Gröbner Walk for Characteristic Sets of Prime Differential Ideals

Oleg Golubitsky

Department of Mathematics
University of Pisa
Via Buonarroti 2, 56127, Pisa, Italy
golub@dm.unipi.it

Abstract. An algorithm which transforms a characteristic set of a prime differential ideal from one Riquier ranking to another is proposed. This paper completes the generalization of the Gröbner walk algorithm to the differential case initiated in [1]. In particular, a differential analogue of the Gröbner walk step is presented. The step is performed by a modified Rosenfeld–Gröbner algorithm, which avoids splittings of the ideal by using the fact that the ideal is prime and a characteristic set of it is already known, as well as performs all reductions within the set of initial forms of the ideal. The statement about the finiteness of the set of leaders of characteristic sets w.r.t. all possible rankings, which serves as a basis for the proof of termination of the differential Gröbner walk and whose proof in [1] is unfortunately incorrect, is reproved. The algorithm is illustrated by an example from [2].

1 Introduction

The problem of efficient transformation of characteristic sets of prime differential ideals from one ranking to another has been addressed in [3] and [2] (actually, these papers present transformation algorithms for regular systems which are closely related to characteristic sets). It is suggested in [3] that the more general case of an arbitrary radical differential ideal can be reduced to that of a prime ideal by performing the computations separately in the prime components of the radical ideal. In this paper, we also take this viewpoint, leaving the development of efficient transformation algorithms that would not involve the computation of prime components for future research. Indeed, this computation is not necessary, because the problem of transformation can be solved for any radical ideal by applying the Rosenfeld–Gröbner algorithm [4], but this straightforward solution does not take advantage of the fact that we already know a characteristic set and, therefore, is inefficient.

The algorithm in [2] is a variation of the Rosenfeld–Gröbner algorithm which avoids splittings of the ideal into several components by using the possibility of checking membership in the prime ideal. The Kähler algorithm in [3] also runs the Rosenfeld–Gröbner algorithm after introducing new differential variables corresponding to the Kähler differentials of the original ones and adding the Kähler differentials of the original equations to the system. The output of the Kähler algorithm is the set of leaders of the target regular system. Alternatively, but only in case the solution of the system depends on finitely many constants, one can apply the DFGLM algorithm [3], which is a differential analogue of the polynomial FGLM algorithm [5]. Once the leaders are found, some polynomials having these leaders and belonging to the differential ideal are recovered (this can also be done only when the solution depends on finitely many constants); these recovered polynomials may not yet constitute a regular system for I, so, in order to obtain one, they are added to the original system, after which the Rosenfeld–Gröbner algorithm is called (the added polynomials speed it up significantly).

The case when the solution of a differential system depends on finitely many constants is completely similar to the case of a zero-dimensional ideal in a polynomial ring, to which the FGLM algorithm is applicable. But even in this restricted case, the complexity of the FGLM algorithm

[0] The work has been supported by the Progetto di Interesse Nazionale “Algebra Commutativa e Computazionale” of the Italian “Ministero dell’Istruzione, dell’Università e della Ricerca Scientifica Tecnologica” and by the RFBR grant no. 02-01-01033.

grows with the dimension of quotient vector space R/I. In the differential case this growth is even more apparent; in some sense the complexity grows polynomially faster. Indeed, the complexity of the final step of the Kähler or DFGLM algorithm depends on the number of differential terms formed by derivatives not exceeding the found leaders; the number of these derivatives intuitively corresponds to the number of monomials "under the staircase" in the polynomial case (i.e., the dimension of R/I), whence the number of their products of degree m corresponds roughly to the mth power of this dimension.

The algorithm proposed in this paper generalizes the polynomial Gröbner walk algorithm to the differential case. The idea of the Gröbner walk is to replace the direct computation of a Gröbner basis w.r.t. to the target ordering by several computations of homogeneous Gröbner bases. The algorithm is applicable to any ideal and, in the zero-dimensional case, its complexity is not related to the dimension of vector space R/I (it depends on "how far apart" the initial and the target orderings are, as well as on the lengths of the initial homogeneous forms of the polynomials). Experiments in [6, 7] show that, apart from very simple cases, the Gröbner walk algorithm [8] is at least as fast as FGLM, and as the dimension of R/I grows, the Gröbner walk becomes much faster.

The key concepts needed for the Gröbner walk are the representation of monomial orderings by weight matrices [9, 10], monomial preorders defined by weight vectors [9–11], and the Gröbner fan [12, 10] of a polynomial ideal. In the differential case, the problem of parameterization of rankings, in general, is very complex [11, 13]. Therefore, we restrict ourselves to the case of Riquier rankings [14, 11], which include orderly and elimination rankings [15, 3]. Theorem of Mora and Robbiano about the finiteness of the Gröbner fan [12, 10] cannot be generalized to the differential case—in fact, the differential analogue of the Gröbner fan can be infinite (see an example in [1]). Nevertheless, the number of steps of the Gröbner walk is always finite, which is also shown in [1] modulo the statement about the finiteness of the set of leaders of characteristic sets w.r.t. different rankings. The proof of this statement in [1] is unfortunately incorrect and, therefore, another proof is presented here.

We generalize the key Gröbner walk lemmas [8, Lemmas 3.1–3.3] to the differential case, where they acquire a significantly different form. In particular, the polynomial ideal generated by the set of initial forms, which plays a key role for the polynomial Gröbner walk, cannot be simply replaced by the differential ideal generated by the initial forms (or its radical). Instead, we notice that the step of the polynomial Gröbner walk algorithm, i.e. computation of a homogeneous Gröbner basis, performs all operations within the *set* of initial forms (which is not an ideal). We modify the Rosenfeld–Gröbner algorithm accordingly, so that all differential reductions are performed within the set of initial forms.

2 Basic Concepts of Differential Algebra

Here we give a short summary of the basic concepts of differential algebra, referring the reader to [16, 17, 15] for a more complete exposition.

Let R be a commutative ring. A *derivation* over R is a mapping $\delta : R \to R$ which for every $a, b \in R$ satisfies

$$\delta(a+b) = \delta(a) + \delta(b), \qquad \delta(ab) = \delta(a)b + a\delta(b)\,.$$

A *differential ring* is a commutative ring endowed with a finite set of derivations $\Delta = \{\delta_1, \dots, \delta_m\}$ which commute pairwise. The commutative monoid generated by the derivations is denoted by Θ. Its elements are *derivation operators* $\theta = \delta_1^{i_1} \cdots \delta_m^{i_m}$, where $i_1, \dots, i_m$ are nonnegative integer numbers.

A *differential ideal* I of differential ring R is an ideal of R stable under derivations, i.e.

$$\forall\, A \in I,\, \delta \in \Delta \quad \delta A \in I\,.$$

For a subset $A \subset R$, denote by $[A]$ the smallest differential ideal containing A; the smallest ideal containing A is denoted by (A). For a set S, S^∞ denotes the set of finite products of elements of S. For a (differential) ideal I, $I : S^\infty$ denotes the following (differential) ideal:

$$I : S^\infty = \{a \in R \mid \exists\, s \in S^\infty \;\; as \in I\}\,.$$

An ideal is called *prime*, if

$$\forall a, b \in R \;\; ab \in I \;\; \Rightarrow \;\; a \in I \;\text{ or }\; b \in I\,.$$

Let $U = \{u_1, \ldots, u_n\}$ be a finite set whose elements are called *differential indeterminates.* Derivation operators apply to differential indeterminates giving *derivatives* θu. Denote by ΘU the set of all derivatives. Let $\mathcal{K}$ be a differential field of characteristic zero. The differential ring of *differential polynomials* $\mathcal{K}\{U\}$ is the ring of polynomials of infinitely many variables $\mathcal{K}[\Theta U]$ endowed with set of derivations Δ.

Let m be a nonnegative integer and n be a positive integer. Let

$$\mathbb{N} = \{0, 1, 2, \ldots\}, \quad \mathbb{N}_n = \{1, \ldots, n\}\,.$$

A *ranking* is a total order $\le$ of $\mathbb{N}^m \times \mathbb{N}_n$ such that for all $a, b, c \in \mathbb{N}^m$, $i, j \in \mathbb{N}_n$,

– $(a, i) \le (b, j) \iff (a + c, i) \le (b + c, j)$
– $(a, i) \ge (0, i)$.

Rankings on $\mathbb{N}^m \times \mathbb{N}_n$ correspond to rankings on the set of derivatives ΘU:

$$\delta_1^{i_1} \cdots \delta_m^{i_m} u_j \le \delta_1^{k_1} \cdots \delta_m^{k_m} u_l \iff (i_1, \ldots, i_m, j) \le (k_1, \ldots, k_m, l)\,.$$

3 Characteristic Sets

Let $\le$ be a ranking on the set of derivatives ΘU, and let $f \in \mathcal{K}\{U\}$, $f \notin \mathcal{K}$. The derivative θu_j of the highest rank present in f is called the *leader* of f (denoted $\mathrm{ld}_\le f$ or $\mathbf{u}_f$ when the ranking is clear from the context). Let $d = \deg_{\mathbf{u}_f} f$. Then $f = \sum_{j=0}^{d} g_j \mathbf{u}_f^j$, where $g_0, \ldots, g_d$ are uniquely defined polynomials free of $\mathbf{u}_f$. Differential polynomial $\mathbf{i}_f = g_d$ is called the *initial* of f, and differential polynomial $\mathbf{s}_f = \sum_{j=1}^{d} j g_j \mathbf{u}^{j-1}$ is called the *separant* of f. The *rank* $\mathrm{rk}_\le f$ is the monomial $(\mathbf{u}_f)^d$. For a set $A \subset \mathcal{K}\{U\}$, the set of initials (separants) of elements of A is denoted $\mathbf{i}_A$ ($\mathbf{s}_A$).

A ranking on the set of derivatives induces a linear order on the set of ranks, if we consider a rank t^d ($t \in \theta U, d > 0$) as a pair (t, d) and compare two such pairs lexicographically. Let $f, p \in \mathcal{K}\{U\}$, $p \notin \mathcal{K}$. Differential polynomial f is *partially reduced* w.r.t. p, if f is free of all proper derivatives $\theta \mathbf{u}_p$ (i.e. $\theta \ne 1$) of the leader of p. If f is partially reduced w.r.t. p and $\deg_{\mathbf{u}_p} f < \deg_{\mathbf{u}_p} p$, then f is said to be *(fully) reduced* w.r.t. p. A polynomial f is called *(partially) reducible* w.r.t. p, if it is not (partially) reduced w.r.t. p.

A differential polynomial f is called *(partially) reduced w.r.t. a set of differential polynomials* $A \subset \mathcal{K}\{U\}$, if it is (partially) reduced w.r.t. every polynomial $p \in A$.

A nonempty subset $A \subset \mathcal{K}\{U\}$ is called *(partially) autoreduced* if every $f \in A$ is (partially) reduced w.r.t. $A \setminus \{f\}$.

Every autoreduced set is finite [17, Chapter I, Section 9]. If $A = \{p_1, \ldots, p_k\}$ is an autoreduced set, then any two leaders $\mathbf{u}_{p_i}$, $\mathbf{u}_{p_j}$ for $1 \le i \ne j \le r$ are distinct; we assume that elements of any autoreduced set are arranged in order of increasing rank of their leaders $\mathbf{u}_{p_1} < \mathbf{u}_{p_2} < \ldots < \mathbf{u}_{p_k}$.

Let $A = \{f_1, \ldots, f_k\}, B = \{g_1, \ldots, g_l\}$ be two autoreduced sets. We say that A has *lower rank than* B and write $\mathrm{rk}_\le A < \mathrm{rk}_\le B$, if either there exists $j \in \mathbb{N}$ such that $\mathrm{rk}_\le f_i = \mathrm{rk}_\le g_i$ $(1 \le i < j)$ and $\mathrm{rk}_\le f_j < \mathrm{rk}_\le g_j$, or $k > l$ and $\mathrm{rk}_\le f_i = \mathrm{rk}_\le g_i$ $(1 \le i \le l)$. If $k = l$ and $\mathrm{rk}_\le f_i = \mathrm{rk}_\le g_i$ $(1 \le i \le k)$, then, by definition, $\mathrm{rk}_\le A = \mathrm{rk}_\le B$.

Any nonempty family of autoreduced sets contains an autoreduced set of the lowest rank [17, Chapter I, Section 10]. For a subset $X \subset \mathcal{K}\{U\}$, an autoreduced subset of X of the lowest rank is called a *characteristic set* of X. Clearly, all characteristic sets of X w.r.t. $\le$ have the same rank. An autoreduced set A is a characteristic set of X if and only if all nonzero elements of X are reducible w.r.t. A.

4 Riquier Rankings and Weight Vectors

A ranking is called a *Riquier ranking*, if for all $a, b \in \mathbb{N}^m$, $i, j \in \mathbb{N}_n$

$$(a,i) \leq (b,i) \iff (a,j) \leq (b,j)\,.$$

Note that $\mathbb{N}^m \times \mathbb{N}_n$ may be embedded into $\mathbb{N}^{n+m}$ as follows:

$$(i_1,\dots,i_m,j) \longmapsto (i_1,\dots,i_m,0,\dots,\overset{(m+j)}{1},\dots,0)\,.$$

Using this embedding, we can characterize Riquier rankings by matrices:

Theorem 1. *[11, Theorem 6] A Riquier ranking is a ranking $\leq$ for which there exists a positive integer s and an $s \times (m+n)$ real matrix M such that*

- *for $k = 1,\dots,m$, k^{th} column c_k of M satisfies $c_k \geq_{\text{lex}} (0,\dots,0)$;*
- *$(i_1,\dots,i_m,j) \leq (k_1,\dots,k_m,l)$ if and only if*

$$M\big(i_1,\dots,i_m,0,\dots,\overset{(m+j)}{1},\dots,0\big) \leq_{\text{lex}} M\big(k_1,\dots,k_m,0,\dots,\overset{(m+l)}{1},\dots,0\big)\,.$$

Vice versa, any $s \times (m+n)$ real matrix M of rank $m+n$ satisfying the above conditions defines a Riquier ranking $\leq_M$.

A vector $\mathbf{w} \in (\mathbb{R}^{m+n})^+$ is called a *weight vector*. For a derivative $\mathbf{u} = \delta_1^{i_1}\cdots\delta_m^{i_m}u_j$, the $\mathbf{w}$-*degree of* $\mathbf{u}$ is defined as the following inner product:

$$\deg_{\mathbf{w}} \mathbf{u} = \mathbf{w}\cdot(i_1,\dots,i_m,0,\dots,\overset{(m+j)}{1},\dots,0)\,.$$

For a differential monomial $\tau = c\prod_\alpha \mathbf{u}_\alpha \notin \mathcal{K}$, define

$$\deg_{\mathbf{w}} \tau = \max_\alpha \deg_{\mathbf{w}} \mathbf{u}_\alpha\,.$$

Let $f = \tau_1 + \ldots + \tau_k$ be a differential polynomial represented as a sum of differential monomials. Let $J = \{i_1,\dots,i_l\}$ be a subset of $\{1,\dots,k\}$ such that for all $j, j' \in J, i \in \{1,\dots,k\} \setminus J$,

$$\deg_{\mathbf{w}} \tau_j = \deg_{\mathbf{w}} \tau_{j'} > \deg_{\mathbf{w}} \tau_i\,.$$

We call differential polynomial

$$\operatorname{in}_{\mathbf{w}} f = \sum_{j\in J} \tau_j$$

the $\mathbf{w}$-*initial form* of f. In other words, $\operatorname{in}_{\mathbf{w}} f$ is the sum of all differential monomials present in f having the highest $\mathbf{w}$-degree.

For a subset $A \subset \mathcal{K}\{U\}$, define

$$\operatorname{in}_{\mathbf{w}} A = \{\operatorname{in}_{\mathbf{w}}(f) \mid f \in A\}\,.$$

A differential polynomial f is called $\mathbf{w}$-*homogeneous*, if $\operatorname{in}_{\mathbf{w}} f = f$; the $\mathbf{w}$-degree of a homogeneous polynomial f is defined to be equal to the $\mathbf{w}$-degree of any of its monomials. For an arbitrary polynomial f, define $\deg_{\mathbf{w}} f = \deg_{\mathbf{w}}(\operatorname{in}_{\mathbf{w}} f)$.

Below we formulate some properties of weight vectors and initial forms (proofs are omitted)

Lemma 1. *If $f, g \in \mathcal{K}\{U\}$ are two homogeneous polynomials such that $\deg_{\mathbf{w}} f = \deg_{\mathbf{w}} g$ and $f + g \neq 0$, then $f+g$ is homogeneous and $\deg_{\mathbf{w}}(f+g) = \deg_{\mathbf{w}} f$.*

Lemma 2. *Let* $f, h \in \mathcal{K}\{U\}$ *be two polynomials such that* $\deg_{\mathbf{w}} h < \deg_{\mathbf{w}} f$. *Then* $\mathrm{in}_{\mathbf{w}}(hf) = h\,\mathrm{in}_{\mathbf{w}} f$.

Lemma 3. *Let* $f \in \mathcal{K}\{U\}$ *be an arbitrary polynomial, and let* h *be a* $\mathbf{w}$*-homogeneous polynomial. Then*

$$\mathrm{in}_{\mathbf{w}}(hf) = \begin{cases} h\,\mathrm{in}_{\mathbf{w}} f, & \deg_{\mathbf{w}} h < \deg_{\mathbf{w}} f \\ hf, & \deg_{\mathbf{w}} h \geq \deg_{\mathbf{w}} f \end{cases} .$$

Lemma 4. *Let* $f \in \mathcal{K}\{U\}$ *and let* $\theta \in \Theta$. *Then*

$$\mathrm{in}_{\mathbf{w}}(\theta f) = \mathrm{in}_{\mathbf{w}}(\theta\,\mathrm{in}_{\mathbf{w}} f) .$$

A weight vector $\mathbf{w}$ and a ranking $\leq$ are *compatible*, if for all derivatives $t_1, t_2 \in \Theta U$, $\deg_{\mathbf{w}} t_1 < \deg_{\mathbf{w}} t_2$ implies $t_1 < t_2$.

Lemma 5. *If* $\leq$ *is a Riquier ranking such that the first row of* $M_{\leq}$ *is proportional to weight vector* $\mathbf{w}$*, then* $\mathbf{w}$ *and* $\leq$ *are compatible.*

Lemma 6. *[1, Lemma 2] If* $\mathbf{w}$ *is compatible with* $\leq$ *and* $f \in \mathcal{K}\{U\}$*, then*

$$\mathrm{ld}_{\leq} f = \mathrm{ld}_{\leq}(\mathrm{in}_{\mathbf{w}} f), \quad \mathrm{rk}_{\leq} f = \mathrm{rk}_{\leq}(\mathrm{in}_{\mathbf{w}} f), \quad \mathbf{i}_f = \mathbf{i}_{\mathrm{in}_{\mathbf{w}} f}, \quad \mathbf{s}_f = \mathbf{s}_{\mathrm{in}_{\mathbf{w}} f} .$$

5 The Step of the Differential Gröbner Walk

Let $\mathbf{w}$ be a weight vector whose first m components are strictly positive[1], and let $\leq, \leq'$ be two rankings compatible with $\mathbf{w}$. Let A be a characteristic set of a prime differential ideal I w.r.t. $\leq$. A single step of the differential Gröbner walk transforms A into a characteristic set A' of I w.r.t. $\leq'$. The algorithm takes advantage of the fact that both rankings are compatible with $\mathbf{w}$ and performs all reductions in $\mathrm{in}_{\mathbf{w}} I$; only the non-zero results of reductions are "lifted" to the ideal I. The algorithm also avoids splittings of the ideal I using the fact that I is prime and that membership in it can be checked, since a characteristic set of I is known.

Our algorithm is a modification of the Rosenfeld–Gröbner algorithm [4] which works not with characteristic sets but with regular systems of equations and inequalities. Below we introduce the corresponding definitions.

Let $\{f, g\}$ be two polynomials reduced w.r.t. each other (assume that $f > g$) such that $\mathrm{ld}_{\leq} f = \theta_1 u$, $\mathrm{ld}_{\leq} g = \theta_2 u$ for some $u \in U$, $\theta_1, \theta_2 \in \Theta$. Denote by θu the least common derivative of $\theta_1 u$ and $\theta_2 u$. The pair $\{f, g\}$ is called a *critical pair with parameter* θu and its Δ*-polynomial* is defined as

$$\Delta(f, g) = \mathbf{s}_g \frac{\theta}{\theta_1} f - \mathbf{s}_f \frac{\theta}{\theta_2} g .$$

For a set $A \subset \mathcal{K}\{U\}$, denote by $\Delta(A)$ the set of all Δ-polynomials of critical pairs formed by the elements of A. For two $\mathbf{w}$-homogeneous polynomials $\bar{f}$, $\bar{g}$, let $\Delta_{\mathbf{w}}(\bar{f}, \bar{g}) = \mathrm{in}_{\mathbf{w}} \Delta(\bar{f}, \bar{g})$.

Lemma 7. *Let* $\mathbf{w}$ *be a weight vector whose first* m *components are positive, and let* $\leq$ *be compatible with* $\mathbf{w}$. *Then for any* $p \in \mathcal{K}\{U\}$, $\theta \in \Theta$, $\theta \neq 1$, $\deg_{\mathbf{w}} \mathbf{s}_p < \deg_{\mathbf{w}} \theta p$.

Proof. By definition, $\mathbf{s}_p \leq \mathrm{ld}_{\leq} p$. If the first m components of $\mathbf{w}$ are positive and $\theta \neq 1$, then $\deg_{\mathbf{w}} \theta\,\mathrm{ld}_{\leq} p > \deg_{\mathbf{w}} \mathrm{ld}_{\leq} p$, which implies the statement of the lemma.

Lemma 8. *Let* $\leq$ *be compatible with* $\mathbf{w}$*, and let* $\bar{f} = \mathrm{in}_{\mathbf{w}} f$, $\bar{g} = \mathrm{in}_{\mathbf{w}} g$. *If* $\Delta_{\mathbf{w}}(\bar{f}, \bar{g}) \neq 0$*, then* $\Delta_{\mathbf{w}}(\bar{f}, \bar{g}) = \mathrm{in}_{\mathbf{w}} \Delta(f, g)$*, otherwise* $\deg_{\mathbf{w}} \Delta(f, g)$ *is less than* $\deg_{\mathbf{w}} v$*, where* v *is the parameter of the critical pair* $\{f, g\}$.

Proof. The statement follows from the definition of Δ-polynomial and Lemmas 7, 1, and 2.

[1] It will become clear later why we need this requirement. Usually this condition is satisfied for all weight vectors involved in the Gröbner walk; we conjecture that the case when some components are zero can also be treated efficiently, however, this requires some additional analysis of the entire Gröbner walk algorithm, which we leave for future research.

For a set $A \subset \mathcal{K}\{U\}$ and a derivative (or an arbitrary polynomial) v, let

$$A_{<v} = \{f \in A \mid f < v\}$$
$$A_{\leq v} = \{f \in A \mid f \leq v\}$$
$$A_{\deg_{\mathbf{w}} v} = \{f \in A \mid \deg_{\mathbf{w}} f \leq \deg_{\mathbf{w}} v\}.$$

We give two lemmas, which will allow us to work with the above sets.

Lemma 9. *Let $A, S \subset \mathcal{K}\{U\}$, and let $v \in \Theta U$. If $f \in ((\Theta A)_{\leq v}) : S^{\infty}_{<v}$, then for all $\theta \in \Theta$, $\theta f \in ((\Theta A)_{\leq \theta v}) : S^{\infty}_{<v}$.*

Proof. It is sufficient to prove the lemma for $\theta = \delta \in \Delta$, then the general case follows by induction on the order of θ.

Since $f \in ((\Theta A)_{\leq v}) : S^{\infty}$, there exist polynomials $p_i \in (\Theta A)_{\leq v}$, $h_i \in \mathcal{K}\{U\}$ ($i \in \{1, \dots, k\}$), $s \in S^{\infty}$ such that

$$sf = \sum_{i=1}^{k} h_i p_i .$$

Differentiating this equality, we obtain

$$\delta s \cdot f + s \cdot \delta f = \sum_{i=1}^{k} \delta h_i \cdot p_i + \sum_{i=1}^{k} h_i \cdot \delta p_i .$$

Multiplying by s and substituting the above sum for sf, we get

$$s^2 \delta f = -\delta s \sum_{i=1}^{k} h_i p_i + s \sum_{i=1}^{k} \delta h_i \cdot p_i + s \sum_{i=1}^{k} h_i \cdot \delta p_i ,$$

which implies that $\delta f \in ((\Theta A)_{\leq \delta v}) : S^{\infty}$.

Lemma 10. *Let $A = 0, S \neq 0$, $A \subset I$, be a system such that for all $g \in I$, $g \in ((\Theta A)_{\deg_{\mathbf{w}} g}) : S^{\infty}$.*

Let $f \in A$, and let $f' \in I$ be any polynomial such that $\operatorname{in}_{\mathbf{w}} f' = \operatorname{in}_{\mathbf{w}} f$. Then for $A' = A \setminus \{f\} \cup \{f'\}$ we also have that for all $g \in I$, $g \in ((\Theta A)_{\deg_{\mathbf{w}} g}) : S^{\infty}$.

Proof. It is sufficient to show that $f \in ((\Theta A')_{\deg_{\mathbf{w}} f}) : S^{\infty}$, then the proof for all $g \in I$ follows by applying Lemma 9.

Since $\operatorname{in}_{\mathbf{w}} f = \operatorname{in}_{\mathbf{w}} f'$, we have $\deg_{\mathbf{w}}(f - f') < \deg_{\mathbf{w}} f$. Hence,

$$f - f' \in ((\Theta(A \setminus \{f\}))_{\deg_{\mathbf{w}} g}) : S^{\infty} ,$$

which implies that $f \in ((\Theta A')_{\deg_{\mathbf{w}} f}) : S^{\infty}$.

A critical pair $\{f, g\}$ with parameter v is *solved* by a set $A \subset \mathcal{K}\{U\}$ if

$$\Delta(f, g) \in ((\Theta A)_{<v}) : (\mathbf{i}_A \cup \mathbf{s}_A)^{\infty} .$$

A set $A \subset \mathcal{K}\{U\}$ is called *coherent*, if all its critical pairs are solved by A.

A system of equations and inequalities $A = 0, S \neq 0$, where $A, S \subset \mathcal{K}\{U\}$, is called *regular* w.r.t. $\leq$, if A is autoreduced and coherent, $\mathbf{i}_A \cup \mathbf{s}_A \subset S$, and every element of S is partially reduced w.r.t. A. Regular system $A = 0, S \neq 0$ is called *regular for a prime ideal I*, if $I = [A] : S^{\infty}$.

If A is a characteristic set of a prime differential ideal I, then the system of equations and inequalities $A = 0, \mathbf{i}_A \cup \mathbf{s}_A \neq 0$ is regular for I. It is also possible to compute a characteristic set of a prime ideal I from a regular system for I by applying [4, Theorem 6].

A regular system for I allows to check membership in I as follows. Let X be the set of all derivatives present in $A \cup S$, and let $M(X)$ be the set of power products over X. Denote by $\tilde{\leq}$ the lexicographic ordering on $M(X)$, where the elements of X are ordered by ranking $\leq$. For a polynomial $f \in \mathcal{K}[X]$, denote by $\operatorname{lm}_{\leq} f$ the leading monomial of f w.r.t. $\tilde{\leq}$. Let B be the Gröbner basis of $(A) : S^{\infty}$ w.r.t. $\tilde{\leq}$; we call B the *Gröbner basis associated with regular system* $A = 0, S \neq 0$.

Lemma 11. *[4, Theorem 5] Let $A = 0, S \neq 0$ be a regular system for I, let B be the associated Gröbner basis, and let f be partially reduced w.r.t. A. Then $f \in I \iff f \in (B)$.*

Given a characteristic set of I, it is easy to obtain one for $\operatorname{in}_{\mathbf{w}} I$:

Lemma 12. *[1, Lemma 3] Let $\leq$ be a ranking and let $\mathbf{w}$ be compatible with $\leq$. Let A be a characteristic set for an ideal I w.r.t. $\leq$. Then $\operatorname{in}_{\mathbf{w}} A$ is a characteristic set of $\operatorname{in}_{\mathbf{w}} I$ w.r.t. $\leq$.*

The "lifting" of a characteristic set from $\operatorname{in}_{\mathbf{w}} I$ to I is also possible according to the following lemma.

Lemma 13. *Let $\leq$ be a ranking compatible with weight vector $\mathbf{w}$ whose first m components are positive. Let $A = 0, S \neq 0$ be a regular system for I w.r.t. $\leq$, and let B be the associated Gröbner basis.*

For every polynomial $\bar{f} \in \operatorname{in}_{\mathbf{w}} I$ one can compute polynomials $f \in ((\Theta A \cup B)_{\leq \bar{f}})$ and $s \in \mathbf{s}^{\infty}_{A\,<\bar{f}}$ such that $\operatorname{in}_{\mathbf{w}} f = s\bar{f}$ by applying the following algorithm:

Algorithm $\operatorname{in}_{\mathbf{w}}^{-1}(\bar{f}, A, B, \mathbf{w}, \leq)$
$f := 0, \quad s := 1$
while $\bar{f}$ is not partially reduced w.r.t. A **do**
let $p \in A$, $\theta \in \Theta$, $\theta \neq 1$, be such that
$\theta \operatorname{ld}_{\leq} p$ is present in $\bar{f}$ and has maximal possible rank.
let $\bar{f} = \operatorname{ld}_{\leq} p \cdot \bar{f}_1 + \bar{f}_2$, where $\bar{f}_2$ is free of $\operatorname{ld}_{\leq} p$.
$\bar{f} := \mathbf{s}_p \bar{f} - \operatorname{in}_{\mathbf{w}}(f_1 \theta p)$
$f := \mathbf{s}_p f + f_1 \theta p$
$s := s \cdot \mathbf{s}_p$
end while
while $\bar{f}$ is not polynomially reduced w.r.t. B **do**
let $q \in B$ be such that
monomial $\operatorname{lm}_{\tilde{\leq}} q$ is present in $\bar{f}$ and is maximal possible w.r.t. $\tilde{\leq}$.
let $\bar{f} = \operatorname{lm}_{\leq} q \cdot \bar{f}_1 + \bar{f}_2$, where $\bar{f}_2$ is free of $\operatorname{lm}_{\leq} q$.
$\bar{f} := \bar{f} - \operatorname{in}_{\mathbf{w}}(f_1 q)$
$f := f + f_1 q$
end while
if $\bar{f} \neq 0$ **then** the polynomial was not in $\operatorname{in}_{\mathbf{w}} I$
else return (f, s)
end

Proof. 1. *Termination.* The first **while** loop terminates, because with each iteration the rank of the highest derivative among the derivatives of leaders of A present in $\bar{f}$ decreases. The second **while** loop terminates, because with each iteration the greatest w.r.t. $\tilde{\leq}$ monomial among the leading monomials of B present in $\bar{f}$ decreases w.r.t. $\tilde{\leq}$.

2. *Correctness.* First, show that the final value of $\bar{f}$, $\bar{f}_t$, is 0 if and only if the initial value of $\bar{f}$, $\bar{f}_0$, is in $\operatorname{in}_{\mathbf{w}} I$. Indeed, according to Lemmas 1, 2, and 7, we have $\bar{f}_t \in \operatorname{in}_{\mathbf{w}} I \iff \bar{f}_0 \in \operatorname{in}_{\mathbf{w}} I$. Hence, if $\bar{f}_t = 0$, we immediately obtain $\bar{f}_0 \in \operatorname{in}_{\mathbf{w}} I$.
Assume that $\bar{f}_t \neq 0$ and show that $\bar{f}_t \notin \operatorname{in}_{\mathbf{w}} I$. Suppose the contrary, and let $f_t \in I$ be such that $\operatorname{in}_{\mathbf{w}} f_t = \bar{f}_t$. Note that $\operatorname{in}_{\mathbf{w}} f_t$ is partially reduced w.r.t. A (as a result of the first **while** loop) and reduced w.r.t. B (as a result of the second **while** loop). Hence, reductions w.r.t. A and B cannot decrease the $\mathbf{w}$-degree of f_t and, in particular, cannot reduce it to 0. According to Lemma 11, $f_t \notin I$, contradiction!
Second, assuming $\bar{f}_t = 0$, show that the constructed polynomials f and s satisfy the condition stated in the lemma, i.e., $\operatorname{in}_{\mathbf{w}} f = s\bar{f}$. Indeed, consider the first **while** loop and the two assignments in it for $\bar{f}$ and f. Let $\bar{f}_o$, f_o be the values of $\bar{f}$ and f before the assignments, and let $\bar{f}_n$, f_n be the corresponding values after the assignments. We have:

$$\bar{f}_n + f_n = \mathbf{s}_p(\bar{f}_o + f_o) + f_1 \theta p - \operatorname{in}_{\mathbf{w}}(f_1 \theta p)\,,$$

which implies that

$$\operatorname{in}_{\mathbf{w}}(\bar{f}_n + f_n) = \operatorname{in}_{\mathbf{w}}(\mathbf{s}_p(\bar{f}_o + f_o)) = \mathbf{s}_p \operatorname{in}_{\mathbf{w}}(\bar{f}_o + f_o)\,.$$

Now consider the second **while** loop and, for the two assignments in it, obtain

$$\mathrm{in}_{\mathbf{w}}(\bar{f}_n + f_n) = \mathrm{in}_{\mathbf{w}}(\bar{f}_o + f_o)\,.$$

Since the initial value of f and the final value of $\bar{f}$ are 0, we obtain the required statement.

Note that initial forms $\mathrm{in}_{\mathbf{w}}(f_1\theta p)$ and $\mathrm{in}_{\mathbf{w}}(f_1 q)$ in the above algorithm can be computed using the formulas from Lemma 3 and Lemma 4.

The above algorithm can also be used to check membership in $\mathrm{in}_{\mathbf{w}} I$. We call the corresponding algorithm as follows:

Algorithm Belongs $(\bar{f},\ A,\ B,\ \mathbf{w},\ \leq)$

A similar algorithm can be used to compute the partial remainder of $\bar{f}$ in $\mathrm{in}_{\mathbf{w}} I$ w.r.t. an autoreduced set $A \subset I$.

Algorithm PartialRem $(\bar{f},\ A,\ \mathbf{w},\ \leq)$
  while $\bar{f}$ is not partially reduced w.r.t. A **do**
    let $p \in A$, $\theta \in \Theta$, $\theta \neq 1$, be such that
      $\theta\,\mathrm{ld}_{\leq} p$ is present in $\bar{f}$ and has maximal possible rank.
    let $\bar{f} = \mathrm{ld}_{\leq} p \cdot f_1 + \bar{f}_2$, where $\bar{f}_2$ is free of $\mathrm{ld}_{\leq} p$.
    $\bar{f} := \mathbf{s}_p \bar{f} - \mathrm{in}_{\mathbf{w}}(f_1\theta p)$
    $f := \mathbf{s}_p f - f_1\theta p$ // This line is added only to facilitate the proof below
  end while
  return $\bar{f}$
end

For the proof of termination of the above algorithm see Lemma 13. Correctness is expressed by the following two lemmas, which will be used later in the proof of correctness of the differential Gröbner walk step.

Lemma 14. *Let* $\mathbf{w}$ *be a weight vector, and let* $\leq$ *be compatible with* $\mathbf{w}$.
Let $A = 0, S \neq 0$ *be a system such that for all* $g \in I$, $g \in ((\Theta A)_{\deg_{\mathbf{w}} g}) : S^{\infty}$.
Take any $f \in A$, *and let* $f' \in I$ *be such that*

$$\mathrm{in}_{\mathbf{w}} f' = \bar{f}' = \mathrm{PartialRem}(\mathrm{in}_{\mathbf{w}} f, A, \mathbf{w}, \leq)\,.$$

Then for $A' = (A \setminus \{f\}) \cup \{f'\}$, *we also have that for all* $g \in I$, $g \in ((\Theta A')_{\deg_{\mathbf{w}} g}) : S^{\infty}$.

Proof. It is sufficient to show that $f \in ((\Theta A')_{\deg_{\mathbf{w}} f}) : S^{\infty}$, after which the proof is completed by applying Lemma 9. Let f'' be the final value for f. Then, if $\bar{f}' \neq 0$, we have $\mathrm{in}_{\mathbf{w}} f'' = \bar{f}'$, otherwise $\deg_{\mathbf{w}} f'' < \deg_{\mathbf{w}} f$. In any case, $\deg_{\mathbf{w}}(f'' - f') < \deg_{\mathbf{w}} f$. Moreover, both $f', f'' \in I$, hence $f'' - f' \in I$. Since for all $g \in I$ we have $g \in ((\Theta A)_{\deg_{\mathbf{w}} g}) : S^{\infty}$, and since $\deg_{\mathbf{w}}(f'' - f') < \deg_{\mathbf{w}} f$, we have

$$f'' - f' \in ((\Theta(A \setminus \{f\}))_{\deg_{\mathbf{w}}(f'' - f')}) : S^{\infty}\,.$$

Hence,

$$f'' \in ((\Theta(A \setminus \{f\} \cup \{f'\}))_{\deg_{\mathbf{w}} f''}) : S^{\infty}\,,$$

which implies that $f \in ((\Theta A')_{\deg_{\mathbf{w}} f}) : S^{\infty}$.

Lemma 15. *If* $\mathrm{PartialRem}(\mathrm{in}_{\mathbf{w}} f, A, \mathbf{w}, \leq) = 0$, *then* f *can be partially reduced w.r.t.* A *in* I *to a polynomial* f' *such that* $\deg_{\mathbf{w}} f' < \deg_{\mathbf{w}} f$.

Proof. The proof of this lemma directly follows from the considerations in the proof of the previous one.

The computation of the full remainder w.r.t. A and $\leq$ in $\mathrm{in}_{\mathbf{w}} I$ may require some liftings to I (i.e. applications of $\mathrm{in}_{\mathbf{w}}^{-1}$), since we cannot guarantee that $\deg_{\mathbf{w}} \mathbf{i}_p < \deg_{\mathbf{w}} p$ for all $p \in A$. Therefore, this procedure also inputs the equations of a regular system $A_0 = 0, S_0 \neq 0$ w.r.t. another ordering $\leq_0$ compatible with $\mathbf{w}$ and the associated Gröbner basis B_0.

Algorithm FullRem ($\bar{f}$, A, $\mathbf{w}$, $\leq$, A_0, B_0, $\leq_0$)
  $\bar{f}$:=PartialRem($\bar{f}$, A, $\mathbf{w}$, $\leq$)
  repeat
    $R := \{p \in A \mid \mathrm{rk}_\leq p$ divides a monomial in $\bar{f}$ and $\deg_\mathbf{w} \mathbf{i}_p < \deg_\mathbf{w} \bar{f}\}$
    if $R \neq \varnothing$ **then**
      let $p \in A$ be such that
        $\mathrm{rk}_\leq p$ is present in $\bar{f}$ and has maximal possible rank.
      let $\bar{f} = \mathrm{rk}_\leq p \cdot f_1 + \bar{f}_2$, where $\bar{f}_2$ is free of $\mathrm{rk}_\leq p$.
      $\bar{f} := \mathbf{i}_p \bar{f} - \mathrm{in}_\mathbf{w}(f_1 p)$
    end if
  until $R = \varnothing$
  repeat
    $R := \{p \in A \mid \mathrm{rk}_\leq p$ divides a monomial in $\bar{f}$ and $\deg_\mathbf{w} \mathbf{i}_p \geq \deg_\mathbf{w} \bar{f}\}$
    if $R \neq \varnothing$ **then**
      let $p \in A$ be such that $\mathrm{rk}_\leq p$ is present in $\bar{f}$ and has maximal possible rank
      let $\bar{f} = \mathrm{rk}_\leq p \cdot f_1 + \bar{f}_2$, where $\bar{f}_2$ is free of $\mathrm{rk}_\leq p$
      $(f', s) := \mathrm{in}_\mathbf{w}^{-1}(\bar{f}, A_0, B_0, \mathbf{w}, \leq_0)$
      $\bar{f} := \mathbf{i}_p f' - s\, \mathrm{in}_\mathbf{w}(f_1 p)$
    end if
  until $R = \varnothing$
  return $\bar{f}$
end

The above algorithm terminates, because with each iteration of either **repeat** loop, the highest rank among the ranks of polynomials from A present in $\bar{f}$ decreases. Correctness is expressed by the following two lemmas, whose proof is similar to that of Lemma 14 and therefore is omitted.

Lemma 16. *Let* $\mathbf{w}$ *be a weight vector, let* $\leq$ *be compatible with* $\mathbf{w}$*.*
Let $A = 0, S \neq 0$ *be a system such that for all* $g \in I$*,* $g \in ((\Theta A)_{\deg_\mathbf{w} g}) : S^\infty$*.*
Take any $f \in A$*, and let* $f' \in I$ *be such that*

$$\mathrm{in}_\mathbf{w} f' = \bar{f}' = \mathrm{FullRem}(\mathrm{in}_\mathbf{w} f, A, \mathbf{w}, \leq, A_0, B_0, \leq_0)\,.$$

Then for $A' = (A \setminus \{f\}) \cup \{f'\}$*, we also have that for all* $g \in I$*,* $g \in ((\Theta A')_{\deg_\mathbf{w} g}) : S^\infty$*.*

Lemma 17. *If* $\mathrm{FullRem}(\mathrm{in}_\mathbf{w} f, A, \mathbf{w}, \leq, A_0, B_0, \leq_0)$*, then* f *can be reduced w.r.t.* A *in* I *to a polynomial* f' *such that* $\deg_\mathbf{w} f' < \deg_\mathbf{w} f$*.*

The following algorithm inputs any set of homogeneous polynomials $\bar{A}$, and for each $\bar{p} \in \bar{A}$ such that $\mathbf{i}_{\bar{p}}$ (or $\mathbf{s}_{\bar{p}}$) belongs to I, reduces $\bar{p}$ by its initial (or separant) and adds the initial form of the initial (separant) to $\bar{A}$. The resulting set consists of polynomials whose initials and separants do not belong to I. Again, we assume that a regular system $A_0 = 0, S_0 \neq 0$ for I w.r.t. $\leq_0$ and a the associated Gröbner basis B_0 are given.

Algorithm Add**is** ($\bar{A}$, $\mathbf{w}$, $\leq$, A_0, B_0, $\leq_0$)
  repeat
    $\bar{C} := \bar{A}$, $\bar{A} := \varnothing$
    for $\bar{f} \in \bar{C}$ **do**
      $(\bar{f}, \bar{D})$:=ReduceBy**is**($\bar{f}$,$\mathbf{w}$, $\leq$, A_0, B_0, $\leq_0$)
      $\bar{A} := \bar{A} \cup \{\bar{f}\} \cup \bar{D}$
    end for
  until $\bar{A} = \bar{C}$
  return $\bar{A}$
end

Algorithm ReduceBy**is** ($\bar{f}$, $\mathbf{w}$, $\leq$, A_0, B_0, $\leq_0$)
// In this algorithm, all initials and separants are taken w.r.t. $\leq$
$\bar{D} := \varnothing$
while Belongs($\mathrm{in}_{\mathbf{w}}\,\mathbf{i}_{\bar{f}}$, A_0, B_0, $\mathbf{w}$, $\leq_0$) **or** Belongs($\mathrm{in}_{\mathbf{w}}\,\mathbf{s}_{\bar{f}}$, A_0, B_0, $\mathbf{w}$, $\leq_0$) **do**
if Belongs($\mathrm{in}_{\mathbf{w}}\,\mathbf{i}_{\bar{f}}$, A_0, B_0, $\mathbf{w}$, $\leq_0$) **then** $\bar{D} := \bar{D} \cup \{\mathrm{in}_{\mathbf{w}}\,\mathbf{i}_{\bar{f}}\}$, $\bar{f} := \bar{f} - \mathbf{i}_{\bar{f}} \cdot \mathrm{rk}_{\leq} \bar{f}$
else $\bar{D} := \bar{D} \cup \{\mathrm{in}_{\mathbf{w}}\,\mathbf{s}_{\bar{f}}\}$, $\bar{f} := \deg_{\mathrm{ld}_{\leq} \bar{f}} \bar{f} \cdot \bar{f} - \mathrm{ld}_{\leq} \bar{f} \cdot \mathbf{s}_{\bar{f}}$
end while
return $(\bar{f}, \bar{D})$
end

Algorithm Add**is** terminates, because algorithm ReduceBy**is**, for any homogeneous polynomial $\bar{f}$, returns a set of polynomials $\{\bar{f}\} \cup \bar{D}$ which are strictly less w.r.t. $\leq$ than $\bar{f}$. Correctness follows from the following lemma:

Lemma 18. *Let* $\mathbf{w}$ *be a weight vector, and let* $\leq$ *be compatible with* $\mathbf{w}$*.*
Let $A = 0, S \neq 0$ *be a system such that for all* $g \in I$, $g \in ((\Theta A)_{\deg_{\mathbf{w}} g}) : S^{\infty}$*.*
Let $\bar{A}' =$Add**is**($\mathrm{in}_{\mathbf{w}} A$,$\mathbf{w}$,$\leq$,$A_0$,$B_0$,$\leq_0$)*, and let* A' *be any set such that* $\mathrm{in}_{\mathbf{w}} A' = \bar{A}'$*. Then for all* $g \in I$*, we also have* $g \in ((\Theta A')_{\deg_{\mathbf{w}} g}) : S^{\infty}$*.*

Proof. It is sufficient to show that if $f \in A$, $\bar{f} = \mathrm{in}_{\mathbf{w}} f$, $(\bar{f}', \bar{D})$ =ReduceBy**is**($\bar{f}$,A, B, $\mathbf{w}$, $\leq$, A_0, B_0, $\leq_0$), $\bar{A}' = \bar{A} \setminus \{\bar{f}\} \cup \{\bar{f}'\} \cup \bar{D}$, and $\mathrm{in}_{\mathbf{w}} A' = \bar{A}'$, then $f \in ((\Theta A')_{\deg_{\mathbf{w}} f}) : S^{\infty}$.

Moreover, it is sufficient to show that this invariant holds for each iteration of the **while** loop inside of the ReduceBy**is** algorithm. Indeed, if $\mathrm{in}_{\mathbf{w}}\,\mathbf{i}_{\bar{f}} \in \mathrm{in}_{\mathbf{w}} I$, then let

$$\bar{f}' = \bar{f} - \mathbf{i}_{\bar{f}} \cdot \mathrm{rk}_{\leq} \bar{f}$$
$$f'' = f - \mathbf{i}_{\bar{f}} \cdot \mathrm{rk}_{\leq} \bar{f}\,,$$

and let f' be any polynomial such that $\bar{f}' = \mathrm{in}_{\mathbf{w}} f'$. As in the proof of Lemma 14, we have $\deg_{\mathbf{w}}(f'' - f') < \deg_{\mathbf{w}} f$, which implies that $f'' \in ((\Theta(A \setminus \{f\} \cup \{f'\}))_{\deg_{\mathbf{w}} f''}) : S^{\infty}$ and

$$f \in ((\Theta(A \setminus \{f\} \cup \{f', \mathbf{i}_{\bar{f}}\}))_{\deg_{\mathbf{w}} f}) : S^{\infty}\,.$$

It remains to note that, according to Lemma 10, replacing $\mathbf{i}_{\bar{f}}$ by any other polynomial with the same $\mathbf{w}$-initial form does not change the above invariant. The case $\mathrm{in}_{\mathbf{w}}\,\mathbf{s}_{\bar{f}} \in \mathrm{in}_{\mathbf{w}} I$ is similar.

Theorem 2. *Let* $\leq$, $\leq'$ *be two rankings compatible with weight vector* $\mathbf{w}$*, whose first* m *components are positive. Given a characteristic set* A *of a prime differential ideal* I *w.r.t.* $\leq$ *and the associated Gröbner basis* B*, the following algorithm* DGWstep *computes a regular system* $C = 0, S \neq 0$ *for* I *w.r.t.* $\leq'$*.*

Algorithm DGWstep (A, B, $\mathbf{w}$, $\leq$, $\leq'$)
$A_0 := A$
$S_0 := \mathbf{i}_A \cup \mathbf{s}_A$ (here initials and separants are taken w.r.t. $\leq$)
$\bar{A} := \mathrm{in}_{\mathbf{w}} A$
repeat
$\bar{A}$:=Add**is**($\bar{A}$,$\mathbf{w}$,$\leq'$,A_0,B,$\leq$)
$\bar{C}$:=characteristic set of $\bar{A}$ w.r.t. $\leq'$
$S := S \cup \mathbf{i}_{\bar{C}} \cup \mathbf{s}_{\bar{C}}$
$C := \{\mathrm{in}_{\mathbf{w}}^{-1}(\bar{f}, A_0, B, \leq) \mid \bar{f} \in \bar{C}\}$
$\bar{R} := (\bar{A} \setminus \bar{C}) \cup \Delta_{\mathbf{w}}(\bar{C}, \leq')$
$\bar{R} := \{$FullRem($\bar{f}$,C,$\mathbf{w}$,$\leq'$,A_0,B,$\leq$) $\mid \bar{f} \in \bar{R}\} \setminus \{0\}$
$\bar{A} := \bar{C} \cup \bar{R}$
until $\bar{R} = \varnothing$
Autoreduce set C w.r.t. $\leq'$
Partially reduce the elements of S w.r.t. C and $\leq'$
return (C, S)
end

Proof. Termination is guaranteed by the fact that with each iteration the rank of $\bar{C}$ decreases. Indeed, reducing a polynomial by its initials and separants can only decrease the rank of the polynomial; hence, the rank of the characteristic set of $\bar{A}$ after the call to Add**is** is less than or equal to the rank of the characteristic set of $\bar{A}$ before this call. Furthermore, if $\bar{R}$ is a non-empty set of polynomials each of which is reduced w.r.t. $\bar{C}$, then the rank of the characteristic set of $\bar{C} \cup \bar{R}$ is strictly less than that of $\bar{C}$.

Let $C = 0, S \neq 0$ be the system constructed by the algorithm. Consider the last iteration of the loop in the DGWstep algorithm before termination. We have that all $\Delta_{\mathbf{w}}$-polynomials of $\bar{C}$ either are equal to 0 or can be reduced to 0 w.r.t. C and $\leq'$ in $\mathrm{in}_{\mathbf{w}} I$. Hence, according to Lemmas 8 and 17, every Δ-polynomial $f \in \Delta(C)$ reduces to a polynomial f' w.r.t. C and $\leq'$ in I, where $\deg_{\mathbf{w}} f' < \deg_{\mathbf{w}} v$ and v is the parameter of the critical pair corresponding to Δ-polynomial f. Therefore, we have $f \in ((\Theta(C \cup \{f'\})_{\leq' v}) : S^\infty$.

Since A is a characteristic set of I w.r.t. $\leq$, every polynomial from I reduces to 0 w.r.t. A and $\leq$. In particular, this implies that $f' \in ((\Theta A)_{\leq f'}) : S_0^\infty$. Since $\leq$ is compatible with $\mathbf{w}$, we have $f' \in ((\Theta A)_{\deg_{\mathbf{w}} f'}) : S_0^\infty$. Now, according to Lemmas 16 and 18, we also obtain that $f' \in ((\Theta C)_{\deg_{\mathbf{w}} f'}) : S^\infty$.

It remains to note that, since $\deg_{\mathbf{w}} f' < \deg_{\mathbf{w}} v$ and $\mathbf{w}$ is compatible with $\leq'$, we have

$$((\Theta C)_{\deg_{\mathbf{w}} f'}) : S^\infty \subset ((\Theta C)_{\leq' v}) : S^\infty ,$$

hence $f \in ((\Theta C)_{\leq' v}) : S^\infty$ and set C is coherent.

When we exit from the **repeat** loop, set $\bar{C}$ is autoreduced. Set C, which is obtained from $\bar{C}$ by applying the $\mathrm{in}_{\mathbf{w}}^{-1}$ operation, may not be autoreduced, but it has the same set of ranks as $\bar{C}$; moreover, for any $f \in C$, the initial of f does not belong to I, hence it cannot be reduced to 0 w.r.t. $C \setminus \{f\}$. Thus, autoreduction of C does not change its rank and, therefore, preserves its coherence.

By construction, $S \supset \mathbf{i}_C \cup \mathbf{s}_C$. The definition of regular system requires that S should be partially reduced w.r.t. C. This is achieved by partially reducing the elements of S w.r.t. C in I at the end of algorithm DGWstep; the validity of this reduction is justified in [2, Section 5]. Therefore, $C = 0, S \neq 0$ is a regular system for I w.r.t. $\leq'$.

To obtain a characteristic set of I w.r.t. $\leq'$ from the regular system $C = 0, S \neq 0$, one can apply the algorithm given in [4, Theorem 6]; as a by-product, this algorithm also computes the associated Gröbner basis, which will be necessary for the next step of the differential Gröbner walk.

6 The Walk

Let A_0 be a characteristic set of I w.r.t. Riquier ranking $\leq_0$ represented by matrix M_0 whose first row is weight vector $\mathbf{w}_0$, and let $\leq_t$ be the target ranking represented by matrix M_t. The walk consists of the following conversion steps.

First, let $\leq_1$ be the ranking defined by matrix $\begin{pmatrix} \mathbf{w}_0 \\ M_t \end{pmatrix}$. Since both $\leq_1$ and $\leq_0$ are compatible with $\mathbf{w}_0$ (due to Lemma 5), we can apply the step of the differential Gröbner walk and compute a characteristic set A_1 w.r.t. $\leq_1$.

Each next step is performed as follows. Suppose, we have computed the characteristic set A_i w.r.t. ranking $\leq_i$ defined by matrix $M_i = \begin{pmatrix} \mathbf{w}_{i-1} \\ M_t \end{pmatrix}$. Let $\mathbf{w}_i$ be the closest to $\mathbf{w}_{i-1}$ point in the semi-interval $(\mathbf{w}_{i-1}, \mathbf{w}_t]$ such that the leader of some differential polynomial in A_i and some other derivative present in that polynomial have the same $\mathbf{w}_i$-degrees. Since A_i is finite and every $f \in A_i$ involves finitely many derivatives, there are finitely many (or zero) possibilities for $\mathbf{w}_i$, so we can always choose the one that is the closest to $\mathbf{w}_{i-1}$. If such $\mathbf{w}_i$ does not exist, A_i already is a characteristic set w.r.t. $\leq_t$, and the algorithm stops. Otherwise, let $\leq'_i$ be the ranking defined by matrix $\begin{pmatrix} \mathbf{w}_i \\ M_i \end{pmatrix}$. Then $\leq'_i$ is compatible with $\mathbf{w}_i$.

Lemma 19. *[1, Lemma 5] A_i is a characteristic set of I w.r.t. $\leq'_i$.*

Let $\leq_{i+1}$ be the ranking defined by the matrix $\begin{pmatrix} \mathbf{w}_i \\ M_t \end{pmatrix}$. Applying the step of the differential Gröbner walk, compute a characteristic set A_{i+1} of I w.r.t. $\leq_{i+1}$. This concludes the conversion step.

7 Termination of the Differential Gröbner Walk

Consider characteristic sets of a given differential ideal I w.r.t. all possible rankings (here we do not need to restrict ourselves to Riquier rankings). For a fixed ranking, there may be infinitely many characteristic sets of I, but, as it follows directly from the definition, their ranks are equal. Since characteristic sets are autoreduced, this is equivalent to the statement that the sets of their leaders coincide. Formally, for a subset $A \subset \mathcal{K}\{U\}$, define the set of leaders of A as $\mathrm{ld}_{\leq}(A) = \{\mathrm{ld}_{\leq} f \mid f \in A\}$. If A_1, A_2 are characteristic sets of I w.r.t. $\leq$, then $\mathrm{ld}_{\leq}(A_1) = \mathrm{ld}_{\leq}(A_2)$. Let

$$\mathrm{Ld}(I) = \{\mathrm{ld}_{\leq}(A) \mid \leq \text{ be a ranking and } A \text{ be a characteristic set of } I \text{ w.r.t. } \leq\}.$$

In other words, $\mathrm{Ld}(I)$ is the family of sets of leaders of characteristic sets of I w.r.t. all possible rankings. In order to show that the differential Gröbner walk algorithm always terminates, we prove in this section that the family $\mathrm{Ld}(I)$ is finite.

Let $t_1, t_2 \in \Theta U$ be two derivatives. We say that t_2 *is a derivative of* t_1, if there exists $\theta \in \Theta$ such that $t_2 = \theta t_1$.

Lemma 20. *[17, Chapter 0, Lemma 15] Let $t_1, t_2, \ldots \subset \Theta U$ be an infinite sequence of derivatives. Then there exist indices $i < j$ such that t_j is a derivative of t_i.*

Theorem 3. *For any differential ideal $I \subset \mathcal{K}\{U\}$, family $\mathrm{Ld}(I)$ is finite.*

Proof. Suppose that $\mathrm{Ld}(I)$ is infinite. For each $L \in \mathrm{Ld}(I)$, denote by $\leq_L$ the corresponding ranking. Then the set $\Sigma = \{\leq_L \mid L \in \mathrm{Ld}(I)\}$ is infinite.

Let $f_1 \in I$ be a differential polynomial, and let $A_1 = \{f_1\}$. Since f_1 contains only a finite number of derivatives, according to the pigeonhole principle, there exists an infinite subset $\Sigma_1 \subset \Sigma$ such that for all $\leq, \leq' \in \Sigma_1$, $\mathrm{ld}_{\leq} f_1 = \mathrm{ld}_{\leq'} f_1$.

Suppose, A_1 is a characteristic set of I w.r.t. a ranking $\leq_1 \in \Sigma_1$. Then A_1 is also a characteristic set of I w.r.t. any ranking $\leq \in \Sigma_1$, since the reduction relations w.r.t. A_1 and any $\leq \in \Sigma_1$ coincide. However, this contradicts the definition of the set of rankings Σ, because characteristic sets corresponding to different rankings in Σ have different sets of leaders. Therefore, A_1 is autoreduced but not a characteristic set of I. Hence, there exists a polynomial $f_2 \in I$ reduced w.r.t. A_1 and any $\leq \in \Sigma_1$.

According to the pigeonhole principle, there exists an infinite subset $\Sigma_2 \subset \Sigma_1$ such that for all $\leq \in \Sigma_2$, the characteristic set of $A_1 \cup \{f_2\}$ is the same and the polynomials in it have the same leaders; call this characteristic set A_2.

The set A_2 cannot be a characteristic set of I for some $\leq \in \Sigma_2$ (according to the definition of Σ), hence there exists a polynomial $f_3 \in I$ reduced w.r.t. A_2 and any ranking $\leq \in \Sigma_2$.

According to the pigeonhole principle, there exists an infinite subset $\Sigma_3 \subset \Sigma_2$ such that for all $\leq \in \Sigma_3$, the characteristic set of $A_2 \cup \{f_3\}$ is the same and the polynomials in it have the same leaders; call this characteristic set A_3.

Proceeding in the same way, we construct an infinite sequence of polynomials $f_1, f_2, \ldots$, an infinite sequence of autoreduced sets $A_0, A_1, \ldots$, and an infinite sequence of sets of rankings $\Sigma_0 \supset \Sigma_1 \supset \ldots$. For each polynomial f_i, one of the following two options is possible:

1. For all $j > i$, $\mathrm{ld}_{\leq} f_j > \mathrm{ld}_{\leq} f_i$ ($\leq \in \Sigma_j$). In this case $f_i \in A_j$ for all $j \geq i$, and we say that f_i *remains in the sequence*.
2. There exists $j > i$ such that $\mathrm{ld}_{\leq} f_j < \mathrm{ld}_{\leq} f_i$ ($\leq \in \Sigma_j$). In this case we say that f_i *is followed by a smaller derivative*, and denote the smallest such j by $\nu(i)$.

Denote by $\nu^k(i)$ the expression $\nu(\nu(\ldots\nu(i)\ldots))$, where ν is applied k times.

Now we will construct a subsequence of $f_1, f_2, \ldots$ contradicting Lemma 20.

If f_1 remains in the sequence, let $i_1 = 1$. Otherwise, if $f_{\nu(1)}$ remains in the sequence, let $i_1 = \nu(1)$. Otherwise, if $f_{\nu^2(1)}$ remains in the sequence, let $i_1 = \nu^2(1)$, and so on. We will either find an index i_1 such that f_{i_1} remains in the sequence, or will construct an infinite sequence

$$f_1, f_{\nu(1)}, f_{\nu^2(1)}, \ldots$$

But the latter is not possible. Indeed, it follows from the definition of $\nu(i)$ that for all $i < j$, $\mathrm{ld}_{\leq} f_{\nu^j(1)} < \mathrm{ld}_{\leq} f_{\nu^i(1)}$ $(\leq \in \Sigma_{\nu^j(1)})$. Hence, $\mathrm{ld}_{\leq} f_{\nu^j(1)}$ is not a derivative of $\mathrm{ld}_{\leq} f_{\nu^i(1)}$, which contradicts Lemma 20.

If f_{i_1+1} remains in the sequence, let $i_2 = i_1 + 1$. Otherwise, if $f_{\nu(i_1+1)}$ remains in the sequence, let $i_2 = \nu(i_1+1)$, and so on. Applying the above argument, we show that the process will eventually stop and we will find an index i_2 such that f_{i_2} remains in the sequence.

Continuing in the same way, we obtain an infinite sequence of indices $i_1 < i_2 < \ldots$ such that for all j, f_{i_j} remains in the sequence. But the fact that both f_{i_j} and f_{i_k} $(i_j < i_k)$ remain in the sequence means that they both belong to the autoreduced set A_{i_k}, therefore $\mathrm{ld}_{\leq} f_{i_k}$ is not a derivative of $\mathrm{ld}_{\leq} f_{i_j}$ $(\leq \in \Sigma_{i_k})$. Thus we have constructed an infinite sequence of derivatives $\{\mathrm{ld}_{\leq_j} f_{i_j} \mid \leq_j \in \Sigma_{i_j}\}$, none of which is a derivative of another one. This contradicts Lemma 20.

During the differential Gröbner walk, we compute a sequence of characteristic sets $A_1, A_2, \ldots$ w.r.t. rankings $\leq_1, \leq_2, \ldots$, where $\leq_i$ are represented by matrices of the form $\begin{pmatrix} \mathbf{w}_{i-1} \\ M_t \end{pmatrix}$ $(i > 0)$, and $\{\mathbf{w}_i\}$ is a sequence of consecutive distinct points in the semi-interval $(\mathbf{w}_0, \mathbf{w}_t]$.

Theorem 4. *Sequences $A_1, A_2, \ldots$ and $\mathbf{w}_1, \mathbf{w}_2, \ldots$ are finite.*

Proof. The proof of this theorem is based on Theorem 3 and can be found in [1].

8 Example

We illustrate the differential Gröbner walk algorithm on an example from [2]. Consider differential ideal generated by the following polynomials: $u_x^2 - 4u,\ u_{xy}v_y - u + 1,\ v_{xx} - u_x$. This ideal is prime and, with respect to the following ranking on derivatives

$$\ldots >_0 v_{xx} >_0 v_{xy} >_0 v_{yy} >_0 u_{xx} >_0 u_{xy} >_0 u_{yy} >_0 v_x >_0 v_y >_0 u_x >_0 u_y >_0 v >_0 u\,,$$

has the following characteristic set:

$$v_{xx} - u_x,\ 4v_y u + u_x u_y - u_x u_y u,\ u_x^2 - 4u,\ u_y^2 - 2u\,.$$

We illustrate the performance of the differential Gröbner walk algorithm by transforming this characteristic set into the one w.r.t. the new ranking

$$\ldots >_t u_x >_t u_y >_t u >_t \ldots >_t v_{xx} >_t v_{xy} >_t v_{yy} >_t v_x >_t v_y > v\,.$$

Both rankings are Riquier rankings and can be specified by the following matrices:

$$M_0 = \begin{pmatrix} 1\,1\,0\,0 \\ 0\,0\,0\,1 \\ 0\,0\,1\,0 \\ 1\,0\,0\,0 \end{pmatrix}, \qquad M_t = \begin{pmatrix} 0\,0\,1\,0 \\ 0\,0\,0\,1 \\ 1\,1\,0\,0 \\ 1\,0\,0\,0 \end{pmatrix}.$$

Step 1. The first step of the Gröbner walk consists of transformation of the original set of polynomials into a regular set w.r.t. ranking $\leq_1$ specified by matrix

$$M_1 = \begin{pmatrix} 1\,1\,0\,0 \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \\ 1\,1\,0\,0 \\ 1\,0\,0\,0 \end{pmatrix}.$$

Note that $\leq_1$ is the same ordering as $\leq_0$ with the roles of differential indeterminates u and v exchanged. The transformation is carried out via the DGWstep algorithm, which works in the set of initial forms. However, in this example, in order to show explicitly how many reductions are saved by this algorithm compared to the standard Rosenfeld–Gröbner, we will perform all computations not with the initial forms but with the entire polynomials. Whenever a reduction decreases the **w**-degree of a polynomial, it implies that the same reduction would reduce the **w**-initial form of this polynomial to 0, and the following reductions are unnecessary (because they will produce 0 anyway). Also, the $\mathrm{in}_{\mathbf{w}}^{-1}$ algorithm needs not be applied, because we work directly with the entire polynomials, at the expense of computing their tails for each reduction.

Let set A consist of the original polynomials (whose ranks w.r.t. $\leq_1$ are underlined):

$$f_1 = \underline{v_{xx}} - u_x, \quad f_2 = u_y(1-u)\underline{u_x} + 4uv_y, \quad f_3 = \underline{u_x^2} - 4u, \quad f_4 = \underline{u_y^2} - 2u\,.$$

The characteristic subset of A is set $C = \{f_2, f_4\}$. Compute the reductions of polynomials in $(A \setminus C) \cup \Delta(C)$ w.r.t. C:

$$\begin{aligned} &f_3 \xrightarrow{f_2} u_x \xrightarrow{f_2} u_y^2 \xrightarrow{f_4} 2\underline{v_y^2} - u^2 + 2u - 1 = f_5 \\ &\Delta(f_2, f_4) = u_{yy} \xrightarrow{(f_4)_y} uu_y(u-1)\underline{v_{yy}} - v_y u_y^2 + 2v_y u - 2v_y u^2 = f_6 \\ &f_1 \xrightarrow{f_2} u_y(1-u)\underline{v_{xx}} + 4uv_y = f_7\,. \end{aligned}$$

In these reduction chains, for the intermediate polynomials, only ranks are shown; in what follows, the reducing polynomials above the reduction arrows will be omitted as well. Also, to obtain the above polynomial f_5, we have cancelled the content of the result of reduction (a polynomial factor that does not belong to the prime ideal); this operation requires polynomial factorization and, in general, may have a high complexity, however, it significantly simplifies the subsequent computations. Now add the results of reductions to the characteristic set, forming a new set $A = \{f_2, f_4, f_5, f_6, f_7\}$. Its characteristic subset is $C = \{f_2, f_4, f_5, f_7\}$. Reduce $(A \setminus C) \cup \Delta(C)$ w.r.t. C:

$$\begin{aligned} &f_6 \xrightarrow{!} u_y^2 \to v_y^2 \to 0 \\ &\Delta(f_5, f_7) = u_{xx} \to u_{xy} \to u_{yy} \to v_{xx} \to v_{xy}^2 \to v_{xy} \to v_{yy} \xrightarrow{!} u_x^2 \to u_x \to u_y^4 \to u_y^2 \to v_y^4 \to 0\,. \end{aligned}$$

The exclamation marks (!) indicate the first reductions that decrease the **w**-degree of the polynomials being reduced. Since all results of reductions are 0, C is a regular set w.r.t. $\leq_1$ (we are not interested in the set of inequalities at this point), and the first step of the differential Gröbner walk is completed (since we work with the entire polynomials and do not need to compute inverse initial forms, it is sufficient to have a regular system, and we do not even need to check whether C forms a characteristic set or not, in order to continue with the next step).

Steps 2 and 3. The closest weight vector to $(1,1,0,0)$ in the semi-interval $((1,1,0,0),(0,0,1,0)]$, such that the leader of some differential polynomial in C and some other derivative present in C have equal **w**-degrees, is $\mathbf{w}_1 = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 0)$. Set C is also a regular set w.r.t. the ranking defined by matrix M_1' obtained by appending M_1 to $\mathbf{w}_1$. The second step consists of computation of a regular set w.r.t. $\leq_2$ specified by matrix $M_2 = \begin{pmatrix} \mathbf{w}_1 \\ M_t \end{pmatrix}$ (we omit the details).

The next weight vector is $\mathbf{w}_2 = (\frac{1}{3}, \frac{1}{3}, \frac{2}{3}, 0)$, and we compute a regular set w.r.t. ranking $\leq_3$ defined by the corresponding matrix. As a result, we obtain the following set of polynomials:

$$-v_{yy}^2 + v_y v_{yy}\underline{v_{xy}} - 2v_y^2 + 1,\ -2v_y^2 + \underline{v_{yy}^4} - 2v_{yy}^2 + 1,\ \underline{v_{xx}} - 2v_{yy},\ -u + \underline{v_{yy}^2}\,.$$

Since the target ranking $\leq_t$ selects the same leaders in the above polynomials as $\leq_3$, they form a regular set w.r.t. $\leq_t$ as well.

The following table summarizes the performance of the differential Gröbner walk and the Rosenfeld–Gröbner algorithm on the above toy example:

Algorithm	# reductions	# nonzero normal forms
Diff. Gröbner walk	42	16
Rosenfeld-Gröbner	62	28

The number of reductions for both algorithms include the number of computations of Δ-polynomials; for the Gröbner walk algorithm the reductions that follow a **w**-degree-decreasing reduction (marked by '!') are not counted (the number of reductions saved in this way is 66). For the Rosenfeld-Gröbner, we applied the same algorithm as above for computing the characteristic set w.r.t. $\leq_t$ directly from that w.r.t. $\leq_0$; the details of this computation are omitted.

9 Conclusion and Open Problems

Our next goal is to implement the differential Gröbner walk algorithm presented here and compare its performance with that of the other algorithms (see [2, 3]) solving the problem of transformation of characteristic sets from one ranking to another. One can also generalize to the differential case various speed-up techniques known for the polynomial Gröbner walk [7, 18] (the version presented in this paper is in this sense a differential analogue of the original version of the polynomial Gröbner walk [8]).

Some theoretical improvements of the algorithm are also possible. For example, one would like to have an algorithm which transforms regular systems from one ranking to another without computing the associated Gröbner bases for the intermediate rankings (the Gröbner basis for the initial ranking is necessary for checking membership in the ideal).

Perhaps, a more difficult problem is to design an algorithm that, given a regular decomposition [4] or a characteristic decomposition [19] of an arbitrary radical differential ideal w.r.t. one ranking, transforms it to the corresponding decomposition w.r.t. another ranking. As it is shown in [19, Example 3.6], an ideal may be characterizable w.r.t. one ranking but not characterizable w.r.t. another. Thus, the decomposition may change, splittings seem to be unavoidable, and it is not obvious how to perform liftings of initial forms to the original ideal.

10 Acknowledgement

The author is sincerely thankful to Professor Carlo Traverso for the invitation to work in his group at the University of Pisa and for the financial support.

References

1. Golubitsky, O.: Transformation of characteristic sets from one ranking to another. In: Proceedings of 8th Rhine Workshop on Computer Algebra. Mannheim, Germany (2002) 225–236
2. Boulier, F., Lemaire, F., Maza, M.M.: PARDI! Publication LIFL 2001-01 (2001)
3. Boulier, F.: Efficient Computation of Regular Differential Systems by Change of Rankings Using Kähler Differentials. Tech. rep., Université Lille I (1999)
4. Boulier, F., Lazard, D., Ollivier, F., Petitot, M.: Representation for the Radical of a Finitely Generated Differential Ideal.In: Proc. ISSAC 1995, ACM Press (1995) 158–166
5. Faugére, J.C., Gianni, P., Lazard, D., Mora, T.: Efficient computation of zero-dimensional Gröbner bases by change of ordering. J. Symb. Comput. **16** (1993) 329–344
6. Amrhein, B., Gloor, O., Küchlin, W.: How fast does the walk run. In: Proc. of RWCA 1996 (1996)
7. Amrhein, B., Gloor, O., Küchlin, W.: Walking faster. In: Proc. DISCO 1996, Karlsruhe, Germany (1996)
8. Collart, S., Kalkbrener, M., Mall, D.: The Gröbner Walk. Dept. of Math., Swiss Federal Inst. of Tech, 8092 Zürich, Switzerland (1993)
9. Robbiano, L.: Term orderings on the polynomial ring. Proc. EUROCAL 1985, Linz, Austria (1985) 513–517
10. O'Shea, D.: Gröbner Fan and Walk. Springer-Verlag Electronic Production (2001)
11. Rust, C.J., Reid, G.J.: Rankings of partial derivatives. In: Proc. ISSAC 1997, W. Küchlin (Ed.), ACM Press, New York (1997) 9–16
12. Mora, T., Robbiano, L.: The Gröbner fan of an ideal. J. Symb. Comput. **6** (1988) 183–208
13. Weispfenning, V.: Differential term-orders. In: Proc. ISSAC 1993, M. Bronstein (Ed.), ACM Press, Kiev (1993)
14. Riquier, C.: Les systèmes d'équations aux dérivées partielles. Gauthier-Villars, Paris (1910)
15. Kondratieva, M.V., Levin, A.B., Mikhalev, A.V., Pankratiev, E.V.: Differential and Difference Dimension Polynomials. Klüver publishers (1999)
16. Ritt, J.: Differential Algebra. Dover (1950)
17. Kolchin, E.R.: Differential Algebra and Algebraic Groups. Academic Press, New York (1973)
18. Tran, Q.-N.: A fast algorithm for Gröbner basis conversion and its applications. J. Symb. Comput. **30** (2000) 451–467
19. Hubert, E.: Factorization-free decomposition algorithms in differential algebra. J. Symb. Comput. **29** (200) 641–662