# A Bound for Rosenfeld-Gröbner Algorithm [1]

Oleg Golubitsky [a,3] Marina Kondratieva [b] Marc Moreno Maza [c,4]
Alexey Ovchinnikov [d,2]

[a] *University of Western Ontario*
*Department of Computer Science*
*London, Ontario, Canada N6A 5B7*

[b] *Moscow State University*
*Department of Mechanics and Mathematics*
*Leninskie gory, Moscow, Russia, 119992*

[c] *University of Western Ontario*
*Department of Computer Science*
*London, Ontario, Canada N6A 5B7*

[d] *North Carolina State University*
*Department of Mathematics*
*Raleigh, NC 27695-8205, USA* [5]

**Abstract**

We consider the Rosenfeld-Gröbner algorithm for computing a regular decomposition of a radical differential ideal generated by a set of ordinary differential polynomials in $n$ indeterminates. For a set of ordinary differential polynomials $F$, let $M(F)$ be the sum of maximal orders of differential indeterminates occurring in $F$. We propose a modification of the Rosenfeld-Gröbner algorithm, in which for every intermediate polynomial system $F$, the bound $M(F) \leqslant (n-1)!M(F_0)$ holds, where $F_0$ is the initial set of generators of the radical ideal. In particular, the resulting regular systems satisfy the bound. Since regular ideals can be decomposed into characterizable components algebraically, the bound also holds for the orders of derivatives occurring in a characteristic decomposition of a radical differential ideal.

*Key words:* differential algebra, characteristic sets, radical differential ideals, decomposition into regular components
*1991 MSC:* 12H05, 13N10, 13P10

## 1. Introduction

This paper is about constructive differential algebra. We consider the following bounding problem in it. The input is a set $F$ of ordinary differential polynomials, that is, ordinary algebraic differential equations. The output is a **bound for orders** of all intermediate polynomials and the output of the Rosenfeld-Gröbner algorithm, which decomposes the radical differential ideal generated by $F$ into characterizable components.

So, our main result concerns algorithms dealing with algebraic differential equations. Many different problems can be attributed to this topic. One can, for instance, test membership to a radical differential ideal, compute the Kolchin dimensional polynomial. Generally, there are two radical differential ideal decomposition algorithms, although they have variations.

The Ritt-Kolchin algorithm (Ritt, 1950, Section V.5 for the ordinary differential case) and (Kolchin, 1973, Section IV.9 for the partial differential case) computes a prime decomposition of a radical differential ideal. This algorithm is based on the concept of characteristic set; it proceeds by computing a sequence of characteristic sets of decreasing rank and terminates because any such sequence is finite (Ritt, 1950, Section I.5), (Kolchin, 1973, Section I.10).

The Ritt-Kolchin algorithm also relies on the solution of the so-called factorization problem: given an autoreduced set, determine whether the corresponding algebraic saturated ideal is prime and, if it is not, find two polynomials outside the ideal whose product belongs to the ideal (Kolchin, 1973, Section IV.9, Problem (a)). Due to the complexity of the factorization problem, it was desirable to avoid it, which was accomplished by the Rosenfeld-Gröbner algorithm proposed in (Boulier et al., 1995). Instead of decomposing a given radical differential ideal into prime components, this algorithm represents it as an intersection of regular differential ideals (Boulier et al., 1995); the correctness of the algorithm, in addition to the above-mentioned theorems, is provided by the Lazard Lemma, which states that regular ideals are radical. Different proofs of this lemma can be found in (Boulier et al., 1997; Morrison, 1999; Hubert, 2000; Boulier et al., 2006).

The Rosenfeld-Gröbner algorithm is the first decomposition algorithm in differential algebra that has been actually implemented upto our knowledge. It forms an integral part of the `diffalg` package in the computer algebra system Maple. Updates of this package are available at `http://www-sop.inria.fr/cafe/Evelyne.Hubert/diffalg/`.

---

*Email addresses:* `oleg.golubitsky@gmail.com` (Oleg Golubitsky), `kondrmar@rol.ru` (Marina Kondratieva), `moreno@csd.uwo.ca` (Marc Moreno Maza), `aiovchin@math.uic.edu` (Alexey Ovchinnikov).

*URLs:* `http://publish.uwo.ca/~ogolubit/` (Oleg Golubitsky), `http://shade.msu.ru/~kondra_m/` (Marina Kondratieva), `http://www.csd.uwo.ca/~moreno/` (Marc Moreno Maza), `http://www.math.uic.edu/~aiovchin/` (Alexey Ovchinnikov).

[1] The work was partially supported by the Russian Foundation for Basic Research, project no. 05-01-00671.

[2] This author was also partially supported by NSF Grant CCR-0096842.

[3] This author was also partially supported by NSERC Grant PDF-301108-2004.

[4] This author was also partially supported by NSERC Grant RGPIN *Algorithms and software for triangular decompositions of algebraic and differential systems.*

[5] *Current address*: University of Illinois at Chicago, Department of Mathematics, Statistics, and Computer Science, 851 S. Morgan Street, Chicago, IL 60607-7045, USA

A more efficient implementation of this algorithm in C language by F. Boulier can be found at the website `http://www.lifl.fr/~boulier/BLAD/`.

Various improvements of the Rosenfeld-Gröbner algorithm have been proposed in (Boulier et al., 1997; Boulier, 1999; Boulier et al., 2001; Hubert, 2000, 2003, 2004; Bouziane et al., 2001). They all avoid the factorization problem and for this reason are called factorization-free. However, no theoretical bound for the computational complexity of any of these algorithms is known.

We make the first step towards the goal of estimating this complexity: we *bound the orders* of all differential polynomials appearing in the computations. The main results of this work are proven only for the **ordinary** case. In order to obtain our bound in Proposition 14, we have modified this algorithm (see Algorithms 3 and 5) a little bit. The main idea is to perform differential reduction very carefully. We do this in Algorithm 2. Then, Theorem 17 allows us to use *any* differential reduction and if the orders of polynomials increase too much we just *truncate* them (see Algorithm 4).

It would be good to have a bound that would tell us how many times we need to differentiate the original system in the beginning of the algorithm, so that the rest of the computation can be performed by a purely algebraic decomposition algorithm, for instance (Wang, 1993) or (Moreno Maza, 1999). Since for algebraic decomposition algorithms complexity estimates are known (see Szántó (1999)), such a bound would yield a complexity estimate for the differential decomposition as well. In this paper, however, we do not provide such a bound and, moreover, conjecture that it would have solved the Ritt problem (Ritt, 1950). We leave the discovery of such bound and/or the proof of this conjecture for future research.

The paper is organized as follows. We give an introduction into differential algebra in Section 2. Then we describe the original Rosenfeld-Gröbner algorithm in Section 3. Section 4 is devoted to the bound on the orders of derivatives computed by a modified version of the Rosenfeld-Gröbner algorithm.

## 2. Definitions and notation

Differential algebra studies systems of polynomial partial differential equations from the algebraic point of view. The approach is based on the concept of differential ring introduced by Ritt. Recent tutorials on the constructive theory of differential ideals are presented in (Boulier, 2000, 2006; Hubert, 2003; Sit, 2002). A differential ring is a commutative ring with the unity endowed with a set of derivations $\Delta = \{\delta_1, \ldots, \delta_m\}$, which commute pairwise. The case of $\Delta = \{\delta\}$ is called *ordinary*. If $R$ is an ordinary differential ring and $y \in R$, we denote $\delta^k y$ by $y^{(k)}$.

Construct the multiplicative monoid $\Theta = \left\{ \delta_1^{k_1} \delta_2^{k_2} \cdots \delta_m^{k_m} \mid k_i \geqslant 0 \right\}$ of *derivative operators*. Let $Y = \{y_1, \ldots, y_n\}$ be a set whose elements are called *differential indeterminates*. The elements of the set $\Theta Y = \{\theta y \mid \theta \in \Theta,\ y \in Y\}$ are called *derivatives*. Derivative operators from $\Theta$ act on derivatives as $\theta_1(\theta_2 y_i) = (\theta_1\theta_2)y_i$ for all $\theta_1, \theta_2 \in \Theta$ and $1 \leqslant i \leqslant n$.

The ring of *differential polynomials* in differential indeterminates $Y$ over a differential field $\mathbf{k}$ is a ring of commutative polynomials with coefficients in $\mathbf{k}$ in the infinite set of variables $\Theta Y$ (see Kolchin (1973); Kondratieva et al. (1999); Ritt (1950)). This ring is denoted $\mathbf{k}\{y_1, \ldots, y_n\}$ or $\mathbf{k}\{Y\}$. We consider the case of $\operatorname{char} \mathbf{k} = 0$ only. An ideal $I$ in $\mathbf{k}\{Y\}$ is called *differential*, if for all $f \in I$ and $\delta \in \Delta$, $\delta f \in I$. We denote differential polynomials by $f, g, h, \ldots$ and use letters $I, J, \mathfrak{p}$ for ideals.

Let $F \subset \mathbf{k}\{y_1, \ldots, y_n\}$ be a set of differential polynomials. For the differential and radical differential ideal generated by $F$ in $k\{y_1, \ldots, y_n\}$, we use notations $[F]$ and $\{F\}$, respectively. We need the notion of reduction for algorithmic computations. First, we introduce a *ranking* on the set of derivatives. A ranking (Kolchin, 1973) is a total order $>$ on the set $\Theta Y$ satisfying the following conditions for all $\theta \in \Theta$ and $u, v \in \Theta Y$:

(1) $\theta u \geqslant u$,

(2) $u \geqslant v \Longrightarrow \theta u \geqslant \theta v$.

Let $u$ be a derivative, that is, $u = \theta y_j$ for a derivative operator

$$\theta = \delta_1^{k_1} \delta_2^{k_2} \cdots \delta_m^{k_m} \in \Theta$$

and $1 \leqslant j \leqslant n$. The *order* of $u$ is defined as

$$\operatorname{ord} u = \operatorname{ord} \theta = k_1 + \ldots + k_m.$$

If $f$ is a differential polynomial, $f \notin \mathbf{k}$, then $\operatorname{ord} f$ denotes the maximal order of derivatives appearing effectively in $f$.

A ranking $>$ is called *orderly* if $\operatorname{ord} u > \operatorname{ord} v$ implies $u > v$ for all derivatives $u$ and $v$. A ranking $>_{el}$ is called an *elimination* ranking if $y_i >_{el} y_j$ implies $\theta_1 y_i >_{el} \theta_2 y_j$ for all $\theta_1, \theta_2 \in \Theta$. Let a ranking $>$ be fixed. The derivative $\theta y_j$ of the highest rank appearing in a differential polynomial $f \in \mathbf{k}\{y_1, \ldots, y_n\} \setminus \mathbf{k}$ is called the *leader* of $f$. We denote the leader by $\operatorname{ld} f$ or $\mathbf{u}_f$. The indeterminate $y_j$ is called the *leading variable* of $f$ and denoted by $\operatorname{lv} f$. Represent $f$ as a univariate polynomial in $\mathbf{u}_f$:

$$f = \mathbf{i}_f \mathbf{u}_f^d + a_1 \mathbf{u}_f^{d-1} + \ldots + a_d.$$

The monomial $\mathbf{u}_f^d$ is called the *rank* of $f$ and is denoted by $\operatorname{rk} f$. Extend the ranking relation on derivatives variables to ranks: $u_1^{d_1} > u_2^{d_2}$ if either $u_1 > u_2$ or $u_1 = u_2$ and $d_1 > d_2$.

The polynomial $\mathbf{i}_f$ is called the *initial* of $f$. Apply any $\delta \in \Delta$ to $f$:

$$\delta f = \frac{\partial f}{\partial \mathbf{u}_f} \delta \mathbf{u}_f + \delta \mathbf{i}_f \mathbf{u}_f^d + \delta a_1 \mathbf{u}_f^{d-1} + \ldots + \delta a_d.$$

The leader of $\delta f$ is $\delta \mathbf{u}_f$ and the initial of $\delta f$ is called the *separant* of $f$, denoted $\mathbf{s}_f$. If $\theta \in \Theta \setminus \{1\}$, then $\theta f$ is called a *proper derivative* of $f$. Note that the initial of any proper derivative of $f$ is equal to $\mathbf{s}_f$.

We say that a differential polynomial $f$ is *partially reduced* w.r.t. $g$ if no proper derivative of $\mathbf{u}_g$ appears in $f$. A differential polynomial $f$ is *algebraically reduced* w.r.t. $g$ if $\deg_{\mathbf{u}_g} f < \deg_{\mathbf{u}_g} g$. A differential polynomial $f$ is *reduced* w.r.t. a differential polynomial $g$ if $f$ is partially and algebraically reduced w.r.t. $g$. Consider any subset $\mathbb{A} \subset \mathbf{k}\{y_1, \ldots, y_n\} \setminus \mathbf{k}$. We say that $\mathbb{A}$ is autoreduced (respectively, algebraically autoreduced) if each element of $\mathbb{A}$ is reduced (respectively, algebraically reduced) w.r.t. all the others.

Every autoreduced set is finite (Kolchin, 1973, Chapter I, Section 9) (but an algebraically autoreduced set in a ring of differential polynomials may be infinite). For autoreduced sets we use capital letters $\mathbb{A}, \mathbb{B}, \mathbb{C}, \ldots$ and notation $\mathbb{A} = A_1, \ldots, A_p$ to specify the list of the elements of $\mathbb{A}$ arranged in order of increasing rank.

We denote the sets of initials and separants of elements of $\mathbb{A}$ by $\mathbf{i}_\mathbb{A}$ and $\mathbf{s}_\mathbb{A}$, respectively. Let $H_\mathbb{A} = \mathbf{i}_\mathbb{A} \cup \mathbf{s}_\mathbb{A}$. Let $S$ be a finite set of differential polynomials. Denote by $S^\infty$ the multiplicative set containing 1 and generated by $S$. Let $I$ be an ideal in a commutative

ring $R$. The *saturated ideal* $I : S^\infty$ is defined as $\{a \in R \mid \exists s \in S^\infty : sa \in I\}$. If $I$ is a differential ideal then $I : S^\infty$ is also a differential ideal (see Kolchin (1973)).

Consider two polynomials $f$ and $g$ in $\mathbf{k}\{y_1, \ldots, y_n\}$. Let $I$ be the differential ideal generated by $g$. Applying a finite number of pseudo-divisions, one can compute a *differential partial remainder* $f_1$ and a *differential remainder* $f_2$ of $f$ w.r.t. $g$ such that there exist $s \in \mathbf{s}_g^\infty$ and $h \in H_g^\infty$ satisfying $sf \equiv f_1$ and $hf \equiv f_2 \mod I$ with $f_1$ and $f_2$ partially reduced and reduced w.r.t. $g$, respectively (see Hubert (2000) for definitions and the algorithm for computing remainders). We denote by $\mathsf{d\text{-}rem}(f, \mathbb{A})$ the differential remainder of a polynomial $f$ w.r.t. an autoreduced set $\mathbb{A}$. Denote also

$$\mathsf{AlgebraicRemainder}\,(f, \mathbb{B}) = \{g \mid g \text{ alg. reduced w.r.t } \mathbb{B},\ hf - g \in (\mathbb{B}) \text{ for some } h \in \mathbf{i}_{\mathbb{B}}^\infty\},$$
$$\mathsf{DifferentialRemainder}\,(f, \mathbb{C}) = \{g \mid g \text{ reduced w.r.t. } \mathbb{C},\ hf - g \in [\mathbb{C}] \text{ for some } h \in H_{\mathbb{C}}^\infty\},$$

where $\mathbb{B}$ is algebraically autoreduced and $\mathbb{C}$ is differentially autoreduced.

Let $\mathbb{A} = A_1, \ldots, A_r$ and $\mathbb{B} = B_1, \ldots, B_s$ be (algebraically) autoreduced sets. We say that $\mathbb{A}$ has lower rank than $\mathbb{B}$ if

- there exists $k \leqslant r, s$ such that $\operatorname{rk} A_i = \operatorname{rk} B_i$ for $1 \leqslant i < k$, and $\operatorname{rk} A_k < \operatorname{rk} B_k$,
- or if $r > s$ and $\operatorname{rk} A_i = \operatorname{rk} B_i$ for $1 \leqslant i \leqslant s$.

We say that $\operatorname{rk} \mathbb{A} = \operatorname{rk} \mathbb{B}$ if $r = s$ and $\operatorname{rk} A_i = \operatorname{rk} B_i$ for $1 \leqslant i \leqslant r$.

The following notion of a characteristic set in characteristic zero is crucial in our further discussions. It was first introduced by Ritt for prime differential ideals, and then extended by Kolchin to arbitrary differential ideals.

**Definition 1** *(Ritt, 1950, Section I.5) An autoreduced subset of the lowest rank in a set $X \subset \mathbf{k}\{Y\}$ is called a characteristic set of $X$.*

A characteristic set exists for any set $X \subset \mathbf{k}\{Y\}$ due to the fact that every family of autoreduced sets contains one of the least rank (Kolchin, 1973, Section I.10, Proposition 3).

As it is mentioned in (Kolchin, 1973, Lemma 8, page 82), in the case of $\operatorname{char} \mathbf{k} = 0$, a set $\mathbb{A}$ is a characteristic set of a proper differential ideal $I$ if each element of $I$ reduces to zero w.r.t. $\mathbb{A}$. Moreover, the leaders and the correspondent degrees of these leaders of any two characteristic sets of $I$ coincide.

**Definition 2** *(Hubert, 2000, Definition 2.6) A differential ideal $I$ in $\mathbf{k}\{y_1, \ldots, y_n\}$ is said to be characterizable if there exists a characteristic set $\mathbb{A}$ of $I$ in Kolchin's sense such that $I = [\mathbb{A}] : H_{\mathbb{A}}^\infty$. We call any such characteristic set $\mathbb{A}$ a characterizing set of $I$.*

In other words, an ideal is characterizable if reduction to zero (by one of its characteristic sets) implies membership. As a consequence of the Lazard Lemma, characterizable ideals are radical (Hubert, 2000, Theorem 4.4).

## 3. Rosenfeld-Gröbner algorithm for the ordinary case

A system of ordinary differential equations and inequalities $\mathbb{A} = 0, H \neq 0$, where $\mathbb{A}, H \subset \mathbf{k}\{Y\}$, is called regular (see Boulier et al. (1995)), if $A$ is autoreduced, $H$ is partially reduced w.r.t. $\mathbb{A}$, and $H \supseteq H_{\mathbb{A}}$, where $H_{\mathbb{A}}$ is the set of initials and separants of elements of $\mathbb{A}$ (in the partial differential case it is also required that the set $\mathbb{A}$ is coherent, but in the ordinary case this condition holds for any autoreduced set $\mathbb{A}$). For a regular system $\mathbb{A} = 0, H \neq 0$, the differential ideal $[\mathbb{A}] : H^\infty$ is also called regular. Every regular ideal is radical (see Boulier et al. (1995)), and, according to the Rosenfeld

Lemma, $f \in [\mathbb{A}] : H^\infty$ if and only if the partial remainder of $f$ w.r.t. $\mathbb{A}$ belongs to the algebraic ideal $(\mathbb{A}) : H^\infty$.

The Rosenfeld-Gröbner algorithm proposed in (Boulier et al., 1995, 1997) computes a regular decomposition of a given radical differential ideal $\{F\}$, i.e., a representation

$$\{F\} = \bigcap_{i=1}^{k} [\mathbb{A}_i] : H_i^\infty,$$

where $[\mathbb{A}_i] : H_i^\infty$ are regular differential ideals.

We begin with the following version of the Rosenfeld-Gröbner algorithm. It is very similar to the original algorithm presented in (Boulier et al., 1995), except for the fact that we are in the ordinary case and need not deal with coherence. We also note that some of the regular systems computed by the version of the algorithm presented here may correspond to unit ideals; this can be checked later on by means of Gröbner basis computations as in (Boulier et al., 1995) or via polynomial GCD computations modulo regular chains as in (Boulier and Lemaire, 2000).

Finally, use the suggestion given in (Boulier et al., 1997, Section 5.5.2) and (Hubert, 2003, Improvements, page 73): it is recommended to reduce the multiplicative set $H$ of initials and separants. If it turns out that one of them reduces to zero, then the corresponding saturated component contains 1 and therefore need not be considered. We incorporate these ideas in Algorithm 1.

Given a set $F$ of differential polynomials, the Rosenfeld-Gröbner algorithm at first computes a characteristic set $\mathbb{C}$ of $F$, i.e., an autoreduced subset of $F$ of the least rank. It may happen that $\operatorname{lv} \mathbb{C} \subsetneq \operatorname{lv} F$ (for example, take $F = \{x + y, y\}$ w.r.t. a ranking such that $x > y$, then $\mathbb{C} = \{y\}$, $\operatorname{lv} \mathbb{C} = \{y\}$, and $\operatorname{lv} F = \{x, y\}$). In other words, inclusion $F_1 \subset F_2$ does not imply that for the corresponding characteristic sets $\mathbb{C}_1$ and $\mathbb{C}_2$, we have $\mathbb{C}_1 \subseteq \mathbb{C}_2$. We need the latter property, in order to obtain the bound, so we are going to relax the requirement that $\mathbb{C}$ is autoreduced.

A subset $\mathbb{C}$ of $\mathbf{k}\{Y\} \setminus \mathbf{k}$ is called a weak d-triangular set (Hubert, 2003, Definition 3.7), if the set of its leaders $\operatorname{ld} \mathbb{C}$ is autoreduced. In the ordinary case, $\mathbb{C}$ is a weak d-triangular set if and only if the leading differential indeterminates $\operatorname{lv} f$, $f \in \mathbb{C}$, are all distinct. A partially autoreduced weak d-triangular set is called d-triangular (Hubert, 2003, Definition 3.7). For a polynomial $f$ and a weak d-triangular set $\mathbb{C}$, the pseudo-remainder $\mathsf{d\text{-}rem}(f, \mathbb{C})$ is defined via (Hubert, 2003, Algorithm 3.13).

We will replace the reduction of $F$ w.r.t. an autoreduced set in the Rosenfeld-Gröbner algorithm by that w.r.t. a weak d-triangular set. We note that the version of the algorithm presented in (Hubert, 2003, Section 6) (Algorithms 6.8, 6.10, and 6.11) also computes differential pseudo-remainders w.r.t. weak d-triangular sets. Since the output regular systems must be partially autoreduced, at the very end, partial autoreduction of the weak d-triangular set $\mathbb{C}$ via (Hubert, 2003, Algorithm 6.8) is carried out.

Alternatively, one could perform partial autoreduction every time a weak d-triangular set is updated. In the following section, we show how to perform this autoreduction, as well as computation of differential pseudo-remainders, so that the inequality

$$M(F \cup H) \leqslant (n-1)! M(F_0 \cup H_0)$$

is preserved (see formulas (1) and (2) below).

**Algorithm 1** Rosenfeld-Gröbner$(F_0, H_0)$

INPUT: *finite sets of differential polynomials* $F_0, H_0$ *and a differential ranking*

OUTPUT: *a finite set* $T$ *of regular systems such that*

$$\{F_0\} : H_0^\infty = \bigcap_{(\mathbb{A},H)\in T} [\mathbb{A}] : H^\infty$$

$T := \varnothing, \quad U := \{(F_0, H_0)\}$

**while** $U \neq \varnothing$ **do**

*Take and remove any* $(F, H) \in U$

$\mathbb{C} :=$ *characteristic set of* $F$

$\bar{F} :=$ d-rem$(F \setminus \mathbb{C}, \mathbb{C}) \setminus \{0\}$

$\bar{H} :=$ d-rem$(H, \mathbb{C}) \cup H_{\mathbb{C}}$

**if** $\bar{F} \cap \mathbf{k} = \varnothing$ **and** $0 \notin \bar{H}$ **then**

**if** $\bar{F} = \varnothing$ **then** $T := T \cup \{(\mathbb{C}, \bar{H})\}$

**else** $U := U \cup \{(\bar{F} \cup \mathbb{C}, \bar{H})\}$

**end if**

**end if**

$U := U \cup \{(F \cup \{h\}, H) \mid h \in H_{\mathbb{C}},\ h \notin \mathbf{k} \cup H\}$

**end while**

**return** $T$

## 4. Modified Rosenfeld-Gröbner algorithm

For a set of differential polynomials $F$ we let

$$m_i(F) = \max_{f\in F} \operatorname{ord}_{y_i} f, \tag{1}$$

that is, $m_i(F)$ is the maximal order of the differential indeterminate $y_i \in Y$ occurring in the set $F$. If $y_i$ does not occur in $F$, we set $m_i(F) = 0$. Let

$$M(F) = \sum_{i=1}^{n} m_i(F). \tag{2}$$

We propose a modification of the Rosenfeld-Gröbner algorithm (see Algorithm 3 below), in which for every intermediate system $(F, \mathbb{C}, H) \in U$, the bound

$$M(F \cup \mathbb{C} \cup H) \leqslant (n-1)!M(F_0 \cup H_0) \tag{3}$$

holds, where $F_0 = 0, H_0 \neq 0$ is the input system of equations and inequalities corresponding to the radical differential ideal $\{F_0\} : H_0^\infty$.

In the formula (3) we have a factor $(n-1)!$. If the number of variables is equal to 1 or 2 it disappears. In the case of $n = 2$ Ritt proved the Jacobi bound for $|F_0| = 2$ and

empty $H_0$ by the direct computation and his result does not have any multiple either. Consider the intuition behind the case of $n \geqslant 3$ by looking at a particular example.

**Example 3** *Let $n \geqslant 3$ and $F_0 = x_1 + x_2 + \ldots + x_n$, ${x_1}'$ with the elimination ranking $x_1 > x_2 > \ldots > x_n$. Then $m_{x_1} = 1$, $m_{x_2} = \ldots = m_{x_n} = 0$ and*

$$M(F_0) = 1 + 0 + \ldots + 0 = 1.$$

*In order to find a characteristic set of the prime differential ideal $[F_0]$ we reduce $x_1'$ w.r.t. $x_1 + x_2 + \ldots + x_n$ and get $x_2' + \ldots + x_n'$. The output consists of two polynomials:*

$$\mathbb{C} = x_2' + \ldots + x_n', x_1 + x_2 + \ldots + x_n.$$

*We have: $m_{x_1}(\mathbb{C}) = 0$ and $m_{x_2}(\mathbb{C}) = \ldots = m_{x_n}(\mathbb{C}) = 1$. Hence,*

$$M(\mathbb{C}) = 0 + 1 + \ldots + 1 = n - 1 = (n-1)M(F_0).$$

*For this particular example, the algorithm stops here, so we obtain a factor of $(n-1)$. In general, further reductions might give new factors of $(n-2), (n-3), \ldots, 2, 1$, which would accumulate into $(n-1)!$. Unfortunately, we do not know an example where all these factors would actually appear, and therefore do not claim that the bound is sharp.*

### *4.1. Algebraic computation of differential remainders*

The Rosenfeld-Gröbner algorithm requires to compute differential pseudo-remainders $R = \mathsf{d\text{-}rem}(F \setminus \mathbb{C}, \mathbb{C})$. If the ranking on derivatives is not orderly, the orders of some (non-leading) derivatives may grow as a result of the differential pseudo-reduction, so that we may have $m_i(R) > m_i(F)$ for some $i \in \{1, \ldots, n\}$. To ensure a bound on $m_i(R)$, we construct a triangular set [6] $\mathbb{B}$, such that the computation of the differential pseudo-remainders $\mathsf{d\text{-}rem}(F, \mathbb{C})$ can be replaced by the computation of algebraic pseudo-remainders $\mathsf{algrem}(F, \mathbb{B})$, and, at the same time, $\mathbb{B}$ satisfies a bound on the orders of derivatives occurring in it.

For a set $\mathbb{B}$ of differential polynomials and a differential indeterminate $v \in \operatorname{lv} \mathbb{B}$, let

$$\mathbb{B}_v = \{f \in \mathbb{B} \mid \operatorname{lv} f = v\}.$$

Assume that $\mathbb{B}$ is algebraically triangular, which implies that for any non-empty subset $\mathbb{A} \subset \mathbb{B}$, elements of $\mathbb{A}$ of the minimal and maximal ranks are uniquely defined and denoted, respectively, $\min \mathbb{A}$ and $\max \mathbb{A}$. Define the following two subsets of $\mathbb{B}$:

$$\mathbb{B}^0 = \{\min \mathbb{B}_v \mid v \in \operatorname{lv} \mathbb{B}\}$$
$$\mathbb{B}^* = \{\max \mathbb{B}_v \mid v \in \operatorname{lv} \mathbb{B}\}.$$

Also, for a set $\{m_i\}_{i=1}^k$ of non-negative integer numbers and an arbitrary set $F$ of differential polynomials, let

$$F_{\{m_i\}} = \{f \in F \mid \operatorname{ord}_{y_i} f \leqslant m_i,\ i = 1, \ldots, k\}.$$

The following algorithm $\mathsf{Differentiate\&Autoreduce}$ (see Algorithm 2), which we are presenting, is quite a *technical tool* helping us to prove our bound. Before we prove its correctness and termination, let us discuss it informally. The triangular set $\mathbb{B}$ computed by the algorithm can be thought of as a result of an autoreduction of a *differential prolongation* of the input set $\mathbb{C} = \{C_1, \ldots, C_k\}$, i.e., of the set

$$\tilde{\mathbb{C}} = \{\delta^j C_i \mid 1 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant m_i - d_i\}.$$ [7]

[6] A set is called triangular if the leaders of its elements are distinct.

[7] Here $d_i$ is the degree of $\operatorname{rk} C_i = y_i^{d_i}$.

**Algorithm 2** Differentiate&Autoreduce($\mathbb{C}, \{m_i\}$)

INPUT: *a weak d-triangular set* $\mathbb{C} = C_1, \ldots, C_k$ *with* $\operatorname{ld}\mathbb{C} = y_1^{(d_1)}, \ldots, y_k^{(d_k)}$,
*and a set of non-negative integers* $\{m_i\}_{i=1}^k$, $m_i \geqslant m_i(\mathbb{C})$

OUTPUT: *set* $\mathbb{B} = \left\{ B_i^j \;\middle|\; 1 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant m_i - d_i \right\}$ *satisfying*

- $\operatorname{rk} B_i^j = \operatorname{rk} C_i^{(j)}$
- $B_i^j$ *are reduced w.r.t.* $\mathbb{C} \setminus \{C_i\}$
- $m_i(\mathbb{B}) \leqslant m_i$, $i = 1, \ldots, k$
- $m_i(\mathbb{B}) \leqslant m_i(\mathbb{C}) + \sum_{j=1}^k (m_j - d_j)$, $i = k+1, \ldots, n$
- $\mathbb{B} \subset \left[\mathbb{B}^0\right] \subset [\mathbb{C}] \subset [\mathbb{B}] : H_{\mathbb{B}}^\infty$
- $H_{\mathbb{B}} \subset H_{\mathbb{C}}^\infty + [\mathbb{C}], \quad H_{\mathbb{C}} \subset (H_{\mathbb{B}}^\infty + [\mathbb{B}]) : H_{\mathbb{B}}^\infty$

**or** $\{1\}$, *if it is detected that* $[\mathbb{C}] : H_{\mathbb{C}}^\infty = (1)$

1 $\mathbb{D} := \mathbb{C}$, $\mathbb{B} := \varnothing$
2 **while** $\mathbb{D} \cup (\delta\mathbb{B}^*)_{\{m_i\}} \neq \varnothing$ **do**
3 $f := \min\left(\mathbb{D} \cup (\delta\mathbb{B}^*)_{\{m_i\}}\right)$
4 **if** $f \in \mathbb{D}$ **then**
5 $\bar{f} := \mathsf{algrem}(f, \mathbb{B})$
6 $\mathbb{D} := \mathbb{D} \setminus \{f\}$
7 **else**
8 $\bar{f} := \mathsf{algrem}(f, \mathbb{B}^0 \cup (\delta\mathbb{B}^0 \setminus \{f\}))$
9 **end if**
10 **if** $\operatorname{rk}\bar{f} \neq \operatorname{rk} f$ **then return** $\{1\}$ **end if**
11 $\mathbb{B} := \mathbb{B} \cup \left\{\bar{f}\right\}$
12 **end while**
13 **return** $\mathbb{B}$

In particular, we have $\operatorname{rk}\mathbb{B} = \operatorname{rk}\tilde{\mathbb{C}}$, unless the autoreduction process cancels one of the initials, in which case we can show that $[\mathbb{C}] : H_{\mathbb{C}}^\infty = (1)$.

However, if one wants to make this autoreduction completely algebraic (in order to control the growth of orders), one has to be careful, because in the above set $\tilde{\mathbb{C}}$ there may appear derivatives of some $\operatorname{ld} C_i$ of order higher than those that appear in $\operatorname{ld}\tilde{\mathbb{C}}$, which cannot be canceled by an algebraic reduction. For example, if $\mathbb{C} = \{y_1, y_2 + y_1'\}$, $m_1 = 1$, $m_2 = 2$, and the ranking is elimination with $y_1 < y_2$, then

$$\tilde{\mathbb{C}} = \{y_1, y_1', y_2 + y_1', y_2' + y_1'', y_2'' + y_1'''\},$$

and in the last two polynomials derivatives $y_1'', y_1'''$ cannot be canceled by algebraic reduction w.r.t. $y_1$ and $y_1'$.

This problem is avoided by computing the elements of $\mathbb{B}$ in the order of increasing rank (which is ensured by line 3 of Algorithm 2). If the polynomials are added to $\mathbb{B}$

in this order, it is guaranteed that the algebraic pseudo-remainder $\bar{f}$ computed in line 5 or 8 does not contain any derivatives which could be reduced differentially, but not algebraically, w.r.t. the current set $\mathbb{B}$. For this reason, algebraic reductions are sufficient for computing $\mathbb{B}$. See Lemma 9 for the precise statement and proof of this fact.

In fact, only the *coefficients* of the polynomial $f$ are being reduced in lines 5 and 8 (that is, $\operatorname{ld} f$ is not among the leaders of the polynomials w.r.t. which it is being reduced; see Lemma 10 for the proof). That is, if $u = \operatorname{ld} f$ and

$$f = a_d u^d + \ldots + a_1 u + a_0,$$

where $a_0, \ldots, a_d$ are free of $u$, one could define

$$\mathsf{coeffAlgrem}\,(f, \mathbb{B}) = b_d u^d + \ldots + b_1 u + b_0,$$

where $b_0, \ldots, b_d$ are polynomials algebraically reduced w.r.t. $\mathbb{B}$ and satisfying

$$h a_i - b_i \in (\mathbb{B}), \qquad i = 0, \ldots, d$$

for some $h \in \mathbf{i}_{\mathbb{B}}^{\infty}$. Then lines 5 and 8 could be equivalently replaced with

5 $\quad \bar{f} = \mathsf{coeffAlgrem}\,(f, \mathbb{B})$

8 $\quad \bar{f} = \mathsf{coeffAlgrem}\,(f, \mathbb{B}^0 \cup \delta\mathbb{B}^0)$

**Example 4** *Let $f = y+x$ and $\mathbb{B} = tx+1$ in the polynomial ring $\mathbf{k}[t, x, y]$ with $t < x < y$. We have*

$$\mathsf{algrem}\,(f, \mathbb{B}) = t(y+x) - (tx+1) = ty - 1 \neq y - 1 = \mathsf{algrem}\,(1, \mathbb{B}) \cdot y + \mathsf{algrem}(x, \mathbb{B}).$$

We illustrate these considerations on the above *differential* example:

(1) Start with $\mathbb{B} = \varnothing$.
(2) Add $y_1$ to $\mathbb{B}$. We have $\mathbb{B}^0 = \{y_1\}$ and $\delta\mathbb{B}^0 = \{y_1'\}$.
(3) The algebraic pseudo-remainder of $y_1'$ w.r.t. $(\delta\mathbb{B}^0 \setminus \{y_1'\}) \cup \mathbb{B}^0$ is $y_1'$. Add it to $\mathbb{B}$.
(4) The algebraic pseudo-remainder of $y_2 + y_1'$ w.r.t. $(\delta\mathbb{B}^0 \setminus \{y_2\}) \cup \mathbb{B}^0$ is $y_2$. Add it to $\mathbb{B}$. We have $\mathbb{B}^0 = \{y_1, y_2\}$ and $\delta\mathbb{B}^0 = \{y_1', y_2'\}$.
(5) The algebraic pseudo-remainder of $y_2'$ w.r.t. $(\delta\mathbb{B}^0 \setminus \{y_2'\}) \cup \mathbb{B}^0$ is $y_2'$. Add it to $\mathbb{B}$.
(6) The algebraic pseudo-remainder of $y_2''$ w.r.t. $(\delta\mathbb{B}^0 \setminus \{y_2'\}) \cup \mathbb{B}^0$ is $y_2''$. Add it to $\mathbb{B}$.
(7) We obtain $\mathbb{B} = \{y_1, y_1', y_2, y_2', y_2''\}$.

Let us make an informal remark which may help an interested reader to cope with rather technical specifications of Algorithm 2. The following group of specifications:

- $\operatorname{rk} B_i^j = \operatorname{rk} C_i^{(j)}$,
- $\mathbb{B} \subset \left[\mathbb{B}^0\right] \subset [\mathbb{C}]$,
- $H_{\mathbb{B}} \subset H_{\mathbb{C}}^{\infty} + [\mathbb{C}]$,

implies that

$$\mathsf{AlgebraicRemainder}(f, \mathbb{B}) \subset \mathsf{DifferentialRemainder}(f, \mathbb{C}),$$

if the order of $f$ w.r.t. $y_i$ does not exceed $m_i$. This is the main property that allows us to use algebraic reduction in Algorithm 3 instead of the differential reduction in Algorithm 1. However, the remaining "inverse" inclusions

$$[\mathbb{C}] \subset [\mathbb{B}] : H_{\mathbb{B}}^{\infty}, \quad H_{\mathbb{C}} \subset (H_{\mathbb{B}}^{\infty} + [\mathbb{B}]) : H_{\mathbb{B}}^{\infty},$$

which are not taken into account by the above relationship between the algebraic and differential remainders, are also necessary for Algorithm 3 to be correct.[8] After the reduction, the orders of derivatives of $y_i$'s appearing in the remainder will not exceed $d_i$ for the leading $y_i$'s (i.e., for $1 \leqslant i \leqslant k$). For the non-leading $y_i$'s, the orders are bounded by the inequality

$$m_i(\mathbb{B}) \leqslant m_i(\mathbb{C}) + \sum_{j=1}^{k}(m_j - d_j), \quad i = k+1, \ldots, n. \tag{4}$$

We will use the following two auxiliary lemmas in the proof of correctness of algorithm Differentiate&Autoreduce.

**Lemma 5** *Let $\mathbb{C}$ be a weak d-triangular set in the ring of differential polynomials $\mathbf{k}\{Y\}$ with derivations $\Delta = \{\delta_1, \ldots, \delta_m\}$. Assume that a ranking on the set of derivatives $\Theta Y$ is fixed. Let $f \in \mathbf{k}\{Y\}$ be a differential polynomial with $\operatorname{ld} f \notin \Theta \operatorname{ld} \mathbb{C}$, and let $f \to_{\mathbb{C}} g$. Then*

- $\operatorname{rk} g < \operatorname{rk} f \;\Rightarrow\; \mathbf{i}_f \in [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$
- $\operatorname{rk} g = \operatorname{rk} f \;\Rightarrow\; \exists\, h \in H_{\mathbb{C}}^{\infty}$ *such that* $h \cdot \mathbf{i}_f - \mathbf{i}_g \in [\mathbb{C}]$, $h \cdot \mathbf{s}_f - \mathbf{s}_g \in [\mathbb{C}]$.

**Proof.** Let $\operatorname{rk} f = u^d$, and let $\mathbb{A} = \{p \in \Theta\mathbb{C} \mid \operatorname{ld} p < u\}$. Then for every $p \in \mathbb{A}$, $p$ and $\mathbf{i}_p$ are free of $u$. Since $f \to_{\mathbb{C}} g$ and $u \notin \Theta \operatorname{ld} \mathbb{C}$, there exist polynomials $h \in \mathbf{i}_{\mathbb{A}}^{\infty}$, $A_1, \ldots, A_k \in \mathbb{A}$ and $\alpha_a, \ldots, \alpha_k \in \mathbf{k}\{Y\}$ such that

$$h \cdot f = g + \sum_{i=1}^{k} \alpha_i A_i. \tag{5}$$

The maximal degree of $u$ present in (5) is equal to $d$. *Replace* every occurrence of $u^d$ by a new variable $v$, and consider (5) as an equality between two polynomials in $v$, in which polynomials $h, A_1, \ldots, A_k$ are free of $v$. We have therefore:

$$h \cdot \frac{df}{dv} = \frac{dg}{dv} + \sum_{i=1}^{k} \frac{d\alpha_i}{dv} A_i.$$

It remains to notice that $\frac{df}{dv} = \mathbf{i}_f$ and

$$\frac{dg}{dv} = \begin{cases} 0, & \operatorname{rk} g < \operatorname{rk} f \\ \mathbf{i}_g, & \operatorname{rk} g = \operatorname{rk} f \end{cases},$$

hence we obtain

- $\operatorname{rk} g < \operatorname{rk} f \;\Rightarrow\; \mathbf{i}_f \in (\mathbb{A}) : \mathbf{i}_{\mathbb{A}}^{\infty} \subset [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$.
- $\operatorname{rk} g = \operatorname{rk} f \;\Rightarrow\; h \cdot \mathbf{i}_f - \mathbf{i}_g \in (\mathbb{A}) \subset [\mathbb{C}]$, where $h \in \mathbf{i}_{\mathbb{A}}^{\infty} \subset H_{\mathbb{C}}^{\infty}$.

Consider now (5) as an equality between two polynomials in $u$, in which $h, A_1, \ldots, A_k$ are free of $u$. We have therefore:

$$h \cdot \frac{df}{du} = \frac{dg}{du} + \sum_{i=1}^{k} \frac{d\alpha_i}{du} A_i.$$

[8] These inclusions are necessary to justify the validity of reducing w.r.t. $\mathbb{B}$ *and* adding to $F$ the initials and separants of $f$, which is not an element of $\mathbb{B}$, but an element of $\bar{\mathbb{C}}$. The initials and separants of $\mathbb{B}$ cannot be added, because this may lead to an increase of the order of derivatives of non-leading differential indeterminates and prevent us from proving the bound.

It remains to notice that $\frac{df}{du} = \mathbf{s}_f$ and, if $\operatorname{rk} g = \operatorname{rk} f$, $\frac{dg}{du} = \mathbf{s}_g$, hence $h \cdot \mathbf{s}_f - \mathbf{s}_g \in (\mathbb{A}) \subset [\mathbb{C}]$, where $h \in \mathbf{i}_{\mathbb{A}}^{\infty} \subset H_{\mathbb{C}}^{\infty}$. $\square$

**Remark 6** *The above lemma also holds when the set of derivations $\Delta$ is empty, in which case $\mathbf{k}\{Y\} = \mathbf{k}[Y]$ is a ring of algebraic polynomials, $\mathbb{C} \subset \mathbf{k}[Y]$ is a triangular set, $\rightarrow_{\mathbb{C}}$ is the algebraic pseudo-reduction relation w.r.t. $\mathbb{C}$, and $[\mathbb{C}] = (\mathbb{C})$ is an ideal in $\mathbf{k}[Y]$.*

**Lemma 7** *(Hubert, 2003, Lemma 6.9) Let $H$ and $K$ be two sets of differential polynomials, and let $I$ be a differential ideal. If $K \subset (H^{\infty} + I) : H^{\infty}$, then $I : H^{\infty} = I : (H \cup K)^{\infty}$.*

The proof of specifications of Algorithm Differentiate&Autoreduce is divided into **three lemmas**. We will:

- first prove the statements about the ranks of the elements of $\mathbb{B}$,
- then about their orders, and
- finally, the inclusions.

All these statements hold *only* if the condition in line 10 is never satisfied, that is, throughout the algorithm $\operatorname{rk} \bar{f} = \operatorname{rk} f$; we assume this in the first two lemmas. In the third one, we will show that, if $\operatorname{rk} \bar{f} \neq \operatorname{rk} f$ for some $f$, then the ideal $[\mathbb{C}] : H_{\mathbb{C}}^{\infty}$ must be the unit ideal.

**Lemma 8** *(1) If the output $\mathbb{B}$ of Algorithm* Differentiate&Autoreduce *is not $\{1\}$, then it has the form*

$$\mathbb{B} = \left\{ B_i^j \;\middle|\; 1 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant m_i - d_i \right\},$$

*where $\operatorname{rk} B_i^j = \operatorname{rk} C_i^{(j)}$.*

*(2) Algorithm* Differentiate&Autoreduce *terminates.*

**Proof.** For $i = 1, \ldots, k$, let

$$\mu_i = \begin{cases} m_i(\operatorname{ld} \mathbb{B}) - d_i, & y_i \in \operatorname{lv} \mathbb{B} \\ -1, & \text{otherwise.} \end{cases}$$

The first statement follows from the following invariants of the **while**-loop:

$$-1 \leqslant \mu_i \leqslant m_i - d_i,\ i = 1, \ldots, k \tag{I1}$$

$$\mathbb{B} = \left\{ B_i^j \;\middle|\; 1 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant \mu_i \right\} \tag{I2}$$

$$\operatorname{rk} B_i^j = \operatorname{rk} C_i^{(j)},\ (1 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant \mu_i) \tag{I3}$$

$$\operatorname{lv} \mathbb{B} \cap \operatorname{lv} \mathbb{D} = \varnothing \tag{I4}$$

$$\mathbb{D} \subset \mathbb{C} \tag{I5}$$

$$\text{For all } f \in \mathbb{B}, g \in \mathbb{D}, \operatorname{rk} f < \operatorname{rk} g. \tag{I6}$$

One can check immediately that the above invariants hold at the beginning of the first iteration of the **while**-loop. Assume that we are at the beginning of some iteration and the invariants hold; show that they will also hold at the end of this iteration. Let $f$ be the polynomial computed in line 3, and let $y_i^{(d)} = \operatorname{ld} f$. We have **two cases**:

- $f \in \mathbb{D}$. By (I5) and the fact that the leading variables of the elements of $\mathbb{C}$ are distinct, we have $\operatorname{rk} f = \operatorname{rk} C_i$. By (I4) $\operatorname{lv} f \notin \operatorname{lv} \mathbb{B}$, whence by definition of $\mu_i$ we have $\mu_i = -1$. Since $\operatorname{rk} \bar{f} = \operatorname{rk} f$, at the end of the iteration we will have $B_i^0 = \bar{f}$ with $\operatorname{rk} B_i^0 = \operatorname{rk} C_i$, and $\mu_i = 0$. Thus, invariants (I1)–(I3) will hold.

Invariants (I4) and (I5) also continue to hold due to the assignments in lines 6 and 11 and the fact that sets $\mathbb{D}$ and $\mathbb{B}$ do not change elsewhere throughout the iteration of the **while**-loop. The choice of $f$ in line 3 and the assignment in line 6 also imply that at the end of the iteration we have $\operatorname{rk} \bar{f} = \operatorname{rk} f < \operatorname{rk} g$ for all $g \in \mathbb{D}$, whence invariant (I6) is preserved.

- $f \in (\delta\mathbb{B}^*)_{\{m_i\}}$. By (I2) and (I3), $\mu_i \geqslant 0$ and $\operatorname{rk} f = \operatorname{rk} C_i^{(\mu_i+1)}$. Hence, at the end of the iteration $\mu_i$ increases by one, while $\bar{f}$ with $\operatorname{rk} \bar{f} = \operatorname{rk} f$ is added to $\mathbb{B}$, thus preserving invariants (I1)–(I3). Note also that $\operatorname{lv} f \in \operatorname{lv} \mathbb{B}$, whence $\operatorname{lv} \mathbb{B}$ is preserved as well. Hence, due to the fact that $\mathbb{D}$ remains unchanged throughout the iteration, invariants (I4) and (I5) are preserved. The facts that $\operatorname{rk} \bar{f} = \operatorname{rk} f \leq \operatorname{rk} g$ for all $g \in \mathbb{D}$ (due to the choice of $f$ in line 3) and that $\operatorname{lv} \bar{f} \notin \operatorname{lv} \mathbb{D}$ (due to (I4)) implies preservation of (I6) at the end of the iteration.

The above also proves the **termination** of the algorithm: at each iteration exactly one of the $\mu_i$ is incremented, whence the number of iterations does not exceed

$$\sum_{i=1}^{k} (m_i - d_i + 1).$$

□

**Lemma 9** *If the output $\mathbb{B}$ of Algorithm* Differentiate&Autoreduce *is not $\{1\}$, then*
*(1) The elements $B_i^j$ of $\mathbb{B}$ are reduced w.r.t. $\mathbb{C} \setminus \{C_i\}$,*
*(2) $m_i(\mathbb{B}) \leqslant m_i$, $i = 1, \ldots, k$,*
*(3) $m_s(\mathbb{B}) \leqslant m_s(\mathbb{C}) + \sum_{t=1}^{k} (m_t - d_t)$, $s = k+1, \ldots, n$.*

**Proof.** The first two statements are implied by the fact that $m_i(\operatorname{rk} \mathbb{B}) \leqslant m_i$, $i = 1, \ldots, k$, which is a consequence of Lemma 8, and the following invariants:

$$m_t\left(B_i^j\right) \leqslant d_t, \ (1 \leqslant i \neq t \leqslant k, \ 0 \leqslant j \leqslant \mu_i) \tag{I7}$$

$$B_i^j \text{ are differentially reduced w.r.t. } \mathbb{B}^0 \setminus \left\{B_i^0\right\} \tag{I8}$$

The invariants hold at the beginning of the first iteration of the **while**-loop, since $\mathbb{B} = \varnothing$. Assume that they hold at the beginning of some iteration; show that they will hold at the end of this iteration as well. We have **two cases**:

- $f \in \mathbb{D}$. Let us show that

$$m_t(f) \leqslant d_t + \mu_t, \quad y_t \in \operatorname{lv} \mathbb{B}. \tag{6}$$

The fact that $y_t \in \operatorname{lv} \mathbb{B}$, according to (I3), implies $\mu_t \geqslant 0$. We may assume that $y_t$ is present in $f$: otherwise $m_t(f) = 0$ and (6) will trivially hold due to the fact that $d_t \geqslant 0$ and $\mu_t \geqslant 0$. According to (I1), two cases are possible:

(1) $0 \leqslant \mu_t < m_t - d_t$. Then there exists a polynomial $g \in (\delta\mathbb{B})^*_{\{m_i\}}$ with $\operatorname{lv} g = y_t$. By (I3), $\operatorname{ld} g = y_t^{(d_t+\mu_t+1)}$. Since, due to (I4), $y_t$ cannot be the leading variable of $f$, yet $y_t$ is present in $f$, $y_t^{(m_t(f))} < \operatorname{ld} f$. Since $f$ is an element of $\mathbb{D} \cup (\delta\mathbb{B})^*_{\{m_i\}}$ of the least rank, $\operatorname{ld} f \leq \operatorname{ld} g$. Combining these statements, we obtain

$$y_t^{(m_t(f))} < \operatorname{ld} f \leq \operatorname{ld} g = y_t^{(d_t+\mu_t+1)},$$

which implies (6).

(2) $\mu_t = m_t - d_t$. Then, due to (I5) and the condition on the input $\mathbb{C}$ we have $m_t(f) \leqslant m_t$, which yields (6).

Inequality (6) and invariant (I7) imply that the algebraic remainder $\bar{f}$ computed in line 5 is differentially reduced w.r.t. $\mathbb{B}^0$ and satisfies

$$m_t\left(\bar{f}\right) \leqslant d_t, \quad y_t \in \operatorname{lv}\mathbb{B}. \tag{7}$$

Note also that due to (I6), $\mathbb{B}$ is differentially reduced w.r.t. $\bar{f}$. Thus, invariant (I8) also holds at the end of the iteration. Taking into account that for all $g \in \mathbb{D}$ we have $\operatorname{rk}\bar{f} = \operatorname{rk} f \leqslant \operatorname{rk} g$, we obtain

$$m_t\left(\bar{f}\right) \leqslant d_t, \quad y_t \in \operatorname{lv}\mathbb{D}. \tag{8}$$

Together inequalities (7) and (8) yield invariant (I7) at the end of the iteration.

- $f \in (\delta\mathbb{B}^*)_{\{m_i\}}$. By (I7), $m_t(f) \leqslant d_t + 1$, for $t$ such that $y_t \in \operatorname{lv}\mathbb{B} \setminus \{\operatorname{lv} f\}$. This inequality and invariant (I7) imply that the algebraic remainder $\bar{f}$ computed in line 8 is differentially reduced w.r.t. $\mathbb{B}^0 \setminus \{B_i^0\}$ and satisfies $m_t(\bar{f}) \leqslant d_t$. Thus, we obtain that invariants (I7) and (I8) also holds at the end of the iteration.

Finally, we prove the **bound for the orders** of non-leading derivatives in the output:

$$m_s(\mathbb{B}) \leqslant m_s(\mathbb{C}) + \sum_{t=1}^{k}(m_t - d_t), \quad s = k+1, \ldots, n.$$

This bound holds due to the following invariant:

$$m_s(\mathbb{B}) \leqslant m_s(\mathbb{C}) + \sum_{\{t:\mu_t \geqslant 0\}} \mu_t, \quad s = k+1, \ldots, n. \tag{9}$$

Assume that (9) holds at the beginning of an iteration, and let $s \in \{k+1, \ldots, n\}$. We then have:

(1) If $f \in \mathbb{D}$, no differentiations occur during the iteration and the sum remains unchanged, whence (9) is preserved.

(2) If $f \in (\delta\mathbb{B}^*)_{\{m_i\}}$, then $f = \delta g$ for some $g \in \mathbb{B}$, whence $m_s(f) \leqslant m_s(\mathbb{B})+1$. Similarly,

$$m_s\left(\mathbb{B}^0 \cup \delta\mathbb{B}^0\right) \leqslant m_s(\mathbb{B}) + 1.$$

Thus, according to line 8, $m_s\left(\bar{f}\right) \leqslant m_s(\mathbb{B}) + 1$, and so at the end of the iteration $m_s(\mathbb{B})$ is increased at most by one. At the same time, as was shown in Lemma 8, Case 2, exactly one of the $\mu_i$ is incremented, whereby the sum in (9) increases by 1. Thus, (9) is preserved.

□

**Lemma 10** *If the output $\mathbb{B}$ of Algorithm* Differentiate&Autoreduce *is not $\{1\}$, then the inclusions*

$$\mathbb{B} \subset [\mathbb{B}^0] \subset [\mathbb{C}] \subset [\mathbb{B}] : H_{\mathbb{B}}^{\infty}, \quad H_{\mathbb{B}} \subset H_{\mathbb{C}}^{\infty} + [\mathbb{C}], \quad H_{\mathbb{C}} \subset (H_{\mathbb{B}}^{\infty} + [\mathbb{B}]) : H_{\mathbb{B}}^{\infty}$$

*hold, otherwise ideal $[\mathbb{C}] : H_{\mathbb{C}}^{\infty}$ is the unit ideal.*

**Proof.** The inclusions are implied by the following invariants:

$$\mathbb{B} \subset \left[\mathbb{B}^0\right] \subset [\mathbb{C}] \tag{I9}$$
$$H_{\mathbb{B}} \subset H_{\mathbb{C}}^{\infty} + [\mathbb{C}] \tag{I10}$$
$$\mathbb{C} \setminus \mathbb{D} \subset [\mathbb{B}] : H_{\mathbb{B}}^{\infty} \tag{I11}$$
$$H_{\mathbb{C}\setminus\mathbb{D}} \subset (H_{\mathbb{B}}^{\infty} + [\mathbb{B}]) : H_{\mathbb{B}}^{\infty} \tag{I12}$$

The invariants hold at the beginning of the first iteration of the **while**-loop, since $\mathbb{B} = \varnothing$ and $\mathbb{D} = \mathbb{C}$. Assume that they hold at the beginning of some iteration; show that either the algorithm terminates at this iteration with the output $\{1\}$ or the invariants will hold at the end of this iteration. We have **two cases**:

- $f \in \mathbb{D}$. Then by (I5) $f \in \mathbb{C}$. Since $\bar{f} = \mathsf{algrem}(f, \mathbb{B})$, we have $\bar{f} \in (\mathbb{B} \cup \{f\})$. Then, according to (I9), $\bar{f} \in [\mathbb{C}]$. As was shown in Lemma 8, Case 1, $\bar{f}$ is added to $\mathbb{B}^0$ in line 11, thus preserving (I9). Next, due to (I4), $\operatorname{ld} f \notin \operatorname{ld} \mathbb{B}$. Thus, Lemma 5 (see also Remark 6) applies to the algebraic remainder computed in line 5. We conclude from it that
$$\operatorname{rk} \bar{f} \neq \operatorname{rk} f \;\;\Rightarrow\;\; \mathbf{i}_f \in [\mathbb{B}] : H_{\mathbb{B}}^{\infty}. \tag{10}$$
We will use this statement later to justify the output $\{1\}$, in case the condition in line 10 is satisfied. For now, assume that $\operatorname{rk} \bar{f} = \operatorname{rk} f$. Then, from Lemma 5, we also have:
$$H_{\bar{f}} \subset H_f \cdot H_{\mathbb{B}}^{\infty} + (\mathbb{B}).$$
Since $f \in \mathbb{C}$, and due to invariants (I9) and (I10), we thus obtain $H_{\bar{f}} \subset H_{\mathbb{C}}^{\infty} + [\mathbb{C}]$. This means that (I10) is also preserved. By definition of the algebraic remainder,
$$f \in \left(\mathbb{B} \cup \left\{\bar{f}\right\}\right) : H_{\mathbb{B}}^{\infty}.$$
Note that line 6 results in adding $f$ to the set $\mathbb{C} \setminus \mathbb{D}$, and this set is not changed elsewhere throughout the iteration. Thus, at the end of the iteration (I11) will hold. Finally, as yet another consequence of Lemma 5,
$$H_f \subset \left(H_{\bar{f}} + (\mathbb{B})\right) : H_{\mathbb{B}}^{\infty}.$$
Taking into account that $\mathbb{C} \setminus \mathbb{D}$ does not change other than in line 6, we thus obtain (I12) at the end of the iteration.
- $f \in \delta\mathbb{B}^*_{\{m_i\}}$. As was shown in Lemma 8, Case 2, $\mathbb{B}^0$ remains unchanged during the iteration in this case. By (I9), $f \in [\mathbb{B}^0]$, whence by definition of the algebraic remainder applied to line 8 we have
$$\bar{f} \in \left(\mathbb{B}^0 \cup \delta\mathbb{B}^0 \cup f\right) \subset \left[\mathbb{B}^0\right].$$
Thus, (I9) is preserved. Next, according to (I2) and (I3), all elements of $\mathbb{B}$, and, hence, all elements of $\delta\mathbb{B}$, have distinct leaders. In particular, if $\operatorname{ld} f \in \operatorname{ld} \delta\mathbb{B}^0$, then $f \in \delta\mathbb{B}^0$, whence $\operatorname{ld} f \notin \operatorname{ld}\left(\delta\mathbb{B}^0 \setminus \{f\}\right)$. In addition, since $f \in \delta\mathbb{B}$, and due to (I2) and (I3), we have $\operatorname{ld} f \notin \operatorname{ld} \mathbb{B}$. Altogether,
$$\operatorname{ld} f \notin \operatorname{ld}\left(\mathbb{B}^0 \cup \left(\delta\mathbb{B}^0 \setminus \{f\}\right)\right).$$
Thus, Lemma 5 (see also Remark 6) applies to the algebraic remainder computed in line 8, yielding (10). We will use this statement later to justify line 10, assuming for now that $\operatorname{rk} \bar{f} = \operatorname{rk} f$. From Lemma 5, we also have:
$$H_{\bar{f}} \subset H_f \cdot H^{\infty}_{\mathbb{B}^0 \cup \delta\mathbb{B}^0} + (\mathbb{B}^0 \cup \delta\mathbb{B}^0) \subset H_f \cdot H_{\mathbb{B}}^{\infty} + [\mathbb{B}].$$

Since $f \in \delta\mathbb{B}$, and due to invariants (I9) and (I10) and the fact that $H_f \subset H_{\mathbb{B}}$, we thus obtain that (I10) is preserved at the end of the iteration. Since the set $\mathbb{C} \setminus \mathbb{D}$ remains unchanged during the iteration and set $\mathbb{B}$ is increased, invariants (I11) and (I12) are automatically preserved. This concludes the study of Case 2.

Suppose now that $\operatorname{rk} \bar{f} < \operatorname{rk} f$ and apply the statement (10), which has been proved above in both cases. According to (I9), $\mathbb{B} \subset [\mathbb{C}]$, hence

$$[\mathbb{B}] : H_{\mathbb{B}}^{\infty} \subset [\mathbb{C}] : H_{\mathbb{B}}^{\infty} \subset [\mathbb{C}] : (H_{\mathbb{B}} \cup H_{\mathbb{C}})^{\infty}.$$

According to (I10), $H_{\mathbb{B}} \subset H_C^{\infty} + [\mathbb{C}]$. Thus, Lemma 7 with $H = H_{\mathbb{C}}$, $K = H_{\mathbb{B}}$, and $I = [\mathbb{C}]$ yields $[\mathbb{C}] : (H_{\mathbb{B}} \cup H_{\mathbb{C}})^{\infty} = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$, whence $[\mathbb{B}] : H_{\mathbb{B}}^{\infty} \subset [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$. In particular, keeping (10) in mind, this implies that

$$\mathbf{i}_f \in [\mathbb{C}] : H_{\mathbb{C}}^{\infty}. \tag{11}$$

Due to (I5) for Case 1, or due to (I10) for Case 2, we also have that

$$\mathbf{i}_f \in H_f \subset H_{\mathbb{C}}^{\infty} + [\mathbb{C}]. \tag{12}$$

Together (11) and (12) imply $[\mathbb{C}] : H_{\mathbb{C}}^{\infty} = (1)$. □

We now summarize what we have just done.

**Proposition 11** *Algorithm* Differentiate&Autoreduce *is correct and terminates.*

**Proof.** The algorithm satisfies its specifications according to Lemmas 8, 9, 10. Also, by Lemma 8, it terminates. □

### *4.2. Comments about our modifications of Rosenfeld-Gröbner*

We are ready to present a modified version of the Rosenfeld-Gröbner algorithm that satisfies the bound. The only place where the orders of derivatives may grow is the pseudoreduction w.r.t. an autoreduced set $\mathbb{C}$. Of course, only the orders of non-leading differential indeterminates may grow, while the orders of the leading ones decrease as a result of reduction (or stay the same if the reduction turns out to be algebraic, but then the orders of non-leading indeterminates do not grow either).

By associating different weights with leading and non-leading indeterminates, we will achieve that the weighted sum of their orders does not increase as a result of reduction. These weights come from the bound in the algorithm Differentiate&Autoreduce. If the set of leading indeterminates changes, so do the weights. However, if we estimate in advance the number of times the set of leading indeterminates can change throughout the algorithm, we can still obtain an overall bound on the orders.

For the original Rosenfeld-Gröbner algorithm, it is not that easy to carry out such an estimate, because some indeterminates may disappear and reappear again among the leading indeterminates of the characteristic set $\mathbb{C}$. For example,

**Example 12** *Let* $F = \{y + z,\ x,\ x^2 + z\}$, *with the elimination ranking* $x > y > z$.

- *We choose its characteristic set as* $\mathbb{C} := \{y + z,\ x\}$.
- *The leading variables of* $\mathbb{C}$ *are* $\{y, x\}$.
- *We put* $\bar{F} := \mathsf{d\text{-}rem}(F \setminus \mathbb{C}, \mathbb{C}) = \{z\}$.
- $F_{\text{new}} := \bar{F} \cup \mathbb{C} = \{z,\ y + z,\ x\}$.

- *As radical differential ideals:*

$$\left\{y+z, x, x^2+z\right\} = [z, y+z, x] : 1^\infty \cap \left\{y+z, x, x^2+z, 1\right\}.$$

- *The new* $\mathbb{C} = \{z,\ x\}$ *is computed from* $F_{\text{new}}$ *and the leading variables have changed!*
- ...
- *Finally,*

$$\left\{y+z, x, x^2+z\right\} = [z, y, x] : 1^\infty = [z, y, x]$$

*and we see that the leaders* $y$ *and* $x$ *have come back.*

Here we see that the leading variables change for a moment. But we need to prevent this from happening in the proof of correctness of the algorithm (see Proposition 14) in formulas (19) and (20).

**Example 13** *Let* $F = \{zy,\ x,\ x^2+z\}$, *with the elimination ranking* $x > y > z$.

- *We choose its characteristic set as* $\mathbb{C} := \{zy,\ x\}$.
- *The leading variables of* $\mathbb{C}$ *are* $\{y, x\}$.
- *We put* $\bar{F} := \mathsf{d\text{-}rem}(F \setminus \mathbb{C}, \mathbb{C}) = \{z\}$.
- $F_{\text{new}} := \bar{F} \cup \mathbb{C} = \{z,\ zy,\ x\}$.
- *As radical differential ideals:*

$$\left\{zy, x, x^2+z\right\} = [z, zy, x] : z^\infty \cap \left\{zy, x, x^2+z, z\right\}.$$

- *The new* $\mathbb{C} = \{z,\ x\}$ *is computed from* $F_{\text{new}}$ *and the leading variables have also changed!*
- *But the first component is trivial:* $1 \in [z, zy, x] : z^\infty$.

The first situation can be remedied by properly relaxing the requirement that $\mathbb{C}$ is autoreduced, while the second one can be detected, after which further computations in this branch of the Rosenfeld-Gröbner algorithm are not necessary. As a result, we obtain an algorithm, in which, as long as an indeterminate appears among the leading indeterminates of the set $\mathbb{C}$, w.r.t. which we reduce, it will stay there until the end.

As mentioned above, we are going to replace the computation of the characteristic set by that of a weak d-triangular subset. It is tempting to simply compute a weak d-triangular subset of the least rank, since this computation is inexpensive and it would give us the desired property that the leading indeterminates do not disappear. However, the termination of the algorithm is not guaranteed then. For example, take the system $F = \{x, xy\}$ in $\mathbf{k}\{x, y\}$, and let $x < y$. The weak d-triangular subset of $F$ of the least rank is $F$ itself. Thus, we obtain a component $\{x, xy\} : x^\infty = (1)$ and another component $\{x, xy, \mathbf{i}_{xy}\}$. However, $\mathbf{i}_{xy} = x$, hence we arrive at the same set $F$ that was given in the input, and the algorithm runs forever.

The reason for the above behavior is that the initials of a weak d-triangular set $\mathbb{C}$, as opposed to an autoreduced set, need not be reduced w.r.t. $\mathbb{C}$. Thus by adding these initials we do not necessarily decrease the rank. The solution comes from the idea of (Boulier et al., 1997, Section 5), (Hubert, 2003, Algorithm 6.11), and (Hubert, 2004, Algorithm 4.1) to construct the weak d-triangular set $\mathbb{C}$ gradually, so that each next polynomial $f$ to be added to $\mathbb{C}$ is reduced w.r.t. $\mathbb{C}$ (thus, we can also safely add the initial and separant of $f$ and guarantee that the rank decreases). In order to be able to construct the set $\mathbb{C}$ gradually, similarly to (Hubert, 2003), we store it as a separate component of the triples $(F, \mathbb{C}, H) \in U$.

The last modification that we are going to do is the replacement of the differential pseudo-reduction w.r.t. $\mathbb{C}$ by the algebraic pseudo-reduction w.r.t. $\mathbb{B}$, which is computed from $\mathbb{C}$ by Algorithm Differentiate&Autoreduce. As a result, we obtain Algorithm RG-Bound.

*4.3. Final algorithm and proof of the bound*

In the proof of the bound, a key role is played by the quantity $M_Z(F)$, which is defined for a finite set $F$ of differential polynomials and a proper subset $Z \subsetneq Y$. Assume that $|Z| = k < n$. As before, for a differential indeterminate $y \in Y$, $m_y(F)$ denotes the highest order of a derivative of $y$ occurring in $F$, or zero, if $y$ does not occur in $F$. Then

$$M_Z(F) := (n-k)\sum_{y\in Z} m_y(F) + \sum_{y\in Y\setminus Z} m_y(F).$$

We also recall the notation

$$M(F) = \sum_{y\in Y} m_y(F).$$

**Proposition 14** *Algorithm 3 is correct and terminates.*

**Proof.** We prove the following invariants of the **while**-loop:

- (I1) $\{F_0\} : H_0^\infty = \bigcap_{(F,\mathbb{C},H)\in U}\{F\cup\mathbb{C}\} : H^\infty \cap \bigcap_{(\mathbb{A},H)\in T}[\mathbb{A}] : H^\infty$
- For all $(F,\mathbb{C},H) \in U$,
  - (I2) $\mathbb{C}$ is d-triangular,
  - (I3) $F \neq \varnothing$ is reduced w.r.t. $\mathbb{C}$
  - (I4) $H_\mathbb{C} \subset H$,
  - (I5) Let $l = |\operatorname{lv}\mathbb{C}|$. Then, if $0 < l < n$,

$$M_{\operatorname{lv}\mathbb{C}}(F\cup\mathbb{C}\cup H) \leqslant (n-1)\ldots(n-l)\cdot M(F_0\cup H_0),$$

if $l = 0$ then

$$M_{\operatorname{lv}\mathbb{C}}(F\cup\mathbb{C}\cup H) = M(F_0\cup H_0),$$

otherwise

$$M(F\cup\mathbb{C}\cup H) \leqslant (n-1)!\cdot M(F_0\cup H_0).$$

The proof is divided into **three parts**: correctness (invariants I1–I4), termination, and proof of the bound (invariant I5). The first two parts follow the standard arguments used in the proof of correctness and termination of the Rosenfeld-Gröbner algorithm.

The invariants hold for the initial triple $(F_0, \varnothing, H_0)$. Assuming that they hold at the beginning of an iteration of the **while** loop, we will show that the invariants also take place at the end of the iteration.

**Correctness.** Let $(F,\mathbb{C},H)$ be the triple taken and removed from $U$. Since $F \neq \varnothing$, we can compute an element $f \in F$ of the least rank. Then $f$, as an element of $F$, is reduced w.r.t. $\mathbb{C}$. Applying (Hubert, 2003, Proposition 6.6), we have

$$\{F\cup\mathbb{C}\} : H^\infty = \{F\cup\mathbb{C}\} : (H\cup H_f)^\infty \cap \{F\cup\{\mathbf{i}_f\}\cup\mathbb{C}\} : H^\infty \cap \{F\cup\{\mathbf{s}_f\}\cup\mathbb{C}\} : H^\infty.$$

We note that, since $\operatorname{rk}\mathbf{i}_f < \operatorname{rk} f$ and $\operatorname{rk}\mathbf{s}_f < \operatorname{rk} f$, polynomials $\mathbf{i}_f$ and $\mathbf{s}_f$ are, respectively, the elements of $F\cup\{\mathbf{i}_f\}$ and $F\cup\{\mathbf{s}_f\}$ of the least rank (and, to repeat, their ranks are less than the rank of the least element of $F$). Moreover, since in the last two triples $(F\cup\{\mathbf{i}_f\},\mathbb{C},H), (F\cup\{\mathbf{s}_f\},\mathbb{C},H)$ only the first component has changed, invariants I2–I5 are preserved for them. For the proof of invariant I1, it remains to show that

$$\{F\cup\mathbb{C}\} : (H\cup H_f)^\infty = \begin{cases} \left[\mathbb{B}^0\right] : \bar{H}^\infty, & \bar{F} = \varnothing \\ \left\{\bar{F}\cup\mathbb{B}^0\right\} : \bar{H}^\infty, & \text{otherwise.} \end{cases} \tag{13}$$

**Algorithm 3** $\mathsf{RGBound}(F_0, H_0)$

INPUT: *finite sets of differential polynomials* $F_0 \neq \varnothing$ *and* $H_0$, *and a differential ranking*

OUTPUT: *a finite set* $T$ *of regular systems such that*

$$\{F_0\} : H_0^\infty = \bigcap_{(\mathbb{A},H)\in T} [\mathbb{A}] : H^\infty \quad \textit{and}$$

$$M(\mathbb{A} \cup H) \leqslant (n-1)!M(F_0 \cup H_0) \textit{ for } (\mathbb{A}, H) \in T.$$

$T := \varnothing, \quad U := \{(F_0, \varnothing, H_0)\}$
**while** $U \neq \varnothing$ **do**
  *Take and remove any* $(F, \mathbb{C}, H) \in U$
  $f :=$ *an element of* $F$ *of the least rank*
  $D := \{C \in \mathbb{C} \mid \operatorname{lv} C = \operatorname{lv} f\}$
  $G := (F \cup D) \setminus \{f\}$
  $\bar{\mathbb{C}} := \mathbb{C} \setminus D \cup \{f\}$
  $\mathbb{B} :=$Differentiate&Autoreduce $\left(\bar{\mathbb{C}}, \left\{m_y(G \cup \bar{\mathbb{C}} \cup H) \mid y \in \operatorname{lv} \bar{\mathbb{C}}\right\}\right)$
  **if** $\mathbb{B} \neq \{1\}$ **then**
    $\bar{F} := \mathsf{algrem}(G, \mathbb{B}) \setminus \{0\}$
    $\bar{H} := \mathsf{algrem}(H, \mathbb{B}) \cup H_{\mathbb{B}}$
    **if** $\bar{F} \cap \mathbf{k} = \varnothing$ **and** $0 \notin \bar{H}$ **then**
      **if** $\bar{F} = \varnothing$ **then** $T := T \cup \left\{\left(\mathbb{B}^0, \bar{H}\right)\right\}$
        **else** $U := U \cup \left\{\left(\bar{F}, \mathbb{B}^0, \bar{H}\right)\right\}$
      **end if**
    **end if**
  **end if**
  **if** $\mathbf{s}_f \notin \mathbf{k}$ **then**
    $U := U \cup \{(F \cup \{\mathbf{s}_f\}, \mathbb{C}, H)\}$
    **if** $\mathbf{i}_f \notin \mathbf{k}$ **and** $\deg_{\mathbf{u}_f} f > 1$ **then** $U := U \cup \{(F \cup \{\mathbf{i}_f\}, \mathbb{C}, H)\}$ **end if**
  **end if**
**end while**
**return** $T$

Given that $\mathbb{C}$ is d-triangular, the three assignments following the computation of $f$ ensure that $\bar{\mathbb{C}}$ is a weak d-triangular set of rank strictly less than $\mathbb{C}$, because the polynomial $f$ is reduced w.r.t. $\mathbb{C}$ and we throw away (from $\mathbb{C}$) all its elements with leading variables "in conflict" with the one of $f$. We note that

$$G \cup \bar{\mathbb{C}} = (F \cup \mathbb{D} \setminus \{f\}) \cup (\mathbb{C} \setminus \mathbb{D}) \cup \{f\} = F \cup \mathbb{C}.$$

Since $H_{\mathbb{C}} \subset H$, we also have $H \cup H_f = H \cup H_{\bar{\mathbb{C}}}$. Therefore,

$$\{F \cup \mathbb{C}\} : (H \cup H_f)^\infty = \left\{G \cup \bar{\mathbb{C}}\right\} : (H \cup H_{\bar{\mathbb{C}}})^\infty . \tag{14}$$

Next, we use the properties of the set $\mathbb{B}$ ensured by Algorithm Differentiate&Autoreduce. Since $H_{\mathbb{B}} \subset H_{\bar{\mathbb{C}}}^\infty + \left[\bar{\mathbb{C}}\right]$, applying Lemma 7 with $K = H_{\mathbb{B}}$, we obtain

$$\left\{G \cup \bar{\mathbb{C}}\right\} : (H \cup H_{\bar{\mathbb{C}}})^\infty = \left\{G \cup \bar{\mathbb{C}}\right\} : (H \cup H_{\bar{\mathbb{C}}} \cup H_{\mathbb{B}})^\infty . \tag{15}$$

The inclusions $\mathbb{B} \subset \left[\bar{\mathbb{C}}\right]$ and $\bar{\mathbb{C}} \subset [\mathbb{B}] : H_{\mathbb{B}}^\infty$ imply that

$$\left\{G \cup \bar{\mathbb{C}}\right\} : (H \cup H_{\bar{\mathbb{C}}} \cup H_{\mathbb{B}})^\infty = \{G \cup \mathbb{B}\} : (H \cup H_{\bar{\mathbb{C}}} \cup H_{\mathbb{B}})^\infty . \tag{16}$$

Using the fact that $H_{\bar{\mathbb{C}}} \subset (H_{\mathbb{B}}^\infty + [\mathbb{B}]) : H_{\mathbb{B}}^\infty$ (see Algorithm 2) and applying Lemma 7 with $K = H_{\bar{\mathbb{C}}}$, we get

$$\{G \cup \mathbb{B}\} : (H \cup H_{\bar{\mathbb{C}}} \cup H_{\mathbb{B}})^\infty = \{G \cup \mathbb{B}\} : (H \cup H_{\mathbb{B}})^\infty. \tag{17}$$

It follows from the definition of the algebraic pseudo-remainder (algrem) that

$$\{G \cup \mathbb{B}\} : (H \cup H_{\mathbb{B}})^\infty = \{\bar{F} \cup \mathbb{B}\} : \bar{H}^\infty. \tag{18}$$

Indeed, $\{G \cup \mathbb{B}\} : (H \cup H_{\mathbb{B}})^\infty = \{\bar{F} \cup \mathbb{B}\} : (H \cup H_{\mathbb{B}})^\infty$. Take now any $f \in \left\{\bar{F} \cup \mathbb{B}\right\} : (H \cup H_{\mathbb{B}})^\infty$. There exists $h \in (H \cup H_{\mathbb{B}})^\infty$ such that $h \cdot f \in \left\{\bar{F} \cup \mathbb{B}\right\}$. If $\bar{h}$ is a remainder of $h$ w.r.t. $\mathbb{B}$ then there exists $h' \in H_{\mathbb{B}}^\infty$ with $h'h - \bar{h} \in (\mathbb{B})$. Hence,

$$\bar{h}f \in \left\{\bar{F} \cup \mathbb{B}\right\}$$

and

$$f \in \left\{\bar{F} \cup \mathbb{B}\right\} : \bar{H}^\infty.$$

The reverse inclusion is done in a similar way. Since $\mathbb{B} \subset \left[\mathbb{B}^0\right]$, we obtain that $\left\{\bar{F} \cup \mathbb{B}\right\} : \bar{H}^\infty = \left\{\bar{F} \cup \mathbb{B}^0\right\} : \bar{H}^\infty$.

The set $\mathbb{B}^0$ is d-triangular, its rank is equal to that of $\bar{\mathbb{C}}$, set $\bar{H}$ is partially reduced w.r.t. $\mathbb{B}^0$ and contains $H_{\mathbb{B}}^0$, and $\bar{F}$ is reduced w.r.t. $\mathbb{B}^0$. Moreover, if $\bar{F} = \varnothing$, we obtain the regular system $\left(\mathbb{B}^0, \bar{H}\right)$, which corresponds to the radical differential ideal $\left[\mathbb{B}^0\right] : \bar{H}^\infty = \left\{\bar{F} \cup \mathbb{B}^0\right\} : H_{\mathbb{B}}^\infty$. Thus, we have proved (13) and also have demonstrated that invariants I2–I4 hold for the triple $\left(\bar{F}, \mathbb{B}^0, \bar{H}\right)$.

**Termination.** At each iteration of the **while**-loop, the triple $(F, \mathbb{C}, H) \in U$ is replaced by at most three triples $\left(\bar{F}, \mathbb{B}^0, \bar{H}\right)$, $(F \cup \{\mathbf{i}_f\}, \mathbb{C}, H)$, and $(F \cup \{\mathbf{s}_f\}, \mathbb{C}, H)$.

Define a relation $\prec$ on the set of all triples $(F, \mathbb{C}, H)$ satisfying I2–I4: let $(F', \mathbb{C}', H') \prec (F, \mathbb{C}, H)$ if and only if either $\operatorname{rk} \mathbb{C}' < \operatorname{rk} \mathbb{C}$, or $\mathbb{C}' = \mathbb{C}$ and the element of the least rank in $F'$ is strictly less than that in $F$. Then $\prec$ is a lexicographic product of two well-orders, which is a well-order. We have shown that in the first triple we have $\operatorname{rk} \mathbb{B}^0 < \operatorname{rk} \mathbb{C}$; in the last two triples the second component $\mathbb{C}$ remains the same, but the elements of the least rank of $F \cup \{\mathbf{i}_f\}$ and $F \cup \{\mathbf{s}_f\}$ are strictly less than the element of $F$ of the least rank. That is, each of the three triples is less than $(F, \mathbb{C}, H)$ w.r.t. the well-order $\prec$.

Therefore, all triples computed by the algorithm can be arranged in a ternary tree, in which $(F_0, \varnothing, H_0)$ is the root, and every path starting from the root is finite. Let $\lambda$ be the maximal length of such a path. Then the number of vertices in the tree does not exceed $\sum_{i=0}^{\lambda} 3^i$. Thus, the tree is finite, whence the algorithm terminates.

**Proof of the bound.** Finally, we have assumed that invariant I5 holds for the triple $(F, \mathbb{C}, H)$. We need to show that it holds for the new triples formed by the algorithm at the end of the loop. These new triples are

$$\left(\bar{F}, \mathbb{B}^0, \bar{H}\right), \ (F \cup \{\mathbf{s}_f\}, \mathbb{C}, H), \ (F \cup \{\mathbf{i}_f\}, \mathbb{C}, H).$$

Consider the first triple $\left(\bar{F}, \mathbb{B}^0, \bar{H}\right)$. Let $l = |\operatorname{lv}\mathbb{C}|$. We will make a general observation, showing how $M_{\operatorname{lv}\mathbb{C}}(K)$ changes for any finite set $K$, when we replace $\mathbb{C}$ by $\bar{\mathbb{C}}$. Two cases are possible:

(1) $\operatorname{lv} f \in \operatorname{lv}\mathbb{C}$. Then $\operatorname{lv}\bar{\mathbb{C}} = \operatorname{lv}\mathbb{C}$ and, if $l < n$, we have

$$M_{\operatorname{lv}\bar{\mathbb{C}}}(K) = M_{\operatorname{lv}\mathbb{C}}(K). \tag{19}$$

The marginal situation of $l = n$ will be further treated in (25).

(2) $\operatorname{lv} f \notin \operatorname{lv}\mathbb{C}$. Then $\operatorname{lv}\bar{\mathbb{C}} = \operatorname{lv}\mathbb{C} \cup \{\operatorname{lv} f\}$ and $|\operatorname{lv}\bar{\mathbb{C}}| = l + 1$. If $l + 1 < n$, we observe that

$$\begin{aligned}
&M_{\operatorname{lv}\bar{\mathbb{C}}}(K) = \\
&= (n-l-1)\sum_{y\in\operatorname{lv}\bar{\mathbb{C}}} m_y(K) + \sum_{y\notin\operatorname{lv}\bar{\mathbb{C}}} m_y(K) = \\
&= (n-l-1)\sum_{y\in\operatorname{lv}\mathbb{C}} m_y(K) + (n-l-1)\cdot m_{\operatorname{lv} f}(K) + \sum_{y\notin\operatorname{lv}\bar{\mathbb{C}}} m_y(K) = \\
&= (n-l-1)\sum_{y\in\operatorname{lv}\mathbb{C}} m_y(K) + (n-l-2)\cdot m_{\operatorname{lv} f}(K) + \\
&\quad + \left(m_{\operatorname{lv} f}(K) + \sum_{y\notin\operatorname{lv}\bar{\mathbb{C}}} m_y(K)\right) = \\
&= (n-l-1)\sum_{y\in\operatorname{lv}\mathbb{C}} m_y(K) + \sum_{y\notin\operatorname{lv}\mathbb{C}} m_y(K) + (n-l-2)\cdot m_{\operatorname{lv} f}(K) \leqslant \\
&\leqslant (n-l)\sum_{y\in\operatorname{lv}\mathbb{C}} m_y(K) + \sum_{y\notin\operatorname{lv}\mathbb{C}} m_y(K) + (n-l-2)\cdot M_{\operatorname{lv}\mathbb{C}}(K) = \\
&= (n-l-1)\cdot M_{\operatorname{lv}\mathbb{C}}(K)
\end{aligned} \tag{20}$$

(here we have used the fact that $m_{\operatorname{lv} f}(K) \leqslant M_{\operatorname{lv}\mathbb{C}}(K)$).

If $\operatorname{lv}\mathbb{C} < n$ and $|\operatorname{lv}\bar{\mathbb{C}}| = n$, we simply note that

$$M(K) \leqslant M_{\operatorname{lv}\mathbb{C}}(K). \tag{21}$$

We are now going to replace $K$ by our sets. Assume for simplicity that

$$\operatorname{ld}\bar{\mathbb{C}} = \left\{y_1^{(d_1)}, \ldots, y_k^{(d_k)}\right\},$$

where $k = l$ or $k = l + 1$. Since all derivatives of $y_i$, $1 \leqslant i \leqslant k$, presented in $F \cup \mathbb{B} \cup H$ of order greater than $d_i$ can be found among $\operatorname{rk}\mathbb{B}$, and since the elements of $\bar{F}$ and $\bar{H} \setminus H_{\mathbb{B}}$ are algebraic pseudo-remainders of $G$ and $H$ w.r.t. $\mathbb{B}$, we have

$$m_i\left(\bar{F} \cup \mathbb{B}^0 \cup \bar{H}\right) \leqslant \begin{cases} d_i, & 1 \leqslant i \leqslant k \\ m_i(G \cup \mathbb{B} \cup H), & k < i \leqslant n. \end{cases} \tag{22}$$

Also, recall that $\mathbb{B}$ satisfies the inequality (see (4))

$$m_i(\mathbb{B}) \leqslant m_i\left(G \cup \bar{\mathbb{C}} \cup H\right) + \sum_{j=1}^{k}(m_j\left(G \cup \bar{\mathbb{C}} \cup H\right) - d_j),\ k < i \leqslant n. \tag{23}$$

Combining (22) and (23), we obtain that

$$\begin{aligned}
M_{\mathrm{lv}\,\bar{\mathbb{C}}}\left(\bar{F} \cup \mathbb{B}^0 \cup \bar{H}\right) &= (n-k)\sum_{i=1}^{k} d_i + \sum_{i=k+1}^{n} m_i\left(\bar{F} \cup \mathbb{B}^0 \cup \bar{H}\right) \leqslant \\
&\leqslant (n-k)\sum_{i=1}^{k} d_i + \sum_{i=k+1}^{n} m_i(G \cup \mathbb{B} \cup H) \leqslant \\
&\leqslant (n-k)\sum_{i=1}^{k} d_i + \sum_{i=k+1}^{n} m_i\left(G \cup \bar{\mathbb{C}} \cup H\right) + \\
&\quad + (n-k)\sum_{j=1}^{k}(m_j\left(G \cup \bar{\mathbb{C}} \cup H\right) - d_j) = \\
&= (n-k)\sum_{i=1}^{k} m_i\left(G \cup \bar{\mathbb{C}} \cup H\right) + \sum_{i=k+1}^{n} m_i\left(G \cup \bar{\mathbb{C}} \cup H\right) = \\
&= M_{\mathrm{lv}\,\bar{\mathbb{C}}}\left(G \cup \bar{\mathbb{C}} \cup H\right)
\end{aligned}$$

and if $k = n$ then

$$M\left(\bar{F} \cup \mathbb{B}^0 \cup \bar{H}\right) = \sum_{i=1}^{n} d_i + 0 = M\left(G \cup \bar{\mathbb{C}} \cup H\right)$$

because $\mathrm{rk}\,\bar{\mathbb{C}} = \mathrm{rk}\,\mathbb{B}^0$. Thus,

$$\begin{aligned}
&M_{\mathrm{lv}\,\bar{\mathbb{C}}}\left(\bar{F} \cup \mathbb{B}^0 \cup \bar{H}\right) \leqslant M_{\mathrm{lv}\,\bar{\mathbb{C}}}\left(G \cup \bar{\mathbb{C}} \cup H\right),\ k < n \\
&M\left(\bar{F} \cup \mathbb{B}^0 \cup \bar{H}\right) \leqslant M\left(G \cup \bar{\mathbb{C}} \cup H\right), \qquad k = n.
\end{aligned} \tag{24}$$

Now, applying (19), (20), or (21) with $K = G \cup \bar{\mathbb{C}} \cup H = F \cup \mathbb{C} \cup H$, we get

$$\begin{aligned}
M_{\mathrm{lv}\,\bar{\mathbb{C}}}\left(\bar{F} \cup \mathbb{B}^0 \cup \bar{H}\right) &\leqslant M_{\mathrm{lv}\,\mathbb{C}}(F \cup \mathbb{C} \cup H), && l = k < n \\
M_{\mathrm{lv}\,\bar{\mathbb{C}}}\left(\bar{F} \cup \mathbb{B}^0 \cup \bar{H}\right) &\leqslant (n-l-1)M_{\mathrm{lv}\,\mathbb{C}}\left(\bar{F} \cup \mathbb{B}^0 \cup \bar{H}\right) \leqslant \\
&\leqslant (n-l-1) \cdot M_{\mathrm{lv}\,\mathbb{C}}(F \cup \mathbb{C} \cup H), && l < k < n \\
M\left(\bar{F} \cup \mathbb{B}^0 \cup \bar{H}\right) &\leqslant M\left(G \cup \bar{\mathbb{C}} \cup H\right) = \\
&= M(F \cup \mathbb{C} \cup H) \leqslant \\
&\leqslant M_{\mathrm{lv}\,\mathbb{C}}(F \cup \mathbb{C} \cup H), && l < k = n \\
M\left(\bar{F} \cup \mathbb{B}^0 \cup \bar{H}\right) &\leqslant M\left(G \cup \bar{\mathbb{C}} \cup H\right) = \\
&= M(F \cup \mathbb{C} \cup H), && l = k = n.
\end{aligned} \tag{25}$$

By taking into account the fact that invariant I5 holds for the triple $(F, \mathbb{C}, H)$, we thus obtain this invariant for the triple $\left(\bar{F}, \mathbb{B}^0, \bar{H}\right)$.

For the last two triples, $(F \cup \{\mathbf{s}_f\}, \mathbb{C}, H)$ and $(F \cup \{\mathbf{i}_f\}, \mathbb{C}, H)$, invariant I5 is preserved simply because $\mathbb{C}$ and $H$ remain the same and $f \in F$. More precisely,

$$\begin{aligned} M_{\mathrm{lv}\,\mathbb{C}}\,(F \cup \{\mathbf{s}_f\} \cup \mathbb{C} \cup H) &= M_{\mathrm{lv}\,\mathbb{C}}\,(F \cup \{\mathbf{i}_f\} \cup \mathbb{C} \cup H) = \\ &= M_{\mathrm{lv}\,\mathbb{C}}(F \cup \mathbb{C} \cup H), \qquad\qquad l < n \\ M\,(F \cup \{\mathbf{s}_f\} \cup \mathbb{C} \cup H) &= M\,(F \cup \{\mathbf{i}_f\} \cup \mathbb{C} \cup H) = \\ &= M(F \cup \mathbb{C} \cup H), \qquad\qquad l = n. \end{aligned} \tag{26}$$

To conclude the proof of the bound for the output regular systems $\left(\mathbb{B}^0, \bar{H}\right)$, we note that it is already given by the invariant I5 when $k = n$, while in case $k < n$ we use inequality (21):

$$M\left(\mathbb{B}^0 \cup \bar{H}\right) \leqslant M_{\mathrm{lv}\,\mathbb{B}^0}\left(\mathbb{B}^0 \cup \bar{H}\right) \leqslant (n-1)! \cdot M(F_0 \cup H_0).$$

□

### *4.4. Reduction-independent algorithm*

The goal of this section is to give an algorithm, whose input is a set $F$ of ordinary differential polynomials and the output is a characteristic decomposition of $\{F\}$ satisfying the bound, which would *not* employ the Differentiate&Autoreduce procedure. We will now allow *any* differential reduction algorithm (and define precisely what we mean by this). After each differential reduction, we check whether the orders of the remainder exceed the bound and, if so, apply a truncation procedure that simply removes from the remainder all differential monomials whose orders exceed the bound. Below we show the truncation procedure in detail (see Algorithms 4 and 5); Theorem 17 and Proposition 18 justify the truncation. We note that the justification of truncation is essentially based on the fact that the bound holds for at least one way of computing the differential remainders, namely the one used in Algorithm 3.

In Algorithm 3 we had to be very careful in the reduction process. The idea was to emulate differential reductions by doing enough differentiations first and then applying purely algebraic reduction. We take care of the orders of derivatives in the first process and do not need to worry about them during the second purely algebraic step. Let us find out why such two-step procedure was necessary. If we reduce w.r.t. an arbitrary d-triangular set, the result of reduction depends on the choice of the reduction path.

**Example 15** *Consider the following differential chain*

$$\mathbb{C} = x(x-1),\ (x-1)y,\ z + y + tx$$

*with the elimination ranking $t < x < y < z$ and the differential polynomial*

$$f = z' + y'.$$

*We can reduce $f$ w.r.t. $\mathbb{C}$ in many different ways and the remainders are very different:*
*(1)*

$$z' + y' \xrightarrow{z'+y'+t'x+tx'} t'x + tx' \xrightarrow{(2x-1)x'} t'(2x-1)x = 2t'x^2 - t'x \longrightarrow$$
$$\xrightarrow{x^2-x} \qquad t'x =: f_1$$

*(2)*

$$z' + y' \xrightarrow{(x-1)y'+x'y} (x-1)z' - x'y \xrightarrow{(x-1)y} (x-1)^2 z' \longrightarrow$$
$$\xrightarrow{z'+y'+t'x+tx'} (x-1)^2(y' + t'x + tx') \longrightarrow 0 =: f_2.$$

We see that the remainder $f_1$ depends on the variable $t'$ that is not in both $f_2$ and $\mathbb{C}$. So, the reason for these so different answers is that the set $\mathbb{C}$ has a non-invertible initial modulo the ideal defined by the lower equations. Speaking informally, if $\mathbb{C}$ is partially autoreduced and its initials and separants are invertible, then the result of reduction is more or less uniquely determined. More precisely, one can show that all results of reduction of a polynomial w.r.t. a d-triangular set with invertible initials and separants lie in a fixed Nötherian ring of algebraic polynomials. In particular, if one of the results of reduction satisfies a certain bound on the order of its derivatives, then any other result of reduction will satisfy this bound as well.

Since we are not in position of reducing w.r.t. a set with invertible initials and separants, we are going to state precisely and prove a slightly weaker statement. Within the scope of this section, let us call polynomial $g$ a *differential remainder* of polynomial $f$ w.r.t. $\mathbb{C}$, if $g$ is reduced w.r.t. $\mathbb{C}$ and there exists $h \in H_{\mathbb{C}}^{\infty}$ such that

$$hf - g \in [\mathbb{C}] : H_{\mathbb{C}}^{\infty}.$$

**Proposition 16** *Let $\mathbb{C}$ be a coherent*[9] *d-triangular set of differential polynomials, $f$ a differential polynomial, and $g$ a differential remainder of $f$ w.r.t. $\mathbb{C}$. Let $X$ be the set of derivatives present in $\mathbb{C}$ and $g$. Let $\bar{g}$ be another differential remainder of $f$ w.r.t. $\mathbb{C}$. Assume that $\bar{g}$ is not in $\mathbf{k}[X]$, i.e., it admits a representation $\bar{g} = a_k u^k + \ldots + a_0$, where $u \notin X$ and $a_0, \ldots, a_k$ are free of $u$. Then*

$$\bar{g} - a_0 \in (\mathbb{C}) : H_{\mathbb{C}}^{\infty}.$$

*In particular, $a_0$ is also a differential remainder of $f$ w.r.t. $\mathbb{C}$.*

**Proof.** Since $g$ and $\bar{g}$ are differential remainders of $f$ w.r.t. $g$, they are both reduced w.r.t. $\mathbb{C}$, and there exist $h, \bar{h} \in H_{\mathbb{C}}^{\infty}$ such that

$$hf - g \in [\mathbb{C}] : H_{\mathbb{C}}^{\infty}, \quad \bar{h}f - \bar{g} \in [\mathbb{C}] : H_{\mathbb{C}}^{\infty}.$$

Consider the differential polynomial

$$\bar{f} := \bar{h}(hf - g) - h(\bar{h}f - \bar{g}) = h\bar{g} - \bar{h}g \in [\mathbb{C}] : H_{\mathbb{C}}^{\infty}.$$

Since $\mathbb{C}$ is a coherent d-triangular set, ideal $[\mathbb{C}] : H_{\mathbb{C}}^{\infty}$ is regular. The polynomial $\bar{f}$ is partially reduced w.r.t. $\mathbb{C}$. Therefore, by the Rosenfeld Lemma $\bar{f} \in (\mathbb{C}) : H_{\mathbb{C}}^{\infty}$. We have

$$\bar{f} = (h \cdot a_k)u^k + \ldots + (h \cdot a_0 - \bar{h} \cdot g)$$

with $\bar{h} \cdot g$ contributing only to $a_0$, because it does not depend on $u$. Since $u$ does not appear in $\mathbb{C}$, the fact that $\bar{f} \in (\mathbb{C}) : H_{\mathbb{C}}^{\infty}$ implies that every coefficient of $\bar{f}$ belongs to this ideal. In particular, $h \cdot a_k$ belongs to $(\mathbb{C}) : H_{\mathbb{C}}^{\infty}$, whence $a_i \in (\mathbb{C}) : H_{\mathbb{C}}^{\infty}$, $1 \leqslant i \leqslant k$. Thus,

$$\bar{g} - a_0 = a_k u^k + \ldots + a_1 u \in (\mathbb{C}) : H_{\mathbb{C}}^{\infty}.$$

[9] The adjective "coherent" makes the statement valid in presence of partial derivatives; in the ordinary case, it can be ignored.

□

We are going to apply the above Proposition as follows. Let $\mathbb{C}$ and $f$ be as in its statement. Suppose we know that there exists a differential remainder $g$ of $f$ w.r.t. $\mathbb{C}$ that satisfies a certain bound $b$ on the order of derivatives occurring in it. We emphasize that we do not need to know $g$, the fact of its existence is sufficient. Compute *any* differential remainder $\bar{g}$ of $f$ w.r.t. $\mathbb{C}$. Then, if $\bar{g}$ does not satisfy the bound $b$, it must contain a derivative $u$ that does not satisfy this bound. By Proposition 16, the constant term of $\bar{g}$, when viewed as a polynomial in $u$, is also a differential remainder of $f$ w.r.t. $\mathbb{C}$. Replace $\bar{g}$ by its constant term; continue such replacements until $\bar{g}$ satisfies the bound $b$. This yields an efficient procedure that computes a differential remainder satisfying the bound (see Algorithm 4).

We have proved the following

**Theorem 17** *Let $\mathbb{C}$ be a coherent d-triangular set of differential polynomials, and let $f$ be a differential polynomial. Let $p_i \geqslant m_i(\mathbb{C})$, $i = 1, \ldots, n$. Assume that there exists a differential remainder of $f$ w.r.t. $\mathbb{C}$, which contains no derivatives of differential indeterminate $y_i$ of order greater than $p_i$, $i = 1, \ldots, n$. Let $g$ be any differential remainder of $f$ w.r.t. $\mathbb{C}$. Then* $\mathsf{Truncate}(g, \{p_i\})$ *is a differential remainder of $f$ w.r.t. $\mathbb{C}$, in which the order of every differential indeterminate $y_i$ does not exceed $p_i$.*

**Algorithm 4** $\mathsf{Truncate}\ (f, \{p_i\})$

INPUT: *a differential polynomial $f$ and numbers $p_i \geqslant 0$*

OUTPUT: **truncation** *of $f$, i.e., the sum of those terms of $f$ that belong to the polynomial ring $R = \mathbf{k}\left[\, y_i^{(k)} \mid 1 \leqslant i \leqslant n,\ 0 \leqslant k \leqslant p_i \right]$*

*Let $f = \alpha_1 + \ldots + \alpha_q$, where $\alpha_i$ are differential monomials*

$g := 0$

**for** $i := 1$ **to** $q$ **do**

  **if** $\alpha_i \in R$ **then** $g := g + \alpha_i$

**end for**

**return** $g$

We are going to modify Algorithm 3, so that there is no necessity to perform differential pseudo-reduction in two steps, via prolongation and purely algebraic reduction. In the new Algorithm 5, it is assumed that procedure $\mathsf{d\text{-}rem}$ computes any differential remainder in the above sense. The key idea is the following: whenever we find a differential remainder w.r.t. $\mathbb{D}$ that does not satisfy the expected bound $b$ (computed by Algorithm 5), by Theorem 17 we can simply truncate this remainder. In order to be able to apply Theorem 17, we are going to prove the existence of a differential remainder satisfying $b$. In fact, we know that sets $\mathbb{B}$, $\bar{F}$, and $\bar{H}$ computed in Algorithm 3 satisfy $b$; it remains to be shown that one can obtain differential remainders w.r.t. $\mathbb{D}$, given the elements of $\mathbb{B}$, $\bar{F}$, and $\bar{H}$. Note that we may assume $\operatorname{rk}\mathbb{D} = \operatorname{rk}\bar{\mathbb{C}}$ (at the end of the **for**-loop), since otherwise all results of truncations are discarded by Algorithm 5.

**Proposition 18** *Algorithm 5 is correct and satisfies the bound.*

**Algorithm 5** RGBound-Reduction-Independent$(F_0, H_0)$

INPUT: *finite sets of differential polynomials* $F_0 \neq \varnothing$ *and* $H_0$, *and a differential ranking*

OUTPUT: *a finite set* $T$ *of regular systems such that*

$$\{F_0\} : H_0^\infty = \bigcap_{(\mathbb{A},H)\in T} [\mathbb{A}] : H^\infty \quad \textit{and}$$

$$M(\mathbb{A} \cup H) \leqslant (n-1)! M(F_0 \cup H_0) \textit{ for } (\mathbb{A}, H) \in T.$$

$T := \varnothing, \quad U := \{(F_0, \varnothing, H_0)\}$

**while** $U \neq \varnothing$ **do**

*Take and remove any* $(F, \mathbb{C}, H) \in U$

$f$ *an element of* $F$ *of the least rank*

$D := \{C \in \mathbb{C} \mid \operatorname{lv} C = \operatorname{lv} f\}$

$G := F \cup D \setminus \{f\}$

$\bar{\mathbb{C}} := \mathbb{C} \setminus D \cup \{f\}$

$\bar{G} := G \cup \bar{\mathbb{C}} \cup H$

$$b := \left\{ m_y\left(\bar{G}\right) \mid y \in \operatorname{lv} \bar{C} \right\} \cup \left\{ m_z\left(\bar{G}\right) + \sum_{y \in \operatorname{lv} \bar{C}} \left( m_y\left(\bar{G}\right) - m_y\left(\operatorname{ld} \bar{\mathbb{C}}\right)\right) \mid z \notin \operatorname{lv} \bar{\mathbb{C}} \right\}$$

$\mathbb{D} := \varnothing$

**for** $C \in \bar{\mathbb{C}}$ *increasingly* **do**

$\mathbb{D} := \mathbb{D} \cup \{\mathsf{Truncate}\left(\mathsf{d\text{-}rem}\left(C, \mathbb{D}\right), b\right)\}$

**end for**

**if** $\operatorname{rk} \mathbb{D} = \operatorname{rk} \bar{\mathbb{C}}$ **then**

$\bar{F} :=$ Truncate $(\mathsf{d\text{-}rem}(G, \mathbb{D}) \setminus \{0\}, b)$

$\bar{H} :=$ Truncate $(\mathsf{d\text{-}rem}(H \cup H_f, \mathbb{D}) \cup H_{\mathbb{D}}, b)$

**if** $\bar{F} \cap \mathbf{k} = \varnothing$ **and** $0 \notin \bar{H}$

**then** $U := U \cup \left\{\bar{F}, \mathbb{D}, \bar{H}\right\}$

**else** $T := T \cup \{(\mathbb{D}, \bar{H})\}$

**end if**

**end if**

**if** $\mathbf{s}_f \notin \mathbf{k}$ **then**

$U := U \cup \{(F \cup \{\mathbf{s}_f\}, \mathbb{C}, H)\}$

**if** $\mathbf{i}_f \notin \mathbf{k}$ **and** $\deg_{\mathbf{u}_f} f > 1$ **then** $U := U \cup \{(F \cup \{\mathbf{i}_f\}, \mathbb{C}, H)\}$ **end if**

**end if**

**end while**

**return** $T$

**Proof.** The proof of correctness, termination, and bound for Algorithm 5 is based on the same invariants of the **while**-loop that were used for Algorithm 3. The only new step we make is the Truncate algorithm whose application we justify now. In order to do this we consider

$$\mathbb{B} = \mathsf{Differentiate\&Autoreduce}\left(\bar{\mathbb{C}}, \left\{m_y\left(\bar{G}\right) \mid y \in \operatorname{lv}\bar{\mathbb{C}}\right\}\right).$$

and show that, at the beginning of each iteration, there exist $B \in \mathbb{B}$ and $h \in H_{\mathbb{D}}^{\infty}$ such that $hB$ is a differential remainder of $C$ w.r.t. $\mathbb{D}$. This statement is a consequence of the following expanded invariant of the **for**-loop, which we are going to prove by induction on the number of iterations. Let

$$\mathbb{B}_{<C} = \{f \in \mathbb{B} \mid \operatorname{ld} f < \operatorname{ld} C\},$$

$B = \mathsf{algrem}(C, \mathbb{B}_{<C})$, $E = \mathsf{d\text{-}rem}(C, \mathbb{D})$, and $D = \mathsf{Truncate}\ (E, b)$. Then

$$\begin{aligned} h' \cdot C - hB &\in [\mathbb{D}] : H_{\mathbb{D}}^{\infty}, \\ B &\in [\mathbb{D} \cup \{D\}] : H_{\mathbb{D}}^{\infty}, \\ H_B &\subset (H_D^{\infty} + [\mathbb{D}]) : H_{\mathbb{D}}^{\infty}, \end{aligned}$$

for some $h, h' \in H_{\mathbb{D}}^{\infty}$. The *inductive base* holds, since at the end of the first iteration we have $B = E = D = C$ and $\mathbb{D} = \{C\}$. For the *inductive step*, we have:

$$h_1 \cdot C - B \in (\mathbb{B}_{<C})$$

for some $h_1 \in H_{\mathbb{B}_{<C}}^{\infty}$. By the inductive assumption

$$[\mathbb{B}_{<C}] \subset [\mathbb{D}] : H_{\mathbb{D}}^{\infty}.$$

Hence,

$$h_1 \cdot C - B \in [\mathbb{D}] : H_{\mathbb{D}}^{\infty}.$$

Also, by the inductive assumption,

$$h_1 \in (H_{\mathbb{D}}^{\infty} + [\mathbb{D}]) : H_{\mathbb{D}}^{\infty}.$$

This means that there exist $h \in H_{\mathbb{D}}^{\infty},\ h' \in H_{\mathbb{D}}^{\infty}$ such that

$$h \cdot h_1 - h' \in [\mathbb{D}].$$

Thus,

$$h' \cdot C - h \cdot B \in [\mathbb{D}] : H_{\mathbb{D}}^{\infty}.$$

By definition of (algebraic) pseudo-remainder, we have

$$B \in (\mathbb{B}_{<C} \cup \{C\}), \quad C \in (E + [\mathbb{D}]) : H_{\mathbb{D}}^{\infty}.$$

By Lemma 5, taking into account the assumption $\operatorname{rk}\mathbb{D} = \operatorname{rk}\bar{\mathbb{C}}$, we have:

$$H_B \subset H_C \cdot H_{\mathbb{B}_{<C}}^{\infty} + (\mathbb{B}_{<C}), \quad H_C \subset (H_E + [\mathbb{D}]) : H_{\mathbb{D}}^{\infty}.$$

By Proposition 16, $E \in D + (\mathbb{D}) : H_{\mathbb{D}}^{\infty}$. By modifying slightly the proof of Lemma 5, we will show that this implies $H_E \subset H_D + (\mathbb{D}) : H_{\mathbb{D}}^{\infty}$. Indeed, using the assumption $\operatorname{rk}\mathbb{D} = \operatorname{rk}\bar{\mathbb{C}}$ (which holds at the end of the **for**-loop), we obtain $\operatorname{rk} D = \operatorname{rk} C = \operatorname{rk} E$; since all leading differential indeterminates in $\bar{\mathbb{C}}$ are distinct, this, in particular, implies that

$$v = \operatorname{ld} D = \operatorname{ld} E \notin \operatorname{ld}\mathbb{D}.$$

Now let $f_1, \ldots, f_k$ be any generators of the ideal $(\mathbb{D}) : H_{\mathbb{D}}^{\infty}$, so that we have

$$E - D = \sum_{i=1}^{k} \alpha_i f_i.$$

By viewing the above equality as one between two polynomials in $v$ and noting that $f_i$ do not involve $v$, we immediately obtain that $\mathbf{i}_E - \mathbf{i}_D \in (\mathbb{D}) : H_{\mathbb{D}}^{\infty}$ and $\mathbf{s}_E - \mathbf{s}_D \in (\mathbb{D}) : H_{\mathbb{D}}^{\infty}$.

Combining the above statements, we obtain the required invariants at the end of the iteration:

$$B \in (\mathbb{B}_{<C} \cup \{C\}) \subset ([\mathbb{D}] : H_{\mathbb{D}}^{\infty} \cup (E + [\mathbb{D}]) : H_{\mathbb{D}}^{\infty}) \subset [\mathbb{D} \cup \{D\}] : H_{\mathbb{D}}^{\infty}$$

and

$$H_B \subset H_C \cdot H_{\mathbb{B}_{<C}}^{\infty} + (\mathbb{B}_{<C}) \subset (H_E + [\mathbb{D}]) : H_{\mathbb{D}}^{\infty} + [\mathbb{D}] : H_{\mathbb{D}}^{\infty} \subset (H_D + [\mathbb{D}]) : H_{\mathbb{D}}^{\infty}.$$

The truncations applied in Algorithm 5 to compute sets $\bar{F}$ and $\bar{H}$ are justified by showing that differential remainders of $G$ and $H \cup H_f$ w.r.t. $\mathbb{D}$ that satisfy the bound $b$ exist and can be similarly obtained from the elements of sets $\bar{F}$ and $\bar{H}$ computed by Algorithm 3. We omit these details. □

## 5. Conclusions

By estimating the orders of derivatives, we have shown that, given a set of ordinary differential polynomials specifying a radical differential ideal $I$, one can construct a Nötherian ring of algebraic polynomials, in which the computation of a characteristic decomposition of $I$ is actually performed. This does not mean that the computation is completely algebraic: differentiations are allowed, but they never lead out of the constructed algebraic ring.

We conjecture that, if one can solve the first problem of computing a characteristic decomposition of a radical differential ideal from generators completely algebraically, i.e., by an algorithm that first differentiates the input polynomials sufficiently many times, and then computes the decomposition without using differentiations, then one can also solve the Ritt problem of computing an irredundant prime (or characteristic) decomposition of a radical differential ideal.

## Acknowledgements

We thank Michael F. Singer, François Boulier, William Sit, Évelyne Hubert, Evgeniy Pankratiev, and the referees for their important suggestions.

## References

Boulier, F., 1999. Efficient computation of regular differential systems by change of rankings using Kähler differentials. Tech. rep., Université Lille I, 59655, Villeneuve d'Ascq, France, ref. LIFL 1999–14, presented at the MEGA 2000 conference. `http://hal.archives-ouvertes.fr/hal-00139738`.

Boulier, F., 2000. Triangularisation de systèmes de polynômes différentiels. Série IC2 (Information, Commande, Communication). Hermès, never published. In French. http://hal.archives-ouvertes.fr/hal-00140006.

Boulier, F., 2006. Réécriture algébrique dans les systèmes d'équations différentielles polynomiales en vue d'applications dans les Sciences du Vivant. Mémoire d'habilitation à diriger des recherches. Université Lille I, LIFL, 59655 Villeneuve d'Ascq, France. http://tel.archives-ouvertes.fr/tel-00137153.

Boulier, F., Lazard, D., Ollivier, F., Petitot, M., 1995. Representation for the radical of a finitely generated differential ideal. In: ISSAC'95: Proceedings of the 1995 international symposium on Symbolic and algebraic computation. ACM Press, New York, NY, USA, pp. 158–166, http://hal.archives-ouvertes.fr/hal-00138020.

Boulier, F., Lazard, D., Ollivier, F., Petitot, M., 1997. Computing representations for radicals of finitely generated differential ideals. Tech. rep., Université Lille I, LIFL, 59655, Villeneuve d'Ascq, France, ref. IT306. December 1998 version published in the HDR memoir of Michel Petitot. http://hal.archives-ouvertes.fr/hal-00139061.

Boulier, F., Lemaire, F., 2000. Computing canonical representatives of regular differential ideals. In: ISSAC'00: Proceedings of the 2000 international symposium on Symbolic and algebraic computation. ACM Press, New York, NY, USA, pp. 38–47, http://hal.archives-ouvertes.fr/hal-00139177.

Boulier, F., Lemaire, F., Moreno Maza, M., 2001. PARDI! In: ISSAC'01: Proceedings of the 2001 international symposium on Symbolic and algebraic computation. ACM Press, New York, NY, USA, pp. 38–47, http://hal.archives-ouvertes.fr/hal-00139354.

Boulier, F., Lemaire, F., Moreno Maza, M., 2006. Well known theorems on triangular systems and the $D^5$ principle. In: Proceedings of Transgressive Computing 2006. Granada, Spain, pp. 79–91, http://hal.archives-ouvertes.fr/hal-00137158.

Bouziane, D., Kandri Rodi, A., Maârouf, H., 2001. Unmixed-dimensional decomposition of a finitely generated perfect differential ideal. Journal of Symbolic Computation 31, 631–649.

Hubert, E., 2000. Factorization-free decomposition algorithms in differential algebra. Journal of Symbolic Computation 29 (4-5), 641–662.

Hubert, E., 2003. Notes on triangular sets and triangulation-decomposition algorithms II: Differential systems. In: Symbolic and Numerical Scientific Computing 2001. pp. 40–87.

Hubert, E., 2004. Improvements to a triangulation-decomposition algorithm for ordinary differential systems in higher degree cases. In: Proceedings of ISSAC 2004. ACM Press, pp. 191–198.

Kolchin, E., 1973. Differential Algebra and Algebraic Groups. Academic Press, New York.

Kondratieva, M., Levin, A., Mikhalev, A., Pankratiev, E., 1999. Differential and difference dimension polynomials. Kluwer Academic Publisher.

Moreno Maza, M., 1999. On triangular decompositions of algebraic varieties. Tech. Rep. TR 4/99, NAG Ltd, Oxford, UK, presented at the MEGA-2000 Conference, Bath, England.

Morrison, S., 1999. The differential ideal $[P] : M^\infty$. Journal of Symbolic Computation 28, 631–656.

Ritt, J., 1950. Differential Algebra. American Mathematical Society, New York.

Sit, W., 2002. The Ritt-Kolchin theory for differential polynomials. In: Differential Algebra and Related Topics, Proceedings of the International Workshop (NJSU, 2–3 November 2000).

Szántó, Á., 1999. Computation with polynomial systems. Ph.D. thesis, Cornell University.

Wang, D. M., 1993. An elimination method for polynomial systems. Journal of Symbolic Computation 16, 83–114.