

COMPUTING CHARACTERISTIC SETS OF ORDINARY RADICAL DIFFERENTIAL IDEALS

BRAHIM SADIK

Abstract. We give upper bounds for the order of the elements in a characteristic set of a regular differential ideal or a radical of a finitely generated differential ideal with respect to some specific orderings. We then show how to compute characteristic sets of these ideals using algebraic methods.

2000 Mathematics Subject Classification: 12H05, 13B25, 13P10.

Key words and phrases: Differential algebra, characteristic sets, differential ideals, Gröbner bases.

1. INTRODUCTION

A characteristic set of an ideal, in a polynomial ring over a commutative field, is a finite set of polynomials that preserves the main properties of the original system. Moreover, this set has the lowest rank among all triangular sets in the ideal. For polynomial rings over commutative fields, Gallo and Mishra [7] realized an efficient algorithm for computing characteristic sets and studied its complexity. For differential polynomial rings over zero characteristic fields and for prime differential ideals, an algorithm has been described by Ollivier [9]. This algorithm applies in some special cases. Computing characteristic sets of prime differential ideals is also one application of the Rosenfeld–Gröbner algorithm developed by Boulier [2], Boulier et al. [4, 3]. The author [13] has studied the complexity of computing characteristic sets of ordinary differential ideals by change of orderings.

An open question (to my knowledge) is the computation of characteristic sets for non-prime differential ideals. In this paper we solve this problem for regular differential ideals and radicals of finitely generated differential ideals in the ordinary case. Our method applies for orderings

$$u_1 \prec \cdots \prec u_q \prec y_1 \prec \cdots \prec y_p,$$

where the first q indeterminates form a parametric set for the ideal we consider. When the ordering is not specified, we give sufficient conditions to compute characteristic sets in these general cases. The paper is arranged as follows: Section 2 is devoted to presenting some definitions and fixing some notations. In Section 3, we give some properties of regular differential ideals and characteristic sets. In the last section, which is the main one, we give upper bounds for the order of the elements in a characteristic set of a regular differential ideal or a radical of a finitely generated differential ideal. In Subsection 4.1 and for regular differential ideals, we show how to find a basis for a polynomial ideal

that contains this characteristic set. Subsection 4.2 is devoted to computing a characteristic set of a radical of a finitely generated differential ideal. For this, we need to apply the Rosenfel–Gröbner algorithm [2, 4, 3] to a finite set of differential polynomials ϕ . Once we have a representation by regular differential ideals, we can apply the Buchberger algorithm [1, 5, 6] to construct a basis from which we extract a characteristic set of the radical differential ideal $\{\phi\}$.

2. SOME DEFINITIONS AND NOTATION

Let \mathcal{F} be a zero characteristic differential field and δ be a derivation on \mathcal{F} . Let $X = \{x_1, \dots, x_n\}$ be a finite set of differential indeterminates over \mathcal{F} and $\Theta X = \{\delta^j x_i \mid 1 \leq i \leq n, j \geq 0\}$. A derivative $\delta^j x_i$ will be denoted $x_{i,j}$. The integer j is the order of $x_{i,j}$, it will be denoted by $\text{ord}(x_{i,j})$. The ring of differential polynomials (d.p.) $\mathcal{R} = \mathcal{F}\{x_1, \dots, x_n\}$ in the differential indeterminates x_1, \dots, x_n with coefficients in \mathcal{F} , is the polynomial ring $\mathcal{F}[\Theta X]$.

Definition 1 ([8], p. 45). A total order \prec on ΘX is called a ranking (or an ordering) if it satisfies the following two conditions:

1. $u \prec \delta u \quad \forall u \in \Theta X$,
2. $u \prec v \implies \delta u \prec \delta v \quad \forall u, v \in \Theta X$.

A ranking \prec on ΘX is an orderly ordering if the following holds:

$$\text{ord}(u) < \text{ord}(v) \implies u \prec v \quad \forall u, v \in \Theta X.$$

A ranking $x_1 \prec \dots \prec x_n$ on ΘX is an elimination ranking if

$$i \leq j \implies x_{i,\ell} \prec x_{j,k} \quad \forall \ell, k \in \mathbb{N}.$$

Fix a ranking \prec on ΘX . Let f be a differential polynomial, not in \mathcal{F} . The leading derivative of f is the greatest element $x_{i,j}$ of ΘX (w.r.t. \prec) that appears in f , we denote it by $\text{Ld}(f)$; the variable x_i will be called the leading variable of f and it will be denoted $\text{Lv}(f)$. Assume that $\text{Ld}(f) = v$ and write $f = I_d v^d + \dots + I_0$ ($I_d \neq 0$), then $I_f = I_d$ is the initial of f and $S_f = \frac{\partial f}{\partial v}$ is the separant of f . The order of f in x_i ($\text{ord}(f, x_i)$) is the maximum integer j such that $x_{i,j}$ appears effectively in f . Let $D(f)$ be the set of all derivatives $x_{i,j}$ that appear effectively in f , the order of f ($\text{ord}(f)$) being $\max\{j : \exists 1 \leq i \leq n \mid x_{i,j} \in D(f)\}$.

Consider now a differential polynomial (d.p.) g that is not in \mathcal{F} . A d.p. f is less than g ($f < g$) if $\text{Ld}(f) \prec \text{Ld}(g)$ or $\text{Ld}(f) = \text{Ld}(g) = v$ and $\text{degree}(f, v) < \text{degree}(g, v)$. If neither $f < g$ nor $g < f$, we say that f and g have the same rank and we write $f \sim g$. We say that f is partially reduced with respect to g if f is free of every derivative of $\text{Ld}(g)$. It is reduced with respect to g if f is partially reduced with respect to g and $\text{degree}(f, \text{Ld}(g)) < \text{degree}(g, \text{Ld}(g))$. Let S be a subset of $\mathcal{F}\{x_1, \dots, x_n\} \setminus \mathcal{F}$, we say that f is reduced (resp. partially reduced) w.r.t. S if it is reduced (resp. partially reduced) with respect to each element of S .

A subset A of \mathcal{R} is called an autoreduced set if every element in A is reduced w.r.t. all the others. An autoreduced set is necessarily finite (see [8], p. 77). If $A = \{A_1, \dots, A_p\}$ is an autoreduced set with $A_1 < A_2 < \dots < A_p$, then

we denote A by $A = A_1, \dots, A_p$. Let $A = A_1, \dots, A_p$ and $B = B_1, \dots, B_q$ be two autoreduced sets, we say that A is less than B ($A < B$) if either there is some $j \leq \min(p, q)$ such that $A_i \sim B_i$ for $i < j$ and $A_j < B_j$, or $q < p$ and $A_i \sim B_i$ for $i \leq q$. If neither $A < B$ nor $B < A$, we say that A and B have the same rank, and we denote $A \sim B$. The pre-order defined above is artinian (see [8, 10]). If F is a subset of \mathcal{R} , then the set of all autoreduced sets of F has a minimal element, which we call a characteristic set of F .

An ideal \mathcal{I} of \mathcal{R} which is closed under derivation is called a differential ideal. The ideal \mathcal{I} is a radical differential ideal if \mathcal{I} is a differential ideal and, for all $f \in \mathcal{R}$, if some power of f belongs to \mathcal{I} , then f is also in \mathcal{I} . If S is a subset of \mathcal{R} , then we denote by (S) , $[S]$ and $\{S\}$, respectively, the ideal, the differential ideal, and the radical differential ideal generated by S .

Partial reduction ([8], p. 77, 78). Let $A = A_1, \dots, A_p$ be an autoreduced set. Then for every differential polynomial F , we can compute a differential polynomial R partially reduced w.r.t. A and integers a_1, \dots, a_p such that

$$S_1^{a_1} \dots S_p^{a_p} F \equiv R \pmod{[A]},$$

where $S_i = S_{A_i}$ for $1 \leq i \leq p$.

Algebraic reduction. Let f and g be two differential polynomials such that f is partially reduced w.r.t. g . Then we can compute a differential polynomial h reduced w.r.t. g and an integer ℓ such that $I_g^\ell f \equiv h \pmod{(g)}$.

Full reduction. A full reduction of a differential polynomial F by an autoreduced set $A = A_1, \dots, A_p$ can be computed as follows: we first reduce partially F w.r.t. A , then we reduce algebraically the result by A_p, A_{p-1} and so on. So we can compute a d.p. $R = \text{prem}(f; A)$ which is reduced w.r.t. A and satisfies

$$I_1^{i_1} \dots I_p^{i_p} S_1^{s_1} \dots S_p^{s_p} f \equiv R \pmod{[A]},$$

where $I_\ell = I_{A_\ell}, S_k = S_{A_k}$ and i_k, s_ℓ are nonnegative integers. In particular, a characteristic set of a differential ideal \mathcal{I} is an autoreduced set of \mathcal{I} that reduces every element of \mathcal{I} to zero.

Let H be a finite set of d.p. and H^∞ be the free multiplicative semigroup generated by 1 and H . For any subset S of d.p., we denote $(S) : H^\infty$ (respectively $[S] : H^\infty$) the ideal of all d.p. f for which there exists $h \in H^\infty$ such that $hf \in (S)$ (respectively $hf \in [S]$). Let A be an autoreduced set of \mathcal{R} , then H_A denotes the set of initials and separants of the elements in A . The differential ideal $[A] : H_A^\infty$ will be called the regular differential ideal associated to A . The notion of regular differential ideals was first introduced by Boulier et al. in [4].

It is known that any radical differential ideal \mathcal{I} is the intersection of a finite number of prime differential ideals $\mathcal{I} = \mathcal{P}_1 \cap \dots \cap \mathcal{P}_r$. The ideals \mathcal{P} are called components of \mathcal{I} . A component \mathcal{P}_i is said to be redundant if $\mathcal{I} = \bigcap_{i \neq j} \mathcal{P}_j$. A component which is not redundant is called a minimal prime component of \mathcal{I} .

A subset $\{u_1, \dots, u_q\}$ of $\{x_1, \dots, x_n\}$ is differentially independent modulo \mathcal{I} if

$$\mathcal{I} \cap \mathcal{F}\{u_1, \dots, u_q\} = (0).$$

It is differentially dependent otherwise. Such a subset is called a parametric set of \mathcal{I} when it is differentially independent modulo \mathcal{I} and its cardinal is maximal. The cardinal of a parametric set of \mathcal{I} is called the dimension of \mathcal{I} and will be denoted by $\dim(\mathcal{I})$.

Let $\{u_1, \dots, u_q\}$ be a subset of $\{x_1, \dots, x_n\}$, then we denote by $\mathcal{F}\langle u_1, \dots, u_q \rangle$ the fraction field $\mathcal{F}(u_{i,j}, j \in \mathbb{N}, 1 \leq i \leq q)$ equipped with the derivation δ .

3. SOME PRELIMINARY PROPERTIES

In this section, $\mathcal{R} = \mathcal{F}\{x_1, \dots, x_n\}$, $\mathcal{R}_s = \mathcal{F}[x_{i,j}, 1 \leq i \leq n, j \leq s]$ and $\mathcal{I}(s) = \mathcal{I} \cap \mathcal{R}_s$ for a differential ideal \mathcal{I} .

Lemma 1. *Let $C = C_1, \dots, C_q$ be a triangular set of \mathcal{R}_s ($\text{Ld}(C_i) \neq \text{Ld}(C_j) \forall i \neq j$). Let H_C be the set of initials and separants of C_i . If L denotes the set of the leading derivatives of the elements of C , then*

- 1) *the ideal $I = (C) : H_C^\infty$ is a radical ideal in \mathcal{R}_s ,*
- 2) *the set $N = \{x_{i,j}, 1 \leq i \leq n, j \leq s\} \setminus L$ provides a parametric set, in a nondifferential sense, for every minimal prime component \mathcal{P} of I .*

Proof. See [3], Theorem 2.1. □

Lemma 2. *Let $A := A_1, \dots, A_p$ be an autoreduced set in \mathcal{R} with respect to an orderly ordering such that $1 \notin \mathcal{I} = [A] : H_A^\infty$. Let $s \geq \max\{\text{ord}(A_i) : 1 \leq i \leq p\}$, then*

$$\mathcal{I}(s) = (\delta^j A_i, \text{ord}(\delta^j A_i) \leq s, 1 \leq i \leq p) : H_A^\infty.$$

Proof. Denote $\mathcal{J}(s) = (\delta^j A_i, \text{ord}(\delta^j A_i) \leq s, 1 \leq i \leq p) : H_A^\infty$. We shall prove that $\mathcal{I}(s) = \mathcal{J}(s)$. The inclusion $\mathcal{J}(s) \subset \mathcal{I}(s)$ is clear. Let us prove the converse one. For this consider a polynomial $f \in \mathcal{I}(s)$. Reducing it partially by A , we get a formula

$$S_1^{a_1} \dots S_p^{a_p} f - R_0 \equiv 0 \pmod{(\delta^j A_i, \text{ord}(\delta^j A_i) \leq s, 1 \leq i \leq p)}.$$

By the Rosenfeld lemma ([12], p. 397), the pseudo-remainder R_0 belongs to $(A) : H_A^\infty$. Since s is great enough we get $(A) : H_A^\infty \subset \mathcal{J}(s)$ and hence $f \in \mathcal{J}(s)$. □

Proposition 1. *Let $A := A_1, \dots, A_p$ be an autoreduced set in \mathcal{R} with respect to an orderly ordering such that $1 \notin \mathcal{I} = [A] : H_A^\infty$. Then*

- \mathcal{I} is a radical differential ideal.
- \mathcal{I} and its minimal prime components have the same differential transcendence function.
- *When $s \geq \max\{\text{ord}(A_i) : 1 \leq i \leq p\}$ the differential transcendence function of \mathcal{I} is equal to $(n - p)(s + 1) + h$, where $h = \sum_{i=1}^p \text{ord}(A_i)$ and n is the number of differential indeterminates.*

Proof.

- See [3].

- By [3], \mathcal{I} and its minimal prime components have characteristic sets which have the same leading derivatives. Hence they have the same differential transcendence function.
- Let us prove the last point. Let $s \geq \max\{\text{ord}(A_i) : 1 \leq i \leq p\}$, then by Lemma 2

$$\mathcal{I}(s) = (\delta^j A_i, j \leq s - \text{ord}(A_i), 1 \leq i \leq p) : H_A^\infty.$$

The cardinal of the family

$$\delta^j A_i, j \leq s - \text{ord}(A_i), 1 \leq i \leq p$$

is equal to $p(s + 1) - \sum_{i=1}^p \text{ord}(A_i)$. Hence the dimension of $\mathcal{I}(s)$ is equal to $(n - p)(s + 1) + \sum_{i=1}^p \text{ord}(A_i)$ by lemma 1. \square

Definition 2. Let $A := A_1, \dots, A_p$ be an autoreduced set in \mathcal{R} w.r.t. an orderly ordering such that $1 \notin \mathcal{I} = [A] : H_A^\infty$. The integer $h = \sum_{i=1}^p \text{ord}(A_i)$ will be called the order of \mathcal{I} . It will be denoted by $\text{ord}(\mathcal{I})$.¹

Remark 1. Let \prec be an orderly ordering and \mathcal{I} be a prime differential ideal in \mathcal{R} . We know that \mathcal{I} admits a characteristic set $C = C_1, \dots, C_p$ w.r.t. \prec such that $\mathcal{I} = [C] : H_C^\infty$. Hence we may define the order of \mathcal{I} as in the last definition.

The following result goes back to [13].

Theorem 1. *Let \mathcal{I} be an ordinary prime differential ideal of order h . Then with respect to any ranking, the ideal \mathcal{I} admits a characteristic set in which the order of each element cannot exceed h .*

We get immediately the following result.

Proposition 2. *Let \mathcal{I} be an ordinary prime differential ideal and u_1, \dots, u_q be elements of $\{x_1, \dots, x_n\}$. Let $h = \text{ord}(\mathcal{I})$ and assume that u_1, \dots, u_q are differentially dependent modulo \mathcal{I} . Then the ideal \mathcal{I} contains a d.p. U that depends only on u_1, \dots, u_q and is of order less than or equal to h .*

Lemma 3. *Let C_1, \dots, C_ℓ be a triangular set ($\text{Ld}(C_i) \neq \text{Ld}(C_j)$ for $i \neq j$) of \mathcal{R} and $f \in \mathcal{R}$. Assume that a derivative v appears effectively in f and not in any C_i for $1 \leq i \leq \ell$. Then f belongs to $(C_1, \dots, C_\ell) : H_C^\infty$ implies that the coefficients of f arranged as a polynomial in v are also in $(C_1, \dots, C_\ell) : H_C^\infty$.*

Proof. We have $f \in (C_1, \dots, C_\ell) : H_C^\infty$. There exist $\alpha \in \mathbb{N}$ and $M_1, \dots, M_\ell \in \mathcal{R}$ such that

$$H_C^\alpha f = M_1 C_1 + \dots + M_\ell C_\ell.$$

Denote $r = \max\{\text{deg}(f, v), \text{deg}(M_i, v) : 1 \leq i \leq \ell\}$ and write f and the polynomials M_i as polynomials in v . Therefore we obtain

$$f = f_r v^r + \dots + f_1 v + f_0$$

¹ Proposition 1 implies that the definition of $\text{ord}(\mathcal{I})$ is independent of A .

and for $1 \leq i \leq \ell$ we get

$$M_i = M_{i,r}v^r + \cdots + M_{i,1}v + M_{i,0}.$$

Furthermore, the equation

$$H_C^\alpha(f_r v^r + \cdots + f_1 v + f_0) = \sum_{i=1}^{\ell} (M_{i,r}v^r + \cdots + M_{i,1}v + M_{i,0})C_i$$

yields

$$H_C^\alpha f_j = M_{1,j}C_1 + \cdots + M_{\ell,j}C_\ell$$

for $1 \leq j \leq r$. This completes the proof of the lemma. \square

Lemma 4. *Let $C := C_1, \dots, C_p$ be a characteristic set of a prime differential ideal \mathcal{I} in \mathcal{R} w.r.t. an orderly ordering \prec . Let $y_i = \text{Lv}(C_i)$ for $1 \leq i \leq p$ and u_1, \dots, u_q be the other differential indeterminates. Then C is also a characteristic set of the prime differential ideal*

$$\mathcal{J} = \left\{ \frac{f}{g}, f \in \mathcal{I}, 0 \neq g \in \mathcal{F}\{u_1, \dots, u_q\} \right\}$$

in $\mathcal{F}\langle u_1, \dots, u_q \rangle \{y_1, \dots, y_p\}$ w.r.t. to the ranking \prec on y_1, \dots, y_p .

Proof. Consider C as an autoreduced set in $\mathcal{F}\langle u_1, \dots, u_q \rangle \{y_1, \dots, y_p\}$. Let $f \in \mathcal{J}$ and $R_0 = \text{prem}(f; C)$. There exists a relation $H_A^\alpha f - R_0 \equiv 0 \pmod{[C]}$ in $\mathcal{F}\langle u_1, \dots, u_q \rangle \{y_1, \dots, y_p\}$. The polynomial R_0 lies in \mathcal{J} , then there exists $0 \neq M \in \mathcal{F}\{u_1, \dots, u_q\}$ such that $MR_0 \in \mathcal{I}$. Since MR_0 is reduced w.r.t. A it must vanish. Thus $R_0 = 0$ and the proof is completed. \square

Lemma 5. *Let $C := C_1, \dots, C_p$ be a characteristic set of a prime differential ideal \mathcal{I} in \mathcal{R} w.r.t. an orderly ordering \prec . Let $y_i = \text{Lv}(C_i)$, $e_i = \text{ord}(C_i, y_i)$ and $f \in \mathcal{R}$ such that $\text{ord}(f, y_i) \leq s$ for $1 \leq i \leq p$ and some integer $s \geq \max\{e_i : 1 \leq i \leq p\}$. Then f lies in \mathcal{I} if and only if it lies in the ideal*

$$(\delta^j C_i, j \leq s - e_i, 1 \leq i \leq p) : H_C^\infty.$$

Proof. Assume that $f \in \mathcal{I}$. Let

$$\{u_1, \dots, u_q\} = \{x_1, \dots, x_n\} \setminus \{y_1, \dots, y_p\}$$

and

$$\mathcal{G} = \mathcal{F}\langle u_1, \dots, u_q \rangle.$$

By the preceding lemma, C_1, \dots, C_p is a characteristic set of the ideal

$$\mathcal{J} = \left\{ \frac{f}{g}, f \in \mathcal{I}, 0 \neq g \in \mathcal{F}\{u_1, \dots, u_q\} \right\}$$

in $\mathcal{G}\{y_1, \dots, y_p\}$ w.r.t. to the ranking \prec on y_1, \dots, y_p . Since the order of f as an element of $\mathcal{G}\{y_1, \dots, y_p\}$ is less than or equal to s , we obtain

$$f \in \mathcal{J}(s) = (\delta^j C_i, j \leq s - e_i, 1 \leq i \leq p) : H_C^\infty$$

by Lemma 2. Therefore we get a relation

$$H_C^\alpha f \equiv 0 \pmod{(\delta^j C_i, j \leq s - e_i, 1 \leq i \leq p)} \text{ in } \mathcal{G}\{y_1, \dots, y_p\}.$$

Multiplying the last relation by a suitable element U of $\mathcal{F}\{u_1, \dots, u_q\}$ we get a formula

$$H_C^\alpha U f \equiv 0 \pmod{(\delta^j C_i, j \leq s - e_i, 1 \leq i \leq p)}.$$

in $\mathcal{F}\{x_1, \dots, x_n\}$. Since $\{u_1, \dots, u_q\}$ is a parametric set for \mathcal{I} , we obtain the desired result. \square

Lemma 6. *Let $C := C_1, \dots, C_p$ be a characteristic set of a prime differential ideal \mathcal{I} in \mathcal{R} with respect to an elimination ordering $x_1 \prec \dots \prec x_n$. Let $h = \text{ord}(\mathcal{I})$ and denote by y_i the leading variable of C_i for $1 \leq i \leq p$. Let s be an integer and f be a differential polynomial such that $\text{ord}(f, y_i) \leq s$ for $1 \leq i \leq p$. Then, $f \in \mathcal{I}$ if and only if $f \in (\delta^j C_i, 1 \leq i \leq p, j \leq s) : H_C^\infty$.*

Proof. The converse implication is clear. Let us prove the direct one. Using Theorem 1, we may assume that $\text{ord}(C_i) \leq h$ for $1 \leq i \leq p$. Let $e_i = \text{ord}(C_i, y_i)$. In each C_i and f , replace each derivative $y_{j,\ell}$ by $y_{j,\ell+h-e_j}$ for $1 \leq j \leq p$, giving a characteristic set $\bar{C} = \bar{C}_1, \dots, \bar{C}_p$ of a prime differential ideal \mathcal{J} with respect to an orderly ordering. Now $f \in \mathcal{I}$ if and only if $\bar{f} \in \mathcal{J}$. Since $\text{ord}(\bar{f}, y_i) \leq s + h$ and $\text{ord}(\bar{C}_i) = h$ for $1 \leq i \leq p$, we have by Lemma 5, $\bar{f} \in (\delta^j \bar{C}_i, 1 \leq i \leq p, j \leq s) : H_{\bar{C}}^\infty$. Hence we are done. \square

4. CHARACTERISTIC SETS OF RADICAL DIFFERENTIAL IDEALS

We recall that $\mathcal{R} = \mathcal{F}\{x_1, \dots, x_n\}$, $\mathcal{R}_s = \mathcal{F}[x_{i,j}, 1 \leq i \leq n, j \leq s]$ and $\mathcal{I}(s) = \mathcal{I} \cap \mathcal{R}_s$ for a differential ideal \mathcal{I} .

In the sequel we assume that 1 is not in any regular differential ideal we consider.

4.1. Regular differential ideals.

Lemma 7. *Let A be an autoreduced set in \mathcal{R} w.r.t. an orderly ordering, $\mathcal{I} = [A] : H_A^\infty$ and $h = \text{ord}(\mathcal{I})$. Let u_1, \dots, u_q be a parametric set for \mathcal{I} and let y_1, \dots, y_p be the other differential indeterminates. Let C_1, \dots, C_p be a characteristic set of \mathcal{I} w.r.t. an elimination ranking $u_1 < \dots < u_q < y_1 < \dots < y_p$.*

Assume that $\text{ord}(C_i, y_i) = e_i$ for $1 \leq i \leq p$, then $\sum_{i=1}^p e_i \leq h$.

Proof. For s great enough, the family

$$u_{i,j}, 1 \leq i \leq q, 0 \leq j \leq s, \quad y_{i,j}, 0 \leq j \leq e_i - 1, 1 \leq i \leq p$$

is algebraically independent modulo the polynomial ideal $\mathcal{I}(s)$. The number of the elements in F is equal to $q(s + 1) + \sum_{i=1}^p e_i$. Since by Proposition 1, the dimension of $\mathcal{I}(s)$ is equal to $q(s + 1) + h$, we get the desired inequality. \square

Lemma 8. *Let A be an autoreduced set in \mathcal{R} w.r.t. an orderly ordering, $\mathcal{I} = [A] : H_A^\infty$ and $h = \text{ord}(\mathcal{I})$. Let u_1, \dots, u_q be a parametric set for \mathcal{I} and let y_1, \dots, y_p be the other differential indeterminates. Then \mathcal{I} admits a characteristic set C_1, \dots, C_p w.r.t. an elimination ranking*

$$u_1 < \dots < u_q < y_1 < \dots < y_p \quad (*)$$

such that $\text{ord}(C_i) \leq 2h$ for $1 \leq i \leq p$.

Proof. Let R_1, \dots, R_p be a characteristic set of \mathcal{I} with respect to the ranking $(*)$. For $1 \leq i \leq p$, let D_i be a coefficient of R_i , that has the same rank as R_i when R_i is arranged as a polynomial in the derivatives $u_{i,j}, 1 \leq i \leq q, j > 2h$. By the previous lemma, we have $\text{ord}(R_i, y_i) \leq h$ for $1 \leq i \leq p$. This implies that $\text{ord}(R_i, y_j) \leq h$ for $1 \leq i, j \leq p$. Hence $\text{ord}(D_i) \leq 2h$ for $1 \leq i \leq p$.

Let \mathcal{P} be a minimal prime component of \mathcal{I} .

- If u_1, \dots, u_q are differentially dependent modulo \mathcal{P} , then by Proposition 2, \mathcal{P} contains a d.p. of order less than or equal to h that depends only on u_1, \dots, u_q .
- Assume that u_1, \dots, u_q is a parametric set for \mathcal{P} and let B_1, \dots, B_p be a characteristic set for \mathcal{P} w.r.t. the same ranking $(*)$. By Proposition 1, \mathcal{I} and \mathcal{P} have the same order and hence we may assume by Theorem 1 that $\text{ord}(B_i) \leq h$ for $1 \leq i \leq p$. Therefore each R_i (for $1 \leq i \leq p$) lies in $(\delta^j B_i, 1 \leq i \leq p, j \leq h) : H_B^\infty$ by Lemma 6. Using Lemma 3, $D_i \in (\delta^j B_i, 1 \leq i \leq p, j \leq h) : H_B^\infty$. Hence D_i belongs to \mathcal{P} for $1 \leq i \leq p$.

Since \mathcal{I} is the intersection of its minimal prime components, we see easily that \mathcal{I} admits a characteristic set C_1, \dots, C_p , where each C_i is a product of D_i and a polynomial in $\mathcal{F}\{u_1, \dots, u_q\}$, such that $\text{ord}(C_i) \leq 2h$ for $1 \leq i \leq p$. \square

We may thus formulate the following theorem.

Theorem 2. *Let $A := A_1, \dots, A_p$ be an autoreduced set in \mathcal{R} w.r.t. to an orderly ordering, $\mathcal{I} = [A] : H_A^\infty$ and $h = \text{ord}(\mathcal{I})$. Then a characteristic set of \mathcal{I} with respect to an elimination ordering*

$$u_1 \prec \dots \prec u_q \prec y_1 \prec \dots \prec y_p$$

where the first q variables form a parametric set for \mathcal{I} , is contained in the polynomial ideal $\mathcal{I}(2h)$ of the polynomial ring \mathcal{R}_{2h} .

Remark 2. Let \prec be a ranking on \mathcal{R} and s be an integer. Then \prec induces an ordering of the derivatives $x_{i,j}; 1 \leq i \leq n; j \leq s$. It should be taken into account anywhere we talk about ordering of the derivatives.

Remark 3. Let $A := A_1, \dots, A_p$ be an autoreduced set in \mathcal{R} w.r.t. to an orderly ordering, $\mathcal{I} = [A] : H_A^\infty$, $h = \text{ord}(\mathcal{I})$ and $e_i = \text{ord}(A_i)$ for $1 \leq i \leq p$. For an integer $s \geq \max\{e_i : 1 \leq i \leq p\}$, the ideal $\mathcal{I}(s)$ is equal to $(\delta^j A_i, 0 \leq j \leq s - e_i, 1 \leq i \leq p) : H_A^\infty$ by Lemma 2. Let x_0 be a new indeterminate and $H = \prod_{i=1}^p S_{A_i} I_{A_i}$. Using the Rabinowitsch “trick” (J. L. Rabinowitsch, Zum Hilbertschen Nullstellensatz. *Math. Ann.* **102**(1930), No. 1, 520) we have

$$\mathcal{I}(s) = (\delta^j A_i, 0 \leq j \leq s - e_i, 1 \leq i \leq p, Hx_0 - 1) \cap \mathcal{R}_s.$$

Assume that we desire to compute a characteristic set for \mathcal{I} w.r.t. an elimination ranking \prec . We first compute a Gröbner basis G of the polynomial ideal

$$(\delta^j A_i, 0 \leq j \leq 2h - e_i, 1 \leq i \leq p, Hx_0 - 1)$$

with respect to a lexicographical ordering on the derivatives, which first eliminates x_0 [1, 5, 6]. Therefore $G \cap \mathcal{R}_{2h}$ is a Gröbner basis for the polynomial ideal $\mathcal{I}(2h)$. Now in the polynomial case, any characteristic set C of G is a characteristic set of $\mathcal{I}(2h)$ (see [11]). Finally, any minimal autoreduced set of C in the differential case is a characteristic set for \mathcal{I} w.r.t. \prec .

Example 1. Consider two differential polynomials: $f_1 = x_{1,1}^2 x_{2,0} + tx_{1,0}$ and $f_2 = x_{1,0} x_{2,1} + x_{1,0} x_{2,0} + tx_{2,0}$ in $\mathbb{Q}(t)\{x_1, x_2\}$, with $\delta = \frac{d}{dt}$. We see easily that $A = f_1, f_2$ is an autoreduced set w.r.t. the orderly ordering such that $x_1 < x_2$. We have $H_A = \{x_{1,1}, x_{2,0}, x_{1,0}\}$ and $\text{ord}([A] : H_A^\infty) = 2$. Our desire is to compute a characteristic set C_1, C_2 for $[A] : H_A^\infty$ w.r.t. the elimination ranking $x_1 \prec x_2$. Since the ideal $\mathcal{I} = [A] : H_A^\infty$ is zero-dimensional its characteristic set is contained in $\mathcal{I}(2) = (f_1, f_2, \delta f_1, \delta f_2) : H_A^\infty$. We get the following set after computation:

$$\begin{aligned} C_1 &= -t^2 x_{1,1} + 2x_{1,2} t x_{1,0} - t x_{1,1}^2 - t x_{1,0} x_{1,1} - x_{1,0} x_{1,1}, \\ C_2 &= x_{1,1}^2 x_{2,0} + t x_{1,0}. \end{aligned}$$

An outlook on the general case. Let $A := A_1, \dots, A_p$ be an autoreduced set in \mathcal{R} w.r.t. an orderly ordering. Let $C := C_1, \dots, C_\ell$ be a characteristic set of $\mathcal{I} = [A] : H_A^\infty$ with respect to another ordering \prec . We see easily that $\ell \geq p$ but the equality cannot be proved. When we have the equality, we can bound the order of the C_i as in Lemma 8. We solve partially this problem by giving a sufficient condition for the equality to hold and in this case we can compute a characteristic set for \mathcal{I} w.r.t. \prec .

Lemma 9. *Let \mathcal{I} be an ordinary differential ideal. Let $C = C_1, \dots, C_\ell$ be a characteristic set for \mathcal{I} with respect to an elimination ordering \prec on x_1, \dots, x_n . Denote $y_i = \text{Lv}(C_i)$ for $1 \leq i \leq \ell$ and let u_1, \dots, u_q be the other differential indeterminates. Then C is also a characteristic set for \mathcal{I} w.r.t. any ordering*

$$u_1 < \dots < u_q < y_1 < \dots < y_p.$$

Proof. It is sufficient to show that C reduces all nonzero elements of \mathcal{I} w.r.t. the new ordering $u_1 < \dots < u_q < y_1 < \dots < y_p$. Since C reduces all nonzero elements of \mathcal{I} to zero, the family u_1, \dots, u_q is differentially independent modulo \mathcal{I} . Therefore a nonzero element f of \mathcal{I} must introduce at least a derivative of one of the variables y_1, \dots, y_p . But f must be reduced by C w.r.t. the ordering \prec on x_1, \dots, x_n , hence it must be reduced by C w.r.t. to the new ordering $u_1 < \dots < u_q < y_1 < \dots < y_p$. \square

Lemma 10. *Let $A := A_1, \dots, A_p$ be an autoreduced set in \mathcal{R} w.r.t. an orderly ordering, $\mathcal{I} = [A] : H_A^\infty$ and $h = \text{ord}(\mathcal{I})$. Let $\{u_1, \dots, u_{n-p}\}$ be a subset of $\{x_1, \dots, x_n\}$ and s be a nonnegative integer that is greater than or equal to h . Then $\{u_1, \dots, u_{n-p}\}$ is a parametric set for \mathcal{I} if and only if the family $u_{i,j}, 1 \leq i \leq n-p, j \leq h$ is algebraically independent modulo the polynomial ideal $\mathcal{I}(s)$.*

Proof. The direct implication is clear. By Lemma 1 \mathcal{I} and its minimal prime components have the same dimension $n - p$ and the same order h . Using Lemma 2, the converse implication is proved. \square

Proposition 3. *Let $A := A_1, \dots, A_p$ be an autoreduced set in \mathcal{R} w.r.t. an orderly ordering, $\mathcal{I} = [A] : H_A^\infty$ and $h = \text{ord}(\mathcal{I})$. Let \prec be an elimination ordering on x_1, \dots, x_n and let B be a Gröbner basis for $\mathcal{I}(2h)$ w.r.t. to the ordering induced by \prec on \mathcal{R}_{2h} . Let $\{y_1, \dots, y_\ell\}$ be the set of the variables which are leading variables of some element in B . Then $\ell = p$ implies that in the differential case a characteristic set of B is a characteristic set of \mathcal{I} w.r.t. \prec .*

Proof. Let $\{u_1, \dots, u_q\} = \{x_1, \dots, x_n\} \setminus \{y_1, \dots, y_p\}$. The family $u_{i,j}, 1 \leq i \leq q, j \leq h$ is algebraically independent modulo $\mathcal{I}(2h)$, therefore u_1, \dots, u_q is a parametric set for \mathcal{I} by Lemma 10. Using Theorem 2 a characteristic set of \mathcal{I} w.r.t. the ordering

$$u_1 \prec \dots \prec u_q \prec y_1 \prec \dots \prec y_p$$

is contained in the ideal $\mathcal{I}(2h)$. Thus we conclude the proof using Lemma 9. \square

Example 2. Let $f_1 = x_{1,0}x_{2,1}^2 + x_{2,1}x_{3,0}, f_2 = x_{2,1}x_{1,1} + tx_{3,1} + t^2 + 1$ in $\mathbb{Q}(t)\{x_1, x_2\}$. The set $A = f_1, f_2$ is an autoreduced set with respect to the orderly ordering $x_3 \prec x_2 \prec x_1$. We have $H_A = \{(2x_{1,0}x_{2,1} + x_{3,0}), x_{2,1}x_{1,0}\}$, $\dim(\mathcal{I} = [A] : H_A^\infty) = 1$ and $\text{ord}(\mathcal{I}) = 2$. We want to compute a characteristic set for \mathcal{I} w.r.t. an elimination ranking such that $x_1 < x_2 < x_3$. After computing a Gröbner basis B for $\mathcal{I}(4)$ w.r.t. the induced ordering, we get that x_1 is not a leading variable of any element in B . By Proposition 3, a characteristic set $C = C_1, C_2$ for \mathcal{I} w.r.t. the ordering $x_1 < x_2 < x_3$ is then contained in the ideal $\mathcal{I}(4)$. We obtain the following polynomials:

$$\begin{aligned} C_1 &= tx_{2,2}x_{1,0} - x_{2,1}x_{1,1} + x_{1,1}x_{2,1}t - t^2 - 1, \\ C_2 &= x_{1,0}x_{2,1} + x_{3,0} \end{aligned}$$

4.2. Radicals of finitely generated differential ideals. Consider a finite subset ϕ of d.p. for which we apply the Rosenfeld-Gröbner algorithm with respect to an orderly ranking (see [4, 3]). This algorithm permits us to compute regular differential ideals $\mathcal{J}_1, \dots, \mathcal{J}_r$, where each ideal \mathcal{J}_i is respectively the regular differential ideal associated to an autoreduced set A_i , such that $\{\phi\} = \mathcal{J}_1 \cap \dots \cap \mathcal{J}_r$. Using Proposition 1, the minimal prime components of each \mathcal{J}_i have the same dimension and the same order. Let q be a maximum of the dimensions of the ideals $\mathcal{J}_i, 1 \leq i \leq r$ and h be the maximum of the orders of the ideals whose dimension is equal to q . Then for $s \gg 0$, the dimension of the polynomial ideal $\{\phi\}(s) = \{\phi\} \cap \mathcal{R}_s$ is equal to $q(s + 1) + h$. The integer q is the dimension of $\{\phi\}$ and h will be called the order of $\{\phi\}$ (we denote it by $\text{ord}(\{\phi\})$).

Theorem 3. *Let ϕ be a finite set of d.p. and $\{\phi\} = [A_1] : H_{A_1}^\infty \cap \dots \cap [A_r] : H_{A_r}^\infty$ be the decomposition given by the Rosenfeld-Gröbner algorithm w.r.t. to an orderly ordering. Let $h = \text{ord}(\{\phi\})$ and h' be a maximum of the orders of the ideals $[A]_i : H_{A_i}^\infty$. Then with respect to any elimination ordering*

$$u_1 \prec \dots \prec u_q \prec y_1 \prec \dots \prec y_p,$$

where the first q indeterminates form a parametric set for $\{\phi\}$, the differential ideal $\{\phi\}$ admits a characteristic set C_1, \dots, C_p such that the order of each C_i cannot exceed $\max\{2h, h'\}$.

Proof. The idea of the proof is very similar to the one used in the proof of Lemma 8.

Let $A := A_1, \dots, A_p$ be a characteristic set of $\{\phi\}$ w.r.t. to the described ordering. Since the dimension of $\{\phi\}(s)$, for $s \gg 0$, is equal to $q(s + 1) + h$, we see, using a similar result of Lemma 7 for $\{\phi\}$, that $\text{ord}(A_i, y_i) \leq h$ for $1 \leq i \leq p$. Therefore $\text{ord}(A_i, y_j) \leq h$ for $1 \leq i, j \leq p$. Next, let D_i , for $1 \leq i \leq p$, be a coefficient of A_i , that has the same rank as A_i when A_i is arranged as a polynomial in the derivatives $u_{i,j}$, $1 \leq i \leq q, j > 2h$.

Let \mathcal{P} be a minimal prime component of $\{\phi\}$.

- Assume that u_1, \dots, u_q form a parametric set for \mathcal{P} . Then $\text{ord}(\mathcal{P}) \leq h$ and \mathcal{P} admits a characteristic set B_1, \dots, B_p with respect to the elimination ordering

$$u_1 \prec \dots \prec u_q \prec y_1 \prec \dots \prec y_p$$

such that $\text{ord}(B_i) \leq h$ for $1 \leq i \leq p$ by Theorem 1. By Lemma 6,

$$A_i \in (\delta^j B_i, 1 \leq i \leq p, j \leq h) : H_B^\infty$$

for $1 \leq i \leq p$. Hence by Lemma 3, \mathcal{P} contains D_i for $1 \leq i \leq p$.

- If u_1, \dots, u_q are differentially dependent modulo \mathcal{P} , then by Proposition 2 \mathcal{P} contains a d.p. that depends only on u_1, \dots, u_q and is of order less than or equal to h' .

Since $\text{ord}(D_i) \leq 2h$, for $1 \leq i \leq p$, we see that \mathcal{I} admits a characteristic set C_1, \dots, C_p with respect to the desired ordering such that each C_i is a product of D_i and a polynomial in $\mathcal{F}\{u_1, \dots, u_q\}$ is of order less than or equal to h' . It is clear that $\text{ord}(C_i) \leq \max\{2h, h'\}$ for $1 \leq i \leq p$. \square

We may thus formulate the following corollary.

Corollary 1. *Let ϕ be a finite set of d.p. and $\{\phi\} = \mathcal{J}_1 \cap \dots \cap \mathcal{J}_r$ be the decomposition given by the Rosenfeld–Gröbner algorithm w.r.t. to an orderly ordering. Let $h = \text{ord}(\{\phi\})$ and h' be a maximum of the orders of the ideals \mathcal{J}_i . Then with respect to any elimination ordering*

$$u_1 \prec \dots \prec u_q \prec y_1 \prec \dots \prec y_p,$$

where the first q indeterminates form a parametric set for $\{\phi\}$, a characteristic set of $\{\phi\}$ can be extracted, following the same way as in Remark 3, from one of the polynomial ideal $\{\phi\}(\max\{2h, h'\})$.

Remark 4. Let $s \gg 0$, then to compute a characteristic set for the polynomial ideal $\{\phi\}(s)$, we have to determine a basis for this ideal. Let $\{\phi\} = \mathcal{J}_1 \cap \dots \cap \mathcal{J}_r$ where each \mathcal{J}_i is the regular differential ideal associated to an autoreduced set A_i for $1 \leq i \leq r$. Using the Rabinowitsch “trick” and the Buchberger algorithm, we can compute bases for the ideals $\mathcal{J}_i(s)$ for $1 \leq i \leq r$. Since

$\{\phi\}(s) = \mathcal{J}_1(s) \cap \dots \cap \mathcal{J}_r(s)$, we can apply the Buchberger algorithm ([1, 5, 6]) to provide a basis for this intersection of ideals.

For the radical of finitely generated differential ideal, we use a similar discussion to the one in the last paragraphs of Subsection 4.1 to get a sufficient condition when the ordering in the variables is not specified.

Proposition 4. *Let ϕ be a finite set of d.p. and h, h' be defined as in Corollary 1. Let \prec be an elimination ordering and B be a Gröbner basis for the ideal $\{\phi\}(\max\{2h, h'\})$ w.r.t. to the ordering induced by \prec . Let $\{u_1, \dots, u_q\}$ be the set of the variables which are not leading variables of any element in B . If the dimension of $\{\phi\}$ is equal to q , then a characteristic set of B in the differential case w.r.t. \prec is a characteristic set of $\{\phi\}$ w.r.t. \prec .*

Remark 5. Consider a zero-dimensional system ϕ ($\dim(\{\phi\}) = 0$) of order equal to h . A characteristic set of $\{\phi\}$ w.r.t. to any ordering is contained in the polynomial ideal $\{\phi\}(h)$.

Example 3. In the ordinary differential ring $\mathbb{Q}\{x_1, x_2\}$ consider the differential polynomials:

$$\begin{aligned} f_1 &= x_{1,2}^2 + 2x_{1,1}x_{2,1} - x_{1,1}^3 - x_{1,0}x_{1,1}x_{2,1}, \\ f_2 &= x_{1,1}^2 + x_{1,0}x_{2,1} + x_{2,2}, \\ g_1 &= x_{1,1}, \\ g_2 &= x_{1,0}x_{2,1} + x_{2,2}, \end{aligned}$$

where $x_{i,j}$ is the j -the order derivative of the differential indeterminate x_i .

With respect to an orderly ordering such that $x_1 < x_2$, both f_1, f_2 and g_1, g_2 are autoreduced sets. We want to compute a characteristic set for the ideal

$$\mathcal{I} = [f_1, f_2] : \{x_{1,2}\}^\infty \cap [g_1, g_2]$$

with respect to an elimination ordering such that $x_1 < x_2$. Both $[f_1, f_2] : \{x_{1,2}\}^\infty$ and $[g_1, g_2]$ are differential ideals of dimension zero. The ideal $[f_1, f_2] : \{x_{1,2}\}^\infty$ is of order 4 and the other ideal $[g_1, g_2]$ is of order 3. The method described in Subsection 4.2 permits to obtain a characteristic set for \mathcal{I} from one of the algebraic ideals $\mathcal{I}(4)$ (Remark 5). A Gröbner basis computation gives the following characteristic set C_1, C_2 where:

$$\begin{aligned} C_1 &= -x_{1,1}^2x_{1,2}^2 + x_{1,1}^5 - x_{1,0}x_{1,2}^3 - 2x_{1,1}^3x_{1,0}x_{1,2} + 2x_{1,1}x_{1,0}x_{1,2}x_{1,3} \\ &\quad + x_{1,1}x_{1,0}^2x_{1,2}^2 - 2x_{1,0}x_{1,1}^4 + 2x_{1,2}^3 + 4x_{1,2}x_{1,1}^3 - 4x_{1,1}x_{1,2}x_{1,3} \\ &\quad - 2x_{1,1}x_{1,0}x_{1,2}^2 + 4x_{1,1}^4, \\ C_2 &= -x_{1,2}^2 - 2x_{1,1}x_{2,1} + x_{1,1}^3 + x_{1,0}x_{1,1}x_{2,1}. \end{aligned}$$

Example 4. Consider the radical differential ideal

$$\mathcal{I} = [x_{2,0}, x_{1,1} - x_{1,0}] \cap [x_{1,0}, x_{2,1} - x_{2,0}]$$

in $\mathbb{Q}\{x_1, x_2\}$. This ideal is of dimension zero and of order 1. Therefore by Subsection 4.2, a characteristic set is contained in the algebraic ideal $\mathcal{I}(1)$ (Remark 5). After computation, we obtain that $C_1 = x_{1,0}x_{2,0}, C_2 = x_{1,1} - x_{1,0}$ is a characteristic set for \mathcal{I} with respect to an orderly ordering such that $x_1 < x_2$.

5. CONCLUSION

We have studied the problem of computing characteristic sets of ordinary radical differential ideals. An open question is to study eventual possibilities to apply our results for computing characteristic sets with respect to any ordering. Another important problem is the extension of our method to the particular case.

REFERENCES

1. T. BECKER and V. WEISPFENNING, Gröbner bases. A computational approach to commutative algebra. *Graduate Texts in Mathematics*, 141. Springer-Verlag, New York, 1993.
2. F. BOULIER, Étude et implantation de quelques algorithmes en algèbre différentielle. *Ph.D. Thesis, L.I.F.L., Lille*, 1994.
3. F. BOULIER, D. LAZARD, F. OLLIVIER, and M. PETITOT, Computing representations for radicals of a finitely generated differential ideals. Available at <http://www.lift.fr/boulier/Publications.html>.
4. F. BOULIER, D. LAZARD, F. OLLIVIER, and M. PETITOT, Representation for the radical of a finitely generated differential ideal. *Proc. ISAAC-95*, 1995.
5. B. BUCHBERGER, Gröbner bases: an algorithmic method in polynomial ideal theory. *Recent trends in multidimensional system theory. Reidel (1985)* 184–232.
6. D. COX, J. LITTLE, and D. O’SHEA, Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra. *Undergraduate Texts in Mathematics. Springer-Verlag, New York*, 1992.
7. G. GALLO and B. MISHRA, Efficient algorithms and bounds for Wu–Ritt characteristic sets. *Effective methods in algebraic geometry (Castiglioncello, 1990)*, 119–142, *Progr. Math.*, 94, Birkhäuser Boston, Boston, MA, 1991.
8. E. R. KOLCHIN, Differential algebra and algebraic groups. *Pure and Applied Mathematics*, Vol. 54. Academic Press, New York–London, 1973.
9. F. OLLIVIER, Le problème de l’identifiabilité structurelle globale: méthodes effectives et Bornes de complexité. *Dh.D. Thesis, Centre de Mathématique, École polytechnique*, 1990.
10. J. F. RITT, Differential Algebra. *American Mathematical Society Colloquium Publications*, Vol. XXXIII, American Mathematical Society, New York, N. Y., 1950.
11. A. KANDRI RODY, Effective methods in the theory of polynomial ideals. *Ph.D. Thesis, Rensselaer Polytechnic Institute, Troy, N. Y.*, 1984.
12. A. ROSENFELD, Specializations in differential algebra. *Trans. Amer. Math. Soc.* **90**(1959), 394–407.
13. B. SADIK, A bound for the order of characteristic set elements of an ordinary prime differential ideal and some applications. *Appl. Algebra Engrg. Comm. Comput.* **10**(2000), No. 3, 251–268.

(Received 17.05.2005; revised 18.05.2006)

Author’s address:

Département de Mathématiques
 Faculté des Sciences Semlalia
 BP 2390 Mandrakes, Morocco
 E-mail: sadik@ucam.ac.ma