GENERALIZED STANDARD BASES WITH APPLICATIONS TO CONTROL

François OLLIVIER
Équipe de Calcul Formel, GAGE
École Polytechnique, F-91128 PALAISEAU CEDEX (France)
URA CNRS n° 169
ollivier@ariana.polytechnique.fr

Februar 1991

Abstract: We illustrate the use of some generalizations of standard bases in control theory by providing an algorithm to test the identifiability of any rational algebraic parametric model given by state equations, or more generally by a characteristic set.

The first part is conceived as an introduction to standard bases and generalized standard bases, hopping it would be comprehensible for people unfamiliar with the subject. In the same spirit, we provide some notions of differential algebra needed to describe the algorithmic methods.

Some simple examples, computed by hand, are provided as an illustration.

Keywords: Standard bases, canonical bases, characteristic sets, computer algebra, differential algebra, identifiability.

1. Introduction

The interest of control theorists in computer algebra began more than ten years ago, due to the need of solving mathematical problems which were out of reach of pure numerical computations. Since then, they have contributed to the development of many aspects of computer algebra, such as the manipulation of non-commutative power series,... and motivated further research on many interesting theoretical problems.

Working in effective algebra, and mostly in the formal resolution of systems of algebraic equations, I discovered identifiability in the work of WALTER, LECOURTIER and RAKSANYI and tried to develop more efficient methods to solve the particular algebraic equations appearing in some identifiability tests.

This very interesting subject led me to differential algebra and the effective resolution of differential equations, which are more and more used in control theory both as a language to express rigorously formal properties of structures, and as a tool to test them on computers (see e.g. [Fl], and [Di]).

A classical way of testing identifiability is to compute first an exhaustive summary of the structure and then to test that it is almost everywhere injective. It is well known that such summaries may be computed for linear structures, using the Markov parameters, or the transfer matrix. Other cases have been investigated (see for example WAJDA in [Wa2]), but no method were known for arbitrary rational differential structure. In [O2 chap. V], I have developed a method to find summaries for generic structures. Anyway, genericity is very difficult to test, even if we can easily provide sufficient conditions. The aim of this paper is to develop a better version of this method which applies to all cases.

Even if I can provide a few examples which may be tested by hand, I don't claim this is sufficient for practical applications. The method is somewhat intricate and clearly deserves to be simplified before we may think of an implementation. The positive aspect is that it involves almost all the generalizations of standard bases known for this moment, providing a very good example to illustrate them. So, my second aim, and perhaps the most important, is to provide a readable introduction to standard bases, and to explain why they could be useful in many problems of control theory.

Standard bases were first defined by HIRONAKA, before BUCHBERGER introduced an algorithm to compute them, relying on successive reduction of critical pairs. However, the idea is so natural that it is not a surprise if some mathematical objects, previously introduced by JANET or LEVY—both working with algebraic differential equations—have a strong flavour of standard bases.

It is indeed surprising that the notion of standard bases has been generalized to other structures, such as differential ideals or subalgebras, only a few years ago. To some extend, this may be because in most situations, generalized standard bases are infinite, a serious drawback for effective applications! But fortunately, we will see it is still possible to use them with a little more care.

2. Standard bases

We will denote by k a field of arbitrary characteristic and by A the k-algebra of polynomials in n variables $k[x_1, \ldots, x_n]$.

2.1. The main idea: linear algebra

A complete description of the main properties of standard bases would exceed the size of this short paper. My goal is to give the main ideas, in order to help understand the next sections, and to encourage the reader to study details in more substantial papers such as [Bu]. I also recommend [DST] as general introduction to the problems and methods of computer algebra.

The basic problem which may be solved using standard bases is the membership problem for ideals. Let's consider an ideal $\mathcal{I}$ of A generated by polynomials $P_1, \ldots, P_\ell$. By definition, $\mathcal{I}$ is the set of polynomials Q such that

$$(1) \qquad Q = \sum_{i=1}^{\ell} M_i P_i \; ; \; M_i \in A.$$

It is well known that the solutions of the algebraic system $P_i(x) = 0$ are also solutions of each polynomial in $\mathcal{I}$. It is often very useful to be able to test if some given polynomial Q belongs to $\mathcal{I}$; we will see examples very soon.

Suppose we know *a priori* a bound d on the degree of polynomials $M_i P_i$ in formula (1). Then, we can solve our problem by using the structure of k-vector space of A. If Q is in $\mathcal{I}$, it should belong to the subspace generated by polynomials of the form

$$(2) \; x_1^{\alpha_1} \cdots x_n^{\alpha_n} P_i \; ; \; i = 1, \ldots, n, \; \alpha_1 + \cdots + \alpha_n + \deg P_i \leq d.$$

This is easily tested using classical linear algebra.

It may be shown that we can actually compute a bound d, depending only of $\deg Q$, $\deg P_1$, $\deg P_\ell$; but it is really huge in general. However, we will investigate this process a little closer... First of all, we need to work in some basis for our calculations. It is convenient to use the natural basis provided by monomials of degree at most d. We also need to chose an ordering for those monomials.

We would like that this ordering was in some way "natural" too. There are many possible choices, but if we remark that monomials form a *monoid* for multiplication (i.e. a semi-group with identity element), we want that our ordering was compatible with this structure, meaning that

A) 1 is the smallest monomial,

B) if $m_1 < m_2$, then $m_3 m_1 < m_3 m_2$.

An immediate solution is the so-called lexicographical ordering, defined by comparing first partial degrees in the first variable, then in the second, and so on. E.g., $x_1 x_2^3 > x_1 x_2^2 x_3^2$.

We can then form a matrix M, whose columns represent polynomials (2) generating our vector space. We can now reduce to a new matrix N, corresponding to a new set of polynomials with leading monomials all different, by performing only permutations and linear combinations of columns.

Example 1. — Let us consider polynomials $P_1 = x_1^2 - x_2^2$, $P_2 = x_1 x_2$ and $P_3 = x_1^2 x_2$. We want to know if $Q = x_1^3 + x_2^3$ belongs to the ideal generated by P_1 and P_2. The matrix M corresponds to polynomials P_1, P_2, $x_1 P_1$, $x_2 P_1$ $x_1 P_2$, $x_2 P_2$ and P_3, the monomials appearing in decreasing order: x_1^3, $x_1^2 x_2$, x_1^2, $x_1 x_2^2$, $x_1 x_2$, x_1, x_2^3, x_2^2, x_2, 1.

$$M = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} . \quad \begin{matrix} x_1^3 \\ x_1^2 x_2 \\ x_1^2 \\ x_1 x_2^2 \\ x_1 x_2 \\ x_1 \\ x_2^3 \\ x_2^2 \\ x_2 \\ 1 \end{matrix}$$

We easily deduce a matrix N of the wanted shape:

$$N = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} . \quad \begin{matrix} x_1^3 \\ x_1^2 x_2 \\ x_1^2 \\ x_1 x_2^2 \\ x_1 x_2 \\ x_1 \\ x_2^3 \\ x_2^2 \\ x_2 \\ 1 \end{matrix}$$

The polynomials corresponding to non zero columns are $x_1^3 - x_1 x_2^2$, $x_1^2 x_2 - x_2^3$, x_1^2, $x_1 x_2^2$, $x_1 x_2$, x_2^3, all of them belonging to $\mathcal{I}$. To test if $Q \in \mathcal{I}$ all we need do is to search for a polynomial in our list having the same leading monomial as Q. Such a polynomial exists. If not, Q would not have been in $\mathcal{I}$. So we may subtract it from Q. We get $x_1 x_2^2 + x_2^3$. We repeat the process and get $2x_2^3$, and then 0, so that $Q \in \mathcal{I}$.

We may remark that there is a full column of zeroes in N. This is because there is a non-trivial relation between the generating polynomials $P_1, \ldots, P_3$, viz. $x_1 P_2 - P_3 = 0$. It is clear that the triangulation process also allows us to secure a basis for relations involving polynomials of degree less than d.

We only have to put this intuitive method in proper form to define actual *standard bases*.

2.2. E-sets

Having chosen an *admissible ordering*, i.e. satisfying conditions A) and B), we discovered that leading monomials should play an important role. What about the set E of leading monomials of all polynomials in some ideal $\mathcal{I}$. What does it look like? We associate to any monomial x^α the point α of $\mathbf{N}^n$.

fig. 1 fig.2

The fig. 1 describes an e-set, meaning that any multiple of a monomial in E belongs to E. The points of E with circles represent the *generators* of the e-set, for any element of E is a multiple of these monomials.

Definition 1 (Standard bases). — *We say that a subset G of an ideal E is a standard basis of $\mathcal{I}$ if the leading monomials of polynomials in G generate the e-set E.*

Suppose we know a standard basis of $\mathcal{I}$. To test whether Q belongs to $\mathcal{I}$, we may first check if its leading monomial is in E, i.e. if it is a multiple of the leading monomial M of $P \in G$. Say $P = cM + R$, and $Q = c'M'M + R'$. Then, we can reduce Q to $Q' = Q - (c'/c)M'P$. We know that $Q \in \mathcal{I}$ iff $Q' \in \mathcal{I}$. But Q' has a leading monomial strictly smaller than Q. We may repeat the process until we find a polynomial which reduces to 0, or which is irreducible, meaning that its leading monomial doesn't belong to E.

This defines the *reduction process*, and it may be proved that it actually stops, for there is no infinite and strictly decreasing chain of monomials, *using an admissible ordering*. We can also use a stronger notion of reduction, *total reductions*, which removes in some polynomial all monomials of E.

Example 2. — $Q = x_1^2 x_2^2 + x_2^2$ is reduced by $P = x_2^2 + x_2$ to $-x_1^2 x_2 + x_2^2$, but it is totally reduced to $-x_1^2 x_2 - x_2$.

The question is now to compute standard bases. We remember how we have used above a triangulation process. E.g. the matrix M above, the columns 4 and 5 were associated to polynomials with the same leading monomials, viz. $x_2 P_1$ and $x_1 P_2$. A step of the triangulation process was to compute the difference $x_1 P_2 - x_2 P_1$. What does this mean for e-sets? Consider the e-set E' generated by the leading monomials of P_1 and P_2 in fig. 2.

The monomial $x_1^2 x_2$ belongs to E_0, but it is both a multiple of the leading monomial of P_1 and P_2; moreover it is the smallest monomial sharing this property. From the point of view of reduction, this means that polynomials having this leading monomials may be reduced in two different ways, using P_1 or P_2. We may reduce $x_1 P_2$ using P_2, then we find 0, or using P_1, and then we find $x_1 P_2 - x_2 P_1 = x_2^3$. This polynomial is called the *S-polynomial* associated to P_1 and P_2. It is not in the e-set E', so that it is irreducible by P_1 and P_2. So, we must add it as a new generator. We get then an e-set E_1. This make appear two new S-polynomials, but we can check that they both reduce to 0.

What does this mean? That we have reached the end of a *completion process* and that P_1, P_2 and x_2^3 form a standard basis of $\mathcal{I} = (P_1, P_2)$, or in other words that E_1 is the e-set of $\mathcal{I}$.

We may sum up all our results in the following theorem.

Theorem 3. — *Let $\mathcal{I}$ be an ideal of A, G a subset of A, then the four following propositions are equivalent:*

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

ii) $G \subset \mathcal{I}$ and for all $P \in \mathcal{I}$, P is reduced to 0 by G, *iii)* $P \in \mathcal{I}$ *iff* P *is reduced to* 0 *by* G,

iv) G *generates* $\mathcal{I}$ *as an ideal, and all S-polynomials between elements of* G *are reduced to* 0 *by* G. ■

2.3. Canonical bases

We will now consider finitely generated k-subalgebras of A. Given a finite set of polynomials $P_1, \ldots, P_\ell$ of A they generate a subalgebra B, containing polynomials Q such that

$$Q = \sum_{i=1}^{p} c_i P_1^{\alpha_{i,1}} \cdots P_\ell^{\alpha_{i,\ell}}.$$

It is possible to extend the definition of standard bases to this new structure. We may remark that the basic idea for standard bases was to use the structure of e-set of the set of leading monomials. Now, if B is a subalgebra, the leading monomials of polynomials in B form a submonoid of the monoid of monomials. This produces the following formal definition.

DEFINITION 1 (Canonical bases). — *A subset* C *of a* k*-subalgebra* B *of* A *is said to be a canonical basis of* B *if the leading monomials of polynomials in* C *generate the whole monoid of leading monomials of polynomials in* B.

Example 2. — Consider the subalgebra $B = k[x_1, x_1^2 + x_2^2]$. Then, the leading monomials of polynomials in B are of the form $x_1^\alpha x_2^{2\beta}$, so that $\{x_1, x_2^2\}$ is a canonical basis of B.

Using this, we may recover the nice properties of standard bases, even if new definitions are more complicated. Let us first investigate reduction. We have seen for standard bases of ideals that a polynomial P was reducible by a set of polynomials S if some monomial M of P was in the e-set generated by leading monomials of S. By analogy, we get the following definition.

DEFINITION 3 (Reduction). — *A polynomial* P *is said to be reducible by a set of polynomials* S *if a monomial* M *of* P *is in the monoid generated leading monomials of* S.

It is here convenient to use the isomorphism between the multiplicative monoid of monomials and the additive monoid $\mathbf{N}^n$ defined by the multidegree $\mathrm{mdeg} x_1^{\alpha_1} \cdots x_n^{\alpha_n} = (\alpha_1, \ldots, \alpha_n)$. If Q is reducible by $P_1, \ldots, P_m$, this means that $\mathrm{mdeg} Q = \sum_i a_i \mathrm{mdeg} Q_i$. Under the assumption that polynomials P are monic, i.e. with leading coefficient 1, Q is reduced by the P_i to $Q - c \prod_i P^{a_i}$.

It is more difficult to define S-polynomials, but we will limit ourselves to intuitive ideas. Again, a leading monomial may be obtained in two different ways, e.g. $(x_1^2)(x_2^2) = (x_1 x_2)^2$, this means there is an S-polynomial involving polynomials $x_1^2 + x_2$, $x_2^2 + 1$ and $x_1 x_2 + x_1$, viz.

$$(x_1^2 + x_2)(x_2^2 + 1) - (x_1 x_2 + x_1)^2 = -2x_1^2 x_2 + x_2^3 + x_2.$$

It may be shown that we only have a finite number of S-polynomials to consider, corresponding to a set of relations between leading monomials generating the ideal of relations between those monomials. We can then reduce those S-polynomials, and if the reduction if non zero, complete our set of generating polynomials with them. We proceed repeating this process until all S-polynomial reduce to zero.

Can we be sure that such a completion process stops? Unfortunately not, but we know that it stops iff the subalgebra admits a finite canonical basis. The trouble is that even finitely generated subalgebras may have infinite canonical bases, as shown by ROBBIANO (see [RS]).

Example 4. — Consider polynomials $x_1 + x_2$, $x_1 x_2$, $x_1 x_2^2$, and the subalgebra B they generate. We have a S-polynomial $(x_1 + x_2)(x_1 x_2^2) - (x_1 x_2)^2 = x_1 x_2^3$, this new polynomial being irreducible. Then, we have a new S-polynomial $(x_1 + x_2)(x_1 x_2^3) - (x_1 x_2)(x_1 x_2^2) = x_1 x_2^4$. Indeed the process never stops, and we have an infinite canonical basis $\{x_1 + x_2, x_1 x_2, \ldots, x_1 x_2^p, \ldots\}$.

3. Differential algebra

3.1. Differential ideals

Joseph Fels RITT, who may be considered as the creator of differential algebra, but was clearly inspired by previous works of Maurice JANET, introduced the notions of differential polynomials, differential ideals and in the same time introduced constructive methods in his proofs, which are very similar to some algorithms having proved their efficiency on modern computers.

From a purely algebraic standpoint, we may regard a differential ring to be a ring with a derivation δ, i.e. an internal mapping such that $\delta(x + y) = \delta(x) + \delta(y)$, and $\delta(xy) = \delta(x)y + x\delta(y)$. A differential field will be a field, which is a differential algebra, e.g. $\mathbf{Q}$ is a differential field with $\delta(x) = 0\ \forall x \in \mathbf{Q}$, and $\mathbf{Q}(x)$ is a differential field for the usual derivation.

The unknowns in algebraic polynomials may be considered as abstract names for arbitrary number, in differential algebra we can regard them as standing for functions. So, differential polynomials will be polynomials in variables $y_1, y_2, \ldots$ and their formal derivatives $x_1', x_1'', \ldots$. It is convenient to denote $x_1'', x_1^{(p)}$ by $x_{1,(2)}, x_{1,(p)}$. We will denote the set of differential polynomials over $\mathcal{F}$ in n variables by $\mathcal{F}\{x_1, \ldots, x_n\}$, $\mathcal{F}$ standing for any differential field. The quotient field of $\mathcal{F}\{x\}$, will be denoted by $\mathcal{F}\langle x\rangle$. It has a natural structure of differential field, using classical rule for the derivation of fractions. We will further denote $\mathcal{F}\{x_1, \ldots, x_n\}$ by $\mathcal{R}$.

To any set of algebraic differential equations Σ, i.e. equations of the form $P(x) = 0$ $P \in \mathcal{R}$, we may associate the differential ideal they generate, being the set of polynomials $Q <$ such that

$$Q = \sum_{i=1}^{\ell} M_i \delta^i(P_i)\ P_i \in \Sigma,\ M_i \in \mathcal{R}.$$

It is the smallest ideal $\mathcal{I}$ of $\mathcal{R}$ such that $\delta\mathcal{I} \subset \mathcal{I}$ and $\Sigma \subset \mathcal{I}$. We denote it by $[\Sigma]$. We say that a differential ideal $\mathcal{I}$ is prime if $PQ \in \mathcal{I}$ implies $P \in \mathcal{I}$ or $Q \in \mathcal{I}$.

3.2. Varieties

Considering a differential algebraic system $\Sigma \subset \mathcal{R}$, we say that $(\eta_1, \ldots, \eta_n) \in \mathcal{G}$, where $\mathcal{G}$ denotes a differential extension of $\mathcal{F}$, is a zero of Σ if $P(\eta) = 0\ \forall P \in \Sigma$. This implies that η is a zero of $[\Sigma]$. E.g., $y \in \mathbf{Q}(y)$ is a zero of $x' - 1$, it is also a zero of $x'' \in [x' - 1]$.

DEFINITION 1. — *We will say that a zero* η *of a prime differential ideal* $\mathcal{I}$ *of* $\mathcal{F}\{x_1, \ldots, x_m\}$ *is generic if* $P(\eta) = 0$ *implies* $P \in \mathcal{I}$.

Example 2. — The zero $x \in \mathbf{Q}(x)$ of $\mathcal{I} = [x'']$ is not a generic zero, for it is also a zero of $x' \notin \mathcal{I}$. The function sin is not a generic zero of $[x'' + x]$, for it is a zero of $(x')^2 + x^2 - 1$, but it is a generic zero of the prime differential ideal $[x'' + x, (x')^2 + x^2 - 1]$.

We may define the algebraic variety associated to an algebraic ideal $\mathcal{I}$ in A as the set of zeroes of $\mathcal{I}$ in K^n, where K is the algebraic closure of k. Considering a differential field $\mathcal{F}$, we may associate to it a *universal extension* $\mathcal{U}$, being such that for all differential extension $\mathcal{F} \subset \mathcal{G} \subset \mathcal{U}$ of $\mathcal{F}$ and all differential ideal $\mathcal{I} \neq [1]$ of $\mathcal{G}\{x_1, \ldots, x_m\}$, $\mathcal{I}$ admits a generic zero in $\mathcal{U}^m$. In the following we suppose that a universal extension $\mathcal{U}$ of $\mathcal{F}$ has been chosen once and for all.

DEFINITION 3. — *The differential algebraic variety $V(\mathcal{I})$ defined by an ideal $\mathcal{I}$ of $\mathcal{R}$ is the set of zeroes of $\mathcal{I}$ in $\mathcal{U}^n$.*

A d. a. variety V is irreducible if for all variety W, $W \subset V$ implies $W = V$.

The ideal $\mathcal{I}(V)$ associated to a d. a. v. V is the set of d. polynomials P such that $P(\eta) = 0\ \forall \eta \in V$.

It may be proved that V is irreducible iff $\mathcal{I}(V)$ is prime. In the following, we will say simply variety for d. a. v., and algebraic varieties for non-differential ones.

4. Generalized standard bases in differential algebra

4.1. Standard Bases of differential ideals

Following the ideas developed above, we first need to define suitable orderings on the set of monomials of $\mathcal{R}$. We say that such an ordering is admissible if

i) $m \geq 1$,
ii) $m_1 > m_2$ implies $m_3 m_1 > m_3 m_2$,
iii) $\delta^\ell m > m\ \ell \neq 0$,
iv) $m_1 > m_2$ implies $\delta^\ell m_1 > \delta^\ell m_2\ \ell \neq 0$.

First of all, we will introduce admissible orderings restricted to the set of derivatives. A simple choice is $x_{i,(j)} < x_{i',(j')}$ if $j < j'$ or $j = j'$ and $i > i'$. We call it the derivation ordering $<_{der}$. Next, we may define an admissible ordering on monomials by considering e.g. the pure lexicographical ordering with the chosen ordering for derivatives.

Examples. — 1) The monomial $m = x_{2,(3)}^3 x_{1,(2)}^2 x_{2,(2)}$ is given with its derivatives in decreasing order for $<_{der}$. According to the lexicographical ordering, it is bigger than $x_{2,(3)}^3 x_{1,(2)} x_{2,(2)}^3$, and smaller than $x_{1,(2)}$, for $x_{1,(2)}$ is greater than the leading derivative of m, and we may consider it appears in m with degree 0.

2) We can define many others admissible orderings. For instance, if $<$ is an admissible ordering, the ordering $<_{\deg}$ defined by $m_1 <_{\deg} m_2$ if $\deg m_1 < \deg m_2$ or $\deg m_1 = \deg m_2$ and $m_1 < m_2$ is admissible.

In order to introduce standard bases, the next step is to extend the derivation to the set of monomials. This may seem impossible for e.g. $(xx')'$ is equal to $xx'' + (x')^2$, which contains two monomials. But we can easily solve this problem, for we only need a convenient formal definition, which may depend of the ordering. So, an ordering been chosen, we define $\delta(m)$ to be the greatest monomial appearing in the polynomial m'.

We call then a differential e-set a set E of monomial such that $mE \subset E$ for all monomial m and $\delta E \subset E$, and denote by $[\Xi]$ the differential e-set generated by a set Ξ of monomials. We denote by $\mathrm{m}P$ the leading monomial of P. Obviously, if $\mathcal{I}$ is a differential ideal, $\mathrm{m}\,\mathcal{I}$ is a differential e-set.

DEFINITION 3. — *A subset G of a differential ideal $\mathcal{I}$ is a standard basis if* $\mathrm{m}\,\mathcal{I} = [\mathrm{m}\,G]$.

We can reduce a polynomial Q by a set of polynomials Σ, if $\mathrm{m}\,Q \in [\mathrm{m}\,\Sigma]$. To avoid intricate details, we will describe the completion process through examples. The reader can refer to [Car], [O4], or [O2 chap. IV § 1]. for a complete exposition.

Examples. — 4) Let us consider the ideal $\mathcal{I} = [x^2 + x + 1]$. The monomial $x^2 x'$ belongs to $[x^2]$, but we may get it in two different ways: it is $x'(x^2)$ or $x\delta(x^2)$. This means we should consider the S-polynomial $x'(x^2 + x + 1) - \frac{1}{2}x(2xx' + x') = \frac{1}{2}xx' + x'$. This polynomial is reduced to $\frac{1}{4}x'$. So we consider a new set $\{x^2 + x + 1, x'\}$, and it may be proved it is now a standard basis of $\mathcal{I}$, for all the remaining S-polynomials will involve derivatives of greater order and we can neglect them, because $x' \in \mathcal{I}$.

5) We now consider $\mathcal{I} = [x^2]$. This time, the first S-polynomial to appear is $x'x^2 - \frac{1}{2}x(x^2)' = 0$. The second is $x''(x^2)' - x'(x^2)'' = -2(x')^3$ this polynomial is irreducible by x^2, so that we must add it to the basis. Continuing this process, we would discover that the basis contains a power of all derivatives $x^{(i)}$, so that the standard basis of $[x^2]$ is infinite.

4.2. Characteristic sets

Characteristic set is the oldest tool to deal with algebraic differential systems, the first explicit notion being due to RITT using the results of JANET. They have proved their efficiency to prove theorems in geometry, under the impulse of WU (see [Wu]). The main idea is to forget the set of leading monomials, and to focus on leading derivatives according to an admissible ordering.

We define the rank of a polynomial P to be $x_{i,(j)}^d$, if $x_{i,(j)}$ is the leading derivative of P, appearing with maximal degree d. If $P \in \mathcal{F}$—we cannot say it is constant!— we take $\mathrm{rk}\,P = 1$ if $P \neq 0$, and ∞ if $P = 0$. We define an ordering on ranks by taking 1 (resp. ∞) to be the smallest (resp. greatest) rank, and $x_{i,(j)}^d < x_{i',(j')}^{d'}$ if $x_{i,(j)} < x_{i',(j')}$, or $x_{i,(j)} = x_{i',(j')}$ and $d < d'$.

We have seen that using standard bases we had a reduction process to eliminate in a polynomial Q all monomials which are multiples of the leading monomials of a given polynomial P and its derivatives. Here, we would like to eliminate all monomials in Q, being a multiple of $\mathrm{rk}\,P$, $\mathrm{rk}\,P'$, and so on. We first remark that if $\mathrm{rk}\,P = x_{i,(j)}^d$, then $\mathrm{rk}\,P' = x_{i,(j+1)}$.

Consider the two polynomials $Q = x'' + x$ and $P = (x')^2 + x^2 - 1$. We remark that $\mathrm{rk}\,Q = \mathrm{rk}\,P'$, so that we would like to make x'' disappear from Q, using $P' = 2x'x'' + 2xx'$. We cannot rely on the reduction process of standard bases, but there is a wider method called pseudo-reduction. We proceed as if P' was a polynomial in one variable x'', and consider the other derivatives as simple coefficients. The leading coefficient of P' is $2x'$, we call it the *initial* $I_{P'}$ of P', and the *separant* S_P of P. Then, we can reduce Q to $S_P Q - P = 0$. In the same way, taking say $Q = (x'')^2$, and $P = x^2(x'') - 1$, we may reduce Q to $I_P Q - x''P = x''$, which is reduced to x^2 using P again.

If we cannot reduce a polynomial Q by a set of polynomial Σ, using pseudo reduction, we say that Q is irreducible by Σ. Polynomials $P_1, \ldots, P_m$, appearing in strictly increasing order, according to their rank and all mutually irreducible, are said to form a *chain*. We remark that the length of a chain is at most the number of variables. We can define an preordering on chains by taking $P_1, \ldots, P_r < Q_1, \ldots, Q_s$ if there exists $i \leq \min(r, s)$ such that

$$\begin{array}{ccc} \mathrm{rk}P_1 & \cdots & \mathrm{rk}P_{i-1} & \mathrm{rk}P_i \\ \| & & \| & \wedge \\ \mathrm{rk}Q_1 & \cdots & \mathrm{rk}Q_{i-1} & \mathrm{rk}Q_i, \end{array}$$

or if $r > s$ and

$$\begin{array}{ccc} \mathrm{rk}P_1 & \cdots & \mathrm{rk}P_s \\ \| & & \| \\ \mathrm{rk}Q_1 & \cdots & \mathrm{rk}Q_s. \end{array}$$

The spirit of this definition is that we want to compare the set of ranks which are not derivatives of the ranks of polynomials $P_i^{(j)}$ and $Q_i^{(j)}$. It is smaller if the chain becomes longer as in the second case above. We only need one more formal definition, before things may become clearer with a few examples.

DEFINITION 1. — *Let $\mathcal{I}$ be a differential ideal, we say that a chain $\mathcal{A}$ is a characteristic set of $\mathcal{I}$ if for all chain $\mathcal{B}$ of polynomials in $\mathcal{I}$ $\mathcal{A} < \mathcal{B}$.*

It may be proved that given a characteristic set $\mathcal{A}$ of a differential ideal $\mathcal{I}$, all polynomials in $\mathcal{I}$ are reduced to 0 by $\mathcal{A}$, using pseudo-reduction. But the reciprocal is false, except if $\mathcal{I}$ is prime.

Example 2. — Consider $\mathcal{I} = [P]$, with $P = (x')^2 + x^2 - 1$, and $Q = x'' + x$. It may be shown that P is a characteristic set of $\mathcal{I}$. The ideal $\mathcal{I}$ is not prime, because $x'(x'' + x) \in \mathcal{I}$, but $x' \notin \mathcal{I}$ and $x'' + x \notin \mathcal{I}$, even if P reduces Q to 0.

Now, take $\mathcal{J} = [P, Q]$, P is also a characteristic set of $\mathcal{J}$, which is a prime ideal, and this is why Q is reduced to 0 by P.

We understand the special interest of characteristic sets for prime differential ideals: they are always finite, and provide a way of solving the membership problem.

4.3. Algorithms

The next step is to build an algorithm to construct characteristic sets. The classical way, following Ritt's idea requires factorization, which is impossible without suitable hypotheses on the ground field $\mathcal{F}$, and very expensive in computation time. We provide a different approach, following an idea of D. LAZARD.

We will limit ourselves to a prime ideal $\mathcal{I}$, and further suppose we can test, using some oracle, whether a given polynomial belongs to $\mathcal{I}$—we will see soon that it is no great limitation for control theory.

The first step is to proceed by repeated reductions, as for standard bases. Suppose $\mathcal{I}$ is generated by $\Sigma = \{P_1, \ldots, P_m\}$. We first build a minimal chain C_1 among those polynomials. We reduce all polynomials in Σ, using C, and form a set S with all the non-zero remainders. If $S = \emptyset$, we stop. If not, we take $\Sigma_2 = \Sigma \cup S$, and form a new minimal chain C_2 with polynomials of Σ_2. We repeat this process until $S = \emptyset$.

At the end, we get a chain $\mathcal{A}$, which is **not** in general a characteristic set. We explain with an example how to complete the process.

Example 1. — Consider the ideal $\mathcal{I} = [P_1, P_2, P_3, P_4]$, with $P_1 = x_3(x_2')^2$, $P_2 = x_2' x_1'' - 1$, $P_3 = x_3''' - x_3''$ and $P_4 = x_3''$. We chose an ordering which respects the order of derivation and form a minimal chain $C_1 = \{P_1, P_2, P_4\}$. Obviously all polynomials are reduced to 0 by C_1. But C_1 is not a characteristic set of $\mathcal{I}$. We first check whether the initials of those polynomials belong to $\mathcal{I}$. The answer of the oracle is $x_3 \in \mathcal{I}$. So we add x_3 to Σ. Repeating then the first process, we get a chain $C_2 = \{x_3, P_2\}$, reducing all polynomials to 0. Then, no initial belong to $\mathcal{I}$. The next and final step is to check that the discriminants of our polynomials do not belong to $\mathcal{I}$. It is obvious in this case—if not just add them to Σ and continue—, so we conclude that C_2 is a characteristic set of $\mathcal{I}$.

Details of the algorithm are developed in [O2 chap. IV § 2].

Remark 2. — We can derive many information from the knowledge of a characteristic set, for example the dimension of the ideal. In the last example, we have 3 variables, and 2 polynomials in the characteristic set, so that the dimension of the ideal is $3 - 2 = 1$.

5. Differential algebraic parametric models

5.1. Definition

Here comes control theory. I hope the reader won't be disappointed by this part after all those algebraic preliminaries. We are now able to define parametric models, generalizing both models given by state equations, and input/output behaviour.

First of all, consider a system given by state equations, where the f_i and g_i are algebraic polynomials.

$$(\Sigma) \qquad \begin{cases} x_1' &= f_1(x, t, u, \theta), \\ &\vdots \\ x_n' &= f_n(x, t, u, \theta), \\ y_1 &= g_1(x, \theta), \\ &\vdots \\ y_m &= g_m(x, \theta). \end{cases}$$

We complete it with initial conditions

$$\begin{aligned} x_1(0) &= c_1(\theta), \\ &\vdots \\ x_n(0) &= c_n(\theta). \end{aligned}$$

Here t denotes the time, u the input or command vector, and θ a vector of parameters.

We can remark that for any ordering on the set of derivatives of x and y, which respects the order of derivation and such that $y > x$ Σ form a characteristic set of the prime differential ideal it generates. The idea is first to check that if P and Q are irreducible by Σ, then PQ is irreducible, and then that $\mathbf{P} \in [\Sigma]$ iff P is reduced to 0 by Σ. This implies that $[\sigma]$ is prime. So, we have a way to solve the membership problem for $[\Sigma]$.

We will now consider a different ordering, such that $x_{i,(j)} > y_{k,(\ell)}$ $\forall i, j, k, \ell$. We can build another characteristic set $\mathcal{A}$ for this new ordering:

$$\begin{aligned} &\{P_1(x_1, \ldots, x_n, y_1, \ldots, y_m, t, u, \theta), \\ &\qquad\vdots \\ &P_n(x_1, \ldots, x_n, y_1, \ldots, y_m, t, u, \theta), \\ &P_{n+1}(x_1, \ldots, x_n, y_1, \ldots, y_m, t, u, \theta), \\ &\qquad\vdots \\ &P_{n+m}(y_1, \ldots, y_m, t, u, \theta)\}. \end{aligned}$$

Using rem. 4.3.2, the dimension of $[\Sigma]$ is 0, so that we have as many polynomials in a characteristic set as we have variables. Then, if the leading derivative of P is $y_{i,(j)}$, P cannot contain a derivative $x_{i',(j')}$, because of the special ordering we use—we say it is an *elimination ordering*. This explains why $\mathcal{A}$ has such a shape.

Example 1. — Consider the model $x_1' = x_1, x_2' = -x_2, y = \frac{1}{2}(x_1 + x_2)$, with initial conditions $x_1(0) = 1, x_2(0) = 1$. Change the ordering. You may compute a new characteristic set $\{x_1 - \frac{1}{2}(y' + y), x_1 - \frac{1}{2}(y' + y), y'' - y\}$. Form the first system, we deduce $x_1'(0) = 1, x_2'(0) = -1$, and so new initial conditions $y(0) = 1, y'(0) = 0$. We may now forget the x and secure a pure input/output model.

This possibility of going from state equations to input output ones by a simple change of ordering produces the following generalization.

DEFINITION 2. — *We call an algebraic differential parametric model a system $\Sigma = \{Q_i(x, y, t.u, \theta)\ i = 1, \ldots, n + m\}$, given by differential polynomials in $\mathcal{F}\langle t, u, \theta\rangle\{x, y\}$, which form a characteristic set of a prime and zero-dimensional ideal $\mathcal{I}$.*

We take for the ground field $\mathcal{F}$ a differential field with field of constants k, e.g. $\mathbf{R}(z)$ whose field of constants is $\mathbf{R}$. We consider the differential extension such that the input vector u is *generic*, meaning that $P(u) = 0$ iff $P = 0$, the time t is a generic solution of $t' = 1$, and the parameters θ are *arbitrary constants*, i.e. generic solutions of $\theta' = 0$ other $\mathcal{F}$. Those definitions are often completed if $k = \mathbf{R}$ with the data of an open set $D \in \mathbf{R}^\ell$, of *admissible parameters*.

$\mathcal{I}$ being zero-dimensional, we may suppose with no loss of generality that the leading derivative of Q_i $i = 1, \ldots, n$ is $x_{i,(j_i)}$, and the leading derivative of Q_{n+i} $i = 1, \ldots, m$ is $y_{i,(i_{m+i})}$. So, this definition can be completed with the following.

The initial conditions of an algebraic differential model are constants $c_{i,j}(\theta, u)$ $i = 1, \ldots, n+m$, $j = 0, \ldots, j_i$, such that $Q_i(c) = 0$ and $S_{Q_i}(c) \neq 0$, for all $i = 1, \ldots, n+m$. The constants $c_{i,j}$ are taken in $\mathcal{G}\langle\theta\rangle$, where $\mathcal{G}$ denotes a differential extension of the ground field $\mathcal{F}$.

The meaning of this construction is that we can associate to such a model, and a vector of analytic input functions u, a unique power series solution with coefficient in the constant field of $\mathcal{G}$.

Examples. — 3) Consider the model $(x')^2 = x + u$, $y = x^2$, with initial conditions $x(0) = 1$, $x'(0) = \sqrt{1 + u(0)}$, $y(0) = 1$. We may recursively compute $x''(0) = \frac{1+u'(0)/(\sqrt{1+u(0)}}{2}$, $y'(0) = 2\sqrt{1 + u(0)}, \ldots$

4) Consider the simple model $x'' = (\theta_1^2 + \theta_2)x' - \theta_1^2\theta_2 x$, $(y')^2 = x'$, with initial conditions $x(0) = 2$, $x'(0) = 2\theta_1^2$, $x''(0) = 2\theta_1^4$, and $y(0) = \sqrt{2}/\theta_1$, $y'(0) = \sqrt{2}\theta_1$. We may take here $\mathcal{F} = \mathbf{Q}$, and $\mathcal{G} = \mathbf{Q}(\sqrt{2})$. This system is a chain for a ordering which respects the order of derivation, and we could check it is associated to a prime ideal. For more simplicity, we have chosen a model with no input function.

It is easily seen that initial conditions are compatible with the system. Of the first equation, we deduce $x'''(0) = 2\theta_1^6, \ldots$ leading to the formal solution: $x = \sum_{i=0}^{\infty} (2\theta_1^{2i}/i!)t^i$. We also get $y''(0) = \sqrt{2}\theta_1^2$, $y'''(0) = \sqrt{2}/2\theta_1^2, \ldots$ and the formal solution $y = \sum_{i=0}^{\infty} (\sqrt{2}\theta_1^{2i-1}/i!)(t/2)^i$.

5.2. Generic models

The notion of genericity may look like a pure algebraic notion, with no great practical meaning. So, I will try to explain briefly what can be the interest for control theory.

Example 1. — We go back to ex. 1.4. We have been able to describe the behaviour of our model by power series. But suppose we need to check whether or not x and y satisfy a given differential equation, $P(x, y) = 0$. The model is given by a characteristic set of a prime ideal $\mathcal{I}$, so we may first check whether we can reduce Q to 0. Of course, it is only a sufficient condition to have $P(x, y) = 0$. It would be sufficient, only if our power series solutions were generic solutions of $\mathcal{I}$. In such a case, we would say that the model is *generic*.

E.g., take $P(x, y) = x' - (\theta_1^2)x$. The model is defined by two equations. Complete them with $z = P(y)$. It is still a characteristic set of a prime ideal for a ordering extending the ordering on x and y, and such that z is greater than x, y and all their derivatives. So, we can compute a characteristic set $\mathcal{B}$ for a new ordering, taking z and its derivatives to be smaller than x and y. The c. s. $\mathcal{B}$ contains a polynomial depending only of z, viz. $z' - \theta_2 z$. We can easily compute initial conditions for z, $z(0) = 0$, and $z'(0) = 0$. This clearly implies that z is 0. So that our model is not generic.

The model defined by $x' = \theta_1^2 x$, $y^2 = x/\theta_1^2$, with initial conditions $x(0) = 2$, and $y(0) = \sqrt{2}/\theta_1$ is *equivalent* to the preceding, meaning that it defines the same power series solution, but it is this time generic.

The conclusion of this example is that, even if we cannot test genericity, we are still able, given a model and a polynomial $P(x, y)$ to decide whether the model satisfies $P(x, y) = 0$.

5.3. Identifiability

I think identifiability is well enough kown to avoid great explanations, and will only provide a formal definition. The reader may refer to [Wa1], for more details.

Definition 1. — *Let $M(\theta)$ be an algebraic diff. parametric model, we associate to it its input/output behaviour $\mathcal{C}(\theta)$, being the function which associates to an input vector u the unique output function which satisfies the initial conditions.*

If the model implies no input function, then $\mathcal{C}(\theta)$ is a constant function.

Definition 2. — *We say that a model $M(\theta)$ is globally (resp. locally) identifiable if $\forall\tau \in D$ $\mathcal{C}(\tau) = \mathcal{C}(\theta)$ (resp. if there exist an open neighbourood $\mathcal{O}$ of θ such that forall $\tau \in \mathcal{O}$ $\mathcal{C}(\tau) = \mathcal{C}(\theta)$) implies $\tau = \theta$.*

Example 3. — Take the model $x' = \theta^2 ux$, $y = x$, then $M(\theta)$ is locally identifiable for $\theta = 1$. It globally identifiable for $\theta = 0$. It would not be globally identifiable for $\theta = 1$ if the domain of admissible parameters is $D = \mathbf{R}$, but it would if $D = \mathbf{R}^+$.

Definition 4. — *We say that a parametric model is structuraly globally (resp. locally) identifiable if there exist a subset E of D of measure zero, such that for all $\theta \in D \setminus E$ $M(\theta)$ is globally (resp. locally) identifiable.*

6. Testing identifiability using standard bases

6.1. The use of exhaustive summaries

The input/output function $\mathcal{C}$ is very uneasy to use for any practical test, which explains the use of exhaustive summaries according to the following definition.

Definition 1. — *We say that a function ρ: $D \subset k^s \mapsto k^s$ is an exhaustive summary of the input/output behaviour of a parametric model if $\mathcal{C}(\theta) = \mathcal{C}(\tau) \iff \theta = \tau$, for all $(\theta, \tau) \in D^2$.*

This means that we may substitute ρ to $\mathcal{C}$ in the definition of identifiability above. Then, to test local identifiability, we only have to check that the jacobian matrix of ρ is of maximal rank r (see [Ra]). Suppose now that the field of constants k is $\mathbf{C}$. Then identifiability means that ρ admits a rational left inverse. This can be tested using a standard basis computation. For more simplicity, if f is a polynomial map, defined by $f_1, \ldots, f_r$, we only need to check whether the ideal $\mathcal{J}$ generated by the system $f_i(x) - f_i(y)$ in the ring $C(y)[x]$ is the ideal $(x_i - y_i)$. The reader may look at [O1] or [O2] for more details on the method.

This condition is obviously sufficient, but not necessary except if K is algebraically closed, corresponding in practice to the complex case which still have some interest for technical problems, even if it is not very often considered for control. But we still get useful informations from this method. On the first hand, the standard basis will give the dimension of $\mathcal{J}$, and it may be proved that the parametric model is locally identifiable iff $\dim \mathcal{J} = 0$. It also gives the degree of $\mathcal{J}$, which bounds the maximal number of real, or complex solutions.

Suppose that D, is a semi-algebraic subset of $\mathbf{R}^r$, i.e. a subset defined by a finite number of polynomial equation, inequations, or inequalities. We would be able then to use the C.A.D. algorithm to answer our problem (see [FGM]). Moreover, it is able to determine the set of parameters for which the system is identifiable, which is the most we can expect. But this is a very expensive algorithm, and even simple models are out of reach for this moment.

6.2. How to compute an exhaustive summary

Now, we would like to compute exhaustive summaries for the general models introduced in def. 5.1.2. In [O2], I have given a method which works only for generic structures. I will explain here briefly how to suppress this hypothesis which is very difficult to test. But first, I need to recall the previous method, because the first step is the same.

The idea is to compute a characteristic set for an ordering which eliminates state variables. Then, we only keep the part of the char. set corresponding to the measure variables, and compute initial conditions for those measure functions as we did in ex. 5.1.3 and 5.1.4. Now, we may make our characteristic set normalized (see [O2 def. IV.2.3.1 p. 96] for the precise definition), which implies that its elements are unique up to multiplication by a non zero element of $\mathcal{F}$. So, having chosen a total ordering on monomials, we may make our char. set unique by taking its polynomials to be monic, i.e. with leading monomial appearing with coefficient 1.

Example 1. — Take the char. set $\{x_1^2 - 2, x_1x_2 + 1\}$. We may substitute to it the normalized char. set $\{x_1^2, 2x_2 + x_1\}$, where the leading variable of the first polynomial, x_1, has been thrown away from the initial of the second polynomial. Now, we make those polynomials monic, so that the second one is replaced by $x_2 + \frac{1}{2}x_1$.

Suppose the structure is generic. Then, for any arbitrary input function u, the output y is generic too, which implies that the knowledge of y implies that of $\mathcal{I}(y)$. But we precisely know a char. set of $\mathcal{I}(y)$, which is unique up to the choice of the ordering. On the other hand, if we know $\mathcal{I}(y)$, and the initial conditions, y is uniquely determined... So, we conclude that the set of coefficients of all monomials in the members of the char. set form an exhaustive summary.

Example 2. — Consider the system $x' = \theta x,\ y = x^2,\ x(0) = 1$. If we eliminate x, we find $y' = \theta^2 y,\ y(0) = 1$, meaning that θ^2 is an exhaustive summary and the parametric model is identifiable if we take $D = \mathbf{R}^+$.

We will deal with non generic parametric models using standard bases. We have seen above that standard bases were not unique. But we may prove that, for any ideal, there exist a unique standard basis G, such that all polynomial $P \in G$ is monic and reduced with respect to $G \setminus \{P\}$. It is called the reduced standard basis. We define the weight wt on the set of differential monomials, by taking $\mathrm{wt}(x_{i,(j)} = j + 1$, so that $\mathrm{wt}(x_{1,(2)}^3 x_2 = 3(2+1) + 1 = 10$. We choose now an admissible ordering which respects wt. E.g. we may sort first according to wt and use the ordering $<_{der}$ of ex. 4.1.1 in case of equality. The reason of this choice is that we need to use an ordering such that for any given monomial there is only a finite number of smaller monomials.

We suppose we have found a char. set $\mathcal{A}$ for y as in the example above. We would like to test that the coefficients in its polynomials form a summary, or else find new algebraic relations for y, leading to a wider ideal and a new smaller char. set. The trouble is that we do not know $\mathcal{I}(y)$ by a set of generators or a characteristic set, but we are still able to test that a given polynomial belongs to it (see ex. 5.1). Let $m = \max_{P \in \mathcal{A}} \mathrm{wt}\, P$. We will build all the elements in the reduced standard basis of $\mathcal{I}(y)$, whose weight is not bigger than m.

6.3. The final step

We have seen in section 2.1 how we could introduce a primitive notion of standard bases, from th standpoint of linear algebra, and in ex. 2.1.1 how we could also find relations between the generators. We can do the same using canonical bases, and find then relations between the generators of the algebra.

We need now to apply this idea to the differential algebra $K\{y\}$ generated by the power series solutions defined by the initial conditions. The differential ideal of relations between them is exactly $\mathcal{I}(y)$. Two problems occur then. The first one is that we are in a differential situation, so that the theory of canonical bases given in section 2.3 should be extended. But the main trouble is to deal with series. The most immediate solution is to restrict to linear algebra, as we did at the beginning.

For any monomial M, we can construct the series $M(y)$ up to an arbitrary order. We consider all monomials M of weight smaller than m. Then, we can consider a matrix with infinite columns, corresponding to those monomials $M(y)$. We take an elementary example.

Example 1. — Take the system $y'' + \theta_1^2 y = 0$, with initial condition $y(0) = 0, y'(0) = \theta_2$. We want to construct the standard basis of $\mathcal{I}(y)$ for some ordering which respects the weight, up to weight 4. The monomials of this weight, or less are $1, y, y^2, y', y^3, yy', y'', y^4, (y')^2, yy'', y'''$. We consider now the matrix L, whose infinite columns correspond to the series associated to those monomials: $c_1 = (1, 0, \ldots)^{\mathrm{T}}$, $c_2 = (0, \theta_2 t, \theta_1^2\theta_2 t^3/3!, \ldots)^{\mathrm{T}}$, and so on. We have 11 columns, so we develop first those series to a reasonable order, say 20. A triangulation, using only column permutations leads to a matrix 21×11 of rank 7. There are left 4 columns of zero—up to order 20—, which correspond to columns $(y')^2 + \theta_1^2 y^2 - 1$, $y''' + \theta_1^2 y'$, $yy'' + \theta_1^2 y^2$, and $y'' + y$. We already now that the three last are really columns of 0, because those polynomials are reducible using $y'' + y$. Concerning the first, perhaps it would become non zero, if we develop the series far enough. But we can easily solve this problem by the method of ex. , which shows that indeed $(y')^2 + \theta_1^2 y^2 - 1 \in \mathcal{I}(y)$.

We conclude that the reduced standard basis of $\mathcal{I}(y)$ is $\{y'' + \theta_1^2 y, (y')^2 + \theta_1^2 y^2 - 1\}$, up to weight 4—it is in fact, as we already know, the whole basis.

This means that, knowing θ_1^2 and θ_2, y is uniquely determined. On the other hand, if we know y, the reduced basis of $\mathcal{I}(y)$ is also uniquely determined, which implies the determination of θ_1^2, because of the unicity of the reduced standard basis. It also implies the knowledge of $y'(0) = \theta_2$. It other words, we have found the wanted exhaustive summary.

7. Conclusion

I hope that this modest presentation of effective methods could be of some interest for control theorists, and that it wouldn't seem to involved, or too naive. I needed to skip many formal definitions and also some purely technical difficulties, so that the exposition of most methods is incomplete.

The next references should help the reader to know more about computer algebra. It should have wide possibilities of applications in control theory, which still need to be developped or widely used.

8. References

[Bel] R. BELLMAN et K.J. ÅSTRÖM, *On structural identifiability*, Math. Biosci., 7, 329–339, 1970.

[Bu] B. BUCHBERGER, *Groebner Bases: an Algorithmic Method in Polynomial Ideal Theory*, Multidimensional Systems Theory, N. K. Bose ed., Reidel, 184–232, 1985.

[Car] G. CARRA'-FERRO, *Gröbner bases and differential ideals*, proceedings of AAECC5, Menorca, Spain, 129–140, Springer Verlag, Juin 1987.

[DST] J.H. DAVENPORT, SIRET, TOURNIER, *Calcul formel*, (english translation exists), Masson, Paris, 1987.

[Di] S. DIOP, *Théorie de l'élimination et principe du modèle interne enautomatique*, thèse de doctorat en science, Univ. Paris Sud, 1989.

[FGM] N. FITCHAS, A. GALLIGO, J. MORGENSTERN, *Precise sequential and parallel complexity for quantifier elimination over algebraically closedfields*, to appear in Journal of Pure and Applied Algebra, 1987.

[Fl] M. FLIESS, *Automatique et corps différentiels*, Forum Math., 1, 1989.

[Ja] M. JANET, *Systèmes d'équations aux dérivées partielles*, J. de Math., 8^{e} série, tome III, 1920.

[KM] D. KAPUR et K. MADLENER, *A Completion Procedure for Computing a Canonical Basis of a k-Subalgebra*, Computers and Math., E. Kaltofen et S. M. Watt ed., Springer, 1989.

[Ko] E. R. KOLCHIN, *Differential Algebra and Algebraic Groups*, Academic Press, New-York, 1973.

[La] D. Lazard, *A New Method for Solving algebraic systems of positive dimension*, prépublication du LITP, Paris VII, n° 89-77, invited conference to AAECC'7, Toulouse, 1989.

[Le] Y. LECOURTIER, *Propriétés structurelles de modèles : études théoriques, tests formels, applications à la catalyse hétérogène*, Thèse de Doctorat ès Sciences, Université Paris-Sud, 1985.

[LLW] Y. LECOURTIER, F. LAMNABHI-LAGUARRIGUE, et E. WALTER, *A Method to Prove that Non-Linear Models can be Unidentifiable*, proceedings of 26^{th} Conference on Decision and Control, Los Angeles, CA, 2144–2145, Décembre 1987.

[Lev] H. LEVI, *On the structure of differential polynomials and on their theory of ideals*, Transactions of the A.M.S., vol 51, 326–365, 1942.

[O1] F. OLLIVIER, *Inversibility of rational mappings and structural identifiability in automatics*, proceedings of ISSAC'89, Portland Oregon, 43–53, ACM Press, 1989.

[O2] F. OLLIVIER, *Le problème de l'identifiabilité structurelle globale : étude théorique, méthodes effectives et bornes de complexité*, Thèse de Doctorat en Science, École Polytechnique, 25 Juin 1990.

[O3] F. OLLIVIER, *Canonical bases: relations with standard bases, finiteness conditions and application to tame automorphisms*, to appear in the proceedings of MEGA'90, Castiglioncello, Birkhauser, 1990.

[O4] F. OLLIVIER, *Standard Bases of differential ideals*, to appear in the proceedings of AAECC'8, Tôkyô, Lecture Notes in Computer Science, Springer, 1990.

[Po4] J.-F. POMMARET, *Effective methods for systems of algebraic partial differential equations*, to appear in the proceedings of MEGA'90, Castiglioncello, 1990.

[Ra] A. RAKSANYI, *Utilisation du calcul formel pour l'étude des systèmes d'équations polynomiales (Applications en modélisation)*, thèse de troisième cycle, Université Paris-Dauphine, 1986.

[Ro] L. ROBBIANO, *On the Theory of Graded Structures*, J. Symb. Comp. 2, 1986.

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

[SS] D SHANNON et 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.

[Wa1] E. WALTER, *Identifiability of State Space Models*, Lect. notes in Biomath. n° 46, Springer 1982.

[Wa2] Collectif : DISTEFANO, LAMNABHI-LAGUARRIGUE, LECOURTIER, RAKSANYI, VAJDA, WALTER, etc..., *Identifiability of parametric models*, E. Walter ed., Pergamon Press, Oxford, 1987.

[WL] E. WALTER et Y. LECOURTIER, *Global approches to identifiability testing for linear and non-linear state space models*, Mathematics and computers in Simulation, XXIV, 472–482, 1982.

[Wu] WU W.-T., *A Zero Structure Theorem for Polynomial Equation Solving and its applications*, proceedings of ISSAC'88, Rome, Springer Verlag, 1988.