A Bound for Orders in Differential Nullstellensatz

Oleg Golubitsky [a,1] Marina Kondratieva [b,2]
Alexey Ovchinnikov [c,3] Agnes Szanto [d,4]

[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, 119991

[c] *University of Illinois at Chicago*
Department of Mathematics, Statistics, and Computer Science
Chicago, IL 60607-7045, USA

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

Abstract

We give the first known bound for orders of differentiations in differential Nullstellensatz for both partial and ordinary algebraic differential equations. This problem was previously addressed in [1] but no complete solution was given. Our result is a complement to the corresponding result in algebraic geometry, which gives a bound on degrees of polynomial coefficients in effective Nullstellensatz [2–10].

This paper is dedicated to the memory of Eugeny Pankratiev, who was the advisor of the first three authors at Moscow State University.

Key words: differential algebra, characteristic sets, radical differential ideals, differential Nullstellensatz
1991 MSC: 12H05, 13N10, 13P10

1 Introduction

Given a system of algebraic partial differential equations $F = 0$, where $F = f_1, \ldots, f_k$, and a differential equation $f = 0$, one can effectively test if f is a differential algebraic consequence of F. In this paper we develop a method that leads to an effective procedure which finds an algebraic expression of some power of f in terms of the elements of F and their derivatives (or shows that such an expression does not exist). This procedure is called *effective differential Nullstellensatz*. A brute-force algorithm solving this problem consists of two steps:

(1) find an upper bound h on the number of differentiations one needs to apply to F and
(2) find an upper bound on the degrees of polynomial coefficients g_i and a positive integer k

such that f^k is a combination of the elements of F together with the derivatives up to the order h and the coefficients g_i. We solve the first problem in the paper. The second problem was addressed and solved in [2] and further analyzed and improved in [3,4]. A purely algebraic solution was given in [5]. A combinatorial approach via Hilbert polynomials was used in [10] (see also [11, Lecture XIII]). Most of the references on the subject can be found in [6–9].

More precisely, our problem is as follows. We are given a finite set F of differential polynomials such that a differential polynomial f belongs to the radical differential ideal generated by F in the ring of differential polynomials. Knowing **only** the orders and degrees of the elements of F and the order of f, we find a non-negative integer h such that f belongs to the radical of the algebraic ideal generated by F and its derivatives up to the order h.

We give a complete solution to this problem using differential elimination. The problem is non-trivial: the first (unsuccessful) attempt was made by Seidenberg [1], where it was conjectured that most likely such a bound would not be found. Here is where the main difficulty is coming from. In order to get the bound using a differential elimination algorithm we need to estimate

Email addresses: Oleg.Golubitsky@gmail.com (Oleg Golubitsky), kondratieva@sumail.ru (Marina Kondratieva), aiovchin@math.uic.edu (Alexey Ovchinnikov), aszanto@ncsu.edu (Agnes Szanto).
[1] This author was partially supported by NSERC Grant PDF-301108-2004.
[2] This author was partially supported by the Russian Foundation for Basic Research, project no. 08-01-90103-Mol$_a$.
[3] This author was partially supported by NSF Grants CCF-0901175 and CCR-0096842.
[4] This author was partially supported by NSF Grant CCR-0347506

how many differentiation steps this algorithm makes. Originally, termination proofs for such algorithms were based on the Ritt-Noetherianity of the ring of differential polynomials, that is: every increasing chain of radical differential ideals terminates. And this result does not say when the sequence terminates. We overcome this problem in our paper.

The article is organized as follows. We introduce basic notions of differential algebra in Section 2. Then we formulate the main result, Theorem 1, in Section 3. In order to achieve this, we bound the length of increasing sequences of radical differential ideals appearing in our differential elimination in Section 5 (see Proposition 9). For that, in Section 4, we first bound the length of dicksonian sequences of tuples of natural numbers with restricted growth of the maximal element in these tuples (Lemma 8). Finally, we apply this to obtain the bound for the differential Nullstellensatz in Theorem 15, from which Theorem 1 follows. We conclude by giving in Section 6 an alternative non-constructive proof of existence of the bound, based on model theory.

There is some previous work on bounding orders in differential elimination algorithms. In the ordinary case, we can bound the orders of derivatives of the output and all intermediate steps of differential elimination [12], and this bound holds for any ranking. Also in the ordinary case, one can give bounds for quantifier elimination [13] and for the orders and degrees of resolvents of prime differential ideals of a certain type [14]. A related bound for involutive prolongation, based on the analysis of stability of Spencer sequences, is obtained in [15].

Note that, unlike the bounds for differential elimination mentioned above, the bound for the differential Nullstellensatz proposed in this paper holds for the PDE case. Our bound is also based on the analysis of differential elimination. But, due to the ranking-independent nature of the differential Nullstellensatz, we could restrict our analysis to orderly rankings, which allowed us to treat not only the ordinary case, but the PDE case as well.

2 Basic differential algebra

One can find recent tutorials on the constructive theory of differential ideals in [16–18]. One also refers to [1,19–28] for differential elimination theory. A differential ring is a commutative ring with unity endowed with a set of derivations $\Delta = \{\partial_1, \ldots, \partial_m\}$, which commute pairwise. The case of $\Delta = \{\delta\}$ is called *ordinary*. Construct the multiplicative monoid

$$\Theta = \left\{ \partial_1^{k_1} \partial_2^{k_2} \cdots \partial_m^{k_m} \;\middle|\; k_i \geqslant 0 \right\}$$

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 Θ 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 ΘY. This ring is denoted by

$$\mathbf{k}\{y_1, \ldots, y_n\}.$$

We consider the case of $\operatorname{char}\mathbf{k} = 0$ only. An ideal I in $\mathbf{k}\{y_1, \ldots, y_n\}$ is called *differential*, if for all $f \in I$ and $\delta \in \Delta$, $\delta f \in I$. Let $F \subset \mathbf{k}\{y_1, \ldots, y_n\}$ be a set of differential polynomials. For the algebraic ideal, differential ideal, and radical differential ideal generated by F in $\mathbf{k}\{y_1, \ldots, y_n\}$, we use notations (F), $[F]$, and $\{F\}$, respectively.

A *ranking* is a total order $>$ on the set ΘY 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 $\theta = \partial_1^{k_1}\delta_2^{k_2}\cdots\partial_m^{k_m} \in \Theta$ 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. Let a ranking $>$ be fixed. The derivative θy_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 $\mathbf{u}_f$. 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 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 derivation $\delta \in \Delta$ 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 δf is $\delta \mathbf{u}_f$ and the initial of δf is called the *separant* of f, denoted $\mathbf{s}_f$. If $\theta \in \Theta \setminus \{1\}$, then θf 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 $\mathcal{A} \subset \mathbf{k}\{y_1, \ldots, y_n\} \setminus \mathbf{k}$. We say that $\mathcal{A}$ is autoreduced (respectively, partial reduced, respectively, algebraically autoreduced) if each element of $\mathcal{A}$ is reduced (respectively, partial reduced, respectively, algebraically reduced) w.r.t. all the others. $\mathcal{A}$ is called weak d-triangular if no element of $\mathcal{A}$ belongs to $\mathbf{k}$ and the set of leaders of $\mathcal{A}$ is autoreduced. A weak d-triangular set $\mathcal{A}$ is called d-triangular if $\mathcal{A}$ is partially reduced.

Every autoreduced set is finite [20, Chapter I, Section 9] (but an algebraically autoreduced set in a ring of differential polynomials may be infinite). Every weak d-triangular set is finite too [16, Proposition 3.9]. For such sets we use capital calligraphic letters $\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$ and notation $\mathcal{A} = A_1, \ldots, A_p$ to specify the list of the elements of $\mathcal{A}$ arranged in order of increasing rank. We denote the sets of initials and separants of elements of $\mathcal{A}$ by $\mathbf{i}_\mathcal{A}$ and $\mathbf{s}_\mathcal{A}$, respectively. Let $H_\mathcal{A} = \mathbf{i}_\mathcal{A} \cup \mathbf{s}_\mathcal{A}$. For a finite set S of differential polynomials denote by S^∞ 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 [20]).

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

- there exists $k \leqslant \min(r, s)$ 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 $\operatorname{rk} \mathcal{A} = \operatorname{rk} \mathcal{B}$ if $r = s$ and $\operatorname{rk} A_i = \operatorname{rk} B_i$ for $1 \leqslant i \leqslant r$. Let v be a derivative in $\mathbf{k}\{y_1, \ldots, y_n\}$. Denote by $\mathcal{A}_v$ the set of the elements of $\mathcal{A}$ and their derivatives that have a leader ranking strictly lower than v. A set $\mathcal{A}$ is called *coherent* if whenever $A, B \in \mathcal{A}$ are such that $\mathbf{u}_A$ and $\mathbf{u}_B$ have a common derivative: $v = \psi \mathbf{u}_A = \phi \mathbf{u}_B$, then

$$\mathbf{s}_B \psi A - \mathbf{s}_A \phi B \in (\mathcal{A}_v) : H_\mathcal{A}^\infty.$$

3 Main result

For a finite set of differential polynomials $F \subset \mathbf{k}\{y_1, \ldots, y_n\}$ let $D(F)$ be the maximal total degree of a polynomial in F. For each i, $1 \leqslant i \leqslant n$, let

$$h_i(F) = \mathrm{ord}_{y_i}(F), \quad H(F) = \max_{1 \leqslant i \leqslant n} h_i(F).$$

For $h \in \mathbb{Z}_{\geqslant 0}$ let $F^{(\leqslant h)}$ denote the set of derivatives of the elements of F of order less than or equal to h. The *Ackermann function* appearing in our main result is defined as follows [29, Section 2.5.5]:

$$\begin{aligned} A(0, n) &= n + 1 \\ A(m + 1, 0) &= A(m, 1) \\ A(m + 1, n + 1) &= A(m, A(m + 1, n)). \end{aligned}$$

Theorem 1 *Let $F \subset \mathbf{k}\{y_1, \ldots, y_n\}$ be a finite set, $0 \neq f \in \{F\}$ and let $t(F, f)$ be the minimal non-negative integer such that*

$$f \in \sqrt{(F^{(\leqslant t(F,f))})}.$$

Then

$$t(F, f) \leqslant A(m + 8, \max(n, H(F \cup f), D(F \cup f))).$$

PROOF. This result will be proved step-by-step in the following sections as described in the introduction and finally established in Theorem 15.

Remark 2 *It is our own choice here to bound $t(F, f)$ using solely the maximal orders and degrees of F and f. One might come up with another bound using more information of F and f. But we emphasise that the bound on orders* **must** *depend on the degrees, number of differential indeterminates, and number of basic differentiations as the following examples show.*

Example 3 *Let $f = 1$ and $F = \left\{y' - 1, y^k\right\}$ in $\mathbf{k}\{y\}$, the ordinary case. In order to express 1 in terms of the elements of F, one has to differentiate y^k k times.*

In the linear and non-linear cases, consider the following examples showing that the bound must depend on the number of variables and derivations.

Example 4 *Let $f = 1$ and $F = \{y_1', y_1 - y_2', \ldots, y_{n-1} - y_n', y_n - a\}$ in the ordinary differential ring $\mathbf{k}\{y_1, \ldots, y_n\}$, where $a \in \mathbf{k}$ is such that $a^{(n)} = 1$. We have to differentiate the first $n - 1$ generators n times to get $y_n^{(n)}$ into the corresponding algebraic ideal. Hence, $t(F, f) = n$.*

Example 5 *Let* $f = 1$ *and* $F = \{y_1^2, y_1 - y_2^2, \ldots, y_{n-1} - y_n^2, 1 - y_n'\} \subset \mathbf{k}\{y_1, \ldots, y_n\}$*, again in the ordinary case. One can show that*

$$\begin{aligned}
F &\subset (y_1, y_2, \ldots, y_n, 1 - y_n') = I_0,\\
F^{(\leqslant 1)} &\subset \left(I_0, y_1', y_2', \ldots, y_{n-1}', y_n''\right) = I_1,\\
F^{(\leqslant 2)} &\subset \left(I_1, y_1'', \ldots, y_{n-2}'', y_{n-1}'' - 2, y_n^{(3)}\right) = I_2,\\
F^{(\leqslant 3)} &\subset \left(I_2, y_1''', \ldots, y_{n-2}''', y_{n-1}''', y_n^{(4)}\right) = I_3,\\
F^{(\leqslant 4)} &\subset \left(I_3, y_1^{(4)}, \ldots, y_{n-2}^{(4)} - 2^2\binom{4}{2}, y_{n-1}^{(4)}, y_n^{(5)}\right) = I_4,\\
&\ldots\\
F^{\leqslant (2^{n-1})} &\subset \left(I_{2^{n-1}-1}, y_1^{(2^{n-1})} - \prod_{k=1}^{n-1}\binom{2^k}{2^{k-1}}^{2^{n-k-1}}, y_2^{(2^{n-1})}, \ldots, y_n^{\left(2^{n-1}+1\right)}\right) =\\
&= I_{2^{n-1}},\\
&\ldots\\
F^{\leqslant (2^n-1)} &\subset \left(I_{2^n-2}, y_1^{(2^n-1)}, y_2^{(2^n-1)}, \ldots, y_n^{(2^n)}\right).
\end{aligned}$$

Therefore, $1 \notin \left(F^{\leqslant (2^n-1)}\right)$*. Thus,* $t(F, f) = 2^n$*, because modulo* $1 - y_n'$ *we have*

$$\begin{aligned}
\left(y_n^{2^n}\right)^{(2^n)} &= 2^n\left(\left(y_n^{2^n-1}\right)y_n'\right)^{(2^n-1)} \equiv 2^n\left(y_n^{2^n-1}\right)^{(2^n-1)} \equiv \ldots \equiv (2^n)!(y_n y_n')' \equiv\\
&\equiv 2^n! y_n'^2 \equiv 1.
\end{aligned}$$

Example 6 *If we replace* F *in the previous example by*

$$G = \left\{u_{x_1}^2, u_{x_1} - u_{x_2}^2, \ldots, u_{x_{m-1}} - u_{x_m}^2, 1 - u_{x_m^2}\right\} \subset \mathbf{k}\{u\}$$

with partial derivatives $\partial_{x_1}, \ldots, \partial_{x_m}$*, we obtain an example which shows that the bound on orders must depend on the number* m *of derivations. Again, the generators will have to be differentiated* 2^m *times to express* 1*.*

4 Bounds on lengths of sequences

The results of this section with be further used in Section 5 to bound lengths of decreasing sequences of autoreduced sets appearing in the differential elimination algorithm that we use. In this section the letters m and n will *not* mean the number of derivations and differential indeterminates, respectively.

We begin by bounding the length of certain sequences of non-negative n-tuples. Call a sequence

$$t_1, t_2, \ldots, t_k$$

of n-tuples *dicksonian*, if for all $1 \leqslant i < j \leqslant k$, there does not exist a non-negative n-tuple t such that

$$t_i + t = t_j.$$

For example, any lexicographically decreasing sequence is dicksonian. By Dickson's Lemma, every dicksonian sequence is finite. Our goal is to obtain an explicit upper bound for the length of a dicksonian sequence, whose elements do not grow faster than a given function, in terms of this function, the first element, and the size n of the tuples. Let

$$\left(a_1^1, \ldots, a_n^1\right), \left(a_1^2, \ldots, a_n^2\right), \ldots, \left(a_1^k, \ldots, a_n^k\right)$$

be a dicksonian sequence of n-tuples of non-negative integers such that

$$\max\left(a_1^j, \ldots, a_n^j\right) \leqslant f(j) \tag{1}$$

for all j, $1 \leqslant j \leqslant k$, where

$$f : \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0}$$

is a fixed function. We say that the *growth of this sequence is bounded by the function* f.

The following proposition closely resembles a particular case of our problem, namely that of

$$f(i) = m + i - 1.$$

However, in Proposition 7 the maximal coordinate must increase by 1 at each step, whereas in our case it is allowed to decrease or remain the same. We will reduce the case of a dicksonian sequence with the growth bounded by a function f from a certain large class of functions that "do not grow too fast", to the one treated in Proposition 7.

Proposition 7 *[30, Proposition 1] Let $t_1, t_2, \ldots, t_k$ be a dicksonian sequence of n-tuples, such that the maximal coordinate of t_i equals $m + i - 1$, for all $1 \leqslant i \leqslant k$. Then the maximal coordinate in the last tuple, t_k, does not exceed*

$$A(n, m-1) - 1,$$

and there exists such a dicksonian sequence for which this bound is reached.

Note that in Proposition 7 we have: m is the maximal coordinate of t_1 and the length k of the sequence is bounded by

$$A(n, m-1) - m.$$

The general case (of any function f, not necessarily from our class) has also been studied in [31] using a different approach. It is shown that the maximal possible length is primitive recursive in f and recursive, but not primitive recursive (if f increases at least linearly), in n. Sequences yielding the maximal

possible length are constructed. Moreover, if f is linear, an explicit expression for the maximal length is given in terms of a generalized Ackermann function. Our statement was motivated by the need to obtain an explicit expression for the bound for a wider class of growth functions.

Let $L_{f,n}$ denote the maximal length of a dicksonian sequence of n-tuples, whose growth is bounded by f. For an increasing function $f : \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0}$, let $\lceil f^{-1}(x) \rceil$ be the least number k such that $f(k) \geqslant x$.

Lemma 8 *Let $f : \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0}$ be an increasing function, and $d \in \mathbb{Z}_{\geqslant 0}$ be a number such that $f(i+1) - f(i) \leqslant A(d, f(i) - 1)$ for all $i > 0$. Then*

$$L_{f,n} < \left\lceil f^{-1}\Big(A(n+d, f(1)-1)\Big)\right\rceil \tag{2}$$

and the maximal entry of the last n-tuple does not exceed

$$A(n+d, f(1)-1).$$

PROOF. Consider a dicksonian sequence

$$\left(a_1^1, \ldots, a_n^1\right),\ \left(a_1^2, \ldots, a_n^2\right), \ldots,\ \left(a_1^k, \ldots, a_n^k\right), \tag{3}$$

whose growth is bounded by f. Construct from (3) a new sequence satisfying the conditions of Proposition 7. Append to the first tuple d new coordinates, each equal to $f(1)$, obtaining the following $(n+d)$-tuple:

$$\left(a_1^1, \ldots, a_n^1, f(1), \ldots, f(1)\right).$$

Then add $f(2) - f(1) - 1$ new $(n+d)$-tuples. The first n coordinates of these tuples are $(a_1^1, \ldots, a_n^1)$. The last d coordinates form a dicksonian sequence of d-tuples, starting with $(f(1), \ldots, f(1))$, with the maximum coordinate growing exactly by 1 at each step. From Proposition 7 and condition

$$f(2) - f(1) \leqslant A(d, f(1) - 1),$$

such sequence exists. The last tuple will have the maximum coordinate equal to $f(2) - 1$. Next, add the tuple

$$\left(a_1^2, \ldots, a_n^2, f(2), \ldots, f(2)\right).$$

Since the growth of (3) is bounded by f, the maximal coordinate in this tuple equals $f(2)$. Continue by adding $f(3) - f(2) - 1$ new $(n+d)$-tuples, whose first n coordinates are $(a_1^2, \ldots, a_n^2)$ and last d coordinates form a dicksonian sequence growing by 1 at each step. Finally, when the tuple

$$\left(a_1^k, \ldots, a_n^k, f(k), \ldots, f(k)\right)$$

is reached, stop. We obtain a sequence of $(n+d)$-tuples in which the maximal coordinate grows by 1 at each step. We will show that this sequence is dicksonian. Suppose that it is not. Let t_j, t_l, $j < l$, be two $(n+d)$-tuples from this sequence, for which there exists a tuple t such that

$$t_l = t_j + t.$$

Let t^I, t^{II} denote the first n coordinates and the last d coordinates of an $(n+d)$-tuple t, respectively. Then we have

$$t_l^I = t_j^I + t^I \quad \text{and} \quad t_l^{II} = t_j^{II} + t^{II}.$$

If t_j and t_l have been added after *the same* tuple of the form

$$p_i = \left(a_1^i, \ldots, a_n^i, f(i), \ldots, f(i)\right),$$

or if t_j coincides with such a tuple p_i and t_l has been added after p_i, the equality

$$t_l^{II} = t_j^{II} + t^{II}$$

contradicts the fact that the last d coordinates of the tuples between p_i and p_{i+1}, including p_i and excluding p_{i+1}, form a dicksonian sequence. If t_j and t_l have been added after *different* tuples p_i and $p_{i'}$, the equality

$$t_l^I = t_j^I + t^I$$

contradicts the fact that sequence (3) is dicksonian. Therefore, our assumption was false and the constructed sequence is dicksonian.

By Proposition 7, the maximum coordinate of its last element does not exceed

$$A(n+d, m-1) - 1.$$

Since the maximum coordinate in the first element is $f(1)$ and grows by 1 at each step, the number of elements in the constructed sequence does not exceed

$$A(n+d, f(1)-1) - f(1).$$

On the other hand, the number of elements in the constructed sequence is:

$$f(2) - f(1) + f(3) - f(2) + \ldots + f(k) - f(k-1) + 1 = f(k) - f(1) + 1.$$

Therefore,

$$f(k) - f(1) + 1 \leqslant A(n+d, f(1)-1) - f(1),$$

that is,

$$f(k) < A(n+d, f(1)-1),$$

and

$$k < \left\lceil f^{-1}\Big(A(n+d, f(1)-1)\Big)\right\rceil.$$

5 Differential elimination algorithm

Using the result of the previous section, we obtain an upper bound for the length of sequences of d-triangular sets of decreasing rank produced by a differential elimination algorithm. The idea is to put in correspondence with such a sequence a dicksonian sequence of tuples, whose growth is bounded by a function derived from the algorithm.

We fix an **orderly** ranking. Algorithm 1 computes a characteristic decomposition of a radical differential ideal given by a set of generators (correctness and termination are proven in Proposition 10). It is designed in such a way that allows us to control:

- the orders and degrees of differential polynomials occurring in all intermediate steps together with
- a **bound** on the number of iterations of this algorithm.

Note that the sets in this characteristic decomposition might not be autoreduced, but they are *weak d-triangular* (as in [16]), that is, the set of leaders autoreduced. Also, in the algorithm:

- the procedure algrem computes an algebraic pseudo-remainder of a polynomial with respect to an algebraic triangular set (a set is called *triangular* if the leaders of its elements are distinct).
- Algorithm MinimalTriangularSubset inputs a finite set of differential polynomials and outputs one of its least rank triangular subsets.

Denote by $\Delta(\mathcal{C})$ the set of "differential S-polynomials" of $\mathcal{C}$ defined in [16, Definition 4.2]. From now on, m and n again denote the numbers of derivations and differential indeterminates, respectively. Here is the main idea behind the algorithm. The proof of correctness can be found in Proposition 10:

(1) At each step of the algorithm, given $(F, \mathcal{C})$, the set $\bar{\mathcal{C}}$ is formed from $\mathcal{C}$ by adding a new polynomial $f \in F$ and removing everything from $\mathcal{C}$ with leaders that are derivatives of $\mathrm{ld}\, f$: these elements form the set D. As a result, the set $\bar{\mathcal{C}}$ satisfies the property that the set of its leaders is differentially autoreduced.
(2) We define the set G comprised of:
   (a) the remaining elements of F,
   (b) the cross-derivatives (differential S-polynomials) of $\bar{\mathcal{C}}$,
   (c) and the elements of D.
(3) We do the reductions in a way that allows us to control the orders of the remainders:
   (a) first differentiate the elements of $\bar{\mathcal{C}}$ to the maximal necessary order b, obtaining a triangular set $\mathcal{B}$,

(b) then autoreduce $\mathcal{B}$ algebraically.
(c) If the algebraic autoreduction changes the leaders of the polynomials in $\mathcal{B}$, then $\mathcal{B}$ must be inconsistent.
(d) If it does not change the leaders, we reduce elements of G algebraically with respect to algebraically autoreduced set $\mathcal{B}$.
(e) If all remainders are zeroes, we stop, otherwise we append the new remainders to the current system F and continue to the next iteration of the **while**-loop.

Algorithm 1 $\mathsf{RGBound}(F_1)$

INPUT: *a set* $F_1 \subset \mathbf{k}\{y_1, \dots, y_n\}$ *with derivations* $\{\partial_1, \dots, \partial_m\}$

OUTPUT: *A finite set* T *of triangular sets such that* $\{F_1\} \subset \bigcap\limits_{\mathcal{C}\in T} \{\mathcal{C}\} : H_{\mathcal{C}}^{\infty}$*;*

if $1 \notin [\mathcal{C}] : H_{\mathcal{C}}^{\infty}$ *then* $\mathcal{C}$ *is coherent and weak d-triangular*

otherwise $1 \in (\mathcal{C}) : H_{\mathcal{C}}^{\infty}$.

$T := \{\varnothing\};\ U := \{(F_1, \varnothing)\}$

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

Take and remove any $(F, \mathcal{C}) \in U$

$f :=$ *an element of* F *reduced w.r.t.* $\mathcal{C}$ *of the least rank*

if $\mathbf{s}_f \notin \mathbf{k}$ **then** $U := U \cup \{(F \cup \mathbf{s}_f, \mathcal{C})\}$ **end if**

if $\mathbf{i}_f \notin \mathbf{k}$ **then** $U := U \cup \{(F \cup \mathbf{i}_f, \mathcal{C})\}$ **end if**

$D := \{C \in \mathcal{C} \mid \operatorname{ld} C = \theta \operatorname{ld} f \text{ for some } \theta \in \Theta\}$

$\bar{\mathcal{C}} := (\mathcal{C} \setminus D) \cup \{f\}$

$G := F \cup \Delta\left(\bar{\mathcal{C}}\right) \cup D \setminus \{f\}$

$b := \max\limits_{g\in G} \operatorname{ord} g$

$\mathcal{B} := \mathsf{MinimalTriangularSubset}\Big(\Big\{\theta C \mid C \in \bar{\mathcal{C}},\ \operatorname{ord}\theta C \leqslant b\Big\}\Big)$

$\bar{\mathcal{B}} := \{\mathsf{algrem}(h, \mathcal{B} \setminus \{h\}) \mid h \in \mathcal{B}\}$

if $\operatorname{rk}\bar{\mathcal{B}} \neq \operatorname{rk}\mathcal{B}$ **then** $T := T \cup \{\mathcal{B}\}$ **else**

$R := \{\mathsf{algrem}\,(g, \mathcal{B}) \mid g \in G\} \setminus \{0\}$

if $R \neq \varnothing$ **then** $U := U \cup \left\{\left(R \cup F, \bar{\mathcal{C}}\right)\right\}$ **else** $T := T \cup \left\{\bar{\mathcal{C}}\right\}$ **end if**

end if

end while

return T

We get the following bounds for the growth of the maximal degrees of the polynomials computed at the i-th iteration of Algorithm 1.

Proposition 9 *Fix $(F_i, \mathcal{C}_i) \neq \varnothing \in U$ and let $(F_{i+1}, \mathcal{C}_{i+1}) \neq \varnothing$ be any of the elements obtained from $(F_i, \mathcal{C}_i)$ after one iteration of the* **while***-loop. We then have*

$$D(F_{i+1} \cup \mathcal{C}_{i+1}) \leqslant (4D(F_i \cup \mathcal{C}_i))^{\binom{2H(F_i \cup \mathcal{C}_i)+m}{m}+1}.$$

PROOF. Consider an iteration of the loop. In the first six lines of the loop the degrees do not change, since adding an initial or a separant does not cause an increase in the degrees. So,

(1) the first place where the degrees may change is the computation of $\Delta\left(\bar{\mathcal{C}}\right)$, that is, computing cross-derivatives. This at most doubles the degrees.
(2) After that, the only places where the degrees of polynomials may increase are calls to $\mathsf{algrem}(g, \mathcal{B})$ for $g \in G$ or $\mathsf{algrem}\,(h, \mathcal{B} \setminus \{h\})$ for $h \in \mathcal{B}$.

In both cases it is a sequence of at most $|\mathcal{B}|$ algebraic pseudodivisions. We will prove the bound for the reduction of a fixed $g \in G$ modulo $\mathcal{B}$, and the other case follows similarly.

Assume that $|\mathcal{B}| = N$, and let $\mathcal{B} = \{B_1, \ldots, B_N\}$ be ordered so that

$$\mathrm{ld}(B_1) > \mathrm{ld}(B_2) > \cdots > \mathrm{ld}(B_N).$$

Let $g^{(0)} := g$ and

$$g^{(t)} := \mathsf{algrem}\,(g, \{B_1, \ldots B_t\})$$

for $t > 0$. Denote the maximal total degree of $g^{(t)} \cup \mathcal{B}$ by $\delta(t)$, $t \geqslant 0$. Note that

$$1 \leqslant \delta(0) \leqslant 2D(F_i \cup \mathcal{C}_i).$$

Then $g^{(t+1)}$ is obtained by the pseudo-division of $g^{(t)}$ with respect to the polynomial B_{t+1}. Thus,

$$g^{(t+1)} = \mathbf{i}^{\epsilon}_{B_{t+1}} g^{(t)} - qB_{t+1},$$

where ϵ is a sufficiently large exponent specified below, q is the pseudo-quotient, and the degree of $g^{(t+1)}$ in $\mathrm{ld}(B_{t+1})$ is smaller that the same degree of B_{t+1}. The exponent ϵ is bounded by

$$\deg_{\mathrm{ld}(B_{t+1})}\left(g^{(t)}\right) - \deg_{\mathrm{ld}(B_{t+1})}(B_{t+1}) + 1 \leqslant \delta(t).$$

Therefore, if $\delta(t) \geqslant 2$ the total degree of $g^{(t+1)}$ is bounded by

$$\delta(t+1) \leqslant \delta(t)\delta(0) + \delta(t) + \delta(0) \leqslant 2\delta(0)\delta(t),$$

because in this case we necessarily have $\delta(0) \geqslant 2$. If $\delta(t) = 1$ then $\mathcal{B}$ consists of linear polynomials and, moreover, the polynomial $g^{(t)}$ is linear as all its

remainders are, that is, $\delta(t+1) \leqslant 1$. These two cases imply that

$$\delta(N) \leqslant (2\delta(0))^{N+1}.$$

Using that

$$\delta(0) \leqslant 2D(F_i \cup \mathcal{C}_i), \quad N \leqslant \binom{b_i + m}{b_i}, \text{ and } \; b_i \leqslant 2H(F_i \cup \mathcal{C}_i),$$

we obtain the claim (the numbers b_i correspond to the number b computed at the i-th iteration of the loop in Algorithm 1).

5.1 Differential bounds for splitting

Consider now the splitting part of differential elimination. Algorithm 1 removes an element $(F, \mathcal{C})$ from U and within one iteration of the **while**-loop converts this element into zero, one, two, or three elements. Moreover, if the set $\mathcal{C}$ does not change, the orders and degrees of the elements of F do not increase after the conversion.

Let $\mathcal{U}$ be the set of all triples $(F, \mathcal{C}, k)$, where $(F, \mathcal{C})$ is a pair removed from the set U at the beginning of the k-th iteration of the **while**-loop (the iterations are numbered starting from 1). Introduce a partial order on $\mathcal{U}$: let

$$(F_1, \mathcal{C}_1, k_1) \succ_0 (F_2, \mathcal{C}_2, k_2)$$

if and only if $k_1 < k_2$, $(F_2, \mathcal{C}_2)$ was added to U at iteration k_1 and was not added to U at any iteration k, $k_1 < k < k_2$. Let the partial order $\succ$ on $\mathcal{U}$ be the transitive closure of the relation $\succ_0$. Each triple $u \in \mathcal{U}$, except $u = (F_1, \varnothing, 1)$, has a unique direct predecessor $u_- \succ_0 u$ and up to three direct successors.

The relation $\succ$ satisfies the following *first* property: if

$$(F_1, \mathcal{C}_1, k_1) \succ (F_2, \mathcal{C}_2, k_2) \tag{4}$$

and a polynomial f is reduced with respect to $\mathcal{C}_2$, it is also reduced with respect to $\mathcal{C}_1$. This is the case because of the inclusion

$$\Theta \operatorname{rk} \mathcal{C}_2 \supseteq \Theta \operatorname{rk} \mathcal{C}_1. \tag{5}$$

that holds by construction of $\mathcal{C}_2$ from $\mathcal{C}_1$.

The *second* property of the relation $\succ$ is that, whenever (4) holds and

$$\mathcal{C}_1 = \mathcal{C}_2,$$

for the elements g_1 and g_2 drawn respectively from F_1 and F_2 at iterations k_1 and k_2, we have

$$\deg g_1 > \deg g_2.$$

This property holds when $(F_1, \mathcal{C}_1, k_1)$ is a direct predecessor of $(F_2, \mathcal{C}_2, k_2)$, because in this case $\mathcal{C}_1 = \mathcal{C}_2$ implies that g_2 is the initial or separant of g_1; by transitivity, it also holds in general for any triples satisfying (4).

Consider Algorithm 1 with input F_1 and the corresponding partially ordered set $\mathcal{U}$. Denote the maximal length of a decreasing chain in $\mathcal{U}$ by $L(F_1)$.

Proposition 10 *Algorithm 1 is correct and terminates. Moreover,*

$$L(F_1) \leqslant \log_2(A(m+7, Q(F_1) - 1)),$$

where

$$Q(F_1) = \max\left(9, n, 2^{9H(F_1)}, D(F_1)\right). \tag{6}$$

PROOF. To demonstrate **correctness** we need to prove that for all $\mathcal{A} \in T$, if $1 \notin [\mathcal{A}] : H_{\mathcal{A}}^{\infty}$ then $\mathcal{A}$ is coherent, weak d-triangular, and

$$\{F_1\} \subseteq \{\mathcal{A}\} : H_{\mathcal{A}}^{\infty}.$$

Note that in the while loop of the algorithm there are two conditions used to add a set $\mathcal{A}$ to T. The first is when $\mathrm{rk}\mathcal{A} \neq \mathrm{rk}\bar{\mathcal{A}}$, where $\bar{\mathcal{A}}$ is the set obtained by taking the algebraic remainders of the elements of $\mathcal{A}$ by the rest of the elements. In this case we have $1 \in (\mathcal{A}) : H_{\mathcal{A}}^{\infty}$ by [12, Lemma 5].

The second case is when the while loop is entered with a pair $(F, \mathcal{C}) \in U$ and we add $\mathcal{A} := \bar{\mathcal{C}}$ to T if all elements of a set G, which contains F, reduces to zero by some derivatives of the elements of $\bar{\mathcal{C}}$. Here $\bar{\mathcal{C}}$ is obtained from $\mathcal{C}$ by adding an element f to $\mathcal{C}$ and removing all elements from $\mathcal{C}$ with leaders which are derivatives of the leader of f, so $\bar{\mathcal{C}}$ remains d-triangular if $\mathcal{C}$ is such. Since $R = \varnothing$, the set $\Delta\left(\bar{\mathcal{C}}\right)$ is reducible to zero with respect to $\bar{\mathcal{C}}$. Therefore, $\bar{\mathcal{C}}$ is coherent by [16, Proposition 4.4].

To see the last claim, note that $F_1 \subset F$ for all $(F, \mathcal{C}) \in U$, so also $F_1 \subset G$, and, thus,

$$\{F_1\} \subset \left\{\bar{\mathcal{C}}\right\} : H_{\bar{\mathcal{C}}}^{\infty} = \{\mathcal{A}\} : H_{\mathcal{A}}^{\infty}.$$

Termination of the algorithm and the **bound** for $L(F_1)$ will be proved as follows. To each element $(F, \mathcal{C}, k)$ of $\mathcal{U}$ we associate an $(m+4)$-tuple in such a way that any sequence of these tuples, corresponding to a decreasing sequence of elements of $\mathcal{U}$ w.r.t. $\succ$, is dicksonian. Note that by definition $L(F_1)$ is

the maximal length of such sequence. For the initial triple $(F_1, \varnothing, 1)$, let the corresponding $(m+4)$-tuple be

$$(0, \ldots, 0, n, 0).$$

For any other triple $(F, \mathcal{C}, k) \in \mathcal{U}$, consider its direct predecessor $(F_-, \mathcal{C}_-, k_-)$, that is, $(F_-, \mathcal{C}_-, k_-) \succ_0 (F, \mathcal{C}, k)$. Let f be the element that was drawn from F_- at the beginning of the k_--th iteration. Let

$$\operatorname{rk} f = \left(\partial_1^{i_1} \ldots \partial_m^{i_m} y_j\right)^d.$$

Let also g be the element drawn from F at the beginning of the k-th iteration. If

$$F = F_- \cup \{\mathbf{i}_f\} \quad \text{or} \quad F = F_- \cup \{\mathbf{s}_f\},$$

this implies that $g = \mathbf{i}_f$ or $g = \mathbf{s}_f$, respectively, and $\mathcal{C} = \mathcal{C}_-$. Then the $(m+4)$-tuple associated to $(F, \mathcal{C}, k)$ is

$$(a_1, \ldots, a_{m+3}, \deg(g)),$$

where $(a_1, \ldots, a_{m+4})$ is the $(m+4)$-tuple associated to $(F_-, \mathcal{C}_-, k_-)$. Otherwise (when f is added to $\mathcal{C}_-$), the $(m+4)$-tuple associated to $(F, \mathcal{C}, k)$ is

$$\tau = (i_1, \ldots, i_m, d, j, n-j, \deg(g)).$$

We need to show that, for any predecessor $\left(\hat{F}, \hat{\mathcal{C}}, \hat{k}\right)$ of $(F, \mathcal{C}, k)$, at least one coordinate of the tuple $\hat{\tau}$ associated to $\left(\hat{F}, \hat{\mathcal{C}}, \hat{k}\right)$ is greater than the corresponding coordinate of the tuple τ associated to $(F, \mathcal{C}, k)$.

If $\hat{\mathcal{C}} = \mathcal{C}$, the statement holds because of the second property of the relation $\succ$. Furthermore, if $\hat{\mathcal{C}} = \varnothing$, the $(m+3)$-rd coordinate of $\hat{\tau}$ equals n, which is greater than $n-j$, the value of the $(m+3)$-rd coordinate in τ (since $j \in \{1, \ldots, n\}$). The non-trivial case of $\hat{\mathcal{C}} \neq \mathcal{C}$ and $\hat{\mathcal{C}} \neq \varnothing$ is considered in detail below. Let

$$\left(\hat{F}^*, \hat{\mathcal{C}}^*, \hat{k}^*\right)$$

be the most recent predecessor of $\left(\hat{F}, \hat{\mathcal{C}}, \hat{k}\right)$ with $\hat{\mathcal{C}}^* \neq \hat{\mathcal{C}}$. Such predecessor exists, because $\hat{\mathcal{C}} \neq \varnothing$. Let $\hat{f}^*$ be the element drawn from $\hat{F}^*$ at iteration $\hat{k}^*$. Because $\left(\hat{F}^*, \hat{\mathcal{C}}^*, \hat{k}^*\right)$ is the most recent predecessor of $\left(\hat{F}, \hat{\mathcal{C}}, \hat{k}\right)$ with $\hat{\mathcal{C}}^* \neq \hat{\mathcal{C}}$, the element $\hat{f}^*$ must have been added to $\hat{\mathcal{C}}^*$ at iteration $\hat{k}^*$ to form $\bar{\mathcal{C}}$, from which then the set $\mathcal{A} = \hat{\mathcal{C}}$ has been computed. Therefore,

$$\operatorname{rk} \hat{f}^* \in \operatorname{rk} \hat{\mathcal{C}}. \tag{7}$$

Let

$$\operatorname{rk} \hat{f}^* = \left(\partial_1^{\hat{i}_1} \ldots \partial_m^{\hat{i}_m} y_{\hat{j}}\right)^{\hat{d}}.$$

Then the tuple $\hat{\tau}$ associated to $\left(\hat{F}, \hat{\mathcal{C}}, \hat{k}\right)$ is

$$\hat{\tau} = \left(\hat{i}_1, \ldots, \hat{i}_m, \hat{d}, \hat{j}, n - \hat{j}, \hat{\rho}\right),$$

where the last element $\hat{\rho}$ is unimportant to us at the moment.

Similarly, let $(F^*, \mathcal{C}^*, k^*)$ be the most recent predecessor of $(F, \mathcal{C}, k)$ with $\mathcal{C}^* \neq \mathcal{C}$. Let f^* be the element drawn from F^* at iteration k^*. Let

$$\operatorname{rk} f^* = \left(\partial_1^{i_1} \ldots \partial_m^{i_m} y_j\right)^d.$$

Then the tuple τ associated to $(F, \mathcal{C}, k)$ is

$$\tau = (i_1, \ldots, i_m, d, j, n - j, \rho),$$

where the last element ρ is again unimportant.

Recall that we need to show that at least one coordinate in $\hat{\tau}$ is greater than the corresponding coordinate in τ. Observe first that if $\hat{j} \neq j$ then either $\hat{j} > j$, or $n - \hat{j} > n - j$. Therefore, we may assume

$$\hat{j} = j.$$

By construction, f^* is reduced w.r.t. $\mathcal{C}^*$. By the first property of the relation $\succ$, it must be reduced w.r.t. $\hat{\mathcal{C}}$ as well. But then, given (7), we obtain that f^* is reduced w.r.t. $\hat{f}^*$. In particular, this implies that $\operatorname{rk} f^*$ is reduced w.r.t. $\operatorname{rk} \hat{f}^*$, which cannot be the case unless at least one of the following inequalities holds:

$$\hat{i}_1 > i_1, \ldots, \hat{i}_m > i_m, \hat{d} > d.$$

This concludes the proof of termination.

Note that if we remove $n-j$ from the τ's, the sequence might not be dicksonian. Indeed, let $m = 1$, $F = \{y_1, y_2\} \subset \mathbf{k}\{y_1, y_2, y_3\}$ with $y_1 < y_2 < y_3$. We then would have $\tau_1 = (0, 1, 1, 1)$ and $\tau_2 = (0, 1, 2, 1)$.

We now switch to proving the **bound**. Let $H_1 = \max(H(F_1), m)$, $H_{k+1} = 2H_k$, $D_1 = D(F_1)$, and

$$D_{k+1} = (4D_k)^{\binom{2H_k+m}{m}+1}.$$

By Proposition 9, the maximal coordinate of the $(m + 4)$-tuple τ_k does not exceed $\max(H_k, D_k, n)$. Let

$$u_1 = \max\left(n, 9, 2^{9H(F)}, D(F)\right), \quad u_{k+1} = 2^{\sqrt[3]{u_k}(2+\log_2 u_k)}.$$

Then the maximal coordinate of τ_k does not exceed u_k for all $k \geqslant 1$. Indeed, we will prove by induction that $H_k \leqslant \frac{1}{9}\log_2 u_k$ and $D_k \leqslant u_k$. For $k = 1$ these

inequalities hold by definition of u_1. Assuming that they hold for H_k, D_k, and u_k, prove them for H_{k+1}, D_{k+1}, u_{k+1}. Since $H_{k+1} = 2H_k$, we have

$$2^{9H_{k+1}} = 2^{9\cdot 2H_k} = \left(2^{9H_k}\right)^2 \leqslant u_k^2 = 2^{2\log_2 u_k} \leqslant 2^{\sqrt[3]{u_k}\log_2 u_k} < u_{k+1},$$

because $u_k \geqslant 9$. Next,

$$\log_2 D_{k+1} = \left(\binom{2H_k + m}{m} + 1\right)(2 + \log_2 D_k) \leqslant 2^{2H_k+m}(2 + \log_2 u_k) \leqslant$$
$$\leqslant 2^{3H_k}(2 + \log_2 u_k) \leqslant \sqrt[3]{u_k}(2 + \log_2 u_k) = \log_2 u_{k+1}.$$

Here we used the fact that $H_k \geqslant m$, as well as the inequality $H_k \leqslant \frac{1}{9}\log_2 u_k$ proven above. Now observe that for $x \geqslant 9$, we have

$$2^{\sqrt[3]{x}(2+\log_2 x)} \leqslant 2^{x+2} - 3 = A(3, x-1).$$

Therefore, the sequence of $(m+4)$-tuples $\tau_0, \tau_1, \tau_2, \ldots$ satisfies the conditions of Lemma 8 with $d = 3$. And, according to this lemma, the length of this sequence does not exceed

$$\left\lceil f^{-1}\Big(A(m+7, f(1)-1)\Big)\right\rceil,$$

where $f(k) = u_k \geqslant 2^k$. We can now plug in $f(1) = u_1$, and replace f^{-1} with $\log_2$.

Corollary 11 *The maximal orders and degrees of polynomials computed by Algorithm 1 do not exceed*

$$A(m+7, Q(F)-1). \tag{8}$$

PROOF. Follows directly from Lemma 8 and Proposition 10.

5.2 Lifting the final bound from splitting

Note that for $f \in \mathbf{k}\{y_1, \ldots, y_n\}$ and $F \subset \mathbf{k}\{y_1, \ldots, y_n\}$ we have

$$1 \in \{F\} : f \iff f \in \{F\}.$$

Lemma 12 *Let $C_1, \ldots, C_p = \mathcal{C} \subset [F]$ be a coherent weak d-triangular set that reduces all elements of F to zero, and let the ranking be orderly. Then for all $f \in \{F\}$ we have*

$$1 \in \left(\mathcal{C}^{(\leqslant q)}\right) : \left(H_{\mathcal{C}}^{\infty} \cup f\right),$$

where $q = \max\left(\operatorname{ord} f, b\right) - \min\limits_{g\in\mathcal{C}} \operatorname{ord} g$ with $b = \max\limits_{g\in\mathcal{C}} \operatorname{ord} g$.

PROOF. We will first construct the sets

$$\mathcal{B} = \mathsf{MinimalTriangularSubset}\left(\{\theta C \mid C \in \mathcal{C},\ \operatorname{ord}\theta C \leqslant b\}\right)$$

and

$$\bar{\mathcal{B}} = \{\mathsf{algrem}(h, \mathcal{B} \setminus \{h\}) \mid h \in \mathcal{B}\}.$$

If $\operatorname{rk}\mathcal{B} \neq \operatorname{rk}\bar{\mathcal{B}}$ then

$$1 \in (\mathcal{B}) : H_{\mathcal{B}}^{\infty} = (\mathcal{B}) : H_{\mathcal{C}}^{\infty}$$

by [12, Lemma 5] and our lemma is proven.

Suppose that $\operatorname{rk}\mathcal{B} = \operatorname{rk}\bar{\mathcal{B}}$ and take the sets $\mathcal{C}$ and $H = H_{\mathcal{C}}$ as the input of [16, Algorithm 6.8]. We get a differential regular system $(\mathcal{A}, H_{\mathcal{A}})$ as the output and $\mathcal{A} = A_1, \ldots, A_p \neq \varnothing$. This means that $\mathcal{A}$ is a coherent d-triangular set such that

$$[\mathcal{C}] : H_{\mathcal{C}}^{\infty} = [\mathcal{A}] : H_{\mathcal{A}}^{\infty}.$$

Note that, since we have $\operatorname{rk}\bar{\mathcal{B}} = \operatorname{rk}\mathcal{B}$ and the ranking is orderly, the elements of $\mathcal{A}$ can be constructed as $\mathsf{algrem}(C, \mathcal{B}_0)$ for some $C \in \mathcal{C}$ and $\mathcal{B}_0 \subset \mathcal{B}$.

It follows from [16, Theorem 4.12] that the ideal $[\mathcal{A}] : H_{\mathcal{A}}^{\infty}$ is radical and, therefore,

$$f \in \{F\} \subset \{\mathcal{C}\} : H_{\mathcal{C}}^{\infty} = \{\mathcal{A}\} : H_{\mathcal{A}}^{\infty} = [\mathcal{A}] : H_{\mathcal{A}}^{\infty}.$$

Let g be a partial pseudo-remainder of f with respect to $\mathcal{A}$. Then, by the Rosenfeld lemma [16, Theorem 4.8], we have

$$g \in (\mathcal{A}) : H_{\mathcal{A}}^{\infty}. \tag{9}$$

Let

$$q_i = b - \operatorname{ord}\mathcal{C}_i = b - \operatorname{ord}\mathcal{A}_i, \quad 1 \leqslant i \leqslant p,$$

and

$$q_0 = \max(0, \operatorname{ord} f - b).$$

Since the ranking is orderly, there exists $h \in H_{\mathcal{A}}^{\infty}$ such that

$$h \cdot f - g \in \left(A_1^{(\leqslant \max(0, \operatorname{ord} f - \operatorname{ord} A_1))}, \ldots, A_p^{(\leqslant \max(0, \operatorname{ord} f - \operatorname{ord} A_p))}\right). \tag{10}$$

Indeed, at each step of the partial pseudo-division the order of the resulting differential polynomial is less than or equal to the one of the previous polynomial and $\operatorname{ord} f - \operatorname{ord} A_i$ represents the maximal number of times one possibly needs to differentiate A_i to perform one step of the partial pseudo-reduction with respect to A_i. For any i, $1 \leqslant i \leqslant p$, we have

$$\begin{aligned}\max(0, \operatorname{ord} f - \operatorname{ord} A_i) &\leqslant \max(\operatorname{ord} f, b) - \operatorname{ord} A_i = \\ &= b - \operatorname{ord} A_i + \max(b, \operatorname{ord} f) - b = q_i + q_0.\end{aligned}$$

Hence, (9) and (10) imply that

$$1 \in \left(A_1^{(\leqslant q_1 + q_0)}, \ldots, A_p^{(\leqslant q_p + q_0)}\right) : (H_{\mathcal{A}}^{\infty} \cup f).$$

On the other hand,

$$\left(A_1^{(\leqslant q_1+q_0)},\dots,A_p^{(\leqslant q_p+q_0)}\right):(f\cup H_{\mathcal{A}}^{\infty})\subset\left(C_1^{(\leqslant q_1+q_0)},\dots,C_p^{(\leqslant q_p+q_0)}\right):(f\cup H_{\mathcal{C}}^{\infty}).$$

Indeed, if $1\leqslant i\leqslant p$, by induction on $r\leqslant q_i$ we shall prove that

$$\left(A_i^{(\leqslant r)}\right)\subset\left(C_1^{(\leqslant q_1)},\dots,C_p^{(\leqslant q_p)}\right):H_{\mathcal{C}}^{\infty}. \tag{11}$$

To prove (11) we note that for any $A_i\in\mathcal{A}$ there exists the following representation

$$hA_i=\sum_{\{k,j\mid \operatorname{ord}\theta_{kj}\leq\operatorname{ord}C_i-\operatorname{ord}C_j\}}\beta_k\theta_{kj}C_j$$

with $h\in H_{\mathcal{C}}^{\infty}$. Then, after differentiating the above expression r times we obtain

$$\left(A_i^{(\leqslant r)}\right)\subset\left(C_1^{(\leqslant \operatorname{ord}C_i-\operatorname{ord}C_1+r)},\dots,C_p^{(\leqslant \operatorname{ord}C_i-\operatorname{ord}C_p+r)}\right):H_{\mathcal{C}}^{\infty}.$$

Note that

$$\operatorname{ord}C_i-\operatorname{ord}C_j+r\leqslant\operatorname{ord}C_i-\operatorname{ord}C_j+b-\operatorname{ord}C_i=q_j,$$

and we have (11).

Now, by [12, Lemma 5] for the polynomials C_i and A_i, since $\operatorname{rk}C_i=\operatorname{rk}A_i$, we have

$$\mathbf{s}_{A_i}h_i-\mathbf{s}_{C_i}\in\left(C_1^{(\leqslant q_1)},\dots,C_p^{(\leqslant q_p)}\right) \tag{12}$$

and

$$\mathbf{i}_{A_i}h_i-\mathbf{i}_{C_i}\in\left(C_1^{(\leqslant q_1)},\dots,C_p^{(\leqslant q_p)}\right). \tag{13}$$

for some $h_i\in H_{\mathcal{C}}^{\infty}$. Let

$$a\in\left(A_1^{(\leqslant q_1+q_0)},\dots,A_p^{(\leqslant q_p+q_0)}\right):(f\cup H_{\mathcal{A}}^{\infty}).$$

This means that

$$afh'\in\left(A_1^{(\leqslant q_1+q_0)},\dots,A_p^{(\leqslant q_p+q_0)}\right) \tag{14}$$

for

$$h'=\mathbf{s}_{A_1}^{j_1}\cdot\ldots\cdot\mathbf{s}_{A_p}^{j_p}\mathbf{i}_{A_1}^{k_1}\cdot\ldots\cdot\mathbf{i}_{A_p}^{k_p}.$$

Multiplying inclusions (12) and (13) by some powers of $\mathbf{s}_{C_i}$ and $\mathbf{i}_{C_i}$ and (14) by h_i, we get

$$afh''\in\left(C_1^{(\leqslant q_1+q_0)},\dots,C_p^{(\leqslant q_p+q_0)}\right),$$

where $h''\in H_{\mathcal{C}}^{\infty}$. Hence,

$$1\in\left(A_1^{(\leqslant q_1+q_0)},\dots,A_p^{(\leqslant q_p+q_0)}\right):(f\cup H_{\mathcal{A}}^{\infty})\subset\left(C_1^{(\leqslant q_1+q_0)},\dots,C_p^{(\leqslant q_p+q_0)}\right):(f\cup H_{\mathcal{C}}^{\infty}).$$

Since

$$q_i + q_0 = b - \operatorname{ord} C_i + \max(b, \operatorname{ord} f) - b \leqslant \max(b, \operatorname{ord} f) - \min_{g \in \mathcal{C}} \operatorname{ord} g = q,$$

the lemma is proven.

Lemma 13 *Let $F \subset \mathbf{k}\{y_1, \ldots, y_n\}$ and $f, f_1, \ldots, f_k \in \mathbf{k}\{y_1, \ldots, y_n\}$. Suppose for some $d \in \mathbb{Z}_{\geqslant 1}$ we have $(f_1 \cdot \ldots \cdot f_k)^d \in (F) : f$. Then*

$$\theta_1 f_1 \cdot \ldots \cdot \theta_k f_k \in \sqrt{\left(F^{\left(\leqslant 4^{(k+1)H+1} d\right)}\right)} : f,$$

where $\theta_i \in \Theta$ with $\operatorname{ord} \theta_i \leqslant H$ for all i, $1 \leqslant i \leqslant k$.

PROOF. It follows from the proof of [32, Lemma 1.7] that if $a^d \in (F)$ then

$$(\partial_i a)^{2d-1} \in \left(F^{(\leqslant d)}\right)$$

for any $a \in \mathbf{k}\{y_1, \ldots, y_n\}$ and $\partial_i \in \Delta$. Therefore,

$$((\partial_i f_1) \cdot f_2 \cdot \ldots \cdot f_k + \ldots + f_1 \cdot \ldots \cdot f_{k-1} \cdot (\partial_i f_k))^{2d-1} \in \left(F^{(\leqslant d)}\right) : f^\infty.$$

Multiplying by $((\partial_i f_1) \cdot f_2 \cdot \ldots \cdot f_k)^{2d-1}$, we obtain

$$((\partial_i f_1) \cdot f_2 \cdot \ldots \cdot f_k)^{2(2d-1)} \in \left(F^{(\leqslant d)}\right) : f^\infty.$$

To make the computation simpler, we have

$$((\partial_i f_1) \cdot f_2 \cdot \ldots \cdot f_k)^{4d} \in \left(F^{(\leqslant d)}\right) : f^\infty.$$

By induction, we conclude that

$$((\theta_1 f_1) \cdot f_2 \cdot \ldots \cdot f_k)^{4^H d} \in \left(F^{\left(\leqslant d\left(1+4+\ldots+4^H\right)\right)}\right) : f^\infty \subset \left(F^{\left(\leqslant 4^{H+1} d\right)}\right) : f^\infty.$$

Similarly, we obtain

$$\begin{aligned}((\theta_1 f_1) \cdot (\theta_2 f_2) \cdot \ldots \cdot f_k)^{4^{2H} d} \in \left(F^{\left(\leqslant 4^{H+1} d + 4^{H+1} 4^H d\right)}\right) : f^\infty = \\ = \left(F^{\left(\leqslant 4^{H+1} d (1+4^H)\right)}\right) : f^\infty.\end{aligned}$$

Finally, by induction we get

$$\begin{aligned}((\theta_1 f_1) \cdot (\theta_2 f_2) \cdot \ldots \cdot (\theta_k f_k))^{4^{kH} d} \in \left(F^{\left(\leqslant 4^{H+1} d \left(1+4^H+\ldots+4^{(k-1)H}\right)\right)}\right) : f^\infty \subset \\ \subset \left(F^{\left(\leqslant 4^{(k+1)H+1} d\right)}\right) : f^\infty,\end{aligned}$$

which finishes the proof.

Let $(F, \mathcal{C}) \in U$. We call a set $\mathcal{A} \in T$ a **general component** of $(F, \mathcal{C})$ if

$$[\mathcal{A}] \subset [F, \mathcal{C}]. \tag{15}$$

By the termination of the algorithm, the general component $\mathcal{A}$ of $(F, \mathcal{C})$ always exists and

$$[\mathcal{A}] \subset \{F, \mathcal{C}\} \subset \{A\} : H_{\mathcal{A}}^{\infty}.$$

In particular, there exists a general component of F_1, that is, of $(F_1, \varnothing)$.

Recall that $t(F, f)$ is the minimal non-negative integer such that

$$f \in \sqrt{(F^{(\leqslant t(F,f))})}.$$

Lemma 14 *For a finite subset $F \subset \mathbf{k}\{y_1, \ldots, y_n\}$ we have:*

$$t(F, f) \leqslant \operatorname{ord} f + H(F) \cdot 2^{L(F)} + 4^{\left(n \cdot 2^{H(F) \cdot 2^{L(F)}+1}+1\right) \cdot t(G,f)+1} d, \tag{16}$$

where

$$d := \max\left(D(f), A\left(m+7, Q(F)-1\right)\right)^{n \cdot 2^{H(F) \cdot 2^{L(F)}+m+\operatorname{ord} f}}, \tag{17}$$

$G \subset \mathbf{k}\{y_1, \ldots, y_n\}$ *is such that*

$$L(G) \leqslant L(F) - 1 \quad \textit{and} \quad H(G) \leqslant H(F) \cdot 2^{L(F)}$$

and $Q(F)$ is defined in formula (6)*.*

PROOF. Let $\mathcal{A}$ be any general component computed by Algorithm 1 (see (15)) and p be the number of elements of $\mathcal{A}$. Note that

$$p \leqslant n \cdot 2^{H(\mathcal{A})+m}. \tag{18}$$

We then have

$$\{F\} = [\mathcal{A}] : H_{\mathcal{A}}^{\infty} \cap \bigcap_{i=1}^{p} \{F, \mathbf{i}_i\} \cap \bigcap_{i=1}^{p} \{F, \mathbf{s}_i\}.$$

If $1 \in (\mathcal{A}) : H_{\mathcal{A}}^{\infty}$, we have

$$\mathbf{s}_1 \cdot \ldots \cdot \mathbf{s}_p \cdot \mathbf{i}_1 \cdot \ldots \cdot \mathbf{i}_p \in \sqrt{(\mathcal{A})}.$$

Therefore,

$$f \cdot \mathbf{s}_1 \cdot \ldots \cdot \mathbf{s}_p \cdot \mathbf{i}_1 \cdot \ldots \cdot \mathbf{i}_p \in \sqrt{(\mathcal{A})}.$$

Consider now the case when $\mathcal{A}$ is as in Lemma 12 that gives us

$$f \cdot \mathbf{s}_1^{j_1} \cdot \ldots \cdot \mathbf{s}_p^{j_p} \cdot \mathbf{i}_1^{k_1} \cdot \ldots \cdot \mathbf{i}_p^{k_p} \in \left(\mathcal{A}^{(\leqslant \operatorname{ord} f)}\right)$$

for some non-negative integers $j_1, \ldots, j_p$ and $k_1, \ldots, k_p$. Therefore,

$$f \cdot \mathbf{s}_1 \cdot \ldots \cdot \mathbf{s}_p \cdot \mathbf{i}_1 \cdot \ldots \cdot \mathbf{i}_p \in \sqrt{(\mathcal{A}^{(\leqslant \operatorname{ord} f)})}.$$

Hence, by [5, Corollary 1.7], which gives an upper bound for degrees in the algebraic Nullstellensatz when the degrees of the generating polynomials are not equal to two, after squaring all elements of $\mathcal{A}^{(\leqslant \operatorname{ord} f)}$ of degree two, we obtain that

$$(f \cdot \mathbf{s}_1 \cdot \ldots \cdot \mathbf{s}_p \cdot \mathbf{i}_1 \cdot \ldots \cdot \mathbf{i}_p)^d \in \left(\mathcal{A}^{(\leqslant \operatorname{ord} f)}\right), \tag{19}$$

where d is defined by (17). Indeed,

$$n \cdot 2^{H(\mathcal{A})+m+\operatorname{ord} f}$$

bounds the number of algebraic indeterminates in $\mathcal{A}^{(\leqslant \operatorname{ord} f)}$ and f,

$$H(\mathcal{A}) \leqslant H(F) \cdot 2^{L(F)}$$

(because at each step of Algorithm 1 the maximal order doubles at most), and by Corollary 11 we have

$$\max\left(4, D\left(\mathcal{A}^{(\leqslant \operatorname{ord} f)}\right)\right) = \max(4, D(\mathcal{A})) \leqslant A\left(m+7, Q(F)-1\right).$$

We also have

$$1 \in \{F, \mathbf{s}_i\} : f \text{ and } 1 \in \{F, \mathbf{i}_i\} : f$$

for all i, $1 \leqslant i \leqslant p$. Let G be $F, \mathbf{i}_i$ or $F, \mathbf{s}_i$ with the maximal $t(G, f)$. Since in T there exists a general component of G, we have

$$f^{k_j} = f_j + h_j,$$

where $f_j \in \sqrt{(F^{(\leqslant t(G,f))})}$, $h_j \in \sqrt{\left(\mathbf{i}_i^{(\leqslant t(G,f))}\right)}$ or $\sqrt{\left(\mathbf{s}_i^{(\leqslant t(G,f))}\right)}$, and k_j is a natural number. Multiplying the above expressions, we obtain that

$$f^{\sum k_j} = g + h, \tag{20}$$

where $g \in \left(F^{(\leqslant t(G,f))}\right)$ and

$$h \in \left((\theta_1 \mathbf{s}_1) \cdot \ldots \cdot (\theta_p \mathbf{s}_p) \cdot (\theta_1' \mathbf{i}_1) \cdot \ldots \cdot (\theta_p' \mathbf{i}_p) | \operatorname{ord}(\theta_k), \operatorname{ord}(\theta_l') \leqslant t(G, f)\right).$$

Moreover, again since at each step of Algorithm 1 the maximal order doubles at most, we have

$$\left(\mathcal{A}^{(\leqslant q)}\right) \subset \left(F^{(\leqslant q + H(F) \cdot 2^{L(F)})}\right)$$

for any $q \in \mathbb{Z}_{\geqslant 0}$. By Lemma 13 and inclusion (19) we have

$$(\theta_1 \mathbf{s}_1) \cdot \ldots \cdot (\theta_p \mathbf{s}_p) \cdot (\theta'_1 \mathbf{i}_1) \cdot \ldots \cdot (\theta'_p \mathbf{i}_p) \in \sqrt{\left(\mathcal{A}^{\left(\leqslant \operatorname{ord} f + 4^{(2p+1)\cdot t(G,f)+1} d\right)}\right)} : f,$$

where d is defined in (17). Hence,

$$(\theta_1 \mathbf{s}_1) \cdot \ldots \cdot (\theta_p \mathbf{s}_p) \cdot (\theta'_1 \mathbf{i}_1) \cdot \ldots \cdot (\theta'_p \mathbf{i}_p) \in \\ \in \sqrt{\left(F^{\left(\leqslant \operatorname{ord} f + H(F)\cdot 2^{L(F)} + 4^{(2p+1)\cdot t(G,f)+1} d\right)}\right)} : f \qquad (21)$$

for all θ_k and θ'_k with $\operatorname{ord}(\theta_k)$, $\operatorname{ord}(\theta'_k) \leqslant t(G,f)$, $1 \leqslant k \leqslant p$. Thus, from inequality (18) and inclusion (21) it follows that

$$h \in \sqrt{\left(F^{\left(\leqslant \operatorname{ord} f + H(F)\cdot 2^{L(F)} + 4^{\left(2n\cdot 2^{H(\mathcal{A})}+1\right)\cdot t(G,f)+1} d\right)}\right)} : f,$$

which finishes the proof because we have representation (20) and $g \in \left(F^{(\leqslant t(G,f))}\right)$.

Theorem 15 *We have*

$$t(F,f) \leqslant A(m+8, \max(n, H(F \cup f), D(F \cup f))). \qquad (22)$$

PROOF. We begin the proof by recalling Corollary 11, which states that at any stage of Algorithm 1 applied to F the orders and degrees of differential polynomials computed by this algorithm do not exceed the bound

$$E := A\left(m+7, Q(F \cup f) - 1\right),$$

where the function Q is defined in formula (6) and $Q(F \cup f) \geqslant Q(F)$. In particular,

$$\operatorname{ord} f \leqslant E, \quad H(F) \leqslant E,$$

and by Proposition 10

$$L(F) \leqslant \log_2 E.$$

It follows directly from the definition of $Q(F)$ that

$$n \leqslant E, \quad m \leqslant E, \; 100 \leqslant E.$$

Using these inequalities, we can bound the quantity d defined in (17) as

$$d \leqslant E^{E\cdot 2^{E^2+2E}} \leqslant E^{E^{E^E}},$$

whence

$$d \cdot 4^d \leqslant 4^{2d} \leqslant E^{E^{E^{E^E}}}.$$

To simplify the latter formula, we note that

$$\underbrace{k^{k^{k^{\cdots}}}}_{p \text{ times}} \leqslant \underbrace{2^{2^{2^{\cdots}}}}_{pk \text{ times}},$$

for all natural numbers k and p, which can be easily derived by induction, using the inequality $ab \leqslant a^b$, which holds for all natural numbers $a, b \geqslant 2$. Thus we get:

$$d \cdot 4^d \leqslant 4^{2d} \leqslant \underbrace{2^{2^{2^{\cdots}}}}_{5E \text{ times}}.$$

This allows us to obtain the following inequality from Lemma 14 for some $G \subset \mathbf{k}\{y_1, \ldots, y_n\}$ such that $L(G) \leqslant L(F) - 1$ and $H(G) \leqslant H(F) \cdot 2^{L(F)}$:

$$t(F,f)+1 \leqslant E+1+E^2+\left(\underbrace{2^{2^{2^{\cdots}}}}_{5E \text{ times}}\right)^{t(G,f)+1} \leqslant \left(3 \cdot \underbrace{2^{2^{2^{\cdots}}}}_{5E \text{ times}}\right)^{t(G,f)+1} \leqslant$$
$$\leqslant \left(\underbrace{2^{2^{2^{\cdots}}}}_{6E \text{ times}}\right)^{t(G,f)+1}.$$

Now we use the fact that

$$A(4,k) = \underbrace{2^{2^{2^{\cdots}}}}_{k+3 \text{ times}} - 3$$

and simplify the above formula as

$$t(F,f)+1 \leqslant A(4,6E)^{t(G,f)+1},$$

and noting that $A(4,6E) \leqslant A(4,A(5,E-1)) = A(5,E)$ yields

$$t(F,f)+1 \leqslant A(5,E)^{t(G,f)+1}.$$

Now recall that the set G, defined in the proof of Lemma 14, is the set obtained from F by Algorithm 1 by adding to it an initial or separant. If now we take

$$E_G := A\left(m+7, Q(G)-1\right),$$

and let G_2 be the set obtained from G at the next iteration of the Algorithm 1 by adding an initial or separant, we can similarly write

$$t(G,f)+1 \leqslant A(5,E_G)^{t(G_2,f)+1}.$$

We continue recursively writing similar inequalities for $G_2, G_3, \ldots$, noting that the length of this chain does not exceed the number of iterations in Algorithm 1, that is, $L(F) \leqslant \log_2 E$. We note also that all quantities $E, E_G, E_{G_2}, \ldots$ arising in these inequalities can be uniformly bounded by

$$\bar{E} := A\left(m+7, \max\left(9, n, 2^{9E}, E\right)\right) = A\left(m+7, 2^{9E}\right) \leqslant A(m+7, A(4,E)),$$

since the orders and degrees are uniformly bounded by E. Thus, we have

$$t(F,f)+1 \leqslant \underbrace{W^{W^{W^{\cdots}}}}_{E \text{ times}},$$

where $W = A(5,\bar{E})$, which implies that

$$\begin{aligned} t(F,f)+1 \leqslant \underbrace{2^{2^{2^{\cdots}}}}_{WE \text{ times}} &\leqslant A(4,WE) \leqslant A\left(4,W^2\right) \leqslant A(4,A(5,W-1)) = \\ &= A(5,W) \leqslant A\left(5,A\left(6,\bar{E}-1\right)\right) = A\left(6,\bar{E}\right) = \\ &= A(6,A(m+7,A(4,E))) \leqslant A(m+6,A(m+7,A(4,E))) = \\ &= A(m+7,A(4,E)+1)) = \\ &= A(m+7,A(4,A(m+7,Q(F\cup f)-1))+1) \leqslant \\ &\leqslant A(m+7,A(m+6,A(m+7,Q(F\cup f)-1))+1) = \\ &= A(m+7,A(m+7,Q(F\cup f))+1). \end{aligned}$$

Note that

$$Q(F\cup f) \leqslant A(4,B) \leqslant A(m+8,B-1)-1,$$

where $B := \max(n, H(F\cup f), D(F\cup f)) \geqslant 1$, since $n \geqslant 1$. Therefore,

$$\begin{aligned} A(m+7,&A(m+7,Q(F\cup f))+1) \leqslant \\ &\leqslant A(m+7,A(m+7,A(m+8,B-1)-1)+1) \leqslant \\ &\leqslant A(m+7,A(m+7,A(m+8,B-1))-1) = \\ &= A(m+7,A(m+8,B)-1) = \\ &= A(m+8,B). \end{aligned}$$

6 Model-theoretic proof of existence of the bound

The following argument was shown to the authors by Michael Singer. In this section we refer the reader for ultrafilters and construction of ultraproducts to books in model theory, for instance [33,34]. Let $\bar{\mathbf{k}}$ be the differential closure of $\mathbf{k}$ (see [35, Definition 3.2] and the references given there) and $q \in \mathbb{Z}_{\geqslant 0}$. We would like to emphasise that in the statement below we had to *fix in advance* the number r of differential polynomials in F to be able to use ultraproducts. So, in Theorem 16 the variable r is quantified before the bounding function β. However, the constructive bound that we obtained in Theorem 15 *does not have* such a restriction, because it depends solely on the orders and degrees in F and f, but not on the number of elements in F.

Theorem 16 *For every $r \in \mathbb{Z}_{\geqslant 0}$ there exists a function $\beta : {\mathbb{Z}_{\geqslant 0}}^3 \to \mathbb{Z}_{\geqslant 0}$ such that for any $q \in \mathbb{Z}_{\geqslant 0}$ and $F \subset \mathbf{k}\{y_1,\ldots,y_n\}$ with*

$$|F| = r, \quad \max(H(F),D(F)) \leqslant q, \quad \textit{and} \quad 1 \in [F]$$

we have

$$1 \in \left(F^{(\leqslant \beta(q,r,n))}\right).$$

PROOF. Assume that the statement is wrong, that is, there exist r, $q \in \mathbb{Z}_{\geqslant 0}$ such that for any $\alpha \in \mathbb{Z}_{\geqslant 0}$ there exist $p_{1,\alpha}, \ldots, p_{r,\alpha} \in \mathbf{k}\{y_1, \ldots, y_n\}$ with

$$\max(H(p_{ij}), D(p_{ij})) \leqslant q$$

such that

$$1 \in [p_{1,\alpha}, \ldots, p_{r,\alpha}]$$

and

$$1 \neq \sum_{i=1}^{r} \sum_{j=0}^{\alpha} q_{i,j} p_{i,\alpha}^{(j)} \tag{23}$$

for all $q_{i,j} \in \mathbf{k}\{y_1, \ldots, y_n\}$ of order less than or equal to $q + \alpha$. Again, it is essential here that r does not depend on α. For a maximal differential ideal M in the differential ring $\prod_{i \in \mathbb{Z}_{\geqslant 0}} \bar{\mathbf{k}}$ denote the differential ring $\left(\prod_{i \in \mathbb{Z}_{\geqslant 0}} \bar{\mathbf{k}}\right)/M$ by K_M. There is a natural differential ring homomorphism

$$\left(\prod_{i \in \mathbb{Z}_{\geqslant 0}} \bar{\mathbf{k}}\right)\{y_1, \ldots, y_n\} \to K_M\{y_1, \ldots, y_n\} =: R.$$

We shall now make a special choice of the maximal differential ideal M. Let $\mathcal{F}$ be the filter consisting of all cofinite subsets of $\mathbb{Z}_{\geqslant 0}$. Then, there exists an ultrafilter $\mathcal{U}$ containing $\mathcal{F}$. Since the field $\bar{\mathbf{k}}$ is differentially closed, by Łoś' theorem [33, Theorem 8.5.3] the ultraproduct

$$K := \prod \bar{\mathbf{k}}/\mathcal{U}$$

is a differentially closed field with the following property.

Let $\bar{a} = (a_0, a_1, a_2, \ldots)$ and $\bar{b} = (b_0, b_1, b_2, \ldots) \in K$. Then, we have: if $\bar{a} = \bar{b}$ then $a_i = b_i$ for infinitely many indices i. We now take M to be the kernel of the differential ring homomorphism

$$\prod_{i \in \mathbb{Z}_{\geqslant 0}} \bar{\mathbf{k}} \to K.$$

Let $\bar{p_i}$ be the image of $(p_{i,1}, p_{i,2}, p_{i,3}, \ldots)$ in R. This is defined correctly as all $p_{i,j}$ have orders and degrees bounded. Assume that $(z_1, \ldots, z_n) \in (K_M)^n$ is a zero of $\bar{p_i}$ for all i. Then, for each i, $1 \leqslant i \leqslant r$, there exists $V_i \subset \mathbb{Z}_{\geqslant 0}$, $V_i \in \mathcal{U}$, such that

$$p_{i,j}(z_{1,j}, \ldots, z_{n,j}) = 0$$

for all $j \in V_i$, where $(z_{t,1}, z_{t,2}, z_{t,3}, \ldots)$ is mapped to z_t under the mentioned differential ring homomorphism for each t, $1 \leqslant t \leqslant n$. Since $V_1 \cap \ldots \cap V_r \in \mathcal{U}$ and $\varnothing \notin \mathcal{U}$, there is an index

$$j \in V_1 \cap \ldots \cap V_r.$$

Therefore,

$$p_{1,j}(z_{1,j}, \ldots, z_{n,j}) = \ldots = p_{r,j}(z_{1,j}, \ldots, z_{n,j}) = 0.$$

Since $\bar{\mathbf{k}}$ is differentially closed, this contradicts to $1 \in [p_{1,j}, \ldots, p_{r,j}]$ in the differential ring $\bar{\mathbf{k}}\{y_1, \ldots, y_n\}$. Therefore, since the field K_M is differentially closed, we have $1 \in [\bar{p_1}, \ldots, \bar{p_r}]$. Hence, there exist $\gamma \in \mathbb{Z}_{\geqslant 0}$ and differential polynomials $\bar{q_{ij}} \in K_M\{y_1, \ldots, y_n\}$ with $\operatorname{ord} \bar{q_{ij}} < \gamma + q$ so that

$$1 = \sum_{i=1}^{r} \sum_{j=0}^{\gamma} \bar{q_{ij}} \bar{p_i}^{(j)}.$$

Again, due to our choice of M (that is, due to the fact that $\mathcal{U}$ is an ultrafilter), there exists $\alpha \in \mathbb{Z}_{\geqslant 0}$ with $\alpha > \gamma$ such that

$$1 = \sum_{i=1}^{r} \sum_{j=0}^{\gamma} q_{ij} p_{i,\alpha}^{(j)},$$

where $q_{i,j} \in \bar{\mathbf{k}}\{y_1, \ldots, y_n\}$ of order less than $\alpha + q$. Since $p_{i,\alpha} \in \mathbf{k}\{y_1, \ldots, y_n\}$ for all i, $1 \leqslant i \leqslant r$, by taking a basis of $\bar{\mathbf{k}}$ over $\mathbf{k}$ we may assume that in fact $q_{i,j} \in \mathbf{k}\{y_1, \ldots, y_n\}$ for all i and j, $1 \leqslant i \leqslant r$, $0 \leqslant j \leqslant \gamma$. This contradicts to (23). Thus, our initial assumption was wrong.

7 Conclusions

We have obtained the first bound on orders for the differential Nullstellensatz. Surely, one can improve the bound and find many applications of it. A general programme which is being realized here is as follows. The differential elimination algorithms would be very useful for applications if there were faster versions of them. Our work on bounding orders could lead to:

(1) understanding complexity estimates for the differential elimination,
(2) developing combined and separated differential and high performance algebraic algorithms.

One of the ideas is, instead of using the usual differential elimination, perform all differentiations at the beginning of the process and then use only fast algebraic methods. We hope that our bounds will contribute to this programme.

8 Acknowledgements

We thank Michael Singer for very helpful comments, support, and for the model theoretic proof of the differential Nullstellensatz. We are grateful to Daniel Bertrand for encouraging us to solve the problem. We appreciate the help of Erich Kaltofen, Teresa Krick, Alice Medvedev, and Eric Schost in finding references to the previous work on the algebraic version of the effective Nullstellensatz, on bounds for the lengths of monomial sequences, and on model theory. We are grateful to the referees for important suggestions.

References

[1] A. Seidenberg, An elimination theory for differential algebra, University of California publications in Mathematics III (2) (1956) 31–66.

[2] G. Hermann, Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, Mathematische Annalen 95 (1) (1926) 736–788.

[3] E. W. Mayr, A. W. Meyer, The complexity of the word problems for commutative semigroups and polynomial ideals, Advances in Mathematics 46 (3) (1982) 305–329.

[4] W. D. Brownawell, Bounds for the degrees in the Nullstellensatz, Annals of Mathematics 126 (3) (1987) 577–591.

[5] J. Kollár, Sharp effective Nullstellensatz, Journal of the Americal Mathematical Society 1 (4) (1988) 963–975.

[6] L. Caniglia, A. Galligo, J. Heintz, Some new effectivity bounds in computational geometry, in: Applied algebra, algebraic algorithms and error-correcting codes (Rome, 1988), Vol. 357 of Lecture Notes in Computer Science, Springer, Berlin, 1989, pp. 131–151.

[7] N. Fitchas, A. Galligo, Nullstellensatz effectif et conjecture de Serre (théorème de Quillen-Suslin) pour le calcul formel, Mathematische Nachrichten 149 (1990) 231–253.

[8] T. Krick, L. M. Pardo, M. Sombra, Sharp estimates for the arithmetic Nullstellensatz, Duke Mathematical Journal 109 (3) (2001) 521–598.

[9] Z. Jelonek, On the effective Nullstellensatz, Inventiones Mathematicae 162 (1) (2005) 1–17.

[10] T. Dubé, A combinatorial proof of the effective Nullstellensatz, Journal of Symbolic Computation 15 (3) (1993) 277–296.

[11] C. Yap, Fundamental problems of algorithmic algebra, Oxford University Press, New York, 2000.

[12] O. Golubitsky, M. Kondratieva, M. Moreno Maza, A. Ovchinnikov, A bound for Rosenfeld-Gröbner algorithm, Journal of Symbolic Computation 43 (8) (2008) 582–610.

[13] D. Grigoriev, Complexity of quantifier elimination in the theory of ordinary differential equations, Lecture Notes Computer Science 378 (1989) 11–25.

[14] L. D'Alfonso, G. Jeronimo, P. Solernó, On the complexity of the resolvent representation of some prime differential ideals, Journal of Complexity 22 (3) (2006) 396–430.

[15] W. Sweeney, The D-Neumann problem, Acta Mathematica 120 (1968) 223–277.

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

[17] W. Sit, The Ritt-Kolchin theory for differential polynomials, in: Differential Algebra and Related Topics, Proceedings of the International Workshop (NJSU, 2–3 November 2000), 2002, pp. 1–70.

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

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

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

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

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

[23] F. Boulier, D. Lazard, F. Ollivier, M. Petitot, 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, 1995, pp. 158–166.

[24] F. Boulier, D. Lazard, F. Ollivier, M. Petitot, Computing representations for radicals of finitely generated differential ideals, Tech. rep., Université Lille I, LIFL, 59655, Villeneuve d'Ascq, France (1997).

[25] F. Boulier, F. Lemaire, 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, 2000, pp. 38–47.

[26] G. Carrà Ferro, A resultant theory for the systems of two ordinary algebraic differential equations, Applicable Algebra in Engineering, Communication and Computing 8 (6) (1997) 539–560.

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

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

[29] N. Cutland, Computability: An Introduction to Recursive Function Theory, Cambridge University Press, 1980.

[30] G. Moreno Socias, An Ackermannian polynomial ideal, Vol. 539 of Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 1991, pp. 269–280.

[31] G. Moreno Socias, Length of polynomial ascending chains and primitive recursiveness, Mathematica Scandinavica 71 (2) (1992) 181–205.

[32] I. Kaplansky, An Introduction to Differential Algebra, Hermann, Paris, 1957.

[33] W. Hodges, A Shorter Model Theory, Cambridge University Press, Cambridge, 2000.

[34] D. Marker, Model Theory: An Introduction, Springer-Verlag, New York, 2002.

[35] P. J. Cassidy, M. F. Singer, Galois theory of parametrized differential equations and linear differential algebraic group, IRMA Lectures in Mathematics and Theoretical Physics 9 (2007) 113–157.