Order Bounds for the Rosenfeld-Gröbner Algorithm

Richard Gustavson [1] Alexey Ovchinnikov [2] Gleb Pogudin [3]

[1]CUNY Graduate Center

[2]CUNY Queens College and Graduate Center

[3]Moscow State University

Kolchin Seminar in Differential Algebra
5 February 2016

Main Result

Let $\mathbf{k}$ be a differential field of characteristic zero with m commuting derivations $\Delta = \{\partial_1, \ldots, \partial_m\}$, and let $g_1, \ldots, g_r \in \mathbf{k}\{y_1, \ldots, y_n\}$ be differential polynomials in n differential indeterminates such that $\mathrm{ord}(g_i) \leq h$ for all $1 \leq i \leq r$.

There exists a finite collection $C_1, \ldots, C_s$ of characteristic sets of the radical differential ideal $I = \sqrt{[g_1, \ldots, g_r]}$ such that

$$I = \bigcap_{j=1}^{s} [C_j] : H_{C_j}^{\infty},$$

where H_{C_j} is the collection of all initials and separants of elements of C_j, and for all $1 \leq j \leq s$, for all $g \in C_j$,

$$\mathrm{ord}(g) \leq h \cdot f_L,$$

where $\{f_k\}$ is the sequence of Fibonacci numbers and L is the length of the longest antichain sequence in $\mathbb{N}^m \times \{1, \ldots, n\}$ of degree growth bounded by $\{f_k\}$.

Outline

Outline

Ring of Differential Polynomials

Fix a differential field $\mathbf{k}$ of characteristic zero with m commuting derivations $\Delta = \{\partial_1, \ldots, \partial_m\}$. The set of derivative operators is denoted

$$\Theta := \left\{ \partial_1^{i_1} \cdots \partial_m^{i_m} : i_j \in \mathbb{N}, 1 \leq j \leq m \right\}.$$

For a set $Y = \{y_1, \ldots, y_n\}$ of differential indeterminates, let

$$\Theta Y := \{\theta y : \theta \in \Theta, y \in Y\}.$$

Then the ring of differential polynomials over $\mathbf{k}$ is

$$\mathbf{k}\{Y\} = \mathbf{k}\{y_1, \ldots, y_n\} := \mathbf{k}[\theta y : \theta y \in \Theta Y].$$

For $\theta = \partial_1^{i_1} \cdots \partial_m^{i_m} \in \Theta$, the order of θ is defined to be

$$\operatorname{ord}(\theta) := i_1 + \cdots + i_m.$$

For $u = \theta y \in \Theta Y$, define $\operatorname{ord}(u) := \operatorname{ord}(\theta)$, and for $f \in \mathbf{k}\{Y\} \setminus \mathbf{k}$, define $\operatorname{ord}(f)$ to be the maximum order of all derivatives that appear in f.

Rankings on ΘY

A ranking on ΘY is a total order $<$ such that for all $u, v \in \Theta Y$ and all $\theta \in \Theta$, $\theta \neq \mathrm{id}$,

- $u < \theta u$
- if $u < v$, then $\theta u < \theta v$.

The ranking is called orderly if in addition

- if $\mathrm{ord}(u) < \mathrm{ord}(v)$, then $u < v$.

Examples: Let $\mathbf{k} = \mathbb{Q}(t)$ with one derivation ∂_t.

- If $Y = \{y\}$, then there is only one possibly ranking:

$$y < y_t < y_{tt} < \cdots$$

- If $Y = \{y, z\}$, two possible rankings are

$$y < z < y_t < z_t < y_{tt} < \cdots$$

which is an orderly ranking, and

$$y < y_t < y_{tt} < \cdots < z < z_t < z_{tt} < \cdots$$

which is not an orderly ranking.

From now on, we fix an orderly ranking.

Leaders, Initials, and Separants

Let $f \in \mathbf{k}\{Y\} \setminus \mathbf{k}$.

- $\mathrm{lead}(f)$ = derivative $u \in \Theta Y$ of highest rank appearing in f
- $\mathrm{init}(f)$ = leading coefficient of f when written as a univariate polynomial in $\mathrm{lead}(f)$
- $\mathrm{sep}(f)$ = $\mathrm{init}(\delta(f))$ for any $\delta \in \Delta$.

For any $A \subseteq \mathbf{k}\{Y\} \setminus \mathbf{k}$, we let

- $\mathfrak{L}(A) := \{\mathrm{lead}(f) : f \in A\}$
- $I_A := \{\mathrm{init}(f) : f \in A\}$
- $S_A := \{\mathrm{sep}(f) : f \in A\}$
- $H_A := I_A \cup S_A$

(Partially) Reduced Differential Polynomials

Given $f, g \in \mathbf{k}\{Y\} \setminus \mathbf{k}$, we say that f is

- partially reduced with respect to g if no proper derivative of $\mathrm{lead}(g)$ appears in f,
- reduced with respect to g if in addition

$$\deg_{\mathrm{lead}(g)}(f) < \deg_{\mathrm{lead}(g)}(g).$$

Example: Let $\mathbf{k} = \mathbb{Q}(s,t)$ and $Y = \{y\}$, with the ranking

$$y < y_s < y_t < y_{ss} < y_{st} < y_{tt} < \cdots$$

Let $p = (y_s + y_t)(y_{ss})^2 + y_s y_{ss} - y_t$. Then

- $\mathrm{lead}(p) = y_{ss}$
- $\mathrm{init}(p) = y_s + y_t$
- $\mathrm{sep}(p) = 2y_{ss}(y_s + y_t)$.

We have the following:

- p is not partially reduced with respect to $q_1 = y_s + y$,
- p is partially reduced with respect to $q_2 = y_t y_{ss} + (y_s)^2$, but not reduced,
- p is reduced with respect to $q_3 = y_{st} - y_{ss}$.

D-Triangular Sets

For $A \subseteq \mathbf{k}\{Y\} \setminus \mathbf{k}$, we say A is:

- (partially) autoreduced if every element of A is (partially) reduced with respect to every other element
- weak d-triangular if $\mathfrak{L}(A)$ is autoreduced
- d-triangular if A is weak d-triangular and partially autoreduced.

Every autoreduced set is d-triangular, and every weak d-triangular set is finite.

Examples: Over $\mathbb{Q}(s,t)\{y\}$ with ranking

$$y < y_s < y_t < y_{ss} < y_{st} < y_{tt} < \cdots$$

- the set $\{y_{tt} - (y_{ss})^2, y_s - y\}$ is weak d-triangular,
- the set $\{y_{tt} - (y_s)^2, y_s - y\}$ is d-triangular,
- the set $\{y_{tt}, y_s\}$ is autoreduced.

Differential (Partial) Remainders

For any set $S \subseteq \mathbf{k}\{Y\}$, let S^∞ be the multiplicative set containing 1 and generated by S. Let $f \in \mathbf{k}\{Y\}$ and $A \subseteq \mathbf{k}\{Y\}$ a weak d-triangular set.

- A differential partial remainder of f with respect to A, denoted pd-red(f, A), is a differential polynomial such that
  - pd-red(f, A) is partially reduced with respect to A
  - there exists $s \in S_A^\infty$ such that

$$sf \equiv \text{pd-red}(f, A) \bmod [A].$$

- A differential remainder of f with respect to A, denoted d-red(f, A), is a differential polynomial such that
  - d-red(f, A) is reduced with respect to A
  - there exists $h \in H_A^\infty$ such that

$$hf \equiv \text{d-red}(f, A) \bmod [A].$$

There are algorithms to compute both pd-red(f, A) and d-red(f, A) (see Hubert 2003, for example), and they have the property that

$$\text{rank}(\text{pd-red}(f, A)), \text{rank}(\text{d-red}(f, A)) \leq \text{rank}(f).$$

Differential Remainders: Example

We work over $\mathbb{Q}(s,t)\{y\}$ with two derivations ∂_s, ∂_t, with ranking

$$y < y_s < y_t < y_{ss} < y_{st} < y_{tt} < \cdots$$

Let $A = \{(y_t)^2 - y_s, y_{ss} - y_t\}$, which is autoreduced, and $f = y_{st}$.

Then as $2y_t = \mathrm{sep}((y_t)^2 - y_s) \in S_A^\infty \subseteq H_A^\infty$ and

$$2y_t y_{st} - y_{ss} = \partial_s((y_t)^2 - y_s) \in [A]$$
$$2y_t y_{st} - y_t = \partial_s((y_t)^2 - y_s) + (y_{ss} - y_t) \in [A],$$

we can take

- pd-red$(f, A) = y_{ss}$
- d-red$(f, A) = y_t$.

Rankings on Weak D-Triangular Sets

Given $f_1, f_2 \in \mathbf{k}\{Y\} \setminus \mathbf{k}$ such that $\deg_{\mathrm{lead}(f_i)}(f_i) = d_i$, we say

$$\mathrm{rank}(f_1) < \mathrm{rank}(f_2)$$

if $\mathrm{lead}(f_1) < \mathrm{lead}(f_2)$ or if $\mathrm{lead}(f_1) = \mathrm{lead}(f_2)$ and $d_1 < d_2$.

Given two weak d-triangular sets $A = \{A_1, \ldots, A_r\}$ and $B = \{B_1, \ldots, B_s\}$, in each case arranged in increasing rank, we say that $\mathrm{rank}(A) < \mathrm{rank}(B)$ if either:

- there exists a $k \leq \min(r, s)$ such that $\mathrm{rank}(A_i) = \mathrm{rank}(B_i)$ for all $1 \leq i < k$ and $\mathrm{rank}(A_k) < \mathrm{rank}(B_k)$, or
- $r > s$ and $\mathrm{rank}(A_i) = \mathrm{rank}(B_i)$ for all $1 \leq i \leq s$.

A characteristic set of a differential ideal $I \subseteq \mathbf{k}\{Y\}$ is an autoreduced set $C \subseteq I$ of minimal rank among all autoreduced subsets of I.

Outline

Δ-Polynomials

If $u = \partial_1^{i_1} \cdots \partial_m^{i_m} y$ and $v = \partial_1^{j_1} \cdots \partial_m^{j_m} y$ for some $y \in Y$, define the least common derivative of u and v to be

$$\mathrm{lcd}(u, v) := \partial_1^{\max(i_1, j_1)} \cdots \partial_m^{\max(i_m, j_m)} y.$$

For $f, g \in \mathbf{k}\{Y\} \setminus \mathbf{k}$, we define the Δ-polynomial of f, and g, denoted $\Delta(f, g)$, as follows. If $\mathrm{lead}(f)$ and $\mathrm{lead}(g)$ have no common derivatives, set $\Delta(f, g) = 0$. Otherwise, let $\phi, \psi \in \Theta$ be such that

$$\mathrm{lcd}(\mathrm{lead}(f), \mathrm{lead}(g)) = \phi(\mathrm{lead}(f)) = \psi(\mathrm{lead}(g)),$$

and define

$$\Delta(f, g) := \mathrm{sep}(g)\phi(f) - \mathrm{sep}(f)\psi(g).$$

Regular Differential Systems

For an ideal $I \subseteq \mathbf{k}\{Y\}$ and a finite set $S \subseteq \mathbf{k}\{Y\}$, we define the saturation ideal to be

$$I : S^\infty := \{a \in \mathbf{k}\{Y\} : \exists s \in S^\infty \text{ with } sa \in I\}.$$

If I is a differential ideal, then $I : S^\infty$ is also a differential ideal.

A pair (A, H) is called a regular differential system if the following four conditions hold:

- A is a d-triangular set
- H is a set of differential polynomials that are all partially reduced with respect to A
- $S_A \subseteq H^\infty$
- for all $f, g \in A$,

$$\Delta(f, g) \in (\Theta A_{<u}) : H^\infty,$$

where $u = \mathrm{lcd}(\mathrm{lead}(f), \mathrm{lead}(g))$.

Regular Differential Ideals

An ideal of the form $[A] : H^\infty$, where (A, H) is a regular differential system, is called a regular differential ideal.

Theorem 1: Rosenfeld's Lemma (Boulier et.al. 1995)

Let (A, H) be a regular differential system. If a differential polynomial p is partially reduced with respect to A, then

$$p \in [A] : H^\infty \iff p \in (A) : H^\infty.$$

Theorem 2 (Boulier et.a. 1995)

If (A, H) is a regular differential system, then $[A] : H^\infty$ is a radical differential ideal.

Differential Regular Chains

A d-triangular set C is a differential regular chain if it is a characteristic set of $[C] : H_C^\infty$. In this case, we call $[C] : H_C^\infty$ a characterizable differential ideal.

Every prime differential ideal is characterizable for any ranking.
Non-prime characterizable differential ideals exist, but they depend on the ranking.

Theorem 3

If C is a differential regular chain, then for any differential polynomial p,

$$p \in [C] : H_C^\infty \iff \text{d-red}(p, C) = 0.$$

Regular and Characteristic Decompositions

Given a radical differential ideal $I \subseteq \mathbf{k}\{Y\}$, a regular decomposition of I is a finite collection of regular differential systems $\{(A_1, H_1), \ldots, (A_r, H_r)\}$ such that

$$I = \bigcap_{i=1}^{r} [A_i] : H_i^{\infty}.$$

A characteristic decomposition of I is a finite collection of differential regular chains $\{C_1, \ldots, C_s\}$ such that

$$I = \bigcap_{i=1}^{s} [C_i] : H_{C_i}^{\infty}.$$

Outline

Rosenfeld-Gröbner Algorithm

Input: Two finite sets $F, K \subseteq \mathbf{k}\{Y\}$.

Output: The empty set if it is determined that $1 \in \{F\} : K^\infty$, and otherwise, a finite set of regular differential systems $\{(A_1, H_1), \ldots, (A_r, H_r)\}$ such that

$$\{F\} : K^\infty = \bigcap_{i=1}^{r} [A_i] : H_i^\infty.$$

In particular, when K contains the single element 1, then $\{F\} : K^\infty = \{F\}$, so the Rosenfeld-Gröbner algorithm computes a regular decomposition of $\{F\}$.

Our Goal

Given a finite subset $A \subseteq \mathbf{k}\{Y\}$, define

$$\mathcal{H}(A) := \max\{\mathrm{ord}(f) : f \in A\}.$$

Given finite subsets $F, K \subseteq \mathbf{k}\{Y\}$, let $h = \mathcal{H}(F \cup K)$. Our goal is to find an upper bound for

$$\mathcal{H}\left(\bigcup_{(A,H)\in\mathcal{A}} (A \cup H)\right)$$

where $\mathcal{A} = \text{Rosenfeld-Gröbner}(F, K)$, in terms of h, m, and n.

From Regular to Characteristic Decomposition

If we have a decomposition

$$\{F\} : K^\infty = \bigcap_{i=1}^{r} [A_i] : H_i^\infty,$$

we can compute, using only algebraic operations, a decomposition of the form

$$\{F\} : K^\infty = \bigcap_{i=1}^{s} [C_i] : H_{C_i}^\infty,$$

where each C_i is a regular differential chain (for example, Hubert 2003).

Thus, if we have an upper bound on $\bigcup_{i=1}^{r} \mathcal{H}(A_i \cup H_i)$, we will also have an upper bound on $\bigcup_{i=1}^{s} \mathcal{H}(C_i)$.

Applications

- The weak differential Nullstellensatz says that a system of polynomial differential equations $F = 0$ is consistent if and only if $1 \notin [F]$. Thus

$$F = 0 \text{ is consistent } \iff \text{Rosenfeld-Gröbner}(F, \{1\}) \neq \varnothing.$$

- More generally, we can test for membership in a radical differential ideal. Using the Rosenfeld-Gröbner algorithm and its extension, we get regular and characteristic decompositions

$$\{F\} = \bigcap_{i=1}^{r} [A_i] : H_i^\infty = \bigcap_{i=1}^{s} [C_i] : H_{C_i}^\infty.$$

Thus for any $p \in \mathbf{k}\{Y\}$,

$$\begin{aligned} p \in \{F\} &\iff \text{pd-red}(p, A_i) \in (A_i) : H_i^\infty \text{ for all } i \\ &\iff \text{d-red}(p, C_i) = 0 \text{ for all } i. \end{aligned}$$

Algorithm: Rosenfeld-Gröbner, [Hubert, Algorithm 6.11]

Data: F, K finite subsets of $\mathbf{k}\{Y\}$
Result: A set $\mathcal{A}$ of regular differential systems such that:

- $\mathcal{A}$ is empty if it has been detected that $1 \in \{F\} : K^\infty$
- $\{F\} : K^\infty = \bigcap_{(A,H)\in\mathcal{A}} [A] : H^\infty$ otherwise

$\mathcal{S} := \{(F, \varnothing, \varnothing, K)\}$;
$\mathcal{A} := \varnothing$;
while $\mathcal{S} \neq \varnothing$ **do**
  $(G, D, A, H) :=$ an element of $\mathcal{S}$;
  $\bar{\mathcal{S}} = \mathcal{S} \setminus (G, D, A, H)$;
  if $G \cup D = \varnothing$ **then**
    $\mathcal{A} := \mathcal{A} \cup$ auto-partial-reduce(A, H);
  else
    $p :=$ an element of $G \cup D$;
    $\bar{G}, \bar{D} := G \setminus \{p\}, D \setminus \{p\}$;
    $\bar{p} :=$ d-red(p, A);
    if $\bar{p} = 0$ **then**
      $\bar{\mathcal{S}} := \bar{\mathcal{S}} \cup \{(\bar{G}, \bar{D}, A, H)\}$;
    else
      if $\bar{p} \notin \mathbf{k}$ **then**
        $\bar{p}_i := \bar{p} - \mathrm{init}(\bar{p})\,\mathrm{rank}(\bar{p})$;
        $\bar{p}_s := \deg_{\mathrm{lead}(\bar{p})}(\bar{p})\bar{p} - \mathrm{lead}(\bar{p})\,\mathrm{sep}(\bar{p})$;
        $\bar{\mathcal{S}} := \bar{\mathcal{S}} \cup \{\mathrm{update}(\bar{G}, \bar{D}, A, H, \bar{p}), (G \cup \{\bar{p}_s, \mathrm{sep}(\bar{p})\}, \bar{D}, A, H \cup \{\mathrm{init}(\bar{p})\}),$
          $(\bar{G} \cup \{\bar{p}_i, \mathrm{init}(\bar{p})\}, \bar{D}, A, H)\}$;
      end
    end
  end
  $\mathcal{S} := \bar{\mathcal{S}}$;
end
return $\mathcal{A}$;

Update

Algorithm: update, [Hubert, Algorithm 6.10]

Data:

- A 4-tuple (G, D, A, H) of finite subsets of $\mathbf{k}\{Y\}$
- A differential polynomial p reduced with respect to A

Result: Another 4-tuple $(\bar{G}, \bar{D}, \bar{A}, \bar{H})$

$u := \mathrm{lead}(p)$;
$G_A := \{a \in A \mid \mathrm{lead}(a) \in \Theta u\}$;
$\bar{A} := A \setminus G_A$;
$\bar{G} := G \cup G_A$;
$\bar{D} := D \cup \{\Delta(p, a) \mid a \in \bar{A}\} \setminus \{0\}$;
$\bar{H} := H \cup \{\mathrm{sep}(p), \mathrm{init}(p)\}$;
return $(\bar{G}, \bar{D}, \bar{A} \cup \{p\}, \bar{H})$;

Auto-partial-reduce

Algorithm: auto-partial-reduce, [Hubert, Algorithm 6.8]

Data: Two finite subsets A, H of $\mathbf{k}\{Y\}$
Result:

- The empty set if it is detected that $1 \in [A] : H^\infty$
- A set with a single regular differential system (B, K) with $\mathfrak{L}(A) = \mathfrak{L}(B)$, $H_B \subseteq K$, and $[A] : H^\infty = [B] : K^\infty$

$B := \varnothing$;
for $u \in \mathfrak{L}(A)$ *increasingly* **do**
  $b :=$ pd-red(A_u, B);
  if rank$(b) =$ rank(A_u) **then**
    $B := B \cup \{b\}$;
  else
    return $(\varnothing)$;
  end
end
$K := H_B \cup \{\text{pd-red}(p, B) : p \in H \setminus H_A\}$;
if $0 \in K$ **then**
  return $(\varnothing)$;
else
  return $\{(B, K)\}$;
end

Outline

Our Goal

Given a finite subset $A \subseteq \mathbf{k}\{Y\}$, define

$$\mathcal{H}(A) := \max\{\mathrm{ord}(f) : f \in A\}.$$

Given finite subsets $F, K \subseteq \mathbf{k}\{Y\}$, let $h = \mathcal{H}(F \cup K)$. Our goal is to find an upper bound for

$$\mathcal{H}\left(\bigcup_{(A,H)\in\mathcal{A}} (A \cup H)\right)$$

where $\mathcal{A} = \text{Rosenfeld-Gröbner}(F, K)$, in terms of h, m, and n.

Order Upper Bound: History

The only previously known upper bound for the orders of the output of the Rosenfeld-Gröbner algorithm was given by Golubitsky, Kondratieva, Moreno Maza, and Ovchinnikov (2008).

They work with only one derivation, $m = 1$, but with an arbitrary (i.e. not necessarily orderly) ranking.

They show that with $F, K \subseteq \mathbf{k}\{y_1, \ldots, y_n\}$ and $h = \mathcal{H}(F \cup K)$, if $\mathcal{A} = \text{Rosenfeld-Gröbner}(F, K)$, then

$$\mathcal{H}\left(\bigcup_{(A,H)\in\mathcal{A}} (A \cup H)\right) \leq h(n-1)!.$$

Our Strategy

Every $(A, H) \in \mathcal{A}$ is formed by applying the algorithm auto-partial-reduce to a 4-tuple $(\varnothing, \varnothing, A', H') \in \mathcal{S}$. Thus we need:

- to bound how auto-partial-reduce increases the order of a collection of differential polynomials, and
- to bound $\mathcal{H}(G \cup D \cup A \cup H)$ for all (G, D, A, H) added to $\mathcal{S}$ throughout the course of the Rosenfeld-Gröbner algorithm. We accomplish this by:
  - determining when the order of the tuple (G, D, A, H) added to $\mathcal{S}$ is larger than the orders of the previous elements of $\mathcal{S}$,
  - bounding $\mathcal{H}(G \cup D \cup A \cup H)$ in this instance, and
  - bounding the number of times we can add such elements to $\mathcal{S}$.

Sequences in the Rosenfeld-Gröbner Algorithm

There is a sequence

$$\{(G_i, D_i, A_i, H_i)\}_{i=1}^{N}$$

corresponding to each regular differential system

$$(A, H) \in \text{Rosenfeld-Gröbner}(F, K),$$

where $N = N_{(A,H)}$, such that:

- $(G_{i+1}, D_{i+1}, A_{i+1}, H_{i+1})$ is obtained from (G_i, D_i, A_i, H_i) during the while loop,
- $(G_1, D_1, A_1, H_1) = (F, \varnothing, \varnothing, K)$, and
- $(A, H) = \text{auto-partial-reduce}(A_N, H_N)$.

Constructing an Antichain Sequence

We will construct a sequence

$$S = \{s_1, s_2, \dots\} \subseteq \Theta Y$$

inductively going along the sequence $\{(G_i, D_i, A_i, H_i)\}$.

Suppose $S_{j-1} = \{s_1, \dots, s_{j-1}\}$, where $S_0 = \varnothing$. A 4-tuple (G_i, D_i, A_i, H_i) can be obtained from $(G_{i-1}, D_{i-1}, A_{i-1}, H_{i-1})$ in two ways:

- We did not perform the update operation. In this case, we do not append a new element to S.
- We performed update with respect to some $p \in \mathbf{k}\{Y\}$.
  - If there exists $s_k \in S_{j-1}$ such that $\mathrm{lead}(p) \leq s_k$, we do not append a new element to S_{j-1}.
  - Otherwise, we let $s_j = \mathrm{lead}(p)$ and define $S_j = \{s_1, \dots, s_j\}$. In the latter case, we set $k_j = i$.

Order Bounds for Antichain Sequence

An antichain sequence in a partially ordered set P is a sequence of elements $\{s_1, s_2, \dots\}$ that are pairwise incompatible in the partial order.

Define a partial order $\preccurlyeq$ on ΘY as follows. For all $u, v \in \Theta Y$, we say

$$u \preccurlyeq v \iff \text{there exists } \theta \in \Theta \text{ with } \theta u = v.$$

Let $\{s_j\}$ be the sequence constructed from the sequence $\{(G_i, D_i, A_i, H_i)\}$, and let

$$\{f_0, f_1, f_2, f_3, \dots\} = \{0, 1, 1, 2, 3, 5, \dots\}$$

be the Fibonacci sequence.

Theorem 4

The sequence $\{s_j\}$ is an antichain sequence in ΘY and for all $j \geq 1$,

$$\operatorname{ord}(s_j) \leq hf_j.$$

Order Bounds for Intermediate Steps

For a given $i \geq 1$, we let anti-k_i be the minimal $j \in \mathbb{N}_{>0}$ such that $i < k_j$.

Theorem 5

Let $\{f_j\}$ be the Fibonacci sequence. For all $i \geq 1$, we have

- $\mathcal{H}\left(\bigcup_{t=1}^{i}(G_t \cup D_t \cup H_t)\right) \leq hf_{\text{anti-}k_i}$,
- $\mathcal{H}\left(\bigcup_{t=1}^{i} A_t\right) \leq hf_{\text{anti-}k_i - 1}$,
- For all distinct elements of $\bigcup_{t=1}^{i} A_t$, the orders of the least common derivatives of their leaders do not exceed $hf_{\text{anti-}k_i}$.

From ΘY to $\mathbb{N}^m \times \mathfrak{n}$

Let $\mathfrak{n} = \{1, \ldots, n\}$. There is a one-to-one correspondence between ΘY and $\mathbb{N}^m \times \mathfrak{n}$ via

$$\partial_1^{i_1} \cdots \partial_m^{i_m} y_k \in \Theta Y \leftrightarrow ((i_1, \ldots, i_m), k) \in \mathbb{N}^m \times \mathfrak{n}.$$

The degree of an element of $\mathbb{N}^m \times \mathfrak{n}$ is defined to be the order of its corresponding element of ΘY. Every antichain sequence in $\mathbb{N}^m \times \mathfrak{n}$ (and thus of ΘY) is finite.

Given an increasing function $f : \mathbb{N}_{>0} \to \mathbb{N}$, we say that f bounds the degree growth of an antichain sequence $\{s_1, \ldots, s_k\} \subseteq \mathbb{N}^m \times \mathfrak{n}$ if $\deg(s_i) \leq f(i)$ for all $1 \leq i \leq k$.

We let $\mathfrak{L}_{f,m}^n$ be the maximal length of an antichain sequence of $\mathbb{N}^m \times \mathfrak{n}$ with degree growth bounded by f; this number exists by Pierce (2014).

Main Result

Theorem 6

Let $F, K \subseteq \mathbf{k}\{Y\}$ be finite sets with $h = \mathcal{H}(F \cup K)$, let $\mathcal{A} = \text{Rosenfeld-Gröbner}(F, K)$, and let $L = \mathfrak{L}^n_{f,m}$, where $f(i) = f_i$ with $\{f_i\}$ the Fibonacci sequence. Then

$$\mathcal{H}\left(\bigcup_{(A,H)\in\mathcal{A}} (A \cup H)\right) \leq h f_L.$$

Proof of Main Theorem

Since ord(pd-red$(p, B)) \leq$ ord(p) for any $p \in \mathbf{k}\{Y\}$ and weak d-triangular set B,

$$\mathcal{H}(B \cup K) \leq \mathcal{H}(A \cup H),$$

where $\{(B, K)\} =$ auto-partial-reduced(A, H). Hence, it suffices to bound $\mathcal{H}(G \cup D \cup A \cup H)$ whenever the tuple (G, D, A, H) is added to $\mathcal{S}$ in the Rosenfeld-Gröbner algorithm.

The antichain sequence $\{s_j\}$ of ΘY determines an antichain sequence of $\mathbb{N}^m \times \mathfrak{n}$ of degree growth bounded by $f(i)$, so the length of this sequence (and thus the sequence $\{s_j\}$) is at most L.

In Theorem 5, it is shown that for all $i < j :=$ anti-k_i, we have

$$\mathcal{H}\left(\bigcup_{t=1}^{i}(G_t \cup D_t \cup A_t \cup H_t)\right) \leqslant hf_j.$$

Since the largest possible j is the length of the antichain sequence, for every (G_i, D_i, A_i, H_i), we have

$$\mathcal{H}(G_i \cup D_i \cup A_i \cup H_i) \leqslant hf_L.$$

Since every (G, D, A, H) added to $\mathcal{S}$ is equal to (G_i, D_i, A_i, H_i) for some i, this completes the proof.

Lengths of Antichain Sequences

In order to apply our main result, we need to be able to determine $\mathfrak{L}^n_{f,m}$.

Let $f : \mathbb{N}_{>0} \to \mathbb{N}$ be an increasing function, and define

$$\Psi_{f,m} : \mathbb{N}_{>0} \times \mathbb{N}^m \to \mathbb{N}$$

by the following relations:

- $\Psi_{f,m}(i, (0, \ldots, 0, u_m)) = i$,
- $\Psi_{f,m}(i-1, (u_1, \ldots, u_r, 0, \ldots, 0, u_m))$
  $= \Psi_{f,m}(i, (u_1, \ldots, u_r - 1, f(i) - f(i-1) + u_m + 1, 0, \ldots, 0))$

  if $r < m-1, u_r > 0$,
- $\Psi_{f,m}(i-1, (u_1, \ldots, u_m))$
  $= \Psi_{f,m}(i, (u_1, \ldots, u_{m-1} - 1, f(i) - f(i-1) + u_m + 1))$

  if $u_{m-1} > 0$.

Lengths of Antichain Sequences (Continued)

Proposition 7 (León Sánchez and Ovchinnikov 2016)

The maximal length of an antichain sequence in $\mathbb{N}^m$ with degree growth bounded by f does not exceed

$$\Psi_{f,m}(1,(f(1),0,\ldots,0)).$$

Define the sequence $\psi_0, \psi_1, \ldots$ by the relations $\psi_0 = 0$ and

$$\psi_{i+1} = \Psi_{f_i,m}(1,(f_i(1),0,\ldots,0)) + \psi_i,$$

where $f_i(x) = f(x + \psi_i)$.

Proposition 8 (León Sánchez and Ovchinnikov 2016)

The maximal length of an antichain sequence in $\mathbb{N}^m \times \mathfrak{n}$ with degree growth bounded by f does not exceed ψ_n.

Case $m = 2, n = 1$

In this case, the maximal length of an antichain sequence is $h + 1$, given by

$$(h, 0), (h - 1, 1), (h - 2, h + 2), \ldots, (1, hf_h - 1), (0, hf_{h+1}).$$

In this case, the orders of the resulting polynomials are bounded by the single-exponential estimate coming from the standard formula for the Fibonacci numbers,

$$hf_{h+1} = \frac{h}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^{h+1} - \left(\frac{1 - \sqrt{5}}{2} \right)^{h+1} \right).$$

This results in the following table:

h	1	2	3	4	5	6	7
hf_{h+1}	1	4	9	20	40	78	147

Case $m = 2$, n arbitrary

In this case, the maximal length of an antichain sequence does not exceed b_n, where b_n satisfies $b_1 = h + 1$ and $b_{n+1} = hf_{b_n+1} + b_n + 1$, which results in the following table:

n	h	b_n	hf_{b_n}
2	1	5	5
2	2	10	110
2	3	20	20,295
2	4	38	$156,352,676$
2	5	72	$\leq 10^{16}$
3	1	14	377
3	2	189	$\leq 10^{40}$
3	3	32,859	$\leq 10^{6868}$

Case $m = 3, n = 1$

We can construct the maximal length antichain sequence of $\mathbb{N}^3$, resulting in the following sequence:

$$(h,0,0),(h-1,1,0),(h-1,0,h+1),(h-2,2h+2,0),\ldots,$$
$$(h-2,0,hf_{2h+6}-(h-2)),\ldots,(h-i,hf_{c_{i-1}+1}-(h-i),0),\ldots,$$
$$(h-i,0,hf_{c_i}-(h-i)),\ldots,(0,hf_{c_{h-1}+1},0),\ldots,(0,0,hf_{c_h}),$$

where the sequence c_i is given by $c_0 = 1$ and for $1 \leq i \leq h$,

$$c_i = c_{i-1} + 1 + hf_{c_{i-1}+1} - (h-i).$$

As a result, the maximal length of an antichain sequence is equal to c_h, so the maximal order is hf_{c_h}.

Table of Values for $m = 3, 4, 5$

Below is a table of some maximal lengths $\mathfrak{L}^n_{f,m}$ and orders $f(\mathfrak{L}^n_{f,m})$, where $f(i) = hf_i$, for $m = 3$, 4, and 5:

m	n	h	length$\leq$	order$\leq$
3	1	1	3	2
3	1	2	10	110
3	1	3	712	10^{149}
3	2	1	433,494,480	$10^{90,594,989}$
4	1	1	5	5
5	1	1	20	6765

Outline

Order Lower Bound: Goal

Our goal is to find a lower bound for

$$\mathcal{H}\left(\bigcup_{(A,H)\in\mathcal{A}}(A\cup H)\right)$$

where $\mathcal{A} = \text{Rosenfeld-Gröbner}(F, K)$.

We do this by presenting an example that comes from the lower bound on degrees of Gröbner bases.

Rosenfeld-Gröbner on Linear Inputs

Proposition 9

Suppose $F, K \subseteq \mathbf{k}\{Y\}$ are composed of linear differential polynomials. If $\mathcal{A} = \text{Rosenfeld-Gröbner}(F, K)$, then either $\mathcal{A} = \varnothing$ or $\mathcal{A} = \{(A, H)\}$ with both A and H composed of linear differential polynomials.

If F consists of homogeneous linear polynomials, then $[F]$ is prime and

$$\text{Rosenfeld-Gröbner}(F, \{1\}) = \{(A, H)\},$$

with (A, H) a linear regular differential system such that

$$[F] = \{F\} = [A] : H^{\infty}.$$

In this case, A is a characteristic set of $[F]$, so it suffices to find a lower bound on linear characteristic sets of differential ideals.

From Algebraic to Linear Differential Polynomials

There is a one-to-one correspondence between polynomials in $\mathbf{k}[x_1, \ldots, x_m]$ and homogeneous linear differential polynomials in $\mathbf{k}\{y\}$ with m derivations and $\mathbf{k}$ a field of constants via

$$f = \sum c_{i_1,\ldots,i_m} x_1^{i_1} \cdots x_m^{i_m} \leftrightarrow \tilde{f} = \sum c_{i_1,\ldots,i_m} \partial_1^{i_1} \cdots \partial_m^{i_m} y.$$

If we have $f_1, \ldots, f_r \in \mathbf{k}[x_1, \ldots, x_m]$, we get can construct a linear characteristic set $C = \{C_1, \ldots, C_s\}$ of $[\tilde{f}_1, \ldots, \tilde{f}_r] \subseteq \mathbf{k}\{y\}$, with each $C_i = \tilde{g}_i$ for some $g_i \in \mathbf{k}[x_1, \ldots, x_m]$.

Proposition 10

With the notation above, $\{g_1, \ldots, g_s\} \subseteq \mathbf{k}[x_1, \ldots, x_m]$ is a Gröbner basis of the ideal $(f_1, \ldots, f_r)$.

Example

This example is by Möller & Mora (1984), based on work by Mayr & Meyer (1982).

$$
\begin{aligned}
P &:= \mathbf{k}[q_{i,j}, c_{i,j}, b_{i,j}, s_j, f_j : 1 \le i \le 4, 0 \le j \le m] \\
I_0 &:= (s_0 c_{i,0} - f_0 c_{i,0} b_{i,0}^h : 1 \le i \le 4) \\
J_{j-1} &:= I_{j-1} + (s_j - q_{1,j} s_{j-1} c_{1,j-1}, q_{1,j} f_{j-1} c_{1,j-1} b_{1,j-1} - q_{2,j} s_{j-1} c_{2,j-1}, \\
&\qquad q_{2,j} f_{j-1} c_{2,j-1} - q_{3,j} f_{j-1} c_{3,j-1}, \\
&\qquad \{q_{2,j} c_{i,j} f_{j-1} b_{2,j-1} - q_{2,j} c_{i,j} f_{j-1} b_{3,j-1} b_{i,j} : 1 \le i \le 4\}) \\
I_j &:= J_{j-1} + (q_{3,j} s_{j-1} c_{3,j-1} b_{1,j-1} - q_{2,j} s_{j-1} c_{2,j-1} b_{4,j-1}, q_{4,j} s_{j-1} c_{4,j-1} - f_j, \\
&\qquad q_{3,j} s_{j-1} c_{3,j-1} - q_{4,j} f_{j-1} c_{4,j-1} b_{4,j-1}).
\end{aligned}
$$

Theorem 11

Any Gröbner basis of $J_{m-1} \subseteq P$ with respect to a degree-compatible monomial order contains an element of degree at least

$$\frac{1}{2} h^{2^{m-1}} + 4.$$

Example (Continued)

Thus, every linear characteristic set of

$$\tilde{J}_{m-1} \subseteq \mathbf{k}\{y\},$$

where $\mathbf{k}$ is equipped with $14(m+1)$ derivations and the generators of $\tilde{J}_{m-1}$ are of order at most h, must contain an element of order $\frac{1}{2}h^{2^{m-1}} + 4$.

Since the output of the Rosenfeld-Gröbner algorithm in this case is a linear characteristic set, this shows that if

$$\{(A, H)\} = \text{Rosenfeld-Gröbner}(F, \{1\}),$$

then

$$\mathcal{H}(A \cup H) \geq \frac{1}{2}h^{2^{m-1}} + 4.$$

Thank you!

References

- F. Boulier, D. Lazard, F. Ollivier, and 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, pages 158-166, New York, NY, USA, ACM Press (1995) http://dx.doi.org/10.1145/220346.220367.
- O. Golubitsky, M. Kondratieva, M. Moreno Maza, and A. Ovchinnikov, *A bound for Rosenfeld-Gröbner algorithm.* Journal of Symbolic Computation, 43(8):582-610 (2008) http://dx.doi.org/10.1016/j.jsc.2007.12.002.
- R. Gustavson, A. Ovchinnikov, and G. Pogudin, *Bounds for orders of derivatives in differential elimination algorithms* (2016) http://arxiv.org/abs/1602.00246.
- E. Hubert, *Notes on triangular sets and triangulation-decomposition algorithms II: Differential systems.* In U. Langer and F. Winkler, editors, Symbolic and Numerical Scientific Computations, volume 2630 of Lecture Notes in Computer Science, pages 40-87, Springer (2003) http://dx.doi.org/10.1007/3-540-45084-X_2.
- O. León Sánchez and A. Ovchinnikov, *On bounds for the effective differential Nullstellensatz.* Journal of Algebra, 449:1-21 (2016) http://dx.doi.org/10.1016/j.jalgebra.2015.10.009.
- H.M. Möller and F. Mora, *Upper and lower bounds for the degree of Gröbner bases.* Eurosam'84, Lecture Notes in Computer Science, 174:172-183 (1984).