative}(a,b) \in (\Theta_{\mathrm{lcd}(u_a,u_b)} A) : H_A^\infty$, $\forall a, b \in A$. An autoreduced set A in $\mathcal{F}\{Y\}$ is coherent if $\textsf{d-rem}(\textsf{X-derivative}(a,b), A) = 0$, $\forall a, b \in A$.

The key result here is a theorem by[4] Rosenfeld (1959) according to which, if A is a coherent autoreduced set, $q \in \mathcal{F}\{Y\}$ partially reduced w.r.t. A belongs to $[A] : H_A^\infty$ iff it belongs to $(A) : H_A^\infty$. This bears as immediate corollary that $p \in [A] : H_A^\infty \;\Leftrightarrow\; \textsf{d-prem}(p, A) \in (A) : H_A^\infty$. The fundamental result to obtain a decomposition into *coherent components* is then the following.

Theorem 4.3. *Let A be an 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. □

Furthermore, 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 4.4. *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 in three steps.

∘ *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 $q \longrightarrow_A \bar q$ so that there exists $h \in H_A^\infty$ such that $h\,q \equiv \bar q \mod [A]$. We have that $\bar q \notin (A) : H_A^\infty$ otherwise q would belong to $[A] : H_A^\infty$ and therefore to P. Nonetheless, $\bar q\,\bar p$ belongs to $[A] : H_A^\infty$ and thus to $(A) : H_A^\infty$ since it is partially reduced w.r.t. A. This says that $\bar p$ belongs to a minimal prime of $(A) : H_A^\infty$. Thus $P \cap \mathcal{F}[\mathfrak{N}(A), \mathfrak{L}(A)]$ 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 $(A) : H_A^\infty$.

∘ *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 prime of $(A) : H_A^\infty$ are the intersection of an essential prime component of $[A] : H_A^\infty$ with $\mathcal{F}[\mathfrak{N}(A), \mathfrak{L}(A)]$.

[4] see also (Kolchin 1973, III.8, lemma 5)

∘ *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 $p \longrightarrow_{C_i} \bar{p}$. 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!).

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

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

We have seen in the previous section 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 Σ of $\mathcal{F}\{Y\}$ it would thus be very nice to be able to find a coherent autoreduced set A such that $\{\Sigma\} = [A]:H_A^\infty$. This is obviously not the general case. We will nonetheless manage to represent $\{\Sigma\}$ as an intersection of such differential ideals.

We will first show how we can compute a coherent autoreduced A that would satisfy 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 4.3. Note that neither Ritt nor Kolchin used this property that $[A]:H_A^\infty$ is radical. The way they would proceed in their decomposition algorithm would rely on a process[5] to decide whether A is a characteristic presentation of a prime differential ideal. In case A were not a characteristic presentation of a prime differential ideal, their 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 $\{\Sigma\} = \{\Sigma, p\} \cap \{\Sigma, q\}$. Only in the case where A is a characteristic presentation of a prime differential ideal, would they be in a position to justify the splitting on the separants.

Boulier *et al.* (1995) already presented a decomposition into coherent component - that are called there regular component. The decomposition was obtained by reworking Seidenberg's elimination scheme. It is interesting that the point of view of Ritt and Seidenberg on reduction do converge.

5.1. Exhibiting a coherent autoreduced set.

Let Σ be a finite set of differential polynomials of $\mathcal{F}\{Y\}$. With a finite number of differentiations and arithmetic operations in $\mathcal{F}\{Y\}$, we can compute a coherent autoreduced set A such that $A \subset [\Sigma]$ and $\forall p \in \Sigma$, $p \longrightarrow_A 0$. Thus $A \subset [\Sigma] \subset [A]:H_A^\infty$. 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: Σ *a set of differential polynomials in* $\mathcal{F}\{Y\}$ *endowed with a ranking.*
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*
  $S := S \cup R \cup D$;
  $A :=$ *Min-Autoreduced* (S);
  $R := \{$*d-rem*$(q, A) \neq 0 \mid q \in R \setminus A\}$;
  $D := \{$*d-rem* (*X-derivative*(a, a'), $A) \neq 0 \mid a, a' \in A\}$;

[5] based on factorizations in tower of algebraic extension (Ritt 1950)

od;
if $S \cap \mathcal{F} \neq \emptyset$ *then*
    return (Null-Sequence);
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. By (Kolchin 1973, I.10, Proposition 3) any decreasing sequence of autoreduced sets is finite. This algorithm thus terminates.

It is worth noting that we can avoid forming certain cross derivatives thanks to an analogue of the second Buchberger criterion (Boulier *et al.* 1997).

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

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

Theorem 5.2. *Given a finite set* Σ *of differential polynomials in* $\mathcal{F}\{Y\}$ *we can compute a finite number of coherent autoreduced sets* $A_1, \ldots, A_r$ *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[6] *of* $\{\Sigma\}$*. Algorithm 5.3 computes such a decomposition into coherent components.*

Algorithm 5.3. Coherent-Components

INPUT: Σ, *a finite set of differential polynomials of* $\mathcal{F}\{Y\}$ *endowed with a ranking.*
OUTPUT: $\mathfrak{A} = A_1, \ldots, A_r$, *a sequence of coherent autoreduced sets such that* $\{\Sigma\} = \bigcap_{i=1}^{r} [A_i]:H_{A_i}^\infty$.

$A :=$ Coherent-Autoreduced $(\Sigma, \mathcal{F}\{Y\})$;
if $A = 1$ *then*
    return (Null-Sequence);
else
    $\mathfrak{A} = A$, Coherent-Components $(\{\Sigma, s_a\}, \mathcal{F}\{Y\})_{a\in A}$, Coherent-Components $(\{\Sigma, i_a\}, \mathcal{F}\{Y\})_{a \in A}$;
fi;

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

Thanks to the properties of coherent components disclosed by Rosenfeld's lemma, this decomposition brings already information. For instance, it already allows us to test membership to $\{\Sigma\}$ (Boulier *et al.* 1995).

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 many different ways. It allows to decouple 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 presentation. Let's note that Ritt and Kolchin enunciated and made use only of the prime ideal case (Kolchin 1973, IV.9, lemma 2) of the following lemma.

[6]called *regular components* in (Boulier *et al.*, 1995, 1997) and (Hubert 1998).

Lemma 6.1. *Let A be an autoreduced set of $\mathcal{F}\{Y\}$. A necessary and sufficient condition for A to be a characteristic presentation in $\mathcal{F}\{Y\}$ is that A be coherent and A is a characteristic presentation 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 $a, b \in A$, $\mathsf{X\text{-}derivative}(a,b) \in [A] \subset [A]:H_A^\infty$. 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 $\mathsf{X\text{-}derivative}(a,b) \in (\Theta_v A) : H_A^\infty$. Now, if A is a characteristic set of $[A]:H_A^\infty$, $[A]:H_A^\infty$ has no non-zero element 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 would exist 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 $[A]:H_A^\infty$. □

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

Proof. Let $B_{i,j}$, $1 \le j \le r_i$, be the characteristic sets of the minimal primes of $(C_i) : I_{C_i}^\infty$; $(C_i) : I_{C_i}^\infty = \cap_{j=1}^{r_i} (B_{ij}):I_{B_{ij}}^\infty$. By Theorem 4.4, B_{ij} is the characteristic set of $[B_{ij}]:H_{B_{ij}}^\infty$, an essential prime component of $[A]:H_A^\infty$.

Let $a, b \in C_i$; $\mathsf{X\text{-}derivative}(a,b)$ belongs to $\cap_{j=1}^{r_i} [B_{ij}] : H_{B_{ij}}^\infty$. Thus, $\mathsf{d\text{-}rem}(\mathsf{X\text{-}derivative}(a,b), C_i)$ belongs to $\cap_{j=1}^{r_i} \left([B_{ij}]:H_{B_{ij}}^\infty \cap \mathcal{F}[\mathfrak{N}(A), \mathfrak{L}(A)]\right)$. As $[B_{ij}] : H_{B_{ij}}^\infty \cap \mathcal{F}[\mathfrak{N}(A), \mathfrak{L}(A)] = (B_{ij}) : H_{B_{ij}}^\infty = (B_{ij}) : I_{B_{ij}}^\infty$ (Theorem 4.4) and $\cap_{j=1}^{r_i} (B_{ij}):I_{B_{ij}}^\infty = (C_i):I_{C_i}^\infty$, we deduct that $\mathsf{d\text{-}rem}(\mathsf{X\text{-}derivative}(a,b), C_i) \in (C_i):I_{C_i}^\infty$. C_i being a characteristic set of $(C_i) : I_{C_i}^\infty$, we are led to the conclusion that $\mathsf{d\text{-}rem}(\mathsf{X\text{-}derivative}(a,b), C_i) = 0$. Therefore C_i is coherent. By Lemma 6.1, C_i is a characteristic set of $[C_i]:H_{C_i}^\infty$. By Theorem 4.4, $[C_i]:H_{C_i}^\infty = \cap_{j=1}^{r_i} [B_{ij}]:H_{B_{ij}}^\infty$ and therefore $[A]:H_A^\infty = \cap_{i=1}^r [C_i]:H_{C_i}^\infty$. This decomposition is furthermore irredundant. □

7. Conclusion

We recapitulate in MAPLE pseudo-code the algorithm for which we have given all the mathematical justifications in this paper. It is very simple and relies only on two ingredients; First a decomposition into coherent components, as described in Section 5. Then, Theorem 6.2 together with Theorem 3.10 justify the fact that a characteristic decomposition of a coherent component can be lifted from an irredundant characteristic decomposition of a zero dimensional radical ideal. The second ingredient is therefore Algorithm 3.8, or an algorithm of the same specification.

Algorithm 7.1. **χ-Decomposition**

INPUT: Σ, *a finite set of differential polynomials of $\mathcal{F}\{Y\}$ endowed with a ranking.*
OUTPUT: $\mathfrak{C} = C_1, \ldots, C_r$, *a sequence of characteristic presentations such that* $\{\Sigma\} = \bigcap_{i=1}^r [C_i]:H_{C_i}^\infty$.

$\mathfrak{A} :=$ *Coherent-Components* $(\Sigma, \mathcal{F}\{Y\})$;
$\mathfrak{C} :=$ *Null-sequence;*
For A *in* $\mathfrak{A}$ *do*
  $C :=$ *0D-Irredundant-χ-Decomposition* $(A, \mathcal{F}(\mathfrak{N}(A))[\mathfrak{L}(A)])$;
  $C :=$ *clear out the denominators in the elements of* C;
  $\mathfrak{C} := C, \mathfrak{C}$
od;

This theoretical simplicity is unfortunately not always reflected by reasonably sized computations. Careful implementation and heuristics are needed to avoid expression swell and to minimize the number of reductions, cross-derivative formations and splittings.

We presented in this paper the basics of an effective decomposition algorithm in differential algebra. The key idea is to work with differential ideals that are not prime, the little drawback being that the results depend on the ranking chosen. This idea was first successfully explored by Boulier (1994, 1995,1997) who used a Seidenberg's like approach.

In this paper we reworked Ritt's approach and saw that the same algebraic results could be used to make this approach effective. We have provided some new concise proofs of these results. We furthermore presented new results that can be applied in both approaches. This results allow to lift a decomposition obtained in polynomial algebra of dimension zero to a differential decomposition. This complete uncoupling of the algebraic and differential operations allow direct improvement and simplification of the algorithms.

Appendix A. Implementation tips

The main work in the purely algebraic part (Algorithm 3.8) of our decomposition algorithm is the computation of the reduced Groebner basis of a zero dimensional radical idea according to a lexicographic term order. We can find in the literature several ways to make this process efficient. Now, the ideal of which we want the Groebner basis is the saturation ideal $(A)\colon H_A^\infty$, where A is an autoreduced set. The point of this appendix is just to show how we can rewrite A so that the traditional Buchberger algorithm is no longer the bottleneck of our Maple implementation.

We work in $\mathcal{K}[x_1,\ldots,x_n]$ with a ranking $x_1 < \ldots < x_s$. We assume $A = a_1, a_2, \ldots, a_n$ where x_j is the leader of a_j, $1 \le j \le n$. We denote i_j, s_j and d_j respectively the initial, the separant and the degree in x_j of a_j.

For $1 \le k \le 2n$, we introduce the dummy indeterminates z_k. They will represent $1/i_k$ and $1/s_{k-n+1}$. We endow $\mathcal{K}[x_1,\ldots,x_n,z_1,\ldots,z_{2n}] = \mathcal{K}[X][Z]$ with a block term order eliminating Z and extending the lexicographic term order $x_1 < \ldots < x_s$. The reduced Groebner basis G of $(A)\colon H_A^\infty$ can be obtain as follow: if G_Z is a Groebner basis of $(a_1,\ldots,a_n, 1-z_1\, i_1, 1-z_1\, i_1, \ldots, 1-z_n\, i_n, 1-z_{n+1}\, s_1, \ldots, 1-z_{2n}\, s_n)$, then $G = G_Z \cap \mathcal{K}[X]$. From practical experience it is nonetheless useful to make some substitution for the a_j and s_j, as explained below.

Let a be an element of $\mathcal{K}[X]$. Let x, s and d be respectively its leader, initial, separant and the degree of a in x. Write $f_d, \ldots, f_0$ the coefficients of the powers of x in a; f_d is the leader of a and $a = f_d\, u^d + f_{d-1}\, u^{d-1} + \ldots + f_0$. We note that $s = d\, f_d\, x^{d-1} + (d-1)\, f_{d-1}\, x^{d-2} + \ldots + f_1 = d\, f_d\, x^{d-1} + (s \mod x^{d-1})$ and $d\, a = s\, x + \tilde{a}$, where $\tilde{a} = \sum_{k=0}^{d-1} f_k\, x^k$. Before computing G_Z, we can therefore replace a_j by $x_j + z_{n+1+j}\, \tilde{a_j}$ and s_j by $d_j\, x_j^{d_j-1} + z_j\, (s_j \mod x_j^{d_j-1})$.

It is also worthwhile not considering plainly the separant and the initials but a set of pairwise prime squarefree factors that generates H_A^∞. These factors are obtained by partial squarefree factorization of the separants and initials.

We can also make the following substitution for the elements of A. If a_j has a content with respect to x_j which does not belong to $\mathcal{K}$ this content divides i_j. We can thus replace a_j by its primitive part according to x_j. Similarly, to decrease the degrees, we can eliminate from a_j the factors which are common with s_j. Thus we can substitute $\frac{a_j}{\gcd(a_j, s_j^2)}$ to a_j.

References

Becker, T., Weispfenning, V. (1993). *Gröbner Bases - A Computational Approach to Commutative Algebra.* Springer-Verlag.

Boulier, F. (1994). *Étude et Implantation de Quelques Algorithmes en Algèbre Différentielle.* PhD thesis, Université de Lille.

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

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

Carra'Ferro, G. (1987). Gröbner bases and differential algebra. In *AAECC*, volume 356 of *Lecture notes in Computer Science*. Springer.

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

Hubert, E. (Avril 1997). *Algebra and Algorithms for Singularities of Implicit Differential Equations*. PhD thesis, Institut National Polytechnique de Grenoble. Possible download from ftp://ftp.imag.fr/pub/Mediatheque.IMAG/theses/97-Hubert.Evelyne/notice-anglais.html.

Hubert, E. (1998). Essential components of an algebraic differential equation. *Journal of Symbolic Computation*. (To appear).

Kalkbrener, M. (1993). A generalized euclidean algorithm for computing triangular representations of algebraic varieties. *Journal of Symbolic Computations*, 15(2):143–167.

Kaplansky, I. (1970). *An Introduction to Differential Algebra*. Hermann.

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

Lazard, D. (1992). Solving zero dimensional algebraic systems. *Journal of Symbolic Computations*, 15:117–132.

Maârouf, H., Kandri Rody, A., Ssafini, M. (1998). Triviality and dimension of a system of algebraic differential equations. *J. Automat. Reason.*, 20(3):365–385.

Mansfield, E. (1991). *Differential Gröbner Bases*. PhD thesis, University of Sydney.

Moreno-Maza, M. (1997). *Calculs de pgcd au-dessus des tours d'extensions simples et résolution des système d'équations algébriques*. PhD thesis, Université Paris 6.

Morrison, S. (1999). To appear.

Ollivier, F. (1990). *Le problème de l'identifiabillité Structurelle Globale: Approche Théorique, Méthodes Effectives et Bornes de Complexité.*. PhD thesis, École Polytechnique.

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

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

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

Szanto, A. (1998). *Computation with polynomial systems*. PhD thesis, Cornell University.

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

MSRI, 1000 CENTENNIAL DRIVE, BERKELEY CA 94720-5070 USA

E-mail address: evelyne @ msri.org