J. Symbolic Computation (2002) **33**, 735–755
doi:10.1006/jsco.2002.0532
Available online at http://www.idealibrary.com on IDEAL®

A Probabilistic Algorithm to Test Local Algebraic Observability in Polynomial Time

ALEXANDRE SEDOGLAVIC†

Projet Algorithmes, INRIA–Rocquencourt, F-78153 Le Chesnay Cedex, France,
Laboratoire GAGE, École polytechnique, F-91128 Palaiseau Cedex, France

The following questions are often encountered in system and control theory. Given an algebraic model of a physical process, which variables can be, in theory, deduced from the input–output behaviour of an experiment? How many of the remaining variables should we assume to be known in order to determine all the others? These questions are parts of the *local algebraic observability* problem which is concerned with the existence of a non-trivial Lie subalgebra of model's symmetries letting the *inputs* and the *outputs* be invariant.

We present a *probabilistic seminumerical* algorithm that proposes a solution to this problem in *polynomial time*. A bound for the necessary number of arithmetic operations on the rational field is presented. This bound is polynomial in the *complexity of evaluation* of the model and in the number of variables. Furthermore, we show that the *size* of the integers involved in the computations is polynomial in the number of variables and in the degree of the system. Last, we estimate the probability of success of our algorithm.

1. Introduction

Local algebraic observability is a structural property of a model and one of the key concepts in control theory. Its earliest definition goes back to the work of Kalman (1961) for the linear case and a large literature is devoted to this subject (see Hermann and Krener, 1977 and the references therein). We base our work on the definition given by Diop and Fliess (1991) of the observability for the class of algebraic systems. The algorithmic aspects of our work are related to the power series approach of Pohjanpalo (1978).

Description of the input

As in the example of Figure 1, an algebraic differential model is usually described in a state space representation by means of

- a vector field describing the evolution of *state variables* (M, P_0, P_1, P_2, P_N) in the function of *inputs* $(\dot{v}_d \neq 0)$ and of *parameters* $(\dot{v}_s = \dot{K}_I = \cdots = \dot{k}_2 = 0)$;
- some *outputs* $(y = P_N)$ which are algebraic functions of these variables.

†E-mail: `Alexandre.Sedoglavic@polytechnique.fr`

0747–7171/02/050735 + 21 $35.00/0

$$
\left\{
\begin{array}{lcl}
\dot{M} & = & \frac{v_s {K_I}^4}{{K_I}^4 + {P_N}^4} - \frac{v_m M}{K_m + M}, \\
\dot{P}_0 & = & k_s M - \frac{V_1 P_0}{K_1 + P_0} + \frac{V_2 P_1}{K_2 + P_1}, \\
\dot{P}_1 & = & \frac{V_1 P_0}{K_1 + P_0} + \frac{V_4 P_2}{K_4 + P_2} - P_1 \left(\frac{V_2}{K_2 + P_1} + \frac{V_3}{K_3 + P_1} \right), \\
\dot{P}_2 & = & \frac{V_3 P_1}{K_3 + P_1} - P_2 \left(\frac{V_4}{K_4 + P_2} + k_1 + \frac{v_d}{K_d + P_2} \right) + k_2 P_N, \\
\dot{P}_N & = & k_1 P_2 - k_2 P_N, \\
y & = & P_N.
\end{array}
\right.
\tag{1}
$$

Figure 1. Model for circadian oscillations in the Drosophila period protein.

The definition of observability given by Diop and Fliess (1991) relies on the theory of differential algebra founded by Ritt (1966) and is based on the existence of algebraic relations between the state variables and the successive derivatives of the inputs and the outputs. These relations are an obstruction to the existence of infinitely many trajectories of the state variables which are solutions of the vector field and fit the same specified input–output behaviour. If there are only finitely many such trajectories, the state variables are said to be locally observable.

EXAMPLE OF APPLICATION

In order to illustrate this notion, let us consider the *local structural identifiability* problem which is a particular case of the observability problem. The question is to decide if some unknown *parameters* of a model are observable considering these parameters as a special kind of state variables θ satisfying $\dot{\theta} = 0$ (see Pohjanpalo, 1978; Walter, 1982; Vajda *et al.*, 1989). If they are not observable, then infinitely many values of these parameters can fit the same observed data and the approximation of these quantities by numerical methods is not possible (see Ljung, 1987 and the references therein).

PREVIOUS WORKS

We consider the local algebraic observability problem under the computer algebra standpoint. The previous studies that enable to test observability mainly rely on characteristic set or standard bases computation as shown in Ollivier (1990) and Ljung and Glad (1990, 1994). We refer to Boulier *et al.* (1995) and Hubert (2000) for an elimination method in differential algebra. The complexity of this method is, at least, exponential in the number of variables and of parameters (see Gallo and Mishra, 1991; Sadik, 2000). Some other techniques, as the local state variable isomorphism approach (Vajda *et al.*, 1989) or the conversion between characteristic set w.r.t. different ranking (Boulier, 1999), can also be used. The complexities of these methods are not known.

CONTRIBUTIONS

We present a probabilistic polynomial-time algorithm which computes the set of observable variables of a model and gives the number of non-observable variables which should be assumed to be known in order to obtain an observable system. Our algorithm certifies that a variable is observable and the answer for a non-observable one is probabilistic with high probability of success. A Maple implementation of this algorithm is available at the URL `http://www.medicis.polytechnique.fr/~sedoglav`.

Furthermore, we present a method which allows to compute a family of symmetries of the model letting the inputs and the outputs be invariant. This part of the paper extends the contributions of Sedoglavic (2001) and it is, as far as we know, a new algorithmic approach. In fact, the previous works lead to the resolution of partial differential equations which may be quickly intractable (see the paper of Vajda *et al.*, 1989 for more details). Our approach relies on the computation of the kernel of a matrix with polynomial coefficients and on the *resolution* of a system of ordinary differential equations. Contrarily to the previous methods, this approach allows us to compute the symmetries of almost all the non-observable models encountered in practice.

A NON-OBSERVABLE MODEL. Let us illustrate our algorithm with the model for circadian oscillations in the Drosophila period protein (Goldbeter, 1995) presented in Figure 1. After 10 s of computation, our implementation shows that:

- the variable M and the parameters $\{v_s, v_m, K_m, k_s\}$ are not observable. All 17 other parameters and variables are observable;
- if M or only one of the non-observable parameters are specified, all the variables and parameters of the resulting system are observable.

These results allow us to focus our attention on just four of the 17 original parameters. Thus, the search for an infinitesimal transformation which leaves the output y and the vector field invariant is simplified and we find a group of symmetries generated by $\{M, v_s, v_m, K_m, k_s\} \to \{\lambda M, \lambda v_s, \lambda v_m, \lambda K_m, k_s/\lambda\}$. Hence, there is an infinite number of possible values for non-observable parameters which fit the same specified output y: this system is certainly unidentifiable.

In the next section, we present more precisely the contributions of this papers.

1.1. NOTATIONS AND MAIN RESULT

Hereafter, we consider a state variable representation with time invariant parameters defined by an algebraic system of the following kind:

$$\Sigma \begin{cases} \dot{\Theta} = 0, & \\ \dot{X} = F(X, \Theta, U), & (2.1) \\ Y = G(X, \Theta, U). & (2.2) \end{cases} \qquad (2)$$

Capital letters stand for vector-valued objects and we suppose that there are:

- ℓ parameters $\Theta := (\theta_1, \ldots, \theta_\ell)$;
- n state variables $X := (x_1, \ldots, x_n)$;
- r input variables $U := (u_1, \ldots, u_r)$;
- m output variables $Y := (y_1, \ldots, y_m)$.

The letter $\dot{X}$ stands for the derivatives of the state variables $(\dot{x}_1, \ldots, \dot{x}_n)$ and the letter F (respectively G) represents n (respectively m) rational functions in $\mathbb{Q}(X, \Theta, U)$ which are denoted by $(f_1, \ldots, f_n)$ (respectively $(g_1, \ldots, g_m)$). The letter d (respectively h) represents a bound on the degree (respectively size of the coefficients) of the numerators and denominators of the f_i's and g_i's.

DATA ENCODING

Hereafter, we represent the system Σ by a *straight-line programme* without division which computes its numerators and denominators and requires L arithmetic operations (see Sections 3.4 and 4 in Bürgisser *et al.*, 1997). For example, the expression $e := (x+1)^5$ is represented by the sequence of instruction $t_1 := x+1,\ t_2 := {t_1}^2,\ t_3 := {t_2}^2,\ e := t_3\, t_1$ and $L = 4$. Hence, the complexity of our input is given by the quantities ℓ, n, r, m, d, h and L. The following theorem is the main result of this paper.

THEOREM 1.1. *Let Σ be a differential system as described in Section* 1.1. *There exists a probabilistic algorithm which determines the set of observable variables of Σ and gives the number of non-observable variables which should be assumed to be known in order to obtain an observable system.*

The arithmetic complexity of this algorithm is bounded by

$$\mathcal{O}(\mathcal{M}(\nu)(\mathcal{N}(n+\ell) + (n+m)L) + m\nu\mathcal{N}(n+\ell))$$

with $\nu \leq n+\ell$ and with $\mathcal{M}(\nu)$ (respectively $\mathcal{N}(\nu)$) the cost of power series multiplication at order $\nu+1$ (respectively $\nu \times \nu$ matrix multiplication).

Let μ be a positive integer, D be $4(n+\ell)^2(n+m)d$ and D' be

$$(2\ln(n+\ell+r+1) + \ln \mu D)D + 4(n+\ell)^2((n+m)h + \ln 2nD).$$

If the computations are done modulo a prime number $p > 2D'\mu$ then the probability of a correct answer is at least $(1-1/\mu)^2$.

For the model presented in Figure 1, the choice of $\mu = 3000$ leads to a probability of success around 0.9993 and the computations are done modulo 10 859 887 151. These computations take 10 s on a PC Pentium III (650 MHz). Furthermore, the new method presented in this papers allows to compute the family of symmetries $\{M, v_s, v_m, K_m, k_s\} \rightarrow \{\lambda M, \lambda v_s, \lambda v_m, \lambda K_m, k_s/\lambda\}$. As far as we know, this computation was not automatically possible with previous methods.

OUTLINE OF THE PAPER

In the next section, we recall some basic definitions of differential algebra and the definition of algebraic observability used in Diop and Fliess (1991) and in Ljung and Glad (1990). Next, we describe the relationship between this framework and the power series approach of Pohjanpalo (1978).

Then, we present the Jacobian matrix derived from the theory of Kähler differentials and used in the local algebraic observability test. This matrix allows to determine the non-observable variables. Furthermore, when the model is not observable, we show that the power series approach allows to compute a family of symmetries of the model letting the inputs and the outputs be invariant.

In the second part of this paper, we present some algorithmic results. In Section 3, we show how to compute some specializations of this matrix using power series expansion of the output and we estimate the related arithmetic complexity. Then, we study the behaviour of the integers involved in the computations and we summarize the probabilistic aspect.

2. Differential Algebra and Observability

Differential algebra can be seen as a generalization to differential equations of the concepts of commutative algebra and algebraic geometry. This theory, founded by Ritt, is an appropriate framework for the definition of algebraic observability introduced by Diop and Fliess (1991). For more details on this theory, we refer to the books of Ritt (1966) and Kolchin (1973); nevertheless, we recall briefly some necessary notions.

DIFFERENTIAL ALGEBRAIC SETTING

Let us denote by k a ground field of characteristic zero. The differential algebra $k\{U\}$ is the k-algebra of multivariate polynomials defined by the infinite set of indeterminates $\{U^{(j)}|\forall j \in \mathbb{N}\}$ and equipped with a derivation $\mathcal{L}$ such that $\mathcal{L}u^{(i)} = u^{(i+1)}$. Its fraction field is denoted by $k\langle U\rangle$.

HYPOTHESES

The inputs U and all their derivatives are assumed to be independent and we consider non-singular solutions of Σ. Thus, we assume that we work in a Zariski open set where the denominators present in Σ do not vanish.

2.1. LOCAL ALGEBRAIC OBSERVABILITY AND DIFFERENTIAL ALGEBRA

Following the interpretation of some algebraic control theory problems presented in Fliess (1989), we consider the differential field $\mathcal{K} := k\langle U\rangle(X, \Theta)$ equipped with the following formal Lie derivation:

$$\mathcal{L} := \frac{\partial}{\partial t} + \sum_{i=1}^{n} f_i \frac{\partial}{\partial x_i} + \sum_{j\in\mathbb{N}} \sum_{u\in U} u^{(j+1)} \frac{\partial}{\partial u^{(j)}}.$$

This derivation is associated with the vector field defined by equations (2.1). Hereafter, we denote $(\mathcal{L}f_1, \ldots, \mathcal{L}f_n)$ by $\mathcal{L}F$ and $\underbrace{\mathcal{L} \circ \cdots \circ \mathcal{L}}_{j \text{ times}}$ by $\mathcal{L}^j$.

Hence, the successive derivation of the output is given by $Y^{(j)} = \mathcal{L}^j G(X, \Theta, U)$ and the differential subfield $k\langle U, Y\rangle$ of $(\mathcal{K}, \mathcal{L})$ by $k\langle U\rangle(G, \mathcal{L}G, \mathcal{L}^2G, \ldots)$. The following definition is taken from Diop and Fliess (1991) (see also Ljung and Glad, 1990). It summarizes the intuitive definition of observability given in the introduction.

Definition. An element z in $\mathcal{K}$ is *locally algebraically observable* with respect to inputs and outputs if it is algebraic over $k\langle U, Y\rangle$. So, the system Σ is locally observable if the field extension $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$ is purely algebraic.

AN OBSERVABLE MODEL. Let us illustrate this definition with the following example:

$$\begin{cases} \dot{x}_3 = x_1\theta - u, \\ \dot{x}_2 = x_3/x_2, \\ \dot{x}_1 = x_2/x_1, \\ y = x_1. \end{cases} \tag{3}$$

Performing an easy elimination on the relations $y = x_1$, $\dot{y} = \mathcal{L}x_1$, $y^{(2)} = \mathcal{L}^2 x_1$ and $y^{(3)} = \mathcal{L}^3 x_1$, we obtain the following differential relations:

$$x_1 = y,\ x_2 = y\dot{y},\ x_3 = y\dot{y}(\dot{y}^2 + y\ddot{y}),\ \theta y = (\dot{y}^2 + y\ddot{y})^2 + y\dot{y}(3\dot{y}\ddot{y} + y\, y^{(3)}) - u. \quad (4)$$

Thus, $x_1,\ x_2,\ x_3$ and θ are observable according to the above Definition. As these relations define a unique solution, these quantities are said to be *globally* algebraically observable (see Ljung and Glad, 1990; Ollivier, 1990).

Remark. These relations depend generically on high order derivatives of the output, so they are not of a great practical interest for parameter estimation. As we focus our attention on local observability, we are going to avoid their computation. Thus, we do not need to perform any elimination.

The above Definition implies that local observability is related to the transcendence degree of the field extension $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$. This property can be tested by a rank computation using Kähler differentials (see Section 2.3) and—as noticed by Diop and Fliess (1991)—this approach leads to the algebraic counterpart of the rank condition introduced by Hermann and Krener (1977) in the differential geometric point of view. Furthermore, the transcendence degree of the field extension $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$ is the number of non-observable variables which should be assumed to be known in order to obtain an observable system. Thus, we notice that Theorem 1.1 is based on the study of this field extension.

Family of symmetries of the model letting the inputs and the outputs be invariant

The algebraic counterpart of the notion of family of symmetries of a model used in observability theory (see Hermann and Krener, 1977; Vajda *et al.*, 1989) is based on the following notion of a group of $k\langle U, Y\rangle$-automorphisms acting on $\mathcal{K}$.

Definition. A group σ_λ—indexed by λ—of $k\langle U, Y\rangle$-automorphisms from $\mathcal{K}$ into $\mathcal{K}$ which leave $k\langle U, Y\rangle$ point to point invariant is such that:

- the *parameter* λ of the group is in a field of constants ($\lambda \in k \Rightarrow \mathcal{L}\lambda = \dot{\lambda} = 0$);
- σ_1 is the identity and for all (λ, μ) in k^2, $\sigma_{\lambda\mu}(\cdot) = \sigma_\lambda(\sigma_\mu(\cdot))$;
- for all λ, σ_λ is a differential automorphism of $(\mathcal{K}, \mathcal{L})$. In fact, $\sigma_\lambda \circ \mathcal{L}$ is equal to $\mathcal{L} \circ \sigma_\lambda$ and for all (a, b) in $\mathcal{K}^2$, for all c in $k\langle U, Y\rangle$ we have:

$$\sigma_\lambda(c) = c, \quad (5)$$

$$\sigma_\lambda(a + b) = \sigma_\lambda(a) + \sigma_\lambda(b), \quad (6)$$

$$\sigma_\lambda(ab) = \sigma_\lambda(a)\sigma_\lambda(b). \quad (7)$$

A non-observable model. The following model is taken from Vajda *et al.* (1989):

$$\begin{cases} \dot{x}_1 = \theta_1\, {x_1}^2 + \theta_2\, x_1\, x_2 + u, \\ \dot{x}_2 = \theta_3\, {x_1}^2 + \theta_4\, x_1\, x_2, \\ y = x_1. \end{cases} \quad (8)$$

The family of symmetries $\sigma_\lambda : \{x_1, x_2, \theta_2, \theta_3, \theta_4, u\} \to \{x_1, \lambda x_2, \theta_2/\lambda, \lambda\theta_3, \theta_4, u\}$ indexed by λ leave the input u, the output $y = x_1$ and all their derivatives invariant. In fact, a simple computation shows that this group is well defined:

$$\sigma_\lambda(\dot{x}_1) = \sigma_\lambda(\theta_1\, {x_1}^2 + \theta_2\, x_1\, x_2 + u) = \theta_1\, {x_1}^2 + \frac{\theta_2}{\lambda}\, x_1\, \lambda x_2 + u = \dot{x}_1,$$

$$\sigma_\lambda(\dot{x}_2) = \sigma_\lambda(\theta_3\, {x_1}^2 + \theta_4\, x_1\, x_2) = \lambda\theta_3\, {x_1}^2 + \theta_4\, x_1\, \lambda x_2 = \lambda \dot{x}_2,$$

$$\Rightarrow \quad \forall i \in \mathbb{N}, \quad \sigma_\lambda\big(y^{(i)}\big) = \sigma_\lambda\big({x_1}^{(i)}\big) = y^{(i)}.$$

This algebraic point of view has the following intuitive geometric interpretation. Let us consider the space $\mathcal{E}$ of coordinates $(x_1, x_2, \theta_2, \theta_3, \theta_4, u, t)$ where t is a solution of $\dot{t} = 1$. A trajectory of the model (8) is a solution of (8) parametrized by u and t. The family of symmetries σ_λ is an infinite family of mapping of $\mathcal{E}$ such that a trajectory is mapped onto another trajectory while t, u and y are left point to point invariant (see Hermann and Krener, 1977; Vajda *et al.*, 1989).

Remark. If an element a of $\mathcal{K}$ is algebraic over $k\langle U, Y\rangle$ then $\sigma_\lambda(a)$ is also algebraic over $k\langle U, Y\rangle$ for all λ and has the same minimal polynomial: there is a finite number of possible actions of σ_λ on a. Hence, if the field extension $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$ is purely algebraic, there is no infinite group of $k\langle U, Y\rangle$-automorphisms as described in the above definition which act on $\mathcal{K}$ and leave $k\langle U, Y\rangle$ point to point invariant. Thus, the existence of such a group proves that the model is not observable.

2.2. A finite description of $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$

Let us denote by $\Phi(X, \Theta, U, t)$ the formal power series in t with coefficients in $\mathcal{K}$ solution of $\dot{\Phi} = F(\Phi, \Theta, U)$ with initial condition $\Phi(X, \Theta, U, 0) := X$. We have:

$$\Phi(X, \Theta, U, t) = X + \sum_{j \in \mathbb{N}^\star} \mathcal{L}^j F(X, \Theta, U)\; t^j/j!.$$

Using this power series, let us define the formal power series in t with coefficients in $\mathcal{K}$ such that $Y(X, \Theta, U, t) := G(\Phi(X, \Theta, U, t), \Theta, U, t)$:

$$Y(X, \Theta, U, t) = G(X, \Theta, U) + \sum_{j \in \mathbb{N}^\star} \mathcal{L}^j G(X, \Theta, U)\; t^j/j!. \tag{9}$$

Example 2.1. For the model (3), with initial conditions $x_1 \neq 0, x_2 \neq 0, x_3, \theta$ and a generic input $u(t) = u + \dot{u}\, t + \ddot{u}\, t^2/2 + u^{(3)}\, t^3/3! + \mathcal{O}(t^4)$, we have

$$\phi_3(t) = x_3 + (\theta\, x_1 - u)\, t - \frac{\dot{u}\, x_1 - \theta\, x_2}{2\, x_1} t^2 + \frac{\theta\, x_3\, {x_1}^2 - \theta\, {x_2}^3 - \ddot{u}\, x_2\, {x_1}^3}{6\, x_2\, {x_1}^3} t^3 + O(t^4),$$

$$\phi_2(t) = x_2 + \frac{x_3}{x_2} t + \frac{\theta x_1 {x_2}^2 - u {x_2}^2 - {x_3}^2}{2 {x_2}^3} t^2 - \frac{{x_2}^4 \dot{u} x_1 - {x_2}^5 \theta + 3 x_3 {x_1}^2 \theta {x_2}^2 - 3 x_3 x_1 u {x_2}^2 - 3 {x_3}^3 x_1}{6 {x_2}^5 x_1} t^3 + O(t^4),$$

$$\phi_1(t) = x_1 + \frac{x_2}{x_1} t + \frac{x_3\, {x_1}^2 - {x_2}^3}{2\, x_2\, {x_1}^3} t^2 + \frac{{x_1}^5 \theta\, {x_2}^2 - {x_1}^4 u\, {x_2}^2 - {x_1}^4 {x_3}^2 - 3\, {x_2}^3 x_3\, {x_1}^2 + 3\, {x_2}^6}{6\, {x_1}^5 {x_2}^3} t^3 + O(t^4).$$

In this model, the output y is equal to ϕ_1 and we retrieve the relations (4) using

$$\begin{aligned} y(t) &= y + \dot{y}\; t + \ddot{y}\; t^2/2 + y^{(3)}\; t^3/3! + O(t^4), \\ &= x_1 + \frac{x_2}{x_1}\, t + \frac{x_3 {x_1}^2 - {x_2}^3}{2\, x_2 {x_1}^3}\, t^2 + \frac{(3\, {x_2}^4 - 3\, x_2 x_3 {x_1}^2 + (x_1 \theta - u) {x_1}^4)\, {x_2}^2 - {x_1}^4 {x_3}^2}{6\, {x_1}^5 {x_2}^3}\, t^3 + O(t^4). \end{aligned}$$

FROM AN INFINITE TO A FINITE NUMBER OF INDETERMINATES

In Pohjanpalo (1978), the power series Y was already used in order to test identifiability. In Diop and Fliess (1991), the authors prove that a finite number of these coefficients are necessary to *describe* the field extension $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$. But in these papers the necessary order of derivation is not bounded. This can be done using the differential algebra point of view (see Section 4 in Sadik, 2000 for a general statement). The following proposition summarizes these results in a field extension framework.

PROPOSITION 2.1. *The differential field $k\langle U, Y\rangle$ is purely algebraic over the differential field $k\langle U\rangle\big(Y, \ldots, Y^{(n+\ell-1)}\big)$.*

PROOF. The transcendence degree of $k\langle U\rangle \hookrightarrow \mathcal{K}$ is equal to $n+\ell$. Hence, the transcendence degree of the field extension $k\langle U\rangle \hookrightarrow k\langle U, Y\rangle$ is bounded by $n+\ell$. It means that, for $i = 1, \ldots, m$, there is an algebraic relation $q_i\big(y_i, \ldots, {y_i}^{(n+\ell)}\big) = 0$. Furthermore, the derivative ${y_i}^{(n+\ell+1)}$ is a rational function of $y_i, \ldots, {y_i}^{(n+\ell)}$ with coefficients in $k\langle U\rangle$.

REMARK. If there is more than a single output, the necessary order of derivation can be smaller than $n+\ell$ and it is denoted by ν. This index of differentiation is a measure of the complexity of our algorithm (see Section 3.4) and generically $\nu = \lfloor (n+\ell)/m \rfloor$. Hereafter, we take ν equal to $n+\ell$.

REMARK. In the above proof, following the hypotheses of Section 2, we assumed that the independent input variables U and all their derivatives were in the ground field. Furthermore, we showed that we just need the first $n+\ell$ derivatives of the output equations. In order to simplify the presentation in the next section, we assume that the ground field is $\mathcal{G} := k(U, Y, \ldots, U^{(n+\ell)}, Y^{(n+\ell)})$.

We now present the properties of the module of Kähler differentials which are used to compute the transcendence degree of $\mathcal{G} \hookrightarrow \mathcal{G}(X, \Theta)$ in practice. When this field extension is not purely algebraic, the Kähler differentials allow us to determine a *derivation* acting on $\mathcal{G}(X, \Theta)$ with $\mathcal{G}$ as field of constant. This last derivation could generate an infinite group of $\mathcal{G}$-automorphisms acting on $\mathcal{G}(X, \Theta)$.

2.3. LINEARIZATION AND RANK CONDITIONS

We consider now the algebraic counterpart of the linearization process in differential geometry. To a field extension $S \hookrightarrow T$, one can associate:

- the T-vector space $\mathrm{Der}_S(T, T)$ of derivations $\partial : T \to T$ s.t. $\forall c \in S,\ \partial c = 0$;
- the T-vector space $\Omega_{T/S}$ of Kähler differentials which can be defined by the following property: $\mathrm{Der}_S(T, T) = \mathrm{Hom}_T(\Omega_{T/S}, T)$. In fact, let $\mathrm{d}z$ be the image of $z \in T$ in this vector space by $\mathrm{d} : T \to \Omega_{T/S}$. For all ∂ in $\mathrm{Der}_S(T, T)$, there exists a unique linear homomorphism $\delta : \Omega_{T/S} \to T$ s.t. $\delta(\mathrm{d}z) = \partial z$.

We refer to Section 16 in Eisenbud (1994) for a standard definition and to Johnson (1969) for a similar construction in differential algebra. In our framework, the $\mathcal{G}(X, \Theta)$-vector space of Kähler differentials is associated to the cokernel of the matrix

$$\frac{\partial\left(Y^{(i)}\right)_{0\le i\le\nu}}{\partial(X,\Theta)} = \begin{pmatrix} \frac{\partial y_1}{\partial x_1} & \cdots & \frac{\partial y_1}{\partial x_n} & \frac{\partial y_1}{\partial \theta_1} & \cdots & \frac{\partial y_1}{\partial \theta_\ell} \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\partial y_m}{\partial x_1} & \cdots & \frac{\partial y_m}{\partial x_n} & \frac{\partial y_m}{\partial \theta_1} & \cdots & \frac{\partial y_m}{\partial \theta_\ell} \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\partial y_1{}^{(\nu)}}{\partial x_1} & \cdots & \frac{\partial y_1{}^{(\nu)}}{\partial x_n} & \frac{\partial y_1{}^{(\nu)}}{\partial \theta_1} & \cdots & \frac{\partial y_1{}^{(\nu)}}{\partial \theta_\ell} \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\partial y_m{}^{(\nu)}}{\partial x_1} & \cdots & \frac{\partial y_m{}^{(\nu)}}{\partial x_n} & \frac{\partial y_m{}^{(\nu)}}{\partial \theta_1} & \cdots & \frac{\partial y_m{}^{(\nu)}}{\partial \theta_\ell} \end{pmatrix}$$

and the $\mathcal{G}(X,\Theta)$-vector space $\mathrm{Der}_{\mathcal{G}}(\mathcal{G}(X,\Theta),\mathcal{G}(X,\Theta))$ is associated to the kernel of this matrix i.e. to the solution of $\partial(Y^{(j)},\, 0\le j\le\nu)/\partial(X,\,\Theta)\,v=0$ where the vector v is expressed on the basis of derivations $(\partial/\partial x_1,\dots,\partial/\partial x_n,\partial/\partial\theta_1,\dots,\partial/\partial\theta_\ell)$.

We recall the following result which motivates the use of Kähler differentials:

Theorem 2.1. (Section 16 in Eisenbud, 1994) *Let us consider S a field of characteristic zero and T a finitely generated field extension of S. If $\{x_\lambda\}\subset T$ is a collection of elements, then $\{\mathrm{d}x_\lambda\}$ is a basis of $\Omega_{T/S}$ as a vector space over T if, and only if, the $\{x_\lambda\}$ form a transcendence basis of T over S.*

Our test for local observability is based on the following straightforward consequences of this theorem.

Corollary 2.1. *If ϕ represents the transcendence degree of the field extension $\mathcal{G}\hookrightarrow\mathcal{G}(X,\Theta)$ then we have: $\phi=(n+\ell)-\mathrm{rank}_{\mathcal{G}(X,\Theta)}\,\partial(Y^{(j)},\,0\le j\le\nu)/\partial(X,\,\Theta)$.*

If the generic rank of $\partial(Y^{(j)},0\le j\le\nu)/\partial(X\setminus\{x_i\},\Theta)$ (respectively $\partial(Y^{(j)},0\le j\le\nu)/\partial(X,\,\Theta\setminus\{\theta_i\})$) is equal to $(n+\ell-1)-\phi$, then the transcendence degree of the field extension $\mathcal{G}\hookrightarrow\mathcal{G}(x_i)$ (respectively $\mathcal{G}\hookrightarrow\mathcal{G}(\theta_i)$) is zero and the variable x_i (respectively the parameter θ_i) is observable.

Furthermore, the transcendence degree of the field extension $\mathcal{G}\hookrightarrow\mathcal{G}(X,\Theta)$ is equal to the dimension of the $\mathcal{G}(X,\Theta)$-vector space $\mathrm{Der}_{\mathcal{G}}(\mathcal{G}(X,\Theta),\mathcal{G}(X,\Theta))$.

In the sequel, the computation of the transcendence degree of the field extension $\mathcal{G}\hookrightarrow\mathcal{G}(X,\Theta)$ is mainly based on the construction and the evaluations of a *straight-line programme* which allows to compute the power series expansion of $Y(X,\Theta,U,t)$. We present the necessary notions in the next section.

2.4. Data Encoding and Complexity Model

The above results can be expressed considering a polynomial f as an element of a vector space; hereafter, we consider an algebraic expression as a function. This classical point of view in numerical analysis is also used in computer algebra for complexity statements or practical algorithms (see Giusti *et al.*, 2001; Schost, 2000 and the references therein). We refer to Section 4 in Bürgisser *et al.* (1997) for more details about this model of computation.

Definition. Let $\mathcal{A}$ be a finite set of variables. A *straight-line programme* over $k[A]$ is a finite sequence of assignments $b_i \leftarrow b' \circ_i b''$ s.t. $\circ_i$ is in $\{+, -, \times, \div\}$ and $\{b', b''\}$ is in $\bigcup_{j=1}^{i-1}\{b_j\} \cup \mathcal{A} \cup k$. Its complexity of evaluation is measured by its length L, which is the number of its arithmetic operations. Hereafter, we use the abbreviation SLP for straight-line programme.

Remark. A SLP representing a rational expression f is a programme which computes the value of f from any values of the ground field such that every division of the programme is possible. The following constructive results taken from Baur and Strassen (1983) allows us to determine a SLP representing the gradient of f.

Theorem 2.2. *Let us consider a* SLP *computing the value of a rational expression f in a point of the ground field and let us denote by L_f its complexity of evaluation. One can construct a* SLP *of length $5L_f$ which computes the value of* $\mathrm{grad}(f)$. *Furthermore, one can construct a* SLP *of length $4L_f$ which computes two polynomials f_1 and f_2 such that $f = f_1/f_2$.*

Remark. Following our presentation, one can construct formally all the expressions introduced in Sections 2.2 and 2.3 with its favorite computer algebra system. But, in order to compute the formal expressions $Y^{(\nu)} = \mathcal{L}^\nu G$ and the associated Jacobian matrix, one has to differentiate ν times the output equations (2.2). As noticed by Valiant (1982), the arithmetic complexity of computing multiple partial derivatives is likely exponential in ν. If the evaluation complexity of the output equations (2.2) is L, by Theorem 2.2, the computation of $Y^{(\nu)}$ requires at least $(5m)^\nu L$ arithmetic operations. This strategy cannot lead to a polynomial time algorithm. For example, the Jacobian matrix of the model (1) cannot be easily computed using Maple with a PC equipped with 128MB of memory.

Remark. The rank computations defined in the previous section are also cumbersome because they are mainly performed on the field $\mathcal{G}(X, \Theta)$. Nevertheless, in order to determine ϕ efficiently, the variables X, Θ and U can be specialized to some generic values in the Jacobian matrix and so, its generic rank can be computed numerically with high probability of success (see Section 3.5).

Thus, the main problem is to avoid the formal computation of $Y^{(i)}$ for $0 \le i \le \nu$. In fact, our strategy is to specialize a linearized system derived from Σ first and to recover the value of ϕ just using numerical computations on a finite field.

3. A Probabilistic Polynomial Time Algorithm

We now present an algorithm which takes as input a state space representation (see model (2)) and return the set of non-observable variables. Furthermore, this algorithm returns the transcendence degree of the field extension $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$ defined in Section 2.1.

In Section 3.1, we present the *variational system* derived from Σ which allows us to compute directly the Jacobian matrix $\partial(Y^{(j)}, 0 \le j \le \nu)/\partial(X, \Theta)$ with X, Θ and U specialized on some given values. Then, we show how this matrix can be determined in polynomial time and we give an estimation of the arithmetic complexity of our algorithm.

The purpose of the Section 3.5 is to study the growth of the integers involved in the computations and to estimate the probability of success of our algorithm.

3.1. VARIATIONAL SYSTEM DERIVED FROM Σ

As shown in Section 2.3, our goal is to compute the generic rank of the Jacobian matrix $\partial(Y^{(j)},\, 0 \le j \le \nu)/\partial(X,\, \Theta)$. Using relation (9), we conclude that:

$$\frac{\partial(Y^{(j)})_{0\le j\le\nu}}{\partial(X,\Theta)} = \mathsf{coeffs}\left(\frac{\partial G}{\partial X}\frac{\partial \Phi}{\partial X}, \frac{\partial G}{\partial X}\frac{\partial \Phi}{\partial \Theta} + \frac{\partial G}{\partial \Theta}\right),$$
$$\text{with } \mathsf{coeffs}\begin{pmatrix} a_{11} + a_{12}t + \mathcal{O}(t^2) \\ a_{21} + a_{22}t + \mathcal{O}(t^2) \end{pmatrix} = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix}.$$

The above equalities lead to the following relation:

$$\frac{\partial(Y^{(j)})_{0\le j\le\nu}}{\partial(X,\Theta)} = \mathsf{coeffs}\left(\nabla Y\left(\Phi, \frac{\partial \Phi}{\partial X}, \frac{\partial \Phi}{\partial \Theta}\right), t^j, j = 0, \ldots, \nu\right), \tag{10}$$

where ∇Y denote the following $n \times (n+\ell)$ matrix:

$$\nabla Y(\Phi, \Gamma, \Lambda, \Theta, U) := \left(\frac{\partial G}{\partial X}\Gamma,\ \frac{\partial G}{\partial X}\Lambda + \frac{\partial G}{\partial \Theta}\right)(\Phi, \Gamma, \Lambda, \Theta, U). \tag{11}$$

Hence, we have to determine the first $\nu = n + \ell$ terms of the power series expansion of $\Phi,\ \Gamma := \partial\Phi/\partial X$ and $\Lambda := \partial\Phi/\partial\Theta$.

VARIATIONAL SYSTEM

Let us denote by $P(\dot{X}, X, \Theta, U) = 0$, the numerators of the rational relations $\dot{X} - F$ $(X, \Theta, U) = 0$ and by ∇P the following expressions:

$$\left\{\begin{array}{ll} P(\dot{X}, X, \Theta, U), & (12.1) \\ \frac{\partial P}{\partial \dot{X}}(X, \Theta, U)\dot{\Gamma} + \frac{\partial P}{\partial X}(\dot{X}, X, \Theta, U)\Gamma, & (12.2) \\ \frac{\partial P}{\partial \dot{X}}(X, \Theta, U)\dot{\Lambda} + \frac{\partial P}{\partial X}(\dot{X}, X, \Theta, U)\Lambda + \frac{\partial P}{\partial \Theta}(\dot{X}, X, \Theta, U). & (12.3) \end{array}\right. \tag{12}$$

The power series $\Phi,\ \Gamma$ and Λ are solutions of the system of ordinary differential equations $\nabla P = 0$ with the associated initial conditions $\Gamma(X, \Theta, U, 0) := \mathrm{Id}_{n\times n}$ and $\Lambda(X, \Theta, U, 0) := 0_{n\times\ell}$. An example is given in Section 4.

3.2. COMPUTATIONAL STRATEGY

With many computer algebra systems, one can compute symbolically the expression of the formal Jacobian matrix $\partial(Y^{(j)},\, 0 \le j \le \nu)/\partial(X,\, \Theta)$. The rank computations described in Corollary 2.1 are sufficient to conclude. Furthermore, if $X,\ \Theta$ and U are specialized on some random values, these computations can be performed numerically with high probability of success.

We summarize this possible strategy in the thin arrows of the following diagram:

$$\begin{tikzcd}[column sep=huge, row sep=large]
\Sigma \arrow[r, "\text{formal computation}"] \arrow[d] & \left(\dfrac{\partial(\mathcal{L}^i G)_{0\leq i\leq \nu}}{\partial\,(X,\Theta)}\right) \arrow[d, "\begin{array}{l} X \,\to\, X_0 \in k^n, \\ \Theta \,\to\, \widetilde{\Theta} \in k^{\ell}, \\ U \,\to\, \widetilde{U} \in (k[t])^r. \end{array}"] \\
\nabla P \arrow[r, Rightarrow, "\text{numerical computation}"] & \left(\dfrac{\partial(\mathcal{L}^i G)_{0\leq i\leq \nu}}{\partial\,(X,\Theta)}\right)_{(X_0,\,\widetilde{\Theta},\,\widetilde{U})}.
\end{tikzcd}$$

As the symbolic computation of the Jacobian matrix is cumbersome, we specialize the parameters on some random integers $\widetilde{\Theta}$ and the inputs U on the power series $\widetilde{U}$ which are truncated at order $n+\ell+1$ with random integer coefficients. Then, we solve the associated system ∇P for some integer initial conditions X_0 and we compute with ∇Y the specialization of $\partial(Y^{(j)},\, 0\leq j\leq \nu)/\partial(X,\,\Theta)$ on $(X_0,\,\widetilde{\Theta})$. This approach is summarized by the thick arrows.

Remark. Let us consider in $k\{x\}$ the prime differential ideal $[\dot{x}+x^2]$. The solution $\eta=0$ is not generic while the formal power series $\eta=\sum_{i\in\mathbb{N}}(-1)^i\, {x_0}^{i+1} t^i$ is a generic solution of this differential ideal. Hence, the differential field $k\langle\eta\rangle$ and the differential field $(\mathcal{K},\mathcal{L}) := (k(x), -x^2\partial/\partial x)$ associated to the above differential ideal are isomorphic. The elementary operations—derivation, multiplication, etc.—in $\mathcal{K}$ can be done using some rewriting techniques while the same operations in $k\langle\eta\rangle$ just require the usual operations on series. The computation of the Jacobian matrix presented later is based on the same idea: we replace the computation done in $\mathcal{K}$ by a computation done on a field of power series.

Remark. The hypothesis $\partial P/\partial\dot{X}\neq 0$ assumed in Section 2 ensures that the differential system $\nabla P(\Phi,\Gamma,\Lambda,\widetilde{\Theta},\widetilde{U})=0$ admits a unique formal solution which can be computed with the Newton operator presented in the next section.

We now present an algorithm which relies on this standpoint. As we are going to replace the field $\mathcal{K}$ by a field of power series, we have to compute the generic power series solutions of ∇P. This is the subject of the following section.

3.3. a quadratic newton operator

The aim of this section is to present the Newton operator used in our algorithm. In Brent and Kung (1978), the authors show that its convergence is quadratic. We work with vector-valued expressions. Thus, the expression (12.1) (respectively (12.2), (12.3)) represents a $n\times 1$ (respectively $n\times n$ and $n\times\ell$) matrix.

encoding of the variational system derived from Σ

From a SLP of length L which encodes Σ, Theorem 2.2 allows to construct effectively another SLP of length $\mathcal{O}\big(\mathcal{N}(n+\ell)+nL\big)$ which encodes the system ∇P ($\mathcal{N}(\nu)$ denotes the cost of $\nu\times\nu$ matrix multiplication). For Φ, Γ and Λ some given series in t, this SLP computes the following $n \times (1+n+\ell)$ matrix with power series coefficients:

$$\left(\begin{array}{c|c|c} p_1(\dot\Phi,\Phi,\widetilde\Theta,\widetilde U) & \frac{\partial P}{\partial \dot X}(\Phi,\widetilde\Theta,\widetilde U)\dot\Gamma & \frac{\partial P}{\partial \dot X}(\Phi,\widetilde\Theta,\widetilde U)\dot\Lambda \quad + \\ \vdots & + & \frac{\partial P}{\partial X}(\dot\Phi,\Phi,\widetilde\Theta,\widetilde U)\Lambda + \\ p_n(\dot\Phi,\Phi,\widetilde\Theta,\widetilde U) & \frac{\partial P}{\partial X}(\dot\Phi,\Phi,\widetilde\Theta,\widetilde U)\Gamma & \frac{\partial P}{\partial \Theta}(\dot\Phi,\Phi,\widetilde\Theta,\widetilde U) \end{array}\right).$$

The expression $p_i(\dot\Phi,\Phi,\widetilde\Theta,\widetilde U)$ represents the power series in t equal to the numerator of $\dot\phi_i - f_i(\Phi,\widetilde\Theta,\widetilde U)$ and, if $\gamma_{i,j} = \partial\phi_i/\partial x_i$, the second $n \times n$ submatrix is:

$$\begin{pmatrix} \frac{\partial p_1}{\partial \dot x_1} & \cdots & \frac{\partial p_1}{\partial \dot x_n} \\ \vdots & & \vdots \\ \frac{\partial p_n}{\partial \dot x_1} & \cdots & \frac{\partial p_n}{\partial \dot x_n} \end{pmatrix}\begin{pmatrix} \dot\gamma_{1,1} & \cdots & \dot\gamma_{1,n} \\ \vdots & & \vdots \\ \dot\gamma_{n,1} & \cdots & \dot\gamma_{n,n} \end{pmatrix} + \begin{pmatrix} \frac{\partial p_1}{\partial x_1} & \cdots & \frac{\partial p_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial p_n}{\partial x_1} & \cdots & \frac{\partial p_n}{\partial x_n} \end{pmatrix}\begin{pmatrix} \gamma_{1,1} & \cdots & \gamma_{1,n} \\ \vdots & & \vdots \\ \gamma_{n,1} & \cdots & \gamma_{n,n} \end{pmatrix}.$$

Let us represent the approximation of Φ (respectively $\Lambda,\ \Gamma$) mod t^{2^j} by Φ_j (respectively $\Lambda_j,\ \Gamma_j$) and denote by E_{j+1} the correction term: $(\Phi-\Phi_j, \Gamma-\Gamma_j, \Lambda-\Lambda_j)$ mod t^{2j+1}. As usual, we construct our Newton operator from the Taylor series expansion of the function ∇P. This yields the following relations:

$$\nabla P(\Phi,\Gamma,\Lambda) = \nabla P(\Phi_j,\Gamma_j,\Lambda_j) + \frac{\partial\,\nabla P}{\partial(\dot X,\dot\Gamma,\dot\Lambda)}\dot E_{j+1} + \frac{\partial\,\nabla P}{\partial(X,\Gamma,\Lambda)}E_{j+1} + \cdots = 0.$$

The remaining terms are of order in t greater than 2^{j+1}. Thus, they are not necessary for the computation of E_{j+1}.

Remark. We consider Φ as a variable in the first column of ∇P and as a constant in the others. Thus, we have the following relations:

$$\frac{\partial\,\nabla P}{\partial(\dot X,\dot\Gamma,\dot\Lambda)} = \left(\frac{\partial P}{\partial \dot X},\frac{\partial P}{\partial \dot X},\frac{\partial P}{\partial \dot X}\right), \qquad \frac{\partial\,\nabla P}{\partial(X,\Gamma,\Lambda)} = \left(\frac{\partial P}{\partial X},\frac{\partial P}{\partial X},\frac{\partial P}{\partial X}\right).$$

The above hypothesis induces a *shift* between the order of correct coefficients of $\Lambda_j,\ \Gamma_j$ and Φ_j. In fact, Λ_j and Γ_j are correct modulo t^{2j-1}. Thus, we need to stop the following operator with $j+1 = \ln_2(n+\ell+1)$ and to repeat one more time the last resolution at the same order.

A NEWTON OPERATOR

The above hypothesis leads to a Newton operator based on the resolution of the following system of linear ordinary differential equations:

$$\frac{\partial P}{\partial \dot X}\,\dot E_{j+1} + \frac{\partial P}{\partial X}\,E_{j+1} + \nabla P = 0 \bmod t^{2^{j+1}}. \tag{13}$$

This system is solved iteratively using $(\Phi_{j+1},\Gamma_{j+1},\Lambda_{j+1}) = (\Phi_j,\Gamma_j,\Lambda_j) + E_{j+1}$ and the initial conditions $\Phi_0 \in \mathbb{Z}^n,\ \Gamma_0 := \mathrm{Id}_{n\times n}$ and $\Lambda_0 := 0_{n\times\ell}$. The resolution of the linear ordinary differential system (13) relies on the method of integrating factors. First, we consider the homogeneous system

$$\frac{\partial P}{\partial \dot X}(\Phi_j,\widetilde\Theta,\widetilde U)\,\dot W_j + \frac{\partial P}{\partial X}(\dot\Phi_j,\Phi_j,\widetilde\Theta,\widetilde U)\,W_j = 0 \bmod t^{2^{j+1}}$$

where W_j denotes a $n \times n$ unknown matrix whose coefficients are truncated series.

Input : $\dot{X} - F(X, \Theta, U),\ \ Y - G(X, \Theta, U)$
Output : Succeed, a Boolean

Preprocessing Construction of the SLP coding $\partial P/\partial \dot{X}, \partial P/\partial X, \partial P/\partial \Theta$.
Initialization Choice of a prime number;

$U \leftarrow$ Random Power Series mod $t^{n+\ell+1}$;
$\Theta \leftarrow$ Random integers; $\Phi \leftarrow$ Random integers;
Succeed $\leftarrow$ true; $\nu \leftarrow 1$; $\Lambda \leftarrow 0_{n\times \ell}$; $\Gamma \leftarrow \mathrm{Id}_{n\times n}$;

while $\nu \leq n + \ell + 1$ **do**
Compute $\partial P/\partial \dot{X},\ \partial P/\partial X$ and ∇P using U, Θ, Φ, Λ and Γ;
$W \leftarrow \mathsf{HomogeneousResolution}(\partial P/\partial \dot{X},\ \partial P/\partial X)$ mod t^{ν};
$(\Phi, \Lambda, \Gamma) \leftarrow (\Phi, \Lambda, \Gamma) + \mathsf{ConstantsVariation}(W, \nabla P)$ mod t^{ν};
$\nu \leftarrow 2\ \nu$; # Increase Order
end while

JacobianMatrix $\leftarrow \mathsf{coeffs}(\nabla Y(\Phi, \Gamma, \Lambda))$;

Test **if** $n + \ell > \mathsf{Rank}$(JacobianMatrix) **then** Succeed := false **end if**

Figure 2. Local algebraic observability test.

INTEGRATION OF THE HOMOGENEOUS SYSTEM

We consider matrices with coefficients in a series ring as series with coefficients in a matrix ring. For example, we have $A \bmod t^{2^{j+1}} = A_0 + A_1 t + \cdots + A_{2^j} t^{2^j}$ where the A_i's are matrices with coefficients in the rational field. Thus, the product, the exponential and, if A_0 is invertible, the inverse of matrices with coefficients in a series ring can be computed at precision j with the classical Newton operator (see Section 5.2 in Brent and Kung, 1978 for more details). For example, if A_0 is invertible and B_j denotes the inverse of A at order t^{2^j}, we have $B_{j+1} = 2B_j - B_j A B_j$.

Furthermore, it is a basic fact from the theory of linear ordinary systems that if $A\dot{W} + A'W = 0$ and A is invertible then $W = \exp(\int A^{-1}A')$ is a matricial solution of this system. Hence, the above homogeneous system can be solved at precision j by a procedure called $\mathsf{HomogeneousResolution}$ in Figure 2. With the same tools, one can check that the formal expression $W^{-1}\int (W(\partial P/\partial \dot{X})^{-1} \nabla P) dt$ deduced from the formula for variation of constants is a solution of system (13) (see Brent and Kung, 1978). This expression can be computed at precision j by a procedure called $\mathsf{ConstantsVariation}$ in Figure 2.

3.4. OUTLINE OF THE ALGORITHM AND ARITHMETIC COMPLEXITY ESTIMATION

We summarize our algorithm in Figure 2. This is a simplified presentation where the technical details are neglected.

A preprocessing is necessary to construct, from a SLP coding Σ, another SLP which encodes the associated variational system ∇P and the expressions used during its integration. This step relies mainly on Theorem 2.2.

The next part of the algorithm consists in the computation at order $n + \ell + 1$ of the power series solution of ∇P. We recall that in one iteration, the number of correct coefficients is doubled (see Brent and Kung, 1978).

After the main loop, the procedure coeffs evaluates ∇Y on the series Φ_j, Γ_j and Λ_j where $j = \ln_2(n + \ell + 1)$; this furnishes the coefficients of the Jacobian matrix (see Section 3.1). Last, the rank computations described in Corollary 2.1 are performed to solve the local observability problem.

Remark. If there is more than one output variable, the evaluation of ∇Y and the rank computations necessary to determine ϕ can be done in the main loop. At the end of the first iteration, ∇Y is a matrix of size $(1 + n + \ell) \times 2$ and its rank is computed; at the end of the second iteration, ∇Y is matrix of size $(1 + n + \ell) \times 4$ and its new rank is computed, etc. The computation can be stopped when the expected rank is reached or when the sequence of computed ranks becomes stationary. Thus, we can determine the necessary order of derivation ν and avoid useless computations.

Hereafter, let L denote the complexity of evaluation of the system Σ and let $\mathcal{M}(j)$ represent the multiplication complexity of two series at order $j + 1$. Using the classical multiplication formula, we have $\mathcal{M}(j) \in \mathcal{O}(j^2)$. Furthermore, let $\mathcal{N}(j)$ denote the number of arithmetic operations sufficient for the multiplication of two square $j \times j$ matrices. Using classical algorithms, we have $\mathcal{N}(j) \in \mathcal{O}(j^3)$.

Proposition 3.1. (Sedoglavic, 2001) *The number of basic arithmetic operations* $\{+, -, \times, \div\}$ *on the ground field used in the algorithm presented in Figure* 2 *is in* $\mathcal{O}(\mathcal{M}(\nu)\big(\mathcal{N}(n + \ell) + (n + m)L\big) + m\nu\mathcal{N}(n + \ell))$.

We have presented the complexity of our algorithm in terms of arithmetic operations on $\mathbb{Q}$. Such an operation requires a time proportional to the size of its operands. Using modular techniques, we control the growth of the integers involved in the computations. We now estimate an upper bound on these integers; this bound will be used in the next Section in order to estimate the probability of success of our algorithm.

3.5. growth of the integers, binary complexity and probabilistic aspects

The forthcoming estimations rely on the formal definition of the Jacobian matrix $\partial(Y^{(j)}, 0 \le j \le \nu)/\partial(X, \Theta)$ and are not dependent on the computations described in Sections 3.1 and 3.3. Let us introduce a measure for the size of a $(n + \ell + r)$-variate polynomial which influences the growth of the integers. For more details on these notions, we refer to Castro *et al.* (2001) and to the references therein.

Definition. Let $\mathcal{A}$ be a finite set of non-zero integers. The *height* of $\mathcal{A}$ is defined as $ht(\mathcal{A}) := \ln|\mathcal{A}|$ with $|\mathcal{A}| := \max\{|\alpha| + 1, \alpha \in \mathcal{A}\}$. The height of a polynomial with integer coefficients is defined by the height of its set of coefficients.

We use the notations introduced in Section 1.1 and we denote by h (respectively d) the maximum height (respectively degree) of the numerator and of the denominator of the expression involved in system Σ.

Proposition 3.2. (Sedoglavic, 2001) *Let* h_0 *be the maximum of heights of the integers* X_0, $\widetilde{\Theta}$ *and of the integer coefficients of* $\widetilde{U}$. *We have,*

- $ht\big(\mathrm{denom}\, Y^{(j)}\,(X_0)\big) \leq (2j+1)(n+m)\Big(h + d(h_0 + 2\ln(n+\ell+r+1))\Big)$;
- $ht\big(\mathrm{numer}\, Y^{(j)}(X_0)\big) \leq (2j+1)(n+m)((2\ln(n+\ell+r+1)+h_0)d+h)$
  $+ (j+1)\ln 2n(n+m)d + (2j+1)\ln(2j+1)$.

MODULAR COMPUTATION

Hence the size of the coefficients of the final specialized Jacobian matrix is mainly linear in the differentiation index ν. But some intermediate computations require integers of bigger size. In order to design an efficient algorithm, we have to avoid this growth using modular techniques.

REMARK. Almost all the operations used in our algorithm can be performed on a finite field $\mathbb{F}_p$. But, when we choose a prime number p, we have to avoid the cancellation of $\partial P/\partial \dot{X}$ mod t and of the determinant of $\partial(Y^{(j)},\, 0 \leq j \leq \nu)/\partial(X,\, \Theta)$.

REMARK. The cancellation of $\partial P/\partial \dot{X}$ mod t can be checked at the beginning of our algorithm. Thus, the probabilistic aspects concern mainly the choice of specialization and of a prime number s.t. the determinant of $\partial(Y^{(j)},\, 0 \leq j \leq \nu)/\partial(X,\, \Theta)$ does not vanish modulo p when this matrix is of full generic rank. The Proposition 3.2 leads to the following estimation.

PROPOSITION 3.3. (SEDOGLAVIC, 2001) *Let μ be a positive integer and κ be $(2\ln(n+\ell+r+1)+\ln D)D+(n+\ell)(2\nu+1)((n+m)h+\ln 2nD)$ with D equal to $(n+\ell)(2\nu+1)(n+m)d$. If $\partial(Y^{(j)},\, 0 \leq j \leq \nu)/\partial(X,\, \Theta)$ is of full generic rank then the determinant of this matrix specialized on random integers in $\{0,\ldots,\mu D\}$ is not divisible by a prime number $p > 2\kappa\mu$ with probability at least $(1-1/\mu)^2$.*

4. Computation of Symmetries (Example)

In this section, we present—by an example—a method which allows to compute an infinite group of symmetries of a non-observable model letting its output and input be invariant. Moreover, we explain some computations presented in the previous section. To do so, we consider the example (8):

$$\begin{cases} \dot{x}_1 = \theta_1\, {x_1}^2 + \theta_2\, x_1\, x_2 + u, \\ \dot{x}_2 = \theta_3\, {x_1}^2 + \theta_4\, x_1\, x_2, \\ y = x_1,\ \dot{u} \neq 0,\ \dot{\theta}_1 = \dot{\theta}_2 = \dot{\theta}_3 = \dot{\theta}_4 = 0. \end{cases}$$

In the next section, we recall the relationship between an automorphism and some derivation of the field $\mathcal{K}$.

4.1. AUTOMORPHISM AND DERIVATION

Let us consider the above non-observable model, the associated field extension $\mathcal{G} \hookrightarrow \mathcal{G}(X,\Theta)$ and σ_λ the infinite group of automorphisms which act on $\mathcal{G}(X,\Theta)$ and leave $\mathcal{G}$ invariant. The expression σ_λ defined earlier can be considered as a mapping from a field of constant into the set of automorphism of $\mathcal{G}(X,\Theta)$. Hence, one can consider the following map:

$$\partial = \frac{\partial \sigma_{1+\lambda}}{\partial \lambda}\Big|_{\lambda=0} : \quad \mathcal{G}(X,\Theta) \to \mathcal{G}(X,\Theta).$$

From the definition of σ_λ, we have:

- property (5) implies that for all c in $\mathcal{G}$, $\partial(c)$ is equal to zero;
- properties (6) and (7) imply that ∂ is $\mathcal{G}$-linear;
- property (7) implies that ∂ satisfies Leibniz rule.

Hence, ∂ is a derivation in $\mathrm{Der}_{\mathcal{G}}(\mathcal{G}(X,\Theta),\mathcal{G}(X,\Theta))$ associated to σ_λ. In the case of the model (8), we have: $\partial = x_2\partial/\partial x_2 - \theta_2\partial/\partial\theta_2 + \theta_3\partial/\partial\theta_3$, if $\mathrm{Der}_{\mathcal{G}}(\mathcal{G}(X,\Theta),\mathcal{G}(X,\Theta))$ is considered as a subspace of the $\mathcal{G}(X,\Theta)$-vector space generated by the usual derivations $\partial/\partial x_1,\ldots,\partial/\partial x_n,\partial/\partial\theta_1,\ldots,\partial/\partial\theta_\ell$.

In Section 4, we are going to consider the opposite situation. First, we notice that, after the use of the algorithm described in Section 3, we know that the variable x_2 and the parameters θ_2,θ_3 are not observable. Then, we are going to use a maximal singular minor of the Jacobian matrix $\partial(Y^{(j)},\, 0\le j\le\nu)/\partial(X,\,\Theta)$ in order to determine a derivation in $\mathrm{Der}_{\mathcal{G}}(\mathcal{G}(X,\Theta),\mathcal{G}(X,\Theta))$. With this derivation, we are going to determine an infinite group of $\mathcal{G}(X,\Theta)$-automorphisms.

4.2. Variational system and seminumerical computations

Proposition 2.1 shows that all our computations can be performed up to the order of derivation 6. Hence, we specialize the input u on the following generic series $1+37\,t+45\,t^2+13\,t^3+34\,t^4+12\,t^5+67\,t^6$. Furthermore, in the computations done later, the order of all series does not exceed 6. Thus, we use the following system of ordinary differential equations in our computation:

$$\begin{cases} \dot{x}_1 = \theta_1\,{x_1}^2 + \theta_2\,x_1\,x_2 + 1 + 37\,t + 45\,t^2 + 13\,t^3 + 34\,t^4 + 12\,t^5 + 67\,t^6, \\ \dot{x}_2 = \theta_3\,{x_1}^2 + \theta_4\,x_1\,x_2. \end{cases} \tag{14}$$

With the notation used in Section 3.1 and in order to construct the variational system, we associate to system (14) the following systems of ordinary differential equations

$$\begin{pmatrix} \dot\gamma_{11} & \dot\gamma_{12} \\ \dot\gamma_{21} & \dot\gamma_{22} \end{pmatrix} = \begin{pmatrix} 2\,\theta_1\,x_1+\theta_2\,x_2 & \theta_2\,x_1 \\ 2\,\theta_3\,x_1+\theta_4\,x_2 & \theta_4\,x_1 \end{pmatrix}\begin{pmatrix} \gamma_{11} & \gamma_{12} \\ \gamma_{21} & \gamma_{22} \end{pmatrix}, \tag{15}$$

$$\begin{pmatrix} \dot\lambda_{11} & \dot\lambda_{12} & \dot\lambda_{13} & \dot\lambda_{14} \\ \dot\lambda_{21} & \dot\lambda_{22} & \dot\lambda_{23} & \dot\lambda_{24} \end{pmatrix} = \begin{pmatrix} 2\,\theta_1\,x_1+\theta_2\,x_2 & \theta_2\,x_1 \\ 2\,\theta_3\,x_1+\theta_4\,x_2 & \theta_4\,x_1 \end{pmatrix}\begin{pmatrix} \lambda_{11} & \lambda_{12} & \lambda_{13} & \lambda_{14} \\ \lambda_{21} & \lambda_{22} & \lambda_{23} & \lambda_{24} \end{pmatrix} + \begin{pmatrix} {x_1}^2 & x_1\,x_2 & 0 & 0 \\ 0 & 0 & {x_1}^2 & x_1\,x_2 \end{pmatrix}, \tag{16}$$

where $\gamma_{i,j}=\partial\bar{x}_i/\partial x_j$ ($\bar{x}_i$ is a series and x_j an initial condition) and $\lambda_{i,j}=\partial\bar{x}_i/\partial\theta_j$. The power series solution of these systems of ordinary equations can be computed up to order 6 with the techniques presented in Section 3.3.

First, the initial conditions and the parameters are specialized on some generic values in a finite field; the whole resolution of systems (14), (15) and (16) is done on a finite field. Using relation (11), we compute the Jacobian matrix $\partial(Y^{(j)},\, 0\le j\le\nu)/\partial(X,\,\Theta)$ and using Corollary 2.1, we conclude that the variable x_1 and the parameters θ_1 and θ_4 are observable.

Hence, if we denote by $\mathcal{F}$ the differential field $k\langle U,Y\rangle(x_1,\theta_1,\theta_4)$, we have the differential field extensions: $k\langle U,Y\rangle \hookrightarrow \mathcal{F} \hookrightarrow \mathcal{K}$. The left-hand extension is algebraic and the right one is transcendental of degree one.

The observable quantities are not significant in the sequel and we specialize them on some generic value. In our example, we take $\theta_1 = 16, \theta_4 = 7$ and the initial condition $x_1(0) = 3$. The variable x_2 and the parameters θ_2 and θ_3 are not specialized and all the following computations are made in the field $\mathbb{Q}(x_2, \theta_2, \theta_3)$.

4.3. A DESCRIPTION OF $Der_{\mathcal{F}}(\mathcal{K}, \mathcal{K})$

Again, and as explained in Section 3.1, integrating the system of ordinary equations defined by (14), (15) and (16) with the associated initial values, one can retrieve the matrix $\partial(Y^{(j)}, 0 \le j \le \nu)/\partial(X, \Theta)$. In our example, the largest singular minor of this matrix is:

$$\begin{pmatrix} \frac{\partial \dot{y}}{\partial x_2} & \frac{\partial \dot{y}}{\partial \theta_2} & \frac{\partial \dot{y}}{\partial \theta_3} \\ \frac{\partial \ddot{y}}{\partial x_2} & \frac{\partial \ddot{y}}{\partial \theta_2} & \frac{\partial \ddot{y}}{\partial \theta_3} \\ \frac{\partial y^{(3)}}{\partial x_2} & \frac{\partial y^{(3)}}{\partial \theta_2} & \frac{\partial y^{(3)}}{\partial \theta_3} \end{pmatrix} = \mathsf{coeffs}\left(\frac{\partial y}{\partial x_2}(t), \frac{\partial y}{\partial \theta_2}(t), \frac{\partial y}{\partial \theta_3}(t)\right) = \mathsf{coeffs}\Big(\gamma_{12}, \lambda_{12}, \lambda_{13}\Big).$$

For demonstration purposes, the transposed of this minor is given below.

$$\begin{pmatrix} 3\,x_2 & \frac{27}{2}\,\theta_3 + 248\,x_2 + 3\,\theta_2\,{x_2}^2 & \left(\frac{99871}{6} + \left(x_2\left(\frac{1261}{3} + \frac{3}{2}\,\theta_2 x_2\right) + 45\,\theta_3\right)\theta_2\right)x_2 + \frac{2793}{2}\,\theta_3 \\ 0 & 27\,\theta_2/2 & 3\,\theta_2\left(15\,\theta_2\,x_2 + 931\right)/2 \\ 3\,\theta_2 & \theta_2\left(248 + 3\,\theta_2\,x_2\right) & \theta_2\left(99871 + \left(x_2(2522 + 9\,\theta_2 x_2) + 135\,\theta_3\right)\theta_2\right)/6 \end{pmatrix}.$$

Thus, one can check that its kernel is $(x_2, -\theta_2, \theta_3)$. Hence, as explained in Section 2.3, the $\mathcal{F}$-vector space $\mathrm{Der}_{\mathcal{F}}(\mathcal{K}, \mathcal{K})$ is generated by the derivation $\partial = x_2\partial/\partial x_2 - \theta_2\partial/\partial\theta_2 + \theta_3\partial/\partial\theta_3$ (compare with the computations done earlier).

COMPUTATION OF THE GROUP OF SYMMETRIES

As noticed in Section 2.1, one can associate to the derivation ∂ a vector field defined in the space of coordinates $(x_2, \theta_2, \theta_3)$. In fact, ∂ is the Lie derivation of the vector field defined by $\partial x_2(\tau)/\partial\tau = x_2(\tau)$, $\partial\theta_2(\tau)/\partial\tau = -\theta_2(\tau)$ and $\partial\theta_3(\tau)/\partial\tau = \theta_3(\tau)$. For the set of initial conditions $x_2(0) = x_2,\ \theta_2(0) = \theta_2,\ \theta_3(0) = \theta_3$, this system has a closed form solution $x_2(\tau) = x_2 \exp(\tau)$, $\theta_2(\tau) = \theta_2 \exp(-\tau)$ and $\theta_3(\tau) = \theta_3 \exp(\tau)$. This solution defines a group of diffeomorphisms of the space of coordinates $(x_2, \theta_2, \theta_3)$ which is associated to the desired infinite group in $\mathrm{Aut}_{\mathcal{F}}(\mathcal{K}, \mathcal{K})$.

In our algebraic framework, we consider the following morphism:

$$\begin{array}{cccc} \mathrm{e}^{\tau\partial} & : & \mathcal{K} & \rightarrow & \mathcal{K}[[\tau]] \\ & & \eta & \rightarrow & \sum_{i\in\mathbb{N}} \partial^{\,i}(\eta)\,\tau^i/i!. \end{array}$$

For the derivation studied here, we notice that ∂x_2 is equal to x_2 and that we have similar formulae for the other non-observable quantities. Hence, if we denote the series $\exp(\tau)$ by λ, the morphism $\mathrm{e}^{\tau\partial}$ from $\mathcal{K}$ in $\mathcal{K}(\lambda)$ defines a multiplicative group in $\mathrm{Aut}_{\mathcal{F}}(\mathcal{K}, \mathcal{K})$.

REMARK. The solution of the above vector field is in a *closed form*, that is the image of the morphism $\mathrm{e}^{\tau\partial}$ is $\mathcal{K}(\lambda)$. We notice that all the encountered examples present this property, but we cannot certify that this fact is always true. We just know that this image is an algebraic extension of $\mathcal{K}(\lambda)$.

Remark. The following example taken from Raksanyi (1986) shows that the group of symmetries can be more complicated than a simple homothety:

$$\begin{cases} \dot{x}_1 = u - (c_1 + c_2)x_1, \\ \dot{x}_2 = c_1x_1 - (c_3 + c_6 + c_7)x_2 + c_5x_4, \\ \dot{x}_3 = c_2x_1 + c_3x_2 - c_4x_3, \\ \dot{x}_4 = c_6x_2 - c_5x_4, \\ y_1 = c_8x_3, \\ y_2 = c_9x_2. \end{cases}$$

Our Maple implementation gives the following results:

- the variables $\{x_2, x_3, x_4\}$ and the parameters $\{c_1, c_2, c_3, c_7, c_8, c_9\}$ are not observable;
- the transcendence degree of the field extension $k\langle U, Y\rangle \hookrightarrow \mathcal{K}$ is 1.

Using the method presented earlier, we compute the following generators of the vector space $\mathrm{Der}_{\mathcal{F}}(\mathcal{K}, \mathcal{K})$:

$$c_1\left(\frac{\partial}{\partial c_1} - \frac{\partial}{\partial c_2}\right) - \frac{c_3(c_1+c_2)}{c_2}\left(\frac{\partial}{\partial c_3} - \frac{\partial}{\partial c_7}\right) + \frac{c_1c_8}{c_2}\frac{\partial}{\partial c_8} - c_9\frac{\partial}{\partial c_9} + x_2\frac{\partial}{\partial x_2} \\ - \frac{x_3c_1}{c_2}\frac{\partial}{\partial x_3} + x_4\frac{\partial}{\partial x_4}.$$

Integrating this vector field, we found the following associated family of symmetries indexed by λ:

$$\begin{array}{lcc lcc} x_2 & \rightarrow & \lambda x_2, & c_3 & \rightarrow & ((1-\lambda)c_1 + c_2)c_3/\lambda c_2, \\ x_3 & \rightarrow & ((1-\lambda)c_1 + c_2)x_3/c_2, & c_7 & \rightarrow & c_7 - c_3(c_1+c_2)(1-\lambda)/\lambda c_2, \\ x_4 & \rightarrow & \lambda x_4, & c_8 & \rightarrow & c_8c_2/((1-\lambda)c_1 + c_2), \\ c_1 & \rightarrow & \lambda c_1, & c_9 & \rightarrow & c_9/\lambda. \\ c_2 & \rightarrow & (1-\lambda)c_1 + c_2, & & & \end{array} \tag{17}$$

Let us be more precise. Given any generator ∂ of $\mathrm{Der}_{\mathcal{F}}(\mathcal{K}, \mathcal{K})$, one can obtain by a simple division another generator such that—for example—the derivative ∂c_1 is equal to c_1. The algorithm presented in Section 3 shows that the transcendence degree of the field $\mathcal{K}$ over $\mathcal{F}$ is 1. Hence, $\mathcal{K}$ is algebraic over $\mathcal{F}(c_1)$. If this field is rational over $\mathcal{F}(c_1)$ then the image of the morphism $\mathrm{e}^{\tau\partial}$ is $\mathcal{K}(\lambda)$. We notice that all the systems encountered in practice are of that type. In this case, one can use the Hermite–Pade approximates in order to determine the group of symmetries. In fact, we have the following theorem.

Theorem 4.1. (Beckermann and Labahn, 1992) *For every power series $s_1, \ldots, s_n$ in $k[[\tau]]$ there exists polynomials $p_1, \ldots, p_n$ in $k[\tau]$ of degree $d_1, \ldots, d_n$ called Hermite–Pade approximates of type $(d_1, \ldots, d_n)$ such that*

$$\exists\, i \in \{1, \ldots, n\} \mid p_i \neq 0 \qquad \text{and} \qquad \sum_{i=1}^{n} p_i s_i = \mathcal{O}\big(\tau^{\sum_{i=1}^{n} d_i + n - 1}\big).$$

One can compute for any v in the set of non-observable quantities $\{x_2, \ldots, c_9\}$ an approximation of the series $\mathrm{e}^{\tau\partial}(v)$ and the Hermite–Pade approximates of type 0 of the series 1, $\exp(\tau)$, $\mathrm{e}^{\tau\partial}(v)$ and $\exp(\tau)\mathrm{e}^{\tau\partial}(v)$ in $\mathbb{Q}(x_2, \ldots, c_9)[[\tau]]$. These approximates allow us to explain the image (17) of $\mathcal{K}$ by $e^{\tau\partial}$. For the above system, we have $c_2 e^{\tau\partial}(x_3)/\, x_3 - (c_1 + c_2) + c_1 \exp(\tau) = 0$ and we conclude that the image of $e^{\tau\partial}(x_3)$ is $((1-\lambda)c_1 + c_2)x_3/c_2$. In this expression, the degree in λ is 1. But, it could be necessary to compute Hermite–Pade approximates of type 0 of the series 1, $\exp(\tau), \ldots, \exp(j\tau)$, $e^{\tau\partial}(v), \ldots, \exp(j\tau)\, e^{\tau\partial}(v)$; again, we notice that we never encountered any real-word system such that j is greater than 2.

Remark. The computations described above require 1.18 s on a PC Pentium III (650 MHz) using Maple. The limiting parts of the automorphism determination is the integration of the variational system using the field $\mathbb{Q}(v_1, \ldots, v_i)$—the v_i's represent non-observable variables and parameters—and the computation of the kernel. Thus, its complexity is exponential in the input size.

5. Conclusion

We have presented a probabilistic polynomial-time algorithm that computes the set of model observable variables and gives the number of non-observable variables which should be assumed to be known in order to obtain an observable system. Our algorithm is mainly based on generic rank computation. As shown in Corollary 2.1, the local observability property is associated to the fact that the used Jacobian matrix is of full rank. Hence, when our process states that a system is observable, this answer is certainly correct. Furthermore, as we are able to compute a group of symmetries for almost all systems encountered in practice, we are able to certify our result. This last computation cannot, to our knowledge, be performed in a polynomial time.

Using the approach presented here and the elimination algorithm presented in Giusti *et al.* (2001) and Schost (2000), one can test the global observability and retrieve the relations between the state variables, the outputs and the inputs. A forthcoming paper will be devoted to this aspect.

References

Baur, W., Strassen, V. (1983). The complexity of partial derivatives. *Theor. Comput. Sci.*, **22**, 317–330.

Beckermann, B., Labahn, G. (1992). A uniform approach for Hermite Padé and simultaneous Padé approximants and their matrix-type generalizations. *Numer. Algorithms*, **3**, 45–54.

Boulier, F. Efficient computation of regular differential systems by change of rankings using Kähler differentials. Preprint 1999-14, LIFL, Université de Lille I, 1999. `http://www.lifl.fr/~boulier`.

Boulier, F., Lazard, D., Ollivier, F., Petitot, M. (1995). Representation for the radical of a finitely generated differential ideal. In Levelt, A. H. M. ed., *Proceedings of ISSAC 1995*, pp. 158–166. ACM.

Brent, R. P., Kung, H. T. (October 1978). Fast algorithms for manipulating formal power series. *J. ACM*, **25**, 581–595.

Bürgisser, P., Clausen, M., Shokrollahi, M. A. (1997). *Algebraic Complexity Theory*, volume 315 of *GMW*, Springer.

Castro, D., Hägele, K., Morais, J. E., Pardo, L. M. (2001). Kronecker's and Newton's approaches to solving: a first comparison. *J. Complexity*, **17**, 212–303.

Diop, S., Fliess, M. (1991). On nonlinear observability. In Commault, C., *et al.*, eds, *Proceedings of ECC'91*, volume 1, pp. 152–157. Hermès.

Eisenbud, D. (1994). *Commutative Algebra with a View Toward Algebraic Geometry.* Volume 150 of *Graduate Texts in Mathematics*, Springer.

Fliess, M. (1989). Automatique et corps différentiels. *Forum Math*, **1**, 227–238.

Gallo, G., Mishra, B. (1991). Efficient algorithms and bounds for Wu-Ritt characteristic sets. In Mora, F., Traverso, C. eds, *Proceedings of MEGA'90,* volume 94 of *Progress in Mathematics*, pp. 119–142. Birkhäuser.

Giusti, M., Lecerf, G., Salvy, B. (2001). A Gröbner free alternative for polynomial systems solving. *J. Complexity*, **17**, 154–211.

Goldbeter, A. (1995). A model for circadian oscillations in the Drosophila period protein. In *Proceedings of the Royal Society London*, B (261), pp. 319–324.
Hermann, R., Krener, A. J. (1977). Nonlinear controllability and observability. *IEEE Trans. Autom. Control*, **AC-22**, 728–740.
Hubert, É. (April/May 2000). Factorisation free decomposition algorithms in differential algebra. *J. Symb. Comput.*, **29**, 641–662.
Johnson, J. (1969). Kähler differentials and differential algebra. *Ann. Math.*, **89**, 92–98.
Kalman, R. E. (1961). On the general theory of control systems. In *Proceedings of ICAC'61*, volume 1, pp. 481–492. London, Butterworths Publication.
Kolchin, E. R. (1973). *Differential Algebra and Algebraic Groups.* New York, Academic.
Ljung, L. (1987). *System Identification—Theory for the User.* PTR Prentice Hall.
Ljung, L., Glad, T. (1990). Parametrization of nonlinear model structures as linear regressions. In *11th IFAC Word Congress*, pp. 67–71.
Ollivier, F. (June 1990). Le problème de l'identifiabilité structurelle globale: approche théorique, méthodes effectives et bornes de complexité. Ph.D. Thesis, École polytechnique.
Pohjanpalo, H. (1978). System identifiability based on the power series expansion of the solution. *Math. Biosci.*, **41**, 21–33.
Raksanyi, A. (1986). Utilisation du calcul formel pour l'étude des systèmes d'équations polynomiales (applications en modélisation). Ph.D. Thesis, Univ. Paris IX.
Ritt, J. F. (1966). *Differential Algebra*, Dover.
Sadik, B. (2000). A bound for the order of characteristic set elements of an ordinary prime differential ideal and some applications. *AAECC*, **10**, 251–268.
Schost, É. (December 2000). Sur la résolution des systèmes polynomiaux à paramètres. Ph.D. Thesis, École polytechnique.
Sedoglavic, A. (2001). A probabilistic algorithm to test local algebraic observability in polynomial time. In Mourrain, B. ed., *Proceedings of ISSAC 2001*, pp. 309–316. ACM Press.
Vajda, S., Godfrey, K. R., Rabitz, H. (1989). Similarity transformation approach to identifiability analysis of non linear comportemental models. *Math. Biosci.*, **93**, 217–248.
Valiant, L. G. (1982). Reducibility by algebraic projections. *L'enseig. Math., IIe Séries*, **28**, 253–268.
Walter, É. (1982). *Identifiability of State Space Model,* volume 46 of *Lectures Notes in Biomathematics*, New York, Springer.

Received 12 November 2001
Accepted 27 February 2002