Bounds and Algorithms in Differential Alegbra: the Ordinary Case

Marc Moreno Maza (Univ. of Western Ontario, Canada)

In Collaboration with

Oleg Golubitsky (Queen's Univ., Canada),

Marina V. Kondratieva (Moscow State Univ., Russia) and

Alexey Ovchinnikov (North Carolina State Univ., USA)

Dagstuhl Seminar, July, 2006.

Ordinary Differential Polynomials

- $\mathbb{K}$ ordinary differential field of characteristic zero with derivation $\delta : \mathbb{K} \longmapsto \mathbb{K}$.
- $Y = \{y_1, \ldots, y_n\}$ differential indeterminates.
- $\delta^\infty Y = \{\delta^m y \mid y \in Y, m \in \mathbb{N}\}$ set of the derivatives.
- $\mathbb{K}\{Y\} = \mathbb{K}[\delta^\infty Y]$ endowed with $\delta : \mathbb{K}\{Y\} \longmapsto \mathbb{K}\{Y\}$: differential ring of differential polynomials.
- An ideal $\mathcal{I} \subset \mathbb{K}\{Y\}$ is differential if for all $f \in \mathcal{I}$ we have $\delta f \in \mathcal{I}$.
- For $F \subset \mathbb{K}\{Y\}$, we denote by (F), $[F]$ and $\{F\}$ the ideal, differential ideal and radical differential ideal generated by F.

Ranking

• Fix $\leq$ a ranking: a total order on derivatives such that for all $u, v \in \delta^\infty Y$ we have

$$u < \delta u \ \text{ and } \ u < v \Rightarrow \delta u < \delta v.$$

• For $f \in \mathbb{K}\{Y\} \setminus \mathbb{K}$, let $u_f = \delta^k y_i$ be the derivative of highest rank occurring in f. Then

$$f = \mathrm{i}_f u_f^d + \mathrm{t}_f \ \text{ with } \ d = \deg(f, u_f) \ \text{ and } \ \mathrm{i}_f = \mathrm{lc}(f, u_f).$$

$\mathrm{lv} f := y_i, \ \mathrm{ld} f := u_f, \ \mathrm{rk} f := u_f^d, \ \mathrm{s} f := \frac{\partial f}{\partial u_f} = \mathrm{i}_{\delta f}.$

• The ranks $u_1^{d_1}$ and $u_2^{d_2}$ are compared as follows:

$$u_1^{d_1} \leq u_2^{d_2} \quad \Longleftrightarrow \quad [u_1 < u_2] \ \text{ or } \ [u_1 = u_2 \text{ and } d_1 \leq d_2].$$

Reduction

- $f \in \mathbb{K}\{Y\}$ is algebraically reduced w.r.t. $g \in \mathbb{K}\{Y\} \setminus \mathbb{K}$ if

$$\deg(f, u_g) < \deg(g, u_g).$$

- $f \in \mathbb{K}\{Y\}$ is partially reduced w.r.t. $g \in \mathbb{K}\{Y\} \setminus \mathbb{K}$ if

$$(\forall k > 0)\ \ \deg(f, \delta^k u_g) = 0.$$

- $f \in \mathbb{K}\{Y\}$ is (fully) reduced w.r.t. $g \in \mathbb{K}\{Y\} \setminus \mathbb{K}$ if algebraically and partially reduced w.r.t. g.

- $A \subset \mathbb{K}\{Y\}$ is autoreduced if $\mathbb{A} \cap \mathbb{K} = \varnothing$ and all $f \in A$ is reduced w.r.t all $g \in A \setminus \{f\}$.

- **Proposition.** *Every autoreduced set $\mathbb{A}$ is finite.*

- For autoreduced sets $\mathbb{A}, \mathbb{B} \subset \mathbb{K}\{Y\}$ we write $\boxed{\mathrm{rk}\mathbb{A} \leq \mathrm{rk}\mathbb{B}}$ whenever

$$[\mathrm{rk}\mathbb{B} \subseteq \mathrm{rk}\mathbb{A}] \ \text{ or } \ [\min(\mathrm{rk}\mathbb{A} \setminus \mathrm{rk}\mathbb{B}) < \min(\mathrm{rk}\mathbb{B} \setminus \mathrm{rk}\mathbb{A})].$$

Regular Ideals and Decompositions

• Let $\mathbb{A}, H \subset \mathbb{K}\{Y\}$. Then, the saturated ideal of A w.r.t. H defined by

$$[\mathbb{A}] : H^{\infty} := \{f \in \mathbb{K}\{Y\} \mid (\exists m \in \mathbb{N})\; h^m f \in [\mathbb{A}]\}$$

is $\mathbb{K}\{Y\}$ or a differential ideal containing $[\mathbb{A}]$.

• Define $\mathrm{I}_{\mathbb{A}} = \{\mathrm{i}_f \mid f \in \mathbb{A}\}$, $\mathrm{S}_{\mathbb{A}} = \{\mathrm{s}_f \mid f \in \mathbb{A}\}$ and $H_A = \mathrm{I}_{\mathbb{A}} \cup \mathrm{S}_{\mathbb{A}}$.

• $[\mathbb{A}] : H^{\infty}$ is called regular if: $\mathbb{A}$ is autoreduced, we have $\boxed{H_{\mathbb{A}} \subseteq H}$ and every $h \in H$ is partially reduced w.r.t. all $a \in \mathbb{A}$.

• **Theorem.** (Rosenfeld, 1959) Assume $[\mathbb{A}] : H^{\infty}$ is regular. Then

$$f \in [\mathbb{A}] : H^{\infty} \quad \Longleftrightarrow \quad \mathsf{part\text{-}rem}(f, \mathbb{A}) \in (\mathbb{A}) : H^{\infty}.$$

• **Theorem.** (Boulier, Lazard, Ollivier & Petitot, 1995) If $[\mathbb{A}] : H^{\infty}$ is regular, then it is also radical.

• For $F_0, H_0 \subset \mathbb{K}\{Y\}$, a regular decomposition of $\{F_0\} : H_0^{\infty}$ is a finite set T of pairs $(\mathbb{A}, H)$ with $[\mathbb{A}] : H^{\infty}$ is regular and $\{F_0\} : H_0^{\infty} = \bigcap_{(\mathbb{A},H)\in T} [\mathbb{A}] : H^{\infty}$.

The Rosenfeld-Gröbner Algorithm

Input: $F_0, H_0 \subset \mathbb{K}\{Y\} \setminus \mathbb{K}$.

Output: a regular decomposition of $\{F_0\} : H_0^\infty$.

$T := \varnothing$; $U := \{(F_0, H_0)\}$
while $U \neq \varnothing$ **do**
  Take and remove any $(F, H) \in U$
  Let $\mathbb{C} \subseteq F$ be autoreduced with least rank
  $R := \textsf{full-rem}(F \setminus \mathbb{C}, \mathbb{C}) \setminus \{0\}$
  $K := \textsf{full-rem}(H, \mathbb{C}) \cup H_{\mathbb{C}}$
  if $R \cap \mathbb{K} = \varnothing$ and $0 \notin K$ **then**
    if $R = \varnothing$ **then** $T := T \cup \{(\mathbb{C}, K)\}$
      else $U := U \cup \{(\mathbb{C} \cup R, K)\}$
  for $h \in H_{\mathbb{C}}$ **repeat** $U := U \cup \{(F \cup \{h\}, H)\}$
return T

Order Bound for the RG algorithm: case $n = 2$

• Let $F \subset \mathbb{K}\{y, z\}$. Let $m_y(F)$ and $m_z(F)$ the maximum order of a derivative in F w.r.t y and z. Define $M(F) = m_y(F) + m_z(F)$.

• **Proposition.** For all (F, H) in RG$(F_0, \varnothing)$, we have $\boxed{M(F) \leq M(F_0).}$

PROOF ▷

- For $(F, H) \in U$, consider $\mathbb{C}, H, K$ as above. We have $\boxed{|\mathbb{C}| \leq 2.}$
- First, look at $|\mathbb{C}| = 1$, say $\mathrm{ld}\mathbb{C} = \{y^{(d_y)}\}$. We have:

$$m_y(\mathbb{C} \cup R) = d_y, m_z(\mathbb{C} \cup R) = m_z(F) + (m_y(F) - d_y).$$

- Second, consider $\mathrm{ld}\mathbb{C} = \{y^{(d_y)}, z^{(d_z)}\}$. We have:

$$M(\mathbb{C} \cup R) = d_y + d_z \leq M(F).$$

- Finally, observe: $G \subseteq F \cup H_{\mathbb{C}} \quad \Rightarrow \quad M(G) \leq M(F)$.

◁

A Bound for the Orders in the RG Algorithm

• For $F \subset \mathbb{K}\{Y\}$, we define $m_i(F)$ the maximum order of $y_i \in Y$ in F. Then

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

• We shall establish a modified RG Algorithm such that each intermediate system $(F, H) \in U$ satisfies

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

• We checked this formula for $n = 2$.

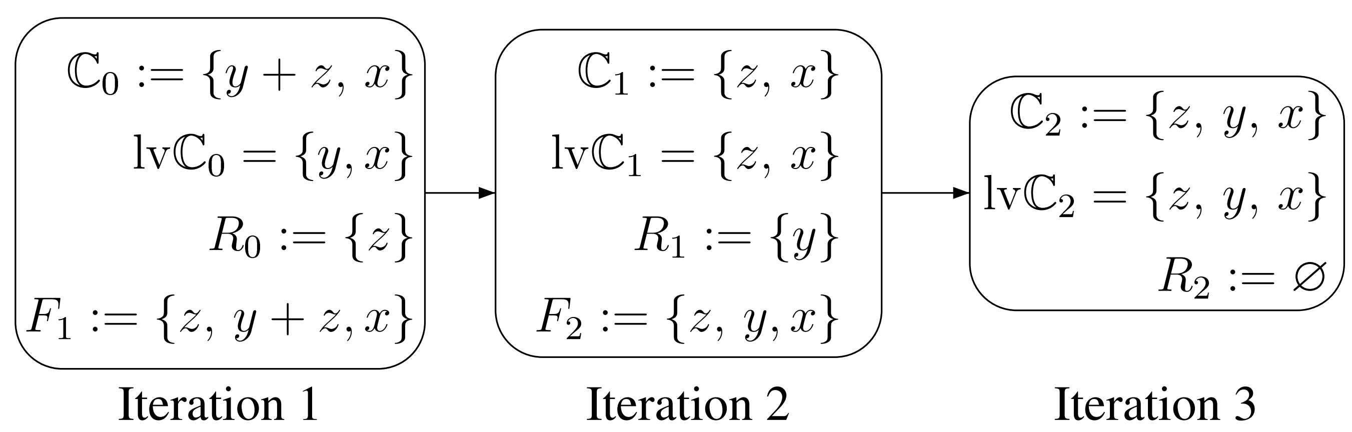
• The techniques used for $n = 2$ are hard to generalize to $n > 2$:

△ Difficulty 1: leading differential indeterminates may become non-leading.

△ Difficulty 2: orders of non-leading ones may increase.

Difficulties with $n > 2$

• Consider $F_0 = \{y + z,\ x,\ x^2 + z\}$ and $H_0 = \varnothing$ for $x > y > z$.



⇒ We will relax the requirement that $\mathbb{C}$ is autoreduced.

Algebraic Computations of Differential Remainders

- Solution 1: use weak d-triangular sets:
  - $\mathbb{C} \subset \mathbb{K}\{Y\} \setminus \mathbb{K}$ is a weak d-triangular set if $\mathrm{ld}\mathbb{C}$ is autoreduced, that is, in the ordinary case

$$(\forall f_1, f_2 \in \mathbb{C})\ f_1 \neq f_2 \Rightarrow \mathrm{lv} f_1 \neq \mathrm{lv} f_2.$$

- Let $\mathbb{C}$ be weak d-triangular subset of F. Define $R := \textsf{part-rem}(F \setminus \mathbb{C}, \mathbb{C})$. If $y_i \notin \mathrm{lv}\mathbb{C}$ we may have $m_i(R) > m_i(F)$ unless the ranking is orderly.

- Solution 2: we construct an algebraic triangular set $\mathbb{B}$ (i.e. leaders are pairwise distinct) such that
  - $\textsf{part-rem}(F \setminus \mathbb{C}, \mathbb{C}) = \textsf{alg-rem}(F, \mathbb{B})$,
  - $\mathbb{B}$ satisfies a bound on the orders of derivatives occurring in it,
  - $\mathbb{B}$ contains a subset $\mathbb{B}^0$ which can be seen as the *partial autoreduction* of $\mathbb{C}$.

The Differentiate&Autoreduce Algorithm Informally

Input: a weak d-triangular set $\mathbb{C} = C_1, \ldots, C_k$ with $\operatorname{ld} \mathbb{C} = y_1^{(d_1)}, \ldots, y_k^{(d_k)}$ and non-negative integers $m_1, \ldots, m_n$ such that $m_i(\mathbb{C}) \leq m_i$ for all $1 \leq i \leq n$.

Output: a triangular set $\mathbb{B}$ which can be seen as the algebraic autoreduction of the differential prolongation of $\mathbb{C}$, i.e. the set

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

• In particular, we have $\operatorname{rk} \mathbb{B} = \operatorname{rk} \tilde{\mathbb{C}}$, unless the process shows $[\mathbb{C}] : H_{\mathbb{C}}^{\infty} = (1)$.

△ Difficulty 3: Making this autoreduction completely algebraic needs some care.

• Consider $\mathbb{C} = \{y_1, y_2 + y_1'\}$ with $m_1 = 1$, $m_2 = 2$, and the elimination raking $y_1 < y_1' < y_1'' < \cdots < y_2 < y_2' < y_2'' < \cdots$.

- Applying the above formula for $\tilde{\mathbb{C}}$ gives $\{y_1, y_1', y_2 + y_1', y_2' + y_1'', y_2'' + y_1'''\}$.
- If polynomials are reduced-and-added to $\mathbb{B}$ in the order of increasing rank

$$\{y_1\} \to \{y_1, y_1'\} \to \{y_1, y_1', y_2\} \to \{y_1, y_1', y_2, y_2'\} \to \{y_1, y_1', y_2, y_2, y_2''\}.$$

The Algorithm Differentiate&Autoreduce

Input: $\mathbb{C} = C_1, \ldots, C_k$ with $\operatorname{ld}\mathbb{C} = y_1^{(d_1)}, \ldots, y_k^{(d_k)}$ and $m_1, \ldots, m_n \in \mathbb{N}$ such that $m_i(\mathbb{C}) \leq m_i$ for all $1 \leq i \leq n$.

Output: $\mathbb{B} = \{B_i^j \mid 1 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant m_i - d_i\}$ with $\operatorname{rk} B_i^j = \operatorname{rk} C_i^{(j)}$ **or** $\{1\}$, if $[\mathbb{C}] : H_{\mathbb{C}}^{\infty} = (1)$ is detected.

$\mathbb{D}$:= $\mathbb{C}$; $\mathbb{B}$:= $\varnothing$
while $\mathbb{D} \neq \varnothing$ **do**
  let $f \in \mathbb{D}$ of the least rank; let $y_i^{(d)} = \operatorname{ld} f$
  $\bar{f}$:= alg-rem$(f, \delta\mathbb{B} \setminus \{f\})$
  if $\operatorname{rk} \bar{f} \neq \operatorname{rk} f$ **then return** $\{1\}$
  $\mathbb{D}$:= $\mathbb{D} \setminus \{f\}$
  if $d < m_i$ **then** $\mathbb{D}$:= $\mathbb{D} \cup \{\delta \bar{f}\}$
  $\mathbb{B}$:= $\mathbb{B} \cup \{\bar{f}\}$
return $\mathbb{B}$

Specifications of the Differentiate&Autoreduce Algorithm

• **Proposition.** The above algorithm satisfies the specifications below:

Input: $\mathbb{C} = C_1, \ldots, C_k$ with $\mathrm{ld}\,\mathbb{C} = y_1^{(d_1)}, \ldots, y_k^{(d_k)}$ and $m_1, \ldots, m_n \in \mathbb{N}$ such that $m_i(\mathbb{C}) \leq m_i$ for all $1 \leq i \leq n$.

Output: $\mathbb{B} = \{B_i^j \mid 1 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant m_i - d_i\}$ with

(i) $\mathrm{rk}\,B_i^j = \mathrm{rk}\,C_i^{(j)}$,

(ii) $\mathbb{B} \subset [\mathbb{B}^0] \subset [\mathbb{C}] \subset [\mathbb{B}] : H_{\mathbb{B}}^{\infty}$, where $\mathbb{B}^0 = \{B_i^0 \mid 1 \leqslant i \leqslant k\}$,

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

(iv) B_i^j are partially reduced w.r.t. $\mathbb{C} \setminus \{C_i\}$,

(v) $$\boxed{m_i(\mathbb{B}) \leqslant \begin{cases} d_i & \text{if} \quad i = 1, \ldots, k \\ m_i + \sum_{j=1}^{k}(m_j - d_j) & \text{if} \quad i = k+1, \ldots, n. \end{cases}}$$

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

Proving the Differentiate&Autoreduce Algorithm

• **Lemma.** Let $\mathbb{C} \subset \mathbb{K}\{Y\}$ be a weak d-triangular set Let $f, g \in \mathbb{K}\{Y\}$ with $\mathrm{lv}\, f \notin \mathrm{lv}\, \mathbb{C}$ and $f \rightarrow_{\mathbb{C}} g$. Then, we have

- $\mathrm{rk}\, g < \mathrm{rk}\, f \;\Rightarrow\; \mathrm{i}_f \in [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$,
- $\mathrm{rk}\, g = \mathrm{rk}\, f \;\Rightarrow\; (\exists\, h \in {H_{\mathbb{C}}}^{\infty})\; h \cdot \mathrm{i}_f - \mathrm{i}_g \in [\mathbb{C}] \text{ and } h \cdot \mathrm{s}_f - \mathrm{s}_g \in [\mathbb{C}]$.

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

• The above lemmas also holds in the PDE case and the purely algebraic case.

Triangular Sets and Characteristic Sets

• $\mathbb{C} \subset \mathbb{K}\{Y\} \setminus \mathbb{K}$ is a triangular set if the elements of $\mathrm{ld}\mathbb{C}$ are pairwise different.

• The triangular set $\mathbb{C}$ is a weak d-triangular set if all $f \in \mathbb{C}$ the leader $\mathrm{ld} f$ is reduced w.r.t. $\mathbb{C} \setminus \{f\}$.

• The weak d-triangular set $\mathbb{C}$ is a d-triangular set if it is partially auto-reduced.

• An autoreduced subset of the lowest rank in $X \subset \mathbb{K}\{Y\}$ is called a (Kolchin) characteristic set of X.

• **Proposition.** Evey $X \subset \mathbb{K}\{Y\}$ admits a characteristic set.

• **Proposition.** Let $\mathcal{I}$ be a proper ideal of $\mathbb{K}\{Y\}$ and $\mathbb{A} \subseteq \mathcal{I}$ autoreduced. Then,

$$\mathbb{A} \text{ characteristic set of } X \iff (\forall f \in \mathcal{I})\ \textsf{full-rem}(f, \mathbb{A}) = 0.$$

• A differential ideal $\mathcal{I} \subset \mathbb{K}\{Y\}$ is characterizable if there exists a Kolchin characteristic set $\mathbb{A}$ of $\mathcal{I}$ such that $\mathcal{I} = [\mathbb{A}] : {H_{\mathbb{A}}}^{\infty}$.

Characteristic Sets and Regular Chains

• Let $\mathbb{C}$ be a triangular set. For all $u \in \mathrm{ld}\mathbb{C}$ define $\mathbb{C}_{\leq u} = \{f \in \mathbb{C} \mid \mathrm{rk} f \leq u\}$, $\mathbb{C}_{<u} = \{f \in \mathbb{C} \mid \mathrm{rk} f < u\}$ and $\mathbb{C}_{\leq u} = \mathbb{C}_{<u} \cup \{C_u\}$. Recall: ODE case.

• $\mathbb{C}$ is a regular chain if for all $u \in \mathrm{ld}\mathbb{C}$ the initial of C_u is non-zero and regular modulo $(\mathbb{C}_{<u}) : \mathrm{I}^{\infty}_{\mathbb{C}_{<u}}$.

• The regular chain $\mathbb{C}$ is separable if for all $u \in \mathrm{ld}\mathbb{C}$ the separant of C_u is non-zero and regular modulo $(\mathbb{C}_{\leq u}) : \mathrm{I}^{\infty}_{\mathbb{C}_{\leq u}}$.

• The regular chain $\mathbb{C}$ is differential if it is a d-triangular set and separable.

• **Theorem.** (Boulier & Lemaire, 2000) Define $\mathbb{A} = \mathsf{Autoreduce}(\mathbb{C})$.

(i) If $\mathbb{C}$ is a differential regular chain, then $\mathbb{A}$ is a characteristic set of $[\mathbb{C}] : H^{\infty}_{\mathbb{C}}$.

(ii) If $\mathbb{C}$ is a characteristic set of $[\mathbb{C}] : H^{\infty}_{\mathbb{C}}$, then $\mathbb{C}$ is a differential regular chain.

Recall: the Rosenfeld-Gröbner Algorithm

Input: $F_0, H_0 \subset \mathbb{K}\{Y\} \setminus \mathbb{K}$.

Output: a regular decomposition of $\{F_0\} : H_0^\infty$.

$T := \varnothing$; $U := \{(F_0, H_0)\}$
while $U \neq \varnothing$ **do**
  Take and remove any $(F, H) \in U$
  Let $\mathbb{C} \subseteq F$ be autoreduced with lowest rank
  $R := \mathsf{full\text{-}rem}(F \setminus \mathbb{C}, \mathbb{C}) \setminus \{0\}$
  $K := \mathsf{full\text{-}rem}(H, \mathbb{C}) \cup H_{\mathbb{C}}$
  if $R \cap \mathbb{K} = \varnothing$ and $0 \notin K$ **then**
    if $R = \varnothing$ **then** $T := T \cup \{(\mathbb{C}, K)\}$
      else $U := U \cup \{(\mathbb{C} \cup R, K)\}$
  for $h \in H_{\mathbb{C}}$ **repeat** $U := U \cup \{(F \cup \{h\}, H)\}$
return T

The Modified Rosenfeld-Gröbner Algorithm

- Instead of handling pairs (F, H) with $F, H \subset \mathbb{K}\{Y\} \setminus \mathbb{K}$
  - representing $\{F\} : H^\infty$
  - to be processed by reducing F, H w.r.t. a characteristic set $\mathbb{C}$ of F,
- the MRGA handles $(F, \mathbb{C}, H)$ with $F, \mathbb{C}, H \subset \mathbb{K}\{Y\} \setminus \mathbb{K}$ and $H_{\mathbb{C}} \subseteq H$,
  - representing $\{F \cup \mathbb{C}\} : H^\infty$, with $\mathbb{C}$ d-triangular,
  - to be processed by

  (1) pushing one $f \in F$ into $\mathbb{C}$ **or** exchanging one $f \in F$ with one $C \in \mathbb{C}$ with $\mathrm{lv} f = \mathrm{lv} C$,

  (2) reducing F, H algebraically w.r.t. a partial prolongation $\mathbb{B}$ of $\mathbb{C}$.

  $\triangle$ Trap: Replacing in RGA characteristic set with weak d-triangular set
  - in each branch $\ldots \to (F_{i,j}, H_{i,j}) \to (F_{i,j+1}, H_{i,j+1}) \to \ldots$ would ensure that we have $\mathrm{lv} C_{i,j} \subseteq \mathrm{lv} C_{i,j+1}$
  - but would not guarantee termination of the algorithm!!!

Input: $F_0, H_0 \subset \mathbb{K}\{Y\} \setminus \mathbb{K}$.

Output: a regular decomposition of $\{F_0\} : H_0^\infty$.

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

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

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

  let $f \in F$ with least rank; let $v = \mathrm{lv} f$

  if $v \in \mathrm{lv}\mathbb{C}$ **then** $D := \{C_v\}$ **else** $D := \varnothing$

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

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

  $\mathbb{B} :=$ Differentiate&Autoreduce $(\bar{\mathbb{C}}, \{m_i(G \cup \bar{\mathbb{C}} \cup H), 1 \leq i \leq n\})$

  if $\mathbb{B} \neq \{1\}$ **then**

    $R :=$ alg-rem$(G, \mathbb{B}) \setminus \{0\}$

    $K :=$ alg-rem$(H, \mathbb{B}) \cup H_{\mathbb{B}}$

    if $R \cap \mathbb{K} = \varnothing$ **and** $0 \notin K$ **then**

      if $R = \varnothing$ **then** $T := T \cup \{(\mathbb{B}^0, K)\}$ **else** $U := U \cup \{(R, \mathbb{B}^0, K)\}$

  for $h \in \{\mathrm{i}_f, \mathrm{s}_f\} \setminus \mathbb{K}$ **repeat** $U := U \cup \{(F \cup \{h\}, \mathbb{C}, H)\}$

return T

The Modified Rosenfeld-Gröbner Algorithm and its Bound

- For $F \subset \mathbb{K}\{Y\}$ recall $M(F) = \sum_{y \in Y} m_y(F)$. For $Z \subset Y$ with $|Z| = k < n$

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

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

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

otherwise

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

Comments on the Previous Results

△ Bad news: The following idea would certainly not lead to an efficient algorithm:

1. Prolongate the input system (F_0, H_0) up to the bound,
2. Emulate the MRGA by some efficient algorithm for algebraic triangular decompositions.

△ Remark: In practice, the regular ideals output by RGA are decomposed into differential regular chains using Gröbner bases (Boulier et al., 1995) or regular chains (Boulier et Lemaire, 2000). Our bound also holds for these differential regular chains.

△ Question: But, may be the idea of prolongation + algebraic emulation is still promising for a simpler problem, such as ranking conversions.

Ranking Conversions via Algebraic Changes of Order

Given: $\mathbb{C}$ characteristic set of prime ideal $\mathcal{I}$ for $\leq$ and a target ranking $\leq'$.

Wanted: $\mathbb{C}'$ characteristic set of $\mathcal{I}$ for $\leq'$.

Idea:

- Consider $\mathbb{D}$ the canonical characteristic set of $\mathcal{I}$ for $\leq'$.
- Assume we know a sufficient differential prolongation of $\mathbb{C}$
  - containing a prime algebraic sub-ideal $\bar{\mathcal{I}}$ in $\mathcal{I}$ with $\mathbb{D} \subset \bar{\mathcal{I}}$,
  - and such that this prolongation is affordable.
- Compute an algebraic characteristic set of $\bar{\mathcal{I}}$ w.r.t. $\leq'$.
- Extract from it a differential characteristic set of $\mathcal{I}$ for $\leq'$.

A Sharper Bound

• **Proposition.** The orders of derivatives occurring in the canonical characteristic set of $\mathcal{I}$ w.r.t. $\leq'$ do not exceed

$$M_1 = |\mathbb{C}| \cdot \max_{C \in \mathbb{C}} \operatorname{ord} C$$

PROOF $\triangleright$

- This was proved by (Golubitsky, Kondratieva and Ovchinnikov, 2005) if $\leq$ is an orderly ranking.
- If $\leq$ is not an orderly ranking, we apply RGA to $(\mathbb{C}, H_{\mathbb{C}})$ for an orderly ranking.
- The number of elements in a characteristic set of a prime (ordinary) differential ideal $\mathcal{I}$ does not depend on the ranking.

$\triangleleft$

Computing the Target Characteristic Set

- Assume that $\mathrm{ld}_{\leq} \mathbb{C} = \{y_1^{(d_1)}, \ldots, y_k^{(d_k)}\}$. Define $m_i = M_1$ for $1 \leq i \leq k$.
- Consider $Q := (\mathbb{A}) : H_{\mathbb{A}}^{\infty}$ where

$$\mathbb{A} = \mathsf{Differentiate\&Autoreduce}(\mathbb{C}, (m_i, 1 \leq i \leq k))$$

Consider $Z := (\delta^{\infty} Y \setminus \delta^{\infty} \mathrm{ld}\mathbb{C}) \cup \mathrm{ld}\mathbb{A}$.

- **Proposition.** We have $Q = \mathcal{I} \cap \mathbb{K}[Z]$. Therefore, Q is a prime (algebraic) ideal of which $\mathbb{A}$ is an algebraic characteristic set for $\leq$.
- **Proposition.** Let $\mathbb{B}$ be an algebraic characteristic set of Q for $\leq'$. For all $y \in Y$, let $E_y \in \mathbb{B}$ with $\mathrm{lv} E_y = y$ and E_y has minimum rank with this property. Let $\mathbb{C}' = \mathsf{Autoreduce}(E_y, y \in Y)$. Then, $\mathbb{C}'$ is a characteristic set of $\mathcal{I}$ for $\leq'$.

Comments on the Previous Results

△ Remark 1: Ranking conversions can be done by algebraic transformations.

△ Remark 2: The bound M_1 can be improved

$$M_{\mathbb{C}} := \min(M_1, M_2) = \min\left(|\mathbb{C}| \cdot \max_{C \in \mathbb{C}} \operatorname{ord} C, \frac{(n-1)!}{(n-|\mathbb{C}|-1)!} \cdot M(\mathbb{C})\right).$$

△ Remark 3: We have a preliminary implementation

- making use of the PALGIE algorithm (Boulier, Lemaire & MMM, 2001) for the algebraic changes of order
- offering performances comparable to RGA on Hubert's test suite.
- We plan to use the modular algorithm for change of order by (Dahan, Jin, MMM & Schost, 2006)
- and compare with the PODI algorithm (Boulier, Lemaire & MMM, 2001).

△ Remark 4: A generalization to the PDE is in progress.

References

[1] P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *Journal of Symbolic Computation*, 28:105–124, 1999.

[2] F. Boulier. Efficient computation of regular differential systems by change of ranking using Kähler differentials. Technical Report 1999-14, LIFL, 1999.

[3] F. Boulier and D. Lazard and F. Ollivier and M. Petitot Representation for the radical of a finitely generated differential ideal In *Proc. ISSAC'95*, pages 158–166, ACM Press, 1995

[4] F. Boulier, F. Lemaire, and M. Moreno Maza. PARDI! In *Proceedings of ISSAC 2001*, pages 38–47. ACM Press, 2001.

[5] X. Dahan, X. Jin, M. Moreno Maza and É. Schost Change of Ordering for Regular Chains in Positive Dimensio Maple Conference 2006

[6] G. Gallo and B. Mishra. Efficient algorithms and bounds for Wu-Ritt

characteristic sets. In *Proc. MEGA'90*, pages 119–142, 1990.

[7] O. Golubitsky. Gröbner walk for characteristic sets of prime differential ideals. In V. Ganzha, E. Mayr, and E. Vorozhtsov, editors, *Proc. 7th Workshop on Comp. Alg. in Sc. Comp.*, pages 207–221. TU München, Germany, 2004.

[8] O. Golubitsky, M. Kondratieva, and A. Ovchinnikov. Canonical characteristic sets of characterizable differential ideals. *Submitted*, 2005.

[9] É. Hubert. Notes on triangular sets and triangulation-decomposition algorithms II: Differential systems. In *Symbolic and Numerical Scientific Computing 2001*, pages 40–87, 2003.

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

[11] M. Moreno Maza. On triangular decompositions of algebraic varieties. Technical Report TR 4/99, NAG Ltd, Oxford, UK, 1999. Presented at the MEGA-2000 Conference, Bath, England.

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

[13] B. Sadik. A bound for the order of characteristic set elements of an ordinary prime differential ideal and some applications. *Applicable Algebra in Engineering, Communication and Computing*, 10(3):251–268, 2000.

[14] 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.

[15] W. T. Wu. A zero structure theorem for polynomial equations solving. *MM Research Preprints*, 1:2–12, 1987.