A Normal Form Algorithm for Regular Differential Chains

François Boulier, François Lemaire

▶ To cite this version:

François Boulier, François Lemaire. A Normal Form Algorithm for Regular Differential Chains. Mathematics in Computer Science, Springer, 2010, 4 (2), pp.185-201. hal-00824964

HAL Id: hal-00824964

https://hal.archives-ouvertes.fr/hal-00824964

Submitted on 22 May 2013

A Normal Form Algorithm For Regular Differential Chains

François Boulier and François Lemaire

Abstract. This paper presents a new algorithm for computing the normal form of a differential rational fraction modulo differential ideals presented by regular differential chains. An application to the computation of power series solutions is presented and illustrated with the new *DifferentialAlgebra* MAPLE package.

Keywords. computer algebra; differential algebra; normal form; regular differential chain; characteristic set; power series.

1. Introduction

This paper presents an algorithm for computing the normal form of a differential rational fraction modulo differential ideals presented by regular differential chains. Regular differential chains, introduced by Lemaire (2002a), slightly generalize Ritt's characteristic sets. An equivalent notion was introduced by Hubert (2000).

Even when restricted to differential polynomials, the normal form algorithm has various applications: it permits to decide the equivalence of two differential polynomials modulo a differential ideal presented by a regular differential chain, and it permits to design and implement FGLM-like (Faugère et al., 1993) algorithms, such as (Boulier, 1999). In this paper, one focuses on its application to the computation of power series solutions of regular differential chains, which is an integration related problem. In this context, it simplifies the exposition of the theory. Indeed, the general formula of a power series expansion of some function $u(x)$ writes:

$$u(x) = u(0) + x\,\dot{u}(0) + \frac{x^2}{2}\,\ddot{u}(0) + \cdots$$

When this function is a solution of some differential ideal, presented by some regular differential chain C, the values $u(0)$, $\dot{u}(0)$ and $\ddot{u}(0)$ cannot be chosen freely, since the functions $u(x)$, $\dot{u}(x)$ and $\ddot{u}(x)$ must annihilate all the equations $p = 0$ such that p belongs to the differential ideal. A simple way to state this basic fact consists in replacing each $u(x)$, $\dot{u}(x)$ and $\ddot{u}(x)$ by its normal form, with respect to C. One gets:

$$u(x) = \mathrm{NF}(u,\, C)(0) + x\ \mathrm{NF}(\dot{u},\, C)(0) + \frac{x^2}{2}\ \mathrm{NF}(\ddot{u},\, C)(0) + \cdots$$

The use of normal forms is not necessary: (Boulier et al., 2009, sect 7) gave a method, which does not rely on any normal form method, but which is more cumbersome. Observe that the use of normal forms may make it easier to find recurrence relations among the monomials of the power series, and thereby, may help finding close form solutions.

A normal form algorithm was already presented by Boulier and Lemaire (2000). However, it only applied to differential polynomials. The algorithm presented here is new, since it applies to rational differential fractions. This new feature permits us to state a new result: Proposition 5.5. It might also be interesting in connection with the integration problem of systems of differential equations since, in this area, considering rational differential fractions rather than basic differential polynomials, may give some more freedom to investigate, say, integrating factors.

The paper is organized as follows. Sections 2 and 3 recall some basics of differential algebra and on regular differential chains. Section 4 introduces an algorithm for computing inverses of differential polynomials modulo differential ideals. This algorithm is applied in Section 5 for the normal form algorithm, which consitutes the main result of this paper. Section 6 develops the application to formal power series. We take this opportunity to widen the audience of an analyticity theorem, proved by Lemaire (2002a). Section 7 shows implementations of these methods in the new *DifferentialAlgebra* MAPLE package, developed by the first author and Edgardo S. Cheb-Terrab. Appendix A provides some detailed material for Sections 4 and 5.

2. Basics of differential algebra

The reference books are that of Ritt (1950) and Kolchin (1973). More recent texts are Buium and Cassidy (1998); Sit (2002); Wang (2003); Hubert (2003b). A *differential ring* R is a ring endowed with finitely many, say m, abstract *derivations* $\delta_1, \ldots, \delta_m$ i.e. unary operations which satisfy the following axioms:

$$\delta(a+b) = \delta(a) + \delta(b), \quad \delta(a\,b) = \delta(a)\,b + a\delta(b), \qquad (\forall\, a,\, b \in R)$$

and which are assumed to commute pairwise. This paper is mostly concerned by a differential polynomial ring R in n *differential indeterminates* $u_1, \ldots, u_n$ with coefficients in a commutative differential field K of characteristic zero, say $K = \mathbb{Q}$. Letting $U = \{u_1, \ldots, u_n\}$, one denotes $R = K\{U\}$, following Ritt and Kolchin. The set of derivations generates a commutative monoid w.r.t. the composition operation. It is denoted:

$$\Theta = \{\delta_1^{a_1} \cdots \delta_m^{a_m} \mid a_1, \ldots, a_m \in \mathbb{N}\}$$

where $\mathbb{N}$ stands for the set of the nonnegative integers. The elements of Θ are the *derivation operators*. If $\theta = \delta_1^{a_1} \cdots \delta_m^{a_m}$ is a derivation operator then $\operatorname{ord}\theta = a_1 + \cdots + a_m$ denotes its *order*. The monoid Θ acts on U, giving the infinite set ΘU of the *derivatives*. One indices derivations with letters e.g. δ_x, δ_y and one denotes derivatives using subscripts e.g. u_{xy} denotes $\delta_x\,\delta_y\,u$.

If A is a finite subset of R, one denotes (A) the smallest ideal containing A w.r.t. the inclusion relation and $[A]$ the smallest differential ideal containing A. Let $\mathfrak{A}$ be an ideal and $S = \{s_1, \ldots, s_t\}$ be a finite subset of R, not containing zero. Then

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

is called the *saturation* of $\mathfrak{A}$ by the multiplicative family generated by S. The saturation of a (differential) ideal is a (differential) ideal (Kolchin, 1973, chap. I, cor. to lem. 1).

Definition 2.1. *A* ranking *is a total ordering over ΘU which satisfies the two following axioms:*

1. *$v \leq \theta v$ for every $v \in \Theta U$ and $\theta \in \Theta$,*
2. *$v < w \Rightarrow \theta v < \theta w$ for every $v,\ w \in \Theta U$ and $\theta \in \Theta$.*

See (Kolchin, 1973, chap. I, sect. 8). Rankings such that $\operatorname{ord}\theta < \operatorname{ord}\phi \Rightarrow \theta u < \phi v$ for every $\theta,\ \phi \in \Theta$ and $u,\ v \in U$ are called *orderly*. Rankings such that $\theta u < \phi u \Rightarrow \theta v < \phi v$ for every $\theta,\ \phi \in \Theta$ and $u,\ v \in U$ are called *Riquier* rankings. These two special types of rankings will be especially useful in section 6.3.

Fix a ranking. Consider some differential polynomial $p \notin K$. The highest derivative v w.r.t. the ranking such that $\deg(p, v) > 0$ is called the *leading derivative* of p. It is denoted $\operatorname{ld} p$. 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. If C is a finite subset of $R \setminus K$ then I_C denotes its set of initials, S_C denotes its set of separants and $H_C = I_C \cup S_C$.

A differential polynomial q is said to be *partially reduced* w.r.t. p if it does not depend on any proper derivative of the leading derivative v of p. It is said to be *reduced* w.r.t. p if it is partially reduced w.r.t. p and $\deg(q, v) < \deg(p, v)$. A set of differential polynomials of $R \setminus K$ is said to be *autoreduced* if its elements are pairwise reduced. Autoreduced sets are necessarily finite (Kolchin, 1973, chap. I, sect. 9). To each autoreduced set C, one may associate the set $L = \operatorname{ld} C$ of the leading derivatives of C and the set $N = \Theta U \setminus \Theta L$ of the derivatives which are not derivatives of any element of L (the derivatives "under the stairs" defined by C).

Ritt's reduction algorithm is a generalization of the classical *pseudoremainder* algorithm defined in (Knuth, 1966, vol. 2, page 407), to differential polynomials. Ritt's algorithm is presented in (Kolchin, 1973, chap. I, sect. 9). Given a differential polynomial p and an autoreduced set C, it permits to compute a set of exponents $a_1, \ldots, a_t \in \mathbb{N}$ and a differential polynomial p' partially reduced w.r.t. C (i.e. w.r.t. each element of C) such that $s_1^{a_1} \cdots s_t^{a_t}\, p \equiv p' \mod [C]$ where $s_1, \ldots, s_t$ denote the separants of the elements of C. Given a differential polynomial p' partially reduced w.r.t. C, it permits to compute a set of exponents $b_1, \ldots, b_t \in \mathbb{N}$ and a differential polynomial p'' reduced w.r.t. C such that $i_1^{b_1} \cdots i_t^{b_t}\, p' \equiv p'' \mod (C)$ where $i_1, \ldots, i_t$ denote the initials of the elements of C. When $p'' = 0$ one says that p' *is reduced to zero by* C.

3. Regular differential chains

In this section, one considers a set $C = \{c_1, \ldots, c_t\}$ of R and one denotes $\mathfrak{A} = [C] : H_C^\infty$. The following definition provides a compact presentation of regular differential chains, which were introduced by (Lemaire, 2002a, déf. 5). Roughly speaking they are finite sets of differential polynomials satisfying both the regular chain condition, introduced by Aubry et al. (1999), and the hypotheses of (Rosenfeld, 1959, Lemma). Very close concepts were introduced by Boulier et al. (2009) and Hubert (2000).

Definition 3.1. *The set C is a* regular differential chain *if it satisfies the following conditions:*

a. *the elements of C are pairwise partially reduced and have distinct leading derivatives ;*

b. *for each $2 \leq k \leq t$, the initial i_k of c_k is regular in $K[N, L]/(c_1, \ldots, c_{k-1}) : (i_1 \cdots i_{k-1})^\infty$;*

c. *for each $1 \leq k \leq t$, the separant s_k of c_k is regular in $K[N, L]/(c_1, \ldots, c_k) : (i_1 \cdots i_k)^\infty$;*

d. *for any pair $\{c_k,\, c_\ell\}$ of elements of C, whose leading derivatives $\theta_k u$ and $\theta_\ell u$ are derivatives of some same differential indeterminate u, the Δ-polynomial*

$$\Delta(c_k,\, c_\ell) = s_\ell\, \frac{\theta_{k\ell}}{\theta_k}\, c_k - s_k\, \frac{\theta_{k\ell}}{\theta_\ell}\, c_\ell\,,$$

where $\theta_{k\ell}$ denotes the least common multiple of θ_k and θ_ℓ, is reduced to zero by C, using Ritt's reduction algorithm.

Consider a regular differential chain C. Condition **a** is the *differentially triangular* condition of (Boulier et al., 2009, def. 3). It implies that C is triangular, algebraically. Algebraic triangularity plus condition **b** is equivalent to the *regular chain* condition of Aubry et al. (1999). Condition **c** is then equivalent to the *squarefree regular chain* condition of Aubry et al. (1999). See also (Boulier et al., 2006). Last, condition **d** is the *coherence* condition, which is the key condition of (Rosenfeld, 1959, Lemma). See Boulier et al. (2009) and Hubert (2000) for almost equivalent notions.

The following Proposition will be used in the next section. It clarifies the relationship between regular differential chains and characteristic sets. It can be found in (Hubert, 2003b, cor. 5.3).

Proposition 3.2. *If C is a regular differential chain, then it has the same rank as any characteristic set of $\mathfrak{A}$.*

Proof. The initials of C do not belong to $(C) : I_C^\infty$. By (Aubry et al., 1999, thm 6.1), they are not reduced to zero by C so that C can be transformed into an autoreduced set, without changing its rank. We can thus assume that C is autoreduced.[1] Since C is squarefree, the separants of C are regular modulo $(C) : I_C^\infty$, and this ideal is equal to $(C) : H_C^\infty$. Thus, by (Aubry et al., 1999, thm 6.1), the set C is a characteristic set (in the non-differential sense) of $(C) : H_C^\infty$ whence, by (Hubert, 2000, lem. 6.1), it is a characteristic set (in the differential sense) of $\mathfrak{A}$. □

4. Inverses

Let C be a regular differential chain of R, defining a differential ideal $\mathfrak{A}$, let $L = \mathrm{ld}\, C$ and $N = \Theta U \setminus \Theta L$.

Definition 4.1. *Let f be a nonzero differential polynomial of R. An* inverse *of f is any fraction p/q of nonzero differential polynomials such that $p \in K[N \cup L]$ and $q \in K[N]$ and $f\,p \equiv q \mod \mathfrak{A}$.*

Roughly speaking, an inverse p/q is a rational fraction equivalent to $1/f$ modulo $\mathfrak{A}$. This statement only makes sense if the denominators q and f are regular modulo $\mathfrak{A}$. This is clear for q, since this polynomial is a nonzero element of $K[N]$, and every nonzero element of $K[N]$ is regular modulo $\mathfrak{A}$, by (Boulier et al., 2006, thm 1.6) and (Boulier et al., 2009, cor. 4 to thm. 3). This is true also for f, whenever an inverse of f exists, Proposition 4.3 shows. Before proving it, one needs the following Lemma, which is a corollary to (Hubert, 2003a, prop. 5.18 and prop. 7.6).

Lemma 4.2. *In the ring $K(N)[L]$, the ideals (C) and $(C) : H_C^\infty$ are equal.*

Proof. Denote $C = \{c_1, \ldots, c_t\}$. Assume $\mathrm{ld}\, c_1 < \cdots < \mathrm{ld}\, c_t$. For each $1 \leq k < t$, denote $C_k = \{c_1, \ldots, c_k\}$. The set C is a regular chain, in the non differential sense. Thus the initial i_k of c_k is regular modulo the ideal $(C_{k-1}) : I_{C_{k-1}}^\infty$ for each $2 \leq k \leq t$. Thus, by (Boulier et al., 2006, cor. 3.2), in the ring $K(N)[L]$, the initial i_k of c_k is invertible modulo the ideal $(C_{k-1}) : I_{C_{k-1}}^\infty$, for each $2 \leq k \leq t$. Let us now place ourselves in $K(N)[L]$. The initial of c_1 lies in $K(N)$ and is invertible. Thus $(C_1) = (C_1) : I_{C_1}^\infty$. Assume that, for some $1 < k \leq t$ one has $(C_{k-1}) = (C_{k-1}) : I_{C_{k-1}}^\infty$. Then i_k is invertible modulo (C_{k-1}) and $(C_k) : I_{C_k}^\infty = (C_k)$. Putting the above argument in an inductive proof, the Lemma is established. □

Proposition 4.3. *The differential polynomial f is regular modulo $\mathfrak{A}$ if and only if f admits an inverse.*

Proof. By (Boulier et al., 2009, cor. 4 to thm. 3), a differential polynomial is regular modulo $\mathfrak{A} = [C] : H_C^\infty$ if and only if its partial remainder with respect to C is regular modulo $(C) : H_C^\infty$. One may thus assume that f is partially reduced with respect to C. This implies that $f \in K[N \cup L]$.

The implication from left to right. One assumes f is regular modulo $(C) : H_C^\infty$. Then f is nonzero. If $f \in K$ then f is regular and admits an inverse. Assume $f \notin K$. By (Boulier et al., 2006, thm. 1.1 and cor. 1.15), it is invertible modulo $(C) : H_C^\infty$ in the ring $K(N)[L]$. In this ring, (C) and $(C) : H_C^\infty$ are the same ideal, by Lemma 4.2 whence there exists a polynomial r such that $r\,f - 1 \in (C)$. Multiplying by some suitable nonzero polynomial $q \in K[N]$ in order to clear denominators and denoting $p = r\,q$, one gets a relation $p\,f - q \in (C)$ in $K[N \cup L]$ hence an inverse of f.

[1] (Aubry et al., 1999, thm 6.1) write that Ritt does not require his characteristic sets to be autoreduced. This is a (minor) mistake, which explains why our proof starts with an autoreduction step.

The implication from right to left. Assume f is not regular modulo $(C) : H_C^\infty$. For each differential polynomial p, the product $f\,p$ is not regular[2] modulo $(C) : H_C^\infty$ and cannot be equivalent to a regular differential polynomial. By (Boulier et al., 2006, thm 1.6), every nonzero $q \in K[N]$ is regular modulo $(C) : H_C^\infty$. Thus f has no inverse. □

```
function Inverse($f$, $C$)
Parameters
  $f$ is a differential polynomial
  $C$ is a regular differential chain
Result
  an inverse of $f$ or an error
Comment
  the code uses the AlgebraicInverse function (Appendix A)
begin
  let $r$ be the partial remainder of $f$ with respect to $C$
  let $h$ be the product of separants of $C$ such that $h\,f \equiv r \mod \mathfrak{A}$
The try-catch statement is only given to emphasize the fact that
the function call may raise exceptions (see Appendix A)
  try
    $p/q$ := AlgebraicInverse($r$, $C$)
  catch:
    error
  end try
  return $h\,p/q$
end
```

FIGURE 1. The Inverse function

Proposition 4.4. *Assume the* Inverse *function of Figure* 1 *returns a fraction $h\,p/q$. Then, this fraction is an inverse of f. Moreover, either $f \in K$ and $h\,p/q = 1/f \in K$, or $f \notin K$, and the leading derivative of $h\,p$ is lower than or equal to that of f.*

Proof. One first proves that $h\,p/q$ is an inverse of f. After the partial reduction, one has $h\,f \equiv r$ modulo $\mathfrak{A}$. Thus, using the fact that $h \in K[N \cup L]$, if p/q is an inverse of r, then $h\,p/q$ is an inverse of f. One thus just needs to assume that the call to AlgebraicInverse succeeds and to prove that p/q is an inverse of r. The rational fraction p/q is the inverse of r modulo (C) in $K(N)[L]$ (Boulier et al., 2006, page 89). One has $p \in K[N \cup L]$ and $q \in K[N]$ and a relation $r\,p - q \in (C)$, in $K(N)[L]$. Multiplying by a suitable polynomial b in $K[N]$, one gets $b\,(r\,p - q) \in (C) \subset (C) : H_C^\infty$ in the ring $K[N \cup L]$. By (Boulier et al., 2006, thm 1.6), the differential polynomial b is regular modulo $(C) : H_C^\infty$. Thus $r\,p - q \in (C) : H_C^\infty$ and p/q is an inverse of r.

One now proves the second claim of the Proposition. The case $f \in K$ is clear. Assume $f \notin K$ and denote $v = \operatorname{ld} f$. The separants which occur in h as factors are the ones of the elements of C actually involved in the reduction process. They have leading derivatives less than or equal to v. The elements of C involved in the computation of the algebraic inverse of r have leading derivatives less than or equal to v (Boulier et al., 2006, page 89). Thus the second claim of the Proposition is proven. □

[2] In a Nötherian ring R, an element b is regular modulo an ideal $\mathfrak{B}$ if and only if it belongs to none of the associated prime ideals of $\mathfrak{B}$. We use this well-know result (Zariski and Samuel, 1958, chap. IV, cor. 3 to thm. 11) with respect to the ideal $(C) : H_C^\infty$ in the ring $K[N \cup L]$. The fact that $N \cup L$ may be infinite does not raise any theoretical difficulty since we may always restrict this set to the finite set of indeterminates which actually occur in C.

The $\mathrm{Inverse}$ function may raise an error, either because f is zero modulo $\mathfrak{A}$, or, because a zero divisor modulo $\mathfrak{A}$ (thereby a factorization of some element of C) is exhibited. In the second case, the exhibited zero divisor may be either f or some differential polynomial arising in some intermediate computation. For that reason, it may happen that the $\mathrm{Inverse}$ function fails to compute an inverse of a differential polynomial f, even if it is regular modulo $\mathfrak{A}$. These issues are detailed in Appendix A.

In the next section, it is assumed that inverses of the initials and separants of C can be computed. The initials and separants are regular modulo $\mathfrak{A}$ so that they admit inverses. However, as stated above, the $\mathrm{Inverse}$ function may fail to compute them. In that case, a factorization of some element of C is exhibited and the chain C can be decomposed into two regular differential chains. We thus assume that such further decompositions are already performed. This assumption definitely makes sense since, close variants of the functions of Appendix A, which may raise the exceptions, were probably applied to the initials and separants of C, in order to check conditions **b** and **c** of Definition 3.1.

5. The normal form algorithm

Definition 5.1. *Let a/b be a rational differential fraction, with b regular modulo $\mathfrak{A}$. A* normal form *of a/b modulo C is any rational differential fraction f/g such that*

1. *f is reduced with respect to C ;*

2. *g belongs to $K[N]$ (and is thus regular modulo $\mathfrak{A}$),*

3. *a/b and f/g are equivalent modulo $\mathfrak{A}$.*

Proposition 5.2. *Let a/b be a rational differential fraction, with b regular modulo $\mathfrak{A}$. The normal form f/g of a/b exists and is unique. In particular,*

4. *a belongs to $\mathfrak{A}$ if and only if its normal form is zero ;*

5. *f/g is a canonical representative of the residue class of a/b in the total fraction ring of $R/\mathfrak{A}$.*

Moreover,

6. *each irreducible factor of g divides the denominator of an inverse of b, or of some initial or separant of C.*

Proof. One first proves the uniqueness of the normal form. Assume f'/g' is another normal form of a/b. Then, by **3**, f/g and f'/g' are equivalent modulo $\mathfrak{A}$, which implies that $f\,g' - f'\,g \in \mathfrak{A}$. By **1** and **2**, $f\,g' - f'\,g$ is reduced with respect to C. According to Proposition 3.2, C has the same rank as any characteristic set of $\mathfrak{A}$. Thus $f\,g' - f'\,g$ must be zero and the two fractions are equal.

One now proves the existence of the normal form. For this, consider the NF function of Figure 2 and replace the instruction "$p_{\mathrm{b}}/q_{\mathrm{b}}$:= Inverse(b, C)" by the statement "let $p_{\mathrm{b}}/q_{\mathrm{b}}$ be an inverse of b". Using Proposition 4.3 and the fact that b is assumed to be regular modulo $\mathfrak{A}$, one gets a "theoretical" version of the NF function which necessarily returns a fraction. It is thus sufficient to prove that this fraction satisfies **1**, **2** and **3**.

1. The differential polynomial r_{t+1} is a partial remainder. It is thus partially reduced with respect to C. By Definition 4.1, the differential polynomials $p_1, \ldots, p_t$ lie in $K[N \cup L]$ i.e. are partially reduced w.r.t. C. Thus f_{t+1} is partially reduced w.r.t. C. Let now $t \geq \ell \geq 1$ be a loop index. Assume $f_{\ell+1}$ is partially reduced w.r.t. C and $\deg(f_{\ell+1},\, v_k) < \deg(c_k,\, v_k)$ for each $t \geq k > \ell$. Consider the sequence of instructions of the loop body. By the specifications of the pseudoremainder algorithm, $\deg(r_\ell,\, v_\ell) < \deg(c_\ell,\, v_\ell)$. Using Proposition 4.4 and the fact that $\deg(i_\ell,\, v_\ell) = 0$, one sees that $\deg(p_\ell,\, v_\ell) = 0$. Thus f_ℓ is partially reduced w.r.t. C and, using the fact that c_ℓ does not depend on $v_{\ell+1}, \ldots, v_t$, one has $\deg(f_\ell,\, v_k) < \deg(c_k,\, v_k)$ for each $t \geq k \geq \ell$. Putting the above argument in an inductive proof, one sees that $f = f_1$ is partially reduced w.r.t. C and $\deg(f_1,\, v_k) < \deg(c_k,\, v_k)$ for each $t \geq k \geq 1$ i.e. that f is reduced w.r.t. C.

```
function $\mathrm{NF}(A,\, C)$
*Parameters*
  *$A$ is a rational differential fraction $a/b$ such that $a,\, b \in R$.*
  *$C$ is a regular differential chain, defining a differential ideal $\mathfrak{A}$.*
*Result*
  *the normal form of $A$ modulo $\mathfrak{A}$ or an error.*
*Assumptions*
  *Inverses of the initials and separants of $C$ are (pre-)computed.*
begin
*The try-catch statement is only given to emphasize the fact that*
*the function call may raise an error*
  try
    $p_{\mathrm{b}}/q_{\mathrm{b}} := \mathrm{Inverse}(b,\, C)$
  catch
    error
  end try
  $(f_{t+2},\, g_{t+2}) := (p_{\mathrm{b}}\, a,\, q_{\mathrm{b}})$
  $p_i/q_i := \mathrm{Inverse}(s_i,\, C)$ for each separant $s_i$ of $C = \{c_1, \ldots, c_t\}$
  using Ritt's partial reduction algorithm, compute $d_1, \ldots, d_t \in \mathbb{N}$ and
                    $r_{t+1} \in K[N \cup L]$ such that $s_1^{d_1} \cdots s_t^{d_t}\, f_{t+2} \equiv r_{t+1} \mod \mathfrak{A}$
  $f_{t+1} := p_1^{d_1} \cdots p_t^{d_t}\, r_{t+1}$
  $g_{t+1} := q_1^{d_1} \cdots q_t^{d_t}\, g_{t+2}$
  denote $v_i = \mathrm{ld}\, c_i$ $(1 \leq i \leq t)$ and assume $v_t > \cdots > v_1$
  for $\ell$ from $t$ to $1$ by $-1$ do
    $r_\ell := \mathrm{prem}(f_{\ell+1},\, c_\ell,\, v_\ell)$
    let $i_\ell$ denote the initial of $c_\ell$
    let $d_\ell \in \mathbb{N}$ be such that $i_\ell^{d_\ell}\, f_{\ell+1} \equiv r_\ell \mod (c_\ell)$
    $p_\ell/q_\ell := \mathrm{Inverse}(i_\ell,\, C)$
    $f_\ell := p_\ell^{d_\ell}\, r_\ell$
    $g_\ell := q_\ell^{d_\ell}\, g_{\ell+1}$
  end do
  return $f_1/g_1$
*the rational fraction may be reduced by means of a gcd computation*
*of multivariate polynomials over the field $K$*
end
```

FIGURE 2. The NF function

2. One actually proves **6**, which implies **2**. All the differential polynomials g_i are products of denominators of inverses of b and of the initials and separants of C. They belong to $K[N]$ by Proposition 4.3. The final reduction may simply remove some factors of g_1.

3. At the beginning of the function, a/b and f_{t+2}/g_{t+2} are equivalent modulo $\mathfrak{A}$. After the partial reduction step,

$$\frac{a}{b} \equiv \frac{f_{t+2}\, s_1^{d_1} \cdots s_t^{d_t}\, p_1^{d_1} \cdots p_t^{d_t}}{g_{t+2}\, s_1^{d_1} \cdots s_t^{d_t}\, p_1^{d_1} \cdots p_t^{d_t}} \mod \mathfrak{A}.$$

Simplify $s_1^{d_1} \cdots s_t^{d_t}\, f_{t+2}$ as r_{t+1} and each product $s_i\, p_i$ as q_i. One sees that a/b is equivalent to f_{t+1}/g_{t+1} modulo $\mathfrak{A}$. Let now $t \geq \ell \geq 1$ be a loop index, consider the sequence of instructions of the loop body and assume that a/b is equivalent to $f_{\ell+1}/g_{\ell+1}$ modulo $\mathfrak{A}$. After the pseudodivision step,

$$\frac{a}{b} \equiv \frac{f_{\ell+1}\, \imath_\ell^{d_\ell}\, p_\ell^{d_\ell}}{g_{\ell+1}\, \imath_\ell^{d_\ell}\, p_\ell^{d_\ell}} \mod \mathfrak{A}.$$

Simplify $\imath_\ell^{d_\ell}\, f_{\ell+1}$ as r_ℓ and each product $i_\ell\, p_\ell$ as q_ℓ. One sees that a/b is equivalent to f_ℓ/g_ℓ. Putting the above argument in an inductive proof, **3** is proved.

This concludes the proof of the existence of the normal form. One proceeds with the three last points.

4. It follows from the uniqueness, **3** and the fact that 0 is a normal form.

5. It follows from **3** and the uniqueness of normal forms.

6. It was proved in **2**, above. □

Proposition 5.3. *Let a/b be a rational differential fraction. If* $\mathrm{NF}(a/b,\, C)$ *returns a rational differential fraction, then this fraction is the normal form of a/b.*

Proof. The proof is given by the existence proof of Proposition 5.2, assuming that the initial call to the $\mathrm{Inverse}$ function succeeds. □

Example 1. *Take $C = \{u_x^2 - 4\,u\}$ and $A = u_{xx}$. The sequence of pairs computed by the* NF *function is $(f_3,\, g_3) = (u_{xx},\, 1)$, $(f_2,\, g_2) = (4\,u_x^2,\, 8\,u)$ and $(f_1,\, g_1) = (16\,u,\, 8\,u)$. The normal form of A is $16\,u/(8\,u) = 2$. This basic example shows that the gcd computation at the end of the* NF *function may be necessary for obtaining a reduced fraction.*

The next proposition is clear but deserves to be stated.

Proposition 5.4. *The* NF *function always succeeds when applied to a differential polynomial.*

The next proposition is one of the results of this paper. Observe that items **(ii)** and **(iii)** could not be stated with the restricted algorithm given by Boulier and Lemaire (2000), which only applies to differential polynomials.

Proposition 5.5. *Let a/b and a'/b' be two rational differential fractions with b and b' regular modulo $\mathfrak{A}$. Denote f/g and f'/g' their normal forms. Then*

(i). $\mathrm{NF}\left(\frac{a}{b} + \frac{a'}{b'}\,,\, C\right) = \frac{f}{g} + \frac{f'}{g'}$,

(ii). $\mathrm{NF}\left(\frac{a}{b} \cdot \frac{a'}{b'}\,,\, C\right) = \mathrm{NF}\left(\frac{f}{g} \cdot \frac{f'}{g'}\,,\, C\right)$,

(iii). $\mathrm{NF}\left(\theta\left(\frac{a}{b}\right),\, C\right) = \mathrm{NF}\left(\theta\left(\frac{f}{g}\right),\, C\right)$ *for each derivation operator θ. Moreover, each irreducible factor of the denominator of this rational differential fraction divides the denominator of an inverse of b, or of some initial or separant of C.*

Proof. **(i)**. The rational differential fraction on the right-hand side writes $(f\,g' + f'\,g)/(g\,g')$. By Definition 5.1, **1** and **2**, applied separately on f/g and f'/g', the numerator $f\,g' + f'\,g$ is reduced with respect to C and the denominator $g\,g'$ belongs to $K[N]$. This fraction thus satisfies Definition 5.1, **1** and **2**. It also satisfies **3**. It is thus a normal form. Equality follows from the uniqueness.

(ii). It follows from Definition 5.1, **3** and the uniqueness property of normal forms.

(iii). The first statement follows from Definition 5.1, **3** and the uniqueness property of normal forms. The second statement follows from Proposition 5.2, **6**. □

Proposition 5.6. *Let a/b be a rational differential fraction. If the normal form of a/b exists, then the normal form of $\theta\,(a/b)$ exists for any derivation operator θ.*

Proof. Let f/g be the normal form of a/b. It is sufficient to consider the case $\operatorname{ord}\theta = 1$. By Proposition 5.5, **(iii)**, the normal form of $\theta\,(a/b)$ is equal to the normal form of $((\theta f)\,g - f\,(\theta g))/g^2$. Using Definition 5.1, **2**, and the fact that g belongs to $K[N]$, this rational fraction is equal to $\mathrm{NF}((\theta f)\,g - f\,(\theta g))/g^2$, which exists by Proposition 5.4. □

6. Power series solutions of regular differential chains

Let C be a regular differential chain of R, defining a differential ideal $\mathfrak{A}$, let $L = \operatorname{ld} C$ and $N = \Theta U \setminus \Theta L$.

6.1. Purely algebraic solutions

Definition 6.1. *Let G_0 be a field extension of K. A map $\phi : \Theta U \to G_0$, which extends to a ring homomorphism $K[\Theta U] \to G_0$, is a* purely algebraic solution *of $\mathfrak{A}$ if ϕ annihilates all the elements of $\mathfrak{A}$.*

Informally speaking, a purely algebraic solution of a differential ideal $\mathfrak{A}$ is obtained by viewing $\mathfrak{A}$ as a non-differential ideal of the ring $K[\Theta U]$ and determining a solution of it. The difficulty, which comes from the fact that the set of unknowns is infinite, is overcome by means of the normal form algorithm. Under technical conditions, the map ϕ can be uniquely defined by fixing its value on the elements on $N \cup L$ only, as shown by the next two propositions.

Proposition 6.2. *Any map ϕ built as follows provides a purely algebraic solution of $\mathfrak{A}$.*

1. *for all $v \in N \cup L$, assign to $\phi(v)$, values, taken in some field extension G_0 of K, which annihilate the elements of C but does not annihilate their initials and separants,*
2. *for all $v \in \Theta L \setminus L$, assign then to $\phi(v)$ the value of $\phi(r)/\phi(h)$ where r is the remainder of Ritt's full reduction of v by C, and h satisfies $h\,v = r \mod \mathfrak{A}$.*

Proof. A proof can be found in (Boulier et al., 2009, Sect. 7). This result is implicitly given by Seidenberg (1956, 1958, 1969) who refers to Ritt (1950). □

The assumption that the initials and the separants must not cancel is needed to avoid $\phi(h)$ to be equal to 0 in the division $\phi(r)/\phi(h)$. The normal form algorithm provides another method for computing a purely algebraic solution of $\mathfrak{A}$.

Proposition 6.3. *Any map ϕ built as follows provides a purely algebraic solution of $\mathfrak{A}$.*

1. *for all $v \in N \cup L$, assign to $\phi(v)$, values, taken in some field extension G_0 of K, which annihilate the elements of C but does not annihilate the denominators of the inverses of the initials and separants of C,*
2. *for all $v \in \Theta L \setminus L$, assign then to $\phi(v)$ the value of $\phi(p)/\phi(q)$ where p/q is the normal form of v.*

Proof. Recall that the function NF is applied to differential polynomials and not to rational differential fractions.

The map ϕ is well-defined. Since C is a squarefree regular chain, the ideal $(C):H_C^\infty$ of the ring $K[N \cup L]$ is not trivial and there exists a prime ideal $\mathfrak{p}$ which contains C and does not contain any element of H_C. The field G_0 may thus be chosen to be the field of fractions of $K[N \cup L]/\mathfrak{p}$. Since the map ϕ does not annihilate the denominators of the inverses of the initials and separants of C, it does not annihilate any denominator of any element of $\mathrm{NF}(\Theta U,\, C)$ by item **6** of Proposition 5.2. The map ϕ is thus well-defined.

The map ϕ provides a purely algebraic solution of $\mathfrak{A}$. It is sufficient to prove that, for any $p \in R$ one has $\phi(p - \mathrm{NF}(p,\, C)) = 0$ since, in the case $p \in \mathfrak{A}$, one has $\mathrm{NF}(p,\, C) = 0$ by item **4** of

Proposition 5.2 whence $\phi(p) = 0$. Now, $\phi(v - \mathrm{NF}(v, C)) = 0$ for all $v \in \Theta U$. It is thus sufficient to prove that, for all $p, p' \in R$, if $\phi(p - \mathrm{NF}(p, C)) = 0$ and $\phi(p' - \mathrm{NF}(p', C)) = 0$ then $\phi(p + p' - \mathrm{NF}(p + p', C)) = 0$ and $\phi(p\,p' - \mathrm{NF}(p\,p', C)) = 0$. The case of the sum is clear by item **1** of Proposition 5.5. Let us prove that $\phi(p\,p' - \mathrm{NF}(p\,p', C)) = 0$. One has $\mathrm{NF}(p\,p', C) \equiv \mathrm{NF}(p, C)\ \mathrm{NF}(p', C) \mod \mathfrak{A}$ by item **2** of Proposition 5.5. Since normal forms are partially reduced w.r.t. C, the computation of $\mathrm{NF}(p\,p', C)$ from the product $\mathrm{NF}(p, C)\ \mathrm{NF}(p', C)$ does not imply any differentiation of elements of C. Thus, the congruence $\mathrm{NF}(p\,p', C) \equiv \mathrm{NF}(p, C)\ \mathrm{NF}(p', C) \mod (C) : I_C^\infty$ holds. Since ϕ cancels the elements of C and does not annihilate their initials, one has the relation $\phi(\mathrm{NF}(p\,p', C)) = \phi(\mathrm{NF}(p, C))\,\phi(\mathrm{NF}(p', C))$ hence $\phi(p\,p' - \mathrm{NF}(p\,p', C)) = 0$. □

Although Propositions 6.2 and 6.3 seem similar, it appears that Proposition 6.3 is slightly more restrictive in the following sense: any set of values for $L \cup N$ satisfying Proposition 6.3 also satisfies Proposition 6.2 but the converse is not true[3].

Indeed, consider an inverse p/q of some initial or separant h of C. Then $p\,h = q \mod \mathfrak{A}$. If $\phi(q) \neq 0$, then necessarily $\phi(h) \neq 0$. However, one might have $\phi(h) \neq 0$ and at the same time $\phi(p) = \phi(q) = 0$, as the following (algebraic) example shows.

Example 2. *Take $C = \{(v - w)\,u - z = 0,\ v^2 - 1 = 0\}$, a single derivation δ_x and a ranking s.t. $u > v > w > z$. Then $L = \{u, v\}$ and $N \cup L = \{u, v, w_{x^i}, z_{x^i} \mid i \geq 0\}$.*

Taking $\phi(u) = 0$, $\phi(v) = -1$, $\phi(w) = 1$, $\phi(z) = 0$ and $\phi(w_{x^i}) = \phi(z_{x^i}) = 0$ for any $i \geq 1$, satisfies the hypotheses of Proposition 6.2 *since $v - w$ is the only non trivial initial and separant, and $\phi(v - w) = \phi(v) - \phi(w) = -1 - 1 = -2$.*

However, an inverse of $v - w$ is $(v + w)/(1 - w^2)$ and $\phi(1 - w^2) = 0$, so that the set of values for ϕ does not satisfy the conditions of Proposition 6.3.

A similar example also shows that the same problem can occur with a separant.

Example 3. *Take $C = \{u^2 + (v - w)\,u = 0,\ v^2 - 1 = 0\}$, a single derivation δ_x and fix a ranking such that $u > v > w$. Then $L = \{u, v\}$ and $N \cup L = \{u, v, w_{x^i} \mid i \geq 0\}$.*

Taking $\phi(u) = 0$, $\phi(v) = -1$, $\phi(w) = 1$ and $\phi(w_{x^i}) = 0$ for any $i \geq 1$, satisfies the hypotheses of Proposition 6.2 *since the separants $2\,u + v - w$ and $2\,v$ satisfy $\phi(2\,u + v - w) = 0 - 1 - 1 = -2$ and $\phi(2\,v) = -2$.*

However, an inverse of the separant $2\,u+v-w$ has the irreducible form $p/((w-1)^2(w+1)^2)$, where p is some polynomial. Since $\phi((w-1)^2(w+1)^2) = 0$, the set of values for ϕ does not satisfy the conditions of Proposition 6.3.

6.2. Formal power series solutions

This section is dedicated to the construction of formal power series solutions of systems of polynomial differential equations. It is the first half of the way leading to analytic solutions. Reference texts for this section are Seidenberg (1958, 1969). See also (Rust et al., 1999; Hubert and Le Roux, 2003). The m derivations $\delta_1, \ldots, \delta_m$ are interpreted as m partial derivations w.r.t. m independent variables $x_1, \ldots, x_m$. If $\theta = \delta_1^{a_1} \cdots \delta_m^{a_m}$ is a derivation operator, one denotes $x^\theta = x_1^{a_1} \cdots x_m^{a_m}$ and $\theta! = a_1! \cdots a_m!$. One looks for *formal power series solutions* of $\mathfrak{A}$ i.e. solutions of the form:

$$\overline{u}_j = \sum c_{j,\theta} \frac{x^\theta}{\theta!}.$$

The coefficients $c_{j,\theta}$ belong to some field extension G_0 of K which depends on the considered system Σ or, more simply, in the field $\mathbb{C}$. First remark: the above formal power series is centered on the origin for simplicity but the arguments hold for formal power series centered on any element of $\mathbb{R}^m$. Second remark: the above setting covers also the case of differential systems with coefficients in the field $\mathbb{Q}(x_1, \ldots, x_m)$. Indeed, it is then sufficient to encode each independent variable x_i as a

[3] Contrarily to what is stated in a preprint version (Boulier and Lemaire, 2007, Sect. 6, Lemma 3) of this paper.

new differential indeterminate z_i and to append to the system under study, the equations $\delta_j\, z_i = 1$ if $i = j$ and 0 otherwise. One thus assumes, without loss of generality, that K is a field of constants.

Proposition 6.4. *Let G_0 be a field extension of K and $\phi : \Theta U \to G_0$ be a map, extending to a ring homomorphism $K[\Theta U] \to G_0$. Then ϕ is a purely algebraic solution of $\mathfrak{A}$ if and only if the n–tuple $\overline{u} = (\overline{u}_1, \ldots, \overline{u}_n)$ is a formal power series solution of $\mathfrak{A}$ where*

$$\overline{u}_j = \sum_{\theta \in \Theta} \phi(\theta u_j)\, \frac{x^\theta}{\theta!}, \quad 1 \leq j \leq n.$$

Moreover, for each differential polynomial $p \in R$, if $\phi(p) \neq 0$ then $p(\overline{u}) \neq 0$.

Proof. See (Seidenberg, 1958, Lemma). If $p \in R$ is a differential polynomial then one has $p(\overline{u}) = \sum \phi(\theta p)\, x^\theta/\theta!$. Therefore $p(\overline{u})$ is zero if and only if $\phi(\theta p)$ is zero for all $\theta \in \Theta$. Thus ϕ is a purely algebraic solution of $\mathfrak{A}$ if and only if $\overline{u}$ is a formal power series solution of $\mathfrak{A}$. The last part of the Proposition is clear. □

6.3. Analytic solutions

In the rest of this section, the differential ideal $\mathfrak{A}$ is assumed to be prime, for simplicity. The results however hold for non-prime ideals also, by considering any of their prime components.

The fact that every prime differential ideal admits an analytic solution is proven in Proposition 6.6. This result is known since the work of Riquier (1910). Riquier's Theorem, which is a generalization of the Cauchy-Kovalevska Theorem, is the basis of (Ritt, 1950, chap. VIII) and of the Embedding Theorem of Seidenberg (1958, 1969). Péladan-Germa (1997) clarified the relationship between characteristic sets and the hypotheses of Riquier's Theorem. More recently, Lemaire (2002a) completely proved this latter anew, by using a more modern formalism and by distinctly separating the proof of the existence of formal power series solutions and the analyticity proof. The key result is:

Proposition 6.5. *Assume the ranking is both Riquier and orderly. Let $(\overline{u}_1, \ldots, \overline{u}_n)$ be a formal power series solution of $\mathfrak{A}$, the coefficients $c_{j,\theta}$ lying in the field of the complex numbers. Let $(\tilde{u}_1, \ldots, \tilde{u}_n)$ be the restriction to N of the solution i.e:*

$$\tilde{u}_j = \sum_{\theta \in \Theta} \tilde{c}_{j,\theta} \frac{x^\theta}{\theta!}, \quad 1 \leq j \leq n$$

defined by $\tilde{c}_{j,\theta} = c_{j,\theta}$ if $\theta u_j \in N$ else zero. In the neighborhood of the origin, the series $\tilde{u}_j$ are analytic if and only if the series $\overline{u}_j$ are analytic.

Proof. See (Lemaire, 2002a, thm, page 50) or Lemaire (2002b). □

Proposition 6.6. *The differential ideal $\mathfrak{A}$ admits an analytic solution.*

Proof. The differential ideal $\mathfrak{A}$ is presented by the chain C. A purely algebraic solution of $\mathfrak{A}$ can be computed, thanks to Proposition 6.2, by solving, in $K[L \cup N]$, the non-differential polynomial system $C = 0,\ h \neq 0$ where h denotes the product of the initials and separants of C. Among all these solutions, choose one such that *only finitely many* nonzero values are assigned to the elements of $L \cup N$ (there is no theoretical difficulty since there are only finitely many derivatives occuring in C). The restrictions to N of these formal power series are analytic since they are polynomials. According to Proposition 6.5, the formal power series are analytic whence $\mathfrak{A}$ admits an analytic solution. □

7. Examples

The example features a PDE system (two dependent variables $u(x, y)$ and $v(x, y)$). All its solutions turn out to be polynomials.

```
> syst := [diff(u(x,y),x)^2-4*u(x,y),
           diff(diff(u(x,y),x),y)*diff(v(x,y),y)-u(x,y)+1,
           diff(diff(v(x,y),x),x)-diff(u(x,y),x)];

                                    /   2          \
         /d         \2              | d           | /d          \
syst := [|-- u(x, y)|  - 4 u(x, y), |----- u(x, y)| |-- v(x, y)| - u(x, y) + 1,
         \dx        /               \dy dx        / \dy         /

    / 2         \
    |d          |   /d         \
    |--- v(x, y)| - |-- u(x, y)|]
    |  2        |   \dx        /
    \dx         /
```

The radical differential ideal that it generates can be represented by a single regular differential chain. Computations are performed with the new *DifferentialAlgebra* MAPLE package.

```
> with (DifferentialAlgebra):
> R := DifferentialRing (derivations = [x,y], blocks = [[v,u]]);
> ideal := RosenfeldGroebner (syst, R);

                     ideal := [regular_differential_chain]

> ideal := ideal[1]:
```

Here are the differential polynomial which form the regular differential chain, denoted using the "jet" notation.

```
> Equations (ideal, ’solved’, notation=jet);

                             -u[x] u[y] u + u[x] u[y]      2
[v[x, x] = u[x], v[y] = -1/4 ------------------------, u[x]  = 4 u,
                                        u


        2
    u[y]  = 2 u]
```

Here is an example of a normal form computation, showing that normal forms commute with products.

```
> A := u[x]^3:
> NFA := NormalForm (A, ideal);
                                NFA := 4 u[x] u

> NF_1_A := NormalForm (1/A, ideal);
                                             u[x]
                              NF_1_A := 1/16 ----
                                               2
                                              u
> NormalForm (NFA * NF_1_A, ideal);
                                       1
```

The following computations show that normal forms commute with derivations.

```
> NF1 := NormalForm (Tools:-Differentiate (A, y, R), ideal);

                              NF1 := 6 u[x] u[y]
```

```
> DNF2 := Tools:-Differentiate (NFA, y, R);

                       DNF2 := 4 u[x, y] u + 4 u[x] u[y]

> NF3 := NormalForm (DNF2, ideal);

                              NF3 := 6 u[x] u[y]
```

The following computations apply the method sketched in this paper, for computing the beginning of a formal power series for $u(x,y)$. It turns out that this truncated series is actually a solution.

```
> serie :=         NormalForm(u,ideal) +
           x   *   NormalForm(u[x],ideal) +
           y   *   NormalForm(u[y],ideal) +
           x^2/2 * NormalForm(u[x,x],ideal) +
           x*y  *  NormalForm(u[x,y],ideal) +
           y^2/2 * NormalForm(u[y,y],ideal);
                                                                   2
                                         2        x y u[x] u[y]     y
         serie := u + x u[x] + y u[y] + x  + 1/2 ------------- + ----
                                                       u           2

> serie_at_0 := subs (u[x]=2*sqrt(u0), u[y]=sqrt(2*u0), u=u0, serie);

                                                     2
                          1/2   1/2          1/2      y      1/2         2
      serie_at_0 := u0 + 2    u0    y + 2 u0    x + ---- + 2    x y + x
                                                     2

> eqns := Equations (ideal, leader=derivative(u));

                 /d         \2              /d         \2
        eqns := [|-- u(x, y)|  - 4 u(x, y), |-- u(x, y)|  - 2 u(x, y)]
                 \dx        /               \dy        /

> simplify (eval (eqns, u(x,y)=serie_at_0));

                                    [0, 0]
```

Appendix A. Computation of the Algebraic Inverse

This section aims at providing the $\mathrm{AlgebraicInverse}$ function of Figure 3, which is called by the $\mathrm{Inverse}$ function. Though purely algebraic, it is stated for differential polynomials. This function first tests if the differential polynomial f, for which an inverse is sought, is zero modulo the ideal defined by the chain C. If it is zero, then the exception “inversion of zero” is raised. If it is nonzero, it performs an inverse computation in the polynomial ring $G[x_1,\ldots,x_n]$ where the x_i are the leading derivatives of the elements of C and G is the field obtained by adjoining all the other derivatives to the field of coefficients K. The inverse computation in $G[x_1,\ldots,x_n]$ is performed by the two functions $\mathrm{AlgebraicInverseNonZero}$ and $\mathrm{ExtendedEuclideanAlgorithm}$, whose principle is known since Della Dora et al. (1985); Moreno Maza and Rioboo (1995). These two functions call recursively each other. They try to compute algebraic inverses of a polynomial modulo a zero-dimensional ideal, by means of the Euclidean algorithm. They can only fail if some relationship

$$\mathbf{u}_1\,f+\mathbf{u}_2\,c_k=\mathbf{u}_3 \mod (C)$$

is exhibited, where f is the polynomial whose inverse is being computed, $\mathbf{u}_3$ is a common divisor of f and the element c_k of C in the ring $G[x_1,\ldots,x_n]/(C)$, and $0<\deg(\mathbf{u}_3,\,x_k)<\deg(c_k,\,x_k)$.

In that case, the exception "inversion of a zero divisor" is raised and the non-trivial factor $\mathbf{u}_3$ of c_k is exhibited.

```
function AlgebraicInverse($f, C$)
Parameters
   $C = \{c_1, \ldots, c_n\}$ is a regular differential chain
   $f$ is a differential polynomial partially reduced w.r.t. $C$
Result
   an inverse of $f$ or one of the two exceptions:
      "inversion of zero"
      "inversion of a zerodivisor"
begin
   Denote $x_k$ the leading derivative of $c_k$ and assume $x_1 < \cdots < x_n$
   Denote $t_1, \ldots, t_m$ the other derivatives occuring in $C$ and $f$
   From now on, perform all computations in the ring $G[x_1, \ldots, x_n]$ where $G = K(t_1, \ldots, t_m)$
   for $k$ from $1$ to $n$ do
      let $i_k$ be the leading coefficient of $c_k$ w.r.t. $x_k$
the next call necessarily succeeds because $C$ is a regular chain, and the inverses of its initials are
assumed to be precomputed
      $\bar{\imath}_k$ := AlgebraicInverseNonZero($i_k, C$)
      $\bar{c}_k$ := rem($\bar{\imath}_k\, c_k,\ \{\bar{c}_1, \ldots, \bar{c}_{k-1}\}$)
   end do
   $\overline{C}$ := $\{\bar{c}_1, \ldots, \bar{c}_n\}$
the regular chain $\overline{C}$ generates the ideal $(C)$ in $G[x_1, \ldots, x_n]$, and involves monic polynomials
   $\overline{f}$ := rem($f,\ \overline{C}$)
   if $\overline{f} = 0$ then
      raise exception "inversion of zero"
   else
      return AlgebraicInverseNonZero($\overline{f},\ \overline{C}$)
   end if
end
```

FIGURE 3. The AlgebraicInverse function

Example 4. *Apply* AlgebraicInverse *to $f = z$ and $C = \{z - y - x,\, y^2 - x^3,\, (x-1)(x+1)(x^2-2)\}$. The computation fails and exhibits the zerodivisor $x - 1$. The exhibited zero divisor permits to split C into two regular chains $C_1 = \{z - y - x,\, y^2 - x^3,\, (x+1)(x^2-2)\}$ and $C_2 = \{z - y - x,\, y^2 - x^3,\, x - 1\}$. The inverse computation of z, restarted over C_1, succeeds and returns $\frac{1}{2}\left((x^2 + x - 1)\, y - x - 2\right)$. The inverse computation of z, restarted over C_2, fails and exhibits the zerodivisor $y + 1$. This zero divisor permits to split C_2 into two regular chains $C_{21} = \{z - y - x,\, y - 1, x - 1\}$ and $C_{22} = \{z - y - x,\, y + 1, x - 1\}$. The inverse computation of z, restarted over C_{21} returns $1/2$. The inverse computation of z, restarted over C_{22}, fails because z is zero modulo C_{22}.*

The above example suggests that it is possible to implement a general normal form function which, when applied to some fraction $A = a/b$ and some regular differential chain C, returns a result in all cases: if no exception is raised, then the result is a normal form else, it is not a normal form but a sequence of two lists:

$$[[\mathrm{NF}_1,\, C_1],\, [\mathrm{NF}_2,\, C_2], \ldots, [\mathrm{NF}_k,\, C_k]], \quad [C_{k+1},\, C_{k+2}, \ldots, C_\ell].$$

```
function AlgebraicInverseNonZero($(f, C)$)
Parameters
  $C = \{c_1, \ldots, c_n\}$ is a regular chain in $G[x_1, \ldots, x_n]$, and only involves monic polynomials
  $f$ is a polynomial in $G[x_1, \ldots, x_n]$, which does not lie in the ideal $(C)$
Result
  an inverse of $f$ in $G[x_1, \ldots, x_n]/(C)$ or the exception “inversion of a zerodivisor”
begin
  if $f \in G$ then
the polynomial $f$, which does not belong to $(C)$, cannot be zero
    return $1/f$
  else
    let $x_k$ be the leading variable of $f$
    $\mathbf{u}$ := ExtendedEuclideanAlgorithm($f$, $c_k$, $x_k$, $C$)
one has $\mathbf{u}_1\, f + \mathbf{u}_2\, c_k = \mathbf{u}_3 \mod (C)$
    if $\mathbf{u}_3 = 1$ then
one has $\mathbf{u}_1\, f = 1 \mod (C)$
      return $\mathbf{u}_1$
    else
the polynomial $\mathbf{u}_3$ divides $c_k$ and is different from $c_k$ since $f$ does not lie in $C$
      raise exception “inversion of a zerodivisor”: $\mathbf{u}_3$
    end if
  end if
end
```

FIGURE 4. The AlgebraicInverseNonZero function

The C_i are regular differential chains, defining differential ideals $\mathfrak{A}_i$ such that

$$\mathfrak{A} = \mathfrak{A}_1 \cap \mathfrak{A}_2 \cap \cdots \cap \mathfrak{A}_\ell .$$

The rational fraction NF_i is the normal form of A in $R/\mathfrak{A}_i$ for $1 \leq i \leq k$. The denominator b of A is zero in $R/\mathfrak{A}_i$ for $k < i \leq \ell$. The fact that purely algebraic splittings of regular differential chains produce regular differential chains can be proven by using (Hubert, 2000, lem. 6.2 and thm. 3.10), as pointed out in (Boulier and Lemaire, 2000, sect. 4.1).

Such a splitting handling function is implemented in the *DifferentialAlgebra* package. Let us illustrate it over the above example:

```
> with (DifferentialAlgebra):
> R := DifferentialRing (derivations = [], blocks = [z,y,x]):
> C := Tools:-PretendRegularDifferentialChain
                ([z-y-x, y^2-x^3, (x-1)*(x+1)*(x^2-2)], R);
                        C := regular_differential_chain

# By default, the NormalForm function does not split cases
> res := NormalForm (1/z, C);
Error, (in DifferentialAlgebra:-NormalForm) regularization of a zero divisor

# A complete function is however implemented
> res := NormalForm (1/z, C, casesplit=true);
                 2
res := [[[1/2 y x  + 1/2 y x - 1/2 y - 1/2 x - 1, regular_differential_chain],

    [1/2, regular_differential_chain]], [regular_differential_chain]]
```

```
function ExtendedEuclideanAlgorithm($f$, $g$, $x_k$, $C$)
Parameters
  $C = \{c_1, \ldots, c_n\}$ is a regular chain in $G[x_1, \ldots, x_n]$ and only involves monic polynomials
  $f$, $g$ are polynomials in $G[x_1, \ldots, x_n]$ ; their leading coeff. w.r.t. $x_k$ do not lie in the ideal $(C)$
Result
  a vector $\mathbf{u} = (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ of polynomials in $G[x_1, \ldots, x_n]$, such that, in $G[x_1, \ldots, x_n]/(C)$,
    the relationship $\mathbf{u}_1\, f + \mathbf{u}_2\, g = \mathbf{u}_3$ holds,
    the polynomial $\mathbf{u}_3$ is a common divisor of $f$ and $g$,
    the leading coefficient of $\mathbf{u}_3$ w.r.t. $x_k$ is $1$
  or the exception "inversion of a zerodivisor"
begin
  $\mathbf{u}$ := $(1,\, 0,\, f)$
  $\mathbf{v}$ := $(0,\, 1,\, g)$
the property $\mathbf{u}_1\, f + \mathbf{u}_2\, g = \mathbf{u}_3 \mod (C)$ is a loop invariant
the set of common divisors of $\mathbf{u}_3$ and $\mathbf{v}_3$ modulo $(C)$ is another loop invariant
  while $\mathbf{v}_3 \neq 0$ do
    let $\imath$ be the leading coefficient of $\mathbf{v}_3$ w.r.t. $x_k$
    $\bar{\imath}$ := AlgebraicInverseNonZero($\imath$, $C$)
compute the remainder componentwise
    $\mathbf{v}$ := rem($\bar{\imath}\, \mathbf{v}$, $C$)
the leading coefficient of $\mathbf{v}_3$ w.r.t. $x_k$ is now $1$
    $q$ := quo($\mathbf{u}_3$, $\mathbf{v}_3$, $x_k$)
    $\mathbf{t}$ := $\mathbf{v}$
    $\mathbf{v}$ := rem($\mathbf{u} - q\, \mathbf{v}$, $\{c_1, \ldots, c_{k-1}\}$)
if $\mathbf{v}_3$ is nonzero then, its leading coefficient w.r.t. $x_k$ does not lie in $(C)$
    $\mathbf{u}$ := $\mathbf{t}$
  end do
the polynomial $\mathbf{u}_3$ is a common divisor of $\mathbf{u}_3$ and $0$, hence a common divisor of $f$ and $g$
  return $\mathbf{u}$
end
```

FIGURE 5. The ExtendedEuclideanAlgorithm function

```
> Equations (res [1,1,2], 'solved');
                           2     2             3     2
              [z = y + x, y  = -x  + 2 x + 2, x  = -x  + 2 x + 2]

> Equations (res [1,2,2], 'solved');
                             [z = 2, y = 1, x = 1]

> Equations (res [2,1], 'solved');
                            [z = 0, y = -1, x = 1]
```

The AlgebraicInverse algorithm may split cases while computing the normal form of a rational fraction a/b, even if b is regular modulo the ideal defined by the regular chain C, since it computes the inverses of many intermediate quantities. In principle, one could avoid these splittings by means of Gröbner bases computations. An expression $\overline{b}$ for the inverse of b can be computed by applying the Buchberger algorithm, over G, on the set $C \cup \{x_{n+1}\, b - 1\}$, where x_{n+1} is some new indeterminate (Rabinowitsch trick). The normal form of a/b is then obtained by computing the normal form of the polynomial $a\, \overline{b}$. This method is useful when one wants to avoid splittings as much as possible. This method is however costly, since it requires one Gröbner basis computation for each normal form computation. Moreover, we believe that the splittings performed by the AlgebraicInverse algorithm are often very interesting, since they correspond to *factorizations* of the equations. They thus should not be avoided.

References

Aubry, P., Lazard, D., Moreno Maza, M., 1999. On the Theories of Triangular Sets. Journal of Symbolic Computation 28, 105–124.

Boulier, F., November 1999. Efficient computation of regular differential systems by change of rankings using Kähler differentials. Tech. rep., Université Lille I, 59655, Villeneuve d'Ascq, France, ref. LIFL 1999–14, presented at the MEGA 2000 conference. `http://hal.archives-ouvertes.fr/hal-00139738`.

Boulier, F., Lazard, D., Ollivier, F., Petitot, M., 2009. Computing representations for radicals of finitely generated differential ideals. Journal of AAECC 20 (1), 73–121, (1997 Techrep. IT306 of the LIFL).

Boulier, F., Lemaire, F., 2000. Computing canonical representatives of regular differential ideals. In: ISSAC'00: Proceedings of the 2000 international symposium on Symbolic and algebraic computation. ACM Press, New York, NY, USA, pp. 38–47, `http://hal.archives-ouvertes.fr/hal-00139177`.

Boulier, F., Lemaire, F., 2007. A computer scientist point of view on Hilbert's differential theorem of zeros. (preprint). `http://hal.archives-ouvertes.fr/hal-00170091`.

Boulier, F., Lemaire, F., Moreno Maza, M., 2006. Well known theorems on triangular systems and the D^5 principle. In: Proceedings of Transgressive Computing 2006. Granada, Spain, pp. 79–91, `http://hal.archives-ouvertes.fr/hal-00137158`.

Buium, A., Cassidy, P., 1998. Differential Algebraic Geometry and Differential Algebraic Groups: From Algebraic Differential Equations To Diophantine Geometry. Amer. Math. Soc., Providence, RI, pp. 567–636.

Della Dora, J., Dicrescenzo, C., Duval, D., 1985. About a new method for computing in algebraic number fields. In: Proceedings of EUROCAL85, vol. 2. Vol. 204 of Lecture Notes in Computer Science. Springer Verlag, pp. 289–290.

Faugère, J.-C., Gianni, P., Lazard, D., Mora, T., 1993. Efficient computation of Gröbner bases by change of orderings. Journal of Symbolic Computation 16, 329–344.

Hubert, É., 2000. Factorization free decomposition algorithms in differential algebra. Journal of Symbolic Computation 29 (4,5), 641–662.

Hubert, É., 2003a. Notes on triangular sets and triangulation–decomposition algorithm I: Polynomial Systems. Symbolic and Numerical Scientific Computing 2001, 243–158.

Hubert, É., 2003b. Notes on triangular sets and triangulation–decomposition algorithm II: Differential Systems. Symbolic and Numerical Scientific Computing 2001, 40–87.

Hubert, É., Le Roux, N., 2003. Computing Power Series Solutions of a Nonlinear PDE System. In: Proceedings of ISSAC 2003. Philadelphia, USA, pp. 148–155.

Knuth, D. E., 1966. The art of computer programming. Addison–Wesley, second edition.

Kolchin, E. R., 1973. Differential Algebra and Algebraic Groups. Academic Press, New York.

Lemaire, F., January 2002a. Contribution à l'algorithmique en algèbre différentielle. Ph.D. thesis, Université Lille I, 59655, Villeneuve d'Ascq, France, (in French).

Lemaire, F., 2002b. Les classements les plus généraux assurant l'analycité des systèmes orthonomes pour des conditions initiales analytiques. In: Victor G. Ganzha, Ernst W. Mayr, Evgenii V. Vorozhtsov (Eds.), proceedings of Computer Algebra in Scientific computation 2002. Institüt für Informatik, Technische Universität München, Yalta, Ukraine, pp. 207–219.

Moreno Maza, M., Rioboo, R., 1995. Polynomial gcd computations over towers of algebraic extensions. In: Proceedings of AAECC11. Springer Verlag, pp. 365–382.

Péladan-Germa, A., 1997. Tests effectifs de Nullité dans des extensions d'anneaux différentiels. Ph.D. thesis, École Polytechnique, Palaiseau, France.

Riquier, C., 1910. Les systèmes d'équations aux dérivées partielles. Gauthier–Villars, Paris.

Ritt, J. F., 1950. Differential Algebra. Dover Publications Inc., New York.

Rosenfeld, A., 1959. Specializations in differential algebra. Trans. Amer. Math. Soc. 90, 394–407.

Rust, C. J., Reid, G. J., Wittkopf, A. D., 1999. Existence and Uniqueness Theorems for Formal Power Series Solutions of Analytic Differential Systems. In: proceedings of ISSAC 1999. Vancouver, Canada.

Seidenberg, A., 1956. An elimination theory for differential algebra. Univ. California Publ. Math. (New Series) 3, 31–65.

Seidenberg, A., 1958. Abstract differential algebra and the analytic case. Proc. Amer. Math. Soc. 9, 159–164.

Seidenberg, A., 1969. Abstract differential algebra and the analytic case II. Proc. Amer. Math. Soc. 23, 689–691.

Sit, W., 2002. The Ritt–Kolchin theory for differential polynomials. In: L. Guo and P. J. Cassidy and W. F. Keigher and W. Y. Sit (Ed.), Proceedings of the international workshop: Differential Algebra and Related Topics. pp. 1–70.

Wang, D., 2003. Elimination Practice: Software Tools and Applications. Imperial College Press, London.

Zariski, O., Samuel, P., 1958. Commutative Algebra. Van Nostrand, New York, Also volumes 28 and 29 of the *Graduate Texts in Mathematics*, Springer Verlag.

François Boulier
Université Lille 1, LIFL, 59655 Villeneuve d'Ascq France
e-mail: `Francois.Boulier@univ-lille1.fr`

François Lemaire
Université Lille 1, LIFL, 59655 Villeneuve d'Ascq France
e-mail: `Francois.Lemaire@univ-lille1.fr`