Bounds and algebraic algorithms for ordinary differential characteristic sets

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

a: School of Computing, Queen's University, Kingston, Ontario, Canada, K7L 3N6, oleg.golubitsky@gmail.com

b: Department of Mechanics and Mathematics, Moscow State University, Leninskie Gory, Moscow, Russia, 119992, kondra_m@shade.msu.ru

c: ORCCA, University of Western Ontario, London, Ontario, Canada, N6A 5B7, moreno@orcca.on.ca

d: Department of Mathematics, North Carolina State University, Raleigh, NC, USA, 27695-8205, aiovchin@ncsu.edu

ISSAC, July, 2006.

Introduction

The Rosenfeld-Gröbner algorithm [1] is a central tool in constructive differential algebra [2,3]. It computes a *regular decomposition* of a radical differential ideal I, i.e., represents I as an intersection of ideals specified by regular systems [1] of differential polynomials. This decomposition allows to solve the membership problem for I.

No complexity estimates are known for the Rosenfeld-Gröbner algorithm. A first natural step towards estimating the complexity is obtaining a bound on the orders of derivatives in the polynomials computed by the Rosenfeld-Gröbner algorithm. For the particular cases of linear systems and systems with two polynomials in two differential indeterminates, relevant bounds are in the works of Jacobi, Ritt [2], Cohn [4], Lando, and Tomasovic. **We prove a bound, which holds for all systems of *ordinary* differential polynomials in n differential indeterminates.**

The performance of Rosenfeld-Gröbner significantly depends on the *ranking* on derivatives. Usually, *elimination rankings* yield more expensive computations than *orderly rankings*. So, the problem of efficient *transformation* of a regular decomposition of a radical differential ideal from one ranking to another arises.

For a prime differential ideal, the problem reduces to the transformation of its *characteristic set* [5,6,7]. We propose a different approach: **an algorithm that transforms the characteristic set algebraically**, taking advantage of the existing efficient techniques for the algebraic case. We have also generalized this approach to address the problem of algebraic transformation of a characteristic decomposition [8] of a radical differential ideal from one ranking to another (omitted in this poster).

Basic concepts

We treat the **ordinary case**, i.e.:

- $\mathbf{k}$ differential field of *characteristic zero* with derivation $\delta : \mathbf{k} \to \mathbf{k}$
- $Y = \{y_1, \ldots, y_n\}$ set of differential indeterminates
- $\Theta Y = \{\delta^i y_j \mid i \geq 0,\ 1 \leq j \leq n\}$ set of derivatives
- $\mathbf{k}\{Y\} = \mathbf{k}[\Theta Y]$ the ring of differential polynomials over $\mathbf{k}$ in n differential indeterminates
- Ranking $\leq$ on derivatives ΘY
- For a differential polynomial f:
  - $\operatorname{lv} f \in Y$ leading variable of f
  - $\operatorname{ld} f = \theta \operatorname{lv} f \in \Theta Y$ leader of f
  - $\operatorname{rk} f = (\operatorname{ld} f)^d$ rank of f
  - $\mathbf{i}_f$ initial of f, $\mathbf{s}_f$ separant of f, $H_f = \{\mathbf{i}_f, \mathbf{s}_f\}$

  For a set of differential polynomials A: $\operatorname{lv} A$, $\operatorname{ld} A$, etc., denote the set of leading variables, the set of leaders, etc., of the elements of A
- Pseudo-reduction relations:
  - f is algebraically reduced w.r.t. A, if no element of $\operatorname{rk} A$ divides a monomial in f
  - f is differentially reduced w.r.t. A, if f is algebraically reduced w.r.t. ΘA
- Algebraically and differentially autoreduced sets
- Characteristic set of F (algebraic or differential): an autoreduced set $A \subset F$ such that no $f \in F$ is reduced w.r.t. A. When the differential characteristic set of F is unique, we denote it $\operatorname{difchar} F$
- Saturated ideals:
  - H^∞ set of all finite products of elements of H
  - $I : H^\infty = \{f \mid \exists h \in H^\infty\ \ hf \in I\}$
- Pseudo-remainders of f w.r.t. A:
  - $\mathsf{algrem}(f, A)$ algebraic pseudo-remainder
  - $\mathsf{d\text{-}rem}(f, A)$ differential pseudo-remainder
  - $\mathsf{d\text{-}rem}(f, A) = \mathsf{algrem}(f, \Theta A)$
- Regular system $(\mathbf{A}, H)$ and ideal $[\mathbf{A}] : H^\infty$:
  - $\mathbf{A}$ is autoreduced
  - H is reduced w.r.t $\mathbf{A}$ and contains $H_{\mathbf{A}}$.

The original Rosenfeld-Gröbner algorithm [1] adapted for the ordinary case:

Algorithm Rosenfeld-Gröbner(F_0, H_0)

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

OUTPUT: a finite set T of regular systems such that $\{F_0\} : H_0^\infty = \bigcap_{(\mathbf{A},H)\in T} [\mathbf{A}] : H^\infty$

```
T := ∅,   U := {(F_0, H_0)}
while U ≠ ∅ do
 | Take and remove any (F, H) ∈ U
 | C := characteristic set of F
 | F̄ := d-rem(F \ C, C) \ {0}
 | H̄ := d-rem(H, C) ∪ H_C
 | if F̄ ∩ k = ∅ and 0 ∉ H̄ then
 | | if F̄ = ∅ then T := T ∪ {(C, H̄)}
 | |            else U := U ∪ {(F̄ ∪ C, H̄)}
 | U := U ∪ {(F ∪ {h}, H) | h ∈ H_C, h ∉ k ∪ H}
return T
```

Bound for the Rosenfeld-Gröbner algorithm

We modify Rosenfeld-Gröbner (based on [8]) to satisfy the following bound. For a differential indeterminate $y \in Y$, let $m_y(F)$ be the maximal order of derivatives of y occurring in F. Let $M(F) = \sum_{y \in Y} m_y(F)$. Then at any intermediate stage of the algorithm

$$M(T \cup U) \leqslant (n-1)! \cdot M(F_0 \cup H_0). \qquad (1)$$

Algorithm RGBound(F_0, H_0)

```
T := ∅,   U := {(F_0, ∅, H_0)}
while U ≠ ∅ do
 | Take and remove any (F, C, H) ∈ U
 | f := an element of F of the least rank
 | D := {g ∈ C | lv g = lv f}
 | G := F ∪ D \ {f}
 | C̄ := C \ D ∪ {f}
 | B := Prolongation(C̄, {m_y(G ∪ C̄ ∪ H) | y ∈ Y})
 | if B ≠ {1} then
 | | F̄ := algrem(G, B) \ {0}
 | | H̄ := algrem(H, B) ∪ H_B
 | | if F̄ ∩ k = ∅ and 0 ∉ H̄ then
 | | | if F̄ = ∅ then T := T ∪ {(difchar B, H̄)}
 | | |            else U := U ∪ {(F̄, difchar B, H̄)}
 | U := U ∪ {(F ∪ {h}, H) | h ∈ H_f, h ∉ k ∪ H}
return T
```

Main changes:

- In the original algorithm, set $\mathbf{C}$ was autoreduced; in Algorithm RGBound, we can only claim that the leading variables of its elements are distinct. As a result, when new pseudo-remainders are replacing old elements of $\mathbf{C}$, no indeterminates disappear from $\operatorname{lv} \mathbf{C}$, i.e., $\operatorname{lv} \bar{\mathbf{C}} \supseteq \operatorname{lv} \mathbf{C}$.
- $\mathsf{d\text{-}rem}(F \setminus \mathbf{C}, \mathbf{C})$ is replaced by $\mathsf{algrem}(G, \mathbf{B})$. Here G plays the role of $F \setminus \mathbf{C}$, while $\mathbf{B}$ is a *differentiated* and *autoreduced* set $\mathbf{C}$ computed by Algorithm Prolongation in such a way that:
  - it can be used in algrem as $\mathbf{C}$ in $\mathsf{d\text{-}rem}$
  - the orders of derivatives of non-leading variables $y \in Y \setminus \operatorname{lv} \bar{\mathbf{C}}$ occurring in $\mathbf{B}$ satisfy

$$m_y(\mathbf{B}) \leq m_y(\bar{\mathbf{C}}) + \sum_{z \in \operatorname{lv} \bar{\mathbf{C}}} [m_z(G \cup \bar{\mathbf{C}} \cup H) - m_z(\operatorname{ld} \bar{\mathbf{C}})].$$

This inequality is the key for proving bound (1).

Algebraic transformation of characteristic sets

1. Given a characteristic set $\mathbf{C}$ of a prime differential ideal I w.r.t. a ranking $\leq$.
2. The orders of derivatives occurring in the canonical characteristic set [9] $\mathbf{D}$ of I w.r.t. any other ranking $\leq'$ do not exceed the bound
$$M := |\mathbf{C}| \cdot \max_{f \in \mathbf{C}} \operatorname{ord} f.$$
3. Algebraic ideal $\bar{I} = I \cap \mathbf{k}\{Y\}_M$, where $\mathbf{k}\{Y\}_M$ is the subring of differential polynomials of order $\leq M$ w.r.t. $\operatorname{lv} \mathbf{C}$, contains $\mathbf{D}$.
4. Compute an algebraic characteristic set of $\bar{I}$ w.r.t. $\leq$:
$$\mathbf{A} := \{\mathsf{algrem}(f, \Theta \mathbf{C} \backslash \{f\}) \mid f \in \Theta \mathbf{C},\ \operatorname{ord} \operatorname{ld} f \leq M\}.$$
5. Given $\mathbf{A}$, compute the canonical algebraic characteristic set $\mathbf{B}$ of $\bar{I}$ w.r.t. $\leq'$, applying one of the existing efficient algebraic algorithms, e.g. [10,11].
6. $\operatorname{difchar} \mathbf{B}$ is the canonical characteristic set of I w.r.t. $\leq'$.

References

[1] F. Boulier, D. Lazard, F. Ollivier, M. Petitot, Representation for the radical of a finitely generated differential ideal, Proc. ISSAC 1995.

[2] J.F. Ritt, *Differential Algebra*, Dover, 1950.

[3] E.R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, 1973.

[4] R. Cohn, The Greenspan bound for the order of differential systems, Proc. AMS, 79(4), 1980.

[5] F. Boulier, Efficient computation of regular differential systems by change of rankings using Kähler differentials, TR Université Lille, 1999.

[6] F. Boulier, F. Lemaire, M. Moreno Maza, PARDI! TR LIFL 2001.

[7] O. Golubitsky, Gröbner walk for characteristic sets of prime differential ideals, Proc. CASC 2004.

[8] E. Hubert, Notes on triangular sets and triangulation-decomposition algorithms II: Differential Systems, Symbolic and Numerical Scientific Computing 2001.

[9] O. Golubitsky, M. Kondratieva, A. Ovchinnikov, Canonical characteristic sets of characterizable differential ideals, Preprint, 2006.

[10] X. Dahan, X. Jin, M. Moreno Maza, É Schost, Change of ordering for regular chains in positive dimension, Proc. Maple Conf. 2006 (to appear).

[11] F. Lemaire, M. Moreno Maza, Y. Xie, The RegularChains library, Proc. Maple Conf. 2005.