

Probabilistic Algorithms for Computing Resolvent Representations of Regular Differential Ideals

Thomas Cluzeau
INRIA - CAFE
2004 route des Lucioles
F-06902 Sophia Antipolis
Thomas.Cluzeau@inria.fr

Evelyne Hubert
INRIA - CAFE
2004 route des Lucioles
F-06902 Sophia Antipolis
Evelyne.Hubert@inria.fr

August 16, 2006

Abstract

In a previous article [14], we proved the existence of resolvent representations for regular differential ideals. The present paper provides practical algorithms for computing such representations. We propose two different approaches. The first one uses differential characteristic decompositions whereas the second one proceeds by prolongation and algebraic elimination. Both constructions depend on the choice of a tuple over the differential base field and their success relies on the chosen tuple to be separating. The probabilistic aspect of the algorithms comes from this choice. To control it, we exhibit a family of tuples for which we can bound the probability that one of its element is separating.

Keywords: differential algebra, differential primitive element, resolvent representation, probabilistic algorithms, differential elimination, change of ranking.

1 Introduction

The primitive element theorem states that an algebraic field extension can be generated by a single element. This has been extended to represent the zero set of zero dimensional polynomial ideals by means of the roots of a single polynomial [21, 23, 3, 1, 38, 24]. Similarly, the cyclic vector construction shows that a linear differential system is equivalent to a single differential equation [4, 16, 33, 12]. The resolvent representation is a generalization of both those

constructions to nonlinear differential systems. Roughly speaking, it entails that systems of ordinary differential equations in a quite general class are birationally equivalent to single differential equations. We offer an example to clarify what this means in practice.

EXAMPLE: *Let us consider the Lotka-Volterra dynamical system*

$$\begin{cases} x' &= a x - b x y, \\ y' &= -c y + d x y. \end{cases}$$

For generic parameters a, b, c, d , this two dimensional system is birationally equivalent to the differential equation

$$(a + c) w'' - w'^2 + (a + c - w) ((c - a) w' - a c w) = 0.$$

The equivalence is given by:

$$x = \frac{w' + c w}{d(a + c)}, \quad y = \frac{a w - w'}{d(a + c)} \quad \text{and} \quad w = b y + d x.$$

Given a differential system, this paper presents practical algorithms for the computation of the equivalent single equation and the rational relationships between its solutions and the solutions of the original system.

Results about resolvent representations are best expressed in the realm of differential algebra [36, 34]. Ritt showed that every prime differential ideal admits a resolvent representation [36]. Effective algorithms in differential algebra have brought to attention a wider class of differential ideals, namely regular differential ideals [7, 8] and characterisable differential ideals [29]. In [14], we generalized the proof of existence of a resolvent representation to regular differential ideals (and thereby to characterisable ideals). The present follow up paper is devoted to effective methods for computing resolvent representations for regular differential ideals¹.

A source of motivation for studying resolvent representations is their analogy with the representation that underlies the complexity analysis of polynomial systems solving in the line of the works of [22, 24, 39, 35]. After the publication of [14], this line of complexity analysis was pursued in [17] on a kind of prime differential ideals of interest in control theory. Though we handle here more general differential ideals, our work does not cover their case of interest. Let us also mention the recent related work [18] for difference ideals, based on [15].

The algorithms we investigate are probabilistic either of Las Vegas type, when one can test the output for correctness, or of Monte Carlo type². The probabilistic aspect comes from the choice of a tuple of elements in the base field: the algorithms succeed in producing a resolvent representation when this tuple

¹As requested by a referee we splitted out the computational method proposed in the initial submission [13] to complete it with its probability analysis here.

²We follow here the terminology of [19, Section 6.5].

is *separating*, i.e., the linear combination of the differential indeterminates it defines assumes distinct values for distinct zeros of the regular differential ideal. It is known [36, 14] that there exists a *discriminating* differential polynomial: a tuple is separating when it does not annihilate that differential polynomial. It then follows that a separating tuple can be chosen in a family of tuples parameterized by constants in the base field [36, II.22]. In this paper, we bound the probability that an element of this family is separating by bounding the order and the degree of such a discriminating differential polynomial in terms of the orders and degrees of the differential polynomials in the input differential chain. This follows the lines of Seidenberg's proof of the differential primitive element theorem [41], as does [17] for the case of prime differential ideals. The bounds on the discriminating differential polynomial are deduced from bounds on a *generic resolvent*. This latter can be obtained by specializing a Chow form of a polynomial ideal obtained by *prolongation* of the input polynomials. The order of the prolongation is essentially determined by Lemma 4.1 and Proposition 4.2. The analogue prolongation order obtained in [17] is rather higher. Our better bound owes to the fact that the problem we treat essentially boils down to computations in differential dimension zero.

A resolvent representation can be obtained from a generic resolvent: this is the point of view taken in [17]. In this paper, we provide other approaches for the computation of resolvent representations. Regular differential ideals are defined by differential chains with respect to a given ranking. Computing resolvent representations can be thought of as a change of ranking problem. We propose two methods. The first one starts by computing a differential characteristic decomposition for the new ranking. In this particular case we manage to characterize the redundant components; recombining the irredundant components by a Chinese remainder technique produces a resolvent representation. The second applies Gröbner bases techniques to a *prolongation* of the input differential system. The appropriate prolongation process is defined in Lemma 4.1. We then provide a mean of testing characterisability of the differential ideal by inspecting the prolongation ideal. A resolvent representation is then deduced. We actually obtain here a method for change of ranking addressing essentially the characterisability issue for that problem. Algorithms for change of rankings for prime differential ideals are provided in [5, 9, 25]. Since prime ideals are characterisable for any ranking, they do not need to handle the characterisability problem. This is however no longer true for regular, nor even characterisable, differential ideals that we deal with here. On the other hand we address particular change of rankings that preserve the parametric set. Conceptually, this boils down to differential dimension zero by enlarging the differential coefficient field.

The paper is organized as follows. In Section 2, we point out the basic notations and definitions of [14] needed in the sequel. We recall the main result in [14], that is the existence of a resolvent representation for regular differential ideals. Section 3 is devoted to a first approach, based on differential characteristic decompositions, for computing resolvent representations. We first give

an algorithm for the prime case. We then generalize it to handle non prime regular differential ideals by taking into account the problem of redundant components: this is the foundation of an algorithm of Monte Carlo type. Using the canonical characteristic decomposition, we further improve the latter algorithm and obtain a Las Vegas procedure. Section 4 introduces a process of prolongation for a differential ideal. We prove a bound for the order up to which one needs to differentiate the input differential polynomials so that a resolvent representation can be obtained by algebraic manipulations on the obtained ideal. Using this prolongation, we propose in Section 5 a second method, based on Gröbner bases techniques, for computing resolvent representations. We address the characterisability issue and deduce a Las Vegas procedure. The two last sections deal with the probability analysis of our algorithms. In Section 6, we establish how to deduce a resolvent representation from a *generic resolvent* for a regular differential ideal. We then exhibit a *discriminating* differential polynomial and prove bounds on its order and degree. We define, in Section 7, a family of tuples parameterized by constants in the base field. A direct application of Zippel-Schwartz Lemma provides a bound for the probability that an element chosen at random in this family is separating, and consequently for the probability of success of our algorithms.

2 Resolvent representation for regular differential ideals

This paper is a direct continuation of [14]. We comply with the definitions and notations used there. We review them very briefly here together with the results that are implicitly required in this paper and give precise reference to [14].

We consider a differential field \mathcal{F} of characteristic zero, with respect to a derivation δ . We assume that \mathcal{F} contains a non constant element; this is a sufficient condition for the existence of elements in \mathcal{F} that do not annihilate a given differential polynomial [36].

Let $Y = \{y_1, \dots, y_n\}$ be a set of differential indeterminates. The set of derivatives of Y is the set of indeterminates $\Theta Y = \{\delta^k y \mid y \in Y, k \in \mathbb{N}\}$ while the set of derivatives of order r and less is noted $\Theta_r Y = \{\delta^k y_i, 1 \leq i \leq n, 0 \leq k \leq r\}$.

In this preliminary section, we split the set of indeterminates into two subsets, $U = \{u_1, \dots, u_m\}$ and $Y = \{y_1, \dots, y_n\}$. The set U represents the *parametric set*. As explained at the end of this section, this set will be considered as being empty in the sequel, with no loss of generality.

The ring of differential polynomials $\mathcal{F}\{U, Y\} = \mathcal{F}[\Theta U, \Theta Y]$ is understood to be endowed with a ranking [14, Section 2.2]. For a set A of differential polynomials, $[A]$ and $\{A\}$ denote respectively the differential ideal and the radical differential ideal generated by A .

The practical notation Δ is used to assemble differential triangular sets in [14,

Section 3.1]. A differential chain A [14, Definition 3.1 and 3.2] defines a regular differential ideal $[A] : H_A^\infty$ [14, Definition 3.2] where H_A denotes the set of initials and separants of A . When A is furthermore a differential regular chain [14, Definition 3.7] it defines a characterizable differential ideal $[A] : H_A^\infty$ [14, Definition 3.5, Theorem 3.8]. In this case A is a characteristic set for $[A] : H_A^\infty$ ensuring thus a membership test [14, Definition 3.4 and 3.5].

Regular and characterizable differential ideals have interesting structural properties that are usually lifted from their related algebraic ideal $(A) : H_A^\infty$ by Rosenfeld lemma [14, Lemma 3.3]. In particular $[A] : H_A^\infty$ is radical. Furthermore if U is the parametric set of A [14, Definition 4.1], then all the prime components of $[A] : H_A^\infty$ admit U as a maximally independent set [14, Definition 4.7, Theorem 4.11 and 3.6]. The relative order [14, Definition 4.7] of any of those prime components with respect to U is the order of A [14, Definition 4.1], [14, Theorem 4.11 and 3.6].

Regular and characterizable differential ideal are all the more interesting that any differential ideal can be written as an intersection of such ideals. When we deal with characterizable differential ideals we call such a representation a characteristic decomposition [14, Definition 3.10].

For convenience we repeat here the definition of resolvent forms, resolvent representations and separating tuples [14, Definition 5.1, 5.6 and 6.1].

DEFINITION 2.1 *We say that a regular differential chain C in $\mathcal{F}\{U, Y, w\}$ (endowed with a ranking such that $U \ll w \ll Y$) has a resolvent form in w with parametric set U if C can be written as: $C = c \Delta \alpha_1 y_1 - \kappa_1 \Delta \dots \Delta \alpha_n y_n - \kappa_n$ where $c, \alpha_1, \dots, \alpha_n, \kappa_1, \dots, \kappa_n \in \mathcal{F}\{U, w\}$ and the leader of c is a derivative of w . We call c the resolvent.*

DEFINITION 2.2 *Let J be a radical differential ideal of $\mathcal{F}\{U, Y\}$. Consider a new differential indeterminate w . We say that J admits the resolvent representation C relatively to U if there exists a differential polynomial ω in $\mathcal{F}\{U, Y, w\}$, $\omega = \alpha w - \kappa$ where $\alpha, \kappa \in \mathcal{F}\{U, Y\}$ and α is not a zero divisor modulo J , such that $\{J + [\omega]\} : \alpha^\infty$ is characterisable for a ranking such that $U \ll w \ll Y$ and its differential characteristic set C has a resolvent form in w with parametric set U .*

DEFINITION 2.3 *Let J be a radical differential ideal in $\mathcal{F}\{U, Y\}$ the essential prime components of which all admit U as a maximally independent set. Consider the extension \bar{J} of J to $\mathcal{F}\langle U \rangle\{Y\}$. A n -tuple $\mu = (\mu_1, \dots, \mu_n) \in \mathcal{F}^n$ is separating for J relative to U if for two distinct zeros $\bar{y} = (\bar{y}_1, \dots, \bar{y}_n)$ and $\tilde{y} = (\tilde{y}_1, \dots, \tilde{y}_n)$ of \bar{J} in a common differential extension of $\mathcal{F}\langle U \rangle$ we have $\mu_1 (\bar{y}_1 - \tilde{y}_1) + \dots + \mu_n (\bar{y}_n - \tilde{y}_n) \neq 0$.*

We proved the existence of a separating tuple by showing the existence of a nonzero differential polynomial g in $\mathcal{F}\{U, \Lambda\}$, where $\Lambda = \{\lambda_1, \dots, \lambda_n\}$, such that if $g(U, \mu) \neq 0$ for some n -tuple $\mu \in \mathcal{F}^n$, then μ is a separating tuple

for $[A] : H_A^\infty$ [14, Lemma 6.2]. Such a polynomial is called a *discriminating polynomial* for $[A] : H_A^\infty$. One contribution of this paper is to exhibit a different discriminating differential polynomial for which we can provide a bound for its order and degree in Λ . A similar result actually comes in [17]. The existence of a separating tuple entails the following theorem of existence of a resolvent representation for regular differential ideals [14, Theorem 6.3]:

THEOREM 2.4 *Let \mathcal{F} be a differential field of characteristic zero that contains a non constant element. Consider A a consistent differential chain in $\mathcal{F}\{U, Y\}$ with parametric set U . Then $[A] : H_A^\infty$ admits a resolvent representation with parametric set U and order the order of A .*

More precisely, if $\mu \in \mathcal{F}^n$ is a separating tuple for $[A] : H_A^\infty$ relative to U , then the differential ideal $\{[A] : H_A^\infty + [w - \mu_1 y_1 - \dots - \mu_n y_n]\}$ of $\mathcal{F}\{U, Y, w\}$ is characterisable for any ranking such that $U \ll w \ll Y$ and its characteristic set has a resolvent form in w with parametric set U .

The differential chain A can also be considered in $\mathcal{F}\langle U \rangle\{Y\}$. The radical differential ideal $[A] : H_A^\infty$ has differential dimension zero when considered in this differential polynomial ring. Since the prime components of $[A] : H_A^\infty$ have empty intersection with $\mathcal{F}\{U\}$, we can recover a resolvent representation of $[A] : H_A^\infty$ in $\mathcal{F}\{U, Y, w\}$ from a resolvent representation in $\mathcal{F}\langle U \rangle\{Y, w\}$. By possibly working over $\mathcal{F}\langle U \rangle$ instead of \mathcal{F} , we assume that the parametric sets of the differential chains considered in the whole paper are empty.

3 Method based on differential characteristic decomposition

In this section, we propose a first approach for computing resolvent representations of regular differential ideals using differential characteristic decomposition calculations. Algorithms 3.4 and 3.7 take as input a differential chain and a tuple μ . Their success relies on μ to be separating. A method to chose the tuple μ with bounded probability of being separating is given in Section 7.3.

Algorithms presented in [11, 43, 8, 29, 10, 31, 32] allow to compute a differential characteristic decomposition of $\{\Sigma\} : H^\infty$ for finite sets Σ and H of differential polynomials. The Maple library *diffalg* [6] implements [8] improved by [29]; see also [30, 31]. For arbitrary Σ and H , no algorithm is known to make the characteristic decomposition irredundant³. The method presented here relies on making the decomposition irredundant in the particular case when we compute the characteristic decomposition of a radical differential ideal that is regular for one ranking. We first explain how it works for prime differential ideals before giving the general method. Note that for prime differential ideals the algorithm [9] could appropriately be used.

³Except when Σ is to consist of a single differential polynomial [36, 34, 28].

3.1 The prime case

Assume $\{\Sigma\}:H^\infty$ is known to be a prime differential ideal. In a differential characteristic decomposition of $\{\Sigma\}:H^\infty$, there is one characterisable component $[C_0]:H_{C_0}^\infty$ the characteristic set C_0 of which is greater than all the other ones. We can assert then that $\{\Sigma\}:H^\infty = [C_0]:H_{C_0}^\infty$. This entails the following procedure for computing a resolvent representation of a prime differential ideal defined by its characteristic set A of order r .

1. Pick up a tuple $\mu = (\mu_1, \dots, \mu_n)$ in \mathcal{F}^n ;
2. Let $B = A \Delta \omega$ where $\omega = w - \mu_1 y_1 - \dots - \mu_n y_n$;
3. Compute a characteristic decomposition $\{B\}:H_B^\infty = \cap_{i=1}^s [C_i]:H_{C_i}^\infty$ according to a differential ranking such that $w \ll Y$;
4. Return the greatest regular differential chain C_0 among the C_i .

Clearly C_0 is of order r and has empty a parametric set. It furthermore satisfies the following specification: if C_0 has resolvent form in w , then the tuple μ is separating for $[A]:H_A^\infty$ and C_0 is a resolvent representation of $[A]:H_A^\infty$.

We illustrate the method with different choices of tuples for a differential system.

EXAMPLE 3.1 The Lotka-Voltera system

$$\begin{cases} x' &= ax - bxy, \\ y' &= -cy + dxy, \end{cases}$$

is represented by the prime differential ideal $P = [A]:H_A^\infty$ where $A = x' - ax + bxy \Delta y' + cy - dxy$ is a differential regular chain for an orderly ranking. Note that $P = [A]:H_A^\infty = [A] = \{A\}$.

It turns out that for the elimination ranking such that $x \ll y$, the characteristic set of P has a resolvent form. Indeed, applying the direct characteristic decomposition algorithm implemented in *diffalg* leads to the decomposition $P = [C_0]:H_{C_0}^\infty \cap [C_1]:H_{C_1}^\infty$ where

$$C_0 = xx'' - x'^2 + x(c - dx)x' - cax^2 + dax^3 \Delta bxy + x' - ax,$$

and

$$C_1 = x \Delta y' + cy.$$

C_0 is a resolvent representation for P .

A similar result is obtained by selecting a ranking such that $y \ll x$. Choosing other linear combinations of x and y we obtain resolvent representations of rather different characters. The most general case is given for instance by $\omega = w - x - y$. To avoid unreadable expressions on this paper, we specialize the

parameters a, b, c, d to $1/2, 1, 1/2, 2$. These values might not be biologically significant, but do not bring any special situation in our computations. The characteristic decomposition of $\{P, w - x - y\}$ computed by *difflg* has a single component. Its characteristic set has a resolvent form in w . It is given by

$$\begin{aligned} & 8w''^2 + 4(3w^2 + 3 - 2(w+6)w')w'' \\ & + 72w'^3 - 2(8w^2 + 9)w'^2 + w(4w-3)(w^2 + 1 - 4w'), \\ & \qquad \qquad \qquad \Delta \\ & (6w' - w - 3)\mathbf{y} + 2w'' - (4w+3)w' + w(2w+1), \\ & \qquad \qquad \qquad \Delta \\ & (6w' - w - 3)\mathbf{x} - 2w'' + (3-2w)w' - w(w-2). \end{aligned}$$

The generic solution of the Lotka-Voltera system can thus be described by the general solution of the above resolvent. Yet this latter admits an essential singular solution that is the zero⁴ of the differential polynomial $4w' - w^2 - 1$.

Other than choosing $\omega = w - x$ or $\omega = w - y$, two other special cases occur. For $\omega = w - cby + dax$, a characteristic decomposition has two components. Specializing the parameters a, b, c, d to $1/2, 1, 1/2, 2$, they are given by

$$\begin{aligned} C_0 = & 16w''^2 + 64ww'w'' + 64w^2w'^2 - 16w^2w' - w^2(1 + 16w^2), \\ & \qquad \qquad \qquad \Delta \\ & 4w\mathbf{y} + 4w'' + 8ww' - w(4w+1), \\ & \qquad \qquad \qquad \Delta \\ & 8w\mathbf{x} + 4w'' + 8ww' + w(4w-1), \end{aligned}$$

and

$$C_1 = w \Delta 2y^2 - y \Delta 2x - y.$$

C_0 is a resolvent representation for $[A]: H_A^\infty$ while C_1 (interestingly?) gives the equilibria of the dynamical system. Nonetheless the resolvent of C_0 also has an essential singular zero that is the general zero of the differential polynomial $16w' + 16w^2 + 1$.

On the other hand, for $\omega = w - by - dx$, we obtain a characteristic decomposition with a single component the characteristic set of which has a resolvent form. This resolvent representation has no singularities. It is given by

$$\begin{aligned} C_0 = & (a+c)w'' - w'^2 + (a+c-w)((c-a)w' - acw), \\ & \qquad \qquad \qquad \Delta \\ & b(a+c)\mathbf{y} + w' - wa, \\ & \qquad \qquad \qquad \Delta \\ & d(a+c)\mathbf{x} - w' - cw. \end{aligned}$$

3.2 A Monte Carlo algorithm

We now generalize the above method for computing resolvent representations of prime differential ideals to regular differential ideals. As in the prime case

⁴it can be described by $w(t) = \tan(\frac{1}{4}(t - t_0))$ where t_0 is an arbitrary constant.

we shall discard redundant components in a characteristic decomposition. We show that we actually obtain an irredundant decomposition when the chosen tuple is separating. A recombination step produces a resolvent representation. The correctness of Algorithm 3.4 below relies on the two following lemmas.

LEMMA 3.2 *Let A be a differential chain in $\mathcal{F}\{Y\}$ with order r . Let $\mu = (\mu_1, \dots, \mu_n) \in \mathcal{F}^n$ and consider $B = A \Delta \omega$ where $\omega = w - \sum_{i=1}^n \mu_i y_i$.*

The components of a characteristic decomposition of $\{B\} : H_B^\infty$ that have non empty parametric set or are of order different from r are redundant.

Let $\{B\} : H_B^\infty = \cap_{i=1}^s [C_i] : H_{C_i}^\infty$ be a characteristic decomposition with the above described components removed. If μ is separating for $[A] : H_A^\infty$, then C_1, \dots, C_s all have resolvent forms in w .

PROOF: By [14, Theorem 3.6 and 4.11], the prime components of $[B] : H_B^\infty = \{B\} : H_B^\infty$ have empty parametric set and order r . Components that do not present those features in the characteristic decomposition must be redundant. If one of those components does not have a resolvent form, it corresponds to prime components for which μ is not separating [14, Theorem 6.3]. \square

LEMMA 3.3 *Let A be a differential chain in $\mathcal{F}\{Y\}$ with order r . Let $\mu = (\mu_1, \dots, \mu_n) \in \mathcal{F}^n$ and consider $B = A \Delta \omega$ where $\omega = w - \mu_1 y_1 - \dots - \mu_n y_n$.*

Assume that μ is a separating tuple for $[A] : H_A^\infty$ and that $\{B\} : H_B^\infty = \cap_{i=1}^m [c_i \Delta C_i] : H_{c_i \Delta C_i}^\infty$ is a characteristic decomposition where each component has a resolvent form in w , order r and empty parametric set.

If $\gcd(c_j, c_k) \notin \mathcal{F}$, for some $j \neq k$, then $\{B\} : H_B^\infty = \cap_{i=1}^s [c'_i \Delta C_i] : H_{c'_i \Delta C_i}^\infty$ where $c'_k = c_k / \gcd(c_j, c_k)$ and $c'_i = c_i$ for $i \neq k$. In particular, if $c_j = c_k$, then we can remove the component $[c_k \Delta C_k] : H_{c_k \Delta C_k}^\infty$ from the characteristic decomposition of $\{B\} : H_B^\infty$.

PROOF: Without loss of generality, we may suppose that $m = 2$. Assume that $\gcd(c_1, c_2) = g \notin \mathcal{F}$ and write $c_1 = c'_1 g$ and $c_2 = c'_2 g$ for some differential polynomials $c'_1, c'_2 \in \mathcal{F}\{w\}$. By [14, Proposition 3.13]

$$\begin{aligned} \{B\} : H_B^\infty &= [c'_1 \Delta C_1] : H_{c'_1 \Delta C_1}^\infty \cap [g \Delta C_1] : H_{g \Delta C_1}^\infty \\ &\quad \cap [c'_2 \Delta C_2] : H_{c'_2 \Delta C_2}^\infty \cap [g \Delta C_2] : H_{g \Delta C_2}^\infty \end{aligned}$$

We argue that $[g \Delta C_1] : H_{g \Delta C_1}^\infty = [g \Delta C_2] : H_{g \Delta C_2}^\infty$ when μ is separating. It is sufficient to prove that $[\tilde{g} \Delta C_1] : H_{\tilde{g} \Delta C_1}^\infty = [\tilde{g} \Delta C_2] : H_{\tilde{g} \Delta C_2}^\infty$ for any irreducible factor \tilde{g} of g that has $w^{(r)}$ as leader. Assume for contradiction that $[\tilde{g} \Delta C_1] : H_{\tilde{g} \Delta C_1}^\infty \neq [\tilde{g} \Delta C_2] : H_{\tilde{g} \Delta C_2}^\infty$ and let \bar{w} be a general zero of \tilde{g} in a differential extension \mathcal{F}' of \mathcal{F} . It can be extended in a unique way to generic zeros (\bar{w}, \bar{Y}_1) and (\bar{w}, \bar{Y}_2) of $[\tilde{g} \Delta C_1] : H_{\tilde{g} \Delta C_1}^\infty$ and $[\tilde{g} \Delta C_2] : H_{\tilde{g} \Delta C_2}^\infty$ respectively.

This produces generic zeros \bar{Y}_1 and \bar{Y}_2 of $[C_1] : H_{C_1}^\infty \cap \mathcal{F}\{Y\}$ and $[C_2] : H_{C_2}^\infty \cap \mathcal{F}\{Y\}$ that satisfy $\mu_1 \bar{y}_{1,1} + \dots + \mu_n \bar{y}_{1,n} = \mu_1 \bar{y}_{2,1} + \dots + \mu_n \bar{y}_{2,n}$ where, for $i = 1, 2$,

$\bar{Y}_i = (\bar{y}_{i,1}, \dots, \bar{y}_{i,n})$. This contradicts the hypothesis that μ is a separating tuple for $[A]:H_A^\infty$. \square

Those two lemmas provide a way to obtain an irredundant characteristic decomposition $\{A \Delta \omega\}:H_{A \Delta \omega}^\infty = \cap_{i=1}^e [d_i \Delta D_i]:H_{d_i \Delta D_i}^\infty$ where the d_i are pairwise relatively prime when μ is a separating tuple for $[A]:H_A^\infty$. Then, we can apply the reconstruction process of [14, Theorem 5.2] to compute a differential chain C_0 having resolvent form in w of order r such that $\{A \Delta \omega\}:H_{A \Delta \omega}^\infty = [C_0]:H_{C_0}^\infty$. We obtain the following algorithm for computing resolvent representations of general regular differential ideals.

ALGORITHM 3.4 Resolvent Representation

Input:

- A differential chain A of $\mathcal{F}\{Y\}$ of order r ,
- A tuple $\mu = (\mu_1, \dots, \mu_n)$ in \mathcal{F}^n .

Output: A differential chain C in $\mathcal{F}\{\omega, Y\}$ of resolvent form in w or fail. When μ is separating, C is a resolvent representation of $[A]:H_A^\infty$.

1. Let $B = A \Delta \omega$ where $\omega = w - \mu_1 y_1 - \dots - \mu_n y_n$;
2. Compute a characteristic decomposition of $\{B\}:H_B^\infty$ according to a differential ranking such that $w \ll Y$;
3. Select the components having order r and empty parametric set;
4. If one of those does not have resolvent form, return fail and stop;
5. Remove common factors of the resolvents according to Lemma 3.3;
6. On the remaining resolvent forms C_1, \dots, C_m , with pairwise relatively prime resolvents, apply the recombination process of [14, Theorem 5.2] to construct C_0 having resolvent form in w of order r such that $[C]:H_C^\infty = [C_1]:H_{C_1}^\infty \cap \dots \cap [C_m]:H_{C_m}^\infty$;
7. Return C .

The correctness of the algorithm directly follows from the two previous lemmas and the discussion above.

Note that the output may have a resolvent form without being a resolvent representation for $[A]:H_A^\infty$. When μ is not separating, we may indeed incorrectly remove some components in Step 5. As a consequence, we can not ensure that the output is correct and we have a Monte Carlo algorithm.

This is illustrated in the following example. The tuple μ is separating for both prime components but not for the whole characterisable differential ideal.

EXAMPLE 3.5 Consider the differential chain $A = y' - \frac{1}{t} y \Delta (x' - y) (x' - \frac{2}{t} x + y)$ in $\mathcal{F}\{x, y\}$ endowed with an orderly ranking. The differential ideal $[A] : H_A^\infty$ is not prime. Take the tuple $\mu = (1, 0)$ and let $\omega = w - x$. A characteristic decomposition of $[A \Delta \omega] : H_{A \Delta \omega}^\infty$ is given by $[A \Delta \omega] : H_{A \Delta \omega}^\infty = [C_1] : H_{C_1}^\infty \cap [C_2] : H_{C_2}^\infty$ where

$$C_1 = w'' - \frac{1}{t} w' \Delta x - w \Delta y - w',$$

$$C_2 = w'' - \frac{1}{t} w' \Delta x - w \Delta y - 2tw + t^2 w'.$$

Lemma 3.3 induces us to remove one of the components in Step 5 of Algorithm 3.4. However C_i ($i = 1$ or 2) is not a resolvent representation for $[A] : H_A^\infty$ so that the output of the algorithm is not correct. Yet another characteristic decomposition is given by $[A \Delta \omega] : H_{A \Delta \omega}^\infty = [C] : H_C^\infty$ where $C = w'' - \frac{1}{t} w' \Delta x - w \Delta (y - w')(y - 2tw + t^2 w')$. For this decomposition we see that $\mu = (1, 0)$ is not separating.

To obtain a correct output on this example, it is necessary to test that the components we remove are indeed identical to others. We can achieve that by using canonical forms.

3.3 A Las Vegas algorithm through canonical characteristic sets

The algorithm in the previous subsection discards components on the provision that they have the same resolvent. If the input tuple is separating this can happen if and only if the two components are equal. As shown in the example above, when the tuple is not separating, two components can have the same resolvent without being equal. To obtain an algorithm that returns a resolvent representation if and only if the tuple is separating and fail otherwise we actually just need to test equality of the components that are candidate for being discarded.

Characterisable differential ideals admit a canonical characteristic set. This canonical characteristic set is actually the one returned by default in *diffalg*⁵. It is therefore easy to test equality of characterisable components.

PROPOSITION 3.6 *A characterisable differential ideal J admits a unique characteristic set C that is autoreduced and such that*

- *the initial of any element of C is free of any leaders of C*
- *an element of C admits no factor that is free of its leader*

Let L be the set of leaders of any characteristic set of J and T the set of derivatives occurring in one differential regular chain A characterising J . The canonical characteristic set C for J is obtained by clearing denominators from

⁵as of Maple 9.5

the reduced Gröbner basis of $(A) : H_A^\infty$ considered in $\mathcal{F}(T)[L]$ with respect to the lexicographical term order induced by the ranking on L .

PROOF: By [31, Theorem 5.2], $(A) : H_A^\infty$ is a characterisable ideal characterized by A . According to [30, Proposition 5.17], characterisable ideals admit a unique characteristic set as described. [30, Proposition 5.16] shows how to obtain it from the reduced Gröbner basis indicated. By [31, Theorem 5.5] restricted to the case of a single component, any characteristic set C of $(A) : H_A^\infty$ is a characteristic set of $J = [A] : H_A^\infty$. Hence the result. \square

We thus obtain canonical characteristic sets for characterisable differential ideals and a mean to compute them given any differential regular chain. As seen from this proof, canonical characteristic sets for characterisable differential ideals immediately follow from the result on algebraic characterisable ideals exhibited in [30, Definition 5.15] and named Gröbner chain. Their name indicates how they are derived. More properties of canonical characteristic sets are presented in [26].

Observe that canonicity of a characteristic set is preserved under the factorisation of one element. In our case of interest, assume that $C = q_1 q_2 \Delta c_1 \Delta \dots \Delta c_n$ is a canonical characteristic set for $[C] : H_C^\infty$ with resolvent form. Then $C_i = q_i \Delta c_1 \Delta \dots \Delta c_n$, $i = 1$ or 2 , is a canonical characteristic set for $[C_i] : H_{C_i}^\infty$ with resolvent form. This leads to the following variation of Algorithm 3.4.

ALGORITHM 3.7 Resolvent Representation

Input:

- A differential chain A of $\mathcal{F}\{Y\}$ of order r ,
- A tuple $\mu = (\mu_1, \dots, \mu_n)$ in \mathcal{F}^n .

Output: A resolvent representation of $[A] : H_A^\infty$ if μ is separating and fail otherwise.

1. Let $B = A \Delta \omega$ where $\omega = w - \mu_1 y_1 - \dots - \mu_n y_n$;
2. Compute a characteristic decomposition of $\{B\} : H_B^\infty$ according to a differential ranking such that $w \ll Y$;
3. Select the components having order r and empty parametric set;
4. If one of those does not have resolvent form, return fail and stop;
5. Compute the canonical characteristic sets for the selected components; They have resolvent form $q_1 \Delta C_1, \dots, q_k \Delta C_k$;
6. While, for some $i \neq j$, q_i and q_j have a common factor g then
 - If $C_i \neq C_j$, then return fail,
 - Else remove C_i and C_j and introduce $\frac{q_i q_j}{g} \Delta C_i$ instead;

7. On the resulting canonical resolvent forms C'_1, \dots, C'_l , with pairwise relatively prime resolvents, apply the recombination process of [14, Theorem 5.2] to construct C having resolvent form in w of order r such that $[C]:H_C^\infty = [C'_1]:H_{C'_1}^\infty \cap \dots \cap [C'_l]:H_{C'_l}^\infty$;

8. Return C .

PROOF: At Step 6, if $q_i = q'_i g$ and $q_j = q'_j g$ then $[q_i \Delta C_i]:H_{q_i \Delta C_i}^\infty \cap [q_j \Delta C_j]:H_{q_j \Delta C_j}^\infty = [q'_i \Delta C_i]:H_{q'_i \Delta C_i}^\infty \cap [g \Delta C_i]:H_{g \Delta C_i}^\infty \cap [q'_j \Delta C_j]:H_{q'_j \Delta C_j}^\infty \cap [g \Delta C_j]:H_{g \Delta C_j}^\infty$. By the argument of Lemma 3.3, if $[g \Delta C_i]:H_{g \Delta C_i}^\infty \neq [g \Delta C_j]:H_{g \Delta C_j}^\infty$, then μ is not separating. By Proposition 3.6 this happens if and only if $C_i \neq C_j$. When $C_i = C_j$ the above intersection is equal to $[q'_i q'_j g \Delta C_i]:H_{q'_i q'_j g \Delta C_i}^\infty$ by [14, Proposition 3.13]. \square

4 Prolongation

We propose here a process of prolongation for a differential chain A in $\mathcal{F}\{Y\}$. For a sufficiently big integer ρ the ρ^{th} prolongation of A shall be an algebraic chain $A_{(\rho)}$ such that

$$[A]:H_A^\infty \cap \mathcal{F}[\Theta_\rho Y] = (A_{(\rho)}):H_{A_{(\rho)}}^\infty.$$

In the sequel, we make two uses for this prolongation. On one hand the method for computing resolvent representation given in the next section relies on algebraic computations bearing on the polynomial ideal $(A_{(\rho)}):H_{A_{(\rho)}}^\infty$. On the other hand, the degree of the ideal $(A_{(\rho)}):H_{A_{(\rho)}}^\infty$ is an ingredient of the bound for the probability of success of our algorithms.

For ρ bigger or equal to the maximal order of a leader of A , we first define

$$\Theta_\rho A = \{\delta^k a \mid a \in A, 0 \leq k \leq \rho - \text{ord}(\text{lead}(a))\}.$$

Note that H_A is the set of initials and separants of $\Theta_\rho A$.

When the ranking induced on Y is orderly, it easily follows from the special case [14, Lemma 3.3] of Rosenfeld's lemma [37], [34, III.8 Lemma 5] that $[A]:H_A^\infty \cap \mathcal{F}[\Theta_\rho Y] = (\Theta_\rho A):H_A^\infty$. When such is not the case, $\Theta_\rho A$ can involve derivatives of order bigger than ρ . The prolongation $A_{(\rho)}$ we define in Lemma 4.1 below remedies this obvious obstruction to the above equality. It differs slightly in its definition from the prolongation defined in [14, §4.1] in that it requires less reductions. The main purpose of the lemma is nonetheless to produce a bound on the additional number h of derivatives of the elements of A that we use to produce the prolongation $A_{(\rho)}$ where only derivatives of order less than ρ appear. To define h we introduce the set K that corresponds to the set of differential indeterminates that appear in an element of A at an order higher

than the leader of this element. This set K is thus empty when we consider an orderly ranking and $h = 0$ then.

Assume $A = a_1 \Delta \dots \Delta a_n$. For ease of index use we shall name the differential indeterminates $Y = \{y_1, \dots, y_n\}$ so that $\delta^{o_i} y_i$ is the leader of a_i , for some non negative integer o_i .

LEMMA 4.1 *Let*

$$h = \max (\{0\} \cup \{o_k - o_i \mid 1 \leq i \leq n, k \in K\}),$$

where $K = \{k \mid \exists j \text{ s.t. } \text{ord}_{y_k} a_j > o_j\}$.

Consider $\rho \geq \max\{o_i \mid 1 \leq i \leq n\}$. For $o_i \leq \kappa \leq \rho$, we can write $\delta^{\kappa - o_i} a_i = s_i \delta^\kappa y_i + t_{i\kappa} \in \Theta_\rho A$, where s_i is the separant of a_i . There is an algorithm to compute $h_{i\kappa} \in S_A^\infty$ and $\tilde{t}_{i\kappa} \in \mathcal{F}[\Theta_\rho Y]$ such that $h_{i\kappa} t_{i\kappa} = \tilde{t}_{i\kappa} \pmod{(\Theta_{\rho+h} A)}$. Then $b_{i\kappa} = h_{i\kappa} s_i \delta^\kappa y_i + \tilde{t}_{i\kappa} \in (\Theta_{\rho+h} A) \cap \mathcal{F}[\Theta_\rho Y]$, and

$$A_{(\rho)} = \{b_{i\kappa} \mid o_i \leq \kappa \leq \rho, 1 \leq i \leq n\},$$

is a chain in $\mathcal{F}[\Theta_\rho Y]$.

PROOF: Since A is a differential chain, a_i can involve only derivatives of y_j of order o_j or less. The only derivatives $\delta^l y_k$ with $l \geq \kappa$ in $t_{i\kappa}$ satisfy $k \in K$ and $l \leq o_k + \kappa - o_i$. Take $\delta^\lambda y_j$ the highest ranking such derivative. Since $j \in K$ we have $\lambda \leq \kappa + (o_j - o_i) \leq \kappa + h$ and $\delta^{\lambda - o_j} a_j = s_j \delta^\lambda y_j + t_{j\lambda} \in (\Theta_{\kappa+h} A)$. Assume

$$s_j^e t_{i\kappa} = \tilde{t}_{i\kappa} + q \delta^{\lambda - o_j} a_j,$$

is a relation of pseudo-division by $\delta^{\lambda - o_j} a_j$, s_j being the separant of a_j . Then $\tilde{t}_{i\kappa}$ and q can only involve derivatives that appear in $t_{i\kappa}$ or $\delta^{\lambda - o_j} a_j$. Furthermore $\tilde{t}_{i\kappa}$ is free of $\delta^\lambda y_j$ and higher ranking derivatives. Just as $t_{i\kappa}$, the derivatives of order greater than λ that appear in $\delta^{\lambda - o_j} a_j$ are some $\delta^l y_k$ for which $k \in K$ and where $l \leq \kappa + (o_k - o_i) \leq \kappa + h$. Indeed we must have $l \leq o_k + \lambda - o_j$ and beside $\lambda \leq \kappa + (o_j - o_i)$. We can therefore iterate the process of pseudo-division by elements of $\Theta_{\rho+h} A$, reducing at each step the rank of the polynomial. The process terminates when we obtain a polynomial $\tilde{t}_{i\kappa}$ free of derivatives of Y of order greater than ρ . The leader of $b_{i\kappa}$ is then $\delta^\kappa y_i$. The ranking of $t_{i\kappa}$ is indeed lower than $\delta^\kappa y_i$ and this ranking does not increase in the reduction process. The leaders of its element being pairwise distinct, $A_{(\rho)}$ is a triangular set. \square

PROPOSITION 4.2 *Let ρ be greater or equal to all the orders of the leaders of a differential chain A in $\mathcal{F}\{Y\}$. Let h and $A_{(\rho)}$ be defined as in Lemma 4.1. Then:*

$$(A_{(\rho)}):H_A^\infty = (\Theta_{\rho+h} A):H_A^\infty \cap \mathcal{F}[\Theta_\rho Y] = [A]:H_A^\infty \cap \mathcal{F}[\Theta_\rho Y].$$

PROOF: We have $A \subset A_{(\rho)} \subset (\Theta_{\rho+h} A):H_A^\infty \subset [A]:H_A^\infty$ so that $(A_{(\rho)}):H_A^\infty \subset (\Theta_{\rho+h} A):H_A^\infty \cap \mathcal{F}[\Theta_\rho Y] \subset [A]:H_A^\infty \cap \mathcal{F}[\Theta_\rho Y]$.

Conversely let $p \in [A] : H_A^\infty \cap \mathcal{F}[\Theta_\rho Y]$ and consider \bar{p} the remainder of p through the algebraic reduction by $A_{(\rho)}$: there exists $h \in H_A^\infty$ such that $hp \equiv \bar{p} \pmod{(A_{(\rho)})}$. Because of the inclusions above, \bar{p} also belongs to $[A] : H_A^\infty \cap \mathcal{F}[\Theta_\rho Y]$. Since all the elements of $\Theta_\rho A \setminus A$ are linear in their leaders, \bar{p} is differentially reduced with respect to A . By [14, Lemma 3.3] it must be that \bar{p} belongs to $(A) : H_A^\infty \subset (A_{(\rho)}) : H_{A_{(\rho)}}^\infty$. Since $hp \equiv \bar{p} \pmod{(A_{(\rho)})}$, it follows that $p \in (A_{(\rho)}) : H_A^\infty$. Thus $[A] : H_A^\infty \cap \mathcal{F}[\Theta_\rho Y] \subset (A_{(\rho)}) : H_A^\infty$. \square

This entails two results. The first one is used in the next section for computing resolvent representations. The second one concerns the degree of the ideal $(A_{(\rho)}) : H_{A_{(\rho)}}^\infty$ and will be used to bound the degree of the polynomials discriminating separating tuples.

PROPOSITION 4.3 *Let ρ be greater or equal to all the orders of the leaders of a differential regular chain A in $\mathcal{F}\{Y\}$. Then the chain $A_{(\rho)}$ defined in Lemma 4.1 is a characteristic set of $(A_{(\rho)}) : H_{A_{(\rho)}}^\infty$ in $\mathcal{F}[\Theta_\rho Y]$ for the induced ranking.*

PROOF: Since A is a differential characteristic set of $[A] : H_A^\infty$, A is also an algebraic characteristic set of $(A) : H_A^\infty$ in $\mathcal{F}[Y_A]$, where Y_A is the set of derivatives of Y that appear in A [29, Lemma 6.1]. Consider q in $\mathcal{F}[\Theta_\rho Y]$ such that $q \in (A_{(\rho)}) : H_{A_{(\rho)}}^\infty$. Let \bar{q} be the reduction of q by $A_{(\rho)}$. Since the elements of $\Theta_\rho Y \setminus Y_A$ appear linearly as leaders of $A_{(\rho)}$, $\bar{q} \in \mathcal{F}[Y_A]$. As \bar{q} also belongs to $(A_{(\rho)}) : H_{A_{(\rho)}}^\infty$, by Proposition 4.2, $\bar{q} \in (A) : H_A^\infty$ while being reduced with respect to A . Thus $\bar{q} = 0$. This ensures that $A_{(\rho)}$ is a characteristic set of $(A_{(\rho)}) : H_{A_{(\rho)}}^\infty$. \square

The notion of degree of an algebraic variety in the affine case has been studied in [27]. The degree of an equidimensional variety is defined as the maximal number of points of intersection with an affine space of complementary dimension. The degree of an hypersurface is bounded by the degree of its defining polynomial. For a general affine algebraic variety the degree is defined as the sum of the degrees of its equidimensional components. Bezout's theorem, in the affine case, is given by an inequality: see [27, Theorem 1]. It entails that a variety defined by n polynomials of degree bounded by d is of degree bounded by d^n .

We shall use those results restated in terms of radical ideals in a polynomial ring. For instance [27, Lemma 2] implies that an elimination ideal has degree bounded by the degree of the ideal.

PROPOSITION 4.4 *Let A be a differential chain in $\mathcal{F}\{Y\}$ of order r . Let d be a bound on the degree of the elements of A in ΘY . Let ρ be greater or equal to all the orders of the leaders of the elements of A and let h and $A_{(\rho)}$ be defined as in Lemma 4.1. Then, the degree of $(A_{(\rho)}) : H_{A_{(\rho)}}^\infty$ is bounded by $d^{n(\rho+h+1)-r}$*

PROOF: Observe first that $\Theta_\rho A$ has $n(\rho+1) - r$ elements of degree bounded by d . Indeed differentiation does not increase the degree and therefore d bounds the degree of all the elements of $\Theta_\rho A$. By Bezout's theorem [27, Theorem 1],

the degree of $(\Theta_\rho A)$ and therefore of $(\Theta_\rho A): H_A^\infty$ is bounded by $d^{n(\rho+h+1)-r}$. The result then follows from Proposition 4.2 since the degree of a variety does not increase by projection [27, Lemma 2]. \square

5 Method based on change of rankings through prolongation

In Section 3, we described a first approach to the computation of resolvent representations for regular differential ideals. This method was based on an existing algorithm for computing characteristic decompositions of radical differential ideals. This section is devoted to another method, essentially based on algebraic computations, leading to a Las Vegas probabilistic algorithm for computing resolvent representations of regular differential ideals. After choosing a tuple and performing the appropriate prolongation, Gröbner bases computations allow to decide if the (differential) ideal is characterisable for the ranking underlying the resolvent representation. When this is the case we can retrieve the characteristic set. If it has a resolvent form, then it is the resolvent representation of the original regular differential ideal. Just as for the algorithms given in Section 3, the success of this algorithm relies on the choice of a separating tuple; probability bounds are given in Section 7.

The algorithm is based on results for change of rankings. Algorithms for performing change of rankings are very useful in practice. Several approaches have been proposed [5, 9, 25]. In [5, 25], the authors generalize methods that exist for change of term order in Gröbner bases while [9] takes advantage of one representation to compute the other. Either of those methods essentially apply to prime differential ideals, those being characterisable for any ranking. Here we consider more general, namely regular, differential ideals and we present an approach that addresses the problem of characterisability in change of rankings.

5.1 Characterizability for fixed parametric set and order

Consider a radical differential ideal J in some $\mathcal{F}\{Y\}$ such that all its essential prime components have a common order r and empty parametric set. Given a description of the prolongation ideal $J_{(r)} = J \cap \mathcal{F}[\Theta_r Y]$, we provide means to decide if J is characterisable for a given ranking on $\mathcal{F}\{Y\}$.

Let B be a differential chain of $\mathcal{F}\{Y\}$ for some ranking and note $J = [B]: H_B^\infty$. We have $J_{(r)} = (B_{(r)}): H_{B_{(r)}}^\infty$ (Proposition 4.2). The question is then whether $[B]: H_B^\infty$ is characterisable for a given ranking on $\mathcal{F}\{Y\}$.

We proceed as follows. Lemma 5.2 asserts that J is a characterisable differential ideal for the chosen differential ranking on $\mathcal{F}\{Y\}$ if and only if $J_{(r)}$ is characterisable for the ranking induced on $\Theta_r Y$. Then a differential characteristic set of J can be extracted from the characteristic set of $J_{(r)}$. Lemma 5.3 gives a

necessary and sufficient condition for $J_{(r)}$ to be characterisable with prescribed parametric set. We shall need the following technical lemma which is an easy consequence of results we have already used in [14].

LEMMA 5.1 *Let J be a radical differential ideal in $\mathcal{F}\{Y\}$ of differential dimension zero such that all its prime components have a common order r . Consider a differential ranking on $\mathcal{F}\{Y\}$. Then*

1. *An irredundant characteristic decomposition $J = \bigcap_{i=1}^s [C_i] : H_{C_i}^\infty$ satisfies that C_i has empty parametric set and order r ; therefore, $C_i \subset \mathcal{F}[\Theta_r Y]$.*

2. *If $q \in \mathcal{F}[\Theta_r Y]$ is a zero divisor modulo J , then q is a zero divisor modulo $J_{(r)} = J \cap \mathcal{F}[\Theta_r Y]$.*

PROOF: The first point comes immediately from [14, Theorem 3.6] and [14, Theorem 4.11].

If q is a zero divisor modulo J , there exists $1 \leq i \leq s$ such that q is a zero divisor modulo $[C_i] : H_{C_i}^\infty$. The second point comes then from the corollary to Rosenfeld's lemma we mentioned after [14, Lemma 3.3]. \square

LEMMA 5.2 *Let J be a radical differential ideal in $\mathcal{F}\{Y\}$ such that all its prime components have a common order r and empty parametric set.*

Consider a differential ranking on $\mathcal{F}\{Y\}$. J is characterisable for this ranking if and only if $J_{(r)} = J \cap \mathcal{F}[\Theta_r Y]$ is a characterisable ideal for the induced ranking on $\Theta_r Y$. Furthermore, if C is the minimal differential triangular set extracted from a characteristic set of $J_{(r)}$, then C is a differential characteristic set of J .

PROOF: By Proposition 4.2 and Proposition 4.3 if J is characterisable so is $J_{(r)}$.

Let \bar{C} be a characteristic set of $J_{(r)}$, i.e., a differential chain contained in $J_{(r)}$ of minimal rank, with respect to the ranking induced on $\mathcal{F}[\Theta_r Y]$.

Assume that $J = \bigcap_{i=1}^s [C_i] : H_{C_i}^\infty$ is an irredundant characteristic decomposition. Then we can write $J_{(r)} = \bigcap_{i=1}^s (C_{i(r)}) : H_{C_{i(r)}}^\infty$. Considering that the extension of $(C_{i(r)}) : H_{C_{i(r)}}^\infty$ to $\mathcal{F}[\Theta_r Y]$ has dimension r , each $(C_{i(r)}) : H_{C_{i(r)}}^\infty$, and therefore $J_{(r)}$, must contain a polynomial in $\mathcal{F}[y, \dots, y^{(r)}]$ for all $y \in Y$. This polynomial must be reduced to zero by \bar{C} . Hence for each $y \in Y$ there is at least one $0 \leq j \leq r$ such that $\delta^j y \in \mathfrak{L}(\bar{C})$.

Let C be the minimal differential triangular set extracted from \bar{C} . Obviously $C \subset J$ and for each $y \in Y$ there is a $0 \leq j \leq r$ such that $\delta^j y \in \mathfrak{L}(C)$. Let $q \in J$ and take $\bar{q} = \mathbf{d}\text{-rem}(q, C)$. Then $\bar{q} \in J \cap \mathcal{F}[\Theta_r Y] = J_{(r)}$ and is furthermore reduced with respect to $C_{(r)}$. It follows that $\bar{q} = 0$ and thus C is a differential characteristic set of J .

So far we have that $C \subset J \subset [C] : H_C^\infty$. Assume that $J_{(r)}$ is characterisable, and therefore $J_{(r)} = (\bar{C}) : H_{\bar{C}}^\infty$. It follows that $H_C \subset \mathcal{F}[\Theta_r Y]$ contains no zero

divisor modulo $J_{(r)}$. By Lemma 5.1 H_C contains no zero divisor of J and thus J is a characterisable differential ideal since we have $[C]:H_C^\infty = J:H_C^\infty = J$. \square

It thus remains to give a procedure to test if $J_{(r)}$ is characterisable for the ranking induced on $\mathcal{F}[\Theta_r, Y]$. We base this test on the necessary and sufficient conditions established in [29]. A challenge would be to give an alternative necessary and sufficient condition that would involve the computation of a single Gröbner basis, following the idea of [2, Theorem 3.3] that applies to prime ideals.

LEMMA 5.3 *Let $\mathcal{K}[V, X]$ be a polynomial ring endowed with a ranking such that $V \ll X$. Let I be an ideal in $\mathcal{K}[V, X]$ and denote I^e its extension to $\mathcal{K}(V)[X]$. Let G be a denominator free reduced Gröbner basis of I^e with respect to the lexicographic term ordering induced on X .*

I is characterisable and has parametric set V if and only if the set of leading terms of G is $\{x^{d_x} | x \in X, d_x \in \mathbb{N}^\}$ and $(G):I_G^\infty = I$, where both ideals are considered in $\mathcal{K}[V, X]$.*

PROOF: Let us assume that I is characterisable with parametric set V . By [29, Lemma 3.5 and Lemma 3.9] the denominator free reduced Gröbner basis of I^e with respect to the lexicographic term ordering induced by the ranking on X has $\{x^{d_x} | x \in X, d_x \in \mathbb{N}^*\}$ for leading terms and G is a characteristic set of I .

If the set of leading terms of G is $\{x^{d_x} | x \in X, d_x \in \mathbb{N}^*\}$, then I^e is zero dimensional and $\text{init}(g) \in \mathcal{K}[V]$ for all $g \in G$. Thus G is a regular chain in $\mathcal{K}[V, X]$ with parametric set V . \square

5.2 A Las Vegas algorithm

Consider a differential regular chain A in $\mathcal{F}\{Y\}$ that has order r . Let $\mu = (\mu_1, \dots, \mu_n)$ be a n -tuple of \mathcal{F} and $\omega = w - \mu_1 y_1 - \dots - \mu_n y_n$. The differential chain $B = A \Delta \omega$ in $\mathcal{F}\{Y, w\}$ has order r for the ranking $Y \ll w$ that extends the original ranking.

If μ is a separating tuple for $[A]:H_A^\infty$, then we showed in [14, Theorem 2.4] that $[B]:H_B^\infty$ is characterisable for any ranking such that $w \ll Y$ and any characteristic set C of $[B]:H_B^\infty$ for this ranking has a resolvent form of order r .

We just saw in Lemma 5.2 and 5.3 how to decide whether $[B]:H_B^\infty$ is characterisable for a ranking such that $w \ll Y$. Doing so we decide if the tuple we started from is separating or not. We now give our second algorithm for finding resolvent representations of regular differential ideals.

ALGORITHM 5.4 Resolvent Representation

Input:

- A differential chain A of $\mathcal{F}\{Y\}$ of order r ,
- A tuple $\mu = (\mu_1, \dots, \mu_n)$ in \mathcal{F}^n .

Output: A resolvent representation of $[A] : H_A^\infty$ if μ is separating and fail otherwise.

1. Let $B = A \Delta \omega$ where $\omega = w - \sum_{i=1}^n \mu_i y_i$; Consider $J = [B] : H_B^\infty$;
2. Let G be a reduced Gröbner basis for $J_{(r)} = (B_{(r)}) : H_{B_{(r)}}^\infty$ in $\mathcal{F}[w, \dots, w^{(r)}][\Theta_r Y]$ for the lexicographic term order induced by a ranking $w \ll Y$;
3. Make the necessary reductions in G to obtain G^e a denominator free reduced Gröbner basis of $J_{(r)}^e$, the extension of $J_{(r)}$ to $\mathcal{F}(w, \dots, w^{(r-1)})[w^{(r)}][\Theta_r Y]$;
4. If one of the following conditions does not hold
 - (a) G^e is a triangular set,
 - (b) the reduced Gröbner basis of $(G^e) : I_{G^e}^\infty$ is equal to G ,
 - (c) the leaders of G^e are $\{(w^{(r)})^d\} \cup \{(\delta^j y) \mid y \in Y, 0 \leq j \leq r\}$ for $d \in \mathbb{N}$,
 then return fail;
5. Else, return $C = G^e \cap \mathcal{F}[w, \dots, w^{(r)}, Y]$.

PROOF: By Lemma 5.3 $J_{(r)}$ is characterisable for the ranking $w \ll Y$ induced on $\mathcal{F}[w, \dots, w^{(r)}][\Theta_r Y]$ if and only if (a), (b) and (c) are satisfied.

The condition on the leaders of G^e in (c) imposes that C has a resolvent form and is the minimal differential triangular set that can be extracted from G^e . By Lemma 5.2, J is thus characterisable for the ranking $w \ll Y$ and C is a differential characteristic set for J . Thus $J = [C] : H_C^\infty$ and C is a resolvent representation of $[A] : H_A^\infty$. This implies in particular that μ is a separating tuple for $[A] : H_A^\infty$.

Conversely, if μ is separating, then $J^{(r)}$ is characterisable for any ranking $w \ll Y$ by Theorem 2.4 and all its characteristic sets for this ranking have rank $\{(w^{(r)})^d\} \cup \{(\delta^j y) \mid y \in Y, 0 \leq j \leq r\}$ for some d . \square

Note that a Gröbner basis G of $J_{(r)}$ according to the lexicographic term order induced by a ranking $w \ll Y$ is a Gröbner basis of $J_{(r)}^e$ for the lexicographic term order induced on $\{w^{(r)}\} \cup \Theta_r Y$. Thus only reductions are needed to obtain the reduced Gröbner basis G^e of $J_{(r)}^e$ from G .

We conclude with the complete treatment of an example. The differential chain presented was already used in [14] to illustrate the proof of existence of a separating tuple.

EXAMPLE 5.5 Consider $\mathbb{Q}(t)\{u, x, y\}$ as endowed with the elimination ranking $u < x < y$. The differential regular chain $A = x'^2 - u^2 x^2 \Delta y' - u y$ admits $\{u\}$ as a parametric set and has order 2 with respect to $\{u\}$. Obviously A is not an irreducible chain and therefore $[A] : H_A^\infty$ is not a prime differential ideal, but

only a characterisable differential ideal. To compute a resolvent representation of $[A]:H_A^\infty$ relative to $\{u\}$, we consider $\mathcal{F} = \mathbb{Q}(t)\langle u \rangle$.

Let us consider the tuple $\mu = (1, 1)$, $B = A \Delta w - x - y$ and $J = [B]:H_B^\infty$. We have $B_{(2)} = A \Delta 2x'x'' - 2u^2xx' - 2uu'x^2 \Delta y'' - uy' - u'y \Delta w - x - y \Delta w' - x' - y' \Delta x'w'' - u^2xx' - uu'x^2 - x'(uy' + u'y)$. We consider $J_{(2)} = (B_{(2)}):H_{B_{(2)}}^\infty$ and $J_{(2)}^e$ its extension to $\mathcal{F}(w, w')[w'', x, x', x'', y, y', y'']$.

The reduced Gröbner basis G of $J_{(2)}$ in $\mathcal{F}[w, w', w'', x, x', x'', y, y', y'']$ with respect to the lexicographic term order given by $w < w' < w'' < x < y < x' < y' < x'' < y''$ is

$$\begin{aligned} &uw'' - u^3w - u'wt, \\ &2u(w' - uw)x + (w' - uw)^2, \\ &\quad y - w + x, \\ &\quad x' - ux - w' + uw, \\ &\quad y' + ux - uw, \\ &ux'' - uu'x - u^3x - u'w' + ww', \\ &\quad y'' + u'x + u^2x - u'w - u^2w. \end{aligned}$$

This provides a Gröbner basis of $J_{(2)}^e$ with respect to the lexicographic term order $w'' < x < y < x' < y' < x'' < y''$. Only a couple of reductions are needed to recover the reduced Gröbner basis G^e of $J_{(2)}^e$:

$$\begin{aligned} &uw'' - u^3w - u'w', \\ &2ux + w' - uw, \quad 2uy + uw - w', \\ &2x' - w' + uw, \quad 2y' - uw - w', \\ &2ux'' + ww' - u'w' - u^3w + u^2w', \\ &2uy'' - ww' - u'w' - u^3w - u^2w'. \end{aligned}$$

G^e is in fact a Gröbner basis of $(G^e):I_{G^e}^\infty$ in $\mathcal{F}[w, w', w'', x, x', x'', y, y', y'']$ with respect to the lexicographic term order $w < w' < w'' < x < y < x' < y' < x'' < y''$ so that $J_{(2)} \neq (G^e):I_{G^e}^\infty$. This shows that $J_{(2)}$, and therefore J , is not characterisable for the ranking $w \ll x, y$ used. Condition (b) is not satisfied in Step 4 of Algorithm 5.4). As seen in [14, Section 7], no pair of constants actually provides a separating tuple.

We shall try again with the tuple $(1, t)$. $B = A \Delta w - x - ty$. The Gröbner basis G of $J_{(2)}$ in $\mathcal{F}[w, w', w'', x, x', x'', y, y', y'']$ with respect to the lexicographic term order given by $w < w' < w'' < x < y < x' < y' < x'' < y''$ is

$$\begin{aligned} &(2tu + 1)w''^2 - 2((tu' + 2u + 2tu^2)w' + u(u - tu')w)w'' + 4u(u + tu')w'^2 \\ &+ (4u^4t - 2u'tu^2 + 4u^3 + 2tu'^2)ww' + (2tu^3u' - 2tu^5 - 3u^4 - u'^2 + 4u^2u')w^2, \\ &\quad (2u^2 - u')x + tww'' - tu^3w - tw'u' + u'w - 2u^2w, \\ &\quad (2u^2 - u')y + u^3w - ww'' + w'u', \\ &\quad (2u^2 - u')x' - 2u^2w' - tww'u' + tu^2w'' + uw'' - u^3w - tu^4w, \\ &\quad (2u^2 - u')y' + u^4w - u^2w'' + uw'u', \\ &\quad (2u^2 - u')x'' + (u' + tu^3 + tu'u)w'' + -(tu' + 2u + tu^2)(u'w' + u^3w), \\ &\quad (2u^2 - u')y'' + w'u'u^2 + u'^2w' - w''u^3 - u'ww'' + u^5w + u'u^3w. \end{aligned}$$

This is also the reduced Gröbner basis G^e of $J_{(2)}^e$ and of $(G^e):I_{G^e}^\infty$. Therefore $J_{(2)}$ is characterisable for the ranking $w < w' < w'' < x < y < x' < y' < x'' < y''$ and G provides a characteristic set for it. It follows that J is characterisable for $w \ll x, y$. Its characteristic set is the differential triangular set extracted from G :

$$\begin{aligned} & (2tu + 1)w''^2 - 2((tu' + 2u + 2tu^2)w' + u(u - tu')w)w'' + 4u(u + tu')w'^2 \\ & + (4u^4t - 2u'tu^2 + 4u^3 + 2tu'^2)ww' + (2tu^3u' - 2tu^5 - 3u^4 - u'^2 + 4u^2u')w^2, \\ & \qquad \qquad \qquad \Delta \\ & \qquad \qquad \qquad (-2u^2 + u')y + w''u - w'u' - u^3w, \\ & \qquad \qquad \qquad \Delta \\ & \qquad \qquad \qquad (-2u^2 + u')x - wu' - w''tu + w'tu' + u^3wt + 2u^2w. \end{aligned}$$

It has a resolvent form. This is therefore a resolvent representation for $[A]:H_A^\infty$.

6 Generic resolvent

In this section, we review Seidenberg's proof of existence of a differential primitive element [41] in the context of regular differential ideals. As in [17], the *generic resolvent* involved allows to produce both a resolvent representation and a discriminating polynomial: a tuple that does not annihilate it is a separating tuple for $[A]:H_A^\infty$. The *generic resolvent* can be seen as a specialization of a Chow form of the prolongation ideal. This is used to produce a bound on the degree of the generic resolvent and thus of the discriminating polynomial.

6.1 Resolvent representation from a generic resolvent

Consider the differential chain $B = A \Delta w - \lambda_1 y_1 - \dots - \lambda_n y_n$, where $\Lambda = (\lambda_1, \dots, \lambda_n)$ and w are new differential indeterminates. This is a characteristic set of $[B]:H_B^\infty$ for the ranking $\Lambda \ll Y \ll w$. Let r be the common order of A and B . As Λ is the parametric set of B^6 , there exist differential polynomials in $[B]:H_B^\infty$ depending only on w and Λ .

DEFINITION 6.1 *A differential polynomial of minimal rank in $[B]:H_B^\infty$ that involves only w and Λ is a generic resolvent of $[A]:H_A^\infty$.*

If C is a characteristic set of $[B]:H_B^\infty$ with respect to a ranking such that $\Lambda \ll w \ll Y$, then the lowest ranking differential polynomial of C is a generic resolvent. The order of a generic resolvent of $[A]:H_A^\infty$ is lower or equal to the order r of A . Also its separant can not belong to $[B]:H_B^\infty$.

⁶Recall that A is assumed to have empty parametric set.

THEOREM 6.2 *Let A be a differential chain in $\mathcal{F}\{Y\}$ of order r . A generic resolvent q of $[A]:H_A^\infty$ is of order r in w . Furthermore the ideal $[B]:H_B^\infty$ of $\mathcal{F}\{\Lambda, w, Y\}$ where $B = A \triangle w - \lambda_1 y_1 - \dots - \lambda_n y_n$ is characterisable for a ranking such that $\Lambda \ll w \ll Y$ with characteristic set $C = q \triangle c_1 \triangle \dots \triangle c_n$, where*

$$c_i = \frac{\partial q}{\partial \lambda_i^{(r)}} + y_i \frac{\partial q}{\partial w^{(r)}} \in [B]:H_B^\infty.$$

PROOF: Let s be the order in w of the generic resolvent $q(\Lambda, w)$. We have $s \leq r$ and shall eventually prove that $s = r$. For the moment we define

$$c_i = \frac{\partial q}{\partial \lambda_i^{(s)}} + y_i \frac{\partial q}{\partial w^{(s)}}.$$

Observe that for a ranking $\Lambda \ll w \ll Y$, c_i has rank y_i .

Since $w \equiv \sum_{i=1}^n \lambda_i y_i \pmod{[B]:H_B^\infty}$ we have

$$\phi(\Lambda, Y) := q \left(\Lambda, \sum_{i=1}^n \lambda_i y_i \right) \in [B]:H_B^\infty \cap \mathcal{F}\{\Lambda, Y\} = [A]:H_A^\infty \otimes \mathcal{F}\langle \Lambda \rangle.$$

In other words, the coefficients of ϕ in Λ belong to $[A]:H_A^\infty$. Thus for all $1 \leq i \leq n$, we have:

$$\frac{\partial \phi}{\partial \lambda_i^{(s)}} = \frac{\partial q}{\partial \lambda_i^{(s)}} \left(\Lambda, \sum_{i=1}^n \lambda_i y_i \right) + y_i \frac{\partial q}{\partial w^{(s)}} \left(\Lambda, \sum_{i=1}^n \lambda_i y_i \right) \in [A]:H_A^\infty \otimes \mathcal{F}\langle \Lambda \rangle,$$

and therefore $c_i \in [B]:H_B^\infty$.

A characteristic set of $[B]:H_B^\infty$ with respect to a ranking such that $\Lambda \ll w \ll Y$ has derivatives of w and of each y_i in its set of leaders. By definition, q can be taken as the lowest rank element of a characteristic set of $[B]:H_B^\infty$ with respect to a ranking such that $\Lambda \ll w \ll Y$. Obviously, in $[B]:H_B^\infty$, we cannot find differential polynomials with leader a derivative of y_i that has lower rank than c_i . Thus C is a characteristic set of $[B]:H_B^\infty$.

When $[B]:H_B^\infty$ is a prime differential ideal, this implies that $[B]:H_B^\infty = [C]:H_C^\infty$ and $s = r$, i.e., q is of order r in w by [14, Theorem 4.11]. The theorem is then clear when $[B]:H_B^\infty$ is prime.

Otherwise, let $[B]:H_B^\infty = \bigcap_{k=1}^l [B_k]:H_{B_k}^\infty$ be an irredundant characteristic decomposition into prime differential ideals. To each B_k we associate $C_k = q_k \triangle c_{1k} \triangle \dots \triangle c_{nk}$ as above. We have $[B_k]:H_{B_k}^\infty = [C_k]:H_{C_k}^\infty$. The q_k are irreducible of order r in w . Since the c_{ik} are uniquely defined by q_k , it must be that the q_k are relatively pairwise distinct. By [14, Theorem 5.2], we can then construct a regular differential chain $C' = q' \triangle c'_1 \triangle \dots \triangle c'_n$ such that $[B]:H_B^\infty = [C']:H_{C'}^\infty$. We have $q' = \prod q_k$ and the rank of c'_i is y_i . Since q' is the lowest rank element of the characteristic set C' of $[B]:H_B^\infty$ it must be that

any generic resolvent has the same rank and is thus of order r . We can actually assume $q = q' = \prod_{k=1}^l q_k$ so that

$$[C]: H_C^\infty = [q \Delta c_1 \Delta \dots \Delta c_n]: s_q^\infty = \bigcap_{k=1}^l [q_k \Delta c_1 \Delta \dots \Delta c_n]: s_{q_k}^\infty.$$

Since $c_i = \frac{\partial q}{\partial \lambda_i^{(r)}} + \frac{\partial q}{\partial w^{(r)}} y_i$, and similarly for c_{ik} in terms of q_k , we have $c_i \equiv \left(\prod_{j \neq k} q_j \right) c_{ik} \pmod{(q_k)}$ and $s_q \equiv \left(\prod_{j \neq k} q_j \right) s_{q_k} \pmod{(q_k)}$ where $s_{q_k} = \frac{\partial q_k}{\partial w^{(r)}}$ is the separant of q_k . Therefore $[C]: H_C^\infty = \bigcap_{k=1}^l [q_k \Delta c_{1k} \Delta \dots \Delta c_{nk}]: s_{q_k}^\infty = [C']: H_{C'}^\infty$ so that $[B]: H_B^\infty = [C]: H_C^\infty$. That implies that $[B]: H_B^\infty$ is characterisable for a ranking $\Lambda \ll w \ll Y$ with characteristic set C . \square

We have the following corollary concerning generic resolvent and prolongation.

COROLLARY 6.3 *A generic resolvent can be obtained as a generator of the ideal $(B_{(r)}): I_{B_{(r)}}^\infty \cap \mathcal{F}[\Theta_r \Lambda][\Theta_r w]$.*

PROOF: By Theorem 6.2 and Lemma 5.2 a generic resolvent is a generator of the ideal $(B_{(r)}): I_{B_{(r)}}^\infty \cap \mathcal{F}[\Theta \Lambda][\Theta_r w]$. Taking $\omega = w - \lambda_1 y_1 - \dots - \lambda_n y_n$ we have

$$B_{(r)} = A_{(r)} \Delta \omega \Delta \omega' \Delta \dots \Delta \omega^{(r)}.$$

We have $\omega^{(i)} = w^{(i)} - \sum_{j=1}^n \sum_{k=0}^i \binom{i}{k} \lambda_j^{(i-k)} y_j^{(k)}$. Thus $B_{(r)}$ involves only derivatives of Λ of order r or less. \square

6.2 Discriminating polynomial

A *discriminating polynomial*, as used in [14, Lemma 6.2], is a differential polynomial $g \in \mathcal{F}\{\Lambda\}$, where $\Lambda = (\lambda_1, \dots, \lambda_n)$, such that $\mu \in \mathcal{F}^n$ is a separating tuple as soon as $g(\mu) \neq 0$. As in [17], we shall actually exhibit a differential polynomial in $\mathcal{F}\{\Lambda, w\}$ with the property that $\mu \in \mathcal{F}^n$ is a separating tuple as soon as $g(\mu, w) \neq 0$.

LEMMA 6.4 *Let q be a generic resolvent for $[A]: H_A^\infty$ and let $C = q \Delta c_1 \Delta \dots \Delta c_n$ be defined as in Theorem 6.2. Let g be the differential polynomial in the differential indeterminates Λ and w defined as the resultant of q and $\frac{\partial q}{\partial w^{(r)}}$ with respect to $w^{(r)}$. If $\mu = (\mu_1, \dots, \mu_n) \in \mathcal{F}^n$ is such that $g(\mu, w) \neq 0$, then the regular chain C_μ obtained by replacing $\lambda_1, \dots, \lambda_n$ by μ_1, \dots, μ_n in C is a resolvent representation of $[A]: H_A^\infty$.*

PROOF: If $g(\mu, w, \dots, w^{(r-1)}) \neq 0$, then μ is so that $\frac{\partial q}{\partial w^{(r)}}(\mu, w)$ is not a zero divisor modulo $q(\mu, w)$. As the separants of C_μ consist only of $\frac{\partial q}{\partial w^{(r)}}(\mu, w)$, C_μ is a differential regular chain. It furthermore has a resolvent form. We have

$$[C_\mu]: s_{q_\mu}^\infty = ([\lambda_1 - \mu_1, \dots, \lambda_n - \mu_n] + [C]: s_q^\infty) \cap \mathcal{F}\{Y, w\},$$

because $[\lambda_1 - \mu_1, \dots, \lambda_n - \mu_n] + [C] : s_q^\infty = [\lambda_1 - \mu_1, \dots, \lambda_n - \mu_n] + [C_\mu] : s_{q_\mu}^\infty = [C_\mu \Delta \lambda_1 - \mu_1 \Delta \dots \Delta \lambda_n - \mu_n] : s_{q_\mu}^\infty$ and $C_\mu \Delta \lambda_1 - \mu_1 \Delta \dots \Delta \lambda_n - \mu_n$ is a differential regular chain with respect to $w \ll Y \ll \Lambda$. Similarly

$$[B_\mu] : H_{B_\mu}^\infty = ([\lambda_1 - \mu_1, \dots, \lambda_n - \mu_n] + [B] : H_B^\infty) \cap \mathcal{F}\{Y, w\}.$$

Now, since $[C] : s_q^\infty = [B] : H_B^\infty$, we obtain $[C_\mu] : s_{q_\mu}^\infty = [B_\mu] : H_{B_\mu}^\infty$ so that C_μ is a resolvent representation for $[A] : H_A^\infty$. \square

6.3 Degree bound

We use a specialization of a Chow form (see [42, 20, 35]) of the prolongation $(A_{(r)}) : I_{A_{(r)}}^\infty$ to bound the degree of a generic resolvent and thus of the corresponding discriminating polynomial.

In $\mathcal{F}[\Theta_r Y]$, $(A_{(r)}) : I_{A_{(r)}}^\infty$ is a radical equidimensional ideal of dimension r . Let d_r be its degree. Corollary 4.4 offers a bound for d_r in terms of the degree of A .

Following [35, Section 5.5.3], a *Chow form* ζ of $(A_{(r)}) : I_{A_{(r)}}^\infty$ is a polynomial in $(r+1)((r+1)n+1)$ variables η_i and $\xi_{i,(j,k)}$ for $0 \leq i, k \leq r$, $1 \leq j \leq n$ that can be defined as a generator of the ideal

$$\left((A_{(r)}) : I_{A_{(r)}}^\infty + (\eta_i - \sum_{j,k} \xi_{i,(j,k)} y_j^{(k)} \mid i = 0, \dots, r) \right) \cap \mathcal{F}[\eta, \xi]. \quad (1)$$

Such a Chow form is a polynomial ζ of degree d_r in each set of variables $\{\eta_i\} \cup \{\xi_{i,(j,k)} \mid 1 \leq j \leq n, 0 \leq k \leq r\}$. Its total degree is thus bounded by $d_r(r+1)$. The following proposition is obtained by observing the analogy of the previous ideal with $(B_{(r)})$ where $B = A \Delta w - \lambda_1 y_1 - \dots - \lambda_n y_n$.

PROPOSITION 6.5 *There exists a generic resolvent for $[A] : H_A^\infty$ that has a total degree in $\Theta_r \Lambda$ and $\Theta_r w$ bounded by $d_r(r+1)$.*

PROOF: Let \tilde{q} be the polynomial obtained from ζ by substituting η_i by $w^{(i)}$ and $\xi_{i,(j,k)}$ by $\binom{i}{k} \lambda_j^{(i-k)}$. By comparing $B_{(r)}$ (see proof Corollary 6.3) and the definition of a Chow form (1), we see that \tilde{q} must belong to $(B_{(r)}) : I_{B_{(r)}}^\infty \cap \mathcal{F}[\Theta_r \Lambda][\Theta_r w]$. By Corollary 6.3, a generic resolvent q of $[A] : H_A^\infty$ is a generator of the ideal $(B_{(r)}) : I_{B_{(r)}}^\infty \cap \mathcal{F}[\Theta_r \Lambda][\Theta_r w]$. Thus q must divide \tilde{q} and therefore its degree is bounded by the degree of \tilde{q} which is the degree of a Chow form. \square

We obtain the following corollary to be used in the next section.

COROLLARY 6.6 *Let A be a differential chain in $\mathcal{F}\{Y\}$ of order r . Let n be the number of elements of A and let d a bound on the degree of the elements of A . Let h be defined as in Lemma 4.1. There exists a discriminating polynomial for $[A] : H_A^\infty$ of degree bounded by*

$$D(2D-1)$$

where

$$D = (r + 1) d^{n(r+h+1)-r}.$$

PROOF: From Lemma 6.4, the resultant g of a generic resolvent q and its separant $\frac{\partial q}{\partial w^{(r)}}$ with respect to the variable $w^{(r)}$ is a discriminating polynomial for $[A]: H_A^\infty$. If D is a bound on the degree of q , then $D(2D-1)$ is a bound on the degree of g . The result then follows from Proposition 6.5 and Corollary 4.4. \square

7 Probability analysis

In this section, we exhibit a family Υ of tuples $\mu = (\mu_1, \dots, \mu_n)$ for which we can bound the probability that one of its element is separating for $[A]: H_A^\infty$. We can then bound the probability of success of Algorithms 3.4, 3.7 and 5.4 by choosing for input a tuple $\mu = (\mu_1, \dots, \mu_n)$ in this family.

7.1 A family Υ of separating tuples

Consider a non zero differential polynomial in $\mathcal{F}\{\Lambda, w\}$ of order r in w and $\Lambda = (\lambda_1, \dots, \lambda_n)$ and total degree D . We look for values of Λ for which this polynomial does not vanish uniformly. Regarding it as a differential polynomial in w it is sufficient to insure that one of its coefficients, a differential polynomial p of $\mathcal{F}\{\Lambda\}$ of order r and degree D or less, does not vanish. In [36, II.22], it is shown that we can find such a specialization μ_1, \dots, μ_n of $\lambda_1, \dots, \lambda_n$ in the family Υ defined below.

DEFINITION 7.1 *Let A be a differential chain in $\mathcal{F}\{Y\}$ of order r . We note Υ the family of tuples $\mu \in \mathcal{F}^n$ defined by*

$$\mu_i = c_{i0} + c_{i1}t + \dots + c_{ir}t^r, \quad 1 \leq i \leq n,$$

where t is a non constant element of \mathcal{F} and $c_{ij} \in \mathcal{C}$, the subfield of constants of \mathcal{F} .

Substituting the above μ_i for the λ_i in p , we obtain a polynomial in t the coefficients of which are polynomials in the c_{ij} of degree bounded by D . We thus require the c_{ij} to be taken so that one of these coefficients does not vanish.

PROPOSITION 7.2 *Let A be a differential chain in $\mathcal{F}\{Y\}$ of order r . Let d be a bound on the degree of the elements of A and h defined as in Lemma 4.1. There exists a polynomial φ in $n(r+1)$ variables c_{ij} ($1 \leq i \leq n$, $0 \leq j \leq r$) of degree bounded by $D(2D-1)$ where $D = (r+1)d^{n(r+h+1)-r}$ such that a tuple $\mu \in \Upsilon$ is separating as soon as $\varphi(c_{ij}) \neq 0$.*

PROOF: The result follows from Corollary 6.6 and the discussion above. \square

7.2 Density of separating tuples in Υ

Now that we have reduced the problem of choosing a separating tuple to the non vanishing of a polynomial of bounded degree we can appeal to Zippel-Schwartz lemma to conclude. The lemma can be found in [44, 40] or [39, Théorème 2 and Corollaire 3, p. 35-36]. We recall it here for convenience.

LEMMA 7.3 *Let k be a field and f be a polynomial in $k[x_1, \dots, x_n]$ of total degree bounded by d . Let Ω be a (finite) subset of k . Then the total number of zeros of f in Ω^n is bounded by $d|\Omega|^{n-1}$. Consequently, the probability for a point uniformly chosen in Ω^n to be a zero of f does not exceed $\frac{d}{|\Omega|}$.*

From this, we have

PROPOSITION 7.4 *Let A be a differential chain in $\mathcal{F}\{Y\}$ of order r . Let d be a bound on the degree of the elements of A and h be defined as in Lemma 4.1. Let Ω be a finite subset of \mathcal{C} , the subfield of constants of \mathcal{F} . Consider $\mu = (\mu_1, \dots, \mu_n) \in \Upsilon$ whose coefficients c_{ij} are chosen uniformly in Ω . The probability for μ to be a separating tuple for $[A]:H_A^\infty$ is at least*

$$1 - \frac{D(2D-1)}{|\Omega|},$$

where

$$D = (r+1)d^{n(r+h+1)-r}.$$

PROOF: The result follows directly from Proposition 7.2 and Lemma 7.3. \square

We obtain the following algorithm for constructing tuples for which we can bound the probability that it is separating.

ALGORITHM 7.5 **Separating Tuple**

Input:

- A differential chain $A \in \mathcal{F}\{Y\}$ of order r ,
- A finite subset Ω of the constant field \mathcal{C} of \mathcal{F} .

Output: A tuple that is separating with probability at least

$$1 - \frac{(r+1)d^{n(r+h+1)-r}(2(r+1)d^{n(r+h+1)-r} - 1)}{|\Omega|}$$

where d is a bound on the degree of the elements of A and h is defined in Lemma 4.1.

1. Let c_{ij} ($1 \leq i \leq n$ and $0 \leq j \leq r$) be chosen uniformly at random in Ω ;
2. Return $\mu = (\mu_1, \dots, \mu_n) \in \Upsilon \subset \mathcal{F}^n$ where

$$\mu_i = c_{i0} + c_{i1}t + \dots + c_{ir}t^r.$$

7.3 Algorithms with bounded probability of success

We have now all the tools to bound the probability for Algorithms 3.4, 3.7, or 5.4 to succeed in computing a resolvent representation provided that the input tuple is produced by Algorithm 7.5. We summarize this by the following final algorithm.

ALGORITHM 7.6 Probabilistic Resolvent Representation

Input:

- A differential chain $A \in \mathcal{F}\{Y\}$ of order r ,
- A finite subset Ω of the constant field \mathcal{C} of \mathcal{F} .

Output: A resolvent representation for $[A]:H_A^\infty$ with probability at least

$$1 - \frac{(r+1)d^{n(r+h+1)-r}(2(r+1)d^{n(r+h+1)-r} - 1)}{|\Omega|},$$

where d is a bound on the degree of the elements of A and h is defined in Lemma 4.1

1. Apply *Separating Tuple* to (A, Ω) to get a tuple μ ;
2. Apply *Resolvent Representation* to (A, μ) .

Step 2 of the above algorithm can call on Algorithm 3.4, 3.7 or 5.4 with the following distinction. Algorithm 3.4 is of Monte Carlo type and we can not test the output for correctness: the algorithm can output a differential chain of resolvent form that is not a resolvent representation of $[A]:H_A^\infty$ (see also Example 3.5). On the other hand Algorithm 3.7 or 5.4 are of Las Vegas type. The output is a resolvent representation of $[A]:H_A^\infty$ as soon as it is not fail. Consequently, running the algorithm sufficiently many times surely leads to a resolvent representation of $[A]:H_A^\infty$. The error probability is then zero: only the running time is a random variable.

References

- [1] M-E. Alonso, E. Becker, M-F. Roy, and T. Wörmann. Zeros, multiplicities, and idempotents for zero-dimensional systems. In *Algorithms in Algebraic Geometry and Applications (Santander, 1994)*, pages 1–15. Birkhäuser, Basel, 1996.
- [2] P. Aubry, D. Lazard, and M. Moreno-Maza. On the theories of triangular sets. *Journal of Symbolic Computation*, 28(1-2):105–124, 1999.
- [3] E. Becker, M. Marinari, T. Mora, and C. Traverso. The shape of the shape lemma. In *ISSAC'94*, pages 129–133. ACM Press, 1994.

- [4] G.D. Birkhoff. Formal theory of irregular linear difference equations. *Acta Mathematica*, 54:205–246, 1930.
- [5] F. Boulier. Efficient computation of regular differential systems by change of rankings using Kähler differentials. Technical Report LIFL 1999-14, LIFL, Université de Lille, 1999.
- [6] F. Boulier and E. Hubert. DIFFALG, a MAPLE package. *Description, help pages and examples of use*. Symbolic Computation Group, University of Waterloo, Ontario, Canada, 1998. Now accessible on <http://www-sop.inria.fr/cafe/Evelyne.Hubert/webdiffalg>.
- [7] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Representation for the radical of a finitely generated differential ideal. In A.H.M. Levelt, editor, *ISSAC'95*, pages 158–166. ACM Press, New York, 1995.
- [8] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Computing representations for radicals of finitely generated differential ideals. Technical Report IT-306, LIFL, 1997. Revised version available at <http://www.lifl.fr/~boulier>.
- [9] François Boulier, François Lemaire, and Marc Moreno Maza. Pardi! In *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation*, pages 38–47 (electronic), New York, 2001. ACM.
- [10] D. Bouziane, A. Kandri Rody, and H. Maârouf. Unmixed-dimensional decomposition of a finitely generated perfect differential ideal. *Journal of Symbolic Computation*, 31(6):631–649, 2001.
- [11] S-C. Chou and X-S. Gao. Automated reasoning in differential geometry and mechanics using the characteristic set method. Part I. An improved version of Ritt-Wu's decomposition algorithm. *Journal of Automated Reasoning*, 10:161–172, 1993.
- [12] R.C. Churchill and J.J. Kovacic. Cyclic vectors. In L. Guo, W.F. Keigher, P.J. Cassidy, and W.Y. Sit, editors, *Differential Algebra and Related Topics*. World Scientific, 2000. Proceedings of the international workshop at Rutgers University at Newark, USA 2-3 November 2000.
- [13] T. Cluzeau and E. Hubert. Resolvent representation for regular differential ideals. Technical Report RR-4200, INRIA Sophia Antipolis, <http://www.inria.fr/rrrt/rr-4200.html>, 2001.
- [14] T. Cluzeau and E. Hubert. Resolvent representation for regular differential ideals. *Applicable Algebra in Engineering, Communication and Computing*, 13(5):395–425, 2003.
- [15] R. Cohn. *Difference algebra*. New York-London-Sydney: Interscience Publishers, a division of John Wiley and Sons. XIV, 1965.

- [16] F. T. Cope. Formal solution of irregular linear differential equations. Part II. *American Journal of Mathematics*, 58:130–146, 1956.
- [17] L. D’Alfonso, G. Jeronimo, and P. Solernó. On the complexity of the resolvent representation of some prime differential ideals. *Journal of Complexity*, 22(3):396–430, 2006.
- [18] X.S. Gao and C.-M. Yuan. Resolvent systems of difference polynomial ideals. In *ISSAC’06*, pages 101 – 108. ACM, 2006.
- [19] von zur J. Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, New York, 1999.
- [20] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Mathematics: Theory & Applications. Birkhäuser Boston Inc., Boston, MA, 1994.
- [21] P. Gianni and T. Mora. Algebraic solution of systems of polynomial equations using Gröbner bases. In *Applied Algebra Algorithms and Error Correcting Codes, AAEC-5*, volume 356 of *Lecture Notes in Computer Science*, pages 247–257. Springer, 1989.
- [22] M. Giusti and J. Heintz. Algorithmes—disons rapides—pour la décomposition d’une variété algébrique en composantes irréductibles et équidimensionnelles. In *Effective methods in algebraic geometry (Castiglione, 1990)*, pages 169–194. Birkhäuser Boston, Boston, MA, 1991.
- [23] M. Giusti and J. Heintz. La détermination des points isolés et de la dimension d’une variété algébrique peut se faire en temps polynomial. In *Computational Algebraic Geometry and Commutative Algebra (Cortona, 1991)*, pages 216–256. Cambridge University Press, Cambridge, 1993.
- [24] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *Journal of Complexity*, 17(1):154–211, 2001.
- [25] O. Golubitsky. Gröbner walk for characteristic sets of prime differential ideals. In V. Ganzha, E. Mayr, and E. Vorozhotsov, editors, *Proceedings 7th workshop on Computer Algebra in Scientific Computing*, 2004.
- [26] O. Golubitsky, M. Kondratieva, and A. Ovchinnikov. Canonical characteristic sets of characterizable differential ideals. <http://www4.ncsu.edu/~aiovchin/papers.html>.
- [27] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoretical Computer Science*, 24(3):239–277, 1983.
- [28] E. Hubert. Essential components of an algebraic differential equation. *Journal of Symbolic Computation*, 28(4-5):657–680, 1999.
- [29] E. Hubert. Factorisation free decomposition algorithms in differential algebra. *Journal of Symbolic Computation*, 29(4-5):641–662, 2000.

- [30] E. Hubert. Notes on triangular sets and triangulation-decomposition algorithms I: Polynomial systems. In F. Winkler and U. Langer, editors, *Symbolic and Numerical Scientific Computing*, number 2630 in Lecture Notes in Computer Science, pages 1–39. Springer Verlag Heidelberg, 2003.
- [31] E. Hubert. Notes on triangular sets and triangulation-decomposition algorithms II: Differential systems. In F. Winkler and U. Langer, editors, *Symbolic and Numerical Scientific Computing*, number 2630 in Lecture Notes in Computer Science, pages 40–87. Springer Verlag Heidelberg, 2003.
- [32] E. Hubert. Improvements to a triangulation-decomposition algorithm for ordinary differential systems in higher degree cases. In *ISSAC 2004*. ACM press, 2004. 191-198.
- [33] N.M. Katz. A simple algorithm for cyclic vectors. *Amer. J. Math.*, 109(1):65–70, 1987.
- [34] E. R. Kolchin. *Differential Algebra and Algebraic Groups*, volume 54 of *Pure and Applied Mathematics*. Academic Press, New York-London, 1973.
- [35] Teresa Krick. Straight-line programs in polynomial equation solving. In *Foundations of computational mathematics: Minneapolis, 2002*, volume 312 of *London Math. Soc. Lecture Note Ser.*, pages 96–136. Cambridge Univ. Press, Cambridge, 2004.
- [36] J. F. Ritt. *Differential Algebra*, volume XXXIII of *Colloquium publications*. American Mathematical Society, 1950. Reprinted by Dover Publications, Inc (1966).
- [37] A. Rosenfeld. Specializations in differential algebra. *Transaction of the American Mathematical Society*, 90:394–407, 1959.
- [38] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Applicable Algebra in Engineering, Communication and Computing*, 9(5):433–461, 1999.
- [39] E. Schost. *Sur la résolution des systèmes polynomiaux à paramètres*. PhD thesis, École polytechnique, 2000.
- [40] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701 – 717, 1980.
- [41] A. Seidenberg. Some basic theorems in differential algebra (characteristic p , arbitrary). *Transaction of the American Mathematical Society*, 73:174–190, 1952.
- [42] I. R. Shafarevich. *Basic algebraic geometry*. Springer-Verlag, New York, 1974. Translated from the Russian by K. A. Hirsch, Die Grundlehren der mathematischen Wissenschaften, Band 213.

- [43] D. Wang. An elimination method for differential polynomial systems. I. *Systems Science and Mathematical Sciences*, 9(3):216–228, 1996.
- [44] R. Zippel. Probabilistic algorithms for sparse polynomials. In *EUROSAM*, number 72 in Lecture Notes in Computer Sciences. Springer, 1979.