Theoretical Computer Science 98 (1992) 137–161
Elsevier

Differential-algebraic decision methods and some applications to system theory

Sette Diop

Laboratoire d'Automatique et de Génie des Procédés, CNRS-Université Claude Bernard, Bât. 721, 43 Bd. du 11 Novembre 1918, 69622 Villeurbanne-France

Abstract

Diop, S., Differential-algebraic decision methods and some applications to system theory, Theoretical Computer Science 98 (1992) 137–161.

This paper provides a general view of differential-algebraic decision methods and their applications to system theory. It includes the basic properties of differential polynomials, reduction procedures and culminates in the concept of characteristic set and its computation. Such topics are well known from the works by Ritt (1950). A characteristic set of a differential ideal is a finite subset from which many properties of the differential ideal are often readily obtainable merely by inspecting its elements. This is the main point of decision methods in differential algebra. We show through some theorems that basic tests in system theory are thus performable by means of a characteristic set of the differential ideal defining a system. Such tests are, say, invertibility, observability, universal external trajectories computation, etc. As far as computation of characteristic sets is constructive, these tests are now available for algebraic systems. Computation of characteristic sets is actually constructive *in principle*, but a general algorithm which is fit for use is wanting. Interesting partial results are proposed. Reduce programs of the algorithms described in this paper are written.

0. Introduction

The aim of this report is to make available to system theory community differential-algebraic decision methods which should be of some interest. The main ideas of decision methods are very old in mathematics; they are often named after Kronecker, Hilbert, Hermann, Tarski, etc. When founding differential algebra, Ritt [12] introduced many of them, providing this new discipline with these powerful tools. The pioneering work by Ritt is now considered standard, thanks to Seidenberg [14], Rosenfeld [13], Kolchin [10], and Sit [15, 16]. This paper hardly contains some novelty in the field of differential-algebraic decision methods, except for its systematic and elementary expository aspect, and some partial results. Our goal is rather to lay down the main lines of applications of these techniques to system theory problems.

We shall report many things from the book by Kolchin [11], merely because we believe that it will be of some interest for system theorists to have a self-contained expository text which is general enough to embrace the main system theory problems and which excludes the generalities in Kolchin's work which are unnecessary for standard applications. This part includes differential polynomial algebras, characteristic sets, differential polynomial dimensions, and some basic decision problems. This text is incomplete in the sense that a general procedure for construction of characteristic sets is not laid down in detail, whereas almost all our results assume the availability of such a construction. However, we may console ourselves with the idea that this construction is possible *in principle*; what is really lacking is merely a fit-for-use algorithm, which certainly will be derived in further studies. Nevertheless, we give an interesting particular case where easy computations lead to characteristic sets of differential ideals.

The last section aims to show some applications of the previous results to system theory problems. The general problem of computing invariants such as dimension, transcendence degrees, etc. is readily solved as soon as we may compute a characteristic set. The problem of realization of ordinary systems (i.e., those defined by algebraic ordinary differential equations) is considered, too. Observability test as well as computation of universal external trajectories are shown to be readily performable on the basis of characteristic sets. Invertibility test is also discussed.

Recall that differential algebra has been introduced in system theory since 1985 by Fliess [6].

Throughout this paper, the word ring will stand for commutative ring with unit element, the word field for commutative field, and the word algebra for associative and commutative algebra with unit element; we assume the characteristic of rings, fields, and algebras to be zero, i.e., the latter contain the field $\mathbb{Q}$ *of rational numbers as a subfield.*

1. Differential polynomial algebras

Let $\mathbf{R}$ be a differential ring with set of derivations Δ. Let δ be the cardinal number of Δ. Let Θ denote the free commutative monoid (denoted multiplicatively) generated by the elements of Δ, with unit element 1. The elements of Θ are called the *derivative operators* of $\mathbf{R}$. For every derivative operator θ, there exists one, and only one, δ-tuple $(e(\partial))_{\partial\in\Delta}$ of natural integers such that $\theta=\prod_{\partial\in\Delta}\partial^{e(\partial)}$; Θ is thus isomorphic to the additive monoid $\mathbb{N}^{\delta}$. The integer $\sum_{\partial\in\Delta}e(\partial)$ is denoted by $o(\theta)$, and called the *order* of θ. A *proper* derivative operator is one with $o(\theta)\geqslant 1$. When $\delta=0$, Θ consists solely of 1, and there is no proper derivative operator.

Recall that the polynomial $\mathbf{R}$-algebra in the family of indeterminates $(T_i)_{i\in\mathbf{I}}$ is denoted by $\mathbf{R}[(T_i)_{i\in\mathbf{I}}]$. Its *monomials* are the following objects:

$$T^{\mu}=\prod_{i\in\mathbf{I}}T_i^{\mu_i},$$

where $\mu=(\mu_i)_{i\in\mathbf{I}}\in\mathbb{N}^{(\mathbf{I})}$[1]. The elements of $\mathbf{R}[(T_i)_{i\in\mathbf{I}}]$ are the (*finite*) linear combinations of monomials in $(T_i)_{i\in\mathbf{I}}$ with coefficients in $\mathbf{R}$:

$$P=\sum_{\mu\in\mathbb{N}^{(\mathbf{I})}} a_\mu T^\mu,$$

where $(a_\mu)_{\mu\in\mathbb{N}^{(\mathbf{I})}}\in\mathbf{R}^{(\mathbb{N}^{(\mathbf{I})})}$.

The polynomial $\mathbf{R}$-algebra in the family of indeterminates indexed by the set of θT_i ($i\in\mathbf{I}$, $\theta\in\Theta$) is denoted by $\mathbf{R}[(\theta T_i)_{i\in\mathbf{I},\,\theta\in\Theta}]$. Its monomials are

$$T^\nu=\prod_{(i,\theta)\in\mathbf{I}\times\Theta}(\theta T_i)^{\nu_{i,\theta}},$$

where $(\nu_{i,\theta})_{(i,\theta)\in\mathbf{I}\times\Theta}=\nu\in\mathbb{N}^{(\mathbf{I}\times\Theta)}$. Its elements are

$$\sum_\nu a_\nu T^\nu,$$

where $(a_\nu)_\nu\in\mathbf{R}^{(\mathbb{N}^{(\mathbf{I}\times\Theta)})}$. $\mathbf{R}[(\theta T_i)_{(i,\theta)\in\mathbf{I}\times\Theta}]$ is made into a differential $\mathbf{R}$-algebra by assuming, for any $\partial\in\Delta$, that

$$\partial(T^\nu)=\sum_{(i,\theta)\in\mathbf{I}\times\Theta}\nu_{i,\theta}T^{\nu'}\cdot(\partial\theta T_i),$$

where, if $\nu=(\nu_{i,\theta})_{(i,\theta)\in\mathbf{I}\times\Theta}$, then $\nu'=(\nu'_{i',\theta'})_{(i',\theta')\in\mathbf{I}\times\Theta}$, with $\nu'_{i',\theta'}=\nu_{i',\theta'}$ for $(i',\theta')\neq(i,\theta)$ and $\nu'_{i,\theta}=\max(\nu_{i,\theta}-1,0)$ (note that ν' should be indexed by (i,θ) since it depends on this object), and

$$\partial\left(\sum_\nu a_\nu T^\nu\right)=\sum_\nu\partial(a_\nu)T^\nu+\sum_\nu a_\nu\partial(T^\nu).$$

The differential $\mathbf{R}$-algebra thus defined is denoted by $\mathbf{R}\{(T_i)_{i\in\mathbf{I}}\}$, and called *the differential polynomial* $\mathbf{R}$*-algebra in the differential indeterminates* $(T_i)_{i\in\mathbf{I}}$. If $\mathbf{I}$ is a finite set with cardinality μ, then $\mathbf{R}\{(T_i)_{i\in\mathbf{I}}\}$ is denoted by $\mathbf{R}\{T_1,T_2,\ldots,T_\mu\}$, or by $\mathbf{R}\{\mathbf{T}\}$ if $\mathbf{I}$ consists of one single element. We note that if $\delta=0$, i.e., if the set of derivations of $\mathbf{R}$ is empty, then $\mathbf{R}\{(T_i)_{i\in\mathbf{I}}\}=\mathbf{R}[(T_i)_{i\in\mathbf{I}}]$.

The integer $o(T^\nu)$ defined as

$$\sum_{\substack{(i,\theta)\in\mathbf{I}\times\Theta\\ \nu_{i,\theta}\neq 0}} o(\theta)$$

is called the *order* of the differential monomial

$$T^\nu=\prod_{(i,\theta)\in\mathbf{I}\times\Theta}(\theta T_i)^{\nu_{i,\theta}}.$$

[1] We agree that if $\mathbf{E}$ is a commutative monoid with e as unit element, and if $\mathbf{I}$ is an arbitrary set, then $\mathbf{E}^{(\mathbf{I})}$ denotes the set of families of elements of $\mathbf{E}$ indexed by $\mathbf{I}$ whose members are all equal to e but are finite in number. When no precision is given on the structure of the monoid $\mathbf{E}$, the obvious one is assumed to be attached to $\mathbf{E}$.

The *order* of a differential polynomial P is the maximum $o(P)$ of the orders of its monomials which have nonzero coefficients.

$\mathbf{R}\{(T_i)_{i\in\mathbf{I}}\}$ is a differential *integral* domain if and only if $\mathbf{R}$ is such.

$\mathbf{R}\{(T_i)_{i\in\mathbf{I}}\}$ is easily seen as the *free* differential $\mathbf{R}$-algebra generated by the set consisting of the T_i $(i\in\mathbf{I})$. Hence, any map f of the set T_i $(i\in\mathbf{I})$ into a differential $\mathbf{R}$-algebra $\mathbf{A}$ extends, in a unique way, to a differential $\mathbf{R}$-algebra morphism $\bar{f}$ of $\mathbf{R}\{(T_i)_{i\in\mathbf{I}}\}$ into $\mathbf{A}$ such that

$$\bar{f}\left(\sum_{\nu} a_\nu T^\nu\right)=\sum_{\nu} a_\nu f(T)^\nu,$$

where, for $\nu=(\nu_{i,\theta})_{(i,\theta)\in\mathbf{I}\times\Theta}$,

$$f(T)^\nu=\prod_{(i,\theta)\in\mathbf{I}\times\Theta}(\theta f(T_i))^{\nu_{i,\theta}}.$$

In particular, if $\mathbf{R}$ and $\mathbf{A}$ are two Δ-differential rings, and if $f:\mathbf{R}\to\mathbf{A}$ is a differential ring morphism and $(t_i)_{i\in\mathbf{I}}$ a family of elements of $\mathbf{A}$, then there is one, and only one, differential ring morphism $\tilde{f}:\mathbf{R}\{(T_i)_{i\in\mathbf{I}}\}\to\mathbf{A}$ such that the restriction to $\mathbf{R}$ of $\tilde{f}$ coincides with f, and $\tilde{f}(T_i)=t_i$ $(i\in\mathbf{I})$. The image through $\tilde{f}$ of P is usually denoted by $P((t_i)_{i\in\mathbf{I}})$, and called the *value* of P at $(t_i)_{i\in\mathbf{I}}$. This allows one to indistinguishably write P or $P((T_i)_{i\in\mathbf{I}})$, as these symbols denote the same object.

2. Characteristic sets

Calculations on a ring usually invoke a basic procedure known as the reduction procedure. In order to provide differential polynomial algebras with such a procedure, it is necessary to define the notion of a differential polynomial reduced with respect to another one as is done for usual polynomials by means of their degrees. The concept of *ranking* is the first step towards that goal. Given a differential ideal by means of one of its sets of generators, does there exist some subset of that ideal the computations on which will make easier the answers to questions on the ideal? A characteristic set of a differential ideal aims to play that role. It is not a set of generators of the ideal but it characterizes the ideal, at least when the ideal is prime. The concept of characteristic set goes back to van der Waerden (who called it basic set) and was extensively studied by Ritt [12]. We start by recalling some basic facts on orderings which may be useful.

2.1. *On ordered sets*

An order $\leqslant$ on a set $\mathbf{S}$ is a relation on $\mathbf{S}$ such that

(i) $x\leqslant x$ $(x\in\mathbf{S})$,

(ii) $x\leqslant y$ and $y\leqslant z \Rightarrow x\leqslant z$ $(x,y,z\in\mathbf{S})$,

(iii) $x\leqslant y$ and $y\leqslant x \Rightarrow x=y$ $(x,y\in\mathbf{S})$.

A relation with only properties (i) and (ii) is called a *pre-order*. A set equipped with an order (pre-order) is said to be an *ordered* (*pre-ordered*) *set*. The notation $x<y$ will stand for its usual meaning: $x\leqslant y$ and $x\neq y$. An order $\leqslant$ on a set $\mathbf{S}$ is said to be *total* (or *linear*) if any couple of the elements of $\mathbf{S}$ can be compared (i.e., for all x, y in $\mathbf{S}$ either $x\leqslant y$ or $y\leqslant x$). By restriction, a subset of an ordered set is also ordered. The product set $\mathbf{S}=\prod_{i\in\mathbf{I}}\mathbf{S}_i$ of a family $(\mathbf{S}_i)_{i\in\mathbf{I}}$ of ordered sets is equipped with a canonical order called the *product order* on $\mathbf{S}$ and defined by

$$(x_i)_{i\in\mathbf{I}}\leqslant(y_i)_{i\in\mathbf{I}} \text{ if } x_i\leqslant y_i \quad (i\in\mathbf{I},\ (x_i)_{i\in\mathbf{I}},(y_i)_{i\in\mathbf{I}}\in\mathbf{S}).$$

The product order on $\mathbf{S}$ is not necessarily total when the orders on the components are all total, as shown by the case of $\mathbb{N}\times\mathbb{N}$ when $\mathbb{N}$ is equipped with its natural order.

An element a of a pre-ordered set $\mathbf{S}$ is said to be *maximal* (*minimal*) if there is no element in $\mathbf{S}$ which is strictly greater (less) than a. An element a of an ordered set $\mathbf{S}$ is called the *greatest* (*least*) element of $\mathbf{S}$ if any element in $\mathbf{S}$ is less (greater) than or equal to a; if such a greatest (least) element exists, it is clearly unique. In a *totally* ordered set maximal and greatest are synonyms, and minimal and least are synonyms, too.

An order on a set is called a *well-order* if every nonempty subset contains a least element. A set equipped with a well-order is said to be *well-ordered*. A well-order is a total order; the converse is not compatible with the axiom of infinity which is usually assumed in set theory. The product order on $\prod_{i\in\mathbf{I}}\mathbf{S}_i$ is not a well-order when the $\mathbf{S}_i$'s are well-orders, as is seen through the example of $\mathbb{N}^2$. When $\mathbf{I}$ is a *well-ordered set*, the product set $\mathbf{S}=\prod_{i\in\mathbf{I}}\mathbf{S}_i$ can be endowed with the order defined as follows.

For all $(x_i)_{i\in\mathbf{I}},(y_i)_{i\in\mathbf{I}}\in\mathbf{S}$, let $(x_i)_{i\in\mathbf{I}}<(y_i)_{i\in\mathbf{I}}$ if, for the least index i such that $x_i\neq y_i$, $x_i<y_i$; this order on $\mathbf{S}$ is called the *lexicographic order* on $\mathbf{S}$. The product set $\mathbf{S}$ equipped with the lexicographic order is called the *lexicographic product set* of $(\mathbf{S}_i)_{i\in\mathbf{I}}$. The lexicographic product order is total as soon as the orders on the components all are well-orders.

Lemma 2.1. *In an ordered set* $\mathbf{S}$ *the following assertions,*

(i) *every decreasing sequence of elements of* $\mathbf{S}$ *is stationary,*

(ii) *every nonempty subset of* $\mathbf{S}$ *has a minimal element,*

are equivalent.

Assume that there is a nonempty subset $\mathbf{S}_1$ of $\mathbf{S}$ which has no minimal element. Hence, for every x in $\mathbf{S}_1$ the subset $\mathbf{S}_1(x)$ consisting of the elements y such that $y<x$ is nonempty. By the axiom of choice, there is a map $f:\mathbf{S}_1\to\mathbf{S}_1$ such that for every x in $\mathbf{S}_1$, $f(x)$ is in $\mathbf{S}_1(x)$. Let x_0 be freely chosen in $\mathbf{S}_1$. The sequence defined by $x_{n+1}=f(x_n)$ is a strictly increasing sequence of elements of $\mathbf{S}$. This shows that (i)$\Rightarrow$(ii). Now assume (ii) and let (x_n) be a decreasing sequence of elements of $\mathbf{S}$. The subset of $\mathbf{S}$ consisting of the elements x_n ($n\in\mathbb{N}$) is nonempty and, hence, has a minimal element x_{n_0}. It is clear that $x_n=x_{n_0}$ for all $n\geqslant n_0$. The implication (ii)$\Rightarrow$(i) is, thus, proved, and the stated equivalence, too.

Lemma 2.2. *In an ordered set* **S** *the following assertion,*

(iii) *every sequence of elements of* **S** *has an increasing subsequence,*

implies the above-mentioned equivalent ones ((i) *and* (ii)). *Assertions* (i), (ii) *and* (iii) *are equivalent if the order on* **S** *is* total. *An ordered set* **S** *is a well-ordered one if and only if it is totally ordered, and if* (i), (ii) *and* (iii) *are equivalent* properties *of* **S**.

The fact that (iii)⇒(i) in any ordered set is clear since from (iii) it follows that there is no sequence of elements of **S** which is strictly decreasing, and the latter condition is equivalent to (i). Now let **S** be a totally ordered set, and (x_n) a sequence of elements of **S**. The subset of **S** consisting of the elements x_n $(n\in\mathbb{N})$ is nonempty and, hence, has a least element x_{n_0}. Again, the subset of **S** consisting of the elements x_n $(n>n_0)$ is nonempty and, hence, has a least element x_{n_1} with $x_{n_0}\leqslant x_{n_1}$. Since this construction leads to a subsequence (x_{n_i}) such that

$$i<j \Rightarrow x_{n_i}\leqslant x_{n_j} \quad (i, j\in\mathbb{N}),$$

(ii)⇒(iii). The last statement of the lemma is clear.

Lemma 2.3. *A finite product* $\mathbf{S}=\prod_{1\leqslant i\leqslant m}\mathbf{S}_i$ *of well-ordered sets, when equipped with the product order, has the above properties* (i), (ii) *and* (iii) (*which then are equivalent*) *but is, in general, not a totally ordered set and a fortiori a well-ordered set.*

The first part of the lemma is straightforward. The second one is clear since (1, 2) and (2, 1) are not comparable with respect to the product order; the product set $\mathbb{N}\times\mathbb{N}$ is not totally ordered.

The finite *lexicographic product set of* $(\mathbf{S}_i)_{i\in\mathbf{I}}$ *is well-ordered as soon as all the* $\mathbf{S}_i$ $(i\in\mathbf{I})$ *are such.*

2.2. *Pre-orders on* $\mathbf{R}\{T_1, \ldots, T_\mu\}$

Let **R** be a nonzero Δ-differential ring, $\partial_1, \ldots, \partial_\delta$ the elements of Δ, and Θ the set of derivative operators of **R**. Let $\mathbf{R}\{T_1, \ldots, T_\mu\}$ be a differential polynomial **R**-algebra in the differential indeterminates $T_1, \ldots, T_\mu$.

A *ranking* of the differential indeterminates $T_1, \ldots, T_\mu$ is a *total order* on the set of derivatives of indeterminates ΘT, consisting of θT_i $(\theta\in\Theta, i\in\{1, \ldots, \mu\})$, which satisfies

(i) $u\leqslant\theta u$ $(u\in\Theta T, \theta\in\Theta)$,

(ii) $u\leqslant v \Rightarrow \theta u\leqslant\theta v$ $(u, v\in\Theta T, \theta\in\Theta)$.

We note that if $\delta=0$, then a ranking of $T_1, \ldots, T_\mu$ is merely a total order of the set consisting of $T_1, \ldots, T_\mu$.

Note that there is a bijective correspondence between ΘT and $\mathbb{N}_\mu^*\times\mathbb{N}^\delta$ induced in an obvious way by the bijection $\partial^{r_1}\cdots\partial^{r_\delta}\mapsto(r_1, \ldots, r_\delta)$ of Θ onto $\mathbb{N}^\delta$, where $\mathbb{N}_\mu^*$ stands for the set of the μ first nonzero elements of $\mathbb{N}$. By means of this correspondence, the

rankings of $T_1, \ldots, T_\mu$ are bijectively in correspondence with the total orders on the set $\mathbb{N}_\mu^* \times \mathbb{N}^\delta$ which satisfy the following conditions corresponding to (i) and (ii) above:

(i') $(i, r_1, \ldots, r_\delta) \leqslant (i, r_1 + e_1, \ldots, r_\delta + e_\delta)$ $((i, r_1, \ldots, r_\delta) \in \mathbb{N}_\mu^* \times \mathbb{N}^\delta, (e_1, \ldots, e_\delta) \in \mathbb{N}^\delta)$;

(ii') $(i, r_1, \ldots, r_\delta) \leqslant (i', r'_1, \ldots, r'_\delta) \Rightarrow (i, r_1 + e_1, \ldots, r_\delta + e_\delta) \leqslant (i', r'_1 + e_1, \ldots, r'_\delta + e_\delta)$ $((i, r_1, \ldots, r_\delta), (i', r'_1 \ldots, r'_\delta) \in \mathbb{N}_\mu^* \times \mathbb{N}^\delta, (e_1, \ldots, e_\delta) \in \mathbb{N}^\delta)$.

Lemma 2.4 (Kolchin [11]). *The product order is clearly not a well-order on* $\mathbb{N}_\mu^* \times \mathbb{N}^\delta$, *but it verifies the following fundamental property: Every sequence of elements of* $\mathbb{N}_\mu^* \times \mathbb{N}^\delta$ *possesses an increasing subsequence whose elements all have the same projection on* $\mathbb{N}_\mu^*$.

Any sequence of elements of $\mathbb{N}_\mu^* \times \mathbb{N}^\delta$ has an increasing subsequence as, by Lemma 2.3, this is a property of any finite product of well-ordered sets equipped with the product order. Now the last components of the elements of such an increasing sequence must be the same beyond some range. It then suffices to take the subsequence beginning at this range and having the same elements as the original sequence. This proves the lemma.

The lexicographic order on $\mathbb{N}_\mu^* \times \mathbb{N}^\delta$ with respect to $(\sum_{1 \leqslant j \leqslant \delta} r_j, i, r_1, \ldots, r_\delta)$ (i.e., the order on $\mathbb{N}_\mu^* \times \mathbb{N}^\delta$ induced by the lexicographic order on $\mathbb{N} \times \mathbb{N}_\mu^* \times \mathbb{N}^\delta$ via the injective map $(i, r_1, \ldots, r_\delta) \mapsto (\sum_{1 \leqslant j \leqslant \delta} r_j, i, r_1, \ldots, r_\delta)$ of $\mathbb{N}_\mu^* \times \mathbb{N}^\delta$ into $\mathbb{N} \times \mathbb{N}_\mu^* \times \mathbb{N}^\delta$) clearly verifies the above properties (i') and (ii') and, hence, corresponds to a ranking of $T_1, \ldots, T_\mu$.

A ranking of $T_1, \ldots, T_\mu$ *is a well-order of the set* ΘT *of derivatives of the differential indeterminates.* This results from the following basic lemma.

Lemma 2.5 (Kolchin [11]). *With respect to any* total *order on* $\mathbb{N}_\mu^* \times \mathbb{N}^\delta$ *which verifies the above property* (i'), $\mathbb{N}_\mu^* \times \mathbb{N}^\delta$ *is well-ordered.*

By Lemma 2.2, a total order on $\mathbb{N}_\mu^* \times \mathbb{N}^\delta$ is a well-order if every sequence in $\mathbb{N}_\mu^* \times \mathbb{N}^\delta$ has an increasing sequence. Since, by Lemma 2.4, any sequence of elements of $\mathbb{N}_\mu^* \times \mathbb{N}^\delta$ has a subsequence whose elements all have the same last component and which is increasing with respect to the product order, it will suffice to show that such an increasing sequence is also increasing with respect to any order $\leqslant$ on $\mathbb{N}_\mu^* \times \mathbb{N}^\delta$, which verifies the property (i'). Let $(i, r_1, \ldots, r_\delta), (i, r'_1, \ldots, r'_\delta) \in \mathbb{N}_\mu^* \times \mathbb{N}^\delta$ be such that $(i, r_1, \ldots, r_\delta)$ is less than or equal to $(i, r'_1, \ldots, r'_\delta)$ with respect to the product order, and let $e_1 = r'_1 - r_1, \ldots, e_\delta = r'_\delta - r_\delta$. We have, by property (i'), $(i, r_1, \ldots, r_\delta) \leqslant (i, r_1 + e_1 = r'_1, \ldots, r_\delta + e_\delta = r'_\delta)$, which proves the stated property.

A ranking is said to be *orderly* if $\delta \geqslant 1$, and if $\theta T_i < \theta' T_j$ whenever $o(\theta) < o(\theta')$. The lexicographic ranking with respect to $(\sum_{1 \leqslant j \leqslant \delta} r_j, i, r_1, \ldots, r_\delta)$ is an orderly ranking of $T_1, \ldots, T_\mu$.

Let $P \in \mathbf{R}\{T_1, \ldots, T_\mu\} \setminus \mathbf{R}$, and let a ranking of $T_1, \ldots, T_\mu$ be given.

The *leader* of P is defined to be the greatest (with respect to the given ranking) derivative θT_i which appears in P, and is denoted by u_P.

If $d = d^{\circ}_{u_P}(P)$ (the degree of P as a polynomial in u_P), then P can be put, in a unique way, into the form

$$P = \sum_{i=0}^{d} I_i u_P^i,$$

where the I_i $(1 \leqslant i \leqslant d)$ are in $\mathbf{R}\{T_1, \ldots, T_\mu\}$ and are free of u_P, $I_d \neq 0$ and every derivative θT_j present in I_i is lower than u_P. The *initial* of $P \in \mathbf{R}\{T_1, \ldots, T_\mu\} \setminus \mathbf{R}$ is defined to be its differential polynomial coefficient I_d in the previous decomposition, and is denoted by I_P. The *separant* of $P \in \mathbf{R}\{T_1, \ldots, T_\mu\} \setminus \mathbf{R}$ is the differential polynomial $\sum_{i=1}^{d} i I_i u_P^{i-1}$ $(= \partial P / \partial u_P)$, and is denoted by S_P. It is clear in our context of characteristic zero that the separant of $P \notin \mathbf{R}$ is never the zero polynomial. The previous objects, leader, initial and separant are, of course, relative to the particular ranking used.

The pre-orders that will be considered on $\mathbf{R}\{T_1, \ldots, T_\mu\}$ are those which extend the total orders that are defined by rankings of $T_1, \ldots, T_\mu$ in the following way. Let a ranking of $T_1, \ldots, T_\mu$ be given. With any differential polynomial P of $\mathbf{R}\{T_1, \ldots, T_\mu\} \setminus \mathbf{R}$ is associated a couple $\omega(P) = (u_P, d^{\circ}_{u_P}(P))$ consisting of its leader and its degree in its leader. We agree that $\omega(P)$ for a P in $\mathbf{R}$ is $(0, 0)$ and that 0 is less than any element of ΘT. The set of couples (u, d), $(u = 0$ or $u \in \Theta T$ and $d \in \mathbb{N})$ is lexicographically ordered in the sense that $(u, d) < (u', d')$ if $u < u'$ or $u = u'$ and $d < d'$. The differential polynomials are ordered according to their associated couples, i.e, we write $P \leqslant Q$, and say that P is of lower rank than or of the same rank as Q if $\omega(P) \leqslant \omega(Q)$. When $\omega(P) = \omega(Q)$, we say that P and Q are of the same rank. The pre-order on $\mathbf{R}\{T_1, \ldots, T_\mu\}$ thus defined is, of course, not an order.

Given a differential polynomial P of $\mathbf{R}\{T_1, \ldots, T_\mu\} \setminus \mathbf{R}$, we may write $\omega(I_P) < \omega(P)$ and $\omega(S_P) < \omega(P)$.

Lemma 2.6 (Ritt [12]). *Any nonempty subset Σ of $\mathbf{R}\{T_1, \ldots, T_\mu\}$ has an element which is of lower rank than or of the same rank as any element of Σ.*

Such an element is in general not unique; we shall nevertheless call it a *least element of Σ*.

This crucial lemma follows immediately from the fact that a ranking defines a well-order on the set ΘT.

2.3. Autoreduced sets. Reduction procedure

Let $\mathbf{R}$ be a nonzero Δ-differential ring and $\mathbf{R}\{T_1, \ldots, T_\mu\}$ a differential polynomial algebra over $\mathbf{R}$, with a given ranking of $T_1, \ldots, T_\mu$.

A differential polynomial $F \in \mathbf{R}\{T_1, \ldots, T_\mu\}$ is said to be *partially reduced with respect to a differential polynomial* $P \in \mathbf{R}\{T_1, \ldots, T_\mu\} \setminus \mathbf{R}$ if F is free of every proper derivative of u_P. We note that if $\delta = 0$, then every $F \in \mathbf{R}\{T_1, \ldots, T_\mu\}$ is partially reduced

with respect to any $P \in \mathbf{R}\{T_1, \ldots, T_\mu\} \setminus \mathbf{R}$. F is said to be *reduced with respect to* P if F is partially reduced with respect to P and either F is free of u_P or $d^\circ_{u_P}(F) < d^\circ_{u_P}(P)$.

F is said to be partially reduced (reduced) with respect to a given subset Σ of $\mathbf{R}\{T_1, \ldots, T_\mu\} \setminus \mathbf{R}$ if F is partially reduced (reduced) with respect to each element of Σ.

A subset Σ of $\mathbf{R}\{T_1, \ldots, T_\mu\} \setminus \mathbf{R}$ is said to be *autoreduced* if each element of Σ is reduced with respect to all the others.

Examples of autoreduced sets are given by sets of single differential polynomials of $\mathbf{R}\{T_1, \ldots, T_\mu\} \setminus \mathbf{R}$. The empty set is an autoreduced set, too.

In an autoreduced set any two elements must have distinct leaders.

Lemma 2.7 (Ritt [12]). *An autoreduced set is necessarily* finite, *and if* $\delta \leqslant 1$, *then its cardinal number cannot exceed* μ.

If there is an infinite autoreduced set $\mathscr{A}$, then the set $u_{\mathscr{A}}$ of the leaders of the elements of $\mathscr{A}$ is infinite since the leaders of two elements of $\mathscr{A}$ must be distinct. It follows that, with respect to the order on ΘT induced by the product order on $\mathbb{N}_\mu^* \times \mathbb{N}^\delta$, we may find in $u_{\mathscr{A}}$, by Lemma 2.4, an increasing sequence of elements which are derivatives of a unique T_i. All the elements of this sequence are proper derivatives of the first one; this is contradictory. The lemma is, thus, proved.

If $\mathscr{A}$ is an autoreduced set, we denote $\prod_{A \in \mathscr{A}} I_A S_A$ by $H_{\mathscr{A}}$ and $\prod_{A \in \mathscr{A}} I_A$ by $I_{\mathscr{A}}$.

Euclidean remainder. Let $\mathbf{R}$ be a ring and $\mathbf{R}[T]$ the polynomial $\mathbf{R}$-algebra in the solely indeterminate T; let $P, Q \in \mathbf{R}[T]$, $Q \neq 0$. We proceed to define what we call the *Euclidean remainder* $P^{\natural}$ *of* P *with respect to* Q, and a corresponding natural integer ι, which is merely a generalization of the notion of remainder when $\mathbf{R}$ is a field. The motivation of this definition will be clear in the sequel. Let I_R and d_R denote the initial and the degree (when $R \neq 0$) of a polynomial $R \in \mathbf{R}[T]$, respectively.

If $P = 0$ or $P \neq 0$ and $d_P < d_Q$, then we let $\iota_0 = 0$ and $P_0 = P$; otherwise, we let $\iota_0 = 1$, $d_0 = d_P - d_Q$, and $P_0 = I_Q P - I_P T^{d_0} Q$. This is the first step of an induction which leads to $P^{\natural}$ and ι.

Let $i \in \mathbb{N}$, and assume d_i, ι_i and P_i to be defined. If $P_i = 0$ or $P_i \neq 0$ and $d_{P_i} < d_Q$, then we let $\iota_{i+1} = \iota_i$ and $P_{i+1} = P_i$; otherwise, we let $\iota_{i+1} = \iota_i + 1$, $d_{i+1} = d_{P_i} - d_Q$, and $P_{i+1} = I_Q P_i - I_{P_i} T^{d_{i+1}} Q$. We have $d_{i+1} < d_i$.

Since the sequence (d_i) of natural integers is strictly decreasing, the above procedure must stop, i.e., there is a least i such that either $P_i = 0$ or $P_i \neq 0$ and $d_{P_i} < d_Q$. By definition, we call $P^{\natural} = P_i$ the *Euclidean remainder of* P *with respect to* Q. It is straightforward to check that, assuming $\iota = \iota_i$, we have

$$I_Q^{\iota} P \equiv P^{\natural} \pmod{(Q)}, \quad \text{with either } P^{\natural} = 0 \text{ or } P^{\natural} \neq 0 \text{ and } d_{P^{\natural}} < d_Q.$$

Remark 2.8. The computation of $P^{\natural}$ and ι involves only the operations (addition and multiplication) of the ring $\mathbf{R}$. If factorization is *constructively performable* in $\mathbf{R}[T]$, then we may slightly improve the above algorithm if I_Q is seen as a factor of I_{P_i}

($I_P = I_{P_i} a$), in which case we rather let ι_{i+1} be ι_i and P_{i+1} be $P_i - aT^{d_{i+1}}Q$. If $\mathbf{R}$ is an integral domain, then we may also perform the classical Euclidean remainder algorithm over the quotient field of $\mathbf{R}$, and then return to polynomials over $\mathbf{R}$ by clearing the denominator of the quotient in an obvious way.

Let $\mathbf{R}\{T_1, \ldots, T_\mu\}$ be a differential polynomial algebra with a given ranking of $T_1, \ldots, T_\mu$, and $\mathscr{A}$ an autoreduced set. Let the elements $A_1, A_2, \ldots, A_\nu$ of $\mathscr{A}$ be increasingly numbered, and let u_j, I_j, S_j and d_j be the leader, initial, separant and degree of A_j $(1 \leqslant j \leqslant \nu)$, respectively.

Partial remainder. We proceed to define the *partial remainder* $F^\dagger$ of any $F \in \mathbf{R}\{T_1, \ldots, T_\mu\}$ with respect to $\mathscr{A}$ and the *corresponding natural integers* σ_j $(1 \leqslant j \leqslant \nu)$.

If F is partially reduced with respect to $\mathscr{A}$ (which is certainly the case if $\delta = 0$), then we let $F_0 = F$ and $\sigma_{j,0} = 0$ $(1 \leqslant j \leqslant \nu)$. Otherwise, $\delta \geqslant 1$, and the set of derivatives θT_l which occur in F and which are proper derivatives of a leader of at least one $A \in \mathscr{A}$ is nonempty and finite. Let v_0 be its greatest element. The set of elements A of $\mathscr{A}$ such that v_0 is a proper derivative of their leaders also has a greatest element A_{j_0}. Let θ_0 be the proper derivative operator such that $v_0 = \theta_0 u_{j_0}$. Regarding F and $\theta_0 A_{j_0}$ as polynomials in v_0, we let F_0 be the Euclidean remainder of F with respect to $\theta_0 A_{j_0}$ and $\sigma_{j_0,0}$ the corresponding integer, and $\sigma_{j,0} = 0$ for all $j \neq j_0$. This is the first step of an induction which leads to the determination of $F^\dagger$ and of the integers σ_j $(1 \leqslant j \leqslant \nu)$.

Let $i \in \mathbb{N}$, and assume $\sigma_{j,i}$ $(1 \leqslant j \leqslant \nu)$, j_i, v_i, and F_i to be defined. If F_i is partially reduced with respect to $\mathscr{A}$, then we let $\sigma_{j,i+1} = \sigma_{j,i}$ $(1 \leqslant j \leqslant \nu)$ and $F_{i+1} = F_i$. Otherwise, $\delta \geqslant 1$, and the set of derivatives θT_l which occur in F_i and which are proper derivatives of a leader of at least one $A \in \mathscr{A}$ is nonempty and finite. Let v_{i+1} be its greatest element. We have $v_{i+1} < v_i$. The set of elements A of $\mathscr{A}$ such that v_{i+1} is a proper derivative of their leaders also has a greatest element $A_{j_{i+1}}$. Let θ_{i+1} be the proper derivative operator such that $v_{i+1} = \theta_{i+1} u_{j_{i+1}}$. Regarding F_i and $\theta_{i+1} A_{j_{i+1}}$ as polynomials in v_{i+1}, we let F_{i+1} be the Euclidean remainder of F_i with respect to $\theta_{i+1} A_{j_{i+1}}$ and $\sigma_{j_{i+1},i+1}$ the corresponding integer, and $\sigma_{j_i,i+1} = \sigma_{j_i,i}, \ldots, \sigma_{j_0,i+1} = \sigma_{j_0,i}$, and $\sigma_{j,i+1} = 0$ for all $j \neq j_{i+1}$, and $j \neq j_i, \ldots$, and $j \neq j_0$.

Since the sequence (v_i) of derivatives of indeterminates is strictly decreasing, the above procedure must stop, i.e., there is a least i such that F_i is partially reduced with respect to $\mathscr{A}$. By definition, we call $F^\dagger = F_i$ the partial remainder of F with respect to $\mathscr{A}$. It is straightforward to check that, assuming $\sigma_j = \sigma_{j,i}$ $(1 \leqslant j \leqslant \nu)$, we have:

(i) $F^\dagger$ is partially reduced with respect to $\mathscr{A}$;

(ii) $\prod_{j=1}^{\nu} S_j^{\sigma_j} F \equiv F^\dagger \pmod{[\mathscr{A}]}$;

(iii) $F^\dagger \leqslant F$.

More precisely, $\prod_{j=1}^{\nu} S_j^{\sigma_j} F - F^\dagger$ is a linear combination over $\mathbf{R}\{T_1, \ldots, T_\mu\}$ of the derivatives θA ($\theta \in \Theta$, $A \in \mathscr{A}$, and $\theta u_A \leqslant u_F$).

We note that the determination of the partial remainder of F with respect to $\mathscr{A}$ and of the corresponding natural integers σ_A ($A \in \mathscr{A}$) involves only the operations (addition, multiplication and derivation) on $\mathbf{R}$.

Simultaneous partial remainders. Let $F_1, F_2, \ldots, F_q$ be elements of $\mathbf{R}\{T_1, \ldots, T_\mu\}$. Let $G_1, G_2, \ldots, G_q$ denote the respective partial remainders of $F_1, F_2, \ldots, F_q$ with respect to $\mathscr{A}$, and let $\sigma_{j,l}$ $(1 \leqslant j \leqslant v,\ 1 \leqslant l \leqslant q)$ denote the corresponding integers. Let $s_j = \max(\sigma_{j,1}, \ldots, \sigma_{j,q})$ $(1 \leqslant j \leqslant v)$ and $F_l^\dagger = \prod_{j=1}^v S_j^{s_j - \sigma_{i,j}} G_i$ $(1 \leqslant l \leqslant q)$. The following properties,

(i) $F_1^\dagger, F_2^\dagger, \ldots, F_q^\dagger$ all are partially reduced with respect to $\mathscr{A}$,

(ii) $\prod_{j=1}^v S_j^{s_j} F_l \equiv F_l^\dagger \pmod{[\mathscr{A}]}$ $(1 \leqslant l \leqslant q)$,

are satisfied; $F_1^\dagger, F_2^\dagger, \ldots, F_q^\dagger$ are called the *simultaneous partial remainders* of F_1, $F_2, \ldots, F_q$ with respect to $\mathscr{A}$.

Remainder. We proceed to define the *remainder* F^* of any $F \in \mathbf{R}\{T_1, \ldots, T_\mu\}$ with respect to $\mathscr{A}$, and the corresponding natural integers ι_j, σ_j $(1 \leqslant j \leqslant v)$.

Let $F^\dagger$ be the partial remainder of F with respect to $\mathscr{A}$, with σ_j $(1 \leqslant j \leqslant v)$ the corresponding integers.

If $F^\dagger$ is reduced with respect to $\mathscr{A}$, then we let $F_0 = F^\dagger$ and $\iota_{j,0} = 0$ $(1 \leqslant j \leqslant v)$. Otherwise, let j_0 be the greatest integer such that $F^\dagger$ is not reduced with respect to A_{j_0}. Let F_0 be the Euclidean remainder of $F^\dagger$ with respect to A_{j_0} (when $F^\dagger$ and A_{j_0} are considered as polynomials in u_{j_0}) and $\iota_{j_0,0}$ the corresponding integer, and $\iota_{j,0} = 0$ for all $j \neq j_0$. This is the first step of an induction which leads to the determination of F^* and of the integers ι_j $(1 \leqslant j \leqslant v)$.

Let $i \in \mathbb{N}$, and assume $\iota_{j,i}$ $(1 \leqslant j \leqslant v)$, j_i, and F_i to be defined. If F_i is reduced with respect to $\mathscr{A}$, then we let $\iota_{j,i+1} = \iota_{j,i}$ $(1 \leqslant j \leqslant v)$ and $F_{i+1} = F_i$. Otherwise, let j_{i+1} be the greatest integer such that F_i is not reduced with respect to $A_{j_{i+1}}$. We note that $j_{i+1} < j_i$. Let F_{i+1} be the Euclidean remainder of F_i with respect to $A_{j_{i+1}}$ (when F_i and $A_{j_{i+1}}$ are considered as polynomials in $u_{j_{i+1}}$) and $\iota_{j_{i+1}, i+1}$ the corresponding integer, and $\iota_{j_i, i+1} = \iota_{j_i, i}, \ldots, \iota_{j_0, i+1} = \iota_{j_0, i}$, and $\iota_{j,i+1} = 0$ for all $j \neq j_{i+1}$, and $j \neq j_i, \ldots$, and $j \neq j_0$.

Since $\mathscr{A}$ is finite, the above procedure must stop, i.e., there is a least i such that F_i is reduced with respect to $\mathscr{A}$. By definition, we call $F^* = F_i$ *the remainder of* F *with respect to* $\mathscr{A}$. It is straightforward to check that, assuming $\iota_j = \iota_{j,i}$ $(1 \leqslant j \leqslant v)$, we have:

(i) F^* is reduced with respect to $\mathscr{A}$;

(ii) $\prod_{j=1}^v I^{\iota_j} S_j^{\sigma_j} F \equiv F^* \pmod{[\mathscr{A}]}$;

(iii) $F^* \leqslant F$.

More precisely, $\prod_{j=1}^v I^{\iota_j} S_j^{\sigma_j} F - F^*$ is a linear combination over $\mathbf{R}\{T_1, \ldots, T_\mu\}$ of the derivatives θA $(\theta \in \Theta,\ A \in \mathscr{A}$, and $\theta u_A \leqslant u_F)$.

Simultaneous remainders. Let $F_1, F_2, \ldots, F_q$ be elements of $\mathbf{R}\{T_1, \ldots, T_\mu\}$. Let $F_1^\dagger$, $F_2^\dagger, \ldots, F_q^\dagger$ be the simultaneous partial remainders of $F_1, F_2, \ldots, F_q$ with respect to $\mathscr{A}$, with s_j $(1 \leqslant j \leqslant v)$ the corresponding integers. If $F_1^\dagger, F_2^\dagger, \ldots, F_q^\dagger$ all are reduced with respect to $\mathscr{A}$, then we let $F_l^0 = F_l^\dagger$ $(1 \leqslant l \leqslant q)$ and $i_j = 0$ $(1 \leqslant j \leqslant v)$. Otherwise, let A_{j_0} be the highest element of $\mathscr{A}$ with respect to which some $F_l^\dagger$ is not reduced. We let P_l be the Euclidean remainders of $F_l^\dagger$ by A_{j_0} (considering $F_l^\dagger$ and A_{j_0} as polynomials in u_{j_0}) and $i_{j_0,0,l}$ $(1 \leqslant l \leqslant q)$ the corresponding integers. Assuming $i_{j,0} = 0$ for all $j \neq j_0$, $i_{j_0,0} = \max(i_{j_0,0,1}, i_{j_0,0,2}, \ldots, i_{j_0,0,q})$, and $F_l^0 = I_{j_0}^{i_{j_0,0} - i_{j_0,0,l}} P_l$ $(1 \leqslant l \leqslant q)$, we have:

$F_1^0, F_2^0, \ldots, F_l^0$ are partially reduced with respect to $\mathscr{A}$, and are reduced with respect to $A_{j_0}, A_{j_0+1}, \ldots, A_v$, and verify that $\prod_{j=1}^{v} I_j^{i_{j,0}} S_j^{s_j} F_l \equiv F_l^0 \pmod{[\mathscr{A}]}$ $(1 \leqslant l \leqslant q)$.

Let $i \in \mathbb{N}$, and assume $i_{j,i}$ $(1 \leqslant j \leqslant v)$, j_i, and F_l^i $(1 \leqslant l \leqslant q)$ to be defined. If F_1^i, F_2^i, $\ldots, F_q^i$ are reduced with respect to $\mathscr{A}$, then we let $F_l^{i+1} = F_l^i$ $(1 \leqslant l \leqslant q)$ and $i_{j,i+1} = i_{j,i}$ $(1 \leqslant j \leqslant v)$. Otherwise, let j_{i+1} be the greatest integer such that one of the F_l^i is not reduced with respect to $A_{j_{i+1}}$. We have $j_{i+1} < j_i$. We let P_l be the Euclidean remainders of the F_l^i by $A_{j_{i+1}}$ (considering F_l^i and $A_{j_{i+1}}$ as polynomials in $u_{j_{i+1}}$) and $i_{j_{i+1},i,l}$ $(1 \leqslant l \leqslant q)$ the corresponding integers, and $i_{j,i+1,l} = 0$ for all $j \neq j_{i+1}$. Assuming $i_{j,i+1} = 0$ for all $j \neq j_{i+1}$, and $j \neq j_i, \ldots$, and $j \neq j_0$, and $i_{j_0,i+1} = i_{j_0,i}, \ldots, i_{j_i,i+1} = i_{j_i,i}$, and $i_{j_{i+1},i+1} = \max(i_{j_{i+1},i+1,1}, i_{j_{i+1},i+1,2}, \ldots, i_{j_{i+1},i+1,q})$, and $F_l^{i+1} = I_{j_{i+1}}^{i_{j_{i+1},i+1} - i_{j_{i+1},i+1,l}} P_l$, we have: $F_1^{i+1}, F_2^{i+1}, \ldots, F_q^{i+1}$ are partially reduced with respect to $\mathscr{A}$, and are reduced with respect to $A_{j_{i+1}}, A_{j_{i+1}+1}, \ldots, A_v$, and verify that $\prod_{j=1}^{v} I_j^{i_{j,i+1}} S_j^{s_j} F_l \equiv F_l^{i+1} \pmod{[\mathscr{A}]}$ $(1 \leqslant l \leqslant q)$.

Since $\mathscr{A}$ is finite, the above procedure must stop, i.e., there is a least i such that $F_1^i, F_2^i, \ldots, F_q^i$ all are reduced with respect to $\mathscr{A}$. By definition, we call $F_1^* = F_1^i$, $F_2^* = F_2^i, \ldots, F_q^* = F_q^i$ the *simultaneous remainders* of $F_1, F_2, \ldots, F_q$ with respect to $\mathscr{A}$. Assuming $i_j = i_{j,i}$ $(1 \leqslant j \leqslant v)$, we have:

(i) $F_1^*, F_2^*, \ldots, F_q^*$ all are reduced with respect to $\mathscr{A}$;

(ii) $\prod_{j=1}^{v} I_j^{i_j} S_j^{s_j} F_l \equiv F_l^* \pmod{[\mathscr{A}]}$ $(1 \leqslant l \leqslant q)$.

2.4. *Coherent autoreduced sets*

If $\mathbf{R}$ is a (nondifferential) ring, $\mathfrak{a}$ an ideal of $\mathbf{R}$, and if $a \in \mathbf{R}$, then $\mathfrak{a} : a^\infty$ denotes the set of $x \in \mathbf{R}$ such that $a^n x \in \mathfrak{a}$ for some $n \in \mathbb{N}$; $\mathfrak{a} : a^\infty$ is an ideal containing $\mathfrak{a}$. $\mathfrak{a} : a^\infty$ is perfect if $\mathfrak{a}$ is such. If $\mathfrak{a}$ is prime and $a \notin \mathfrak{a}$, then $\mathfrak{a} : a^\infty = \mathfrak{a}$.

Let $\mathbf{R}$ be a differential ring.

If $\mathfrak{a}$ is a differential ideal, then $\mathfrak{a} : a^\infty$ is a differential ideal; see [11, Section 1.2, Corollary of Lemma 1] for a proof.

Let $\mathbf{k}$ be a differential field and $\mathbf{k}\{T_1, \ldots, T_\mu\}$ a differential polynomial algebra provided with a ranking of $T_1, \ldots, T_\mu$.

For a given autoreduced set $\mathscr{A}$ of $\mathbf{k}\{T_1, \ldots, T_\mu\}$ and a given derivative of indeterminate v, we denote by $\mathscr{A}_v$ the set of differential polynomials θA $(\theta \in \Theta, A \in \mathscr{A}$, and $\theta u_A < v)$.

An autoreduced set $\mathscr{A}$ is said to be coherent *if, whenever $A, A' \in \mathscr{A}$, and u_A and $u_{A'}$ have a least common derivative $v = \theta_A u_A = \theta_{A'} u_{A'}$, we have $S_{A'} \theta_A A - S_A \theta_{A'} A' \in (\mathscr{A}_v) : H_{\mathscr{A}}^\infty$.*

If $\mathscr{A}$ is a coherent autoreduced set, then for all $A, A' \in \mathscr{A}$ if u_A and $u_{A'}$ have a common derivative $w = \theta u_A = \theta' u_{A'}$, then $S_{A'} \theta A - S_A \theta' A' \in (\mathscr{A}_w) : H_{\mathscr{A}}^\infty$; for a proof see [11, Section IV.9].

If $\delta \leqslant 1$, then every autoreduced set is coherent. An autoreduced set with at most one element is coherent, too.

Lemma 2.9. *An autoreduced set $\mathscr{A}$ is coherent if and only if any element of $[\mathscr{A}] : H_{\mathscr{A}}^\infty$ which is partially reduced with respect to $\mathscr{A}$ is in $(\mathscr{A}) : H_{\mathscr{A}}^\infty$.*

If $\mathscr{A}$ is a coherent autoreduced set, then $[\mathscr{A}]: H_{\mathscr{A}}^{\infty}$ is prime (perfect) if $(\mathscr{A}): H_{\mathscr{A}}^{\infty}$ is prime (perfect).

The first part of this lemma is due to Rosenfeld [13]. See [11, Section III.8, Lemmas 5 and 6] for a proof. For $\delta = 0$ this lemma is not really informative. Its main interest, as indicated by its authors, is in bridging the gap between differential polynomial algebras and the underlying polynomial algebras.

An easy consequence is the following lemma.

Lemma 2.10. *If $\mathscr{A}$ is a coherent autoreduced set, then any element of $\{\mathscr{A}\}: H_{\mathscr{A}}^{\infty}$ which is partially reduced with respect to $\mathscr{A}$ is in $\langle \mathscr{A} \rangle : H_{\mathscr{A}}^{\infty}$.*

If $\mathscr{A}$ is a coherent autoreduced set, then $\{\mathscr{A}\}: H_{\mathscr{A}}^{\infty}$ is prime if and only if $\langle \mathscr{A} \rangle : H_{\mathscr{A}}^{\infty}$ is so.

2.5. Characteristic sets

Let $\mathbf{R}\{T_1, \ldots, T_\mu\}$ be a differential polynomial algebra with a given ranking of $T_1, \ldots, T_\mu$.

Let $\mathscr{A}$ and $\mathscr{A}'$ be two autoreduced sets with elements $A_1, A_2, \ldots, A_\nu$ and $A'_1, A'_2, \ldots, A'_{\nu'}$, respectively, numbered in increasing order. We define a pre-order on the set of autoreduced sets of $\mathbf{R}\{T_1, \ldots, T_\mu\}$ by assuming that $\mathscr{A} < \mathscr{A}'$ (we then say that $\mathscr{A}$ is of lower rank than $\mathscr{A}'$, or that $\mathscr{A}$ is lower than $\mathscr{A}'$) if one of the following two conditions is satisfied:

(i) There is some natural integer j such that $1 \leqslant j \leqslant \min(\nu, \nu')$, and A_i and A'_i $(1 \leqslant i < j)$ are of the same rank and $A_j < A'_j$;

(ii) $\nu > \nu'$, and A_i and A'_i $(1 \leqslant i \leqslant \nu')$ are of the same rank.

We say that $\mathscr{A}$ and $\mathscr{A}'$ are of the same rank if $\nu = \nu'$ and if A_i and A'_i $(1 \leqslant i \leqslant \nu)$ are of the same rank. If $\mathscr{A} < \mathscr{A}'$ or $\mathscr{A}$ and $\mathscr{A}'$ are of the same rank, then we write $\mathscr{A} \leqslant \mathscr{A}'$.

The relation $\leqslant$ thus defined clearly is a pre-order. Any two autoreduced sets may be compared, i.e., one of the relations $\mathscr{A} \leqslant \mathscr{A}'$, $\mathscr{A}' \leqslant \mathscr{A}$ holds. Moreover, we have the following lemma.

Lemma 2.11 (Ritt [12]). *A nonempty set $\mathscr{E}$ of autoreduced sets contains a* least element, *i.e., an element $\mathscr{A}$ such that $\mathscr{A} \leqslant \mathscr{A}'$ $(\mathscr{A}' \in \mathscr{E})$.*

The elements of an autoreduced set are supposed to be numbered in increasing order. Let $\mathscr{E}_0 = \mathscr{E}$, and define $\mathscr{E}_i$ $(i \in \mathbb{N}, i > 0)$ to be the set of elements $\mathscr{A}$ of $\mathscr{E}_{i-1}$ such that $\mathscr{A}$ is with cardinal number greater than or equal to i, and such that A_i is a least element of the set of the ith differential polynomials of the elements of $\mathscr{E}_{i-1}$. This decreasing sequence of subsets of $\mathscr{E}$ must terminate by $\mathscr{E}_i = \emptyset$ for some i since, otherwise, the leaders v_i of the ith differential polynomials of the elements of $\mathscr{E}_i$ would be a sequence of derivatives of indeterminates which are not proper derivatives of one of them; this would contradict Lemma 2.4. Since $\mathscr{E}_0 = \mathscr{E}$ is nonempty, there exists an

$i \in \mathbb{N}$ such that $\mathscr{E}_{i+1} = \emptyset$ and any element of $\mathscr{E}_i$ is a least element of $\mathscr{E}$. This proves the lemma. This proof is due to Kolchin [11].

Remark 2.12. If a differential polynomial $P \in \mathbf{R}\{T_1, \ldots, T_\mu\} \setminus \mathbf{R}$ is reduced with respect to an autoreduced set $\mathscr{A}$, then P and the elements A of $\mathscr{A}$ which are reduced with respect to P form an autoreduced set which is lower than $\mathscr{A}$. It results from this that an autoreduced set $\mathscr{A}$ of a family $\mathscr{P}$ of differential polynomials (i.e., an autoreduced set made up with elements of $\mathscr{P}$) is a minimal element of the set of autoreduced sets of $\mathscr{P}$ if and only if $\mathscr{P}$ does not contain any element of $\mathbf{R}\{T_1, \ldots, T_\mu\} \setminus \mathbf{R}$ which is reduced with respect to $\mathscr{A}$.

Let $\mathfrak{a}$ be a differential ideal of $\mathbf{R}\{T_1, \ldots, T_\mu\}$ and $\mathscr{A}$ an autoreduced set with elements in $\mathfrak{a}$.

If $\delta \geqslant 1$, and $\mathscr{A}$ is a least element of the set of autoreduced sets of $\mathfrak{a}$, then for any $A \in \mathscr{A}$,

$$S_A \notin \mathfrak{a} \Rightarrow I_A \notin \mathfrak{a}.$$

Indeed, if A is in $\mathscr{A}$, and if $I_A \in \mathfrak{a}$, then $A - I_A u_A^d \in \mathfrak{a}$, where $d = d^\circ_{u_A}(A)$ is such that $d \geqslant 1$. Since $A - I_A u_A^d$ is reduced with respect to $\mathscr{A}$, it results from the minimality of $\mathscr{A}$ that $A - I_A u_A^d \in \mathbf{R}$. Now $0 = \partial(A - I_A u_A^d)/\partial u_A = S_A - d I_A u_A^{d-1} \in \mathfrak{a}$; hence, $S_A \in \mathfrak{a}$. This proves the assertion.

It follows that if $\mathfrak{a}$ is a *proper* differential ideal of $\mathbf{R}\{T_1, \ldots, T_\mu\}$, and if $\mathscr{A}$ is a minimal autoreduced set of $\mathfrak{a}$, then the separant of an element of $\mathscr{A}$ cannot be in $\mathfrak{a}$ if it is not a nonzero noninvertible element of $\mathbf{R}$. (This assertion depends on the assumption that the characteristic is zero.) Consequently, *if $\mathbf{R}$ is a differential field, then the separant of an element of a minimal autoreduced set of a proper differential ideal is not is this ideal.*

A characteristic set of a differential ideal $\mathfrak{a}$ of $\mathbf{R}\{T_1, \ldots, T_\mu\}$ is defined to be a minimal element of the set of autoreduced sets $\mathscr{A}$ of $\mathfrak{a}$ such that $I_A \notin \mathfrak{a}$ and $S_A \notin \mathfrak{a}$ $(A \in \mathscr{A})$.

It follows from this definition and what precedes it that *an autoreduced set $\mathscr{A}$ of a differential ideal $\mathfrak{a}$ is a characteristic set of $\mathfrak{a}$ if and only if $\mathfrak{a} \setminus \mathbf{R}$ contains no differential polynomial P reduced with respect to $\mathscr{A}$ and such that $I_A \notin \mathfrak{a}$ and $S_A \notin \mathfrak{a}$.*

When $\delta \geqslant 1$, the empty set is the characteristic set of a differential ideal $\mathfrak{a}$ if and only if the separant of any element of $\mathfrak{a} \setminus \mathbf{R}$ is in $\mathfrak{a}$. For $\delta = 0$ the empty set is the characteristic set of an ideal $\mathfrak{a}$ if and only if the initial of any element of $\mathfrak{a} \setminus \mathbf{R}$ is in $\mathfrak{a}$.

The zero ideal and the unit ideal are with characteristic sets the empty set. Conversely, if $\mathbf{R}$ is a differential field $\mathbf{k}$, then any differential ideal $\mathfrak{a}$ of $\mathbf{k}\{T_1, \ldots, T_\mu\}$ is with characteristic set the empty set only if $\mathfrak{a}$ is the zero or unit ideal.

Lemma 2.13 (Rosenfeld [13]). *Let $\mathbf{k}$ be a differential field, $\mathbf{k}\{T_1, \ldots, T_\mu\}$ a differential polynomial algebra with a given ranking of $T_1, \ldots, T_\mu$, and let $\mathfrak{a}$ be a differential ideal of $\mathbf{k}\{T_1, \ldots, T_\mu\}$, with $\mathscr{A}$ an autoreduced subset of $\mathfrak{a}$.*

$\mathfrak{a}$ is a prime differential ideal with characteristic set $\mathscr{A}$ if and only if $\mathfrak{a}=[\mathscr{A}]:H_{\mathscr{A}}^{\infty}$, $\mathscr{A}$ is coherent, and $(\mathscr{A}):H_{\mathscr{A}}^{\infty}$ is prime and does not contain a nonzero element reduced with respect to $\mathscr{A}$.

For a proof see [11, Section IV.9].

A characteristic set of a differential ideal of $\mathbf{k}\{T_1,\ldots,T_\mu\}$ is a coherent autoreduced set.

Lemma 2.14 (Rosenfeld [13]). *A coherent autoreduced set $\mathscr{A}$ is a characteristic set of $\{\mathscr{A}\}:H_{\mathscr{A}}^{\infty}$ if and only if it is a characteristic set of $\langle\mathscr{A}\rangle:H_{\mathscr{A}}^{\infty}$.*

A coherent autoreduced set $\mathscr{A}$ is a characteristic set of $[\mathscr{A}]:H_{\mathscr{A}}^{\infty}$ if and only if it is a characteristic set of $(\mathscr{A}):H_{\mathscr{A}}^{\infty}$.

An autoreduced set $\mathscr{A}$ of $\mathbf{k}\{T_1,\ldots,T_\mu\}$ is said to be *orthonomic* if its elements are of degree 1 in their leaders.

This definition is somewhat more general than that in [12, Section VIII.10]. The notion of orthonomic systems goes back to Riquier. We call a *polynomial* orthonomic autoreduced set an orthonomic autoreduced set whose elements are with initials 1.

Lemma 2.15. *If $\mathscr{A}$ is a coherent orthonomic autoreduced set of $\mathbf{k}\{T_1,\ldots,T_\mu\}$, then there is no nonzero element of $[\mathscr{A}]:I_{\mathscr{A}}^{\infty}$ that is reduced with respect to $\mathscr{A}$, and $[\mathscr{A}]:I_{\mathscr{A}}^{\infty}$ is prime with characteristic set $\mathscr{A}$.*

Let $A_1<A_2<\cdots<A_\nu$ be the elements of $\mathscr{A}$. Assume that there is a $P\in[\mathscr{A}]:I_{\mathscr{A}}^{\infty}$, $P\neq 0$, and that P is reduced with respect to $\mathscr{A}$. By Lemma 2.9, $P\in(\mathscr{A}):I_{\mathscr{A}}^{\infty}$. We may thus write

$$I_{\mathscr{A}}^{n}P=\sum_{i=1}^{s}P_iA_i+P_0, \qquad (*)$$

for some $n\in\mathbb{N}$, and $P_0=0$. One of the P_i's must be nonzero, and we may assume that s is the least integer such that there exists an $n\in\mathbb{N}$, and a P_0 is free of the leader of A_s, and $P_s\neq 0$. Writing every P_i as a polynomial in u_{A_s}, then, by a degree argument (note that $I_{\mathscr{A}}^{n}P$ is free of u_{A_s}), we see that the same equation $(*)$ may be written with $s-1$ in place of s. This is contradictory and proves the first part of the lemma. Now, let P and Q be two elements of $\mathbf{k}\{T_1,\ldots,T_\mu\}$ with product in $[\mathscr{A}]:I_{\mathscr{A}}^{\infty}$. Let P^* and Q^* be the respective remainders of P and Q with respect to $\mathscr{A}$. The product P^*Q^* is in $[\mathscr{A}]:I_{\mathscr{A}}^{\infty}$ and is reduced with respect to $\mathscr{A}$; then, by the first part, $P^*Q^*=0$. Hence, P or Q is in $[\mathscr{A}]:I_{\mathscr{A}}^{\infty}$. This proves the primality of $[\mathscr{A}]:I_{\mathscr{A}}^{\infty}$, and the lemma, too. A version of this lemma, valid for differential **R**-algebras of arbitrary characteristic is given in [11, Section III.8, Exercise 1].

2.5.1. The Ritt algorithm

We proceed to give more insight in the construction (which we name after Ritt) of characteristic sets. For any finite family Σ of differential polynomials $P_1,P_2,\ldots,P_s$ of

$\mathbf{k}\{T_1, \ldots, T_\mu\}$, we first give a way to compute the minimal autoreduced set $\mathbf{A}(\Sigma)$ of Σ. If Σ contains a nonzero element of the ground field or if all its elements are zero, then we agree that $\mathbf{A}(\Sigma)$ is the empty set. Otherwise, we assume, as we may, that the P_i's are numbered in increasing order, and we let $\mathbf{A}(\Sigma)$ consist of P_1. For $i=2$ to s if P_i is reduced with respect to $\mathbf{A}(\Sigma)$, then we remove from $\mathbf{A}(\Sigma)$ its elements which are not reduced with respect to P_i, and we add P_i to $\mathbf{A}(\Sigma)$; it is easy to check that the new $\mathbf{A}(\Sigma)$ is lower than the previous one (see Remark 2.12). If P_i is not reduced with respect to $\mathbf{A}(\Sigma)$, then we skip it. At the end ($i=s$) of this procedure we have at hand the minimal autoreduced set $\mathbf{A}(\Sigma)$ of Σ since the latter does no more contain any element which is reduced with respect to $\mathbf{A}(\Sigma)$ and which is not in $\mathbf{k}$.

Now let Σ_0 be Σ, and $\mathbf{A}(\Sigma_0)$ be the minimal autoreduced set of Σ_0.

Assume Σ_i, and $\mathbf{A}(\Sigma_i)$ constructed. Let Σ_i' be the union of the complement of $\mathbf{A}(\Sigma_i)$ in Σ_i, and the subset of $[\Sigma_i]$ consisting of the differential polynomials $S_{A'}\theta A - S_A \theta' A'$ for all A, A' in $\mathbf{A}(\Sigma_i)$ having a least common derivative w of their leaders: $w=\theta u_A = \theta' u_{A'}$. Let Σ_i^* be the set of remainders with respect to $\mathbf{A}(\Sigma_i)$ of the elements of Σ_i'. Let $\Sigma_{i+1}=\Sigma_i \cup \Sigma_i^*$. Either Σ_i^* consists solely of the zero polynomial or else $\mathbf{A}(\Sigma_{i+1}) < \mathbf{A}(\Sigma_i)$.

Clearly, there exists an i such that Σ_i^* consists solely of the zero polynomial since, by Lemma 2.11, there does not exist a strictly decreasing sequence of autoreduced sets in $\mathbf{k}\{T_1, \ldots, T_\mu\}$. We denote $\mathbf{A}(\Sigma_i)$ by $\mathbf{C}(\Sigma)$.

It is clear that $\mathbf{C}(\Sigma)$ is a coherent autoreduced set, that $[\Sigma] \subseteq [\mathbf{C}(\Sigma)] : H_{\mathscr{A}}^\infty$, and that if $\mathbf{C}(\Sigma)=\emptyset$, then $\emptyset$ is the characteristic set of $[\Sigma]=\{\Sigma\}$ ($=\mathbf{0}$ or $\mathbf{k}\{T_1, \ldots, T_\mu\}$).

We know, by Lemma 2.13, that if $(\mathbf{C}(\Sigma)) : H_{\mathscr{A}}^\infty$ is prime and does not contain any nonzero element reduced with respect to $\mathbf{C}(\Sigma)$, then $[\mathbf{C}(\Sigma)] : H_{\mathscr{A}}^\infty$ is prime, $[\Sigma]=[\mathbf{C}(\Sigma)] : H_{\mathscr{A}}^\infty$, and $\mathbf{C}(\Sigma)$ is a characteristic set of $[\Sigma]$ ($=\{\Sigma\}$). The following lemma is thus an easy consequence of Lemma 2.15.

Lemma 2.16. *If $\mathbf{C}(\Sigma)$ is orthonomic, then it is a characteristic set of $[\Sigma]$, and $[\Sigma]$ is prime.*

2.5.2. Systems of parametric indeterminates

Ritt [12] introduced the concept of parametric indeterminates, which we shall use in the following. We recall its definition and basic properties. Let $\mathfrak{p}$ be a nonzero prime differential ideal of $\mathbf{k}\{T_1, \ldots, T_\mu\}$. A subset V of $T_1, \ldots, T_\mu$ is called a *system (or set) of parametric indeterminates of* $\mathfrak{p}$ if $\mathfrak{p}$ does not contain any element which involves derivatives of the elements of V without involving derivatives of the T_i's not in V, and if, for each T_i not in V, there is an element of $\mathfrak{p}$ which involves only derivatives of T_i and some elements of V.

Let V be a system of parametric indeterminates of $\mathfrak{p}$, and let $\mathscr{A}$ be a characteristic set of $\mathfrak{p}$ such that V is the subset of $T_1, \ldots, T_\mu$ whose elements are those without derivatives involved as leaders of any element of $\mathscr{A}$. We say that $\mathscr{A}$ *defines* V. Each T_i not in V has a least derivative which is the leader of some element A_i of $\mathscr{A}$; we say that A_i *introduces* T_i.

Recall that the differential dimension diff dim(p) of p is defined to be the differential transcendence degree of $\mathbf{k}\{T_1, \ldots, T_\mu\}/\mathfrak{p} = \mathbf{k}\{\tau_1, \ldots, \tau_\mu\}$ over $\mathbf{k}$, where τ_i is the residue class of T_i mod p. We have the following lemma.

Lemma 2.17. *$T_{i_1}, T_{i_2}, \ldots, T_{i_m}$ form a system of parametric indeterminates of* p *if and only if $\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_m}$ form a differential transcendence basis of $\mathbf{k}\{\tau_1, \ldots, \tau_\mu\}$ over* $\mathbf{k}$. *The number of elements of any set of parametric indeterminates of* p *is, thus, equal to* diff dim(p). *Any characteristic set of* p defines *a system of parametric indeterminates of* p. *Conversely, if $T_{i_1}, T_{i_2}, \ldots, T_{i_m}$ form a system V of parametric indeterminates of* p, *then V is* defined *by any characteristic set of* p *with respect to any ranking such that the derivatives of $T_{i_1}, T_{i_2}, \ldots, T_{i_m}$ all are lower than the T_i's not in V.*

The proof is straightforward. See also Lemma 4.2.

3. Differential dimension polynomial

The concept of Hilbert polynomial is known in algebraic geometry as a measure of the size of an algebraic variety. It has been discovered by Kolchin that differential-algebraic geometry is provided with such a polynomial, where its role is actually more crucial. Recall that the differential dimension of an irreducible system is the differential transcendence degree of the differential algebra associated with that system. Kolchin [10, 11] showed that this measure of size of a system is not sufficiently fine. The differential dimension polynomial is a better candidate, and is a right one [16]; see also [9]. A differential dimension polynomial is a polynomial in one indeterminate with rational coefficients, carrying with it much information on the invariants of an irreducible system.

3.1. Numerical polynomials

By a *numerical polynomial* we mean an element χ of the polynomial algebra $\mathbb{Q}[\xi]$ in one indeterminate with coefficients in the field $\mathbb{Q}$ of rational numbers such that $\chi(r) \in \mathbb{N}$ for sufficiently large $r \in \mathbb{N}$. The set of numerical polynomials is totally ordered according to: $\chi < \chi'$ if $\chi(r) < \chi'(r)$ for sufficiently large $r \in \mathbb{N}$. Denoting $\xi(\xi-1)\cdots(\xi-i+1)/i!$ by $\binom{\xi}{i}$, we have: χ is a numerical polynomial if and only if χ may be written in the form $\sum_{i=0}^{s} a_i \binom{\xi+i}{i}$ for some $s \in \mathbb{N}$, and a_i in the ring $\mathbb{Z}$ of rational integers. If $\chi = \sum_{i=0}^{s} a_i \binom{\xi+i}{i}$ and $\chi' = \sum_{i=0}^{s} b_i \binom{\xi+i}{i}$, then $\chi < \chi'$ if and only if $(a_s, \ldots, a_0) < (b_s, \ldots, b_0)$ lexicographically.

Given a finite subset $\mathbf{E}$ of $\mathbb{N}^\delta$, Kolchin [11] and then Sit [15, 16] showed that we may effectively compute a numerical polynomial $\chi_{\mathbf{E}}$ verifying the following:

(i) *For every sufficiently large $r \in \mathbb{N}$ the number of elements $(r_1, \ldots, r_\delta)$ of $\mathbb{N}^\delta$ which are not greater than (with respect to the product order) or equal to any element of* $\mathbf{E}$ *and which verify that $r_1 + \cdots + r_\delta \leqslant r$ is equal to $\chi_{\mathbf{E}}(r)$.*

(ii) $d^\circ(\chi_{\mathbf{E}}) \leqslant \delta$; *equality occurs if and only if* $\mathbf{E}$ *is empty, in which case* $\chi_{\mathbf{E}} = \binom{\xi+\delta}{\delta}$.
(iii) $\chi_{\mathbf{E}} = 0$ *if and only if* $(0, \ldots, 0) \in \mathbf{E}$.

3.2. Differential dimension polynomial

Let $\mathbf{K}$ be a finite-type differential field extension of $\mathbf{k}$, $\tau = (\tau_1, \ldots, \tau_\mu)$ a set of generators of $\mathbf{K}$ over $\mathbf{k}$, i.e., $\mathbf{K} = \mathbf{k}\langle \tau_1, \ldots, \tau_\mu \rangle$, $\mathfrak{p}$ the defining differential ideal of $\mathbf{K}$ over $\mathbf{k}$, i.e., $\mathfrak{p}$ is the set of differential polynomials in $\mathbf{k}\{T_1, \ldots, T_\mu\}$ that vanish at τ and is such that $\mathbf{K}$ is the quotient field of $\mathbf{k}\{T_1, \ldots, T_\mu\}/\mathfrak{p}$, and $\mathscr{A}$ a characteristic set of $\mathfrak{p}$ with respect to some *orderly* ranking of $T_1, \ldots, T_\mu$. For each i, $1 \leqslant i \leqslant \mu$, let $\mathbf{E}_i$ be the subset of $\mathbb{N}^\delta$ consisting of the elements $(r_1, \ldots, r_\delta)$ such that $\partial^{r_1} \cdots \partial^{r_\delta} T_i$ is the leader of some element of $\mathscr{A}$. The numerical polynomial $\chi_{\tau/\mathbf{k}} = \chi_{\mathbf{E}_1} + \cdots + \chi_{\mathbf{E}_\mu}$ verifies the following:

(i) *For every sufficiently large* $r \in \mathbb{N}$ *the (nondifferential) transcendence degree over* $\mathbf{k}$ *of* $\mathbf{k}((\theta\tau_i)_{\theta \in \Theta(r),\, 1 \leqslant i \leqslant \mu})$ *is equal to* $\chi_{\tau/\mathbf{k}}(r)$.
(ii) $d^\circ(\chi_{\tau/\mathbf{k}}) \leqslant \delta$.
(iii) *If we write* $\chi_{\tau/\mathbf{k}} = \sum_{i=0}^{\delta} a_i \binom{\xi+i}{i}$, *then* a_δ *is equal to the differential transcendence degree of* $\mathbf{k}\langle \tau_1, \ldots, \tau_\mu \rangle$ *over* $\mathbf{k}$.

$\chi_{\tau/\mathbf{k}}$ depends on the choice of τ, and, thus, is not an invariant of the differential field extension $\mathbf{K}$ of $\mathbf{k}$. Sit [15] showed that the set of numerical polynomials is actually well-ordered relative to the previously defined order. Sit [16] takes the least element of the set of numerical polynomials $\chi_{\tau/\mathbf{k}}$, where τ runs over the generators of the finite-type differential field extension $\mathbf{K}$ of $\mathbf{k}$; and then obtains a numerical polynomial, $\chi_{\mathbf{K}/\mathbf{k}}$, which does not depend on particular generators of $\mathbf{K}$ over $\mathbf{k}$. However, in general $\chi_{\mathbf{K}/\mathbf{k}} = \chi_{\mathbf{K}'/\mathbf{k}}$ does not imply that $\mathbf{K}$ and $\mathbf{K}'$ are isomorphic differential field $\mathbf{k}$-extensions; and we do not know how to compute $\chi_{\mathbf{K}/\mathbf{k}}$.

4. Some basic decision problems

4.1. Prime component decomposition

The state of affairs of this problem is rather poor. The problem is solvable provided that the same problem is solvable for polynomial algebras.

4.2. Membership problem

The membership problem is trivially solved if we can decompose any differential ideal into prime components and if we can find a characteristic set of any prime differential ideal.

Lemma 4.1 (Ritt [12]). *Let* $\mathbf{k}$ *be a differential field, and* $\mathbf{k}\{T_1, \ldots, T_\mu\}$ *a differential polynomial algebra provided with a ranking of* $T_1, \ldots, T_\mu$. *If* $\mathfrak{a}$ *is a prime differential ideal of* $\mathbf{k}\{T_1, \ldots, T_\mu\}$ *with characteristic set* $\mathscr{A}$, *then for any differential polynomial* P, $P \in \mathfrak{a}$ *if*

and only if the remainder of P *with respect to* $\mathscr{A}$ *is* 0. *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are two prime differential ideals with characteristic sets* $\mathscr{A}$ *and* $\mathscr{B}$, *respectively, then* $\mathfrak{a}=\mathfrak{b}$ *if and only if* $\mathscr{A}\subseteq\mathfrak{b}$, $S_{\mathscr{A}}\notin\mathfrak{b}$, *and* $S_{\mathscr{B}}\notin\mathfrak{a}$, *where* $S_{\mathscr{A}}$ *(respectively,* $S_{\mathscr{B}}$*) denotes the product of the separants of the elements of* $\mathscr{A}$ *(respectively,* $\mathscr{B}$*).*

The proof of this result is straightforward.

4.2. Elimination theory

Elimination theory is one of the key tools in algebra. Its role in differential algebra was stressed enough by Ritt [12] and by the outstanding paper by Seidenberg [14]. Application of this theory to system theory was first attempted in [1, 2]; see also [3] for a recent related result. One of the basic questions dealing with elimination theory consists in deriving the equations of the projection of a differential-algebraic set along some of the coordinates. We know that this projection is not closed. The second question addressed by elimination theory is the computation of the equations of the closures of the above projections of differential-algebraic sets. This last question is not addressed in [14]. The following lemma is a rather standard straightforward solution based on the construction of characteristic sets.

Lemma 4.2. *Let* $\mathfrak{a}$ *be a differential ideal of* $\mathbf{k}\{T_1,\ldots,T_\mu\}$. *Let* V *be a subset of* $T_1,\ldots,T_\mu$, $\mathbf{k}\{V\}$ *the differential polynomial algebra in the elements of* V, *and let a ranking be fixed such that the derivatives of the elements of* V *all are lower than the* T_i*'s not in* V. *If* $\mathscr{A}$ *is a characteristic set of* $\mathfrak{p}$, *then* $\mathscr{A}\cap\mathbf{k}\{V\}$ *is one for* $\mathfrak{p}\cap\mathbf{k}\{V\}$.

5. Applications to system theory

We provide some examples of applications of the above differential algebraic decision methods. We could not be exhaustive. More applications should be expected in further communications.

5.1. Computation of invariants

Let there be an irreducible system $\mathscr{X}$ defined by a set of algebraic differential equations, $P_1(\tau_1,\tau_2,\ldots,\tau_\mu)=0$, $P_2(\tau_1,\tau_2,\ldots,\tau_\mu)=0,\ldots,P_s(\tau_1,\tau_2,\ldots,\tau_\mu)=0$, with coefficients in a differential field $\mathbf{k}$. The variables $\tau_1,\tau_2,\ldots,\tau_\mu$ of $\mathscr{X}$ are usually partitioned into inputs, outputs, etc. Assume that such a partition is done and that the variables are renamed according to our notations. The *number of independent inputs* that we denote by m is an invariant of the system and is defined to be the *differential dimension* or the *differential transcendence degree* of $\mathbf{k}\langle\mathscr{X}\rangle=\mathbf{k}\langle\tau_1,\tau_2,\ldots,\tau_\mu\rangle$ over $\mathbf{k}$. m is independent of the partition of the variables, and may be readily obtained from any characteristic set of the defining differential ideal $\mathbf{I}(\mathscr{X})=\{P_1,P_2,\ldots,P_s\}$

of $\mathscr{X}$ over $\mathbf{k}$ merely by inspecting this characteristic set. See Lemma 2.17 for more details.

Moreover, we already reported (Section 3) that the differential dimension polynomial is more informative than the simple differential dimension. See Section 3 for more details. Further studies on this numerical polynomial should bring out more insight into the structure of a system merely by inspecting this polynomial.

5.2. Realization

We refer to [7] for a differential-algebraic theory of realization. The main point of this theory is the fact that realizations of a given system are not necessarily in the classical form introduced in system theory by Kalman. Input derivatives as well as implicit algebraic differential equations should be included in the state equations. In deriving such realizations Fliess uses the primitive-element theorem. A constructive realization theory may be derived from characteristic set techniques. We have the following theorem.

Theorem 5.1. *Let $\mathscr{X}$ be an ordinary irreducible system given by its external behavior $\mathbf{k}\langle u, y\rangle$. Let U and Y be ranked such that any derivative of U is less than any derivative of Y, and let $\mathscr{A}$ be a characteristic set of the defining differential ideal of $\mathbf{k}\langle u, y\rangle$. Let the elements of $\mathscr{A}$ be $A_1 < A_2 < \cdots < A_p$, with A_i introducing Y_i. A minimal realization*

$$
\begin{cases}
\dot{x}_1 = x_2, \\
\dot{x}_2 = x_3, \\
\vdots \\
\dot{x}_{n_1 - 1} = x_{n_1}, \\
A_1(\dot{x}_{n_1}, x_1, \ldots, x_{n_1}) = 0, \\
\dot{x}_{n_1 + 1} = x_{n_1 + 2}, \\
\vdots \\
\dot{x}_{n_1 + n_2 - 1} = x_{n_1 + n_2}, \\
A_2(\dot{x}_{n_1 + n_2}, x_1, \ldots, x_{n_1 + n_2}) = 0, \\
\vdots \\
\dot{x}_{n_1 + \cdots + n_{p-1} + 1} = x_{n_1 + \cdots + n_{p-1} + 2}, \\
\vdots \\
\dot{x}_{n_1 + \cdots + n_p - 1} = x_{n_1 + \cdots + n_p}, \\
A_p(\dot{x}_{n_1 + \cdots + n_p}, x_1, \ldots, x_{n_1 + \cdots + n_p}) = 0
\end{cases}
$$

of $\mathscr{X}$ is obtained by assuming

$$\begin{cases} x_1 = y_1, \\ x_2 = \dot{y}_1, \\ \vdots \\ x_{n_1} = y_1^{(n_1-1)}, \\ \vdots \\ x_{n_1+\cdots+n_{p-1}+1} = y_p, \\ x_{n_1+\cdots+n_{p-1}+2} = \dot{y}_p, \\ \vdots \\ x_{n_1+\cdots+n_p} = y_p^{(n_p-1)}. \end{cases}$$

We stress the well-known fact that such a realization procedure may be unsuitable when one looks for state equations where input derivatives appear with lowest possible orders. The problem of finding realizations with least derivatives of the input has been characterized by Freedman and Willems [17] from a *local* point of view. Further studies using techniques from differential algebra will follow this paper, giving a characterization of systems which are *globally* realizable.

5.2.1. Irreducibility of state space systems

The irreducibility of systems described by

$$\mathscr{X} \begin{cases} \dot{x}_i = \dfrac{p_i(x,u)}{q_i(x,u)}, & 1 \leqslant i \leqslant n, \\ y_j = \dfrac{f_j(x,u)}{g_j(x,u)}, & 1 \leqslant j \leqslant p \end{cases}$$

is often referred to in the literature. By means of characteristic-set techniques, we provide the following justification of such an assumption. We first have to put the problem in terms of our general setting. Assuming

$$P_i(U, Y, X) = q_i(U, X) X_i^{(1)} - p_i(U, X) \quad (1 \leqslant i \leqslant n),$$

$$P_{n+i}(U, Y, X) = g_i(U, X) Y_i - f_i(X) \quad (1 \leqslant i \leqslant p),$$

where $\mathscr{X}$ is, by definition, the locally closed subset consisting of the (u, y, x) which annul all the P_i's without annulling any of the q_i's and the g_i's. Let a ranking of U, Y, X be fixed such that any derivative of $U_1, U_2, \ldots, U_m$ is lower than $X_1, X_2, \ldots, X_n$ which, in turn, are lower than $Y_1, Y_2, \ldots, Y_p$. Then the set $\mathscr{A}$ consisting of $P_1, \ldots, P_{n+p}$ is

readily a coherent orthonomic autoreduced set. By Lemma 2.15, $\mathfrak{p}=[\mathscr{A}]:I_{\mathscr{A}}^{\infty}$ is a prime differential ideal with characteristic set $\mathscr{A}$ (where $I_{\mathscr{A}}=\prod_{1\leqslant i\leqslant n} q_i \prod_{1\leqslant j\leqslant p} g_j$). The points (u, y, x) of $\mathscr{X}$ are easily seen as annulling each $P\in\mathfrak{p}$. Conversely, if (u, y, x) annuls each $P\in\mathfrak{p}$ without annulling $I_{\mathscr{A}}$, then (u, y, x) is a point of $\mathscr{X}$. This shows that $\mathscr{X}$ is the intersection of the differential closed set defined by $\mathfrak{p}$, and the differential open set defined by $I_{\mathscr{A}}\neq 0$. The adherence of $\mathscr{X}$ is clearly the differential closed set defined by $\mathfrak{p}$. Hence, $\mathscr{X}$ is irreducible. We have just proved the following lemma (compare with Moog et al. [18]).

Lemma 5.2. *$\mathscr{X}$ is irreducible if the p_i's, q_i's, f_i's and g_i's are differential polynomials of order 0 in the x_i's. (Notice that input derivatives may be present in the expressions of the p_i's, q_i's, f_i's and g_i's.)*

5.3. Observability theory

We refer to [4, 5] for an algebraic theory of observability. We recall that the observability of an irreducible system $\mathscr{X}$ (with $\mathbf{k}\langle\mathscr{X}\rangle=\mathbf{k}\langle u, y, z\rangle$, $u=(u_1, u_2, \ldots, u_m)$, $y=(y_1, y_2, \ldots, y_p)$, $z=(z_1, z_2, \ldots, z_n)$) means the algebraicity of z over $\mathbf{k}\langle u, y\rangle$. We denote the degree of z_i over $\mathbf{k}\langle u, y\rangle$ (which is defined to be the degree of the minimal polynomial of z_i over $\mathbf{k}\langle u, y\rangle$ if z_i is algebraic over $\mathbf{k}\langle u, y\rangle$, or 0 otherwise) by $d^{\circ}_{u,y}(z_i)$. An observable variable is one with degree greater than or equal to 1. The degree of an observable variable is sometimes called its *degree of observability*. The following theorem is a new test of observability based on the construction of a characteristic set of the defining differential ideal of $\mathscr{X}$ (compare with [8]).

Theorem 5.3. *Let a ranking of $\mathbf{k}\{U, Y, Z\}$ be fixed such that any derivative of the components of U and Y is lower than $Z_1, Z_2, \ldots, Z_n$. Let $\mathscr{A}$ be a characteristic set of $\mathbf{I}(\mathscr{X})$. If $\mathscr{X}$ is observable (with respect to u and y), then each Z_i is (effectively) introduced in $\mathscr{A}$ by a differential polynomial of order zero and with degree $\leqslant d^{\circ}_{u,y}(z_i)$ in Z_i $(1\leqslant i\leqslant n)$. Conversely, if each Z_i $(1\leqslant i\leqslant n)$ is introduced in $\mathscr{A}$ by a differential polynomial of order zero and degree d_i in Z_i, then $\mathscr{X}$ is observable, $d^{\circ}_{u,y}(z_i)\geqslant d_i$, and $d^{\circ}_{u,y}(z_i)$ divides $d_i\cdot\cdots\cdot d_2\cdot d_1$ (hence, $d^{\circ}_{u,y}(z_1)=d_1$).*

Assume that $\mathscr{X}$ is observable. Let P_i be the polynomial of $\mathbf{k}\{U, Y\}[Z_i]$ obtained by substituting U and Y for u and y, respectively, in the minimal polynomial of z_i over $\mathbf{k}\langle u, y\rangle$ and by multiplying by the least common multiple of the denominators. By multiplying P_i by the product of some powers of the initials and separants of the elements of $\mathscr{A}\cap\mathbf{k}\{U, Y\}$, we may substitute the simultaneous remainders of the coefficients of P_i for these coefficients, and then consider P_i as reduced with respect to $\mathscr{A}\cap\mathbf{k}\{U, Y\}$; having done this transformation of P_i, we still have P_i with degree $d^{\circ}_{u,y}(z_i)$ in Z_i since the initial of P_i could not have been reduced to zero by the fact that it is not in $\mathbf{I}(\mathscr{X})\cap\mathbf{k}\{U, Y\}$. Now, if Z_i is not introduced in $\mathscr{A}$ by a differential polynomial of order 0 and degree $\leqslant d^{\circ}_{u,y}(z_i)$, then the corresponding P_i would be

reduced with respect to $\mathscr{A}$, which would contradict the nonnullity of P_i. Conversely, assume that each Z_i is introduced in $\mathscr{A}$ by a differential polynomial of order 0 and degree d_i. It is then clear that z_1 is algebraic over $\mathbf{k}\langle u, y\rangle$, z_2 is algebraic over $\mathbf{k}\langle u, y\rangle(z_1)$, etc., and z_n is algebraic over $\mathbf{k}\langle u, y\rangle(z_1, \ldots, z_{n-1})$. This implies that $\mathscr{X}$ is observable. The rest of the proof is classical in the theory of algebraic extensions. We note that, by the primality of $\mathbf{I}(\mathscr{X})$, and the fact that $\mathscr{A}$ is a characteristic set of $\mathbf{I}(\mathscr{X})$, the differential polynomials in $\mathscr{A}$ which introduce $z_1, \ldots, z_n$ are irreducible over the fields $\mathbf{k}\langle u, y\rangle, \mathbf{k}\langle u, y\rangle(z_1), \ldots, \mathbf{k}\langle u, y\rangle(z_1, \ldots, z_{n-1})$, respectively; hence, the degrees of $\mathbf{k}\langle u, y\rangle(z_1)$, $\mathbf{k}\langle u, y\rangle(z_1, z_2), \ldots, \mathbf{k}\langle u, y\rangle(z_1, \ldots, z_n)$ over $\mathbf{k}\langle u, y\rangle$ are given by d_1, $d_2 \cdot d_1, \ldots, d_n \cdot \cdots \cdot d_2 \cdot d_1$, respectively. This completes the proof.

Remark 5.4. Note that Theorem 5.3 carries with it the relativity of the concept of observability, i.e., if we need to test the observability of any variables with respect to any others, then the theorem contains an indication to a way to perform that test by ranking these variables conveniently.

5.3.1. Observability and minimal realization

It could have been thought that the minimality of a realization is equivalent to the controllability and observability of that realization. This is not so. The point is that the minimality of a realization of an ordinary system is equivalent to its observability only. Let us proceed to prove this.

We assume that the components of the input are independent, i.e., they are differential indeterminates.

Recall (see [6]) that the *order* $o(\mathscr{X})$ of an irreducibile ordinary system $\mathscr{X}$ is defined to be the (nondifferential) transcendence degree $\operatorname{tr} d^{\circ}_{\mathbf{k}\langle u\rangle} \mathbf{k}\langle u, y\rangle$ of $\mathbf{k}\langle u, y\rangle$ over $\mathbf{k}\langle u\rangle$.

A realization

$$\begin{cases} \dot{x}_i = f_i(x, u), & 1 \leqslant i \leqslant n, \\ y_j = h_j(x, u), & 1 \leqslant j \leqslant p \end{cases}$$

of $\mathscr{X}$ is said to be *minimal* if the number of components n of x is equal to $o(\mathscr{X})$.

Let the above equations be a realization of $\mathscr{X}$. We have

$$n = \operatorname{tr} d^{\circ}_{\mathbf{k}\langle u\rangle} \mathbf{k}\langle u\rangle(x) = \operatorname{tr} d^{\circ}_{\mathbf{k}\langle u\rangle} \mathbf{k}\langle u, y, x\rangle = \operatorname{tr} d^{\circ}_{\mathbf{k}\langle u, y\rangle} \mathbf{k}\langle u, y, x\rangle + o(\mathscr{X}). \qquad (*)$$

The second and third equalities in $(*)$ are clear. Let us prove the first one. With respect to any ranking of $\mathbf{k}\{U, Y, X\}$ such that the derivatives of U and X all are lower than the components of Y, and these derivatives are orderly ranked, the equations of the above realization are readily a characteristic set of $\mathbf{k}\langle u, y, x\rangle$. By Lemma 4.2, the equations

$$\dot{x}_i = f_i(x, u), \quad 1 \leqslant i \leqslant n$$

form a characteristic set of $\mathbf{k}\langle u, x\rangle$. This proves that there is no nontrivial (nondifferential) algebraic relation between the x_i's, i.e., the x_i's are algebraically independent over $\mathbf{k}\langle u\rangle$.

We have just shown the following theorem.

Theorem 5.5. *A realization of an irreducible ordinary system is minimal if and only if it is observable.*

5.3.2. On universal external trajectories

Recall that the universal external trajectories of $\mathscr{X}$ are the specializations of u and y for which there exist expressions of the respective minimal polynomials of the components of z whose denominators are not annulled by these specializations of u and y. Universal inputs of $\mathscr{X}$ would be readily obtainable from a characteristic set of $\mathscr{X}$ if the minimal polynomials of the components of z are such. This is wanting. However, we have the following partial result.

Theorem 5.6. *Let a ranking of $\mathbf{k}\{U, Y, Z\}$ be fixed such that any derivative of the components of U and Y is lower than any component of Z. If $\mathscr{X}$ is observable and possesses an orthonomic characteristic set $\mathscr{A}$, then the universal external trajectories of $\mathscr{X}$ are characterized by means of the initials of the elements of $\mathscr{A}$ which introduce the components of Z, respectively.*

This theorem is quite an immediate consequence of the previous one.

5.4. Invertibility

We refer to [6] for an algebraic theory of invertibility. We recall that the invertibility of an irreducible system $\mathscr{X}$ (with $\mathbf{k}\langle\mathscr{X}\rangle = \mathbf{k}\langle u, y, z\rangle$, $u = (u_1, u_2, \ldots, u_m)$, $y = (y_1, y_2, \ldots, y_p)$, $z = (z_1, z_2, \ldots, z_n)$) reads as the equality of the differential output rank of $\mathscr{X}$ and the (differential) dimension of $\mathscr{X}$. The following theorem is a new test of invertibility based on the construction of a characteristic set of the defining differential ideal of $\mathscr{X}$.

Theorem 5.7. *Let a ranking of $\mathbf{k}\{U, Y, Z\}$ be fixed such that the derivatives of the components of Y are all lower than the components of U and Z. Let $\mathscr{A}$ be a characteristic set of $\mathbf{I}(\mathscr{X})$. $\mathscr{X}$ is invertible if and only if the system of parametric indeterminates of* $\mathfrak{p}$ *defined by $\mathscr{A}$ is a subset of Y.*

This is quite an immediate consequence of Lemma 2.17.

References

[1] S. Diop, Théorie de l'Élimination et Principe du Modèle Interne en Automatique, Thèse de Doctorat, Université Paris-Sud, Orsay, 1989.

[2] S. Diop, Elimination in control theory, *Math. Control Signals Systems* **4** (1991) 17–32.

[3] S. Diop, Closedness of morphism of differential algebraic sets. Applications to system theory *Forum Math.*, to appear.
[4] S. Diop and M. Fliess, On nonlinear observability, in: C. Commault et al., eds., *Proc. 1st European Control Conf.* (Hermès, Paris, 1991) 152–157.
[5] S. Diop and M. Fliess, Nonlinear observability, identifiability, and persistent trajectories, in: *Proc. 30th IEEE Conf. on Decision and Control* (IEEE Press, New York, 1991) 714–719.
[6] M. Fliess, Automatique et corps différentiels, *Forum Math.* **1** (1989) 227–238.
[7] M. Fliess, Generalized controller canonical forms for linear and nonlinear dynamics, *IEEE Trans. Automat. Control* **35** (1990) 994–1001.
[8] S.T. Glad, Differential algebraic modelling of nonlinear systems, in: M.A. Kaashoek, J.H. van Schuppen and A.C.M. Ran, eds., *Realization and Modelling in System Theory, Proc. MTNS-89* (Birkhäuser, Boston, 1989) 97–105.
[9] J. Johnson, Differential dimension polynomials and a fundamental theorem on differential modules, *Amer. J. Math.* **91** (1969) 239–248.
[10] R.E. Kolchin, The notion of dimension in the theory of algebraic differential equations, *Bull. Amer. Math. Soc.* **70** (1964) 570–573.
[11] R.E. Kolchin, *Differential Algebra and Algebraic Groups* (Academic Press, New York, 1973).
[12] J.F. Ritt, *Differential Algebra* (American Mathematical Society, New York, 1950).
[13] A. Rosenfeld, Specializations in differential algebra, *Trans. Amer. Math. Soc.* **90** (1959) 394–407.
[14] A. Seidenberg, An elimination theory for differential algebra, *Univ. California Publications Math. (N.S.)* **3** (1956) 31–65.
[15] W.Y. Sit, Well-ordering of certain numerical polynomials, *Trans. Amer. Math. Soc.* **212** (1975) 37–45.
[16] W.Y. Sit, Differential dimension polynomials of finitely generated extensions, *Proc. Amer. Math. Soc.* **68** (1978) 251–257.
[17] M.I. Freedman and J.C. Willems, Smooth representations of systems with differentiated inputs, *IEEE Trans. Automat. Control* **23** (1978) 16–22.
[18] C.H. Moog, J. Perraud, P. Bentz and Q.T. Vo, Prime differential ideals in nonlinear rational control systems, in: *Proc. NOLCOS '89*, 178–182.