Extended Characteristic Sets of Finitely Generated Differential Ideals

Giuseppa Carra'Ferro [1] and Vladimir P. Gerdt [2]

[1] Dipartimento di Mathematica e Informatica
Universitá di Catania
Viale A. Doria 6
95125 Catania, Italy
carra@dmi.unict.it
[2] Laboratory of Information Technologies
Joint Institute for Nuclear Research
141980 Dubna, Russia
gerdt@jinr.ru

Abstract. In this paper we describe an algorithm for computation of an extended characteristic set for a differential ideal generated by a finite number of differential polynomials. This algorithm improves the Kolchin-Ritt algorithm by using algebraic Gröbner bases in the sense that it constructs an extended characteristic set which has rank either less than or equal to the one from the Kolchin-Ritt algorithm. We give explicit examples when the inequality holds.

1 Introduction

The notion of characteristic set was first introduced by Ritt [1] for differential ideals of ordinary differential polynomials, it was extended by Kolchin to the partial case [2] and now it is used in many distinct mathematical theories. Such notion extends the Janet theory [3] of passive orthonomic systems of algebraic differential equations. Janet also introduced implicitly the notion of multiplicative and nonmultiplicative derivatives in order to complete a system of orthonomic algebraic differential equations to its passive or involutive form. These notions were extended in the so-called formal theory of differential equations [4] and generalized in [5, 6]; now it is a good tool for studying systems of algebraic differential equations and their completion to involution [7]. Wu used the notion of characteristic set [8] in his algorithms for automatic deduction in elementary and algebraic differential geometry and now the corresponding Ritt algorithm for finding an extended characteristic set is known as Wu-Ritt algorithm. It is well known the use of characteristic sets of polynomial ideals as alternative to the Gröbner bases, introduced by Buchberger [9], in many problems of algebraic system solving. The characteristic set is then alternative to differential Gröbner bases introduced by [10] and [11] and studied also in [12]. Unfortunately there is no general algorithm that allows to find a characteristic set of a differential ideal generated by a finite number of differential polynomials. In the polynomial case it is always possible to find the characteristic set of a polynomial ideal when a Gröbner basis of the ideal with respect to a lexicographic term ordering is known [17]. In the general case some procedures that use extended characteristic sets are known for the decomposition of the differential radical ideal associated with a system of algebraic differential equations [13–16]. All such theories use either the well known Wu-Ritt algorithm in the polynomial case and in the ordinary differential case or the Kolchin-Ritt algorithm based on the Rosenfeld lemma [18] for finding an extended characteristic set, which is very often different from the characteristic set. In this paper we show that if we modify the classical Kolchin-Ritt algorithm for extended characteristic sets by using Gröbner bases in the intermediate steps of the algorithm, then we get an autoreduced set that has a rank less than or equal to the usual extended characteristic set, and then it is more near to a characteristic set, which has the minimal rank.

2 Preliminaries

Let K be a zero characteristic *differential field* with a finite set of mutually commuting *derivations* $\{\partial_1, \cdots, \partial_n\}$, and let $\Theta = \{\theta = \partial_1^{\alpha_1} \cdots \partial_n^{\alpha_n} \mid (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n\}$ be the monoid of *derivation operators*. The *least common multiple* of $\theta, \vartheta \in \Theta$ will be written as $lcm(\theta, \vartheta)$.

We shall denote by $\mathbb{R} = \mathbb{K}\{y_1, \ldots, y_m\}$ the *differential polynomial ring* [1, 2] with the set of *differential indeterminates* $\{y_1, \ldots, y_m\}$ and by $\mathbb{V} = \{\theta y_j \mid \theta \in \Theta, 1 \le j \le m\}$ the set of variables in $\mathbb{R}$. If $f \in \mathbb{R}$ contains the variable v, then we denote the degree of v in f by $\deg_v(f)$. The order of derivative $\theta = \partial_1^{\alpha_1} \cdots \partial_n^{\alpha_n}$ is $\sum_{i=1}^n \alpha_i$ and will be denoted by $\mathrm{ord}(\theta)$. If $\mathrm{ord}(\theta) > 0$, the derivation operator θ is said to be *proper*.

Definition 1. [2] A total order on $\mathbb{V}$ is called *a ranking* if it satisfies

1. $(\forall \theta \in \Theta \setminus \{1\})\ (\forall v \in \mathbb{V})\ [\ v \prec \theta v\ ]$
2. $v_1 \prec v_2\ (v_1, v_2 \in \mathbb{V})$ iff $(\forall \theta \in \Theta)\ [\ \theta v_1 \prec \theta v_2\ ]$

A ranking $\prec$ is said to be *orderly* if $\theta y_j \prec \vartheta y_k$ $(1 \le i, k \le m)$ whenever $\mathrm{ord}(\theta) < \mathrm{ord}(\vartheta)$ and *elimination* if $y_j \succ y_k$ implies $\theta y_j \succ \vartheta y_k$ for any $\theta, \vartheta \in \Theta$.

Lemma 1. [2] *A ranking on $\mathbb{V}$ is a well (admissible) ordering.*

Proof. Suppose that there exists an infinite decreasing sequence of elements in $\mathbb{V}$ with respect to $\prec$. Then there exists at least one i $(1 \le i \le n)$ such that $\theta_1 y_i \succ \theta_2 y_i \succ \cdots$ is an infinite decreasing sequence. By Definition 1, the ranking $\prec$ induces a total order $\prec_i$ on the set $V_i = \{\theta y_i \mid \theta \in \Theta\}$. Since the set V_i is a monoid isomorphic to $\mathbb{N}^n$, the total order $\prec_i$ is a term ordering on $\mathbb{N}_0^n$ by its own definition. The properties (1)–(2) in Definition 1 imply that $\prec_i$ is a well ordering, and, hence, the decreasing sequence $\{\theta_l \mid l \in \mathbb{N}\}$ is stationary. It follows that $\prec$ is a well ordering.

Other properties of rankings can be found in [19] and [20].

Definition 2. [2] Given a ranking $\prec$ on $\mathbb{V}$ and a differential polynomial $f \in \mathbb{R} \setminus \{0\}$, the variable θy_i of maximal ranking which is contained in f is called the *leading variable* or *leader* of f and will be denoted by u_f. Thus, f can be written as $f = \sum_{j=0}^d I_j u_f^j$ with $u_{I_j} \prec u_f$ $(0 \le j \le d)$. I_d is called the *initial* of f and will be denoted by I_f. The initial of $\partial f / \partial u_f$ is called the *separant* of f and will be denoted by S_f.

Definition 3. Given a finite set $F \subset \mathbb{R} \setminus \{0\}$, we shall denote by H_F the set of initials and separants of elements in F, and by (F) the algebraic ideal generated by F in the polynomial ring $\mathbb{K}[V_1]$ where $V_1 \subset \mathbb{V}$ is the finite subset of variables which occur in F. Then $(F) : H_F^\infty$ is the *saturation of* (F) *with respect to* H_F, that is, an ideal in $\mathbb{K}[V_1]$ such that for any its element $g \in (F) : H_F^\infty$ there exists a power product h of elements in H_F providing $h\, g \in (F)$.

3 Ritt Reduction

In this section we consider one of the reduction algorithms [1, 2, 13–15]. Suppose a ranking $\prec$ is fixed.

Definition 4. Let $f, g \in R \setminus \{0\}$. f is said to be *R-partially reduced with respect to* g[1] if f does not contain any proper derivative of u_g. f is said to be *R-reduced with respect to* g if f is R-partially reduced and $\deg_{u_g} f < \deg_{u_g} g$.

Theorem 1. *Let $f, g \in R \setminus \{0\}$. If f is not R-partially reduced with respect to g, then this reduction can be done in a finite number of steps.*

Proof. Assume that f contains a proper derivative θu_g. The equality $\theta g = S_g \theta u_g + h$ with $u_h \prec \theta u_g$ implies that the polynomial f can be pseudodivided [21] by θg. Let r_1 be the pseudoremainder. The condition $\deg_{u_g} \theta g = 1$ implies that $u_{r_1} \prec \theta u_g = u_{\theta g}$. Let $\theta_1 = \theta$. If r_1 still contains a proper derivative $\theta_2 u_g$ of u_g the preudodivision can be applied to r_1 again to produce the pseudoremainder r_2. By proceeding in this way we obtain a sequence of pseudoremainders $r_1, r_2, \cdots$ with $u_{r_1} \prec \theta_1 u_g$, $u_{r_2} \prec \theta_2 u_g \prec \theta_1 u_g$ and so on. Since $\succ$ is a well ordering by Lemma 1, the sequence $\theta_1 u_g \succ \theta_2 u_g \succ \cdots$ is finite and the sequence $r_1, r_2, \cdots$ terminates with a pseudoremainder which is R-partially reduced with respect to g.

Lemma 2. *Let $f, g \in \mathbb{R} \setminus \{0\}$. Suppose that f is R-partially reduced but not R-reduced with respect to g. Then f can always be R-reduced with respect to g in a finite number of steps.*

Proof. Let $d_1 = \deg_{u_g} g$ and $d_2 = \deg_{u_g} f$. By hypotesis $d_1 \le d_2$, and f can be R-reduced with respect to g by means of pseudodivision: $I_g g^{d_2 - d_1 + 1} f = p\, g + r$ where the pseudoremainder r is R-reduced with respect to g.

[1] R stands here after Ritt.

Definition 5. If $f \in \mathbb{R}$ is R-reduced (R-partially reduced) with respect to $g \in \mathbb{R}$, we shall say that f is in the *R-normal form (R-partial normal form) with respect to* g and write $f = RNF(f,g)$ ($f = RPNF(f,g)$). If $G \subset \mathbb{R}$ is a finite set we shall say that f is in the *R-normal form (R-partial normal form) with respect to* G and write $f = RNF(f,G)$ ($f = RPNF(f,G)$) if $f = RNF(f,g)$ ($f = RPNF(f,g)$) for every element $g \in G$.

Remark 1. Given $f, g \in \mathbb{R} \setminus \{0\}$, the procedures described in the proofs of Theorem 1 and Lemma 2 give algorithms for the computation of $RPNF(f,g)$ and $RNF(f,g)$, respectively which we fix as constituents of other algorithms described below.

Definition 6. Let F be a subset of $\mathbb{R} \setminus \{0\}$. F is said to be *autoreduced* if for every pair $f, g \in F$ the equalities $f = RNF(f,g)$ and $g = RNF(g,f)$ hold.

Theorem 2. [2] *Every autoreduced set $F \subset \mathbb{R} \setminus \{0\}$ is finite.*

Proof. Assume that F is autoreduced and infinite. Then there is i ($1 \leq i \leq n$) with an infinite autoreduced subset G of F such that for each $g \in G$ $u_g = \theta y_i$ for some $\theta \in \Theta$. Consider the set $U = \{u_g \mid g \in G\}$. Since the monoid Θ is isomorphic $\mathbb{N}^n$, by Dickson's lemma [22] there may be only finitely many distinct derivation operators θ such that in any pair θ_1, θ_2 of them one operator is not multiple of another. Because G is R-partially reduced, it follows that there are infinitely many distinct elements in G with the same leading variable. But then one derivative of a pair of such elements is pseudodivisible by another that contradicts our assumption.

Remark 2. If a finite set F is autoreduced, then we shall write it as a sorted set $F = \{f_1, \ldots, f_s\}$ with $u_{f_1} \prec u_{f_2} \prec \cdots \prec u_{f_s}$.

Remark 3. If $f \in \mathbb{R}$ is not R-reduced with respect to an autoreduced set $F = \{f_1, \ldots, f_s\}$ of $\mathbb{R}$, then f can be R-reduced with respect to F in a finite number of steps. It is sufficient to R-reduce f sequentially with respect to f_i ($1 \leq i \leq s$) in such a way R-partial reduction is done and then R-reduction. By Theorem 1 and Lemma 2 this is done in a finite number of steps. If r is the last pseudoremainder, then $r = RNF(f,F)$. Below we present an algorithm to compute r

The following algorithm **R-NormalForm**, given $p \in \mathbb{R} \setminus \{0\}$, a ranking $\prec$ and an autoreduced set $F \subset \mathbb{R} \setminus \{0\}$ provides computation of the R-normal form $RNF(p,F)$. *Correctness* and *termination* of this algorithm follow from Theorem 1, Lemma 2 and Remarks 1–3. The reduction process described in the algorithm is equivalent to that one given by Kolchin [2] when only R-partial reduction is done. But with R-reduction involved, algorithm **R-NormalForm** is different from the Kolchin algorithm, and equivalent to that described by Ritt [1].

Remark 4. The first **while***-loop in algorithm* **R-NormalForm** *performs partial R-reductions as described in the proof of Theorem 2 and, thus, computes the R-partial normal form of h modulo F. The second* **while***-loop performs the remaining R-reductions and thus completes computation of R-normal form h modulo F. With all this going on, different paths in the reduction process may end up with different value of the R-normal form. In particular, given f and F, the reduction path in the algorithm and, hence, its output may vary if the ranking is changed as the following example shows.*

Algorithm: R-NormalForm

Input: $p \in \mathbb{R}$, a differential polynomial; $F = \{f_1, \ldots, f_s\} \subset \mathbb{R}$, an autoreduced set; $\prec$, a ranking
Output: $h = RNF(p,F)$

```
1: h := p
2: while exist f ∈ F such that h contains a proper derivative of u_f do
3:    choose such f with the highest u_f w.r.t. ≺
4:    h := RPNF(h, f)
5: od
6: while exist f ∈ F such that h contains u_f and deg_{u_f}(h) ≤ deg_{u_f}(f) do
7:    choose such f with the highest u_f w.r.t. ≺
8:    h := RNF(h, f)
9: od
```

Example 1. $F := \{\partial_2 x, x\partial_1 y, \partial_2 y\}$, $f = \partial_1\partial_2 y - 1$. *Consider the elimination ranking (see Definition 1) with* $x \prec y$. *If* $\partial_1 \prec \partial_2$, *then, in accordance with algorithm* **R-NormalForm**, *we must do first the R-reduction with respect to* $\partial_2 y$: $f \to f - \partial_1(\partial_2 y) = -1$. *Thus,* $RNF(f, F) = -1$. *If we change the ranking taking* $\partial_2 \prec \partial_1$, *then we must do first the R-reduction of* f *with respect to* $x\partial_1 y - 1$ *and then with respect to* $\partial_2 y$:

$$f \to x^2 f - x\partial_2(x\partial_1 y - 1) + \partial_2 x((x\partial_1 y - 1) - \partial_2 x = -x^2.$$

This gives $RNF(f, F) = -x^2$.

4 Characteristic Sets

Definition 7. [1, 2] Given a ranking $\prec$ on $\mathbb{V}$ and a differential polynomial $f \in \mathbb{R} \setminus \mathbb{K}$, $u_f^{\deg_{u_f} f}$ will be called a *rank* of f and denoted by $\mathrm{rank}(f)$. Given two polynomials $f, g \in \mathbb{R} \setminus \mathbb{K}$, $\mathrm{rank}(f)$ is said to be less than $\mathrm{rank}(g)$ if $u_f \prec u_g$, or if $u_f = u_g$ and $\deg_{u_f} f < \deg_{u_g} g$. In this case we shall write $\mathrm{rank}(f) < \mathrm{rank}(g)$.

Let now $F = \{f_1, \ldots, f_s\}$ and $G = \{g_1, \ldots, g_t\}$ be finite autoreduced sets of nonzero differential polynomials sorted in accordance with Remark 2. Then F is said to be of rank less than G and written as $\mathrm{rank}(F) < \mathrm{rank}(G)$ if one of the two alternatives holds:

1. There is $i \le \min(s, t)$ such that $\mathrm{rank}(f_j) = \mathrm{rank}(g_j)$ for $1 \le j < i$ and $\mathrm{rank}(f_i)$ is less than $\mathrm{rank}(g_i)$.
2. $s > t$ and $\mathrm{rank}(f_j) = \mathrm{rank}(g_j)$ for $1 \le j \le t$.

F and G have the same rank if $s = t$ and $\mathrm{rank}(f_i) = \mathrm{rank}(g_i)$ for all i.

Definition 8. [1] Let A be a subset of $\mathbb{R}$ and $\succ$ be a ranking. A finite subset F of A is called a *characteristic set* of A if it is autoreduced and has the minimal rank among all the autoreduced subsets of A. All the characteristic sets of A have the same rank.

Definition 9. [2] An ideal of $\mathbb{R}$ which is stable under derivative operators in Θ is called a *differential ideal*. Let F be a subset of $\mathbb{R}$. The minimal differential ideal containing F is called the *differential ideal generated by* F and will be denoted by $[F]$. The ideal [F] is the intersection of all the differential ideals containing F. Similarly to the algebraic ideals (see Definition 3) we define the *saturation of* $[F]$ *with respect to* H_F as a differential ideal $[F] : H_F$ such that if $g \in [F] : H_F^\infty$, then there exists a power product h of elements in H_F providing $h\, g \in [F]$.

Definition 10. [14, 18] Let $p, q \in \mathbb{R} \setminus \{0\}$ be a pair of differential polynomials such that $u_p = \theta y_i$ and $u_q = \vartheta y_i$. Then if $lcm(\theta, \vartheta)$ is distinct from both θ and ϑ the *Δ-polynomial* $\Delta(p, q)$ of p, q is defined as

$$\Delta(p, q) = S_q \frac{lcm(\theta, \vartheta)}{\theta} p - S_p \frac{lcm(\theta, \vartheta)}{\vartheta} q,$$

where S_p and S_q are separants of p and q, respectively. Otherwise, if $\mathrm{rank}(p) \ge \mathrm{rank}(q)$ then the *Δ-polynomial* $\Delta(p, q)$ of p, q is defined as

$$\Delta(p, q) = RNF(p, q)$$

and as

$$\Delta(p, q) = RNF(q, p)$$

if $\mathrm{rank}(p) < \mathrm{rank}(q)$.

Definition 11. [13] An autoreduced subset G of $\mathbb{R} \setminus \{0\}$ is called *coherent* if for every pair $g_1, g_2 \in G$ generating Δ-polynomial the condition $RNF(\Delta(g_1, g_2), G) = 0$ holds.

Remark 5. Rosenfeld[18] defined coherence as follows. An autoreduced set F *is coherent if for any pair* $f, g \in F$ *of its elements such that* $u_f = \theta_1 y_i$, $u_g = \theta_2 y_i$ *the condition* $\Delta(f, g) \in (F_\nu) : H_F^\infty$ *holds where* F_ν *is the set* $F_\nu = \{\vartheta p \mid p \in F\}$ *with* $\vartheta u_p \prec lcm(\theta_1, \theta_2) y_i$. *This coherence condition is necessary and sufficient for* F *to be the characteristic set of a prime differential ideal* $[F] : H_F^\infty$. *Any autoreduced set, coherent in accordance with Definition 11, is also coherent in the sense of Rosenfeld [13].*

Definition 12. (cf. [2]) Given a differential ideal Id and an autoreduced set $G \subset Id$, the set G will be called *Id-coherent* if for every pair $f_1, f_2 \in Id$ with $u_{f_1} = \theta y_i$ and $u_{f_2} = \vartheta y_i$ $RNF(\Delta(f_1, f_2), G) = 0$.

Theorem 3. *Let Id be a differential ideal in $\mathbb{R}$, $G \subset Id$ be an autoreduced subset and $\prec$ be a ranking. Then the following are equivalent:*

(i). G is a characteristic set of Id with respect to $\prec$,
(ii). if $f \in Id$, then $RNF(f, G) = 0$,
(iii). G is Id-coherent.

Proof. $(i) \Longrightarrow (ii)$ by Definition 8. $(ii) \Longrightarrow (iii)$ by Definition 12 and the fact that $g_1, g_2 \in Id$ implies $\Delta(g_1, g_2) \in Id$. $(iii) \Longrightarrow (i)$ because there are no nonzero elements in Id reduced with respect to G. Indeed, suppose that there exists $f \in Id$, that is R-reduced with respect to G. Let δ_i be a derivation for some $I = 1, \ldots, n$. Since $f + \delta_i(f) \in Id$ and $\Delta(f + \delta_i(f), \delta_i(f)) = f$, (iii) implies $RNF(f, G) = 0$. Thus, there is no nonzero differential polynomial $f \in Id$ that is R-reduced with respect to G.

Lemma 3. *Let F be a finite subset of $\mathbb{R}$. Then there exists a subset G of F such that G is autoreduced and each $f \in F \setminus G$ is not R-reduced with respect to G.*

Proof. The set G can be computed by the following algorithm [1]

Algorithm: CharacteristicSet

Input: F, a finite subset of $\mathbb{R} \setminus \{0\}$
Output: G, a characteristic set of F

```
 1: G := ∅
 2: if F ∩ 𝕂 ≠ ∅ then
 3:    choose any f ∈ F ∩ 𝕂
 4:    G = {f}
 5: else
 6:    choose f ∈ F of the minimal rank
 7:    F := F \ {f}
 8:    G := G ∪ {f}
 9:    while F ≠ ∅ do
10:       choose g ∈ F of the minimal rank
11:       F := F \ {g}
12:       if g = RNF(g, G) then
13:          G := G ∪ {g}
14:       fi
15:    od
16: fi
```

The output set G is a characteristic set of F by construction and Definitions 7–8. The algorithm terminates in a finite number of steps, because F is finite.

Remark 6. If G is computed for F by the above algorithm we shall write $G = CharacteristicSet(F)$.

5 Kolchin-Ritt Algorithm

In his book [1] Ritt introduced an algorithm that, given a set F of ordinary differential polynomials, constructs a finite set $\tilde{F}$ such that $[F] = [\tilde{F}]$ and a subset G of $\tilde{F}$ such that G is a characteristic set of $\tilde{F}$. After the work of Wu [8] this set is often called an *extended characteristic set* of F. Furthermore, the algorithm is now known as Wu-Ritt algorithm.

By extending the Wu-Ritt algorithm to the partial differential case, given a finite subset F of differential polynomials in $\mathbb{R}$, it is possible to construct another finite subset $\tilde{F} \in \mathbb{R}$ such that $[F] = [\tilde{F}]$ and $\tilde{F}$ contains an autoreduced and coherent subset G which is the characteristic set of $\tilde{F}$. The algorithm for computation of G is known as Kolchin-Ritt algorithm [12].

We present this algorithm in a form different from that in paper [12] and prove its correctness and termination.

Algorithm: Kolchin-Ritt I

Input: $F \in \mathbb{R} \setminus \{0\}$, a finite subset; $\prec$, a ranking
Output: $\tilde{F}, G \subset \mathbb{R} \setminus \{0\}$ such that $[\tilde{F}] = [F]$ and
$G \subseteq \tilde{F}$ is the extended characteristic set

1: $\tilde{F} := F$
2: $G := CharacteristicSet(F)$
3: $B := \{\Delta(f_i, f_j) \mid f_i, f_j \in F,\ \mathrm{rank}(f_i) \leq \mathrm{rank}(f_j)\} \cup \tilde{F} \setminus G$
4: **while** $B \neq \emptyset$ **do**
5: **choose** $k \in B$ of the lowest rank
6: $h := RNF(k, G)$
7: **if** $h \neq 0$ **then**
8: $\tilde{F} := \tilde{F} \cup \{h\}$
9: $G := CharacteristicSet(\tilde{F})$
10: $B := B \cup \{\Delta(h, f) \mid f \in \tilde{F}\} \setminus \{k\}$
11: **fi**
12: **od**

Correctness. Let $\tilde{F}_0 = F$ and let $\tilde{F}_i$ and B_i be the values of $\tilde{F}$ and B, respectively, after ith execution of the **while**-loop. Then

$$F = \tilde{F}_0 \subseteq \tilde{F}_1 \subseteq \tilde{F}_2 \subseteq \cdots$$

The algorithm maintains the loop invariant $[F] = [\tilde{F}_i]$. Indeed, since the current set B_i of Δ-polynomials satisfies $B_i \subset [\tilde{F}_{i-1}]$ we deduce that $[\tilde{F}_i] = [\tilde{F}_{i-1} \cup B_i] = [\tilde{F}_{i-1}]$. Therefore, $[F] = [\tilde{F}_i]$.

Termination. Let now G_i be the value of G after the ith execution of the **while**-loop and $G_0 = CharacteristicSet(F)$). Then

$$\mathrm{rank}(G_0) \geq \mathrm{rank}(G_1) \geq \mathrm{rank}(G_2) \geq \cdots$$

By Ritt [1] and Kolchin [2], in every set of differential polynomials there exists an autoreduced subset of the minimal rank. Such subset is coherent by the rank minimality. Thereby, the chain of G_i terminates.

Example 2. $F = \{f_1, f_2, f_3\}$, $f_1 := \partial_2 x$, $f_2 := x\partial_1 y - 1$, $f_3 := \partial_2 y$. *For the elimination ranking* $x \prec y$, $\partial_1 \prec \partial_2$ *the set* f *is autoreduced and coherent. Thus,* G=F. *One can also show that*

$$[F] = [\partial_2 x, x\partial_1 y - 1, \partial_2 y, \partial_1^2 y + \partial_1 x(\partial_1 y)^2]$$

and $\{\partial_2 x, x\partial_1 y - 1, \partial_2 y, \partial_1^2 y + \partial_1 x(\partial_1 y)^2\}$ *is the differential Gröbner basis [10, 11] of [F]. G is the characteristic set of* $[F]$, *because* $[F] = [G] = [G] : x^\infty$ *and* $x \notin [F]$.

Now consider the differential polynomial $f = \partial_1\partial_2 y - 1 \notin [F]$. *If we R-reduce* f *with respect to* g_3 *we obtain* $h_1 = RNF(f, f_3) = -1$ *and* $h_1 = RNF(h_1, F)$. *However, if we use another chain of reduction we find* $h_2 = RNF(f, f_2) = -x$ *and again* $h_2 = RNF(h_2, F)$.

Remark 7. As Example 2 shows, the R-reduction chain of $p \in \mathbb{R}$ *with respect to elements of the characteristic set of a differential ideal* $[F]$ *(unlike its differential Gröbner basis) may end up with different results depending on the sequence of the elementary reductions. If* $p \in [F]$, *then the reduction sequence always ends with zero. It should be mentioned that in algorithm* **R-NormalForm** *(Sect.3) the elementary reduction sequence is fixed.*

Remark 8. As it follows from the structure of algorithm **Kolchin-Ritt I** *and the above analysis of its correctness, the sets* F, $\tilde{F}$ *and* G *satisfy the relation* $[G] \subseteq [F] = [\tilde{F}]$. *Generally,* $G \subset [F]$ *and below we demonstrate this fact by explicit examples.*

Since the above algorithm, generally, constructs not a characteristic set of a differential ideal $Id \subset \mathbb{R}$, but an extended characteristic set $G \subset [F]$, one can try to improve the algorithm in the following sense. An improved version constructs an extended characteristic set $\tilde{G}' \subset [F]$ such that $\mathrm{rank}(G') \leq \mathrm{rank}(G)$ and there are examples when the inequality holds.

Algorithm: Kolchin-Ritt II

Input: $F \in \mathbb{R} \setminus \{0\}$, a finite subset; $\prec$, a ranking
Output: $\tilde{F}, G \in \mathbb{R} \setminus \{0\}$ such that $[\tilde{F}] = [F]$ and
$G \subseteq \tilde{F}$ is the extended characteristic set

1: $\tilde{F} := F$
2: $h := 1$
3: **while** $h \neq 0$ **do**
4: $\quad \tilde{F} := GB(\tilde{F})$
5: $\quad G := CharacteristicSet(\tilde{F})$
6: $\quad$ **while** there exist $g, g' \in G$ such that $u_g = \theta y_i \preceq u_{g'} = \theta' y_i$ **do**
7: $\quad\quad$ **choose** such g, g' with $\Delta(g, g')$ of the lowest rank
8: $\quad\quad h := RNF(\Delta(g, g'), G)$
9: $\quad\quad$ **if** $h \neq 0$ **then**
10: $\quad\quad\quad \tilde{F} := \tilde{F} \cup \{h\}$
11: $\quad\quad$ **fi**
12: $\quad$ **od**
13: **od**

This improved version of algorithm **Kolchin-Ritt I** is based on the use of the algebraic Gröbner basis for some specified term order, for instance, the lexicographical order induced by the ranking $\prec$. Given an intermediate polynomial set $\tilde{F}$, its algebraic Gröbner basis denoted by $GB(\tilde{F})$.

Correctness and *termination* of this algorithm follows from those of algorithm **Kolchin-Ritt I** and of Buchberger algorithm for computation of algebraic Gröbner basis.

Example 3. $F := \{xy^2, yz-1, xv-\partial z\}$. *Consider the elimination ranking (see Definition 1) with* $x \prec y \prec z \prec v$. *Then, in accordance with the algorithm* **Kolchin-Ritt I**, *we have* $\tilde{F} := F$ *and* $G := \{xy^2, yz-1\}$. *If we use the algorithm* **Kolchin-Ritt II** *we have* $\tilde{F}_1 := \{x, yz-1, \partial z\}$ *and* $G_1 := \{x, \partial y, yz-1\}$, *which has rank less than* G.

Example 4. $F := \{xy^2, y\partial_1 z - x, \partial_2 z\}$. *Consider the elimination ranking with* $x \prec y \prec z$ *and* $\partial_1 x \prec \partial_2 x \prec \partial_1 y \prec \partial_2 y \prec \partial_1 z \prec \partial_2 z$. *Then, in accordance with the algorithm* **Kolchin-Ritt I**, *we have* $\tilde{F} := F$ *and* $G := \{xy^2, y\partial_1 z - x, \partial_2 z\}$. *If we use the algorithm* **Kolchin-Ritt II** *we have* $\tilde{F}_1 := \{x^3, x^2y, xy^2, y\partial_1 z - x, \partial_2 z\}$ *and* $G_1 := \{x^3, x^2y, \partial_2 z\}$, *which has rank less than* G.

6 Acknowledgements

The work was supported in part by the grant Intas 99-1222. The second author was also partially supported by the RFBR grants 00-15-96691 and 01-01-00708.

References

1. Ritt, J.F.: *Differential Algebra*, AMS Publication, New York (1950)
2. Kolchin, E.R.: *Differential Algebra and Algebraic Groups*, Academic Press, New York (1973)
3. Janet, M.: *Leçons sur les Systèmes d'Equations aux Dérivées Partielles*, Cahiers Scientifiques, IV, Gauthier-Villars, Paris (1929)
4. Pommaret, J.F.: *Systems of Partial Differential Equations and Lie Pseudogroups*, Gordon & Breach, New York (1978)
5. Gerdt, V.P., Blinkov, Yu.A.: Involutive Bases of Polynomial Ideals. *Math. Comp. Simul.* **45** (1998) 519–542; Minimal Involutive Bases. *Math. Comp. Simul.* **45** (1998) 543–560
6. Gerdt, V.P.: Completion of Linear Differential Systems to Involution. In: *Computer Algebra in Scientific Computing / CASC'99*, V.G.Ganzha, E.W.Mayr and E.V.Vorozhtsov (Eds.), Springer-Verlag, Berlin (1999) 115–137
7. Calmet, J., Hausdorf, M., Seiler, W.M.: A Constructive Introduction to Involution. *Proc. Int. Symp. Applications of Computer Algebra - ISACA 2000*, Allied Publishers, New Delhi (2001) 33–50
8. Wu, W.-T.: *On the Foundation of Algebraic Differential Geometry.* System Sciences and Mathematical Sciences **2** (1989) 289–312

9. Buchberger, B.: Gröbner Bases: an Algorithmic Method in Polynomial Ideal Theory. In: *Recent Trends in Multidimensional System Theory*, Bose, N.K. (ed.), Reidel, Dordrecht (1985) 184–232
10. Carra'Ferro, G.: Gröbner Bases and Differential Algebra. *Lec. Not. in Comp. Sci.* **356** (1987) 129–140
11. Ollivier, F.: Standard Bases of Differential Ideals. *Lec. Not. in Comp. Sci.* **508** (1990) 304–321
12. Mansfield, E., Clarkson, P.A.: Application of the Differential Algebra Package `diffgrob2` to Classical Symmetries of Differential Equations, *J. Symb. Comp.* **23** (1997) 517–533
13. Boulier, F., Lazard, D., Ollivier, F., Petitot, M.: Representation for the Radical of a Finitely Generated Differential Ideal. In: *Proceedings of ISSAC'95*, A.H.M. Levelt (ed.), ACM Press, New York (1995) 158–166
14. Boulier, F., Lazard, D., Ollivier, F., Petitot, M.: Computing Representations for Radicals of Finitely Generated Differential Ideals. *Technical report*, LIFL, Université Lille I (1997)
15. Hubert, E.: Factorization-free Decomposition Algorithms in Differential Algebra, *J. Symb. Comp.* **29** (2000) 641–662
16. Bouziane, D., Rody, A.K., Maârouf, H.: Unmixed-dimensional Decomposition of a Finitely Generated Perfect Differential Ideal, *J. Symb. Comp.* **31** (2001) 631–649
17. Aubry, F., Lazard, D., Moreno Maza, M.: On the Theories of Triangular Sets, *J. Symb. Comp.* **28** (1999) 105–124
18. Rosenfeld, A.: Specializations in Differential Algebra. *Trans. Amer. Math. Soc.* **90** (1959) 394–407
19. Carra'Ferro, G., Sit, W.Y.: On Term-Orderings and Rankings. Computational Algebra, G. Fischer, P. Loustaunau, J. Shapiro, E. Green, D. Farkas (Eds.), Marcel Dekker, New York (1994) 31–77
20. Rust, C.J., Reid, G.J.: Rankings of Partial Derivatives. In: *Proc. ISSAC'97*, W.Küchlin (ed.), ACM Press (1997) 9–16
21. Knuth, D.E.: *The Art of Computer Programming, Volume 2, Seminumerical Algorithms*, Addison-Wesley (1969)
22. Cox, D., Little, J., O'Shea, D.: *Ideals, Varieties and Algorithms*, 2nd Edition, Springer-Verlag, New York (1996)