Efficient computation of regular differential systems by change of rankings using Kähler differentials

François Boulier

Publication LIFL 1999–14

Efficient computation of regular differential systems by change of rankings using Kähler differentials

François Boulier
Université des Sciences et Technologies de Lille
Laboratoire d'Informatique Fondamentale de Lille
59655 Villeneuve d'Ascq CEDEX
email: boulier@lifl.fr

6 décembre 1999 (révisé en mars 2000)

LABORATOIRE D'INFORMATIQUE FONDAMENTALE DE LILLE
UPRES–A 8022
UNIVERSITÉ DES SCIENCES ET TECHNOLOGIES DE LILLE
U.F.R. I.E.E.A. Bât. M3 – 59655 VILLENEUVE D'ASCQ CEDEX
Tél. (+33) 3 20 43 47 24 – Télécopie (+33) 3 20 43 65 66 – E-mail direction@lifl.fr

Abstract

We present two algorithms to compute a regular differential system for some ranking, given an equivalent regular differential system for another ranking. Both make use of Kähler differentials. One of them is a lifting for differential algebra of the FGLM algorithm and relies on normal forms computations of differential polynomials and of Kähler differentials modulo differential relations. Both are implemented in MAPLE V. A straightforward adaptation of FGLM for systems of linear PDE is presented too. Examples are treated.

Keywords

differential algebra, Kähler differentials, FGLM.

Introduction

Regular[1] differential systems permit to represent the radicals of differential polynomial ideals as Gröbner bases or triangular sets permit to represent usual polynomial ideals. As for Gröbner bases, regular differential systems depend on admissible orderings, called rankings. The Rosenfeld–Gröbner algorithm [4, 5] which computes regular differential systems given any finite system of polynomial ODE or PDE and any ranking $\mathcal{R}$ is implemented in the `diffalg` package of the MAPLE VR5 standard library.

In this paper, we are concerned by the problem: given a differential system $A = 0,\ S \neq 0$ regular w.r.t. some ranking $\mathcal{R}$, defining some regular differential ideal $\mathfrak{r}$ and given some ranking $\tilde{\mathcal{R}} \neq \mathcal{R}$, compute a differential system $\tilde{A} = 0,\ \tilde{S} \neq 0$ regular w.r.t. $\tilde{\mathcal{R}}$ and equivalent to $A = 0,\ S \neq 0$ i.e. defining the same regular differential ideal $\mathfrak{r}$.

A straightforward solution consists of course of running the Rosenfeld–Gröbner algorithm over $A = 0,\ S \neq 0$ for the new ranking $\tilde{\mathcal{R}}$ but this is not efficient. The algorithms described in this paper use the fact that a representation of $\mathfrak{r}$ by a regular differential system is already available in order to compute $\tilde{A} = 0,\ \tilde{S} \neq 0$.

The paper is motivated by the following fact. Let Σ be a differential system that we want to study by representing it by regular differential ideals. The rankings which provide the most interesting informations (most of the time, elimination rankings) usually make the computation utterly memory and time expensive while there usually exists rankings which require nearly no computation (most of the time, orderly rankings).

The situation is indeed very similar to that of Gröbner bases (but perhaps still more striking): the Buchberger's algorithm is often very efficient for total degree orderings and often very inefficient for elimination orderings. In the particular case of a zero dimensional ideal $\mathfrak{a}$ of a polynomial ring $R = K[X]$, the algorithm FGLM [11] solves the problem we consider: computing a Gröbner of $\mathfrak{a}$ for an admissible ordering, knowing a Gröbner basis of $\mathfrak{a}$ for some different ordering. FGLM relies on the following principles.

[1] We precise some of the terms used in this introduction in the next section.

1. A polynomial $\lambda_1 t_1 + \cdots + \lambda_s t_s$ (where the λ's are coefficients in K and the t's are terms over X) lies in $\mathfrak{a}$ if and only if the terms $t_1, \ldots, t_s$ are linearly dependent over K in the factor ring $R/\mathfrak{a}$.

2. Detecting a linear dependency between $t_1, \ldots, t_s$ in $R/\mathfrak{a}$ amounts to detect a linear dependency between the normal forms of $t_1, \ldots, t_s$, assimilating these latter to vectors of elements of K.

3. The known Gröbner basis permits to compute normal forms.

The FGLM algorithm then enumerates the terms $t_1, \ldots, t_s$ by increasing order w.r.t. the new ordering. The relations found are the polynomials of the new Gröbner basis. The hypothesis $\dim \mathfrak{a} = 0$ implies there are only finitely many irreducible terms w.r.t. any Gröbner basis of $\mathfrak{a}$ and ensures the termination of FGLM.

The algorithms we present for differential algebra are not as efficient as FGLM (apart perhaps the algorithm for systems of linear PDE which is a special case and very close to FGLM) but solve anyway the problem under consideration. They proceed in three steps:

1. first compute only the set of leaders $v_1, \ldots, v_t$ of $\tilde{A}$. More precisely, one computes t sets of derivatives $W_1, \ldots, W_t$ such that v_i is the greatest derivative of W_i (for each i) w.r.t. the new ranking $\tilde{\mathcal{R}}$ and such that $\mathfrak{r} \cap K[W_i] \neq (0)$. See sections 4 and 5 ;

2. knowing W_i, compute a nonzero polynomial $f_i \in \mathfrak{r} \cap K[W_i]$ for each i (section 6) ;

3. use $f_1, \ldots, f_t$ in order to speed up the computation of $\tilde{A} = 0,\ \tilde{S} \neq 0$ using Rosenfeld–Gröbner.

The second step, determining f_i knowing W_i, is performed by applying exactly the same principles as FGLM. To carry it out, we had to define a normal form of a differential polynomial modulo a regular differential ideal $\mathfrak{r}$ (algorithm NF). The known regular differential system permits to compute normal forms.

The first step relies on the computation of Kähler differentials [14, 13] which "linearize the problem". To perform it, we give two algorithms (we assume for a while that $\mathfrak{r}$ is a prime ideal of a differential polynomial ring R and denote G the differential field of fractions of $R/\mathfrak{r}$).

The first algorithm (called Kähler) readily applies a key theorem (theorem 5) on Kähler differentials, using a coding trick, and calling Rosenfeld–Gröbner.

The second one (algorithm dfglm) can be viewed as a lifting of FGLM for regular differential systems but it only applies for differential systems the solutions of which depend on finitely many arbitrary constants. It is however more efficient than Kähler. It applies the following principles:

1. there exists a nonzero differential polynomial in $\mathfrak{r} \cap K[w_1, \ldots, w_s]$ (where $w_1, \ldots, w_s$ are derivatives) if and only if the Kähler differentials of $w_1, \ldots, w_s$ are linearly dependent over G in $\Omega_{G/K}$ (theorem 4) ;

2. detecting a linear dependency over G between these differentials amounts to detect a linear dependency between their normal forms, assimilating these latter to vectors of elements of G (theorem 8) ;

3. the known regular differential system $A = 0,\ S \neq 0$ permits to compute normal forms of Kähler differentials in $\Omega_{G/K}$ (algorithm DNF).

The dfglm algorithm then enumerates all the derivatives of the differential indeterminates by increasing order w.r.t. the new ranking. The hypothesis that the solutions of $\mathfrak{r}$ only depend on finitely many arbitrary constants plays the same role as the zero dimension hypothesis in FGLM and ensures the termination of dfglm.

In general the differential ideal $\mathfrak{r}$ is not prime but its total ring of fractions is isomorphic to a direct product of differential fields which all admit a same transcendence basis over K (proposition 1) and we explain how to handle the general case.

A pedagogic example is completely discussed. Applying our methods over Euler's equations for a perfect fluid, we prove the pressure satisfies an autonomous fifth order PDE (section 7). Fact which does not seem to be known.

A secondary result of the paper is the algorithm fglm_for_linear_PDE which only applies for systems of linear PDE (section 8). It is given a linear differential system $A = 0$ (there are no inequations when the system is linear) regular w.r.t. a ranking $\mathcal{R}$ the solutions of which depend on finitely many arbitrary constants and a new ranking $\tilde{\mathcal{R}} \neq \mathcal{R}$. It does compute the desired differential system $\tilde{A} = 0$ regular w.r.t. $\tilde{\mathcal{R}}$ (not only its set of leaders). It is very close to the original FGLM. It may be useful for solving a system of linear PDE A by seeking ODE in the differential ideal $[A]$ and running a linear ODE solver e.g. [7]. This idea was already developed by [20] with a different method. We apply our algorithm over a famous example of E. Cartan.

We do not address complexity issues.

1 Differential algebra

We only provide a short presentation. The reference books are [21] and [15]. We also refer to the MAPLE VR5 `diffalg` package and thus to the articles [4, 5] which present it. An example is provided in section 1.1.

A *derivation* over a ring R is a map $\delta : R \to R$ which satisfies, for every $a, b \in R$

$$\begin{aligned} \delta(a+b) &= \delta a + \delta b, \\ \delta(a\,b) &= (\delta a) b + a (\delta b). \end{aligned}$$

A *differential ring* is a ring endowed with finitely many derivations which commute pairwise. The commutative monoid generated by the derivations is denoted Θ. Its elements are the *derivation operators* $\theta = \delta_1^{a_1} \cdots \delta_m^{a_m}$ where the a_i are nonnegative integer numbers. The sum of the exponents a_i, called the *order* of the operator θ, is denoted $\operatorname{ord}\theta$. The identity operator is the unique operator with order 0. The other ones are called *proper*. If $\phi = \delta_1^{b_1} \cdots \delta_m^{b_m}$ then $\theta\phi = \delta_1^{a_1+b_1} \cdots \delta_m^{a_m+b_m}$. If $a_i > b_i$ for each $1 \leq i \leq m$ then $\theta/\phi = \delta_1^{a_1-b_1} \cdots \delta_m^{a_m-b_m}$.

A *differential ideal* $\mathfrak{a}$ of R is an ideal of R stable under derivation i.e. such that

$$a \in \mathfrak{a} \Rightarrow \delta a \in \mathfrak{a}.$$

Let A be a nonempty subset of R. We denote (A) the ideal generated by A. We denote $[A]$ and $\sqrt{[A]}$ the differential ideal and the radical of the differential ideal generated by A which are respectively the smallest differential ideal and the smallest radical differential ideal which contain A. If $\mathfrak{a}$ is an ideal of R and $S = \{s_1, \ldots, s_t\}$, we denote $\mathfrak{a} : S^\infty$ the *saturation* of $\mathfrak{a}$ by S which is the ideal

$$\mathfrak{a} : S^\infty = \{p \in R \mid \exists a_1, \ldots, a_t \in \mathbb{N}, \text{ such that } s_1^{a_1} \cdots s_t^{a_t}\, p \in \mathfrak{a}\}.$$

Let $U = \{u_1, \ldots, u_n\}$ be a set of *differential indeterminates*. Derivation operators apply over differential indeterminates giving *derivatives* θu. We denote ΘU the set of all the derivatives. Let K be a differential field. The differential ring of the differential polynomials built over the alphabet ΘU with coefficients in K is denoted $R = K\{U\}$.

A *ranking* is a total ordering over the set of the derivatives [15, page 75] satisfying the following axioms

1. $\delta v > v$ for each derivative v and derivation δ,
2. $v > w \Rightarrow \delta v > \delta w$ for all derivatives v, w and each derivation δ.

One distinguishes *orderly* rankings, which satisfy:

$$\operatorname{ord}\theta > \operatorname{ord}\phi \Rightarrow \theta u > \phi v \quad \text{for all } u, v \in U$$

from *elimination* rankings which satisfy:

$$u > v \Rightarrow \theta u > \phi v \quad \text{for all } u, v \in U \text{ and } \theta, \phi \in \Theta.$$

Fix a ranking. The greatest indeterminate v occuring in a differential polynomial p is called the *leader* of p. The leading coefficient of p w.r.t. v is called the *initial* of p. The differential polynomial $\partial p/\partial v$ is called the *separant* of p. Assume $p \notin K$. Let v be the leader of p and $d = \deg(p, v)$. A differential polynomial q is said to be *partially reduced* w.r.t. a differential polynomial $p \notin K$ if no proper derivative of v occurs in q. It is said to be *reduced* w.r.t. p if it is partially reduced w.r.t. p and $\deg(q, v) < d$.

A set A of differential polynomials is said to be *differentially triangular* if it is triangular and if its elements are pairwise partially reduced. It is said to be *autoreduced* if its elements are pairwise *reduced*.

If A is a set of differential polynomials and v is a derivative then $A_v = \{\theta p \mid \operatorname{ld}\theta p \leq v\}$. Thus R_v denotes the set of all the differential polynomials having leader less than or equal to v.

A pair $\{p_1, p_2\}$ of differential polynomials is said to be a *critical pair* if the leaders of p_1 and p_2 are derivatives of some same differential indeterminate u (say $\operatorname{ld} p_1 = \theta_1 u$ and $\operatorname{ld} p_2 =$

$\theta_2 u$). If A is a set of differential polynomials then pairs(A) denotes all the pairs that can be formed with any two elements of A. Let $\{p_1, p_2\}$ be a critical pair. Denote θ_{12} the least common multiple between θ_1 and θ_2 and assume $\theta_{12} \neq \theta_1$ and $\theta_{12} \neq \theta_2$. The Δ–polynomial $\Delta(p_1, p_2)$ is

$$\Delta(p_1, p_2) = s_2 \, \frac{\theta_{12}}{\theta_1} \, p_1 - s_1 \, \frac{\theta_{12}}{\theta_2} \, p_2$$

where s_1, s_2 denote the separants of p_1 and p_2. Let $A = 0,\ S \neq 0$ be a system of differential polynomial equations and inequations. The critical pair $\{p_1, p_2\}$ is said to be *solved* by $A = 0,\ S \neq 0$ if there exists a derivative $v < \theta_{12} u$ such that

$$\Delta(p_1, p_2) \in (A_v) : (S \cap R_v)^\infty.$$

Definition 1 *(regular differential systems)*

A differential system $A = 0,\ S \neq 0$ of a differential polynomial ring R is said to be a regular differential system *(for a ranking $\mathcal{R}$) if*

C1 *A is differentially triangular,*

C2 *S contains the separants of the elements of A and is partially reduced w.r.t. A,*

C3 *all the pairs $\{p,\ p'\} \in \mathrm{pairs}(A)$ are solved by $A = 0,\ S \neq 0$ (coherence property).*

If $A = 0,\ S \neq 0$ is a regular differential system then the ideal $[A] : S^\infty$ (resp. $(A) : S^\infty$) is called the *regular differential ideal* (resp. *regular algebraic ideal*) defined by the system.

The Rosenfeld–Gröbner algorithm [3, 4, 5] is implemented in the MAPLE VR5 `diffalg` package. Given any finite family Σ of differential polynomials and any ranking, it represents the radical of the differential ideal $[\Sigma]$ generated by Σ as an intersection of regular differential ideals presented by regular differential systems.

$$\sqrt{[\Sigma]} = [A_1] : S_1^\infty \cap \cdots \cap [A_t] : S_t^\infty.$$

If $A = 0,\ S \neq 0$ is a regular differential system, we call *derivatives under the stairs of A* the elements of ΘU which are not derivatives of any leader of element of A. See section 1.1 for an explanation of this terminology. Denote N this set and L the set of the leaders of the elements of A. Then $K[L, N]$ is the ring of the differential polynomials partially reduced w.r.t. A.

Regular systems enjoy the following properties. See [5].

Theorem 1 *Let $A = 0,\ S \neq 0$ be a regular differential system of $R = K\{U\}$. Let L denote the set of leaders of A and N the set of the derivatives under the stairs of A. Then*

- *the regular algebraic ideal $(A) : S^\infty$ is radical (Lazard's lemma) ;*
- *if $\mathfrak{b}$ denotes a prime ideal minimal over $(A) : S^\infty$ then the set N furnishes a transcendence basis of the field of fractions of $R/\mathfrak{b}$ over K (Lazard's lemma) ;*
- *we have $[A] : S^\infty \cap K[L, N] = (A) : S^\infty$ (Rosenfeld's lemma) ;*

- *the regular differential ideal $[A] : S^\infty$ is radical (lifting of Lazard's lemma) ;*
- *there is a bijection between the prime differential ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ which are minimal over $[A] : S^\infty$ and the prime ideals $\mathfrak{b}_1, \ldots, \mathfrak{b}_t$ which are minimal over $(A) : S^\infty$ given by $\mathfrak{p}_i \cap K[L, N] = \mathfrak{b}_i$ (lifting of Lazard's lemma) ;*
- *the system $A = 0,\ S \neq 0$ admits a purely algebraic solution, viewed as a polynomial system of $K[L, N]$, if and only if it admits a differential solution ;*
- *every purely algebraic solution of the system $A = 0,\ S \neq 0$, viewed as a polynomial system of $K[L, N]$, can be extended in a unique way as a differential solution.*

Proposition 1 seems to be new.

Proposition 1 *Let $A = 0,\ S \neq 0$ be a regular differential system of R and $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be the differential prime components of $[A] : S^\infty$. Let K_i be the differential field of fractions of $R/\mathfrak{p}_i$. Then the total ring of fractions of $R/[A] : S^\infty$ is isomorphic to the direct product of differential fields $G = K_1 \times \cdots \times K_t$.*

Proof Let $1 \leq i \neq j \leq t$ be two indices. By the Chinese Remainder Theorem [10, Exercise 2.6, page 79] it is sufficient to prove that the sum $\mathfrak{p}_i + \mathfrak{p}_j = (1)$ in G. Since $[A] : S^\infty$ is radical by the lifting of Lazard's lemma, this amounts to prove that there exists $f_i \in \mathfrak{p}_i$ and $f_j \in \mathfrak{p}_j$ such that $f_i + f_j$ belongs to none of the $\mathfrak{p}$.

Let X denote the finite set of derivatives occuring in $A \cup S$. Let $\mathfrak{b}_i = \mathfrak{p}_i \cap K[X]$. By the lifting of Lazard's lemma again $\mathfrak{b}_1, \ldots, \mathfrak{b}_t$ are the minimal primes of $(A) : S^\infty$ in $K[X]$. By Lazard's lemma, all these ideals have the same dimension d. We claim $\mathfrak{b}_i + \mathfrak{b}_j$ is not contained in the union of the $\mathfrak{b}$. On one hand, if it were, it would be contained in one of them by the prime avoidance lemma and would have dimension[2] $\geq d$. On another hand, $\mathfrak{b}_i + \mathfrak{b}_j$ is a proper divisor of $\mathfrak{b}_i$ and $\mathfrak{b}_j$ since both are minimal over $(A) : S^\infty$. Thus $\dim \mathfrak{b}_i + \mathfrak{b}_j < d$.

Thus there exists $f_i \in \mathfrak{b}_i$ and $f_j \in \mathfrak{b}_j$ such that $f_i + f_j$ belongs to none of the $\mathfrak{b}$. The polynomial $f_i + f_j \in K[X]$ thus it belongs to none of the $\mathfrak{p}$ by the lifting of Lazard's lemma. Since $f_i \in \mathfrak{p}_i$ and $f_j \in \mathfrak{p}_j$, the proposition is proved. □

1.1 An example

We will follow the next example throughout this paper. It is a system of three differential polynomial equations.

$$\Sigma \left\{ \begin{array}{l} u_x^2 - 4u = 0, \\ u_{xy} v_y - u + 1 = 0, \\ v_{xx} - u_x = 0. \end{array} \right.$$

There are two derivations $\partial/\partial x$ and $\partial/\partial y$ and two differential indeterminates u, v (meaning we are looking for two functions $v(x, y)$ and $u(x, y)$ of two independent variables). We denote $u_x = \partial u/\partial x$ and $u_{xy} = \partial^2 u/\partial x \partial y$. The derivatives ocuring in Σ are $u_x, u, v_y, u_{xy}, v_{xx}$.

[2] We use the fact that if $\mathfrak{p} \subset \mathfrak{p}'$ are two prime ideals then $\dim \mathfrak{p} \geq \dim \mathfrak{p}'$; if moreover $\dim \mathfrak{p} = \dim \mathfrak{p}'$ then $\mathfrak{p} = \mathfrak{p}'$. See for instance [15, proposition 4, page 20].

Let's fix the following ranking $\mathcal{R}$. This is the ranking w.r.t. which computations are nearly immediate.

$$\cdots > v_{xx} > v_{xy} > v_{yy} > u_{xx} > u_{xy} > u_{yy} > v_x > v_y > u_x > u_y > v > u.$$

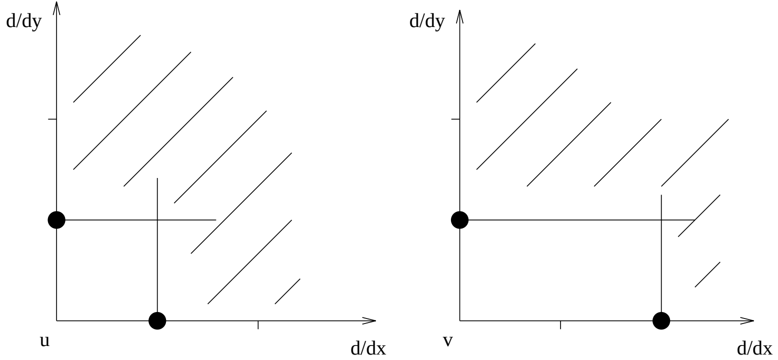
The leaders of the elements of Σ w.r.t. $\mathcal{R}$ are u_x, u_{xy}, v_{xx}. Running the Rosenfeld–Gröbner algorithm over Σ and $\mathcal{R}$, we get only one regular differential ideal

$$\sqrt{[\Sigma]} = [A] : S^{\infty}$$

where

$$A \left\{ \begin{array}{l} v_{xx} - u_x, \\ 4v_y u + u_x u_y - u_x u_y u, \\ u_x^2 - 4u, \\ u_y^2 - 2u \end{array} \right.$$

and $S = \{s_2, s_3, s_4\}$ where $s_2 = 4u$, $s_3 = 2u_x$ and $s_4 = 2u_y$ is the set of the nonconstant separants of the elements of A. The set of leaders of the elements of A w.r.t. $\mathcal{R}$ is $L = \{v_{xx}, v_y, u_x, u_y\}$. The following diagrams show the sets of derivatives of the differential indeterminates u and v. The leaders are presented by black circles. The areas which contain their derivatives are striped.



The set of derivatives lying in the nonstriped areas is the set N of the derivatives under the stairs. The set $N = \{v_x, v, u\}$ is finite here but does not need in general to be so. When finite, its cardinal is an invariant of the ideal[3] and gives the number of arbitrary constants the solutions of the system depend on. Here are the solutions of Σ, computed using the `diffalg` package, the arbitrary constants being denoted c_0, c_1 and c_2.

$$\begin{aligned} u(x,y) &= c_0 + c_3\,x + c_4\,y + x^2 + \frac{2\,c_4}{c_3}\,xy + \frac{1}{2}\,y^2, \\ v(x,y) &= c_1 + c_2\,x - \frac{c_4c_3 - c_4c_3c_0}{4\,c_0}\,y + \frac{c_3}{2}\,x^2 + c_4\,xy \\ &\qquad + \frac{c_0}{c_3}\,y^2 + \frac{1}{3}\,x^3 + \frac{c_4}{c_3}\,x^2y + \frac{1}{2}\,xy^2 + \frac{c_4}{6\,c_3}\,y^3. \end{aligned}$$

The other constants c_3 and c_4 are algebraic over c_0, c_1 and c_2. They satisfy:

$$c_3^2 = 4\,c_0, \quad c_4^2 = 2\,c_0, \quad c_0 \neq 0.$$

[3] It is the degree of algebraic transcendency of the field of fractions of $R/\mathfrak{p}$ over K, where $\mathfrak{p}$ is any differential prime component of $[A] : S^{\infty}$.

Finally, let's say that we would like to compute a differential system $\tilde{A} = 0,\ \tilde{S} \neq 0$ regular w.r.t. the following elimination ranking $\tilde{\mathcal{R}}$ and such that $[A] : S^\infty = [\tilde{A}] : \tilde{S}^\infty$.

$$\cdots > u_x > u_y > u > \cdots > v_{xx} > v_{xy} > v_{yy} > v_x > v_y > v.$$

Running Rosenfeld–Gröbner directly over Σ and $\tilde{\mathcal{R}}$ makes the memory of the computer explode.

1.2 Gröbner bases

Gröbner bases are presented in [9, 2]. Let $R = K[X]$ be a polynomial ring. A *term* over X is a power product of elements of X. If B is a Gröbner basis then $\xrightarrow[B]{*}$ denotes the reduction by the basis B, using the classical reduction algorithm of the Gröbner basis theory, which rewrites a term as a polynomial.

Let $S = \{s_1, \ldots, s_t\}$. To each s_k we associate an indeterminate $\overline{s}_k$ over R and denote $\overline{S} = \{\overline{s}_1, \ldots, \overline{s}_t\}$. A Gröbner basis of $S^{-1}(A)$ is obtained by computing a Gröbner basis of $(A \cup \{s\overline{s} - 1 \mid s \in S\})$. Modulo the relation $s\overline{s} - 1$, each $\overline{s} = 1/s$. See [10, Exercise 2.2, page 79].

2 Normal form of a differential polynomial

Let $A = 0,\ S \neq 0$ be a regular differential system. Denote L the set of its leaders and N the derivatives under the stairs. Given any differential polynomial $f \in R$, the following algorithm (Ritt's algorithm of partial reduction) computes a triple $[h, \overline{h}, r]$ such that h is a power product of s's and $\overline{h}$ is the corresponding product of $\overline{s}$'s and $r \in K[L, N]$ is a differential polynomial satisfying

$$\begin{aligned} h\,f &= r \quad (\bmod\ [A]), \\ f &= \overline{h}\,r \quad (\bmod\ S^{-1}[A]). \end{aligned}$$

By prem(f, g, u) we denote a function which computes the pseudo–remainder of the polynomial f by the polynomial g, viewed as univariate polynomials in the indeterminate u.

```
partial_rem($f$, $A$)
begin
  $h := 1$; $\overline{h} := 1$; $r := f$
  while $r \notin K[L, N]$ do
    let $w$ be the highest derivative w.r.t. the ranking which appears
      in $r$ and is also a proper derivative of the leader $v$ of some $p \in A$
    let $\theta \in \Theta$ be such that $\theta v = w$ and $s$ denote the separant of $p$
    $h := h\, s^{\deg(r,w)}$; $\overline{h} := \overline{h}\, \overline{s}^{\deg(r,w)}$; $r :=$ prem($r$, $\theta p, w$)
  od
  return $[h, \overline{h}, r]$
end
```

Lemma 1 *Let* $f \equiv f' \pmod{[A]{:}S^\infty}$ *be two polynomials and denote* $[h,\, \overline{h},\, r] = \mathsf{partial\_rem}(f,\, A)$ *and* $[h',\, \overline{h}',\, r'] = \mathsf{partial\_rem}(f',\, A)$*. Then* $\overline{h} r \equiv \overline{h}' r' \pmod{S^{-1}(A)}$*.*

Proof Using the specifications of the reduction algorithm we have $rh' \equiv r'h \pmod{[A]{:}S^\infty}$ whence, using Rosenfeld's lemma, $rh' \equiv r'h \pmod{(A) : S^\infty}$. Multiply both sides by $\overline{h}\overline{h}'$, simplify by $h\overline{h} = h'\overline{h}' = 1$ and use the fact that $S^{-1}\left((A) : S^\infty\right) = S^{-1}(A)$. □

Notice that, if $[h,\, \overline{h},\, r] = \mathsf{partial\_rem}(f,\, A)$, then the fraction r/h is not necessarily a canonical representative of f. Consider again the example of section 1.1 and take $f = 2v_{yy}$. Then $r/h = 4u/u_x$. Take $f' = u_x$. Then $r'/h' = u_x/1$. Observe we have $r/h \neq r'/h'$ though $2v_{yy} \equiv u_x \pmod{[A] : S^\infty}$ for $u_x^2 - 4u \in [A] : S^\infty$.

```
NF($f$, $A$)
begin
  $[h,\, \overline{h},\, r] := \mathsf{partial\_rem}(f,\, A)$
  let $B$ be a Gröbner basis of $S^{-1}(A)$
  let $\overline{f}$ be such that $\overline{h}\, r \xrightarrow[B]{*} \overline{f}$
  return $\overline{f}$
end
```

Theorem 2 *The polynomial* $\mathsf{NF}(f,\, A)$ *belongs to* $K[L, N, \overline{S}]$ *and we have*

$$f \equiv \mathsf{NF}(f, A) \pmod{S^{-1}[A]}.$$

It is a canonical representative of the residue class of f *in* $S^{-1}R/S^{-1}[A]$*.*

Proof The first claim comes from the specifications of the reduction algorithm partial_rem and of the Gröbner basis reduction algorithm [2, proposition 5.27]. Let's assume now that $f \equiv f' \pmod{[A] : S^\infty}$. Let $[h, \overline{h}, r] = \mathsf{partial\_rem}(f,\, A)$ and $[h', \overline{h}', r'] = \mathsf{partial\_rem}(f',\, A)$. By lemma 1 we have $r\overline{h} \equiv r'\overline{h}' \pmod{(B)}$. Since a polynomial which is irreducible by a Gröbner basis B is a canonical representative of its residue class modulo (B) [2, proposition 5.38 (vi)], the canonicity claim is proved. □

Using our implementation of the NF algorithm, we find $\mathsf{NF}(2v_{yy}, A) = u_x = \mathsf{NF}(u_x, A)$. This example shows also that theorem 3 below would not hold at all if NF did not compute canonical representatives ! This theorem is important: it basically says that determining if there exists a linear dependency between differential polynomials $p_1, \ldots, p_t$ in a factor ring $R/[A] : S^\infty$ amounts to determine if there exists a linear dependency between their normal forms, regarding them as vectors of elements of K.

Theorem 3 *Let* $p_1, \ldots, p_t \in R$ *be differential polynomials. There exists* $\lambda_1, \ldots, \lambda_t \in K$ *such that* $\lambda_1 p_1 + \cdots + \lambda_t p_t \in [A] : S^\infty$ *if and only if* $\lambda_1\, \mathsf{NF}(p_1, A) + \cdots + \lambda_t\, \mathsf{NF}(p_t, A) = 0$*.*

Proof On one hand $p \in [A] : S^\infty$ if and only if $\mathsf{NF}(p, A) = 0$ (theorem 2); on another one $\lambda_1\, \mathsf{NF}(p_1, A) + \cdots + \lambda_t\, \mathsf{NF}(p_t, A)$ is equal to its normal form. □

3 Kähler differentials

See [10, chapter 16] for a presentation of Kähler differentials in the purely algebraic case and [13] for Kähler differentials in differential algebra.

Definition 2 *Let K be a field. If G is an algebra over K then the module of Kähler differentials of G over K, denoted $\Omega_{G/K}$ is the module over G generated by the set $\{\mathrm{d}(b) \mid b \in G\}$ such that*

$$\begin{aligned} \mathrm{d}(b+b') &= \mathrm{d}(b) + \mathrm{d}(b') \quad \textit{for all } b, b' \in G \\ \mathrm{d}(b\,b') &= b\,\mathrm{d}(b') + b'\,\mathrm{d}(b) \quad \textit{for all } b, b' \in G \\ \mathrm{d}(a) &= 0 \quad \textit{for all } a \in K. \end{aligned}$$

From the definition, follows the fact that $\mathrm{d}(a/b) = (\mathrm{d}(a)\,b - a\,\mathrm{d}(b))/b^2$ for every $a/b \in G$.

Proposition 2 *If K is a differential field and G is a differential algebra over K then $\Omega_{G/K}$ has a canonical structure of differential module over G such that*

$$\delta \mathrm{d}(b) = \mathrm{d}(\delta b) \quad \textit{for all } b \in G \textit{ and derivation } \delta \textit{ over } G.$$

Proof [13, proposition, page 93]. □

The following theorem is purely algebraic.

Theorem 4 *If K is a field of characteristic zero and G is a field extension of K then the elements $\eta_1, \ldots, \eta_r$ of G are algebraically independent over K if and only if $\mathrm{d}(\eta_1), \ldots, \mathrm{d}(\eta_r)$ are linearly independent over G.*

Proof [10, theorem 16.14, page 400] or [13, lemma, page 94]. □

Theorem 5 *Let K be a differential field. If G is a finitely generated differential field extension of K, say $G = K\langle \eta_1, \ldots, \eta_r \rangle$, then $\Omega_{G/K}$ is generated by $\mathrm{d}(\eta_1), \ldots, \mathrm{d}(\eta_r)$ as a differential vector space over G.*

Proof [13, lemma, page 94]. □

Theorem 6 *If $G_1, \ldots, G_r$ are algebras over K and $G = G_1 \times \cdots \times G_r$ then*

$$\Omega_{G/K} = \Omega_{G_1/K} \times \cdots \times \Omega_{G_r/K}.$$

Proof [10, proposition 16.10, page 398]. □

4 The algorithm Kähler

Let's consider again the system of $R = K\{U\}$ given in section 1.1.

$$A \left\{ \begin{array}{l} v_{xx} - u_x, \\ 4v_y u + u_x u_y - u_x u_y u, \\ u_x^2 - 4u, \\ u_y^2 - 2u. \end{array} \right.$$

We are looking for a differential system $\tilde{A} = 0,\ \tilde{S} \neq 0$ equivalent to $A = 0,\ S \neq 0$ for the elimination ranking

$$\cdots > u_x > u_y > u > \cdots > v_{xx} > v_{xy} > v_{yy} > v_x > v_y > v.$$

The Kähler differentials in $\Omega_{R/K}$ of the elements of A are

$$\mathrm{d}(A) \left\{ \begin{array}{l} \mathrm{d}(v_{xx}) - \mathrm{d}(u_x), \\ 4u\mathrm{d}(v_y) + (u_x - u_y u)\mathrm{d}(u_x) + (u_x - u_x u)\mathrm{d}(u_y) + (4v_y - u_x u_y)\mathrm{d}(u), \\ 2u_x \mathrm{d}(u_x) - 4\mathrm{d}(u), \\ 2u_y \mathrm{d}(u_y) - 2\mathrm{d}(u). \end{array} \right.$$

Let's assume that the differential ideal $[A] : S^\infty$ is prime and denote G the differential field of fractions of $R/[A] : S^\infty$. We apply theorem 5 to compute the set of leaders of $\tilde{A}$. To make the set $\mathrm{d}(A)$ generates $\Omega_{G/K}$ as a differential vector space over G, we may just

1. define two new differential indeterminates du and dv ;

2. code the differentials $\mathrm{d}(\theta u)$ and $\mathrm{d}(\phi v)$ which occur in $\mathrm{d}(A)$ as derivatives θdu and ϕdv of the new differential indeterminates ;

3. enlarge the so transformed system $\mathrm{d}(A)$ with the equations $A = 0$ and the inequations[4] $S \neq 0$ in order to have the coefficients of the differentials taken in G (i.e. mod $[A]{:}S^\infty$) ;

$$\left\{ \begin{array}{l} dv_{xx} - du_x, \\ 4udv_y + (u_x - u_y u)du_x + (u_x - u_x u)du_y + (4v_y - u_x u_y)du, \\ 2u_x du_x - 4du, \\ 2u_y du_y - 2du, \\ v_{xx} - u_x, \\ 4v_y u + u_x u_y - u_x u_y u, \\ u_x^2 - 4u, \\ u_y^2 - 2u. \end{array} \right.$$

4. run Rosenfeld–Gröbner over the enlarged system for the suitable ranking:

   (a) the derivatives of du and dv are ranked according to $\tilde{\mathcal{R}}$;

[4] The inequations are important, to avoid useless splittings.

(b) every derivative of du or dv is ranked higher than any derivative of u or v ;

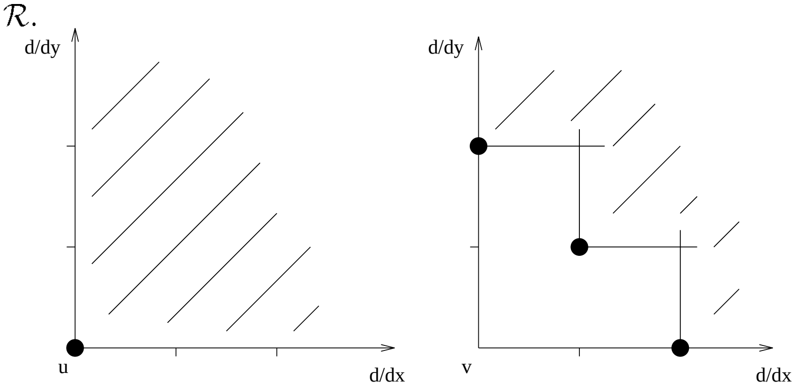
(c) the derivatives of u and v are ranked according to $\mathcal{R}$ (so that Rosenfeld–Gröbner does not waste time modifying the equations of A).

The Rosenfeld–Gröbner algorithm quickly computes a regular differential system. We do not give the equations in R which are the ones of A. The other ones are

$$du = \frac{u_y u_x}{2u} dv_y, \quad dv_{xx} = \frac{u_y}{u} dv_y, \quad dv_{xy} = \frac{u_x}{2u} dv_y, \quad dv_{yy} = \frac{u_y}{2u} dv_y.$$

We can immediately deduce from this computation that the leaders of $\tilde{A}$ are $u, v_{xx}, v_{xy}, v_{yy}$ and, using theorem 4, that for each set $W_1 = \{u, v_y\}$, $W_2 = \{v_{xx}, v_y\}$, $W_3 = \{v_{xy}, v_y\}$ and $W_4 = \{v_{yy}, v_y\}$ we have $[A] : S^\infty \cap K[W_i] \neq (0)$.

The following diagram shows the derivatives of u and v. The leaders of the elements of $\tilde{A}$ are presented by black circles. The areas which contain their derivatives are striped. We may then verify that the number of derivatives lying under the stairs for the ranking $\tilde{\mathcal{R}}$ is the same as for $\mathcal{R}$.



What if $[A] : S^\infty$ is not prime ? We may consider (proposition 1 and theorem 6) that we perform the computations separately modulo the differential prime components of $[A] : S^\infty$. We give in section 6.1 a method to verify the correctness of the result.

5 The algorithm dfglm

5.1 Normal form of a Kähler differential

Consider again the example of section 1.1. The system $\mathrm{d}(A)$ may be viewed as a rewrite system which rewrites the differentials of the leaders of the elements of A as linear combinations of $\mathrm{d}(w)$ where $w \in N$ with coefficients in $K[L, N, \overline{S}]$. Recall $\overline{s}$ denotes the formal inverse of s.

$$\mathrm{d}(A) \left\{ \begin{array}{l} \mathrm{d}(v_{xx}) \to \mathrm{d}(u_x), \\ \mathrm{d}(v_y) \to -\overline{s_2}(u_x - u_y u)\mathrm{d}(u_x) - \overline{s_2}(u_x - u_x u)\mathrm{d}(u_y) - \overline{s_2}(4v_y - u_x u_y)\mathrm{d}(u), \\ \mathrm{d}(u_x) \to 4\overline{s_3}\mathrm{d}(u), \\ \mathrm{d}(u_y) \to 2\overline{s_4}\mathrm{d}(u). \end{array} \right.$$

We denote $\xrightarrow[\mathrm{d}(A)]{*}$ the reduction by the rewrite system $\mathrm{d}(A)$. For instance,

$$3\mathrm{d}(v_{xx}) + \mathrm{d}(v) \xrightarrow[\mathrm{d}(A)]{*} 3\mathrm{d}(u_x) + \mathrm{d}(v).$$

Let's generalize and consider any regular differential system $A = 0,\ S \neq 0$ of R. Denote L the set of leaders of A and N the set of derivatives lying under the stairs. Consider the following algorithm.

```
DNF($f$, $A$)
begin
  let $B$ be a Gröbner basis of $S^{-1}(A)$
  $[h, \overline{h}, r]$ := partial_rem($f$, $A$)
  $d := (\mathrm{d}(r)h - r\mathrm{d}(h))\overline{h}^2$
  let $\overline{d}$ be such that $d \xrightarrow[\mathrm{d}(A)]{*} \xrightarrow[B]{*} \overline{d}$
  return $\overline{d}$
end
```

Proposition 3 *Denote $G = S^{-1}R/S^{-1}[A]$. The differential* DNF$(f,\ A)$ *is a linear combination of* $\mathrm{d}(w)$ *where $w \in N$ with coefficients in $K[L, N, \overline{S}]$. It is equivalent to* $\mathrm{d}(f)$ *in* $\Omega_{G/K}$.

Proof The specifications of the reduction algorithm imply that d is a linear combination of $\mathrm{d}(w)$ where $w \in L \cup N$ with coefficients in $K[L, N, \overline{S}]$. Since $\mathrm{d}(A)$ rewrites the $\mathrm{d}(w)$ where $w \in L$ in terms of the $\mathrm{d}(w')$ where $w' \in N$, the first claim is proved.

The second claim comes from the facts that if $p \in S^{-1}[A]$ then $\mathrm{d}(p) = 0$ in $\Omega_{G/K}$, that $f = \overline{h}r \pmod{S^{-1}[A]}$ and that $A \subset S^{-1}[A]$. □

Proposition 4 *Let $A = 0,\ S \neq 0$ be a regular differential system of R and G the total ring of fractions of $R/[A] : S^\infty$. For every $\lambda_1, \ldots, \lambda_t \in G$ and $w_1, \ldots, w_t \in N$, if*

$$\lambda_1 \mathrm{d}(w_1) + \cdots + \lambda_t \mathrm{d}(w_t) = 0 \quad \textit{in} \quad \Omega_{G/K} \tag{1}$$

then $\lambda_1 = \cdots = \lambda_t = 0$.

Proof Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the differential prime components of $[A] : S^\infty$. Denote G_i the field of fractions of $R/\mathfrak{p}_i$. By proposition 1 and theorem 6 $\Omega_{G/K} \simeq \Omega_{G_1/K} \times \cdots \times \Omega_{G_n/K}$. If a nontrivial relation (1) held in $\Omega_{G/K}$ then such a nontrivial relation would hold in some $\Omega_{G_i/K}$ too and by theorem 4 the set N would be algebraically dependent modulo $\mathfrak{p}_i$. This contradiction to theorem 1 proves the proposition. □

Theorem 7 *Let $A = 0,\ S \neq 0$ be a regular differential system. Denote $G = S^{-1}R/S^{-1}[A]$. The differential* DNF$(f,\ A)$ *is a canonical representative of* $\mathrm{d}(f)$ *in* $\Omega_{G/K}$.

Proof Assume $\mathrm{d}(f) = \mathrm{d}(f')$ in $\Omega_{G/K}$. We have DNF(f, A) = DNF(f', A) in $\Omega_{G/K}$ by proposition 3. Both these differentials are linear combinations of $\mathrm{d}(w)$ where $w \in N$. Proposition 4 implies their coefficients are pairwise equal (as elements of G). Since these coefficients are denoted by canonical representatives (proposition 2) the differentials DNF(f, A) and DNF(f', A) are syntactically equal. □

Theorem 8 *Assume $[A]:S^\infty$ is prime. Let $\{v_1, \ldots, v_t\}$ be a set of derivatives. Then $K[v_1, \ldots, v_t] \cap [A]:S^\infty \neq (0)$ if and only if there exist $\lambda_1, \ldots, \lambda_t \in K[L, N, \overline{S}]$ such that*

$$\lambda_1 \,\mathsf{DNF}(v_1, A) + \cdots + \lambda_t \,\mathsf{DNF}(v_t, A) \xrightarrow[B]{*} 0$$

where B is a Gröbner basis of the ideal $S^{-1}(A)$ (the reduction applying on the coefficients of the differential).

Proof Denote G the fraction field of $R/[A]:S^\infty$. By definition, $K[v_1, \ldots, v_t] \cap [A]:S^\infty \neq (0)$ if and only if the images in G of the derivatives $v_1, \ldots, v_t$ are algebraically dependent over K i.e. (theorem 4) if and only if there exists $\mu_1, \ldots, \mu_t \in G$ such that

$$\mu_1 \mathrm{d}(v_1) + \cdots + \mu_t \mathrm{d}(v_t) = 0 \quad \text{in} \quad \Omega_{G/K} \tag{2}$$

Multiplying the μ coefficients by some nonzero element of G to clear the denominators, replacing them by their normal forms and substituting $\mathsf{DNF}(v_i, A)$ to each $\mathrm{d}(v_i)$ (using proposition 3) we see relation (2) is equivalent to

$$\lambda_1 \,\mathsf{DNF}(v_1, A) + \cdots + \lambda_t \,\mathsf{DNF}(v_t, A) = 0 \quad \text{in} \quad \Omega_{G/K} \tag{3}$$

where the λ coefficients belong to $K[L, N, \overline{S}]$. By proposition 3 the differential on the left hand side of (3) is a linear combination of $\mathrm{d}(w)$ where $w \in N$. Thus by proposition 4 relation (3) holds if and only if all its coefficients are zero modulo $S^{-1}[A]$ i.e. (using Rosenfeld's lemma) if and only if they are all reduced to zero by the Gröbner basis B of $S^{-1}(A)$. □

Assume $[A] : S^\infty$ is prime. The above theorem permits us to look for the existence of a differential polynomial in $[A]:S^\infty \cap K[v_1, \ldots, v_t]$ by interpreting $\mathsf{DNF}(v_1, A), \ldots, \mathsf{DNF}(v_t, A)$ as vectors and performing (say) gaussian elimination. A Gröbner basis of $S^{-1}(A)$ being sufficient to test equality with zero. This is applied in the dfglm algorithm of the next section.

The ideal $[A]:S^\infty$ is prime if and only if $(A):S^\infty$ is prime (this is a corollary to Rosenfeld's lemma). So the primality test is algorithmic.

Assume $[A]:S^\infty$ is not prime. Then the total ring of fractions of $R/[A]:S^\infty$ is isomorphic to a product of fields $K_1 \times \cdots \times K_n$ (proposition 1). We may run the gaussian elimination algorithm over the product and consider we are computing in parallel over each component. If a linear combination of $\mathsf{DNF}(v_i, A)$ is reduced to zero then it is zero over all the components; if nonzero, then it is nonzero over at least one of the components. More satisfactory, each time we need to invert some element in G, we could test if it is invertible or not (this is algorithmic by [5, corollary 4.1, point 3] but rather expensive). If it is not then a splitting of the ideal $[A] : S^\infty$ is discovered and computations can go on by considering separately the two cases. This is the same idea as the one applied in commutative algebra in [16, 17, 1].

It is also sometimes possible to perform computations as if G were a field and verify the correctness of the result afterwards (section 6.1).

5.2 An analogue of the FGLM algorithm

The following algorithm applies theorem 8 in the case of a regular differential system $A = 0,\ S \neq 0$ such that the set N of derivatives under the stairs is finite and the ideal $[A] : S^\infty$ is prime. In that case, $\Omega_{G/K}$ is a finite vector space over the field of fractions of $R/[A] : S^\infty$.

The algorithm is directly inspired from the FGLM algorithm [11]. Assume $A = 0,\ S \neq 0$ is a regular differential system for some ranking $\mathcal{R}$. Given another ranking $\tilde{\mathcal{R}}$, we are looking for a regular differential system $\tilde{A} = 0,\ \tilde{S} \neq 0$ such that $[A] : S^\infty = [\tilde{A}] : \tilde{S}^\infty$. The algorithm dfglm below returns the list of the leaders of $\tilde{A}$.

- *to_see* is a list of derivatives to consider. This list is ordered increasingly w.r.t. $\tilde{\mathcal{R}}$.
- *new_leaders* is the list of the leaders of the elements of $\tilde{A}$.
- *new_irr* is the list of the derivatives which are not derivatives of any element of $\tilde{A}$.
- the function call update(v, *to_see*) inserts the derivatives of v w.r.t. all the derivations $\delta_1, \ldots, \delta_m$ in the list *to_see*. Duplicates are removed. The list is sorted increasingly w.r.t. $\tilde{\mathcal{R}}$.

```
dfglm($A = 0,\ S \neq 0,\ \tilde{\mathcal{R}}$)
begin
  $to\_see$ := the list of the differential indeterminates $u_1, \ldots, u_n$ sorted increasingly w.r.t. $\tilde{\mathcal{R}}$
  $new\_leaders := \emptyset$
  $new\_irr := \emptyset$
  while $to\_see \neq$ the empty list do
    $v :=$ first($to\_see$)
    $to\_see :=$ tail($to\_see$)
    if $v$ is not a derivative of any element of $new\_leaders$ then
      if there exists a linear dependency over $G$
                  between DNF($v, A$) and $\{$DNF($w, A$) $\mid w \in new\_irr\}$ then
        $new\_leaders := new\_leaders \cup \{v\}$
      else
        $new\_irr := new\_irr \cup \{v\}$
      fi
      $to\_see :=$ update($v, to\_see$)
    fi
  od
  $new\_leaders$
end
```

Why should dfglm be better than Kähler ? We do not have any proof of that conjecture but a strong hint: the completion process performed by Rosenfeld–Gröbner over systems of linear PDE is close to the completion process performed by the Buchberger's algorithm (it is the same when the linear PDE depend on only one differential indeterminate and have constant coefficients) while the behaviour of dfglm is close to the one of FGLM. And it is known that computing a Gröbner basis by change of orderings using FGLM is much faster than calling the Buchberger's algorithm.

5.2.1 An example

We detail the computation over the system given in section 1.1. We assume the differential ideal $[A] : S^\infty$ is prime. We have $\overline{s_2} = 1/(4u)$ and $\overline{s_3} = 1/(2u_x)$ and $\overline{s_4} = 1/(2u_y)$. The differentials $\mathsf{DNF}(v, A)$ are linear combinations of $\mathrm{d}(u)$, $\mathrm{d}(v)$ and $\mathrm{d}(v_x)$. We take for $\tilde{\mathcal{R}}$ the elimination ranking

$$\cdots > u_x > u_y > u > \cdots > v_{xx} > v_{xy} > v_{yy} > v_x > v_y > v.$$

1. Initially *to_see* $= [v, u]$. The lists *new_irr* and *new_leaders* are empty.

2. The derivative v is picked from *to_see* and stored in *new_irr*. We have $\mathsf{DNF}(v, A) = \mathrm{d}(v)$. After update we get *to_see* $= [v_y, v_x, u]$.

3. The derivative v_y is picked from *to_see*. Its differential
$$\mathsf{DNF}(v_y, A) = \frac{u_x u_y - 4v_y}{4}\mathrm{d}(u)$$
is not linearly dependent on $\mathsf{DNF}(v, A) = \mathrm{d}(v)$. Thus v_y is stored in *new_irr*. After update we get *to_see* $= [v_x, v_{yy}, v_{xy}, u]$.

4. The derivative v_x is picked from *to_see*. Its differential $\mathsf{DNF}(v_x, A) = \mathrm{d}(v_x)$ is not linearly dependent on $\mathsf{DNF}(v, A)$ and $\mathsf{DNF}(v_y, A)$. Thus v_x is stored in *new_irr*. After update we get *to_see* $= [v_{yy}, v_{xy}, v_{xx}, u]$.

5. The derivative v_{yy} is picked from *to_see*. Its differential
$$\mathsf{DNF}(v_{yy}, A) = \frac{\overline{s_4}(u_x u_y - 4v_y)}{2}\mathrm{d}(u)$$
satisfies a linear relation with $\mathsf{DNF}(v_y, A)$. Thus v_{yy} is stored in *new_leaders*.

6. The derivative v_{xy} is picked from *to_see*. Its differential $\mathsf{DNF}(v_{xy}, A) = 2\overline{s_4}\mathrm{d}(u)$ satisfies a linear relation with $\mathsf{DNF}(v_y, A)$. Thus v_{xy} is stored in *new_leaders*.

7. The derivative v_{xx} is picked from *to_see*. $\mathsf{DNF}(v_{xx}, A) = \overline{s_4}(u_x u_y - 4v_y)\mathrm{d}(u)$ satisfies a linear relation with $\mathsf{DNF}(v_y, A)$. Thus v_{xx} is stored in *new_leaders*.

8. The derivative u is picked from *to_see*. Its differential $\mathsf{DNF}(u, A) = \mathrm{d}(u)$ satisfies a linear relation with $\mathsf{DNF}(v_y, A)$ thus is stored in *new_leaders*.

9. The list *to_see* is empty. The list $[u, v_{xx}, v_{xy}, v_{yy}]$ of the leaders of $\tilde{A}$ is returned.

The dfglm algorithm can easily be transformed to provide with each new leader v a set of derivatives $v'_1, \ldots, v'_t$ such that $[A] : S^\infty \cap K[v, v'_1, \ldots, v'_t] \neq \emptyset$. Over the above example, the algorithm would return

$$[\{u, v_y\}, \{v_{xx}, v_y\}, \{v_{xy}, v_y\}, \{v_{yy}, v_y\}].$$

This is the same answer as the one given by Kähler !

6 Searching a polynomial knowing the alphabet

This algorithm follows either Kähler or dfglm. Let W be a set of derivatives such that $[A]:S^\infty \cap K[W] \neq (0)$. We are looking for a nonzero polynomial. For this, we enumerate all the terms $t_1, \ldots$ over W by increasing total degree. At every step j we consider $t_1, \ldots, t_j$ and we apply theorem 3 to search $\lambda_1, \ldots, \lambda_j \in K$ such that $\lambda_1 t_1 + \cdots + \lambda_j t_j \in [A]:S^\infty$ or to determine no such coefficients exist. Continuing the example of section 1.1 and applying this method, we obtain the system

$$\hat{A} \left\{ \begin{array}{lcl} f_1 & = & u^2 - 2u - 2v_y^2 + 1, \\ f_2 & = & v_{xx}^4 - 8v_{xx}^2 - 32v_y^2 + 16, \\ f_3 & = & v_{xy}^4 - 4v_{xy}^2 - 8v_y^2 + 4, \\ f_4 & = & v_{yy}^4 - 2v_{yy}^2 - 2v_y^2 + 1. \end{array} \right.$$

Observe in general $\hat{A} \neq \tilde{A}$ and even $[\hat{A}]:\hat{S}^\infty \neq [\tilde{A}]:\tilde{S}^\infty$. However the elements of $\hat{A}$ are differential polynomials of lowest order w.r.t. $\tilde{\mathcal{R}}$ which belong to $[A]:S^\infty$. They are very useful to speed up the completion process of the Rosenfeld–Gröbner algorithm. Applying Rosenfeld–Gröbner over $A \cup \hat{A} = 0$, $S \neq 0$ (where $A = 0$, $S \neq 0$ is the system obtained in section 1.1) for the ranking $\tilde{\mathcal{R}}$ we immediately get the desired system

$$\tilde{A} \left\{ \begin{array}{l} u - v_{yy}^2, \\ v_{xx} - 2v_{yy}, \\ v_y v_{xy} - v_{yy}^3 + v_{yy}, \\ v_{yy}^4 - 2v_{yy}^2 - 2v_y^2 + 1. \end{array} \right.$$

6.1 Verifying the correctness of the result

Now, we may verify $[A]:S^\infty = [\tilde{A}]:\tilde{S}^\infty$ by verifying [5, corollary 4.1] on one hand that $A \subset [\tilde{A}]:\tilde{S}^\infty$ and no element of S divides zero modulo $[\tilde{A}]:\tilde{S}^\infty$, on another hand that $\tilde{A} \subset [A]:S^\infty$ and that no element of $\tilde{S}$ divides zero modulo $[A]:S^\infty$. This final verification proves that the computations we performed assuming $[A]:S^\infty$ was prime were correct.

7 Euler's equations for an incompressible fluid

Written as a system of polynomial differential equations, Euler's equations for an incompressible fluid in two dimensions are (example taken from [19])

$$\Sigma \left\{ \begin{array}{l} v_t^1 + v^1 v_x^1 + v^2 v_y^1 + p_x = 0, \\ v_t^2 + v^1 v_x^2 + v^2 v_y^2 + p_y = 0, \\ v_x^1 + v_y^2 = 0. \end{array} \right.$$

The differential indeterminates are v^1, v^2, p where v^1 and v^2 are the two coordinates of the speed and p is the pressure. The derivations are $\partial/\partial x, \partial/\partial y$ and $\partial/\partial t$. The base field is the field $K = \mathbb{Q}$ of the rational numbers.

For some orderly ranking, the Rosenfeld–Gröbner algorithm applied over Σ returns a unique regular differential system $A = 0$ (the leaders appear on the left hand side of the equations)

$$A \left\{ \begin{array}{l} p_{xx} = -2v^2_x v^1_y - 2(v^2_y)^2 - p_{yy}, \\ v^1_t = -v^2 v^1_y - p_x + v^2_y v^1, \\ v^1_x = -v^2_y, \\ v^2_t = -v^1 v^2_x - v^2 v^2_y - p_y. \end{array} \right.$$

The system A is orthonomic (i.e. all leaders appear linearly and the initials are 1). This proves the differential ideal $[\Sigma] = [A]$ is prime [15, lemma 2, page 167]. A derivative of each differential indeterminate appears as a leader of some element of A. Since the ranking is orderly, the ideal has differential dimension zero [15, theorem 6, page 115]. This proves that $[\Sigma] \cap K\{p\} \neq (0)$.

Observe it is not difficult to compute a nonzero differential polynomial in $[\Sigma] \cap K\{v^1\}$ or in $[\Sigma] \cap K\{v^2\}$ (see [19] for a sixth order polynomial and [3, page 94] for a fifth order one). It is however a challenge to compute some nonzero differential polynomial belonging to $[\Sigma] \cap K\{p\}$!

Using theorem 8 we could solve a first step of this problem by (nearly) proving that $[\Sigma] \cap K[X] \neq (0)$ where X is the following alphabet of 39 derivatives:

$$\begin{aligned} X \;=\; & \{p_{ttxxx}, p_{ttxxy}, p_{ttxyy}, p_{ttyyy}, p_{txxxx}, p_{txxxy}, p_{txxyy}, p_{txyyy}, p_{tyyyy}, p_{xxxxx}, p_{xxxxy}, p_{xxxyy}, \\ & p_{xxyyy}, p_{xyyyy}, p_{yyyyy}, p_{ttxx}, p_{ttyy}, p_{txxx}, p_{txxy}, p_{txyy}, p_{tyyy}, p_{xxxx}, p_{xxxy}, p_{xxyy}, p_{xyyy}, p_{yyyy}, \\ & p_{txx}, p_{txy}, p_{tyy}, p_{xxx}, p_{xxy}, p_{xyy}, p_{yyy}, p_{xx}, p_{xy}, p_{yy}, p_x, p_y\} \end{aligned}$$

The idea was: enumerating the derivatives of the pressure p by increasing order and apply theorem 8 to determine the existence of a relation in the differential ideal. Observe we are not in the hypotheses of the dfglm algorithm for the solutions of Σ do not depend on finitely many arbitrary constants (i.e. N is infinite). We can however use this algorithm by halting computations as soon as a leader is found. We make sure to find one because the differential dimension is zero. However, the coefficients of the normal forms of the Kähler differentials were huge and made the memory of the computer explode. So we applied the fact that A is orthonomic which implies that the factor ring $K[L, N]/(A)$ is a free algebra: the sum and the product of two normal forms is still a normal form. For this reason, we could evaluate the normal forms as integer numbers to simplify computations. This is because of this use of evaluation that we say we only nearly proved our claim.

We tried afterwards to seek a differential polynomial in $[\Sigma] \cap K[X]$ using theorem 3 but could not succeed (even evaluating normal forms to floating point numbers and using PSLQ [12]) because of the large number of monomials to consider.

8 A linear example of Cartan

The situation is simpler in the case of a system of linear PDE (there is no need of Kähler differentials). We illustrate it over the following system Λ of six linear PDE.

$$\begin{array}{l}
-\frac{1}{2}(x^2)^2 V^1_{x^2} + V^5_{x^2} = 0,\\
-x^2x^3V^1_{x^3} + x^2V^4_{x^3} - V^3 + V^4_{x^1} - x^3V^1_{x^1} + x^3V^4_{x^4} - (x^3)^2V^1_{x^4} + \frac{1}{2}(x^2)^2V^4_{x^5} - \frac{1}{2}(x^2)^2x^3V^1_{x^5} = 0,\\
-(x^2)^2V^1_{x^3} + x^2V^3_{x^3} - V^2 + V^3_{x^1} - x^2V^1_{x^1} + x^3V^3_{x^4} - x^3x^2V^1_{x^4} + \frac{1}{2}(x^2)^2V^3_{x^5} - \frac{1}{2}(x^2)^3V^1_{x^5} = 0,\\
-\frac{1}{2}(x^2)^3V^1_{x^3} + x^2V^5_{x^3} - V^2x^2 + V^5_{x^1} - \frac{1}{2}(x^2)^2V^1_{x^1} + x^3V^5_{x^4}\\
\qquad\qquad\qquad\qquad -\frac{1}{2}x^3(x^2)^2V^1_{x^4} + \frac{1}{2}(x^2)^2V^5_{x^5} - \frac{1}{4}(x^2)^4V^1_{x^5} = 0,\\
-x^3V^1_{x^2} + V^4_{x^2} = 0,\\
-x^2V^1_{x^2} + V^3_{x^2} = 0.
\end{array}$$

Applying the Rosenfeld–Gröbner algorithm over Λ for some orderly ranking $\mathcal{R}$, we find a regular differential system $A = 0$ made of linear PDE with coefficients in $\mathbb{Q}(x^1, \ldots, x^5)$ the solutions of which depend on 14 arbitrary constants. There are no inequations since the elements of A are linear. Here is the ranking $\mathcal{R}$

- if $|\theta| > |\phi|$ then $\theta V^i > \phi V^j$ for any i, j,
- if $|\theta| = |\phi|$ and $\theta > \phi$ w.r.t. the lex. order $x^1 > \cdots > x^5$ then $\theta V^i > \phi V^j$ for any i, j,
- if $i < j$ then $\theta V^i > \theta V^j$.

We do not give A which is a bit too large, just its set of leaders:

$$\begin{array}{c}
V^5_{x^4x^5x^5},\ V^5_{x^5x^5x^5},\ V^3_{x^4x^4},\ V^4_{x^4x^4},\ V^5_{x^4x^4},\ V^3_{x^4x^5},\ V^4_{x^4x^5},\ V^2_{x^5x^5},\ V^3_{x^5x^5},\ V^4_{x^5x^5},\ V^1_{x^1},\ V^2_{x^1},\\
V^3_{x^1},\ V^4_{x^1},\ V^5_{x^1},\ V^1_{x^2},\ V^2_{x^2},\ V^3_{x^2},\ V^4_{x^2},\ V^5_{x^2},\ V^1_{x^3},\ V^2_{x^3},\ V^3_{x^3},\ V^4_{x^3},\ V^5_{x^3},\ V^1_{x^4},\ V^2_{x^4},\ V^1_{x^5}.
\end{array}$$

We are looking now for a differential system $\tilde{A} = 0$ regular w.r.t. the following ranking $\tilde{\mathcal{R}}$ and such that $[A] = [\tilde{A}]$. The ranking $\tilde{\mathcal{R}}$ is the elimination ranking $V^1 > \cdots > V^5$ where the derivatives of each V^i are ranked w.r.t. the orderly ranking:

- if $|\theta| > |\phi|$ then $\theta V^i > \phi V^i$,
- if $|\theta| = |\phi|$ then $\theta V^i > \phi V^i$ if $\theta > \phi$ for w.r.t. lexical ordering $x^1 > \cdots > x^5$.

Applying the Rosenfeld–Gröbner algorithm over Λ and $\tilde{\mathcal{R}}$ takes a lot of time. We interrupted the computation after a few minutes.

Now, for linear PDE, we can design a variant of the FGLM algorithm which does compute the desired differential system $\tilde{A} = 0$ (and not only its set of leaders !) regular w.r.t. $\tilde{\mathcal{R}}$ in a few seconds, starting from the differential system regular w.r.t. $\mathcal{R}$. Indeed, this variant of FGLM is very close to FGLM.

```
fglm_for_linear_PDE($A = 0$, $\tilde{\mathcal{R}}$)
begin
  $to\_see$ := the list of the differential indeterminates $u_1, \ldots, u_n$ sorted increasingly w.r.t. $\tilde{\mathcal{R}}$
  $new\_leaders$ := $\emptyset$
  $\tilde{A} := \emptyset$
  $new\_irr := \emptyset$
  while $to\_see \neq$ the empty list do
    $v :=$ first($to\_see$)
    $to\_see :=$ tail($to\_see$)
    if $v$ is not a derivative of any element of $new\_leaders$ then
      if there exists some $\lambda_w \in K$ ($w \in new\_irr$) s.t. $\mathsf{NF}(v, A) = \sum \lambda_w \, \mathsf{NF}(w, A)$ then
        $new\_leaders := new\_leaders \cup \{v\}$
        $\tilde{A} := \tilde{A} \cup \{v - \sum \lambda_w w\}$
      else
        $new\_irr := new\_irr \cup \{v\}$
      fi
      $to\_see :=$ update($v, to\_see$)
    fi
  od
  $\tilde{A}$
end
```

Running fglm_for_linear_PDE over $A = 0$ and $\tilde{\mathcal{R}}$ we have got in a few seconds the desired system $\tilde{A} = 0$. Here is the set of leaders of $\tilde{A}$:

$$V^1_{x^1},\ V^1_{x^2},\ V^1_{x^3},\ V^1_{x^4},\ V^1_{x^5},\ V^2,\ V^3,\ V^4_{x^1x^1},\ V^4_{x^1x^4},\ V^4_{x^4x^4},\ V^4_{x^2},\ V^4_{x^3},\ V^4_{x^5},$$
$$V^5_{x^3x^3x^3},\ V^5_{x^3x^3x^5}, V^5_{x^3x^5x^5},\ V^5_{x^4x^5x^5},\ V^5_{x^5x^5x^5},\ V^5_{x^1x^1},\ V^5_{x^1x^2},\ V^5_{x^1x^3},\ V^5_{x^1x^4},$$
$$V^5_{x^1x^5},\ V^5_{x^2x^2},\ V^5_{x^2x^3},\ V^5_{x^2x^4},\ V^5_{x^2x^5},\ V^5_{x^3x^4},\ V^5_{x^4x^4}.$$

8.1 A note on this system

The system Λ arises during the determination of the Lie symmetries of the dynamical system Σ below, first studied by E. Cartan [8]. See [18] for the mathematical theory. The system Σ has five state variables x^i and two commands $u^1(t), u^2(t)$ which are arbitrary functions.

$$x^1_t = u^1, \quad x^2_t = u^2, \quad x^3_t = u^1x^1, \quad x^4_t = u^1x^2, \quad x^5_t = \frac{1}{2}u^1(x^2)^2.$$

We are interested in the vector fields which generate the Lie symmetries of Σ which leave t invariant. Such symmetries are local diffeomorphisms which transform the five variables x^i and map any admissible trajectory of Σ to another one. We transform Σ as a Pfaffian system:

$$\mathrm{d}(x^1) = u^1\mathrm{d}(t), \quad \mathrm{d}(x^2) = u^2\mathrm{d}(t), \quad \mathrm{d}(x^3) = u^1x^1\mathrm{d}(t),$$
$$\mathrm{d}(x^4) = u^1x^2\mathrm{d}(t), \quad \mathrm{d}(x^5) = \tfrac{1}{2}u^1(x^2)^2\mathrm{d}(t).$$

Eliminating $\mathrm{d}(t)$ and the commands, we get three forms of Pfaff in five variables.

$$\mathrm{d}(x^3) = x^2\mathrm{d}(x^1), \quad \mathrm{d}(x^4) = x^3\mathrm{d}(x^1), \quad \mathrm{d}(x^5) = \frac{1}{2}(x^2)^2\mathrm{d}(x^1).$$

We enlarge them with one 2–form (below), computed using the `close` function of the `liesymm` package of MAPLE. Let's call Ω the so closed system.

$$\mathrm{d}(x^1) \wedge \mathrm{d}(x^2) = 0.$$

The symmetries of Σ are then given by vector fields $V = (V^1, \ldots, V^5)$ with five components such that the Lie derivative of each element of Ω w.r.t. V is equal to zero modulo Ω. Computing modulo Ω we rewrite $\mathrm{d}(x^3), \mathrm{d}(x^4), \mathrm{d}(x^5)$ in terms of $\mathrm{d}(x^1)$ and $\mathrm{d}(x^2)$. We thus get a system of four linear equations in $\mathrm{d}(x^1)$ and $\mathrm{d}(x^2)$ (one of them is identically zero) with linear PDE in the V^i and their derivatives for coefficients. The symmetries are thus given by the common zeros of these coefficients. This is the system Λ, computed with the `determine` function of `liesymm`.

Conclusion

We believe this paper contributes to prove that being able to compute normal forms is important since it allows to perform easily linear algebra in factor structures. In particular, the algorithms presented in this paper rely on the computation of the normal form of a fraction p/s in $S^{-1}R/S^{-1}(A)$ where $A = 0,\ S \neq 0$ is a triangular system. This computation is possible using Gröbner bases methods but there does not seem to be any known method based on triangular sets and pseudo–reduction[5]. This is a pain for we implemented since 1998 versions (joint work with François Lemaire) of Rosenfeld–Gröbner in MAPLE and C++ using different versions of the `lextriangular` triangularization algorithm [16, 17] instead of Gröbner bases and we would like to completely avoid these latter.

The author would like to thank M. Petitot for indicating him theorem 4, for the algorithm Kähler and for the analysis of Cartan's example.

References

[1] Philippe Aubry. *Ensembles triangulaires de polynômes et résolution de systèmes algébriques. Implantation en Axiom.* PhD thesis, Université Paris VI, 1999.

[2] Thomas Becker and Volker Weispfenning. *Gröbner Bases: a computational approach to commutative algebra*, volume 141 of *Graduate Texts in Mathematics*. Springer Verlag, 1991.

[3] François Boulier. *Étude et implantation de quelques algorithmes en algèbre différentielle.* PhD thesis, Université Lille I, 59655, Villeneuve d'Ascq, France, 1994.

[4] François Boulier, Daniel Lazard, François Ollivier, and Michel Petitot. Representation for the radical of a finitely generated differential ideal. In *proceedings of ISSAC'95*, pages 158–166, Montréal, Canada, 1995.

[5] François Boulier, Daniel Lazard, François Ollivier, and Michel Petitot. Computing representations for radicals of finitely generated differential ideals. Technical report, Université Lille I, LIFL, 59655, Villeneuve d'Ascq, France, 1997. (technical report IT306 of the LIFL, available at `http://www.lifl.fr/~boulier/jsc6.ps.gz`).

[5] After this paper was written, this problem was solved by François Lemaire and the author in [6].

[6] François Boulier and François Lemaire. Computing canonical representatives of regular differential ideals. (publication interne LIFL 2000–01, submitted to Issac 2000).

[7] Manuel Bronstein. On solutions of linear ordinary differential equations in their coefficient field. *Journal of Symbolic Computation*, 13:413–439, 1992.

[8] Élie Cartan. *Les systèmes différentiels extérieurs et leurs applications géométriques.* Hermann, Paris, 1945.

[9] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties and Algorithms. An introduction to computational algebraic geometry and commutative algebra.* Undergraduate Texts in Mathematics. Springer Verlag, New York, 1992.

[10] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics.* Springer Verlag, 1995.

[11] Jean-Charles Faugère, Patricia Gianni, Daniel Lazard, and Teo Mora. Efficient computation of Gröbner bases by change of orderings. *Journal of Symbolic Computation*, 16:329–344, 1993.

[12] Helaman R. P. Ferguson, David H. Bailey, and Stephen Arno. Analysis of PSLQ, An Integer Relation Finding Algorithm. *Mathematics of Computation*, 1999. (to appear).

[13] Joseph Johnson. Kähler differentials and differential algebra. *Annals of Mathematics*, 89:92–98, 1969.

[14] Erwin Kähler. *Einfürhung in die Theorie der Systeme von Differentialgleichungen.* Teubner, Leipzig, Germany, 1934.

[15] Ellis R. Kolchin. *Differential Algebra and Algebraic Groups.* Academic Press, New York, 1973.

[16] Daniel Lazard. Solving Zero–dimensional Algebraic Systems. *Journal of Symbolic Computation*, 13:117–131, 1992.

[17] Marc Moreno Maza. *Calculs de Pgcd au–dessus des Tours d'Extensions Simples et Résolution des Systèmes d'Équations Algébriques.* PhD thesis, Université Paris VI, France, 1997.

[18] Peter J. Olver. *Equivalence, Invariants and Symmetry.* Cambridge University Press, New York, 1995.

[19] Jean-François Pommaret. New Perspectives in Control Theory for Partial Differential Equations. *IMA Journal of Mathematics Control and Information*, 9:305–330, 1992.

[20] Gregory J. Reid and David K. McKinnon. Solving systems of linear pdes in their coefficient field by recursively decoupling and solving odes. Technical report, Dept. of Maths of the University of British Columbia, Vancouver, Canada, 1992.

[21] Joseph Fels Ritt. *Differential Algebra.* Dover Publications Inc., New York, 1950.