On the Regularity Property of Differential Polynomials Modulo Regular Differential Chains

François Boulier, François Lemaire, Alexandre Sedoglavic

On the Regularity Property of Differential Polynomials Modulo Regular Differential Chains*

François Boulier[1], François Lemaire[1], and Alexandre Sedoglavic[1]

Université Lille I, LIFL, 59655 Villeneuve d'Ascq, France
Francois.Boulier@univ-lille1.fr
Francois.Lemaire@lifl.fr
Alexandre.Sedoglavic@lifl.fr

Abstract. This paper provides an algorithm which computes the normal form of a rational differential fraction modulo a regular differential chain if, and only if, this normal form exists. A regularity test for polynomials modulo regular chains is revisited in the nondifferential setting and lifted to differential algebra. A new characterization of regular chains is provided.

1 Introduction

This paper is concerned by methods for deciding whether a polynomial f (multivariate, over a field, say, $\mathbb{Q}$) is regular (i.e. not a zerodivisor) modulo a polynomial ideal defined by a regular chain C, which is a set of polynomials. For casual readers, this regularity property may seem quite exotic, compared to (say) the membership property to polynomial ideals. It is however very important and is pretty much related to the problem of computing the solutions of the system of polynomial equations $C = 0$. For instance, if f is proved to be a zerodivisor, then a factorization of some element of C is exhibited, which permits to split the set of equations to be solved, into two simpler sets. Moreover, as we shall see, regularity testing is strongly related to the problem of computing normal forms of polynomials modulo the ideal defined by the regular chain C, which are canonical representatives of the residue class ring defined by C. These comments are stated in the nondifferential case, for simplicity. However, they all have a counterpart for polynomial differential equations, i.e. in differential algebra.

Normal forms have many applications. In differential algebra, they make it easier to compute power series solutions, as pointed out in [2]. In both nondifferential and differential algebra, they permit to search linear dependencies between rational fractions modulo regular chains, by searching linear dependencies between their normal forms, modulo "nothing" (one of the key ideas of [10],

* This work has benefited from the support of the French ANR (decision number ANR-2010-BLAN-0109-03). It benefited also of many exchanges with Markus Rosenkranz and Georg Regensburger.

developed in the differential case in [3]). The very same principle, applied on the derivatives of rational differential fractions, may help to find first integrals.

The motivation for this paper comes from very fruitful remarks of a few reviewers of [2]. In that paper, a normal form algorithm is given for rational differential fractions modulo regular differential chains [2, Figure 2, Algorithm NF]. This normal form algorithm ultimately relies on an algorithm for computing the inverse of a nondifferential polynomial, modulo the ideal defined by a nondifferential regular chain. However, the algorithm provided in [2] may fail to compute the inverse, even if the inverse does exist [2, last comments of section 4]. A few reviewers of [2] then asked if it is possible to provide a complete algorithm, based on regular chains related methods[1], for computing normal forms if, and only if, these normal forms exist. In this paper, we provide the following results:

1. a complete normal form algorithm (Figure 1 and Theorem 4) ;
2. a revisited algorithmic characterization of the polynomials which are regular modulo the ideal defined by a nondifferential regular chain (Theorem 1) and its generalization in differential algebra (Theorem 3) ;
3. a new characterization of regular chains (Theorem 2).

The first result is an answer to the reviewers request. The second one improves former results of [18] and [8] in the nondifferential setting. It completes the proof of [14, Theorem 2.4] and extends this theorem in differential algebra. The third one permits to generalize [14, Theorem 2.4] and [1, Theorem 6.1].

2 Basics of Differential Algebra

The reference books are [16] and [13]. 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, for each derivation δ:

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

and which are assumed to commute pairwise. This paper is mostly concerned with 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*. The monoid Θ acts multiplicatively on U, giving the infinite set ΘU of the *derivatives*.

[1] Observe that, in principle, each required inverse could be easily obtained by using Rabinowitsch's trick and by running the Buchberger algorithm. However, Gröbner bases are not regular chains related methods. Moreover, the method could be costly.

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 [13, chapter I, Corollary to Lemma 1].

Fix a *ranking*, i.e. a total ordering over ΘU satisfying some properties [13, chapter I, section 8]. 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 $\mathrm{ld}\, p$. 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 [13, chapter I, section 9]. To each autoreduced set C, one may associate the set $L = \mathrm{ld}\, C$ 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).

The following definition is borrowed from [2, Definition 3.1].

Definition 1. *The set $C = \{c_1, \ldots, c_n\}$ 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 $2 \leq k \leq n$, the initial i_k of c_k is regular in $K[N \cup L]/(c_1, \ldots, c_{k-1}) : (i_1 \cdots i_{k-1})^\infty$;*
- **c** *for each $1 \leq k \leq n$, the separant s_k of c_k is regular in $K[N \cup L]/(c_1, \ldots, c_k) : (i_1 \cdots i_k)^\infty$;*
- **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 [13, chapter I, section 9].

Triangularity plus condition **b** is the *regular chain* condition of [1]. Autoreduced regular differential chains are the same objects as Ritt characteristic sets. See [2, Proposition 3.2].

3 The Normal Form of a Rational Differential Fraction

All the results of this section are borrowed from [2]. Let C be a regular differential chain of R, defining a differential ideal $\mathfrak{A} = [C] : H_C^\infty$. Let $L = \mathrm{ld}\, C$ and $N = \Theta U \setminus \Theta L$. The normal form of a rational differential fraction is introduced in [2, Definition 5.1 and Proposition 5.2], recalled below.

Definition 2. *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 $\mathfrak{A}$ (in the sense that $a\,g - b\,f \in \mathfrak{A}$).*

Proposition 1. *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 .*

Recall that the normal form algorithm relies on the computation of inverses of differential polynomials, defined below.

Definition 3. *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 $f\,p \equiv q \mod \mathfrak{A}$.*

4 On the Regularity Property of Polynomials

Though this section only addresses algebraic (i.e. nondifferential) questions, we state it with the terminology of the differential algebra. Consider a triangular set C in the polynomial ring $S = K[N \cup L]$. The ideal defined by C, in S, is $\mathfrak{B} = (C) : I_C^\infty$. Assume that $C = \{c_1, \ldots, c_n\}$, that the leading derivative (leading variable) of c_k is x_k and that $x_1 < \cdots < x_n$. It is possible to define the *iterated resultant* of any polynomial f w.r.t. C as follows. See [18, Definition 5.2] or [19, Definition 1.2]. See [8, Definition 4] or [15, Definition 1] for a close definition. See [7] for a definition in a more general setting.

$$\mathrm{res}(f, C) = \mathrm{res}(\cdots \mathrm{res}(f, c_n, x_n), \ldots, c_1, x_1) \tag{1}$$

where $\mathrm{res}(f, c_k, x_k)$ denotes the usual resultant of f and c_k w.r.t. x_k. The next lemma is borrowed from [18, Lemma 5.2]. Together with the two following ones, it prepares the proof of Theorem 1.

Lemma 1. *Let f be any polynomial. There exist polynomials p, $q_1, \ldots, q_n$ such that*

$$p\, f = q_1\, c_1 + q_2\, c_2 + \cdots + q_n\, c_n + \mathrm{res}(f,\, C)\,. \tag{2}$$

Proof. By [17, section 5.8, identity (5.21)], there exist two polynomials p_n and g_n such that

$$p_n\, f = g_n\, c_n + \mathrm{res}(f,\, c_n,\, x_n)\,. \tag{3}$$

There exist two polynomials p_{n-1} and g_{n-1} such that

$$p_{n-1}\ \mathrm{res}(f,\, c_n,\, x_n) = g_{n-1}\, c_{n-1} + \mathrm{res}(\mathrm{res}(f,\, c_n,\, x_n),\, c_{n-1},\, x_{n-1}) \tag{4}$$

hence such that

$$p_{n-1}\, p_n\, f = p_{n-1}\, g_n\, c_n + g_{n-1}\, c_{n-1} + \mathrm{res}(\mathrm{res}(f,\, c_n,\, x_n),\, c_{n-1},\, x_{n-1})\,. \tag{5}$$

Continuing, we obtain (2).

The two following lemmas are easy.

Lemma 2. *Let f, g be two polynomials. Then* $\mathrm{res}(f\, g,\, C) = \mathrm{res}(f,\, C)\ \mathrm{res}(g,\, C)$.

Proof. By induction on the number n of elements of C. If $n = 1$ then the lemma is the well-known multiplicativity property of resultants. See [9, section 3.1, exercises 3, 8 and 10] or [7, page 349]. If $n > 1$, assume inductively that the lemma holds for $C_{n-1} = \{c_1, \ldots, c_{n-1}\}$. Then $\mathrm{res}(f\, g,\, C) = \mathrm{res}(\mathrm{res}(f\, g,\, c_n,\, x_n),\, C_{n-1})$. Then, by the induction hypothesis and the multiplicativity property of resultants, $\mathrm{res}(f\, g,\, C)$ is equal to $\mathrm{res}(\mathrm{res}(f,\, c_n,\, x_n),\, C_{n-1})\ \mathrm{res}(\mathrm{res}(g,\, c_n,\, x_n),\, C_{n-1})$, which, in turn, is equal to $\mathrm{res}(f,\, C)\ \mathrm{res}(g,\, C)$.

Lemma 3. *Let $2 \leq k < n$ be an index and f be any polynomial such that* $\deg(f,\, x_\ell) = 0$, *for $k < \ell \leq n$. There exists a positive integer m such that* $\mathrm{res}(f,\, C) = \mathrm{res}(f,\, C_k)^m$.

Proof. It is an easy consequence of Lemma 2 and of the fact that, if $\deg(f, x) = 0$ and $\deg(g, x) > 0$ then $\mathrm{res}(f,\, g,\, x) = f^{\deg(g,\, x)}$.

In the sequel, a polynomial $f \in S$ is said to be regular modulo $\mathfrak{B}$ (recall $\mathfrak{B} = (C) : I_C^\infty$) if it is a regular element of the ring $S/\mathfrak{B}$. Regular elements and zerodivisors of a ring are defined as in [21, chapter I, § 5].

Theorem 1. *Assume C is a regular chain. A polynomial f is regular modulo $\mathfrak{B}$ if, and only if,* $\mathrm{res}(f,\, C) \neq 0$. *Together with the iterated resultant $q = \mathrm{res}(f,\, C)$, one can compute a polynomial p such that*

$$p\, f = q \mod \mathfrak{B}$$

If f is a zerodivisor modulo $\mathfrak{B}$ then $q = 0$, else p/q is an inverse of f modulo $\mathfrak{B}$.

Proof. The triangularity of C ensures that $\mathrm{res}(f, C) \in K[N]$. Thus, if the first part of the Theorem is proved, the second one follows immediately by Lemma 1.

In order to prove the first part of the Theorem, we first show that we can reduce our problem to the zerodimensional case[2]. Denote $S_0 = K(N)[L]$, and $\mathfrak{B}_0 = (C) : I_C^\infty$ in the ring S_0. By [5, Theorem 1.6], the multiplicative family of the nonzero elements of $K[N]$, is regular modulo $\mathfrak{B}$. Thus the ring $S_0/\mathfrak{B}_0$ is a subring of the total ring of fractions of $S/\mathfrak{B}$ [21, chapter IV, § 9]. Thus, f is regular modulo $\mathfrak{B}$ in S if, and only if, $f/1$ is regular modulo $\mathfrak{B}_0$ in S_0 [21, chapter I, § 19, Corollary 1].

Assume C is a regular chain in S. Then it is a zerodimensional regular chain in S_0. By [8, Lemma 4], an element $f/1$ is regular modulo $\mathfrak{B}_0$ in S_0 if, and only if, $\mathrm{res}(f, C) \neq 0$. Therefore, a polynomial f is regular modulo $\mathfrak{B}$ if, and only if, $\mathrm{res}(f, C) \neq 0$.

The next three lemmas prepare Theorem 2, which gives a necessary and sufficient condition that a triangular set C needs to satisfy in order to be a regular chain. Thus, recall that C is only supposed to be a triangular set.

Lemma 4. *Assume $\mathfrak{B}$ is proper. Let f be any polynomial. If $\mathrm{res}(f, C) \neq 0$ then f is regular modulo $\mathfrak{B}$.*

Proof. Let $\mathfrak{p}$ be any associated prime ideal of $\mathfrak{B}$ (such a $\mathfrak{p}$ exists for $\mathfrak{B}$ is proper). Take Formula (2) modulo $\mathfrak{p}$. The triangularity of C implies that $\mathrm{res}(f, C) \in K[N]$. By [5, Theorem 1.6] and the hypothesis, $\mathrm{res}(f, C) \neq 0 \mod \mathfrak{p}$. Since the elements of C are zero modulo $\mathfrak{p}$, the polynomial f is nonzero modulo $\mathfrak{p}$, i.e. is regular modulo $\mathfrak{B}$ by [21, chapter IV, § 6, Corollary 3].

The following lemma is new.

Lemma 5. *Assume $\mathfrak{B}$ is proper. Assume that, for any polynomial f which is regular modulo $\mathfrak{B}$, we have $\mathrm{res}(f, C) \neq 0$. Then C is a regular chain.*

Proof. The initials of the elements of $C = \{c_1, \ldots, c_n\}$ are regular modulo $\mathfrak{B}$ by [21, chapter IV, § 6, Corollary 3, and § 10, Theorem 17] and the fact that $\mathfrak{B}$ is proper. Thus, by assumption, for each $1 \leq k \leq n$, we have $\mathrm{res}(i_k, C) \neq 0$, where i_k denotes the initial of c_k. Thus, by Lemma 3 and the fact that $\deg(i_k, x_\ell) = 0$ for $k \leq \ell \leq n$, we have $\mathrm{res}(i_k, C_{k-1}) \neq 0$, where $C_{k-1} = \{c_1, \ldots, c_{k-1}\}$. Then, by Lemma 4, the initial i_k is regular modulo $(C_{k-1}) : I_{C_{k-1}}^\infty$. Thus C is a regular chain.

The following lemma is part of [8, Theorem 1].

Lemma 6. *Let h denote the product of the initials of the elements $c_2, \ldots, c_n$ of C. If $\mathrm{res}(h, C) \neq 0$ then C is a regular chain.*

[2] We are actually proving a very close variant of [5, Theorem 1.1].

Proof. Denote $C_k = \{c_1, \ldots, c_k\}$, for $1 \leq k \leq n$. By Lemma 2, Lemma 3 and the hypothesis, $\mathrm{res}(i_k, C_{k-1}) \neq 0$, for all $2 \leq k \leq n$. The ideal $(C_1) : I_{C_1}^{\infty}$ is proper. By Lemma 4, and the fact that $\mathrm{res}(i_2, C_1) \neq 0$, the initial i_2 is regular modulo $(C_1) : I_{C_1}^{\infty}$. The set C_2 is thus a regular chain and $(C_2) : I_{C_2}^{\infty}$ is proper. By Lemma 4, and the fact that $\mathrm{res}(i_3, C_2) \neq 0$, the initial i_3 is regular modulo $(C_2) : I_{C_2}^{\infty}$. Continuing, one concludes that C is a regular chain.

In the following theorem, the implication $2 \Rightarrow 1$ is new. The equivalence between the other points is a consequence of [8, Theorem 1] and [14, Theorem 2.4].

Theorem 2. *Let C be a triangular set. The three following properties are equivalent.*

1. *C is a regular chain ;*
2. *a polynomial f is regular modulo $\mathfrak{B}$ if, and only if,* $\mathrm{res}(f, C) \neq 0$ *;*
3. $\mathrm{res}(h, C) \neq 0$*, where h denotes the product of the initials of the elements $c_2, \ldots, c_n$ of C.*

Proof. The implication $1 \Rightarrow 2$ is a corollary to Theorem 1. The implication $2 \Rightarrow 1$: since $\mathrm{res}(1, C) \neq 0$ for any triangular set C, Property 2 implies that $\mathfrak{B}$ is proper ; the implication is thus a corollary to Lemma 5. The implication $3 \Rightarrow 1$ is Lemma 6. The implication $2 \Rightarrow 3$: Property 2 implies that $\mathfrak{B}$ is proper ; thus h is regular modulo $\mathfrak{B}$ by [21, chapter IV, § 6, Corollary 3, and § 10, Theorem 17]. Thus $\mathrm{res}(h, C) \neq 0$.

Comparison of Theorem 1 with other works. Inspecting the proof of Lemma 6, we see that Property 3 is equivalent to [19, Definition 1.3 (normal ascending chains)], which refers to [20], i.e. that $\mathrm{res}(i_k, C) \neq 0$ for $2 \leq k \leq n$, where i_k denotes the initial of c_k. Therefore, normal ascending chains and regular chains are exactly the same objects.

An algorithm for computing the inverse of a polynomial modulo a regular chain can be found in [15, Algorithm 3]. This algorithm relies on the hypothesis that the polynomial to be inverted is regular modulo the ideal defined by the chain. It relies on a different method (linear system solving) and is not proved.

Another algorithm for computing the inverse of a polynomial modulo a regular chain can be found in [6, Algorithm Invert]. It is based on a Gröbner basis computation. It is based on Kalkbrener's definition of regular chains [12] and thus computes an inverse of a polynomial modulo the intersection of all the prime ideals which contain the ideal defined by the chain, which have dimension $|N|$ and do not meet the multiplicative family M generated by the nonzero elements of $K[N]$, i.e. modulo the radical of the ideal defined by the regular chain. However, [6] misses [5, Theorem 1.6] which implies that $\mathfrak{B}$ has the same set of associated prime ideals as its radical, hence that the computed inverse also is an inverse modulo $\mathfrak{B}$.

Theorem 1 enhances [8, Lemma 4] which is stated in the zerodimensional case only, and does not provide the inverse computation.

Theorem 1 enhances also [18, Proposition 5.3]. Indeed, this Proposition states that $\mathrm{res}(f, C) \neq 0$ if, and only if, the polynomial f does not annihilate on any "regular zero" of C, where "regular zeros" are defined as generic zeros of the associated prime ideals of $\mathfrak{B}$ which have dimension $|N|$ and do not meet the multiplicative family M generated by the nonzero elements of $K[N]$ (see [18, Definition 5.1]). However, [18] misses [5, Theorem 1.6] which states that this property is held by all the associated prime ideals of $\mathfrak{B}$. See the comments on [6, Algorithm Invert].

The fact that a polynomial f is regular modulo $\mathfrak{B}$ if, and only if, $\mathrm{res}(f, C) \neq 0$ is already stated in [14, Theorem 2.4]. However, the proof of that Theorem just refers to [8] and [18] and thus misses the use of [5, Theorem 1.6].

Relationship between Theorem 1 and [5, Theorem 1.6]. Theorem 1 implies "easily" [5, Theorem 1.6] in the particular case of regular chains, i.e. that the associated prime ideals of $\mathfrak{B}$ have dimension $|N|$ and do not meet the multiplicative family M generated by the nonzero elements of $K[N]$. This remark is interesting for [5, Theorem 1.6] is one of the most difficult results of the regular chains theory. See [5]. It stresses, moreover, the strong relationship between the two theorems.

Proof. The regular chain C is a triangular set. Thus, for any nonzero $f \in K[N]$ the iterated resultant $\mathrm{res}(f, C)$ also is a nonzero element of $K[N]$. Thus, by Theorem 1, for any associated prime ideal $\mathfrak{p}$ of $\mathfrak{B}$, we have $\mathfrak{p} \cap M = \varnothing$ whence $\dim \mathfrak{p} \geq |N|$. Since the initials of the element of C do not lie in $\mathfrak{p}$, the derivatives $x_1, \ldots, x_n$ are algebraically dependent over N modulo $\mathfrak{p}$ and $\dim \mathfrak{p} \leq |N|$. Therefore, $\dim \mathfrak{p} = |N|$.

Observe that Theorem 1 does not hold for general triangular sets, while [5, Theorem 1.6] does. This claim is easily proved by an example. Take $f = x - 1$ and $C = \{x^2 - 1, (x - 1)\, y^2 - 2\}$ with $x < y$. The set C is triangular but is not a regular chain, for the initial $x - 1$ of the second element of C is not regular modulo the ideal defined by the first element. The ideal $\mathfrak{B}$ is generated by $\{x + 1, y^2 + 1\}$. It is prime, hence equal to its unique associated prime, if we assume $K = \mathbb{Q}$. The polynomial f is regular modulo $\mathfrak{B}$. However, $\mathrm{res}(f, C) = 0$.

Computational comment. For computational purposes, it is desirable to avoid computing the resultant with respect to x_k of polynomials which do not both depend on x_k, as in [8, Definition 4] and [15, Definition 1]. The iterated resultant is then defined as follows:

$$\mathrm{res}(f, C) = \overline{\mathrm{res}}(\cdots \overline{\mathrm{res}}(f, c_n, x_n), \ldots, c_1, x_1)\,, \tag{6}$$

where $\overline{\mathrm{res}}(f, c_k, x_k)$ is equal to $\mathrm{res}(f, c_k, x_k)$ if $\deg(f, x_k) > 0$ else is equal to f. Lemma 1 still holds with this definition of iterated resultants. By Lemma 2 and Lemma 3, the vanishing conditions of the iterated resultant $\mathrm{res}(f, C)$ are the same with Formula (1) as with Formula (6). Therefore, Theorems 1 and 2 also hold with Formula (6).

Computation of algebraic inverses and normal forms. Consider the triangular set $C = \{(x-1)(x-2), y^2-1\}$ for the ordering $y > x$. Since the initials are equal to 1, it is a regular chain. Consider the polynomial $f = (x-1)y + (x-2)$. We have $pf = -1 = \mathrm{res}(f, C)$, where $p = (-yx + y + x - 2)(2x - 3)$. Thus f is regular modulo the ideal $\mathfrak{B} = (C) : I_C^\infty$. Its inverse is $-p$ modulo $\mathfrak{B}$. Observe that the function [2, Inverse] would have failed to compute the inverse of f, since it would have tried to invert the initial $x-1$ of f modulo $\mathfrak{B}$, which is a zerodivisor modulo $\mathfrak{B}$, before computing the remainder of y^2-1 by f in the algorithm provided in [2, Figure 5]. Therefore, $\mathrm{NF}(1/f, C)$ succeeds with the new algorithm, given in Figure 1, while it fails with the old one, because of the inverse computation of f, w.r.t. C.

5 On the Regularity Property of Differential Polynomials

In this section, C denotes a regular differential chain of the differential polynomial ring R, defining a differential ideal $\mathfrak{A} = [C] : H_C^\infty$. Let $L = \mathrm{ld}\, C$ and $N = \Theta U \setminus \Theta L$.

The following Theorem provides an algorithm for deciding if a differential polynomial is regular modulo a differential ideal defined by a regular differential chain, and, if it is, for computing an inverse of it.

Theorem 3. *Let f be any differential polynomial, r be its partial remainder w.r.t. C and h a product of initials and separants of C such that $hf = r \mod \mathfrak{A}$. Together with the iterated resultant $q = \mathrm{res}(r, C)$, it is possible to compute a polynomial p such that*

$$pr = q \mod (C) : I_C^\infty$$

If f is a zerodivisor modulo $\mathfrak{A}$ then $q = 0$, else hp/q is an inverse of f modulo $\mathfrak{A}$.

Proof. The key arguments are the following: on the one hand, by [4, Corollary 4 to Theorem 3], a differential polynomial is regular modulo $\mathfrak{A}$ if, and only if, its partial remainder with respect to C is regular modulo $\mathfrak{B} = (C) : H_C^\infty$; on the other hand, $\mathfrak{B} = (C) : I_C^\infty$ by [11, Lemma 6.1].

If f is a zerodivisor modulo $\mathfrak{A}$, then r is a zerodivisor modulo $\mathfrak{B}$ and $q = 0$ by Theorem 1. Assume f is regular modulo $\mathfrak{A}$. Then r is regular modulo $\mathfrak{B}$ and q is a nonzero element of $K[N]$ by Theorem 1. Since $\mathfrak{B} \subset \mathfrak{A}$, we have $hpf = q \mod \mathfrak{A}$. Thus hp/q is an inverse of f modulo $\mathfrak{A}$.

A complete algorithm for computing the normal form of a rational differential fraction is presented in Figure 1. This algorithm is obtained from [2, The NF function, Figure 2] by udpating the method applied for computing inverses.

Theorem 4. *Let a/b be a rational differential fraction and C be a regular differential chain. If b is a zerodivisor modulo $\mathfrak{A}$, then $\mathrm{NF}(a/b, C)$ raises an error, else $\mathrm{NF}(a/b, C)$ returns the normal form of a/b modulo C.*

Proof. The Theorem is simply a restatement of [2, Proposition 5.3], taking into account the fact that inverses are computed using a method (Theorem 3) which succeeds if, and only if, the polynomial to be inverted is invertible.

Comment. The algorithm presented in Figure 1 has a drawback with respect to [2, The NF function, Figure 2]: if the denominator of the rational fraction is a zerodivisor, the algorithm does not exhibit a factorization of some element of C. This drawback may be easily overcome if one computes resultants by means of pseudoremainder sequences.

---

function NF(a/b, C)
Parameters
  a/b is a rational differential fraction such that a, $b \in R$.
  C is a regular differential chain, defining a differential ideal $\mathfrak{A}$.
Result
  if b is regular modulo $\mathfrak{A}$, then the normal form of a/b modulo $\mathfrak{A}$, else an error
begin
Regularity test and inverse computation of the denominator
  Apply Theorem 3 over b:
    if b is a zerodivisor modulo $\mathfrak{A}$ then
      error "the denominator is a zerodivisor modulo $\mathfrak{A}$"
    end if
    Denote $p_\mathrm{b}/q_\mathrm{b}$ an inverse of b modulo $\mathfrak{A}$
Inverse computation of the separants (they are necessarily regular)
  Apply Theorem 1 over each separant s_i of $C = \{c_1, \ldots, c_n\}$ and
                denote p_i/q_i an inverse of s_i modulo $\mathfrak{A}$
  $(f_{n+2},\, g_{n+2}) := (p_\mathrm{b}\, a,\, q_\mathrm{b})$
  Using Ritt's partial reduction algorithm, compute $d_1, \ldots, d_n \in \mathbb{N}$ and
                $r_{n+1} \in K[N \cup L]$ such that $s_1^{d_1} \cdots s_n^{d_n}\, f_{n+2} \equiv r_{n+1} \mod \mathfrak{A}$
  $f_{n+1} := p_1^{d_1} \cdots p_n^{d_n}\, r_{n+1}$
  $g_{n+1} := q_1^{d_1} \cdots q_n^{d_n}\, g_{n+2}$
  Denote $x_i = \mathrm{ld}\, c_i$ $(1 \leq i \leq n)$ and assume $x_n > \cdots > x_1$
  for ℓ from n to 1 by -1 do
    $r_\ell := \mathrm{prem}(f_{\ell+1},\, c_\ell,\, x_\ell)$
    Let i_ℓ denote the initial of c_ℓ
    Let $d_\ell \in \mathbb{N}$ be such that $i_\ell^{d_\ell}\, f_{\ell+1} \equiv r_\ell \mod (c_\ell)$
Inverse computation of an initial (it is necessarily regular)
    Apply Theorem 1 over i_ℓ and denote p_ℓ/q_ℓ an inverse of i_ℓ modulo $\mathfrak{A}$
    $f_\ell := p_\ell^{d_\ell}\, r_\ell$
    $g_\ell := q_\ell^{d_\ell}\, g_{\ell+1}$
  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

Fig. 1. The NF function

Bibliography

[1] Philippe Aubry, Daniel Lazard, and Marc Moreno Maza. On the Theories of Triangular Sets. *Journal of Symbolic Computation*, 28:105–124, 1999.

[2] François Boulier and François Lemaire. A Normal Form Algorithm for Regular Differential Chains. *Mathematics in Computer Science*, 4(2):185–201, 2010. 10.1007/s11786-010-0060-3.

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

[4] François Boulier, Daniel Lazard, François Ollivier, and Michel Petitot. Computing representations for radicals of finitely generated differential ideals. *Applicable Algebra in Engineering, Communication and Computing*, 20(1):73–121, 2009. (1997 Techrep. IT306 of the LIFL).

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

[6] Driss Bouziane, Abdelillah Kandri Rody, and Hamid Maârouf. Unmixed–Dimensional Decomposition of a Finitely Generated Perfect Differential Ideal. *Journal of Symbolic Computation*, 31:631–649, 2001.

[7] Laurent Busé and Bernard Mourrain. Explicit factors of some iterated resultants and discriminants. *Mathematics of Computation*, 78:345–386, 2009.

[8] Changbo Chen, François Lemaire, Marc Moreno Maza, and Wei Pan. Comprehensive Triangular Decompositions. In *Proceedings of CASC'07*, pages 73–101, 2007.

[9] David Cox, John Little, and Donal O'Shea. *Using Algebraic Geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer Verlag, New York, 2nd edition, 2005.

[10] 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.

[11] Évelyne Hubert. Factorization free decomposition algorithms in differential algebra. *Journal of Symbolic Computation*, 29(4,5):641–662, 2000.

[12] Mickael Kalkbrener. A Generalized Euclidean Algorithm for Computing Triangular Representations of Algebraic Varieties. *Journal of Symbolic Computation*, 15:143–167, 1993.

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

[14] François Lemaire, Marc Moreno Maza, Wei Pan, and Yuzhen Xie. When does (T) equal sat(T) ? In *Proceedings of thee International Symposium on Symbolic and algebraic computation*, pages 207–214. ACM Press, 2008.

[15] Banghe Li and Dingkang Wang. *An Algorithm for Transforming Regular Chain into Normal Chain*, volume 5081 of *Lecture Notes in Computer Science*, pages 236–245. Springer Berlin / Heidelberg, 2008.

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

[17] Bruno Louis van der Waerden. *Algebra*. Springer Verlag, Berlin, seventh edition, 1966.

[18] Dongming Wang. Computing Triangular Systems and Regular Systems. *Journal of Symbolic Computation*, 30:221–236, 2000.

[19] Lu Yang, Xiaorong Hou, and Bican Xia. A complete algorithm for automated discovering of a class of inequality-type theorems. *Science in China Series F: Information Sciences*, 44(1):33–49, 2001.

[20] Lu Yang, Jingzhong Zhang, and Xiaorong Hou. An Efficient Decomposition Algorithm for Geometry Theorem Proving Without Factorization. *Proceedings of ASCM*, pages 33–41, 1995.

[21] Oscar Zariski and Pierre Samuel. *Commutative Algebra*. Van Nostrand, New York, 1958. Also volumes 28 and 29 of the *Graduate Texts in Mathematics*, Springer Verlag.