Bounds and algebraic algorithms in differential algebra: the ordinary case[1]

Oleg Golubitsky
Ontario Research Centre for Computer Algebra
University of Western Ontario
London, Ontario
Canada, N6A 5B7
oleg.golubitsky@gmail.com

Marina V. Kondratieva
Department of Mechanics and Mathematics
Moscow State University
Leninskie gory, Moscow
Russia, 119 992
kondra_m@shade.msu.ru

Marc Moreno Maza
Ontario Research Centre for Computer Algebra
University of Western Ontario
London, Ontario
Canada, N6A 5B7
moreno@orcca.on.ca

Alexey Ovchinnikov
Department of Mathematics
North Carolina State University
Raleigh, North Carolina
USA, 27695-8205
aiovchin@ncsu.edu

Abstract

Consider the Rosenfeld-Groebner algorithm for computing a regular decomposition of a radical differential ideal. We propose a bound on the orders of derivatives occurring in all intermediate and final systems computed by this algorithm. We also reduce the problem of conversion of a regular decomposition of a radical differential ideal from one ranking to another to a purely algebraic problem.

Keywords: differential algebra, characteristic sets, radical differential ideals, regular decomposition.

1 Introduction

Consider the ring of ordinary differential polynomials $\mathbf{k}\{Y\}$, where $\mathbf{k}$ is a differential field of characteristic 0 with derivation δ, and $Y = \{y_1, \ldots, y_n\}$ is a set whose elements are called differential indeterminates. Let $F \subset \mathbf{k}\{Y\}$ be a set of differential polynomials, then $[F]$ and $\{F\}$ denote the differential and radical differential ideals generated by F in $\mathbf{k}\{Y\}$, respectively. A differential ideal may not have a finite generating system, while a radical differential ideal always has one according to the Basis Theorem [13]. One of the central problems in constructive differential algebra is the problem of computing a canonical representation for a radical differential ideal.

The problem, in general, remains open, but an important contribution to it is provided by the Rosenfeld-Gröbner algorithm [2]. This algorithm inputs a set of differential polynomials F and a ranking [9] on the set of derivatives of the indeterminates. By applying differential pseudo-reductions [13, 9] to the elements of F and considering their initials and separants H_F (these operations depend on the ranking), the algorithm constructs finitely many systems of the form $F_i = 0$, $H_i \neq 0$, where $F_i, H_i \subset \mathbf{k}\{Y\}$, $i = 1, \ldots, m$. At any intermediate step of the algorithm, these systems are equivalent to F: each solution of $F = 0$ is a solution of $F_i = 0,\ H_i \neq 0$ for some i and vice versa. The algorithm terminates when all systems $F_i = 0,\ H_i \neq 0$ become regular [2]. The resulting regular decomposition $\{F\} = \bigcap_{i=1}^m [F_i] : H_i^\infty$ solves the membership problem for $\{F\}$ [2]: $f \in \{F\}$ iff the

[1]The work has been supported by the Russian Foundation for Basic Research, project no. 05-01-00671, by NSF Grant CCR-0096842, by NSERC Grant PDF-301108-2004, and by NSERC Grant RGPIN *Algorithms and software for triangular decompositions of algebraic and differential systems.*

differential pseudo-remainder of f w.r.t. F_i belongs to the algebraic ideal $(F_i) : H_i^\infty$, for all $i \in \{1, \ldots, m\}$.

Computational complexity of the Rosenfeld-Gröbner algorithm is an open problem. Yet for the corresponding algebraic problem of computing a regular decomposition of a radical algebraic ideal in $\mathbf{k}[Y]$, bounds on complexity are known [15]. Thus, the first natural step towards obtaining complexity bounds in the differential case would be estimating the orders of derivatives occurring in the polynomials computed by the Rosenfeld-Gröbner algorithm. For systems of linear differential polynomials and systems of two differential polynomials in two indeterminates, Ritt [12] has proved that the Jacobi bound on the orders holds. The Rosenfeld-Gröbner algorithm was discovered later, but Ritt's techniques provide the starting point for our analysis of this algorithm.

2 Bound on the orders of derivatives

Our first result provides a bound for the orders of derivatives occurring in the systems $F_i = 0,\ H_i \neq 0$ (for an arbitrary ranking). Let $m_i(F)$ be the maximal order of a derivative of the i-th indeterminate occurring in F, and let

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

We propose a modification of the Rosenfeld-Gröbner algorithm, in which for every intermediate system $F_i = 0,\ H_i \neq 0$, we have

$$M(F_i \cup H_i) \leq (n-1)!M(F).$$

Given a set F of differential polynomials and a ranking, the conventional Rosenfeld-Gröbner algorithm at first computes a characteristic set $\mathbb{C}$ of F, i.e., an autoreduced subset of F of the least rank. We replace this computation by that of a weak d-triangular subset of F of the least rank, which we call a *weak characteristic set* of F. A set $\mathbb{C} \subset \mathbf{k}\{Y\} \setminus \mathbf{k}$ is called a weak d-triangular set [8, Definition 3.7], if the set of its leaders $\operatorname{ld}\mathbb{C}$ is autoreduced. In the ordinary case, $\mathbb{C}$ is a weak d-triangular set if and only if the leading differential indeterminates $\operatorname{lv} f$, $f \in \mathbb{C}$, are all distinct. The differential pseudo-remainder of a polynomial f w.r.t. a weak d-triangular set $\mathbb{C}$ is defined via [8, Algorithm 3.13]. Weak characteristic sets satisfy the following property essential for the proof of our bound:

Lemma 1 *Let F be a set of differential polynomials, and let $\mathbb{C}$ be a weak characteristic set of F. Then* $\operatorname{lv}\mathbb{C} = \operatorname{lv} F$*.*

Second, the Rosenfeld-Gröbner algorithm computes the differential pseudo-remainders of $F \setminus \mathbb{C}$ w.r.t. $\mathbb{C}$. The orders of derivatives of non-leading indeterminates (i.e., those not in $\operatorname{lv}\mathbb{C}$) occurring in these pseudo-remainders may be higher than those in F (unless the chosen ranking is orderly). In order to control this growth of orders, we construct a *differential prolongation* of the weak characteristic set $\mathbb{C}$, i.e., an algebraically triangular set $\mathbb{B}$ such that the differential pseudo-reduction of $F \setminus \mathbb{C}$ w.r.t. $\mathbb{C}$ can be replaced by the algebraic pseudo-reduction w.r.t. $\mathbb{B}$. We give the specification of the algorithm computing the differential prolongation, leaving out the details of the computation:

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

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

OUTPUT: set $\mathbb{B} = \{B_i^j \mid 1 \leq i \leq k,\ 0 \leq j \leq m_i - d_i\}$ satisfying

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

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

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

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

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

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

We obtain the following modification of the Rosenfeld-Gröbner algorithm:

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

INPUT: sets of differential polynomials F_0, H_0

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

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

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

3 Algebraic conversion of characteristic sets

Our second result is a reduction of the problem of conversion of a regular decomposition of a radical differential ideal from one ranking to another to a purely algebraic problem. For the algebraic case, efficient modular algorithms are currently being developed [4] and implemented using the `RegularChains` library in Maple [10]; a parallel implementation on a shared memory machine in `Aldor` is also in progress [11].

We note that each regular component $[F_i] : H_i^\infty$ can be decomposed further into an intersection of characterizable differential ideals [7] of the form $I_j = [\mathbb{C}_j] : H_{\mathbb{C}_j}^\infty$, where $\mathbb{C}_j$ is an autoreduced subset of I_j of the least rank (called a characteristic set [9] of I_j). Then we obtain a characteristic decomposition $\{F\} = \bigcap_{j=1}^t I_j$ of the radical differential ideal.

A prime differential ideal I is characterizable w.r.t. any ranking, and for any characteristic set $\mathbb{C}$ of I, we have $I = [\mathbb{C}] : H_{\mathbb{C}}^\infty$. The minimal differential prime components (called the essential prime components) of a characterizable ideal $I = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$ correspond to the minimal prime components of the algebraic ideal $(\mathbb{C}) : H_{C}^{\infty}$ [7]: an autoreduced set $\mathbb{A}$ is a characteristic set of a minimal prime of $(\mathbb{C}) : H_{\mathbb{C}}^{\infty}$ if and only if $\mathbb{A}$ is a characteristic set of an essential prime component of I; the corresponding algebraic and differential prime components are equal to $(\mathbb{A}) : H_{\mathbb{A}}^{\infty}$ and $[\mathbb{A}] : H_{\mathbb{A}}^{\infty}$, respectively. Moreover, the leading derivatives of $\mathbb{A}$ coincide with those of $\mathbb{C}$.

We first consider a **special case**, when the given characterizable ideal $I = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$ is prime, and it is required to convert its characteristic set $\mathbb{C}$ from one ranking to another (the problem of efficient conversion of characteristic sets of prime differential ideals from one ranking to another has been addressed in [1, 3, 5]).

Given the orders of derivatives occurring in $\mathbb{C}$, we provide a bound on the orders of derivatives occurring in a characteristic set of I w.r.t. the target ranking. Based on [14, Theorem 24] (if the target ranking is an elimination ranking) or [6, Theorem 6] (for an arbitrary target ranking), we can show that a bound of $n \cdot \max m_i(\mathbb{C})$ holds.

Using this bound, we find a prime algebraic sub-ideal $J \subset I$, which contains a characteristic set $\bar{\mathbb{C}}$ of I w.r.t. the target ranking. Then we compute the canonical algebraic characteristic set of J w.r.t. the target ranking and extract from it the canonical characteristic set of I.

We have carried out a preliminary implementation of this algorithm in Maple, using the `RegularChains` library.

Now consider the **general case**, when we are given an arbitrary characterizable differential ideal $I = [\mathbb{C}] : H_{\mathbb{C}}^{\infty}$ and need to compute its characteristic decomposition w.r.t. another ranking. Since the essential prime components of I correspond to the minimal primes of the algebraic ideal $(\mathbb{C}) : H_{\mathbb{C}}^{\infty}$, and thus their characteristic sets can be computed from $\mathbb{C}$ without applying differentiations, we have the bound $M = n \cdot \max m_i(\mathbb{C})$ for the characteristic sets of the essential primes of I w.r.t. the target ranking.

Let $d = \max_{f \in \mathbb{C}}(M - \operatorname{ord} \operatorname{ld} f)$, where $\operatorname{ld} f$ denotes the leading derivative of f w.r.t. the initial ranking and $\operatorname{ord} \operatorname{ld} f$ is its order, and let

$$\mathbb{C}^{(d)} = \{f^{(k)} \mid f \in \mathbb{C},\ 0 \le k \le d\}.$$

Applying a purely algebraic (and factorization-free) algorithm to the ideal $J = (\mathbb{C}^{(d)}) : H_{\mathbb{C}}^{\infty}$, we compute its decomposition $J_1' \cap \ldots \cap J_l'$ into algebraic "bi-characterizable" components, i.e., ideals characterizable w.r.t. both initial and target rankings.

We observe that a component J_i', whose characteristic set w.r.t. the initial ranking has a set of leaders distinct from $\operatorname{ld} \mathbb{C}^{(d)}$, is a redundant component, i.e., $J = \cap_{j \neq i} J_j'$. So, we can assume that the characteristic sets of J_i' have leaders equal to $\operatorname{ld} \mathbb{C}^{(d)}$ for all $i = 1, \ldots, l$. We prove then that every minimal prime component Q of J_i' is also a minimal prime component of J, hence it corresponds to an essential prime component P of I.

Now, due to the choice of d, every minimal prime of $J = (\mathbb{C}^{(d)}) : H_{\mathbb{C}}^{\infty}$ contains a differential characteristic set of the corresponding essential prime of I w.r.t. any ranking. We take the canonical algebraic characteristic set of J_i' w.r.t. the target ranking and extract from it the canonical characteristic set $\mathbb{B}_i$ of I_i'. Since the essential primes of I_i' are those essential primes of I that contain the minimal primes of J_i', we obtain a characteristic decomposition w.r.t. the target ranking:

$$I = \bigcap_{i=1}^{l} I_i' = \bigcap_{i=1}^{l} [\mathbb{B}_i] : H_{\mathbb{B}_i}^{\infty}.$$

References

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

[2] F. Boulier, D. Lazard, 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.

[3] F. Boulier, F. Lemaire, and M. Moreno Maza. PARDI! Technical report, LIFL, 2001.

[4] X. Dahan, X. Jin, M. Moreno Maza, and É Schost. Change of ordering for regular chains in positive dimension. In Ilias S. Kotsireas, editor, Maple Conference 2006, pages 26–43, 2006.

[5] 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.

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

[7] E. Hubert. Factorization-free decomposition algorithms in differential algebra. *J. Symb. Comput.*, 29:641–662, 2000.

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

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

[10] F. Lemaire, M. Moreno Maza, and Y. Xie. The `RegularChains` library. In Ilias S. Kotsireas, editor, Maple Conference 2005, pages 355–368, 2005.

[11] M. Moreno Maza and Y. Xie. Parallelization of triangular decomposition. In *Proc. of Algebraic Geometry and Geometric Modeling'06*, Spain, 2006. University of Barcelona.

[12] J.F. Ritt. Jacobi's problem on the order of a system of differential equations. *The Annals of Mathematics*, 36(2):303–312, 1935.

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

[14] 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.

[15] Á. Szántó. *Computation with Polynomial Systems*. PhD thesis, Cornell University, 1999.