ON THE GENERALISED RITT PROBLEM AS A COMPUTATIONAL PROBLEM

OLEG GOLUBITSKY, MARINA KONDRATIEVA, AND ALEXEY OVCHINNIKOV

To our advisor, Eugeny V. Pankratiev

Abstract. The Ritt problem asks if there is an algorithm that tells whether one prime differential ideal is contained in another one if both are given by their characteristic sets. We give several equivalent formulations of this problem. In particular, we show that it is equivalent to testing if a differential polynomial is a zero divisor modulo a radical differential ideal. The technique used in the proof of equivalence yields algorithms for computing a canonical decomposition of a radical differential ideal into prime components and a canonical generating set of a radical differential ideal. Both proposed representations of a radical differential ideal are independent of the given set of generators and can be made independent of the ranking.

1. Introduction

The Ritt problem is an algebraic treatment of the following phenomenon occurring with differential equations. One can show that the solution set to the differential equation $y'^2 - 4y = 0$ consists of a family of parabolae and the zero special solution. The solution set to the equation $y'^2 - 4y^3 = 0$ consists of hyperbolae and the zero solution as well. The major difference between these two solution sets is that in the first case the zero solution is not a limit of the family while in the second case it is. In the algebraic language, the first equation does not generate a prime differential ideal, while the second one does. The Ritt problem is a generalisation of this phenomenon to the case of several non-linear algebraic PDEs.

More precisely, consider a differential polynomial ring over a differential field of characteristic zero. J.F. Ritt has shown that every radical differential ideal can be uniquely represented as a finite intersection of its essential prime components, which are the minimal prime differential ideals containing it. We call the problem of computing the characteristic sets of the essential prime components, given a finite set of generators of a radical differential idea, the generalised Ritt problem. As of today, the problem remains largely unsolved, with some important special cases having been treated by J.F. Ritt, H. Levi, E.R. Kolchin, and R.M. Cohn [12, 14, 18, 3, 4].

We give a precise formulation of this problem as a computational problem, emphasise its dependence on the differential field, and then reformulate the problem to

2000 *Mathematics Subject Classification.* Primary 12H05; Secondary 13N10.

Key words and phrases. Differential algebra, Ritt problem, prime decomposition.

The work was partially supported by the Russian Foundation for Basic Research, project no. 05-01-00671.

The first author was also partially supported by NSERC Grant PDF-301108-2004.

The third author was also partially supported by NSF Grant CCR-0096842.

make it field-independent. One of the versions of the Ritt problem that we discuss here is given in terms of zero-divisors modulo an ideal. In particular, when we test primality by definition for a pair of polynomials each not in the ideal we need to determine whether their product is in the ideal. This sentence has two universal quantifiers, one for each polynomial. We show that it is sufficient to quantify with respect to just one polynomial.

To illustrate these ideas we also exhibit an algorithm whose input is a finite set F of differential polynomials and the output is a collection of prime differential ideals given by their characteristic sets such that:

- the radical differential ideal I generated by F is the intersection of the prime differential ideals and
- this set of prime differential ideals is uniquely determined just by the ideal I and does not depend on the chosen set of generators F.

We hope that the approach we propose in this paper will bring us closer to determining decidability of the Ritt problem.

2. Basic definitions

Let $\mathbf{k}$ be a differential field of characteristic zero with derivations $\Delta = \{\delta_1, \ldots, \delta_m\}$. Let $Y = \{y_1, \ldots, y_n\}$ be a finite set of differential indeterminates and

$$\Theta Y := \left\{\delta_1^{i_1} \cdot \ldots \cdot \delta_m^{i_m} y_j \mid i_k \geqslant 0, 1 \leqslant k \leqslant m;\ 1 \leqslant j \leqslant n\right\}.$$

The ring of differential polynomials $\mathbf{k}\{Y\}$ is the ring of commutative polynomials $\mathbf{k}[\Theta Y]$ with the natural structure of a Δ-ring.

Let I be a radical differential ideal in $\mathbf{k}\{Y\}$, that is, a radical ideal stable under the action of Δ. A prime differential ideal P is called an *essential prime component* of I if $I \subseteq P$ and there is no prime differential ideal Q satisfying $I \subseteq Q \subsetneq P$. According to [18], every radical differential ideal I has finitely many essential prime components and equals their intersection; every prime differential ideal containing I must contain an essential prime component of I; and every set of prime differential ideals whose intersection equals I contains the set of essential prime components of I as a subset. The *generalised Ritt problem* is: given a radical differential ideal, find its essential prime components.

To formulate it as a computational problem, we need to fix an encoding of the input (a radical differential ideal in $\mathbf{k}\{Y\}$), and of the output (a finite set of prime differential ideals in $\mathbf{k}\{Y\}$). A radical differential ideal is usually given by a finite generating set of differential polynomials. To be able to compute with them, we have to assume that $\mathbf{k}$ is a computable differential field. The following definition is directly derived from [17, Definition 5], see [15]:

Definition 1. *A differential ring R is called computable, if there exists an embedding*

$$i : R \to \mathbb{N}$$

such that

1. *The image $i(R)$ is a recursive subset of $\mathbb{N}$*
2. *The addition, multiplication, and derivation functions induced on this image by the addition, multiplication, and derivations on R are computable functions.*

The embedding i in the above definition is called an *admissible indexing* of R. If $\mathbf{k}$ is a computable differential field, then the ring of differential polynomials $\mathbf{k}\{Y\}$ is a computable differential ring: the value of an admissible indexing $j : \mathbf{k}\{Y\} \to \mathbb{N}$ can be effectively computed for each differential polynomial $f \in \mathbf{k}\{Y\}$, given the indices of its coefficients w.r.t. the indexing $i : \mathbf{k} \to \mathbb{N}$ [17].

Having fixed such an indexing j, we can unambiguously say that a differential polynomial $f \in \mathbf{k}\{Y\}$ is *given*, meaning that actually $j(f)$ is given. A prime differential ideal can be given either by a generating set (since it is radical), or by a characteristic set. The latter is defined as follows. Define a ranking on ΘY as a total order relation $\leq$ satisfying:

$$u \leq \delta u, \quad u \leq v \ \Rightarrow \delta u \leq \delta v$$

for all $u, v \in \Theta Y$, $\delta \in \Delta$. For a differential polynomial $f \in \mathbf{k}\{Y\} \setminus \mathbf{k}$, call the derivative of the highest rank effectively present in f the leader of f, denoted $u = \mathrm{ld}_{\leq} f$. If the degree of f w.r.t. u is d, then u^d is called the rank of f, denoted $\mathrm{rk}_{\leq} f$. The ranking then extends to the set of ranks:

$$u_1^{d_1} \leq u_2^{d_2} \iff u_1 < u_2 \text{ or } (u_1 = u_2 \text{ and } d_1 \leq d_2)$$

and to the set of all finite sets of ranks: $R_1 \leq R_2$ iff either $R_1 = R_2$, or else the minimal element of the symmetric difference $(R_1 \setminus R_2) \cup (R_2 \setminus R_1)$ belongs to R_1. All three relations: $\leq$ on the set of derivatives, $\leq$ on the set of ranks, and $\leq$ on the set of finite sets of ranks, are well-orderings.

Rankings are introduced, in order to be able to effectively represent prime differential ideals by their characteristic sets, which allow to test membership and solve other algorithmic problems. The latter are defined as follows.

A differential polynomial f is said to be reduced w.r.t. a differential polynomial g, if for any derivative operator $\theta \in \Theta$, the degree of f w.r.t. to the the leader of θg is less than that of θg. A set of differential polynomials is called autoreduced, if each element of this set is reduced w.r.t. the rest. Every autoreduced set is finite. Among all autoreduced subsets of a given set of differential polynomials X, choose one with the least set of ranks (which exists, because $\leq$ is a well-ordering on the set of finite sets of ranks). This set is called a characteristic set of X. Note that the characteristic set may not be unique, but its set of ranks is.

Consider a differential polynomial f as a polynomial in its leader u. Then the leading coefficient of f is called its initial, and the initial of any proper derivative θf, where $\theta \in \Theta \setminus \{1\}$, is called the separant of f. For a finite set $\mathcal{C}$ of differential polynomials, denote by $H_{\mathcal{C}}$ the product of the initials and separants of its elements. It is a well-known fact (see e.g. [12]) that every prime differential ideal P can be represented by its characteristic set $\mathcal{C}$ as

$$P = [\mathcal{C}] : H_{\mathcal{C}}^{\infty},$$

that is, as the differential ideal generated by $\mathcal{C}$ and saturated by the initials and separants of $\mathcal{C}$. We will extensively exploit this representation in the paper.

3. Main result

3.1. **Different ways of posing the Ritt problem.** We give a list of equivalent formulations of the Ritt problem below and will use one of them to attack the problem. We note that the equivalence takes place only for the fields $\mathbf{k}$ with a *splitting algorithm*, that is, an algorithm which, given a univariate polynomial $f \in$

$\mathbf{k}[x]$, determines whether f is irreducible. This requirement is usually imposed in the context of polynomial factorisation problems over $\mathbf{k}$ (see, e.g., [20, 16]). Examples of computable fields with splitting algorithm include the fields of rational numbers and rational functions, and their algebraic closures. An example of a computable field without splitting algorithm is given in [16]: take a computably enumerable but non-computable subset S of the natural numbers, and consider the field $\mathbb{Q}[\sqrt{p_n} : n \in S]$, where p_n is the n-th prime. By considering the field of fractions over this field, we obtain a non-trivial differential field without splitting algorithm. As in [15, Section 5], we suggest to think of the Ritt problem, especially of its third and fourth formulations in the theorem below, as a generalisation of the polynomial factorisation problem.

Theorem 1. *The following problems are equivalent over a computable differential field of characteristic zero with a splitting algorithm (an algorithmic solution for any one of them will also provide algorithms for the rest):*

(1) *Given a characteristic set of a prime differential ideal, find a set of its generators.*
(2) *Given the characteristic sets of two prime differential ideals I_1 and I_2, determine whether $I_1 \subset I_2$.*
(3) *Compute a non-redundant prime decomposition of a radical differential ideal.*
(4) *Given a radical differential ideal specified by a set of generators, determine whether it is prime.*
(5) *Given a radical differential ideal specified by a set of generators, compute its prime decomposition together with the generators of the prime components as radical differential ideals.*
(6) *Given a radical differential ideal I specified by a set of generators and a differential polynomial f, determine whether f is a zero-divisor modulo I.*

Proof. $1 \Rightarrow 2$ Assume that we have an algorithm for finding generators of a prime differential ideal specified by its characteristic set. Applying this algorithm to the characteristic set of I_1, compute its generator system F_1, i.e., $I_1 = \{F_1\}$. Then $I_1 \subset I_2$ if and only if $F_1 \subset I_2$.

$2 \Rightarrow 3$ Given a radical differential ideal $\{F\}$, one can apply the Ritt-Kolchin algorithm [12, Section IV.9], [13, Algorithm 5.5.15], [19, Section 10] to compute its prime decomposition

$$\{F\} = P_1 \cap \ldots \cap P_k,$$

where each prime component is represented by its characteristic set.

Note that the Ritt-Kolchin algorithm requires to test whether algebraic ideals of the form $(\mathcal{C}) : H_{\mathcal{C}}^{\infty}$, where $\mathcal{C}$ is a coherent [12, Section III.8] autoreduced set, are prime and, if not, to find two polynomials not from the ideal, whose product belongs to the ideal. Apart from this test, the Ritt-Kolchin algorithm can be executed over any computable differential field of characteristic zero.

The special case of $\mathcal{C}$ consisting of a single univariate polynomial shows that the existence of a splitting algorithm over $\mathbf{k}$ is necessary for the above primality test. We will show that it is also sufficient. For the proof of sufficiency of slightly stronger requirements see [13, Section 5.5].

Indeed, if $\mathcal{C}$ is coherent autoreduced, then the ideal $(\mathcal{C}) : H_{\mathcal{C}}^{\infty}$ is radical [2, 9]. A basis of this ideal can be computed over any computable field using Gröbner bases [5, Section 4.4]. Then, the generators of the associated primes of the ideal can be computed over any computable field with the splitting algorithm [6]. If there is only one associated prime, the ideal is prime. Otherwise, by picking in each associated prime a polynomial that does not belong to the other associated primes (which can be done with Gröbner bases over any computable field), we can find the required product.

Assume that we have an algorithm for checking inclusion of prime differential ideals. Then in the above decomposition we can remove all redundant components, i.e., those P_i that contain another P_j. The resulting components will be essential, since any prime decomposition of a radical ideal contains all essential components. Hence, we obtain the non-redundant (essential) decomposition of $\{F\}$.

$3 \Rightarrow 4$ Assume that we have an algorithm for computing a non-redundant (=essential) prime decomposition of a radical differential ideal $\{F\}$. Then $\{F\}$ is prime if and only if this decomposition consists of one component.

$4 \Rightarrow 1$ Given a characteristic set $\mathcal{C}$ of a prime differential ideal P. Consider the algebraic ideals $J_i = \left(\mathcal{C}^{(i)}\right) : H_{\mathcal{C}}^{\infty}$, $i = 0, 1, 2, \ldots$, where

$$\mathcal{C}^{(i)} = \{\theta f \mid \operatorname{ord}\theta \leq i,\ f \in \mathcal{C}\}.$$

Let F_i be a system of generators of J_i (e.g., its Gröbner basis). By the basis theorem, there exists an index i such that $\{F_i\} = P$.

Assume that we have an algorithm for determining whether a radical differential ideal $\{F\}$ is prime. Applying this algorithm to $\{F_i\}$, $i = 0, 1, 2, \ldots$, find the least i such that $\{F_i\}$ is prime. Then, since $\mathcal{C}$ is a characteristic set of $\{F_i\}$, we will have $\{F_i\} = P$, hence F_i generates P as a radical differential ideal.

$1 \Rightarrow 5$ Given a radical differential ideal, one can apply the Ritt-Kolchin algorithm to compute its prime decomposition, where each prime component is represented by its characteristic set. Assuming that we have an algorithm for computing generators of a prime differential ideal, given its characteristic set, we obtain the generators of the components.

$5 \Rightarrow 3$ Assume that we have an algorithm for computing a prime decomposition of a radical differential ideal together with the generators of the prime components. Then we can check inclusion of the components as in the proof $1 \Rightarrow 2$ and thus exclude redundant components as in $2 \Rightarrow 3$.

$3 \Rightarrow 6$ Assume that we have an algorithm for computing an essential prime decomposition $I = P_1 \cap \ldots \cap P_k$ of a radical differential ideal $I = \{F\}$.

Lemma 1. *A differential polynomial f is a zero-divisor modulo I if and only if it belongs to an essential prime component of I.*

Proof. Let f be a zero-divisor modulo I. Then by definition there exists a differential polynomial $g \notin I$ such that $fg \in I$. Since $g \notin I$, there exists an essential prime component P_i of I which does not contain g, yet $fg \in I$ implies $fg \in P_i$. Since P_i is prime, we obtain $f \in P_i$.

Vice versa, let f be an element of an essential prime component of I. Let $P_{i_1}, \ldots, P_{i_l}$ be the essential prime components of I not containing f.

Then for the ideal $I : f = \{g \mid gf \in I\}$, we have

$$I : f = (P_1 \cap \ldots \cap P_k) : f = (P_1 : f) \cap \ldots \cap (P_k : f) = P_{i_1} \cap \ldots \cap P_{i_l}.$$

Since $P_1 \cap \ldots \cap P_k$ is a non-redundant prime decomposition of I, we obtain $I : f \neq I$, hence f is a zero-divisor modulo I. □

Example 1. *Consider the examples we mentioned in the introduction. Let* $J_1 = \{y'^2 - 4y\}$, $J_2 = \{y'^2 - 4y^3\} \subset \mathbf{k}\{Y\}$. *Their prime decompositions are*

$$J_1 = \left[y'^2 - 4y\right] : y'^\infty \cap [y]$$

and

$$J_2 = \left[y'^2 - 4y^3\right] : y'^\infty \cap [y].$$

Differentiating $y'^2 - 4y$, *we obtain that the polynomial* y' *is a zero-divisor modulo* J_1 *and, therefore, the component* $[y]$ *is essential for* J_1*. On the other hand, according to the results of Ritt (see* [18]*, a slightly different proof of this was given by Cohn), to compute generators of the main component of a first order equation it is sufficient to differentiate it as many times as its degree. Computing the Gröbner basis of the algebraic saturated ideal we obtain that* y' *is not essential for* J_2*. By Lemma 1, this means that* y' *is not a zero-divisor modulo* J_2 *and* J_2 *is prime.*

$6 \Rightarrow 1$ The proof of this implication is similar to $[4 \Rightarrow 1]$.

Given a characteristic set $\mathcal{C}$ of a prime differential ideal P. Consider the algebraic ideals $J_i = \left(\mathcal{C}^{(i)}\right) : H_\mathcal{C}^\infty$, $i = 0, 1, 2, \ldots$. Let F_i be a system of generators of J_i. By the basis theorem, there exists an index i such that $\{F_i\} = P$. Note that the product $H_\mathcal{C}$ of initials and separants of $\mathcal{C}$ is not a zero-divisor modulo $\{F_i\}$, since

$$P = \{F_i\} \subseteq \{F_i\} : H_\mathcal{C}^\infty \subseteq [\mathcal{C}] : H_\mathcal{C}^\infty = P.$$

Assume that we have an algorithm for determining whether a polynomial f is a zero-divisor modulo a radical differential ideal $\{F\}$. Applying this algorithm to $H_\mathcal{C}$ and $\{F_i\}$, $i = 0, 1, 2, \ldots$, find the smallest index i such that the $H_\mathcal{C}$ is not a zero-divisor modulo $\{F_i\}$ (as we have shown above, such an index exists). Then $\{F_i\} : H_\mathcal{C}^\infty = \{F_i\}$. On the other hand, $\{F_i\} : H_\mathcal{C}^\infty = P$, since $\mathcal{C} \subset \{F_i\}$. Thus, $\{F_i\} = P$.

□

3.2. **Canonical prime decomposition of a radical differential ideal.** In this section we will show how one can produce a prime decomposition of a radical differential ideal I given by a finite set of generators F that does not depend on this particular choice of generators. A good candidate for this decomposition would be the essential prime decomposition but, again, it is still unknown whether the latter is computable. Our procedure is based on two simple observations contained in Lemma 2 and Proposition 1.

Assume that a ranking is fixed. Then a prime differential ideal has a canonical characteristic set uniquely determined by the ideal [1, 8, 10, 11]. And given $F \subset \mathbf{k}\{Y\}$ we can compute some prime decomposition

$$I = \{F\} = \bigcap_{i=1}^{k} [\mathcal{C}_i] : H_{\mathcal{C}_i}^\infty, \tag{1}$$

where $\mathcal{C}_i$ are the canonical characteristic sets of the corresponding prime differential ideals.

Lemma 2. *Let $\mathcal{C}$ be a characteristic set of the highest rank among $\mathcal{C}_1, \ldots, \mathcal{C}_k$. Then the ideal $P := [\mathcal{C}] : H_{\mathcal{C}}^\infty$ is an essential prime component of I of the highest rank, among all essential prime components of I.*

Proof. Let $Q = [\mathcal{B}] : H_{\mathcal{B}}^\infty$, where $\mathcal{B}$ is the canonical characteristic set of Q, be an essential prime component of I such that $P \supseteq Q$. Because of this inclusion and the definition of the characteristic set as an autoreduced subset of the least rank, we have $\operatorname{rk}\mathcal{C} \le \operatorname{rk}\mathcal{B}$. Moreover, since Q is an essential prime component of I, it must be among the ideals $[\mathcal{C}_i] : H_{\mathcal{C}_i}^\infty$, $i = 1, \ldots, k$, which means that $\mathcal{B} = \mathcal{C}_l$ for some l, $1 \leqslant l \leqslant k$. Thus, due to the choice of $\mathcal{C}$, we have $\operatorname{rk}\mathcal{C} \ge \operatorname{rk}\mathcal{B}$. We conclude therefore that $\operatorname{rk}\mathcal{C} = \operatorname{rk}\mathcal{B}$. Hence, according to [8, Lemma 13], prime differential ideals P and Q are equal. □

Proposition 1. *Let $I = \{F\}$ be a radical differential ideal, and let $\mathcal{C} = C_1, \ldots, C_l$ be a finite set of differential polynomials satisfying $\mathcal{C} \subset I \subset [\mathcal{C}] : H_{\mathcal{C}}^\infty$. Then* [1]

$$I = [\mathcal{C}] : H_{\mathcal{C}}^\infty \cap I : C_1 \cap \ldots \cap I : C_l \cap \{F \cup H_{\mathcal{C}}\}.$$

Proof. Let

$$f \in [\mathcal{C}] : H_{\mathcal{C}}^\infty \cap I : C_1 \cap \ldots \cap I : C_l \cap \{F \cup H_{\mathcal{C}}\}.$$

Then

$$C_i \cdot f \in I,\ 1 \leqslant i \leqslant l$$

and there exists $h \in H_{\mathcal{C}}^\infty$ such that

$$h \cdot f \in [\mathcal{C}].$$

We then have

$$h \cdot f^2 \in f \cdot [\mathcal{C}] \subset \{f \cdot C_1, \ldots, f \cdot C_l\} \subset I.$$

and, therefore, $f \in \{F\} : H_{\mathcal{C}}^\infty$. Since due to, for example, [9, Proposition 2.1]

$$\{F\} = \{F\} : H_{\mathcal{C}}^\infty \cap \{F \cup H_{\mathcal{C}}\},$$

we conclude that $f \in I$. The other inclusion follows from $I \subset [\mathcal{C}] : H_{\mathcal{C}}^\infty$. □

If in decomposition (1) there are several characteristic sets of the highest rank, say, $\mathcal{C}_1, \ldots, \mathcal{C}_q$, and $\mathcal{C}_i = C_{i,1}, \ldots, C_{i,p_i}$, $1 \leqslant i \leqslant q$, then

$$I = [\mathcal{C}_1] : H_{\mathcal{C}_1}^\infty \cap I : C_{1,1} \cap \ldots \cap I : C_{1,p_1} \cap \{F \cup H_{\mathcal{C}_1}\} \cap \ldots \\ \cap [\mathcal{C}_q] : H_{\mathcal{C}_q}^\infty \cap I : C_{q,1} \cap \ldots \cap I : C_{q,p_q} \cap \left\{F \cup H_{\mathcal{C}_q}\right\}. \tag{2}$$

Note that $\mathcal{C}_1, \ldots, \mathcal{C}_q$ and, therefore, all ideals in (2) are uniquely determined by I, that is, they do not depend on the choice of generators of I. Moreover, the ideals

$$I : C_{i,j} \tag{3}$$

and

$$\{F \cup H_{\mathcal{C}_i}\} \tag{4}$$

strictly contain I, $1 \leqslant i \leqslant q$, $1 \leqslant j \leqslant p_i$. Indeed, all $C_{i,j}$ are elements of essential prime components of I, therefore $I : C_{i,j} \supsetneq I$. And, since $H_{\mathcal{C}_i}$ does not belong to

[1]Admitting a slight abuse of notation in this formula, we denote by $F \cup H_{\mathcal{C}}$ the union of the set F and the singleton set containing $H_{\mathcal{C}}$.

the corresponding essential prime component $[\mathcal{C}_i] : H_{\mathcal{C}_i}^\infty$, it does not belong to I, and we have $\{F \cup H_{\mathcal{C}_i}\} \supsetneq I$.

By the Ritt-Raudenbush theorem, a strictly increasing chain of radical differential ideals terminates. Therefore, by computing recursively the canonical, generator-independent prime decomposition of (3) and (4), we obtain a generator-independent decomposition of the original ideal I. We note that the prime decomposition required in step (1) can be computed for the radical ideals given in a saturated form, as in (3).

3.3. **Ranking-independent canonical decomposition and generators.** Even though the canonical prime decomposition computed by the method described in the previous section is independent of the given generators of the radical ideal I, it does depend on the choice of ranking. It is possible to obtain a ranking-independent canonical prime decomposition via the following modification. As in (1), compute any prime decomposition of I. Then, instead of extracting the characteristic sets of the highest rank w.r.t. a fixed chosen ranking (this step is ranking-dependent), take all prime components whose canonical characteristic sets have the highest rank w.r.t. *some* ranking, and consider all *these* characteristic sets instead of the above $\mathcal{C}_1, \ldots, \mathcal{C}_q$. This step can be accomplished by computing the universal characteristic set [7] for each prime component. The remaining steps are the same.

Finally, from the canonical prime decomposition

$$I = \bigcap_{i=1}^{k} [\mathcal{C}_i] : H_{\mathcal{C}_i}^\infty$$

one can obtain a canonical set of generators of the radical differential ideal, which depends only on this ideal. For $j = 0, 1, 2, \ldots$ consider the algebraic ideal

$$I_j = \bigcap_{i=1}^{k} \left(\mathcal{C}_i^{(j)}\right) : H_{\mathcal{C}_i}^\infty$$

and compute its Gröbner basis $\mathcal{B}_j$ w.r.t. the lexicographic term order induced on power products of derivatives by the ranking (if a ranking-independent canonical set of generators is sought, compute the universal Gröbner basis). Stop at the least value of j such that $\{\mathcal{B}_j\} = I$, and output $\mathcal{B}_j$. Such j exists, because $I = \bigcup_{j=0}^{\infty} I_j$. Note that the equality of two radical differential ideals given by generators can be checked by testing membership of generators of one ideal to the other ideal.

4. Acknowledgemenets

We thank Michael Singer and William Sit for their helpful suggestions and support, and Russell Miller for the introduction to the theory of computable fields and subsequent discussions of this topic in connection with the Ritt problem.

References

1. F. Boulier and F. Lemaire, *Computing canonical representatives of regular differential ideals*, ISSAC'00: Proceedings of the 2000 international symposium on Symbolic and algebraic computation (New York, NY, USA), ACM Press, 2000, pp. 38–47.
2. François Boulier, Daniel Lazard, François Ollivier, and Michel Petitot, *Representation for the radical of a finitely generated differential ideal*, ISSAC'95: Proceedings of the 1995 international symposium on Symbolic and algebraic computation (New York, NY, USA), ACM Press, 1995, pp. 158–166.

3. R.M. Cohn, *Specializations of differential kernels and the Ritt problem*, Journal of Algebra **61** (1979), no. 1, 256–268.
4. ———, *Valuations and the Ritt problem*, Journal of Algebra **101** (1986), no. 1, 1–15.
5. David Cox, John Little, and Donald O'Shea, *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*, Springer, 1996, Second edition.
6. David Eisenbud, Craig Huneke, and Volmer Vasconcelos, *Direct methods for primary decomposition*, Inventiones Mathematicae (1992), no. 110, 207–235.
7. O. Golubitsky, *Gröbner fan and universal characteristic sets of prime differential ideals*, Journal of Symbolic Computation **41** (2006), no. 10, 1091–1104.
8. O. Golubitsky, M.V. Kondratieva, and A. Ovchinnikov, *Algebraic transformation of differential characteristic decompositions from one ranking to another*, Journal of Symbolic Computation **44** (2009), doi:10.1016/j.jsc.2008.07.002, to appear.
9. E. Hubert, *Factorization-free decomposition algorithms in differential algebra*, Journal of Symbolic Computation **29** (2000), no. 4-5, 641–662.
10. ———, *Notes on triangular sets and triangulation-decomposition algorithms I: Polynomial systems.*, Symbolic and Numerical Scientific Computing 2001, 2003, pp. 1–39.
11. ———, *Notes on triangular sets and triangulation-decomposition algorithms II: Differential systems*, Symbolic and Numerical Scientific Computing 2001, 2003, pp. 40–87.
12. E.R. Kolchin, *Differential algebra and algebraic groups*, Academic Press, New York, 1973.
13. M.V. Kondratieva, A.B. Levin, A.V. Mikhalev, and E.V. Pankratiev, *Differential and difference dimension polynomials*, Kluwer Academic Publisher, 1999.
14. H. Levi, *On the structure of differential polynomials and on their theory of ideals*, Transactions of the American Mathematical Society **51** (1942), no. 3, 532–568.
15. R.G. Miller, *Computability and differential fields: a tutorial*, Proceedings of the Second International Workshop on Differential Algebra and Related Topics (L. Guo and W. Sit, eds.), 2008, (to appear).
16. ———, *Computable fields and Galois theory*, Notes of the American Mathematical Society **55** (2008), no. 7, 798–807.
17. M. O. Rabin, *Computable algebras, general theory and theory of computable fields*, Transactions of the American Mathematical Society **95** (1960), no. 2, 341–360.
18. J.F. Ritt, *Differential algebra*, American Mathematical Society, New York, 1950.
19. W.Y. Sit, *The Ritt-Kolchin theory for differential polynomials*, Differential Algebra and Related Topics, Proceedings of the International Workshop (NJSU, 2–3 November 2000), 2002, pp. 1–70.
20. Franz Winkler, *Polynomial algorithms in computer algebra*, Springer, 1996.

University of Western Ontario, Department of Computer Science, London, Ontario, Canada, N6A 5B7

E-mail address: `Oleg.Golubitsky@gmail.com`

Moscow State University, Department of Mechanics and Mathematics, Leninskie gory, Moscow, Russia, 119991

E-mail address: `kondratieva@sumail.ru`

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

E-mail address: `aiovchin@math.uic.edu`