Standard Bases of Differential Ideals (1)

François Ollivier

Laboratoire d'Informatique de l'X (LIX) (2)
École Polytechnique
F-91128 Palaiseau Cedex (France)

cffoll@frpoly11.BITNET
ollivier@cmep.polytechnique.fr

September, 1990

Abstract: The aim of this paper is to introduce a new definition of standard bases of differential ideals, allowing more general orderings than the previous one, given by Giuseppa Carrá-Ferro, and following the general definition of standard bases, given in [O3], valid for algebraic ideals, canonical bases of subalgebras, etc.

Differential standard bases, as canonical bases, suffer a great limitation: they can be infinite, even for ideals of finite type. Nevertheless, we can sometimes bound the order of intermediate computations, necessary to make some elements of special interest appear in the basis.

As an illustration, we consider a differential rational map $f: \mathbf{A}^n_{\mathcal{F}} \mapsto \mathbf{A}^n_{\mathcal{F}}$, and show that if f is birational, then $\operatorname{ord} f^{-1} \le n \operatorname{ord} f$. Partial standard bases computations provide then two algorithms to test the existence of f^{-1}. The first one is also able to determine the inverse, if any. The second only determines existence, but we can provide a bound of complexity depending only of n, $\operatorname{ord} f$ and the number of derivatives.

0. Introduction

The theory of standard bases introduced here is not a new variant of the standard bases of $\mathcal{D}$-modules introduced by Castro [Cas]. We will deal with commutative differential rings, not rings of differential operators.

Effective—or almost effective—methods for solving systems of differential algebraic equations go back to the work of Riquier and Janet (cf. [Ja] 1920). Their results have been then improved by Ritt ([R1] 1932, [R2] 1950) who gets an effective method only

(1) Partially supported by GDR G0060 *Calcul Formel, Algorithmes, Langages et Systèmes* and PRC *Mathématiques et Informatique*.

(2) Équipe *Algèbre et Géométrie Algorithmiques, Calcul Formel*, SDI CNRS n° 6176 et Centre de Mathématiques, Unité de Recherche Associée au CNRS n° D0169

if the ground field allows effective factorization. This drawback has been removed by SEIDENBERG ([S] 1956), whose method has been recently implemented by Sette DIOP [D]. The original method of Ritt has also been studied by WU, first in the algebraic case, and then in the differential one. It is particularly interesting for automatic theorem proving in elementary geometry (see [Ch]). Another point of view on this matter may be found in the work of POMMARET [P2], who uses the language and results of the formal theory of partial differential equations, initiated by SPENCER.

Nevertheless, for the best of my knowledge, no method has been developed yet to answer the membership problem for a differential ideal. The computation of a characteristic set only gives partial results: the polynomial in the ideals are reduced to 0, but the reciprocal is false except for prime ideals. Furthermore, no general method has been given to compute a genuine characteristic set, and not only a coherent and autoreduced set.

We can hope that a generalization of standard bases will give a satisfactory answer. Indeed, in [Car] (1987), Giuseppa CARRA'-FERRO introduced a definition for differential standard bases. We provide here a more general one, allowing a wider class of orderings, and underlying the connections with the theory of standard bases, canonical bases, etc, following the abstract definition given in [O3]. The main trouble is that differential standard bases are in general infinite. This was already the case for canonical bases of subalgebras (see [KL], [RS], [O2]).

We are still able to prove that a completion process converges to a standard basis, meaning that after a finite number of steps we will get a basis up to a given order of derivation. We have no way yet to determine the complexity of a partial computation, nor to check it has been performed without using explicit information on the structure of the ideal, and theoretical results of differential algebra.

Anyway, this is not so far from the algebraic situation, which may be intractable, except for "well behaved" ideals. We provide an illustration of this point of view by giving algorithms to test whether a differential rational map admits an inverse. We had already proved complexity bounds for algebraic rational maps and polynomial ones (see [O1], [O2] and [O3]), using a theorem of O. GABBER. We extend this theorem to differential maps, proving that $\operatorname{ord} f^{-1} \leq n \operatorname{ord} f$, if n is the number of variables. This work is a by-product of our interest in control theory and modeling, where the search for effective and efficient tests for abstract properties of structures, as identifiability, requires such theoretical investigations (see [O1] and [O3]).

1. Standard bases

We will denote by $\mathcal{F}$ a differential field of characteristic zero.

1.1. Preliminary results of differential algebra

We limit ourselves to the essential results and definitions needed in the following. Details may be found in the classical books of RITT [R1] and [R2], or in KOLCHIN [Ko], KAPLANSKY [Ka], and POMMARET [P1]. I will mostly follow the exposition and notations of [Ko].

DEFINITION 1. *A differential ring is a ring with a finite set $\Delta = \{\delta_1, \ldots, \delta_m\}$ of differential operators, i.e. internal mappings δ satisfying*

$$\delta(a\,b) = \delta\,a\,b + a\,\delta\,b$$
$$\delta(a+b) = \delta\,a + \delta\,b,$$

and such that $\delta_i\,\delta_j = \delta_j\,\delta_i$.

A differential field is a field which is a differential ring.

DEFINITION 2. *A differential ideal of a differential ring is an ideal $\mathcal{I}$, such that $\forall \delta \in \Delta\ \delta\,\mathcal{I} \subset \mathcal{I}$.*

Following classical notations, we denote by (S), the ideal generated by S, and by $[S]$ the differential ideal generated by S.

DEFINITION 3. *A differential ideal $\mathcal{I}$ is said to be perfect if $a^n \in \mathcal{I}$ implies $a \in \mathcal{I}$*

The perfect ideal generated by Σ is denoted by $\{\Sigma\}$.

DEFINITION 4. *We will denote by Θ the abelian free monoïd generated by Δ. For any set X, we denote by $\Theta\,X$ the set of derivatives $\Theta \times X$. The element (θ, x) will by written $x_{(\theta)}$. There is an action of Θ on $\Theta\,X$ defined by $\tau\,x_{(\theta)} = x_{(\tau\,\theta)}$.*

The algebra of differential polynomials $\mathcal{F}\{X\}$ will be the algebra $\mathcal{F}[\Theta\,X]$ with the unique set of derivations Δ extending derivations on $\mathcal{F}$ and such that $\delta x_{(\theta)} = x_{(\delta\,\theta)}$. $\mathcal{F}\{X\}$ is a differential algebra over $\mathcal{F}$. Those derivations also extend to the field of fractions of $\mathcal{F}\{X\}$, denoted by $\mathcal{F}\langle X\rangle$. We call a monomial of $\mathcal{F}\{X\}$, a polynomial which is a product of derivatives or 1, and a term the product of a monomial by a non-zero element of $\mathcal{F}$.

Lemma 5. If Σ is a subset of a differential ring R (resp. a differential R-algebra A), then the differential ideal (resp. R-algebra) generated by Σ is equal to $(\Theta\,\Sigma)$ (resp. $R[\Theta\,\Sigma]$). ∎

In general, if $\mathcal{G}$ is a differential field extension of $\mathcal{F}$, and η a subset of $\mathcal{G}$, we denote by $\mathcal{F}\langle\eta\rangle$, the differential field extension of F generated by η. If R is a differential ring and Σ a subset of a R-algebra A, we denote by $R\{\Sigma\}$ the differential R-algebra generated by Σ. From now on, we will only consider differential polynomials over a field $\mathcal{F}$ of characteristic zero, with finite set of variables $X = \{x_1, \ldots, x_n\}$. The set of derivatives of the field $\mathcal{F}$ will be $\Delta = \{\delta_1, \ldots, \delta_m\}$.

THEOREM 6. *If $\mathcal{I}$ is a perfect differential ideal of $\mathcal{F}\{X\}$, then there exists a finite set Σ of differential polynomials such that $\mathcal{I} = \{\Sigma\}$.*

PROOF. See [Ko]. ∎

This is the best we can do. The set of differential polynomials is not noetherian.

THEOREM 7. *If $\mathcal{I}$ is a perfect ideal of $\mathcal{F}\{X\}$, then there exists a unique set $\{\mathcal{I}_1, \ldots, \mathcal{I}_r\}$ of prime ideals such that*

$$\mathcal{I} = \bigcap_{i=1}^{r} \mathcal{I}_i,$$

and $\mathcal{I}_i \not\subset \mathcal{I}_j$ $i \neq j$. Those prime ideals are said to be the components of $\mathcal{I}$.

DEFINITION 8. *Let $\mathcal{I}$ be a prime differential ideal of $\mathcal{F}\{X\}$, $(\eta_1, \ldots, \eta_n)$ a n-uple of elements in a differential field extension $\mathcal{G}$ of $\mathcal{F}$. η will be said to be a generic zero of $\mathcal{I}$ over $\mathcal{F}$ if $\{P \in \mathcal{F}\{X\} | P(\eta) = 0\} = \mathcal{I}$. The generic zeroes of $[0]_{\mathcal{F}[x]}$ are called generic elements of $\mathcal{G}$ over $\mathcal{F}$.*

An extension $\mathcal{U}$ of $\mathcal{F}$ is said to be universal if for all finite extension $\mathcal{F} \subset \mathcal{G} \subset \mathcal{U}$, all finite set X and all prime differential ideal $\mathcal{I} \subset \mathcal{G}\{X\}$, there exists a generic zero of $\mathcal{I}$ over $\mathcal{G}$ in $\mathcal{U}$.

All differential fields admit a universal extension (see [Ko]). This notion is in fact the same as the universal domains of Weil, if the set of derivatives is empty. It allows to throw away some logical difficulties in the definition of differential algebraic varieties given by Ritt. They may be defined as the sets of zeroes of differential ideals in a universal extension $\mathcal{U}$, chosen once and for all. The variety associated to an ideal $\mathcal{I}$ is denoted by $V(\mathcal{I})$. The differential affine space of dimension r over $\mathcal{F}$, $\mathbf{A}^r_{\mathcal{F}}$, is the set of zeroes of $[0]$ $\mathcal{U}^r$. We refer to [Ko] for more details on differential algebraic geometry and conclude this short introduction by a powerful result first proved by RITT in the ordinary differential case, and latter extended by KOLCHIN.

DEFINITION 9. *The order of $\theta = \prod_{i=1}^r \delta_i^{\alpha_i}$ is $\sum_{i=1}^r \alpha_i$, and the order of a derivative $\theta\, x$ is the order of θ. We denote by Θ_r the set of derivation operators of order less than or equal to r and by $\mathrm{ord}\, v$ the order of a derivative. The order of a differential polynomial is the maximal order of its derivatives.*

PROPOSITION 10. *Let $\mathcal{I}$ be a prime ideal of $\mathcal{F}\{X\}$, η a generic zero of $\mathcal{I}$, the function $H : \mathbf{N} \mapsto \mathbf{N}$ such that $H(r)$ is the (algebraic) transcendance degree of $\mathcal{F}(\Theta_r \eta)$ over $\mathcal{F}$ is equal to a polynomial $\omega_{\eta/\mathcal{F}}$ for r great enough. Furthermore*

$$\omega_{\mathcal{I}}(r) = \sum_{i=1}^{m} a_i \binom{r+i}{i},$$

where a_m is the differential dimension of $\mathcal{I}$, i.e. the differential transcendance degree of $\mathcal{F}\langle\eta\rangle$ over $\mathcal{F}$. ■

The greatest i such that $a_i \neq 0$ will be called the *differential type* of $\mathcal{I}$, $\tau_{\mathcal{I}}$, and $a_{\tau_{\mathcal{I}}}$ the *typical differential dimension* of $\mathcal{I}$. As $\omega_{\eta/\mathcal{F}}$ does only depend of $\mathcal{I}$, we can also denote it by $\omega_{\mathcal{I}}$. If V is an irreducible algebraic differential variety defined by a prime ideal $\mathcal{I}$, we extend to it the definitions given above.

THEOREM 11. *(Ritt–Kolchin) Let $\mathcal{I} = \{P_1, \ldots, P_r\}$, where the maximal order of the P_i is e, and $\mathcal{J}$ a component of $\mathcal{I}$, whose differential type is $m-1$, then the typical differential dimension of $\mathcal{J}$ is less than or equal to $n\, e$.*

PROOF. See [Ko chap. IV § 17 p. 199] ■

1.2. Admissible orderings. Reduction

We need to define suitable orderings to allow reductions in $\mathcal{F}\{X\}$. This implies to strengthen the definitions valid in the pure algebraic case to take derivations into account.

Definition 1. *Let $<$ be a total ordering on the set $\mathcal{M}$ of monomials of $\mathcal{F}\{X\}$. We extend derivations to $\mathcal{M}$ by taking δM to be the maximal monomial involved in the polynomial δM. By convention, $\delta 1 = 1$. The order $<$ is said to be admissible if*

a) $M > 1$ $M \neq 1$,

b) $M > M'$ implies $M''M > M''M'$,

c) $\delta M > M$ $M \neq 1$,

d) $M > M'$ implies $\delta M > \delta M'$.

If $<$ is admissible, we denote by $\mathrm{lm} P$ the leading monomial of P, by $\mathrm{lc} P$ its leading coefficient. We call reductum of P the polynomial $P - \mathrm{lc}\, P\, \mathrm{lm}\, P$.

So we define $\delta\, M$ in $\mathcal{M}$ to be $\mathrm{lm}(\delta\, M)$. I think no misunderstanding can result of this notation, which will be useful later.

We now need to describe some admissible orderings. For this, we first define admissible orderings, i.e. rankings in the words of Ritt, on the set of derivatives $\Theta\, X$. They are orderings which satisfy c) and d) in the definition above. Considering elements of Θ as monomials, e.g. in $\mathbf{Q}[\Delta]$, we take an admissible ordering on Θ. We extend it to $\Theta\, X$ with the following definitions.

Definition 2. *The ordering on $\Theta\, X$ defined by $x_{i,(\theta)} < x_{i',(\theta')}$ if $i < i'$ or $i = i'$ and $\theta < \theta'$ is said to be the lexicographical ordering extending $<$.*
The ordering defined by $x_{i,(\theta)} < x_{i',(\theta')}$ if $\theta < \theta'$ or $\theta = \theta'$ and $i < i'$ is the derivation ordering extending $<$.

It is easily seen that those orderings are admissible (see [Ko chap. 0 § 17 p. 50]).

Remark 3. If $<$ on Θ respects the order, then the derivation ordering $<$ on $\Theta\, X$ respects the order too, it is said then to be *orderly*.

Let $<$ be an admissible ordering on derivatives, we can extend it to monomials of $\mathcal{F}\{X\}$ in the following way. Consider two monomials $M = \prod_{i=1}^{r} \upsilon_i^{\alpha_i}$ and $M' = \prod_{i=1}^{s} \nu_i^{\beta_i}$, where the υ_i and ν_i appear in strictly decreasing order. We take $M < M'$ if there exists $j \leq r, s$ such that $\upsilon_i = \nu_i$ $i < j$, $\alpha_i = \beta_i$ $i < j$, $\upsilon_j < \nu_j$ or $\upsilon_j = \nu_j$ and $\alpha_j < \beta_j$.

Proposition 4. *The ordering $<$ defined above is an admissible well ordering on monomials. If $<$ is orderly, its extension to monomials is also orderly, i.e. $\mathrm{ord}\, P > \mathrm{ord}\, Q$ implies $P > Q$.*

proof. It is immediate that a) and b) are satisfied. In order to prove c) and d), we only have to remark that $\delta\, m = \delta\, \upsilon_1\, \upsilon_1^{\alpha_1 - 1} \prod_{i=2}^{r} \upsilon_i^{\alpha_i}$. If $<$ is orderly on derivatives, then $\mathrm{ord}\, P < \mathrm{ord}\, Q$ implies that the leading derivative of P is smaller than that of Q, so that $P < Q$.

We now show that $<$ is a well ordering. It is known that all admissible orderings on variables are well orderings (see [Ko]). Consider now an infinite sequence $M_0 > M_1 > \cdots$ of monomials. The leading derivatives of these monomials appear in decreasing order, so that for some integer r the chain they form will become stationary. Let υ be the leading derivative of M_i for $i > r$. The degree in υ of M_i $i > r$ will be decreasing too, so that for $i \geq s \geq r$ this degree becomes a constant integer d. Dividing M_i by υ^d, for $i \geq s$, we secure a new strictly decreasing sequence of monomials, whose leading derivatives are smaller than v. Repeating the argument, we build an infinite strictly decreasing sequence of derivatives: a contradiction. ■

So admissible orderings on monomials actually exist. It will be useful to consider other orderings than those coming from the previous propositions. We may first remark that if P is a differential polynomial of degree d, then $\theta\, P$ is also of degree d, moreover if P is homogeneous, $\theta\, P$ is homogeneous too. We shall need some more convenient grading on $\mathcal{F}\{X\}$, defined by taking the weight of a monomial $\prod_{i=1}^{r} v_i^{\alpha_i}$ equal to $\sum_{i=1}^{r} \alpha_i \operatorname{ord} v_i$. A polynomial whose monomials are of the same weight is called *isobaric*. The maximal weight of monomials of a polyomial P is called the weight of P ($\operatorname{wt} P$). The derivative $\delta\, P$ of an isobaric polynomial is not in general isobaric, except if the coefficients of P lie in the field of constants of $\mathcal{F}$, but for all polynomial $P \notin \mathcal{F}$ $\operatorname{wt}\theta\, P = \operatorname{wt} P + \operatorname{ord}\theta$—we only consider characteristic zero!

Lemma 5. If $<$ is an admissible ordering on monomials, we get a new admissible ordering $\prec$ by taking $M \prec M'$ if $\deg M < \deg M'$ or if $\deg M = \deg M'$ and $M < M'$. The same applies when considering the weight, or the partial degree according to some subset of X.

If $<$ is a well ordering, then $\prec$ is also a well ordering ■

Remark 6. More generally, we can use all the admissible gradings defined in [Ko chap I § 7 p. 72].

Recursive use of this lemma allows to build a wide class of orderings, for example elimination orderings. In the following, we will suppose that such an ordering $<$ has been chosen once and for all.

We now come to reduction.

Definition 7. *We say that a polynomial P is elementarily reduced by Q to R if there exist a monomial M and a derivation operator θ such that $\operatorname{lm} P = M \operatorname{lm}\theta\, Q$ and $R = P - (\operatorname{lc} P/\operatorname{lc} Q)\, M\, \theta\, Q$. We write it $P \xrightarrow{Q} R$. We say that P is elementarily reduced to R by a set of polynomials Σ if there exists $Q \in \Sigma$ such that $P \xrightarrow{Q} R$. P will be said to be reduced to R by Σ if there exists a chain of elementary reductions*

$$P = P_0 \xrightarrow{\Sigma} P_1 \xrightarrow{\Sigma} \cdots \xrightarrow{\Sigma} P_r = R.$$

We denote it by $P \xrightarrow{\Sigma *} R$.

We say that P is totally reduced to R by Σ if P is reduced to R by Σ or if the reductum of P is totally reduced to R' by Σ and $R' = lc\, P \operatorname{lm} P + R'$. P is irreducible by Σ if there is no Q such that $P \xrightarrow{\Sigma} Q$.

Remark 8. If we use the fact that $\theta \operatorname{lm} P = \operatorname{lm}(\theta\, P)$, for $P \notin \mathcal{F}$, with the extension of derivations to monomials made above, it becomes obvious that the reducibility of P by Q only depends of the leading monomials of P and Q. It is then easily that, if P is reducible by Q, the weight (or degree) of the leading monomial of P is not less than that of Q. It is also obvious that $P \xrightarrow{Q} R$ implies $\operatorname{lm} R < \operatorname{lm} P$.

Lemma 9. $P \xrightarrow{\Sigma_*} 0$, *iff* $P = \sum_{i=1}^{r} M_i\,\theta_i\,P_i$, *where the* M_i *are terms, and the* P_i *polynomials in* Σ, *with* $\mathrm{lm}(M_i\,\theta_i\,P_i) > \mathrm{lm}(M_j\,\theta_j\,P_j)$ $i < j$. ∎

We can build an effective reduction process which takes a polynomial P and a finite list of polynomials Σ and returns a polynomial R such that $P \xrightarrow{\Sigma_*} R$ and R is irreducible by Σ. We begin by reduction with respect to a single polynomial. We use the syntax of the IBM computer algebra system Scratchpad II for the algorithms.

REDUCTION ALGORITHM

reduction(P, Q) == reduction$(P, Q, 1)$
reduction(P, Q, r) ==
  $\deg \mathrm{lm} P > \deg \mathrm{lm}\, Q$ or $\mathrm{wt}\,\mathrm{lm}\,P > \mathrm{wt}\,\mathrm{lm}\,Q$ => return P
  $\mathrm{lm}\,Q \backslash \mathrm{lm}\,P$ => return reduction$(P - (\mathrm{lc}\,P/\mathrm{lc}\,Q)\,(\mathrm{lm}\,P/\mathrm{lm}\,Q)\,Q, Q)$
  for $i \in [r, \ldots, m]$ repeat
    if $(P_2 :=$ reduction$(P, \delta_i\,Q, i)) \neq P$ then return reduction(P_2, Q)
  P

PROOF. We first prove that the process stops and returns P if it is irreducible by Q. If we can apply the remark above, it stops on the first line. If not, the process is recursively repeated with derivatives of P. As their weight increases by 1 at each new step, the remark will necessarily apply after a finite number of steps. Now, if P is reducible, its leading monomial needs to be a multiple of the leading monomial of some $\theta\,Q$. A solution will to be found by trying all successive derivatives of Q, whose leading monomials have weight less or equal to the weight of P, which is done. We perform then an elementary reduction, and repeat the process. It needs to stop, for $<$ is a well ordering, and so there is no infinite sequence of elementary reductions. ∎

It is now simple to get a reduction algorithm for a list of polynomials, or for total reduction.

1.3. Definitions

DEFINITION 1. *Considering the multiplicative monoïd* $\mathcal{M}$ *of monomials in* $\mathcal{F}\{X\}$, *with the derivations acting on it as in def. 2.1, we call a subset* E *a differential monoïdeal if it is a monoïdeal—i.e. if* $\mathcal{M}E \subset E$*—, and if* $\Delta\,E \subset E$.

REMARK 2. Obviously, the set of leading monomials of a differential ideal is a differential monoïdeal. Of course the "derivations" defined on $\mathcal{M}$ are not real ones, but the mere reflect of derivations acting on polynomials. Indeed, the mapping δ_i themselves do not need to be derivations. We only need that $\mathrm{lm}\delta\,P = \mathrm{lm}\delta(\mathrm{lm}\,P)$ and that $\delta(P+Q) = \delta\,P + \delta\,Q$, so that we could use more general differential operators, say $d = \delta_1^2 - \delta_2^3$ and define standard bases for d-ideals, i.e. ideals $\mathcal{I}$ such that $d\mathcal{I} \subset \mathcal{I}$, but for this we would need a more complicated definition of reduction, and a wider class of syzygies (see [O3]).

Using derivations, we are indeed able to restrict the set of syzygies to consider, for given a product of monomials $M\,M'$, $\delta(M\,M')$ equals $\delta\,M\,M'$ or $M\,\delta\,M'$, so that the differential monoïdeal generated by a subset E of $\mathcal{M}$ is equal to $\mathcal{M}\,\Theta\,E$ (see subsection 4. bellow).

Definition 3. *A subset G of a differential ideal $\mathcal{I}$ is said to be a standard basis if $\mathrm{lm}\, G$ generates $\mathrm{lm}\,\mathcal{I}$ as a differential monoïdeal.*

Theorem 4. *Let G be a set of polynomials, $\mathcal{I}$ a differential ideal. Then the following propositions are equivalent:*

i) G is a standard basis of $\mathcal{I}$,

ii) $G \subset \mathcal{I}$ and there is no non-zero element of $\mathcal{I}$ reduced with respect to G,

iii) $G \subset \mathcal{I}$ and all the elements of $\mathcal{I}$ are reduced to 0 by G,

iv) a differential polynomial is in $\mathcal{I}$ iff it is reduced to 0 by G.

proof. $i) \Longrightarrow ii)$. If G is a standard basis of $\mathcal{I}$ it is a subset of $\mathcal{I}$. Now, the leading monomial of any non-zero polynomial in $\mathcal{I}$ is in $\mathcal{M}\,\Theta\,\mathrm{lm}\,G$ using remark 2 above, so that it is reducible by G.

$ii) \Longrightarrow iii)$. As $G \subset \mathcal{I}$, if $P \xrightarrow{G} Q$ with $P \in \mathcal{I}$, then $Q \in \mathcal{I}$, so that we can perform repeated reductions using ii). As chains of reductions are finite, *the result of any reduction process* is 0, which is more than iii).

$iii) \Longrightarrow iv)$. $\Rightarrow$ is immediate from iii). $\Leftarrow$ Again, as $G \subset \mathcal{I}$, if $P \xrightarrow{G_*} 0$, P needs to be in $\mathcal{I}$.

$iv) \Longrightarrow i)$. All polynomials in G are reduced to 0 by G, so that $G \subset \mathcal{I}$. As all polynomials in $\mathcal{I}$ are reduced to 0 by G, they are reducible, so that $\mathrm{lm}\,\mathcal{I} \subset \mathcal{M}\,\Theta\,\mathrm{lm}\,G$. Using the first part of the proof, we have indeed equality. ∎

Definition 5. *A standard basis G of $\mathcal{I}$ is said to be minimal if $\mathrm{lm}\,G$ is a minimal set of generators of $\mathrm{lm}\,\mathcal{I}$. A minimal standard basis G is called reduced if all polynomials $P \in G$ are totally reduced by $G \setminus \{P\}$.*

Proposition 6. *Any ideal admits minimal standard bases and a unique reduced standard basis. An ideal admits a finite standard basis iff it admits a finite minimal standard basis. In this case, all the minimal standard bases are finite.* ∎

1.4. Characterization

We have completed the easiest part with definitions. The completion process will rely on more tedious results.

Definition 1. *Let P and Q be two differential polynomials, we call a syzygy between P and Q a 2-uple $(M\,\theta\,P, M'\,\theta'\,Q)$, where $M, M' \in \mathcal{M}$, $\theta, \theta' \in \Theta$, of polynomials with the same leading monomials. An essential syzygy is a syzygy with M and M' minimal and such that there is no other syzygy $(N\,\tau\,P, N'\,\tau'\,Q)$ satisfying $\vartheta(N\,\tau\,\mathrm{lm}\,P) = M\,\theta\,\mathrm{lm}\,P$ and $\vartheta(N'\,\tau'\,\mathrm{lm}\,Q) = M'\,\theta'\,\mathrm{lm}\,Q$ for some ϑ, the derivations being taken in $\mathcal{M}$.*

We call S-polynomial associated to the syzygy (U, V), the polynomial $\mathrm{lc}\,V\,U - \mathrm{lc}\,U\,V$. The rank of the syzygy will be the common leading monomial of U and V.

Example 2. Consider ordinary differential polynomials in $\mathcal{F}\{x\}$. There is only one admissible ordering on Θ and $\Theta\,x$. We choose the ordering on monomials coming from prop. 2.4. Take $\mathcal{I} = \{x^2\}$. There is an essential syzygy $(\delta x\, x^2, x\,\delta(x^2))$. The syzygy $(\delta^2 x\, x^2, x\,\delta^2(x^2))$ is not essential. The only essential syzygies different from that already given are of the form $(\delta^{n+1} x\,\delta^n(x^2), \delta^n x\,\delta^{n+1}(x^2))$ $n \geq 1$. This shows that syzygies may involve twice the same polynomial, and that there is in general an infinite number of essential syzygies.

DEFINITION 3. *Let Σ be a set of polynomials, P a polynomial in $[\Sigma]$. We call rank of P with respect to Σ the smallest monomial M such that* (1) $P = \sum_{i=1}^{r} Q_i\,\theta_i\,P_i$, *where the P_i belong to Σ, the Q_i are terms and $\mathrm{lm}\,Q_i\,\theta_i\,P_i \leq M$.*

REMARK 4. The rank of P is greater than or equal to the leading monomial of P. If P is reduced to 0 by Σ, it is equal to $\mathrm{lm}\,P$. We may consider, e.g. $\Sigma = \{\delta_1 x + \delta_3 x, \delta_2 x + \delta_3 x\}$ and $P = \delta_1\delta_3 x - \delta_2\delta_3 x$, assuming pure lexicographical ordering on Θ with $\delta_1 > \delta_2 > \delta_3$. Then, P is of rank $\delta_1\delta_2 x > \mathrm{lm}\,P$ with respect to Σ. If P is the S-polynomial associated to a syzygy between elements of Σ, then the rank of P is less than or equal to the rank of the syzygy. We can further notice that if P is of rank M, Q of rank N, then $Q\,P$ is of rank at most $N\,M$, and that $\theta\,P$ is of rank at most $\theta\,M$.

THEOREM 5. *G is a standard basis of the differential ideal $\mathcal{I}$ iff G generates $\mathcal{I}$ and all the S-polynomials associated to the set of essential syzygies between elements of G are reduced to 0 by G.*

PROOF. $\Longrightarrow$ is obvious since S-polynomials are in $\mathcal{I}$.
The reciprocal is the consequence of the following more precise theorem. ∎

THEOREM 6. *Let M be a monomial, Σ be set of polynomials, such that all S-polynomials associated to the set of essential syzygies between elements of Σ of rank less than or equal to M are reduced to 0 by Σ. Then, if P is of rank less than or equal to M with respect to Σ, P is reduced to 0 by Σ.*

PROOF. Suppose it is not so. Among the P of minimal rank N which do not satisfy the conclusion, we choose one with smallest r in formula (1) of def. 3. The integer r is greater than 1. If not, P would be reduced to 0 by P_1. Now, we may decompose the sum (1) in two parts, e.g. $P = R_1 + R_2$ with $R_1 = Q_1\,\theta_1\,P_1$ and $R_2 = \sum_{i=2}^{r} Q_i\,\theta_i\,P_i$. Obviously, R_1 and R_2 need to be reducible, for they admit a decomposition (1) with a sum of at most $r-1$ polynomials with leading monomials at most N. This implies that R_1 and R_2 have the same leading monomial and opposite leading coefficients: if not P would be reducible.

We first prove that r is greater than 2. If $r = 2$, the polynomial $P = Q_1\,\theta_1\,P_1 + Q_2\,\theta_2\,P_2$ is the product of a S-polynomial, by a non zero element of $\mathcal{F}$. Without loss of generality we may suppose it is a S-polynomial. If this syzygy is essential, P is reducible: a contradiction. If not, suppose Q_1 and Q_2 are not minimal. They admit a proper common factor L, and P/L is of rank smaller than N, so that it is reducible and so is P: another contradiction.

The last case is when there exists a syzygy (U, V) between P_1 and P_2 such that $N = \mathrm{lm}\,\vartheta\,U = \mathrm{lm}\,\vartheta\,V$ for $\vartheta \neq 1$. The rank of (U, V) is less than N, so that the S-polynomial S associated to (U, V) is reduced to 0. This implies that the rank of ϑS is $\vartheta \mathrm{lm} S$, strictly less than N. Now, we may develop:

$$\vartheta\,S = a\,P + \text{a sum (1) of rank less than } N,$$

where $a \in \mathcal{F}$ $a \neq 0$. Hence P is of rank less than N: a final contradiction to $r = 2$.
Using lemma 2.9, we may now decompose R_2 as a sum (1) $\sum_{i=1}^{s} Q'_i\,\theta'_i\,P'_i$, with

$$\mathrm{lm}(Q'_i\,\theta'_i\,P'_i) > \mathrm{lm}(Q'_j\,\theta'_j\,P'_j)\ i < j.$$

Let $T = Q_1\,\theta_1\,P_1 + Q'_1\,\theta'_1\,P'_1$, R_1 and R_2 having opposite leading terms $\mathrm{lm}T < N$. Furthermore $r > 2$ implies that T is reducible, so that T is of rank less than N. If we write P as $T + \sum_{i=2}^{s} Q'_i\,\theta'_i\,P'_i$, we conclude that P is of rank less than $N = \mathrm{rank}\,P$. ∎

The main idea is very general and follows a scheme for the proof of analogous theorems in other generalizations of standard bases (see [O3] where the proof of prop. 2.1.13 is very similar).

1.5. Completion process

We now have enough material for investigating a completion process. The first step is to build, or rather to enumerate a set of essential syzygies. Differential syzygies between elements of Σ are algebraic syzygies between elements of $\Theta\,\Sigma$. So we can use the criteria detecting unuseful syzygies valid in the algebraic case. We will mostly use two of them, as an illustration.

Criterion 1. If $(M\,\theta\,P, N\,\tau\,Q)$ is an essential syzygy such that $M = \mathrm{lm}\,\tau\,Q$, then the associated S-polynomial is reduced to 0 by the set $\{P, Q\}$. ∎

Corollary 1. *If P and Q are polynomials whose leading monomials are linear, i.e. are mere derivatives $\theta\,x_i$ and $\tau\,x_j$, then if $x_i \neq x_j$ all syzygies between P and Q are reduced to* 0 *by $\{P, Q\}$. If $x_i = x_j$, then we only have to consider the syzygy $(\tau'\,P, \theta'\,Q)$, where τ' and θ' are such that $\tau'\,\theta = \theta'\,\tau = \mathrm{gcd}(\theta, \tau)$.* ∎

Criterion 2. If $P, Q, R \in \Sigma$, $S = (U, V)$ is an algebraic syzygy between $\theta\,P$ and $\tau\,Q$, $\mathrm{lm}\,\vartheta R$ divides the rank of S and the algebraic syzygies between $\theta\,P$ and ϑR, $\tau\,Q$ and ϑR are both reduced to 0 by Σ, then S is reduced to 0 by Σ. ∎

Criterion 3. If some derivative $\theta\,P$ is reduced to 0 by Σ, no syzygy involving a derivative $\tau\,\theta\,P$ needs to be considered. ∎

This simply rephrases well known results for algebraic standard bases (see [Bu]). More details on this mater may be found in [O3].

In the following completion process, G is the list which tends to a standard basis as the process goes. It will be indeed a standard basis if it stops. L_1 is the list of polynomials or derivatives of polynomials already considered, and L_2 is the list of newly appeared polynomials or derivatives, which should be used to try new syzygies. L_3 is the list of polynomials coming from the reduction of S-polynomials.

We suppose that *buildSyz*(L_1, L_2) is a procedure which returns all algebraic syzygies between two derivatives in the list L_2, or a derivative in L_1 and one in L_2; it uses criteria 1 and 2 to discard useless syzygies, when possible. The procedure *isRed(S)* returns P if the syzygy corresponds to the algebraic reduction of the derivative P and 0 otherwise.

We can also use cor. 1 to test if there is no more syzygies to consider. Except if the ideal is [1], this is the only way I know to reduce to a finite set of syzygies—we may imagine cases where the basis is finite and there is still an infinite number of syzygies to consider. Indeed the main example of ideals with finite standard bases are linear ones (see [Car cor. 5 p. 138]).

The procedure *linTestY*(L_1, L_2) returns *true* if the two following conditions are satisfied:

a) there is no more syzygies between elements of L_2 to consider, using cor. 1,

b) the leading derivatives of polynomials in L_2 are all strictly greater than the derivatives appearing in the leading monomials of polynomials in L_1.

Of course, we are sometimes lucky enough to build a finite standard basis *and* finish the completion process even in non-linear cases (see bellow ex. 6.5).

COMPLETION PROCESS

```
completionProcess(Σ) ==
  -- First suppress 0 and remove duplicate polynomials
  Σ := removeDuplicates delete(0, Σ)
  -- If there is a constant polynomial it is finished
  for P ∈ Σ repeat if P ∈ ℱ then return [1]
  G := Σ; L₁ := Σ; L₂ := Σ; L₃ := []
  while L₂ ≠ [] repeat
  -- We use cor. 1 to test if all remaining syzygies may be discarded
    if linTest(L₁, L₂) then return G
    -- We construct new syzygies between "old" polynomials in L₁ and "new" ones in L₂,
    -- or two new polynomials in L₂
    lSyz := buildSyz(L₁, L₂)
    for S ∈ lSyz repeat
      -- If the syzygy is the algebraic reduction of a derivative,
      -- all syzygies involving this derivative may be removed
      P := isRed(S); delete(P, G); delete(P, L₁); delete(P, L₂)
      if (R := reduction (sPol(S), L)) ≠ 0 then
        -- If non-zero, the reduction of the S-polynomial is kept in L₃
        L₃ := cons(R, L₃)
        -- If R ∈ ℱ it is finished
        if R ∈ ℱ then return [1]
    G := append(G, L₃)
    -- Derivatives already considered are appended to L₁
    L₁ := removeDuplicates append(L₁, L₂)
    -- New polynomials coming from the reduction of S-polynomials
    -- and new derivatives are collected in L₂
    L₂ := append(L₃, [δ P|(δ, P) ∈ Δ × L₂])
    L₃ := [] output(G)
  G
```

THEOREM 2. *If the process stops it returns a minimal standard basis G of Σ. Otherwise, let G_i denote the set of polynomials, which is returned by the process at the end of the i^{th} loop, then:*

a) $G = \bigcup_{i=1}^{\infty} G_i$ is a standard basis of Σ,

b) $G' = \bigcap_{i=1}^{\infty} \bigcup_{j=i}^{\infty} G_j$ is a minimal standard basis.

PROOF. At the beginning, $G = \Sigma$, so G generates $[\Sigma]$. During the process, if a polynomial is removed from G, then its reduction is added to G. So G still generates $[\Sigma]$. In both cases, all the S-polynomials coming from syzygies between elements of G, which are not thrown away using the criteria are reduced to 0 by G, so that is a standard basis using theo. 4.5.

For the same reason, $\bigcup_{j=i}^{\infty} G_j$ is a standard basis for all i, so that G' is also a standard basis. As a polynomial $P \in G'$ is irreducible by $G' \setminus \{P\}$, G' is minimal. ∎

REMARK 3. If we use an orderly ordering, or a ordering which respects the weight, we can modify this process to make it stop if there is no more syzygies to compute, with order or weight less than or equal to a given integer.

If think a few words are necessary to stress on the difference on the completion process given there, and the approach in [Car]. G. Carrá-Ferro proceeds by repeated computations of algebraic standard bases, so that the same work may be done many times. We only have here one process based on reduction of differential syzygies, which do not appear in her paper.

This allows sometimes to prove we have secured a finite basis, simply because the process stops (ex. 6.5 bellow), as she needs in all cases to rely on some a priori mathematical knowledge. Of course, those improvements are far to solve everything.

1.6. Examples

Before considering examples, first a few remarks.

REMARK 1. The completion process only uses the operations of the ground field, so that the polynomials in the standard basis have coefficients in the subfield generated by the coefficients of the input polynomials.

REMARK 2. If $\mathcal{I} = [P_1, \ldots, P_r]$, where the P_i are homogeneous, the standard basis, which is the limit of our construction process will be homogeneous, as well as the reduced standard basis of $\mathcal{I}$. The same apply with isobaric polynomials, if all their coefficients are constants. In such cases, the weight, or degree of the polynomials in any basis cannot be less than the minimal weight or degree of the generators. So, considering a finite set Σ of isobaric polynomials with constant coefficients, we only have to run the completion process up to $\mathrm{wt}\, P$ in order to test if P belongs to $[\Sigma]$.

REMARK 3. Suppose we are given an ordinary differential ideal generated by a system of state or pseudo state equations :

$$x_{1,(r_1)} = P_1(x_{1,(r_1-1)}, \ldots, x_1, \ldots, x_{n,(r_n-1)}, \ldots, x_n)$$

$$\vdots$$

$$x_{n,(r_n)} = P_n(x_{1,(r_1-1)}, \ldots, x_1, \ldots, x_{n,(r_n-1)}, \ldots, x_n).$$

For any orderly ordering $\{x_{i,(r_i)} - P_i\}$ is already the reduced standard basis of the generated ideal, and the procedure given above will stop. It it also a characteristic set.

EXAMPLE 4. We consider the ideal $\mathcal{I} = [x^2]$ already given in [Car], using the same ordering as in example 4.2. RITT has shown that $(u')^{2p-1}$ belongs to $[u^p]$, so that for all r, $x_{(r)}^q \in \mathcal{I}$ for some integer q, which is greater than 1, using remark 2 above. Furthermore, $x_{(r)}^q$ can only be reduced by a polynomial in the basis with leading monomial $x_{(r)}^s$ $s \le q$. As $x_{(r)}^s$ is the smallest monomial of weight $r\, s$, it is in the reduced basis. So $[x^2]$ has no finite standard basis.

This shows that standard bases may be actually infinite, and even worse that it may be indeed the general case, for this example is very simple.

EXAMPLE 5. We now consider $\mathcal{I} = [P]$, where $P = x^2 + x + 1$. The first syzygy which appears is $(x'\, P, x\, P')$. The associated S-polynomial is $x\, x' + 2\, x'$ which is reduced to $3/2\, x'$, using P'. We add x' to the basis. P' is reduced to 0 by x'. Using crit. 3, all syzygies involving $P^{(s)}$ $s \leq 1$ may be discarded. P and x' are mutually totally irreducible, and using crit. 1, there is no syzygy involving only x'. Hence, the reduced standard basis of $\mathcal{I}$ is finite and equal to $\{x^2 + x + 1, x'\}$. In our process, P' is deleted from L_2. The only polynomial in L_2 is x', and $L_1 = \{P\}$. So the process stops using *linTest*.

As shown by this example there also exist non-trivial ideals with finite standard bases, *which may be found in a finite number of steps by our completion process.*

Standard bases are often used to perform elimination of a set of variables. If we are lucky enough to secure a finite standard basis for a suitable ordering, this also works in the differential case.

PROPOSITION 6. *Let $\mathcal{I}$ be a differential ideal of $\mathcal{F}\{X\}$, Y a subset of X. Using lemma 2.5, we take any ordering $<$ on monomials and build a new ordering $\prec$ by considering first the degree of polynomials in the variables Y. If G is a standard basis of $\mathcal{I}$ for $\prec$, then the subset $G' = \{P \in G | \operatorname{lm} P \in \mathcal{F}\{X \setminus Y\}\}$ is a standard basis of $\mathcal{I} \cap \mathcal{F}\{X \setminus Y\}$.*

PROOF. Due to the properties of $\prec$, all polynomials in G' are in $\mathcal{F}\{X \setminus Y\}$, and polynomials in this subring cannot be reduced by the elements of $G \setminus G'$. So a polynomial in $\mathcal{F}\{X \setminus Y\}$ is in $\mathcal{I}$ iff it is reduced to 0 by G'. We conclude using th. 4.5. ∎

2. Application to birational mappings

2.1. A bound on the order of the inverse

We consider here a rational differential mapping $f : \mathbf{A}^n_{\mathcal{F}} \mapsto \mathbf{A}^n_{\mathcal{F}}$, defined by n differential fractions $f_1, \ldots, f_n$ in $\mathcal{F}\langle x_1, \ldots, x_n \rangle$. We will develop algorithmic methods to test whether f admits a rational inverse and to find it.

In the purely algebraic case, there is a theorem, that allows to bound the degree of f^{-1} knowing the degree of f. Its exact origin is not known, but a proof, due to O. GABBER may be found in [Ba]. Following the definition in [Ba], the degree of f is the maximal degree of polynomials P_i and $Q_1 \cdots Q_n$ if f is defined by the fractions P_i/Q_i.

THEOREM 1. *Let k be an algebraic field of arbitrary characteristic, $f : \mathbf{A}^n_k \mapsto \mathbf{A}^n_k$ be a birational mapping of degree d, then $\deg f^{-1} \leq (deg\ f)^{n-1}$.* ∎

Our aim is to prove an analogous theorem for differential birational mappings. The proof of Gabber uses Bézout's theorem. In the differential case, we can substitute to it th. 1.1.11, which Ritt called indeed a differential analog of Bézout's theorem. The analogy is in fact very strong, for despite a few more technicalities due to the differential stuff, the proof mostly follows the algebraic one.

DEFINITION 2. *The order of a rational differential mapping is the maximal order of the fractions that define it.*

This definition does obviously not depend on the choice of coordinates.

DEFINITION 3. *Let P be an irreducible differential polynomial. Using some admissible ordering on derivatives, we denote by υ_P the leading variable of P. The initial of P will be the leading coefficient of P, considered as a polynomial in $\mathcal{F}[\nu < \upsilon_P][\upsilon_P]$, and the separant of P is the polynomial $\frac{\partial P}{\partial \upsilon_P}$.*

PROPOSITION 4. *Let $P \in \mathcal{F}\{X\}$ be irreducible, the set $\{Q \in \mathcal{F}\{X\} | \exists (a,b) \in \mathbf{N}^2 \; Q\, S_P^a \mathcal{I}_P^b \in [P]\}$ is a prime ideal, which is a component of $\{P\}$. It is called the general component of P.*

PROOF. See [Ko]. ∎

Lemma 5. Let P be an irreducible polynomial of order r in $\mathcal{F}\{X\}$, V the variety defined by the general component of P, $H_1, \ldots, H_{n-1}$ be generic hyperplanes of $A^n_{\mathcal{F}}$, i.e. varieties defined by polynomials $L_i = \left(\sum_j^n \epsilon_{i,j}\, x_j\right) - \epsilon_{i,0}$, where the $\epsilon_{i,j}$ are generic over $\mathcal{F}$. Then $V \cap \bigcap_{i=1}^{n-1} H_i$ is an irreducible variety of differential type $m-1$ and of typical differential dimension r over $\mathcal{F}\langle\epsilon\rangle$.

PROOF. There is a characteristic set Σ of $\bigcap_{i=1}^{n-1} H_i$ for some orderly ordering, with $x_n > \cdots > x_1$, which is of the form $\{x_2 - a_2 x_1 - b_2, \ldots, x_n - a_n x_1 - b_n\}$. We can reduce P by Σ by replacing in P x_i by $a_i x_1 + b_i$. The result of this reduction is an irreducible polynomial $S(x_1)$, of the same order as P. We claim that $\{S, x_n - a_n x_1 - b_n, \ldots, x_2 - a_2 x_1 - a_2\}$ is a characteristic set of the prime ideal defining $W = V \cap \bigcap_{i=1}^{n-1} H_i$. This is true, using [Ko chap. IV § 9 lemma 2 p. 167 and discussion of Problem (a) p. 169–170], because S is irreducible in $\mathcal{F}\langle\epsilon\rangle$ and the other polynomials are all absolutely irreducible.

From the proof of [Ko chap. II § 12 th. 6 p. 115], we deduce that $\omega_V(r) = \binom{r+m}{m} - \binom{r+m-\operatorname{ord} P}{m}$. By an elementary calculation, we can see that the type of W is $m-1$ and its typical differential dimension $\operatorname{ord} P$. ∎

Dealing with a rational mapping, we denote by $f\,V$ the Zariski closure of the set theoretical image $f(V)$. Any generic point in $f\,V$ is obviously in the set theoretical image.

THEOREM 6. *Let $\mathcal{F}$ be a differential field of characteristic zero with set of derivations $\Delta = \{\delta_1, \ldots, \delta_m\}$, $f : A^n_{\mathcal{F}} \mapsto A^n_{\mathcal{F}}$ be a birational differential mapping, then* $\operatorname{ord} f^{-1} \le n \operatorname{ord} f$.

PROOF. Take generic hyperplanes $H_0, H_1, \ldots, H_{n-1}$ over $\mathcal{F}$ in $A^n_{\mathcal{G}}$. $f\,H_0$ is an irreducible variety which is the general component of an irreducible polynomial P of order $\operatorname{ord} f^{-1}$. Indeed, let H_0 be defined by the linear polynomial L_0 as in lemma 5, and R_i/S_i be the fractions defining f^{-1}, then, dividing the numerator of $L(R/S)$, considered as a polynomial in the $\epsilon_{i,j}$, by its content in $\mathcal{F}\{X\}$, we secure a suitable polynomial.

So, using the lemma, $f\,H_0 \cap \bigcap_{i=1}^{n-1} H_i$ is an irreducible variety of differential type $m-1$ and typical dimension $\operatorname{ord} f^{-1}$ over $\mathcal{G}$. Let η be a generic zero of that variety.

We now consider the extension $\mathcal{G}\langle f^{-1}\,\eta\rangle$. It is $\mathcal{G}$-isomorphic to $\mathcal{G}\langle\eta\rangle$, for f is birational. So using [Ko chap. II § 12 prop. 15 p. 117], $\omega_{\eta/\mathcal{G}}(r-h) \le \omega_{f^{-1}\,\eta/\mathcal{G}}(r) \le \omega_{\eta/\mathcal{G}}(r+h)$, for some integer h. So those extensions have the same type and the same typical dimension $\operatorname{ord} f^{-1}$.

Using birational equivalence, $f^{-1}\,\eta$ is a generic point of the irreducible variety $V = H_0 \cap \bigcap_{i=1}^{n-1} f^{-1}\,H_i$. Consider the set of polynomials

$$\Sigma = \{L_0, \operatorname{denom} L_i(P/Q)\ 1 \le i \le n-1\},$$

where L_i is a linear equation defining H_i, and $f_i = P_i/Q_i$. The set $\{T \in \mathcal{F}\{X\} | \exists a \in \mathbf{N}^n\ T \prod Q_i^{a_i} \in [\Sigma]\}$ is the prime ideal defining V (this is almost the situation of th. 2.1). This ideal is then a component of $\{\Sigma\}$, which is defined by a set of equations of maximal order $\operatorname{ord} f$. We can now apply theo 1.1.11 to show that $\operatorname{ord} f^{-1} \le n \operatorname{ord} f$. ∎

2.2. Algorithms

We still denote by P_i and Q_i the numerator and denominator of the fractions f_i

THEOREM 1. *Let $f_1, \ldots, f_p$ be rational differential fractions in $\mathcal{F}\langle X\rangle$. Then, the ideal*

$$\mathcal{J} = [P_i(x) - Q_i(x)\,T_i\ 1 \le i \le p; Q_1(x) \cdots Q_p(x)u - 1]_{\mathcal{F}\{x,T,u\}}$$

is prime. $\mathcal{J} \cap \mathcal{F}\{x, T\}$ is the ideal defining the graph of the mapping $f: A^n_{\mathcal{F}} \mapsto \mathbf{A}^p_{\mathcal{F}}$ induced by the f_i. A fraction U/V is in $\mathcal{F}\langle X\rangle$ iff there exists in $\mathcal{J}$ a polynomial of the form $S(T)U(x) - R(T)V(x)$ such that $S(T) \notin \mathcal{J}$. Furthermore, $U/V = (R/S)(f)$.

PROOF. The proof is the same as in the algebraic case (See [SS], or [O1]). It may be found in details in [O3]. ∎

By luck, some results of commutative algebra remain true, without any modification, in the differential case!

COROLLARY 2. *The mapping f is birational iff $p = n$ and for all $x_i \in X$ there exists in $\mathcal{J}$ a polynomial of the form $S_i(T)\,x_i - R_i(T)$, where $S_i \notin \mathcal{J}$. In this case, the fractions R_i/S_i define f^{-1}.* ∎

COROLLARY 3. *There exists an algorithm using a standard basis computation to test if f is birational and find its inverse.*

PROOF. Using classical arguments on orderings (see [O1]), we know that polynomials of the wanted form will appear during the computation of the reduced standard basis of $\mathcal{J}$, for an ordering which eliminates u and then X.

Let Σ be the set of generators of $\mathcal{J}$. Using th. 1.6, $S_i(T)\,x_i - R_i(T) \in \mathcal{F}(\Theta_{n\operatorname{ord} f}\Sigma)$, so that we have no use to consider syzygies involving polynomials of order greater than $(n+1)\operatorname{ord} f$. We can simply compute an algebraic standard basis of the ideal $\mathcal{J}' = (\Theta_{n\operatorname{ord} f}\Sigma)$, or use a slightly modified version of the procedure given above by discarding derivatives of order greater than $(n+1)\operatorname{ord} f$ which makes it an algorithm. ∎

THEOREM 4. *If $f_1, \ldots, f_p$ are rational differential fractions equal to P_i/Q_i, then the ideal*

$$\mathcal{I} = [Q_i(y)P_i(x) - P_i(y)Q_i(x)\ 1 \le i \le n;\ u\operatorname{lcm}(Q_1(x)\ \cdots\ Q_i(x)) - 1]_{\mathcal{F}\langle f\,y\rangle[x,u]}$$

is prime. A fraction $R/S \in \mathcal{F}\langle x\rangle$ belongs to $\mathcal{F}\langle f\rangle$ iff $R(x) - \frac{R(y)}{S(y)}S(x)$ belongs to $\mathcal{I}$.

PROOF. The proof in the differential case is exactly similar to the algebraic one, which may be found in [O1]. A detailed proof is given in [O3] ∎

We need to remark that $\mathcal{I}$ is prime only as an ideal in $\mathcal{F}\langle f(y)\rangle[x,u]$. For example $[x^2-y^2]_{\mathcal{F}\langle y^2\rangle[x]}$ is prime, but of course $[x^2-y^2]_{\mathcal{F}\langle y\rangle[x]}$ is not.

COROLLARY 5. *Let $f\colon \mathbf{A}^n_{\mathcal{F}} \mapsto \mathbf{A}^n_{\mathcal{F}}$ be a rational differential mapping defined by $f_1,\ldots,f_n$ as above, then f is birational iff $\forall\, 1 \le i \le n\ x_i - y_i \in \mathcal{I}$.*
Moreover, the rank of $x_i - y_i$ over the generating polynomials of $\mathcal{I}$, with respect to some orderly ordering, is of order less than or equal to $(n+1)\operatorname{ord} f$.

PROOF. The first part is immediate from the theorem. The second is a consequence of theo. 1.6. ∎

This result gives another algorithm to test if f is birational. Indeed, we only have to compute the standard basis of $\mathcal{I}$ up to order $(n+1)\operatorname{ord} f$, and test if $x_i - y_i$ reduces to 0. But under this form, we have lost the expression of the inverse and still have no control of the degree of computations, without a bound on the degree of f^{-1}.

Denote by Σ the set of generators of $\mathcal{I}$, by r the bound $(n+1)\operatorname{ord} f$, and by X' the set $X \cup \{u,v\}$ We compute a standard basis of $\mathcal{I}_i = [\Sigma;\ v(x_i-y_i)-1]_{\mathcal{F}\langle f\, y\rangle[X']}$. f is birational iff $\mathcal{I}_i = [1]$ for all i. Still using theo. 1.6, this means that

$$1 \in (\Theta_r\,\Sigma \cup \{v(x_i-y_i)-1\})_{\mathcal{F}(\Theta_r f(y))[\Theta_r X']}\,.$$

So we only have to consider $N = O\left((n+2)((n+1)\operatorname{ord} f)^m\right)$ derivatives. Using the effective nullstellensatz of KOLLÁR, we may bound the degree of intermediate computations by $d = (\deg f)^N$. Using a classical argument, we may reduce to the triangulation of a linear system of size at most $M \times (n+2)M$, where $M = O\left((\deg f)^{N^2}\right)$ is the maximal number of monomials. The coefficients are in $\mathcal{F}\{y\}$, and of degree $\deg f$ at most. The number of elementary operations in $\mathcal{F}[y]$ is polynomial in $(n+2)M$. If we use the method of BAREISS, the intermediate coefficients are minors of the matrix, so that their degree may be bounded by $D = M \deg f$ and their size by $S = O\left(D^N\right)$. The cost of any elementary operation in $\mathcal{F}[y]$ in term of elementary operations in $\mathcal{F}$ is polynomial in S. We get then the following theorem.

THEOREM 6. *We can test that f is birational with a complexity in elementary operations in $\mathcal{F}$ polynomial in $(n+2)MS$, i.e. polynomial in*

$$O\left((n+2)(\deg f)^{(n+2)^3((n+1)(\operatorname{ord} f))^{3m}}\right).$$

∎

Of course, we cannot use exactly the completion process described above to prove this theorem, because we would not be able to control the size of coefficients.

3. Conclusion

By itself, the definition of differential standard bases introduced here provides puzzling algorithmic and combinatoric problems. For example the enumeration of essential syzygies is non trivial, and one could ask whether there exists a more efficient way than trying all algebraic syzygies between derivatives.

The problem remains open of finding a satisfactory method to answer the membership problem for differential ideals. A careful study of the structure of differential ideals with finite, or infinite bases could be an inspiration to develop better and always finishing methods. But one of the main issues would be to provide an effective differential nullstellensatz, i.e. if $[P_1, \ldots, P_k] = [1]$, $\operatorname{ord} P_i \leq e$, $\deg P_i \leq d$ to secure a bound $r(n, m, k, e, d)$ such that $(\Theta_r P) = (1)$, of which we would deduce many results of complexity using differential standard bases computations.

4. References

[Ba] H. BASS et al. *The jacobian conjecture: reduction of degree and formal expansion of the inverse*, Bulletin of the A.M.S. vol. 7, n° 2, 1982.

[Bu] B. BUCHBERGER, *A criterion for detecting unecessary reductions in the construction of Groebner bases*, proceedings of EUROSAM'79, Marseille, Lect. Notes in Computer Science 72, 2–31, Springer Verlag, 1979.

[Car] G. CARRA'-FERRO, *Gröbner Bases and Differential Ideals*, proceeding of AAECC'5, Lect. Notes in Computer Science 356, 129–140, Spinger Verlag, 1987.

[Cas] F. CASTRO, *Théorèmes de division dans les opérateurs différentiels et calculs des multiplicités*, Thèse de troisième cycle, Université Paris VII, 19 Octobre 1984.

[Ch] CHOU Shang-Ching, *Mechanical geometry theorem proving*, D. Reidel pub. co., 1988.

[D] Sette DIOP, *Théorie de l'élimination et principe du modèle interne en automatique*, thèse de doctorat, université Paris-Sud, 1989.

[Ja] M. JANET, *Sur les systèmes d'équations aux dérivées partielles*, Journ. de Math. (8$^{\text{e}}$ série), tome III, 1920.

[Ka] I. KAPLANSKY, *An introduction to differential algebra*, Hermann, Paris, 1957.

[KM] Deepak KAPUR and Klaus MADLENER, *A Completion Procedure for Computing a Canonical Basis of a k-Subalgebra*, Computers and Mathematics, E. Kaltofen and S. M. Watt editors, Springer, 1989.

[Ko] E. R. KOLCHIN, *Differential algebra and algebraic groups*, Academic Press, 1973.

[Koll] J. KOLLÁR, *Sharp effective nullstellensatz*, J. Am. Math. Soc. 1, (963-975), 1988.

[O1] F. OLLIVIER, *Inversibility of rational mappings and structural identifiability in automatics*, proc. of ISSAC'89, Portland, Oregon, ACM Press, 1989.

[O2] F. OLLIVIER, *Canonical bases: relations with standard bases, finiteness conditions and application to tame automorphisms*, to appear in the proceedings of MEGA'90, Castiglioncello.

[O3] F. OLLIVIER, *Le problème de l'identifiabilité : approche théorique, méthodes effectives et étude de complexité*, Thèse de Doctorat en Sciences, École Polytechnique, Juin 1990.

[P1] J. F. POMMARET, *Differential Galois theory*, Gordon and Breach, New-York, 1983.

[P2] J. F. POMMARET, *Effective method for systems of algebraic partial differential equations*, preprint, 1989.

[R1] J. F. RITT, *Differential equations from the algebraic standpoint*, A.M.S. col. publ. vol. XIV, 1932.

[R2] J. F. RITT, *Differential algebra*, A.M.S. col. publ. vol. XXXIII, 1950.

[RS] L. ROBBIANO and M. SWEEDLER, *Subalgebra Bases*, preprint, Cornell Univ., 1989.

[S] A. SEIDENBERG, *An elimination theory for differential algebra*, Univ. California Publications in Math., (N.S.), 3, n° 2, 31–65, 1956.

[SS] D. SHANNON and M. SWEEDLER, *Using Groebner bases to determine algebra membership, split surjective algebra homomorphisms and determine birational equivalence*, preprint 1987, appeared in J. Symb Comp. 6 (2-3).