Journal of Symbolic Computation 46 (2011) 1114–1138

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

A geometric index reduction method for implicit systems of differential algebraic equations

L. D'Alfonso [a], G. Jeronimo [b,c], F. Ollivier [d,1], A. Sedoglavic [e], P. Solernó [b,c]

[a] Departamento de Ciencias Exactas, Ciclo Básico Común, Universidad de Buenos Aires, Ciudad Universitaria, 1428 Buenos Aires, Argentina

[b] Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, 1428 Buenos Aires, Argentina

[c] CONICET, Argentina

[d] LIX, UMR CNRS – École Polytechnique no 7161, F-91128 Palaiseau, France

[e] LIFL, UMR CNRS – Université de Lille I no 8022, F-59655 Villeneuve d'Ascq, France

ARTICLE INFO

Article history:
Received 26 August 2010
Accepted 20 May 2011
Available online 13 June 2011

Keywords:
Implicit systems of Differential Algebraic Equations
Index
Kronecker algorithm
Geometric resolution

ABSTRACT

This paper deals with the index reduction problem for the class of quasi-regular DAE systems. It is shown that any of these systems can be transformed to a generically equivalent first order DAE system consisting of a single purely algebraic (polynomial) equation plus an under-determined ODE (a *differential Kronecker representation*) in as many variables as the order of the input system. This can be done by means of a Kronecker-type algorithm with bounded complexity.

1. Introduction

In this paper, we consider implicit, ordinary differential algebraic equation (DAE) systems

$$\Sigma := \begin{cases} f_1\left(X, \dot{X}, \dots, X^{(e_1)}\right) = 0, \\ \qquad\vdots \\ f_n\left(X, \dot{X}, \dots, X^{(e_n)}\right) = 0, \end{cases} \tag{1}$$

E-mail addresses: lisi@cbc.uba.ar (L. D'Alfonso), jeronimo@dm.uba.ar (G. Jeronimo), francois.ollivier@lix.polytechnique.fr (F. Ollivier), Alexandre.Sedoglavic@univ-lille1.fr (A. Sedoglavic), psolerno@dm.uba.ar (P. Solernó).

[1] Tel.: +33 1 69 33 40 58; fax: +33 1 69 33 41 58.

0747-7171/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2011.05.012

where, for any integer i, $1 \leq i \leq n$, f_i is a polynomial in the variables $X := \{x_1, \ldots, x_n\}$ and in their jth ($1 \leq j \leq e_i$) time derivatives $X^{(j)} := \left\{{x_1}^{(j)}, \ldots, {x_n}^{(j)}\right\}$, with coefficients in a differential field $\mathbb{K}$ of characteristic 0.

One of the main invariants of DAE systems is their *differentiation index*. There are several definitions of differentiation indices not all completely equivalent (see for instance Brenan et al., 1996; Campbell and Gear, 1995; Fliess et al., 1995; Kunkel and Mehrmann, 2006; Le Vey, 1994; Pantelides, 1988; Poulsen, 2001; Pritchard and Sit, 2007; Pryce, 2001; Rabier and Rheinboldt, 1994; Reid et al., 2001; Seiler, 1999), but in every case it represents a measure of the implicitness of the given system in a fixed coordinates set. For instance, for first order equations, differentiation indices provide bounds for the number of total derivatives of the system needed in order to obtain in the same set of coordinates an explicit ODE system which is verified by all the solutions of the original system (see Brenan et al. 1996, Definition 2.2.2).

Since explicitness is strongly related to the existence of classical solutions, a differentiation index should also bound the number of derivatives needed in order to obtain existence and uniqueness theorems (see Pritchard, 2003; Pritchard and Sit, 2007; Rabier and Rheinboldt, 1994). From the point of view of numerical resolution, it is desirable for the DAE to have an index as small as possible. As shown in Brenan et al. (1996, Section 2.5.3), for first order systems a reduction of the index can be achieved by differentiating the algebraic constraints, but the numerical solution of the resulting system do not satisfy necessarily the original equations.

Main contributions. In this article we address the index reduction problem for a ubiquitous class of quasi-regular DAE systems (see Sections 2.2 and 2.3). We show that any of these systems is generically equivalent to a related (in a non-intrinsic way) first order DAE system $\underline{\Sigma}$ with a particular structure. This new system consists of a single purely algebraic (polynomial) equation plus an under-determined ODE (see Definition 4). Indeed, $\underline{\Sigma}$ would be a *semi-explicit DAE system* in the usual sense *outside a hypersurface* (see for instance Brenan et al. (1996, Section 1.2)) with differentiation index 1 (see Proposition 11). It is a well-known fact that this class of systems can be handled successfully by means of numerical methods (see Petzold and Lötstedt, 1986; Lötstedt and Petzold, 1986; Brenan, 1983). We will refer to $\underline{\Sigma}$ as a *(differential) Kronecker representation* (cf. Giusti et al., 2001).

In order to illustrate our construction, let us consider a DAE system Σ in three differential variables x, y, λ arising from a variational problem describing the motion of a pendulum of length 1, where g is the gravitational constant and the unknown λ is a Lagrange multiplier:

$$\Sigma = \begin{cases} x^{(2)} - \lambda x &= 0, \\ y^{(2)} - \lambda y + g = 0, \\ x^2 + y^2 - 1 &= 0. \end{cases} \tag{2}$$

The differentiation index of Σ is $\sigma = 4$, as shown in D'Alfonso et al. (2009, Example 2). For this system, our algorithm computes the following index 1 differential Kronecker representation

$$\underline{\Sigma} = \begin{cases} \dot{u_1} &= u_2, \\ \dot{u_2} &= u_1\left(g\upsilon - \frac{{u_2}^2}{(1-{u_1}^2)}\right), \\ \upsilon^2 + {u_1}^2 - 1 = 0. \end{cases}$$

Note that the first two equations in $\underline{\Sigma}$ form an under-determined ODE, whereas the last one is purely algebraic.

The index reduction problem has already been considered in several previous articles (see for instance Gear, 1988, 1989; Kunkel and Mehrmann, 2006; Mattsson and Söderlind, 1993). The techniques applied in these works are based on the computation of sufficiently many successive derivatives of the original equations combined with rewriting procedures relying on the Implicit Function Theorem, elimination of critical equations, introduction of dummy derivatives, etc.

Our approach also makes use of the computation of successive derivatives, as many as the index, but, unlike the methods mentioned above, we deal with the system of all these new equations in a purely algebraic way. This new system defines an algebraic variety in a suitable jet space and we parametrize this variety by means of the points of a hypersurface. This construction, originally introduced by Kronecker, is known as a *geometric resolution* (see Giusti et al., 2001; Schost, 2003; Durvye and Lecerf, 2007 and the references therein). In order to keep track of the differential structure, we use the parametrizations to construct a vector field over the hypersurface defining the Kronecker representation $\underline{\Sigma}$. A result of the same flavor (i.e. a univariate differential equation plus parametrizations of the variables) may be given by means of the notion of primitive element of an extension of differential fields. This construction, due to (Ritt (1932), see also Seidenberg, 1952), is known as a *resolvent representation* of the system Σ (see Cluzeau and Hubert, 2003, 2008; D'Alfonso et al., 2006 for effective versions of it).

With respect to most known index reduction approaches, our method is symbolic and, in some sense, automatic: it does not make use of the Implicit Function Theorem as it is the case in Gear (1988) or Gear (1989) and it does not rely on any smart choice of ad hoc equations as in Kunkel and Mehrmann (2006). A previous purely algebraic approach to this problem can be found in Pritchard and Sit (2007), where an algorithm for index reduction relying on Gröbner bases computations is constructed.

The construction proposed in this paper can be done algorithmically within an admissible complexity by applying well-known techniques from computer algebra (see Schost, 2003; Lecerf, 2003). However, our approach only works under certain assumptions on the input system (for instance, quasi-regularity, primality of the differential ideal and of algebraic prolongation ideals) which we are not able to check effectively. In addition, our algorithms make some random choices of parameters in order to fulfill generic conditions. This introduces an error probability that could be estimated from upper bounds on the degrees of polynomials giving the conditions by applying the Zippel–Schwartz principle (see Zippel, 1979; Schwartz, 1980).

The number of variables of our Kronecker representation is the order of the *differential ideal* associated to the input system plus one and it is always lower than those involved in the index reduction methods of previous papers. In the first order case, where it is easy to compare, this number is at most $n + 1$ and in the general case, it is bounded by the Jacobi number of the system (see Jacobi, 1865; Kondratieva et al., 1982; Ollivier and Sadik, 2007; D'Alfonso et al., 2009). A further advantage of our method is that it preserves the constraints of the initial conditions of the original system and then we do not need to compute constants of integration.

Outline. The paper is organized as follows: in Section 2, the basic notions and previous results needed throughout the article are introduced. The core of the paper is in Section 3 where the Kronecker representation $\underline{\Sigma}$ is constructed. In Section 4, we study the relation between the solutions of both systems Σ and $\underline{\Sigma}$. Finally, two appendices are included: the first one contains some Bertini-type results from commutative algebra we need and the second one is devoted to existence and uniqueness theorems for DAE systems.

2. Preliminaries

In this section, we introduce some notations used throughout the paper and we recall some basic definitions from elementary (differential) algebraic geometry for the readers' convenience. Furthermore, we discuss the assumptions on the systems considered and some results concerning the differentiation index and the order of these systems. Finally, we recall briefly the notion of geometric resolution and the complexity to compute it.

2.1. Basic notions and notations

Let $\mathbb{K}$ be a characteristic zero field equipped with a derivation δ. For instance $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$ with $\delta = 0$, or $\mathbb{K} = \mathbb{Q}(t)$ with the usual derivation $\delta(t) = 1$, etc.

As in the Introduction, for any set of $X := \{x_1, \dots, x_n\}$ of n (differential) indeterminates over $\mathbb{K}$, we denote by ${x_i}^{(j)}$ the jth successive formal derivative of the variable x_i (following Newton's notation, its first derivative is also denoted by $\dot{x}_i$) and we use the following notations:

$$X^{(j)} := \left\{{x_1}^{(j)}, \dots, {x_n}^{(j)}\right\} \quad \text{and} \quad X^{[j]} := \left\{X, \dot{X}, X^{(2)}, \dots, X^{(j)}\right\}.$$

The derivation δ can be extended to a derivation in the polynomial ring $\mathbb{K}\left[X^{(j)},\ j \in \mathbb{N}_0\right]$ as follows: for any differential polynomial q in $\mathbb{K}\left[X^{(j)},\ j \in \mathbb{N}_0\right]$ the following classical recursive relations hold for the successive total derivatives of q:

$$q^{(0)} := q, \qquad q^{(j)} := \delta\left|q^{(j-1)}\right| + \sum_{h\in\mathbb{N}_0}\sum_{1\le i\le n} \frac{\partial q^{(j-1)}}{\partial {x_i}^{(h)}} {x_i}^{(h+1)}, \quad \text{for } j \ge 1,$$

where $\delta\left|q^{(j-1)}\right|$ denotes the polynomial obtained from $q^{(j-1)}$ by applying the derivative δ to all its coefficients. The (non-Noetherian) polynomial ring $\mathbb{K}\left[X^{(j)},\ j \in \mathbb{N}_0\right]$ with this derivation is denoted by $\mathbb{K}\{x_1, \dots, x_n\}$ (or simply $\mathbb{K}\{X\}$) and is called the ring of *differential polynomials*.

Given a finite set of (differential) polynomials $Q := \{q_1, \dots, q_\nu\}$ in $\mathbb{K}\{X\}$, we write $[Q]$ to denote the smallest ideal of $\mathbb{K}\{X\}$ stable under differentiation, i.e. the smallest ideal containing $q_1, \dots, q_\nu$ and all their derivatives of arbitrary order. The ideal $[Q]$ is called the *differential ideal* generated by Q. Furthermore, for every integer j, we extend our previous notations as follows :

$$Q^{(j)} := \left\{{q_1}^{(j)}, \dots, {q_\nu}^{(j)}\right\} \quad \text{and} \quad Q^{[j]} := \left\{Q, \dot{Q}, Q^{(2)}, \dots, Q^{(j)}\right\}.$$

Let us introduce also some notions concerning elementary algebraic geometry.

Let $Y := \{y_1, \dots, y_m\}$ be (algebraic) indeterminates over the field $\mathbb{K}$; we write $\mathbb{K}[Y]$ to denote the polynomial ring in m variables over $\mathbb{K}$. Let $\overline{\mathbb{K}}$ be a fixed algebraic closure of $\mathbb{K}$. Given some polynomials $p_1, \dots, p_\rho$ in $\mathbb{K}[Y]$, the set $\left\{\mathcal{Y} \in \overline{\mathbb{K}}^m,\ p_1(\mathcal{Y}) = \cdots = p_\rho(\mathcal{Y}) = 0\right\}$ is called an *algebraic variety definable over* $\mathbb{K}$ (or simply a *variety* if $\mathbb{K}$ is clear from the context). The affine space $\overline{\mathbb{K}}^m$ is endowed with a topology (the so-called *Zariski topology*) where the closed sets are exactly the algebraic varieties definable over $\mathbb{K}$. We denote this topological space by $\mathbb{A}^m$. The space $\mathbb{A}^m$ is a Noetherian space and then every closed set is an irredundant union of a finite number of irreducible closed sets.

Given an algebraic variety $\mathcal{V}$ included in $\mathbb{A}^m$ we denote by $I(\mathcal{V})$ the ideal in $\mathbb{K}[Y]$ of all the polynomials that vanish on $\mathcal{V}$ and by $\mathbb{K}[\mathcal{V}] := \mathbb{K}[Y]/I(\mathcal{V})$ the *coordinate ring* of $\mathcal{V}$.

2.2. *The considered system: primality assumption*

Here we recall some notations concerning the DAE systems considered in this paper and state a natural primality assumption necessary in the sequel.

Let n denote a fixed non-negative integer. Throughout the paper, we consider DAE systems of the following type:

$$\Sigma := \begin{cases} f_1\left(X, \dot{X}, \dots, X^{(e_1)}\right) = 0, \\ \qquad\qquad\vdots \\ f_n\left(X, \dot{X}, \dots, X^{(e_n)}\right) = 0, \end{cases}$$

where, for every $1 \le i \le n, f_i$ is a polynomial in the variables X and the derivatives $X^{(j)}$, with $1 \le j \le e_i$; the coefficients of these polynomials are in the field $\mathbb{K}$. Each non-negative integer e_i denotes the maximal derivation order appearing in the polynomial f_i. We write $e := \max\{e_i\}$ for the maximal derivation order that occurs in Σ and we assume that e is greater than or equal to 1. As done previously, we use the following notations:

$$F := \{f_1, \dots, f_n\}, \quad F^{(j)} := \left\{{f_1}^{(j)}, \dots, {f_n}^{(j)}\right\} \quad \text{and} \quad F^{[j]} := \left\{F, \dot{F}, F^{(2)}, \dots, F^{(j)}\right\}.$$

Let $[F] \subset \mathbb{K}\{X\}$ be the differential ideal generated by the polynomials F. We introduce also the following auxiliary (Noetherian) polynomial rings and ideals: for every j in $\mathbb{N}_0$, $\mathsf{R}^{(j)}$ denotes the polynomial ring $\mathbb{K}\left[X^{[j]}\right]$ and $\mathsf{pr}^{(j)}F$ the ideal in $\mathsf{R}^{(j-1+e)}$ generated by the total derivatives of the defining equations up to order $j-1$, namely $\mathsf{pr}^{(j)}F := (F^{[j-1]})$ (this ideal is usually known as the $(j-1)$th *prolongation ideal*). We set $\mathsf{pr}^{(0)}F := (0)$ by definition.

For $i = 0, \dots, n$ in $\mathbb{N}$ and for every integer j, we will assume that the ideals generated by the polynomials $F^{[j-1]}, {f_1}^{(j)}, \dots, {f_i}^{(j)}$ *are all prime ideals* in their respective rings. In particular, the differential ideal $[F]$ is a prime differential ideal in the ring $\mathbb{K}\{X\}$.

2.3. Quasi-regular DAE systems and prime complete intersection

In this section, we establish a relationship between the notion of *quasi-regularity* of a differential system and an algebraic property – complete intersection – that is required by the geometric elimination algorithm used in this paper. The notion of *quasi-regularity* appears implicitly in Johnson (1978) (in terms of Kähler differentials) in order to generalize a conjecture of Janet to nonlinear systems.

Definition 1. Let Γ be a DAE system given in the ring $\mathbb{K}\{X\}$ by differential polynomials $Q := \{q_1, \ldots, q_\nu\}$ of order bounded by a non-negative integer e. Let $\mathfrak{p}$ be a prime differential ideal containing $[Q]$. We say that Γ is *quasi-regular at* $\mathfrak{p}$ if for every integer j in $\mathbb{N}_0$, the Jacobian matrix of the polynomials $Q^{[j]}$ with respect to the set of variables $X^{[j+e]}$ has full row rank over the domain $\mathsf{R}^{(j+e)}/(\mathsf{R}^{(j+e)} \cap \mathfrak{p})$. We say that Γ is *quasi-regular* if it is quasi-regular at any *minimal* prime differential ideal containing $[Q]$.

For the systems Σ considered in this paper, since the ideal $[F]$ is assumed to be prime, the quasi-regularity of Σ is equivalent to saying that for each integer j, the Jacobian matrix of the polynomials $F^{[j]}$ with respect to the set of variables $X^{[j+e]}$ has full row rank over the domain $\mathsf{R}^{(j+e)}/(\mathsf{R}^{(j+e)} \cap [F])$.

Under our assumptions we have the following straightforward consequence (see D'Alfonso et al. (2009, Proposition 3)):

Proposition 1. *If the system Σ is quasi-regular, then for $i = 0, \ldots, n$ and every j in $\mathbb{N}_0$, the polynomials $F^{[j-1]}, f_1^{(j)}, \ldots, f_i^{(j)}$ form a regular sequence in the polynomial ring $\mathsf{R}^{(j+e)}$. In particular, the prolongation ideals $\mathsf{pr}^{(j)}F$ are prime complete intersection ideals.*

2.4. Differentiation index

We introduce here the notion of differentiation index of quasi-regular DAE systems used in this paper. We keep the hypotheses on the system Σ made in Section 2.2 and, from now on, we also assume that *Σ is quasi-regular*.

Consider the following chain $\mathcal{C}$ of (prime) ideals in the polynomial ring $\mathsf{R}^{(e-1)}$:

$$\mathcal{C}: \quad 0 = \mathsf{pr}^{(0)}F \cap \mathsf{R}^{(e-1)} \subseteq \mathsf{pr}^{(1)}F \cap \mathsf{R}^{(e-1)} \subseteq \cdots \subseteq \mathsf{pr}^{(j)}F \cap \mathsf{R}^{(e-1)} \subseteq \cdots \subseteq [F] \cap \mathsf{R}^{(e-1)}.$$

Since $\mathsf{R}^{(e-1)}$ is a Noetherian ring, the ideal chain $\mathcal{C}$ eventually becomes stationary. Clearly, the biggest proper ideal of the chain must be $[F] \cap \mathsf{R}^{(e-1)}$.

Definition 2. The *differentiation index* σ of the system Σ is the minimum integer j at which the chain $\mathcal{C}$ becomes stationary; more precisely,

$$\sigma := \min\left\{j \in \mathbb{N}_0 \mid \mathsf{pr}^{(j)}F \cap \mathsf{R}^{(e-1)} = \mathsf{pr}^{(j+h)}F \cap \mathsf{R}^{(e-1)},\ \forall h \in \mathbb{N}\right\}.$$

Clearly, we have $\sigma = \min\{j \in \mathbb{N}_0 \mid \mathsf{pr}^{(j)}F \cap \mathsf{R}^{(e-1)} = [F] \cap \mathsf{R}^{(e-1)}\}$.

The differentiation index can also be defined by means of Jacobian matrices related to the input system (see D'Alfonso et al. (2009, Theorem 8 and Definition 9)). From this alternative definition, we deduce the following result (see D'Alfonso et al. (2009, Theorem 10)):

Theorem 2. *The differentiation index σ satisfies:*

$$\begin{aligned}\sigma &= \min\{j \in \mathbb{N}_0 \mid \mathsf{pr}^{(j+h-e+1)}F \cap \mathsf{R}^{(h)} = \mathsf{pr}^{(j+h-e+2)}F \cap \mathsf{R}^{(h)}\} \\ &= \min\{j \in \mathbb{N}_0 \mid \mathsf{pr}^{(j+h-e+1)}F \cap \mathsf{R}^{(h)} = [F] \cap \mathsf{R}^{(h)}\}\end{aligned}$$

for every integer $h \geq e - 1$.

The techniques used in D'Alfonso et al. (2009) rely on the structure of the Jacobian matrices involved. Here we give an alternative proof of the above result for the particular case $h = e$ based on the characteristic set theory (see Kolchin, 1973; Mishra, 1993).

Lemma 1. *If, for some integer j, $\mathsf{pr}^{(j)}F \cap \mathsf{R}^{(e)} = \mathsf{pr}^{(j+1)}F \cap \mathsf{R}^{(e)}$, then $\mathsf{pr}^{(j)}F \cap \mathsf{R}^{(e)} = [F] \cap \mathsf{R}^{(e)}$.*

Proof. Let $\mathcal{A}$ be an algebraic characteristic set of the prime ideal $\mathrm{pr}^{(j)}F \cap \mathrm{R}^{(e)}$ for some orderly ranking on derivatives. From $\mathcal{A}$ we extract a minimal chain $\mathcal{B}$ as follows: from all the polynomials in $\mathcal{A}$ with the same leading variable we take the one with the minimal order of derivation in this variable. We claim that $\mathcal{B}$ is autoreduced in the differential meaning.

This is equivalent to the fact that, if $x_i^{(h)}$ is the leading derivative of some element B of $\mathcal{B}$, then this derivative does not appear in some other element. As we use an orderly ranking, the $e-h$ first derivatives of B belong to $\mathrm{R}^{(e)}$ and, since by assumption $\mathrm{pr}^{(j+1)}F \cap \mathrm{R}^{(e)} = \mathrm{pr}^{(j)}F \cap \mathrm{R}^{(e)}$, they belong to $\mathrm{pr}^{(j)}F \cap \mathrm{R}^{(e)}$. Then, the derivatives $x_i^{(\ell)}$, $h < \ell \le e$, are the leading derivatives of these elements of $\mathrm{pr}^{(j)}F \cap \mathrm{R}^{(e)}$. These derivatives appear with degree 1 and with initial equal to S_B, the separant of B, that does not belong to $\mathrm{pr}^{(j)}F \cap \mathrm{R}^{(e)}$. So they are the leading derivatives, with degree 1, of some elements of $\mathcal{A}$, and they do not appear in other elements of this characteristic set. Hence our claim.

So, $\mathcal{B}$ is the characteristic set of some prime differential ideal $\mathcal{P} \subset [F]$ (see Boulier et al., 2009). Now, it is easily seen that all polynomials in $\mathrm{pr}^{(j)}F \cap \mathrm{R}^{(e)}$ are reduced to 0 by $\mathcal{B}$, which implies that $F \subset \mathcal{P}$, so that $[F] = \mathcal{P}$, and also that $\mathrm{pr}^{(j)}F \cap \mathrm{R}^{(e)} = [F] \cap \mathrm{R}^{(e)}$. $\square$

2.5. *Hilbert–Kolchin regularity: independent variables*

Now we recall in a geometric framework the notion of initial conditions associated to a given differential system. Under our assumptions, the differential dimension of the prime differential ideal $[F]$ is 0 (see e.g. Kondratieva et al., 2009). So, following Kolchin (1973, Chapter II, Section 12, Theorem 6), the transcendence degree of the fraction field of the domain $\mathrm{R}^{(j)}/(\mathrm{R}^{(j)} \cap [F])$ over the ground field $\mathbb{K}$ becomes constant for all j sufficiently big. This constant is a non-negative integer called *the order of* $[F]$ and it is denoted by $\mathrm{ord}[F]$.

The minimum of the indices j_0 such that the order of $[F]$ equals the transcendence degree of the fraction field of $\mathrm{R}^{(j)}/(\mathrm{R}^{(j)} \cap [F])$ over $\mathbb{K}$ for all $j \ge j_0$ is known as *the Hilbert–Kolchin regularity of the ideal* $[F]$. In our situation, the Hilbert–Kolchin regularity of $[F]$ is bounded by $e-1$ (see D'Alfonso et al. (2009, Theorem 12)).

From the results of the previous subsection, it follows that the differentiation index of the system Σ is at most $en - \mathrm{ord}[F]$ (for more precise bounds see, for instance, D'Alfonso et al. (2009)).

Since the fraction fields of the domains $\mathrm{R}^{(e-1)}/(\mathrm{R}^{(e-1)} \cap [F])$ and $\mathrm{R}^{(e)}/(\mathrm{R}^{(e)} \cap [F])$ have the same transcendence degree over $\mathbb{K}$, from the canonical inclusion

$$\mathrm{R}^{(e-1)}/(\mathrm{R}^{(e-1)} \cap [F]) \hookrightarrow \mathrm{R}^{(e)}/(\mathrm{R}^{(e)} \cap [F]),$$

we conclude that there exists in $X^{[e-1]}$ a subset U of $\mathrm{ord}[F]$ many variables that is a transcendence basis of both these fields. Moreover, we may also choose U in such a way that $x_j^{(h)} \in U$ implies $x_j^{(\ell)} \in U$ for every $0 \le \ell \le h$, e.g. U may be chosen as the set of derivatives that are not leading derivatives of the algebraic characteristic set $\mathcal{A}$ in the proof of Lemma 1.

Example. Consider the pendulum example (2) from the Introduction. In this case, $e = 2$ and so, the Hilbert–Kolchin regularity is bounded by 1. Since the differentiation index of Σ is $\sigma = 4$ (see D'Alfonso et al. (2009, Example 2)), using the notation $F := \{x^{(2)} - \lambda x, y^{(2)} - \lambda y + g, x^2 + y^2 - 1\}$, we have

$$\begin{aligned} \mathrm{R}^{(1)} \cap [F] &= \mathrm{R}^{(1)} \cap \mathrm{pr}^{(4)}F \\ &= (x^2 + y^2 - 1,\ \dot{y}x^2 - yx\dot{x} - \dot{y}, x\dot{x} + y\dot{y}, \dot{x}^2 + \dot{y}^2 - yg + \lambda, \dot{\lambda} - 3\dot{y}g). \end{aligned}$$

Then, the order of the system equals 2 and $U := \{x, \dot{x}\}$ is a common transcendence basis of the fraction fields of $\mathrm{R}^{(1)}/(\mathrm{R}^{(1)} \cap [F])$ and $\mathrm{R}^{(2)}/(\mathrm{R}^{(2)} \cap [F])$.

2.6. *Geometric resolution of algebraic varieties and Kronecker algorithm*

In this section, we introduce a classical tool in effective Algebraic Geometry, the *geometric resolution* of an equidimensional variety, which is a key ingredient in our index reduction method.

Let us recall informally this notion (for simplicity, we assume that $\mathbb{K}$ is algebraically closed and of characteristic 0): suppose that a d-dimensional *irreducible* affine variety $\mathcal{V}$ in the m-dimensional ambient space $\mathbb{A}^m$ is given. Then the field $\mathbb{K}(\mathcal{V})$ of rational functions over $\mathcal{V}$ has transcendence degree d over the ground field $\mathbb{K}$. Therefore, there exist d variables, say $y_1, \ldots, y_d$, such that the extension field $\mathbb{K}(y_1, \ldots, y_d) \hookrightarrow \mathbb{K}(\mathcal{V})$ is finite. These variables are called *parametric* or *free* variables. The Primitive Element Theorem (see for instance Lang (2002, Section V.4, Theorem 4.6)) asserts that there exists an element υ in $\mathbb{K}(\mathcal{V})$ such that $\mathbb{K}(\mathcal{V}) = \mathbb{K}(y_1, \ldots, y_d)[\upsilon]$; moreover, the element υ can be taken as a generic $\mathbb{K}$-linear combination of the remaining variables $y_{d+1}, \ldots, y_m$. The minimal polynomial q of υ over $\mathbb{K}(y_1, \ldots, y_d)$ defines an irreducible hypersurface $\mathcal{H} := \{q = 0\}$ in the affine space $\mathbb{A}^d \times \mathbb{A}^1$ (q can be taken with coefficients in the polynomial ring $\mathbb{K}[y_1, \ldots, y_d]$). Since each of the (non-free) variables $y_{d+1}, \ldots, y_m$, as elements of the field $\mathbb{K}(\mathcal{V})$, can be written as a rational function in the variable υ over the field $\mathbb{K}(y_1, \ldots, y_d)$, it follows that a dense open subset of the irreducible variety $\mathcal{V}$ can be rationally parametrized from a dense open subset of the hypersurface $\mathcal{H}$.

Definition 3. The 4-tuple consisting of the parametric set $\{y_1, \ldots, y_d\}$, the element υ, its minimal polynomial q, and the rational parametrizations is called a *parametric geometric resolution of the variety* $\mathcal{V}$.

If the variety $\mathcal{V}$ is not irreducible but equidimensional, a similar construction can be reproduced with suitable changes (see, for instance Schost (2003, Section 2)).

From the algorithmic point of view, assuming the variety $\mathcal{V}$ is defined by a set of polynomials F encoded by a straight-line program of length L, a parametric geometric resolution of $\mathcal{V}$ can be computed through the following steps (see Schost, 2003):

1. take a point $\mathcal{Y}$ in $\mathbb{K}^d$ and compute a geometric resolution of the zeros of the system obtained by specializing $Y = \mathcal{Y}$ in F;
2. apply a formal Newton lifting process.

The overall complexity is dominated by the running time of Step 2, which requires

$$O_{\log}\left((mL + m^4)\mathbf{M}(\rho)\mathbf{M}_s(4\deg(\mathcal{V}), d) + md^2\rho\mathbf{M}(\deg(\mathcal{V}))\mathbf{M}_s(4\deg(\mathcal{V}), d-1)\right) \tag{3}$$

operations in $\mathbb{K}$, where ρ stands for the degree of the projection $\mathcal{V} \to \mathbb{A}^d$ mapping a point to its coordinates $(y_1, \ldots, y_d)$, $\mathbf{M}(i)$ denotes the cost of the arithmetic operations with univariate polynomials of degrees bounded by i with coefficients in a ring – we can take $\mathbf{M}(i) = O(i\log^2(i)\log\log(i))$ – and $\mathbf{M}_s(i, j)$ the cost of j-variate series multiplication at precision i, that can be taken less than $O_{\log}\big(\mathbf{M}\binom{i+j}{j}\big)$.

We may also consider a particular kind of parametric geometric resolution of the variety $\mathcal{V}$ that we call a *Noether parametric geometric resolution* which involves an additional condition: the natural morphism $\mathbb{K}[y_1, \ldots, y_d] \to \mathbb{K}[\mathcal{V}]$ must be not only injective but also integral (i.e. it verifies Noether's Normalization Lemma). We are not able to ensure the existence of a set of variables $y_1, \ldots, y_d$ for which the variety $\mathcal{V}$ is in Noether position, but this can be achieved by a (generic) $\mathbb{Q}$-linear change of coordinates (see, for instance Eisenbud (1995, Chapter 13)).

If the variety $\mathcal{V}$ is defined by a reduced regular sequence F of polynomials with degrees bounded by D, the Kronecker algorithm (using a global Newton lifting) described in Giusti et al. (2001) computes a Noether parametric geometric resolution of $\mathcal{V}$ with running time

$$O\left(m\,(mL + m^{\omega})\left(\mathbf{M}(\delta D)^2 + \mathbf{M}(\delta)\sum_{i=0}^{\lceil \log_2(\delta)\rceil} \mathbf{a}(2^i)\right)\right), \tag{4}$$

where δ is the maximum of the degrees of the varieties successively defined by the polynomials F, and, for every positive integer j, $\mathbf{a}(j)$ is the cost of the arithmetic operations in the quotient $R/\mathfrak{m}^j$, where R is a polynomial ring with coefficients in $\mathbb{K}$ in d variables and $\mathfrak{m}$ is the maximal ideal generated by the variables (ω denotes the linear algebra constant).

We point out that the Kronecker algorithm works iteratively, by adding one equation at a time, and computes at each step a set of parametric variables in Noether position, a suitable specialization point for these variables, and a geometric resolution of the corresponding zero-dimensional fiber of the considered variety, within complexity $O\big(m\,(mL + m^{\omega})\,\mathbf{M}(\delta D)^2\big)$.

3. A related vector field over an algebraic hypersurface

In this section, we exhibit a new DAE system $\underline{\Sigma}$ related (in a non-intrinsic way) to the original one Σ. This new DAE system, a *Kronecker representation*, has a very particular structure: a single purely algebraic (polynomial) equation $q = 0$ plus an under-determined ODE system (see Definition 4). In particular, $\underline{\Sigma}$ could be compared to a *semi-explicit DAE system* in the usual sense (see, for instance Brenan et al. (1996, Section 1.2)), *but only outside a hypersurface*. Moreover, we will prove that the differentiation index of $\underline{\Sigma}$ is 1 (see Proposition 11).

The polynomial equation $q = 0$ is obtained by means of a geometric resolution of a suitable algebraic variety $\mathcal{V}$ associated to the input DAE system Σ and its first σ successive derivatives. The definition of $\mathcal{V}$ depends on the choice of certain sets U, W of free variables modulo $\mathrm{pr}^{(\sigma+1)}F$, as it is explained in Section 3.1. Sections 3.2 and 3.3 are devoted to the algorithmic construction of the variety $\mathcal{V}$ (including the computation of σ, U and W) and a geometric resolution of this variety. The differential equations of $\underline{\Sigma}$ are introduced in Section 3.4.

We leave for Section 4 the analysis of the relations between the solutions of both DAE systems Σ and $\underline{\Sigma}$.

3.1. The prolonged algebraic system and its partial specialization

We keep the notations and assumptions introduced in Section 2 related to the DAE input system Σ.

We recall that U denotes a subset of $X^{[e-1]}$ that is a transcendence basis of the fraction fields of the domains $\mathrm{R}^{(e-1)}/([F] \cap \mathrm{R}^{(e-1)})$ and $\mathrm{R}^{(e)}/([F] \cap \mathrm{R}^{(e)})$. Following Section 2.5 such a basis exists, and its cardinality is $\mathrm{ord}[F]$. Recall that σ denotes the differentiation index of Σ introduced in Section 2.4.

Proposition 3. 1. *The variables U as elements of the ring $\mathrm{R}^{(e+\sigma)}/\mathrm{pr}^{(\sigma+1)}F$ remain algebraically independent over $\mathbb{K}$.*
2. *Let W be a subset of $X^{[\sigma+e]}$ such that $\{U, W\}$ is a transcendence basis of the fraction field of $\mathrm{R}^{(e+\sigma)}/\mathrm{pr}^{(\sigma+1)}F$. Then every variable in W has order at least $e + 1$; in other words, W is a subset of $\{X^{(j)};\ e + 1 \le j \le e + \sigma\}$.*

Proof. Note that Theorem 2 (for $h = e$) or Lemma 1 imply that the canonical inclusion of $\mathrm{R}^{(e)}$ in $\mathrm{R}^{(e+\sigma)}$ induces an injective $\mathbb{K}$-algebra morphism $\mathrm{R}^{(e)}/([F] \cap \mathrm{R}^{(e)}) \hookrightarrow \mathrm{R}^{(e+\sigma)}/\mathrm{pr}^{(\sigma+1)}F$. In particular, this inclusion preserves $\mathbb{K}$-algebraically free elements and then the statement (1) follows. In order to prove the second assertion simply observe that U is a transcendence basis of the fraction field $\mathrm{R}^{(e)}/([F] \cap \mathrm{R}^{(e)})$ and then, for every $1 \le i \le n$, $\{U, x_i^{(e)}\}$ is an algebraically dependent set modulo $[F] \cap \mathrm{R}^{(e)}$, and the same holds in $\mathrm{R}^{(e+\sigma)}/\mathrm{pr}^{(\sigma+1)}F$. $\square$

Let W be a subset of $\left\{X^{(j)};\ e + 1 \le j \le e + \sigma\right\}$ verifying the second assertion in Proposition 3 (observe that if $\sigma = 0$ there are no variables W); since $\mathrm{pr}^{(\sigma+1)}F$ is a complete intersection prime ideal of the polynomial ring $\mathrm{R}^{(e+\sigma)}$ (Proposition 1), we have that the cardinality of $\{U, W\}$ equals the number of variables of the polynomial ring $\mathrm{R}^{(e+\sigma)}$ minus the number of elements of the regular sequence defining $\mathrm{pr}^{(\sigma+1)}F$. In other words,

$$\mathrm{card}\{U, W\} = \dim \mathrm{R}^{(e+\sigma)} - (\sigma + 1)n = (e + \sigma + 1)n - (\sigma + 1)n = ne.$$

Let s be the cardinality of W, that is $s = ne - \mathrm{ord}[F]$. For any differential polynomial f in $\mathbb{K}\{X\}$ and any point $\mathcal{W}$ in $\mathbb{A}^s$ denote by $f|_{\mathcal{W}}$ the polynomial obtained by replacing in f the variables W by the corresponding value $\mathcal{W}$.

Proposition 4. *There exists a nonempty Zariski open subset of $\mathbb{A}^s$ such that for any $\mathcal{W}$ in this set and for all integer i such that $1 \le i \le \sigma + 1$, the following conditions are satisfied:*

1. *The sequence $F^{(j)}|_{\mathcal{W}}$ for $0 \le j \le i - 1$ is a reduced regular sequence in $\mathrm{R}^{(e+\sigma)}$. In particular, the ideals $\mathrm{pr}^{(i)}F + (W - \mathcal{W})$ in $\mathrm{R}^{(e+\sigma)}$ are radical and complete intersection.*
2. *No prime component of these ideals $\mathrm{pr}^{(i)}F + (W - \mathcal{W})$ contains a nonzero polynomial pure in U.*

Proof. The proposition is a consequence of the results given in Appendix A. The first statement follows directly from Theorem 19 and for the second one we apply Corollary 18 (remark that the ideals $\mathrm{pr}^{(i)}F$ are supposed to be prime). $\square$

Example. Consider again the pendulum example from the Introduction (2). Recall that, for this system, we have $e = 2$ and $\sigma = 4$, and that $U := \{x, \dot{x}\}$ is a common transcendence basis of the fraction fields of $\mathrm{R}^{(1)}/([F] \cap \mathrm{R}^{(1)})$ and $\mathrm{R}^{(2)}/([F] \cap \mathrm{R}^{(2)})$.

It is not difficult to see that $\{x, \dot{x}, \lambda^{(3)}, \lambda^{(4)}, \lambda^{(5)}, \lambda^{(6)}\}$ is a transcendence basis of the fraction field $\mathrm{Frac}(\mathrm{R}^{(e+\sigma)}/\mathrm{pr}^{(\sigma+1)}F) = \mathrm{Frac}(\mathrm{R}^{(6)}/\mathrm{pr}^{(5)}F)$, that is, we can take $W := \{\lambda^{(3)}, \lambda^{(4)}, \lambda^{(5)}, \lambda^{(6)}\}$ as in Proposition 3.

Due to the structure of the system F and its successive derivatives, any specialization of the variables W in a point $\mathcal{W} \in \mathbb{Q}^4$ in the generators of $\mathrm{pr}^{(5)}F$ leads to a reduced regular sequence. Then, the conditions in Theorem 19 below and, therefore in Proposition 4, hold.

Now we introduce an algebraic variety defined by the prolonged equations of the input system Σ up to order σ followed by a specialization of the variables W. Fix a specialization point $\mathcal{W}$ in $\mathbb{A}^s$ and suppose it belongs to the Zariski open set given by Proposition 4.

Notation 5. *Let* $\mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}}$ *be the ideal spanned by the subset* $F^{[\sigma]}|_{\mathcal{W}}$ *of* $\mathbb{K}[X^{[e+\sigma]} \setminus W]$*. We denote by* $\mathcal{V}$ *the algebraic (equidimensional) variety in* $\mathbb{A}^{\mathrm{ord}[F]+(1+\sigma)n}$ *defined by the ideal* $\mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}}$ *and by* $\mathcal{V}_1 \cup \cdots \cup \mathcal{V}_N$ *the irreducible decomposition of* $\mathcal{V}$.

Remark 1. The ideal $\mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}}$ may actually fail to be prime for all values of $\mathcal{W}$ in a dense set, as shown by the following example: $x_1^{(2)} - {x_2^{(2)}}^2 = 0, x_2 = 0$. It is easy to see that $\sigma = 2$ and we may choose $\{x_1^{(4)}, x_2^{(4)}\}$ as the set W. Then, for an orderly ordering, an algebraic characteristic set (in fact, a system of generators) of $\mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}}$ is $2{x_2^{(3)}}^2 - \mathcal{W}_1, x_1^{(3)}, x_1^{(2)}, x_2^{(2)}, \dot{x}_2, x_2$. We see that the ideal is prime if and only if $\mathcal{W}_1/2$ is not a square in $\mathbb{K}$. Moreover, even in the prime case, the field extension associated to $\mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}}$ is a non-trivial algebraic extension of degree 2 of the field associated to the ideal $[F] \cap \mathrm{R}^{(e)}$, which is 1. On the other hand, we could choose also W as the set $\{x_2^{(4)}, x_2^{(3)}\}$; in this case $\mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}}$ is prime and its associated variety is birational equivalent to $V([F] \cap \mathrm{R}^{(e)})$.

Finding whenever possible, such a choice of W, remains a subject for further investigations.

Example. In the pendulum example, by specializing the variables $W = \{\lambda^{(3)}, \lambda^{(4)}, \lambda^{(5)}, \lambda^{(6)}\}$ to $\mathcal{W} = 0$, we obtain the ideal:

$$\mathrm{pr}^{(5)}F|_0 = (x^{(2)} - \lambda x, y^{(2)} - \lambda y + g, x^2 + y^2 - 1, -\lambda\dot{x} + x^{(3)} - x\dot{\lambda}, -\lambda\dot{y} + y^{(3)} - y\dot{\lambda}, 2x\dot{x} + 2y\dot{y}, -2\dot{\lambda}\dot{x} - \lambda x^{(2)} + x^{(4)} - x\lambda^{(2)}, -2\dot{\lambda}\dot{y} - \lambda y^{(2)} + y^{(4)} - y\lambda^{(2)}, 2\dot{x}^2 + 2xx^{(2)} + 2\dot{y}^2 + 2yy^{(2)}, -3\lambda^{(2)}\dot{x} - 3\dot{\lambda}x^{(2)} - \lambda x^{(3)} + x^{(5)}, -3\lambda^{(2)}\dot{y} - 3\dot{\lambda}y^{(2)} - \lambda y^{(3)} + y^{(5)}, 6x^{(2)}\dot{x} + 2xx^{(3)} + 6y^{(2)}\dot{y} + 2yy^{(3)}, -6\lambda^{(2)}x^{(2)} - 4\dot{\lambda}x^{(3)} - \lambda x^{(4)} + x^{(6)}, -6\lambda^{(2)}y^{(2)} - 4\dot{\lambda}y^{(3)} - \lambda y^{(4)} + y^{(6)}, 8x^{(3)}\dot{x} + 6(x^{(2)})^2 + 2xx^{(4)} + 8y^{(3)}\dot{y} + 6(y^{(2)})^2 + 2yy^{(4)})$$

generated by 15 polynomials in $\mathbb{Q}[x^{[6]}, y^{[6]}, \lambda^{[2]}]$, which defines the 2-dimensional variety $\mathcal{V} \subset \mathbb{A}^{17}$.

Observe that the algebraic variety $\mathcal{V}$ is not intrinsically associated to the input DAE system because its definition depends on the choice of the transcendence basis U, the variables W, and the point $\mathcal{W}$ where the variables W are evaluated.

Let us also remark that the second assertion in Proposition 4 states that the projection on the U-space of any irreducible component $\mathcal{V}_i$ is *dominant*; i.e. the closure of the image of $\mathcal{V}_i$ by the projection on the variables U is the whole space $\mathbb{A}^{\mathrm{ord}[F]}$ or equivalently, the natural ring map $\mathbb{K}[U] \to \mathbb{K}[\mathcal{V}_i]$ is injective.

The following proposition shows that the identity $[F] \cap \mathrm{R}^{(e)} = \mathrm{pr}^{(\sigma+1)}F \cap \mathrm{R}^{(e)}$ (see Theorem 2 and Lemma 1) remains correct after specialization in a suitable $\mathcal{W}$:

Proposition 6. *Let* $\mathcal{W}$ *in* $\mathbb{A}^s$ *chosen as in Proposition 4. Then the identity* $[F] \cap \mathrm{R}^{(e)} = \mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}} \cap \mathrm{R}^{(e)}$ *holds.*

Proof. Since $[F] \cap \mathsf{R}^{(e)} = \mathsf{pr}^{(\sigma+1)}F \cap \mathsf{R}^{(e)}$ and the variables W do not appear in the ring $\mathsf{R}^{(e)}$, the ideal $[F] \cap \mathsf{R}^{(e)}$ is included in $\mathsf{pr}^{(\sigma+1)}F|_{\mathcal{W}} \cap \mathsf{R}^{(e)}$. On the other hand, if $\mathfrak{p}$ is a primary component of $\mathsf{pr}^{(\sigma+1)}F|_{\mathcal{W}}$, we have that $\mathbb{K}[U] \hookrightarrow \mathsf{R}^{(e+\sigma)}/\mathfrak{p}$ (because of the choice of $\mathcal{W}$ verifying Proposition 4). Then $\mathfrak{p} \cap \mathsf{R}^{(e)}$ is a prime ideal of dimension at least $\mathrm{ord}[F]$ containing $[F] \cap \mathsf{R}^{(e)}$, which is a prime ideal of dimension $\mathrm{ord}[F]$. Hence both prime ideals are the same. Since the argument holds for any primary component of $\mathsf{pr}^{(\sigma+1)}F|_{\mathcal{W}}$, the proposition follows. $\square$

In other words, this proposition says that *all* differential conditions of order at most e induced by the input system can be generated by differentiation of the original equations up to order σ followed by the specialization $W \mapsto \mathcal{W}$.

In particular, if $\mathbb{K} = \mathbb{R}, \mathbb{C}$, suppose that $\varphi := (\varphi_1, \ldots, \varphi_n)$ is a classical analytic solution of the DAE system Σ defined locally in a neighborhood of 0. Then, Proposition 6 implies that for any t in $\mathbb{R}$ small enough, the complex vector formed by the derivatives up to order e of the function φ evaluated at the instant t is a point of the algebraic variety $V([F] \cap \mathsf{R}^{(e)})$, *independently* of the choice of the variables U, W and the point $\mathcal{W}$ in $\mathbb{A}^s$.

We point out that, for our algorithmic purposes, in the sequel we will choose the point $\mathcal{W}$ at random and assume that all the previous conditions hold.

3.2. A parametric geometric resolution of the variety $\mathcal{V}$

We will now consider a parametric geometric resolution (see Definition 3) for the equidimensional variety $\mathcal{V}$ introduced in Notation 5.

From Proposition 4 we observe first that the variables U are a *parametric set* with respect to the equidimensional algebraic variety $\mathcal{V} := \mathcal{V}_1 \cup \cdots \cup \mathcal{V}_N$, since the canonical morphism $\mathbb{K}[U] \to \mathbb{K}[\mathcal{V}_i]$ is injective and since the relations $\mathrm{ord}[F] = \mathrm{card}\, U = \dim \mathcal{V}_i$ hold for all $i = 1, \ldots, N$. In particular, no linear change of coordinates is necessary in order to obtain free variables with respect to the irreducible components of $\mathcal{V}$. Secondly, the ideal $\mathsf{pr}^{(\sigma+1)}F|_{\mathcal{W}}$ is radical and so, it is the defining ideal of $\mathcal{V}$. Moreover, it is generated by the regular sequence $F^{[\sigma]}|_{\mathcal{W}}$.

These facts imply that for each prime ideal $I(\mathcal{V}_i)$ associated to $\mathsf{pr}^{(\sigma+1)}F|_{\mathcal{W}}$ defined in Notation 5, $I(\mathcal{V}_i) \otimes \mathbb{K}(U)$ is a 0-dimensional prime ideal in the polynomial ring with coefficients in $\mathbb{K}(U)$ and variables $X^{[e+\sigma]} \setminus \{U, W\}$. Hence the Jacobian determinant of the polynomials $F^{[\sigma]}|_{\mathcal{W}}$ with respect to these variables $X^{[e+\sigma]} \setminus \{U, W\}$ does not vanish identically over any component $\mathcal{V}_i$.

Thus the requirements of Schost (2003, Section 2.1) are fulfilled and a parametric geometric resolution $\left(U, \upsilon, q, \left\{\left(\frac{p_i}{q'}\right), 1 \leq i \leq (1+\sigma)n\right\}\right)$ exists. Here υ is a $\mathbb{Q}$-linear combination of the variables $X^{[e+\sigma]} \setminus \{U, W\}$, q the square-free polynomial in $\mathbb{K}[U, \upsilon]$ of positive degree in υ defining a hypersurface $\mathcal{H}$ in $\mathbb{A}^{\mathrm{ord}[F]} \times \mathbb{A}^1$, and q' the partial derivative $\frac{\partial q}{\partial \upsilon}$. The fractions $\frac{p_i}{q'}$ in $\mathbb{K}(U, \upsilon)$ are the parametrizations of the remaining variables. More precisely, each p_i can be written as

$$p_i = \frac{a_i(U, \upsilon)}{b_i(U)} \tag{5}$$

where $a_i(U, \upsilon)$ in $\mathbb{K}[U, \upsilon]$ and $b_i(U)$ in $\mathbb{K}[U] \setminus \{0\}$ are coprime polynomials verifying that $\deg_\upsilon a_i < \deg_\upsilon q$; furthermore, for each variable y in $X^{[e+\sigma]} \setminus \{U, W\}$, there exists an integer j such that $b_j(U)q'y - a_j(U, \upsilon)$ vanishes on the variety $\mathcal{V}$.

We define the *total ring of fractions* of the variety $\mathcal{V}$ in the usual way as the Artinian ring $\mathbb{K}(\mathcal{V}) := \mathbb{K}(\mathcal{V}_1) \times \cdots \times \mathbb{K}(\mathcal{V}_N)$ and analogously for $\mathcal{H}$. Therefore, from the canonical ring inclusions $\mathbb{K}[U] \hookrightarrow \mathbb{K}[\mathcal{H}] \hookrightarrow \mathbb{K}[\mathcal{V}]$, by means of the geometric resolution and passing to the total ring of fractions, we infer that the relations $\mathbb{K}(U) \hookrightarrow \mathbb{K}(\mathcal{H}) \cong \mathbb{K}(\mathcal{V})$ hold. The inverse application $\mathbb{K}(\mathcal{V}) \to \mathbb{K}(\mathcal{H})$ is induced by the parametrization $y \mapsto \frac{p_i}{q'}$, for y in $X^{[e+\sigma]} \setminus \{U, W\}$.

From a more geometrical point of view, these facts can be stated in the following way. Consider the linear map $\Psi : \mathbb{A}^{\mathrm{ord}[F]+(\sigma+1)n} \to \mathbb{A}^{\mathrm{ord}[F]+1}$ defined as $X^{[e+\sigma]} \setminus \{W\} \mapsto (U, \upsilon)$. For each irreducible component $\mathcal{V}_i$ of $\mathcal{V}$ the restriction of Ψ to $\mathcal{V}_i$ induces an isomorphism between suitable nonempty Zariski open sets of $\mathcal{V}_i$ and of the irreducible component $\mathcal{H}_i = \overline{\Psi(\mathcal{V}_i)}$ of $\mathcal{H}$. In other words, the components $\mathcal{V}_i$ and $\mathcal{H}_i$ are birationally equivalent, i.e. the fields of rational functions $\mathbb{K}(\mathcal{V}_i)$ and $\mathbb{K}(\mathcal{H}_i)$ are $\mathbb{K}$-isomorphic.

Example. In the pendulum example, in order to obtain a parametric geometric resolution of the associated variety $\mathcal{V} \subset \mathbb{A}^{17}$, we consider the linear form $\upsilon := y$, which is a primitive element with respect to the parametric variables $U = \{x, \dot{x}\}$. The minimal polynomial of this linear form is

$$q = \upsilon^2 + x^2 - 1.$$

Now, for each variable $z \in \{x^{(i)}, 2 \le i \le 6;\ y^{(j)}, 1 \le j \le 6;\ \lambda^{(h)}, 0 \le h \le 2\}$, we have polynomials $b_z(U)$ in $\mathbb{Q}[U]$ and $a_z(U, \upsilon)$ in $\mathbb{Q}[U, \upsilon]$ such that

$$b_z(U)\frac{\partial q}{\partial \upsilon}(U, \upsilon)\, z - a_z(U, \upsilon)$$

vanishes over $\mathcal{V}$. For instance,

$$\begin{array}{llll} b_{\dot{y}} &= 1, & a_{\dot{y}} &= -2x\dot{x}, \\ b_{\lambda} &= 1 - x^2, & a_{\lambda} &= -2\dot{x}^2\upsilon + 2g(1 - x^2)^2, \\ b_{\dot{\lambda}} &= 1, & a_{\dot{\lambda}} &= -6gx\dot{x}, \\ b_{x^{(2)}} &= 1 - x^2, & a_{x^{(2)}} &= -2x\dot{x}^2\upsilon + 2gx(1 - x^2)^2, \\ b_{y^{(2)}} &= 1, & a_{y^{(2)}} &= -2gx^2\upsilon - 2\dot{x}^2, \\ b_{\lambda^{(2)}} &= 1, & a_{\lambda^{(2)}} &= 6g^2x^2\upsilon - 6g\dot{x}^2. \end{array} \tag{6}$$

In the next section, we will discuss how to compute the differentiation index σ and the sets of variables U and W. After the specialization of the variables W at a randomly chosen point $\mathcal{W}$, a parametric geometric resolution of $\mathcal{V}$ can be probabilistically computed from these data and a straight-line program encoding the polynomials F by applying the algorithm in Schost (2003, Theorem 2) (see Section 2.6).

In order to estimate the running time of this algorithm in terms of the input size, we use the following complexity estimate for the computation of successive derivatives.

Remark 2. From a straight-line program of length L encoding the input polynomials F, we can obtain a straight-line program of length $O\big(((e + \sigma)en + L)\sigma^2\big)$ encoding all the polynomials $F^{[\sigma]}$ (see Matera and Sedoglavic (2003, Section 5.2) or D'Alfonso et al. (2006, Lemma 21)).

We deduce the following complexity result (see (3) in Section 2.6):

Proposition 7. *A parametric geometric resolution of $\mathcal{V}$ can be computed over the field $\mathbb{K}$ from F, σ, U by a probabilistic algorithm with*

$$O_{\log}\left(\mathtt{N}\left((\mathbf{L} + \mathtt{N}^3)\mathbf{M}(\rho) + (\mathrm{ord}[F])^2\, \rho\, \mathbf{M}(\deg(\mathcal{V}))\right)\mathbf{M}_s(4\deg(\mathcal{V}), \mathrm{ord}[F])\right)$$

operations in $\mathbb{K}$, where $\mathtt{N} = \mathrm{ord}[F] + (1 + \sigma)n$, $\mathbf{L} = ((e + \sigma)en + L)\sigma^2$ and ρ stands for the degree of the projection $\mathcal{V} \to \mathbb{A}^{\mathrm{ord}[F]}$ mapping $X^{[e+\sigma]} \setminus W$ to U.

Remark 3. If the variables U are chosen in such a way that for every variable $x_j^{(h)} \in U$, all its previous derivatives $x_j^{(\ell)}$, for $0 \le \ell \le h$, also belong to U, the representation given in Proposition 7 allows us to obtain a characteristic set of the ideal for some ranking on derivatives, using for instance the method described in Dahan et al. (2008).

Taking into account that the polynomials $F^{[\sigma]}|_{\mathcal{W}}$ form a reduced regular sequence, we can apply alternatively the algorithms in Giusti et al. (2001) (see Section 2.6) to compute a Noether parametric geometric resolution of the variety $\mathcal{V}$. Using the previous notations, this leads to the following complexity result (see (4)).

Proposition 8. *A Noether parametric geometric resolution of $\mathcal{V}$ can be computed over the field $\mathbb{K}$ from $F^{[\sigma]}|_{\mathcal{W}}$ by means of a probabilistic algorithm which runs in time*

$$O\left(\mathtt{N}\,(\mathtt{N}\mathbf{L} + \mathtt{N}^{\omega})\left(\mathbf{M}(\mathtt{D}d)^2 + \mathbf{M}(\mathtt{D})\sum_{i=0}^{\lceil \log_2(\mathtt{D}) \rceil} \mathbf{a}(2^i)\right)\right),$$

where d is the degree of the input polynomials F and $\mathtt{D}$ is the maximum of the degrees of the varieties successively defined by the polynomials $F^{[\sigma]}|_{\mathcal{W}}$.

3.3. Computing σ, U and W

Up to now, we have assumed σ, U and W to be known *a priori*. This may often be the case for U for obvious physical reasons (for example, one does not need to compute the equations of a mechanical system such as the pendulum to know which quantities could be arbitrarily chosen), but the variables W are introduced mainly for technical reasons. Nevertheless, we will see that suitable sets U and W may be probabilistically computed within a similar complexity as in the previous section.

According to Theorem 2 or Lemma 1 in order to compute σ it is enough to find the minimum j_0 such that $\mathrm{pr}^{(j)}F \cap \mathrm{R}^{(e)} = \mathrm{pr}^{(j+1)}F \cap \mathrm{R}^{(e)}$ (then this minimum j_0 is $\sigma + 1$). By the primality assumption of these ideals it suffices to compare their dimensions. Following D'Alfonso et al. (2008, Proposition 2 and Remark 3) or D'Alfonso et al. (2009, Proposition 6), the dimension of the ideal $\mathrm{pr}^{(j)}F \cap \mathrm{R}^{(e)}$ is equal to $(e - j + 1)n + \mathrm{rank}(\partial F^{(r)}/\partial X^{(h)})_{1\le r<j,\ e<h<e+j}$, the rank being computed modulo the prime ideal $\mathrm{pr}^{(j)}F$. Our algorithm, summarized in **Algorithm DiffIndex** below, computes successively the ranks to obtain the dimension of the ideals $\mathrm{pr}^{(j)}F$, and it stops when two consecutive dimensions coincide.

To do this we apply the **Kronecker** algorithm (see Giusti et al., 2001; Durvye and Lecerf, 2007 and Section 2.6) to compute, for every j, a set of parametric variables Y giving a Noether position, a suitable specialization point $\mathcal{Y}$ and a geometric resolution of its corresponding fiber for the algebraic variety defined by $\mathrm{pr}^{(j)}F$ (see step (2c)). This geometric resolution allows us to reduce the rank computation modulo $\mathrm{pr}^{(j)}F$ to a probabilistic rank computation modulo a principal ideal by means of the specialization of the variables into the corresponding rational parametrizations (see steps (2c)). Finally, the rank computation is achieved by means of a subroutine **RankMod** (see step (2f)) which applies Gaussian elimination over univariate polynomials modulo a univariate polynomial.

Algorithm DiffIndex

1. $\tau := 0, \nu := en, j := 1$
2. **while** $\tau < \nu$ **do**
   (a) $j := j + 1$
   (b) $\tau := \nu$
   (c) $(Y = \mathcal{Y}, \upsilon, q, \mathbf{p}) :=$ **Kronecker**$(\mathrm{pr}^{(j+1)}F)$
   (d) $J := (\partial F^{(r)}/\partial X^{(h)})_{1\le r\le j,\ e<h\le e+j}$
   (e) $\widehat{J} := J|_{Y=\mathcal{Y},\ X^{[e+j]}\setminus Y=\mathbf{p}/q'}$
   (f) $R :=$ **RankMod**$(\widehat{J}, q)$
   (g) $\nu := (e - j)n + R$
   end do
3. Return $\sigma := j - 1$.

Note that due to the recursive structure of the Kronecker algorithm (see Giusti et al., 2001), if the equality of the dimensions does not hold, the geometric resolution already computed is taken as input for the next step.

Taking into account the length of a straight-line program computing the successive derivatives of F (see Remark 2), and the complexities of the Kronecker algorithm (see Section 2.6) and of the matrix rank computation (see, for instance, von zur Gathen and Gerhard, 1999), we deduce that the overall complexity of the above algorithm is

$$O\left((e+\sigma)^4 n^4 (\sigma^2 + L)\,\mathbf{M}(\delta d)^2\right)$$

where δ is the maximum of the degrees of the varieties successively defined by the polynomials $F^{[\sigma]}$, L is the length of a straight-line program encoding the input polynomials F, and d is an upper bound for their degrees.

Once the differentiation index is obtained, we are able to compute a transcendence basis $\{U, W\}$ of the fraction field of $\mathrm{R}^{(e+\sigma)}/\mathrm{pr}^{(\sigma+1)}F$ as in Proposition 3 by considering the Jacobian matrix of the polynomials $F^{[\sigma]}$ with respect to the variables $X^{(e+\sigma)}, \ldots, \dot{X}, X$ (see D'Alfonso et al. (2006, Lemma 19)).

After a Gauss triangulation of this matrix, the variables indexing columns with no pivot give a transcendence basis modulo $\mathrm{pr}^{(\sigma+1)}F$. The set U corresponds to those variables of order at most $e-1$ and the set W to the remaining ones. This is done algorithmically in a similar way as in the previous algorithm and within the same complexity bounds.

Proposition 9. *Using the previous notation, the differentiation index σ of the system F and the sets of variables U and W can be computed from the input polynomials F by means of a probabilistic algorithm with running time of order $O\left((e+\sigma)^4 n^4(\sigma^2+L)\,\mathbf{M}(\delta d)^2\right)$.*

The previous computations might simplify the obtention of a parametric geometric resolution of the variety $\mathcal{V}$. This question, and its computational interest, are left to further investigations.

3.4. An associated vector field over the hypersurface

In this section, we define a vector field on the algebraic hypersurface $\mathcal{H}$ defined in $\mathbb{A}^{1+\mathrm{ord}[F]}$ by $\{q=0\}$ and introduced in Section 3.2. Moreover, we introduce the new first order, quasi-regular system $\underline{\Sigma}$ having differentiation index 1, whose solutions will enable us to obtain solutions of the given system Σ.

Consider a parametric geometric resolution of the variety $\mathcal{V}$ introduced in Notation 5 and let

$$\left(U, \upsilon, q, \left\{\frac{p_i}{q'}, 1 \le i \le (1+\sigma)n\right\}\right)$$

be the parametric variables, the primitive element, its minimal square-free polynomial and the parametrizations respectively.

The linear map $\Psi : \mathbb{A}^{\mathrm{ord}[F]+(1+\sigma)n} \to \mathbb{A}^{1+\mathrm{ord}[F]}$ defined as $X^{[e+\sigma]} \setminus W \to (U, \upsilon)$ (recall that υ is a $\mathbb{Q}$-linear combination of the variables $X^{[e+\sigma]} \setminus \{U, W\}$) gives, by restriction, a morphism of algebraic varieties between $\mathcal{V}$ and $\mathcal{H}$ and so, it induces a dual $\mathbb{K}$-morphism $\Psi^\star$ between the Artinian rings $\mathbb{K}(\mathcal{H})$ and $\mathbb{K}(\mathcal{V})$. From the properties satisfied by the geometric resolution, we have that $\Psi^\star$ is an isomorphism of $\mathbb{K}$-algebras and its inverse morphism $\Phi^\star$ is defined, by means of the parametrizations, as the dual of the (rational, not necessarily polynomial) morphism of algebraic varieties: $\Phi : \mathcal{H} \to \mathcal{V}$ defined by $(U, \upsilon) \to (U, \frac{p_i}{q'} | 1 \le i \le (1+\sigma)n)$. Let us observe that both ring morphisms $\Psi^\star$ and $\Phi^\star$ fix the variables U.

Since the parametric set U has been chosen as a subset of $X^{[e-1]}$, the set $\dot{U}$ of derivatives of U is included in $X^{[e]}$ and so, by Proposition 3, the relation $\dot{U} \cap W = \emptyset$ holds. In particular, U and $\dot{U}$ remain invariant after specialization of the variables W at any point $\mathcal{W}$ in $\mathbb{K}^s$.

Fix a variable $\dot{u}_i$ of the set $\dot{U}$ $(1 \le i \le \mathrm{ord}[F])$. We have the following.

(a) If $\dot{u}_i$ is in U, there exists a unique integer h such that $1 \le h \le \mathrm{ord}[F]$ and $\dot{u}_i = u_h$.
(b) If $\dot{u}_i$ is not in U, there exists a unique index j such that $1 \le j \le (1+\sigma)n$ and

$$\Phi^\star(\dot{u}_i) = \frac{p_j}{q'}(U, \upsilon) = \frac{1}{b_j(U)} \frac{a_j}{q'}(U, \upsilon).$$

Definition 4. Let $\underline{\Sigma}$ be the square DAE system in the $\mathrm{ord}[F]+1$ differential unknowns U, υ:

$$\underline{\Sigma} := \begin{cases} \dot{u}_i - u_h & = 0, \text{ for all } \dot{u}_i \text{ verifying condition (a)} \\ b_j(U)q'(U,\upsilon)\dot{u}_i - a_j(U,\upsilon) & = 0, \text{ for all } \dot{u}_i \text{ verifying condition (b)} \\ q(U,\upsilon) & = 0. \end{cases}$$

We denote by $\underline{F} := \underline{f_1}, \ldots, \underline{f_{1+\mathrm{ord}[F]}}$ the polynomials in $\mathbb{K}[U, \dot{U}, \upsilon]$ defining the system $\underline{\Sigma}$ and by $[\underline{F}]$ the differential ideal generated by them in $\mathbb{K}\{U, \upsilon\}$.

Example. In order to construct the associated system $\underline{\Sigma}$ to the pendulum example (2), recall that $U := \{x, \dot{x}\}$ are parametric variables and $\upsilon := y$ is a primitive element.

If we denote $u_1 := x$ and $u_2 := \dot{x}$, we have that $\dot{u_1} \in U$ (see condition (a) above) and $\dot{u_2} \notin U$ (see condition (b) above). Taking into account the parametrizations given in (6), it follows that the system $\underline{\Sigma}$ from Definition 4 is

$$\underline{\Sigma} = \begin{cases} \dot{u_1} - u_2 & = 0, \\ 2\upsilon(1-{u_1}^2)\dot{u_2} - 2u_1{u_2}^2\upsilon - 2gu_1(1-{u_1}^2)^2 & = 0, \\ \upsilon^2 + {u_1}^2 - 1 & = 0. \end{cases}$$

By inverting $\frac{\partial q}{\partial \upsilon}(U, \upsilon) = 2\upsilon$ modulo $q(U, \upsilon)$ and dividing the second equation by $(1 - {u_1}^2)$, we get the simplified Kronecker representation

$$\underline{\Sigma} = \begin{cases} \dot{u_1} & = u_2, \\ \dot{u_2} & = u_1\left(g\upsilon - \frac{{u_2}^2}{(1-{u_1}^2)}\right), \\ \upsilon^2 + {u_1}^2 - 1 & = 0. \end{cases}$$

Let $q = q_1 \cdots q_r$ be the decomposition of q as a product of irreducible factors in the polynomial ring $\mathbb{K}[U, \upsilon]$. Since the variables U are algebraically independent modulo the ideal $(q) \subset \mathbb{K}[U, \upsilon]$, we have $\deg_\upsilon q_i > 0$ for all integer i. For each factor q_i let $\mathfrak{p}_i$ be the ideal $[\underline{f_1}, \ldots, \underline{f_{\mathrm{ord}[F]}}, q_i]$ in $\mathbb{K}\{U, \upsilon\}$.

Proposition 10. *The ideal $[\underline{F}]$ is a radical quasi-regular differential ideal in $\mathbb{K}\{U, \upsilon\}$ and its minimal primes are $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$.*

Proof. Let us define $B(U) := \prod b_j(U)$. From the particular form of the polynomials $\underline{F}$ we observe that the ring $\mathbb{K}\{U, \upsilon\}/[\underline{F}]$ is isomorphic to a subring of the localization of $\mathbb{K}[U, \upsilon]/(q)$ at the polynomial Bq'. Since q is assumed to be square-free, the ring $\mathbb{K}[U, \upsilon]/(q)$ has no nonzero nilpotent elements and the same property remains true for any localization of it. Therefore, the ideal $[\underline{F}]$ is radical. Similarly, each ring $\mathbb{K}\{U, \upsilon\}/\mathfrak{p}_i$ is isomorphic to a subring of the localization of $\mathbb{K}[U, \upsilon]/(q_i)$ at Bq', which is a domain since q_i' is irreducible in $\mathbb{K}[U, \upsilon]$; thus the ideals $\mathfrak{p}_i$ are prime.

From the previous argument, we observe that the canonical map $\mathbb{K}[U] \to \mathbb{K}\{U, \upsilon\}/[\underline{F}]$ is injective and no polynomial in $\mathbb{K}[U]$ is a zero divisor of the ring $\mathbb{K}\{U, \upsilon\}/[\underline{F}]$. Since $[\underline{F}]$ is a radical ideal, it has only finitely many minimal (hence associated) prime ideals (see Ritt (1950, Chapter 1, Section 16)) and so, none of these minimal primes contains a nonzero polynomial in $\mathbb{K}[U]$.

Fix a minimal prime $\mathfrak{p}$ of $[\underline{F}]$. Since q is an element of $[\underline{F}] \subseteq \mathfrak{p}$, there is an irreducible factor q_{i_0} of q lying in the ideal $\mathfrak{p}$. Moreover, exactly one of these irreducible factors belongs to $\mathfrak{p}$ since they are pairwise coprime in $\mathbb{K}(U)[\upsilon]$ (otherwise, Bézout's Identity would imply the existence of a nonzero polynomial in $\mathfrak{p} \cap \mathbb{K}[U]$, leading to a contradiction). We will show now that $\mathfrak{p}_{i_0}$ is included in $\mathfrak{p}$.

Since the total successive derivatives of the polynomials $\underline{f_1}, \ldots, \underline{f_{\mathrm{ord}[F]}}$ belong to $\mathfrak{p}$ and $[\underline{F}]$ is a subset of $\mathfrak{p}$, it suffices to prove that, for all integer j, the total derivatives ${q_{i_0}}^{(j)}$ belong to $\mathfrak{p}$ (note that $\mathfrak{p}$ is not *a priori* necessarily a differential ideal). This can be done by recursion in j. For $j = 0$, there is nothing to prove. Otherwise, for $j \geq 0$, we have that $q^{(j+1)} = \sum_{|h|=j+1} \frac{(j+1)!}{h_1!\ldots h_r!} {q_1}^{(h_1)} \ldots {q_r}^{(h_r)}$ is in $[\underline{F}] \subseteq \mathfrak{p}$, which implies by induction hypothesis that the expression ${q_{i_0}}^{(j+1)} \prod_{i \neq i_0} q_i$ is in $\mathfrak{p}$. Since $\prod_{i \neq i_0} q_i$ is not in $\mathfrak{p}$, we conclude that ${q_{i_0}}^{(j+1)}$ is in $\mathfrak{p}$.

Again, from the special form of the polynomials $\underline{F}$, it is easy to see that the system is quasi-regular at each minimal prime differential ideal $\mathfrak{p}_i$ and then, $[\underline{F}]$ is quasi-regular (see Definition 1). □

The previous proposition ensures that the hypotheses of D'Alfonso et al. (2009, Section 2) are fulfilled. Hence, all the considerations concerning the differentiation index, the order and the Hilbert–Kolchin regularity explained there can be applied to our new DAE system $\underline{\Sigma}$. In particular, we can compute the differentiation index of $\underline{\Sigma}$ at each minimal prime $\mathfrak{p}$ as in D'Alfonso et al. (2009, Section 3.1).

Proposition 11. *Let $\mathfrak{p}$ be a minimal prime differential ideal containing $[\underline{F}]$. Then the DAE system $\underline{\Sigma}$ has $\mathfrak{p}$-differentiation index* 1.

Proof. Following Proposition 10, let q_i in $\mathbb{K}[U, \upsilon]$ be an irreducible factor of q such that $\mathfrak{p}_i = [\underline{f_1}, \ldots, \underline{f_{\mathrm{ord}[F]}}, q_i]$. Then, the fraction field $\mathbb{K}(\mathfrak{p}_i)$ of $\mathbb{K}\{U, \upsilon\}/\mathfrak{p}_i$ can be identified in a natural way with the fraction field of the domain $\mathbb{K}[U, \upsilon]/(q_i)$; in particular $\mathbb{K}[U]$ may be regarded as a subring of $\mathbb{K}(\mathfrak{p}_i)$.

Let $\mathfrak{J}_1$ be the square Jacobian matrix of the polynomials $\underline{f_1}, \ldots, \underline{f_{\mathrm{ord}[F]+1}}$ with respect to the variables $\dot{U}$ and $\dot{\upsilon}$. Then $\mathfrak{J}_1$ is the diagonal matrix:

$$\mathfrak{J}_1 = \begin{pmatrix} \boxed{\mathrm{Id}} & \cdots & 0 \\ \vdots & \boxed{C} & \vdots \\ 0 & \cdots & 0 \end{pmatrix},$$

where C is a diagonal matrix with the elements $b_j(U)q'$ in the diagonal. Since $b_j(U)q'$ is nonzero in the domain $\mathbb{K}[U, \upsilon]/(q_i)$ for all index j, we deduce that $\mathfrak{J}_1$ has rank $\mathrm{ord}[F]$ over the field $\mathbb{K}(\mathfrak{p}_i)$.

Consider now $\mathfrak{J}_2$ the Jacobian matrix of the $2(\mathrm{ord}[F] + 1)$ many polynomials $\underline{F}, \dot{\underline{F}}$ with respect to the $2(\mathrm{ord}[F] + 1)$ many variables $\dot{U}, \dot{\upsilon}, U^{(2)}, \upsilon^{(2)}$. We have the following.

$$\mathfrak{J}_2 = \left(\begin{array}{ccc|c} & \mathfrak{J}_1 & & 0 \\ \hline * & \cdots & * & \\ \vdots & & \vdots & \mathfrak{J}_1 \\ * & \cdots & q' & \end{array}\right).$$

Therefore, the rank of $\mathfrak{J}_2$ over $\mathbb{K}(\mathfrak{p}_i)$ is equal to $2\,\mathrm{ord}[F] + 1$ (recall that the last row and column of $\mathfrak{J}_1$ are both 0).

Then, the relation $\dim_{\mathbb{K}(\mathfrak{p}_i)} \ker {}^t\mathfrak{J}_1 = 1 + \mathrm{ord}[F] - \mathrm{rank}_{\mathbb{K}(\mathfrak{p}_i)}(\mathfrak{J}_1) = 1$ holds and thus, the equality $\dim_{\mathbb{K}(\mathfrak{p}_i)} \ker {}^t\mathfrak{J}_2 = 2(1 + \mathrm{ord}[F]) - \mathrm{rank}_{\mathbb{K}(\mathfrak{p}_i)}(\mathfrak{J}_2) = 1$ holds. Thus, from D'Alfonso et al. (2009, Definitions 5 & 9 and Theorem 8), we conclude that the $\mathfrak{p}_i$-differentiation index of the system $\underline{\Sigma}$ equals 1. □

3.5. Summary of the algorithm

Here we summarize the algorithm described along the previous subsections which, taking as input the system Σ, produces the associated system $\underline{\Sigma}$.

Algorithm IndexReduction

Input: A straight-line program encoding the polynomials F defining Σ.
Output: A straight-line program encoding polynomials $\underline{F}$ defining $\underline{\Sigma}$.

1. $\sigma :=$ **DiffIndex**(F) (see Section 3.3)
2. $U, W :=$ **TranscendenceBasis**$(\mathrm{pr}^{(\sigma+1)}F)$ (see Proposition 9)
3. Choose a specialization point $\mathcal{W}$ for the variables W at random.
4. Compute a parametric geometric resolution of the variety $\mathcal{V}$ defined by $\mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}}$ (see Proposition 7).
5. Construct the equations in $\underline{\Sigma}$ following Definition 4.

3.6. About singularities

Our hypotheses imply that we will not encounter singularities such as in the well-known system $\dot{x}^2 - 4x = 0$: the main component of the perfect differential ideal $\{\dot{x}^2 - 4x\}$, which is the prime differential ideal $[\dot{x}^2 - 4x, x^{(2)} - 2]$, crosses the singular component defined by $x = 0$. It means that we will get in trouble when $x(t) = 0$ and no linear change of variable can solve the problem. Only an algebraic (or differential) change of variable such as taking $y = x^{1/2}$ (or $y = \dot{x}$) can reduce the original system to two regular components $\dot{y} = 2$ (corresponding to the main component) and $y = 0$

(corresponding to the singular component). Such things cannot happen if the system defines a single prime component as we assume here.

However, once υ has been chosen as a generic linear combination of the original variables and their derivatives, the new system $\underline{\Sigma}$ may have singularities, that are the places where the separant of its nonlinear equation vanishes. But, if such points are quasi-regular, we may find a new system $\underline{\Sigma}$ corresponding to a different definition of υ, for which possible singularities will occur at different places. So, we can avoid singularities by using different local charts. We illustrate this situation using again the pendulum example.

Example. In the pendulum example, we chose the linear form $\upsilon := y$ as a primitive element. The minimal polynomial of this linear form is

$$q = \upsilon^2 + x^2 - 1,$$

the separant of which vanishes for $y = 0$. Now we could also have chosen $\upsilon := x$ and get the minimal polynomial

$$q = \upsilon^2 + y^2 - 1,$$

the separant of which vanishes for $x = 0$. Obviously, the separants for these two systems cannot vanish at the same time.

Of course, such changes of coordinates are not easy to handle inside a numerical integrator.

4. Recovering solutions of Σ from solutions of $\underline{\Sigma}$

In this section, we will show that for almost all compatible initial condition, any solution of the system $\underline{\Sigma}$ introduced in Definition 4 can be locally lifted to a solution of the input system Σ. Moreover, we will prove that almost any local solution of Σ may be recovered from a solution of $\underline{\Sigma}$; more precisely, our main result states that there is a dense Zariski open set $\mathcal{O}$ of the variety of initial conditions such that for any point $\mathcal{X}$ in $\mathcal{O}$ there locally exists a unique solution of Σ with initial condition $\mathcal{X}$ that can be obtained by lifting a solution of $\underline{\Sigma}$.

We shall assume that the ground differential field $\mathbb{K}$ is a subfield of the field of complex numbers $\mathbb{C}$ and the solutions of the involved systems are solutions in the classical sense. The arguments we will use can be easily extended to any differential subfield $\mathbb{K}$ of the field of rational complex functions $\mathbb{C}(t)$ by considering t as a new unknown variable and adding the equation $\dot{t} = 1$.

In order to lift solutions $\underline{\varphi}$ of $\underline{\Sigma}$ to solutions φ of Σ, we start by introducing a dense Zariski open subset of the hypersurface $\underline{\mathcal{H}}$ that defines suitable initial conditions determining those solutions of $\underline{\Sigma}$ that we will be able to lift.

Let $x_i^{(j)}$, $0 \le j \le e-1$, $1 \le i \le n$, be a variable that does not belong to the set U. Let $\mathtt{Ass}\,(\mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}})$ be the set of the associated primes of the radical ideal $\mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}}$ and let $\cap\,\mathfrak{p}$, where $\mathfrak{p}$ runs over $\mathtt{Ass}\,(\mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}})$, be the primary decomposition of $\mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}}$ (see Proposition 4 and Notation 5). Then, for each component $\mathfrak{p}$ (which is a prime ideal with $\dim \mathfrak{p} = \mathrm{card}\, U$) there exists an irreducible polynomial $p_{ji\mathfrak{p}}$ in $\mathbb{K}[U, x_i^{(j)}]$ that lies in $\mathfrak{p}$.

Let p_{ji} be the least common multiple of the polynomials $(p_{ji\mathfrak{p}})_{\mathfrak{p}\in\mathtt{Ass}\,(\mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}})}$. Note that p_{ji} is the product of the polynomials $p_{ji\mathfrak{p}}$, without repeated factors:

$$p_{ji} = \prod_{\mathfrak{p}\in\mathtt{A}} p_{ji\mathfrak{p}} \quad \text{for some subset } \mathtt{A} \text{ of } \mathtt{Ass}\,(\mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}}). \tag{7}$$

Therefore, we have that p_{ji} is in $\mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}}$. Moreover, observe that no $\mathfrak{p}$ in $\mathtt{Ass}\,(\mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}})$ contains $\frac{\partial p_{ji}}{\partial x_i^{(j)}}$. In fact, the following relation holds:

$$\frac{\partial p_{ji}}{\partial x_i^{(j)}} = \sum_{\mathfrak{p}\in\mathtt{A}} \frac{\partial p_{ji\mathfrak{p}}}{\partial x_i^{(j)}} \prod_{\mathfrak{p}'\neq\mathfrak{p},\, \mathfrak{p}'\in\mathtt{A}} p_{ji\mathfrak{p}'}.$$

Now, if $\mathfrak{p}$ is in $\mathtt{A}$ then $\frac{\partial p_{ji\mathfrak{p}}}{\partial x_i^{(j)}} \prod_{\mathfrak{p}'\neq\mathfrak{p}} p_{ji\mathfrak{p}'}$ is not in $\mathfrak{p}$. Since all the remaining terms of the sum are multiples of $p_{ji\mathfrak{p}}$ they lie in $\mathfrak{p}$, and we conclude that $\frac{\partial p_{ji}}{\partial x_i^{(j)}}$ is not in $\mathfrak{p}$. The same argument runs identically if $\mathfrak{p}$ is not in $\mathtt{A}$.

Consider now the rational (not necessarily polynomial) map $\Phi : \mathcal{H} \to \mathcal{V}$ associated to the parametrization of $\mathcal{V}$ from $\mathcal{H}$. Observe that for any polynomial p in $\mathbb{K}[X^{[e+\sigma]} \setminus W]$ there exists a non-negative integer h (depending on p) such that $B(U)^h \frac{\partial q}{\partial \upsilon}(U, \upsilon)^h p\big(\Phi(U, \upsilon)\big)$ is a polynomial in $\mathbb{K}[U, \upsilon]$, where $B(U)$ is the polynomial introduced in the proof of Proposition 10.

Notation 12. *Let h be a positive integer such that*

$$p_0(U, \upsilon) := B(U)^h \tfrac{\partial q}{\partial \upsilon}(U, \upsilon)^h \prod_{x_i^{(j)} \notin U} \frac{\partial p_{ji}}{\partial x_i^{(j)}}\big(\Phi(U, \upsilon)\big)$$

is a polynomial in $\mathbb{K}[U, \upsilon, x_i^{(j)}]$ *divisible by* $B\frac{\partial q}{\partial \upsilon}$. *Note that, since* $\frac{\partial p_{ji}}{\partial x_i^{(j)}}\big(U, x_i^{(j)}\big)$ *is not in* $\mathfrak{p}$ *for each primary component* $\mathfrak{p}$ *of* $\mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}}$, *the set*

$$\mathcal{G}_0 := \mathcal{H} \cap \{p_0 \neq 0\}$$

is a Zariski open set which is dense in the hypersurface $\mathcal{H}$. *Observe that* $\mathcal{G}_0$ *is included in the definition domain of the rational map* Φ.

Consider the projection $\pi_1 : \mathbb{A}^{(1+\sigma)n+\mathrm{ord}[F]} \to \mathbb{A}^{(1+e)n}$ to the coordinates $\big(x, \dot{x}, \ldots, x^{(e)}\big)$. Since the relation $[F] \cap \mathrm{R}^{(e)} = \mathrm{pr}^{(\sigma+1)}F|_{\mathcal{W}} \cap \mathrm{R}^{(e)}$ holds (see Proposition 6), we conclude that $\overline{\pi_1(\mathcal{V})} = V\big([F] \cap \mathrm{R}^{(e)}\big)$. In the sequel, we denote by $\mathcal{S} = V\big([F] \cap \mathrm{R}^{(e)}\big)$. In particular, if the point $(\mathcal{U}_0, \upsilon_0)$ is in $\mathcal{G}_0$, the point $\pi_1(\Phi(\mathcal{U}_0, \upsilon_0))$ is in $\mathcal{S}$.

Now we will show that an analytic solution $\underline{\varphi}$ of the DAE system $\underline{\Sigma}$ such that the point $\underline{\varphi}(0)$ is in $\mathcal{G}_0$ can be lifted to a solution φ of the DAE system Σ:

Theorem 13. *Suppose that* $\underline{\varphi} : (-\varepsilon, \varepsilon) \to \mathbb{C}^{1+\mathrm{ord}[F]}$ *is an analytic solution of the DAE system* $\underline{\Sigma}$ *such that* $\underline{\varphi}(t)$ *is in* $\mathcal{G}_0$ *for all t and let*

$$\varphi(t) = \big(\varphi_0(t), \ldots, \varphi_e(t)\big) := \pi_1 \circ \Phi\,(\underline{\varphi}(t))$$

where $\varphi_j = (\varphi_{j,1}, \ldots, \varphi_{j,n})$ *for* $j = 0, \ldots, e$. *Then* $\varphi_0 : (-\varepsilon, \varepsilon) \to \mathbb{C}^n$ *is a well-defined analytic function that is a solution of the input DAE system* Σ.

Proof. Since $\underline{\varphi}(t)$ is in the subset $\mathcal{G}_0$ of $\mathrm{Dom}(\Phi)$, the map φ_0 is well defined and analytic.

In order to prove that φ_0 is a solution of Σ, first note that, since the image of $\pi_1 \circ \Phi \circ \underline{\varphi}$ is included in the variety $\mathcal{S}$, every polynomial in $[F] \cap \mathrm{R}^{(e)}$ vanishes at $(\pi_1 \circ \Phi \circ \underline{\varphi})(t)$ for all t. In particular, this holds for each equations in Σ.

Then, it suffices to show that the coordinate functions of φ verify the following relations

$$\frac{\mathrm{d}}{\mathrm{d}t}\varphi_{j,i}(t) = \varphi_{j+1,i}(t) \tag{8}$$

for every integer $0 \le j \le e-1,\ 1 \le i \le n$ and for any $t \in (-\varepsilon, \varepsilon)$. To do so, one can consider two cases.

First suppose that i, j are such that the variable $x_i^{(j)}$ is an element, say u_h, of the transcendence basis U of $\mathrm{Frac}(\mathrm{R}^{(e-1)}/[F] \cap \mathrm{R}^{(e-1)})$ chosen in Section 3.1. Hence $\varphi_{j,i}(t)$ is equal to $\underline{\varphi_h}(t)$ and relation (8) agrees with the equation corresponding to u_h in $\underline{\Sigma}$ after the specialization $(U, \upsilon) \mapsto \underline{\varphi}(t)$. Therefore, this relation is satisfied because $\underline{\varphi}$ is a solution of $\underline{\Sigma}$.

Suppose now that $x_i^{(j)}$ is not an element of U and let p_{ji} be its associated minimal polynomial in $[F] \cap \mathbb{K}[U, x_i^{(j)}] \subset [F] \cap \mathrm{R}^{(e-1)}$ as in (7). By taking the total derivative of p_{ji}, we obtain the following relation:

$$\frac{\mathrm{d}}{\mathrm{d}t}p_{ji} = \sum_h \frac{\partial p_{ji}}{\partial u_h}\big(U, x_i^{(j)}\big)\,\dot{u_h} + \frac{\partial p_{ji}}{\partial x_i^{(j)}}\big(U, x_i^{(j)}\big)\,x_i^{(j+1)} \in [F] \cap \mathrm{R}^{(e)}.$$

Therefore $\frac{\mathrm{d}}{\mathrm{d}t}p_{ji}(\varphi(t)) = 0$ for any $t \in (-\varepsilon, \varepsilon)$; more precisely, if $\varphi_U, \varphi_{\dot{U}}$ stand for the coordinates of $\varphi(t)$ corresponding to U and $\dot{U}$ respectively, we have $\dot{p_{ji}}(\varphi_U, \varphi_{\dot{U}}, \varphi_{j,i}, \varphi_{j+1,i}) = 0$. Since we have already proved relation (8) for every u_h, it follows that

$$\sum_h \frac{\partial\, p_{ji}}{\partial u_h}(\varphi_U, \varphi_{j,i})\,\frac{\mathrm{d}}{\mathrm{d}t}\varphi_{u_h}(t) + \frac{\partial\, p_{ji}}{\partial {x_i}^{(j)}}(\varphi_U, \varphi_{j,i})\varphi_{j+1,i}(t) = 0. \tag{9}$$

On the other hand, the polynomial p_{ji} is in $[F] \cap \mathrm{R}^{(e)}$ and, therefore, $p_{ji}(\varphi(t)) = 0$. By differentiating this identity with respect to t we obtain

$$\sum_h \frac{\partial\, p_{ji}}{\partial u_h}(\varphi_U(t), \varphi_{j,i}(t))\frac{\mathrm{d}}{\mathrm{d}t}\varphi_{u_h}(t) + \frac{\partial\, p_{ji}}{\partial {x_i}^{(j)}}(\varphi_U(t), \varphi_{j,i}(t))\frac{\mathrm{d}}{\mathrm{d}t}\varphi_{j,i}(t) = 0. \tag{10}$$

Since we assume that $\underline{\varphi}(t)$ is in $\mathcal{G}_0$, in particular we have

$$\frac{\partial\, p_{ji}}{\partial {x_i}^{(j)}}(\varphi_U(t), \varphi_{j,i}(t)) = \frac{\partial\, p_{ji}}{\partial {x_i}^{(j)}}(\Phi \circ \underline{\varphi}(t)) \neq 0.$$

Now, relation (8) is an immediate consequence of identities (9) and (10). □

We have already shown above how we can recover a solution of the original system Σ from a solution of the new system $\underline{\Sigma}$. Now we will show that almost every solution of Σ can be recovered from a solution of $\underline{\Sigma}$. We will apply the results of uniqueness and existence of solutions contained in Appendix B.

Recall that $[\underline{F}]$ is the differential ideal of $\mathbb{K}\{U, \upsilon\}$ defined by the system $\underline{\Sigma}$ (see Definition 4). Let $\underline{\mathcal{S}}$ be the variety $V([\underline{F}] \cap \mathbb{K}[U, \upsilon, \dot{U}, \dot{\upsilon}])$ in $\mathbb{A}^{2\mathrm{ord}[F]+2}$ and $\widetilde{\pi} : \underline{\mathcal{S}} \to \mathcal{H}$ the projection $(U, \upsilon, \dot{U}, \dot{\upsilon}) \mapsto (U, \upsilon)$.

Theorem 14. *There exist dense Zariski open sets $\mathcal{O} \subset \mathcal{S}$ and $\underline{\mathcal{O}} \subset \underline{\mathcal{S}}$ such that, for every point $(\mathcal{X}_0, \ldots, \mathcal{X}_e)$ in $\mathcal{O}$, there exist $\epsilon > 0$, a point $(\mathcal{U}_0, \upsilon_0, \dot{\mathcal{U}}_0, \dot{\upsilon}_0)$ in $\underline{\mathcal{O}}$ and an analytic function $\underline{\varphi} : (-\epsilon, \epsilon) \to \mathbb{C}^{1+\mathrm{ord}[F]}$ that is a solution of the system $\underline{\Sigma}$ with initial conditions $\underline{\varphi}(0) = (\mathcal{U}_0, \upsilon_0)$ satisfying:*

- $(\underline{\varphi}, \dot{\underline{\varphi}}) : (-\epsilon, \epsilon) \to \underline{\mathcal{O}}$,
- $(\pi_1 \circ \Phi)(\underline{\varphi}(t)) = \big(\varphi(t), \ldots, \varphi^{(e)}(t)\big) : (-\epsilon, \epsilon) \to \mathcal{O}$, *where φ is the unique analytic solution of the system Σ with initial conditions $\big(\varphi(0), \ldots, \varphi^{(e-1)}(0)\big) = (\mathcal{X}_0, \ldots, \mathcal{X}_{e-1})$.*

Proof. Let $\mathcal{Q}$ be the dense Zariski open set of regular points of $\mathcal{S}$ where the projection to $V\big([F] \cap \mathrm{R}^{(e-1)}\big)$ is unramified and $\underline{\mathcal{Q}_0}$ be the dense Zariski open set of regular points of $\underline{\mathcal{S}}$ where the projection $\widetilde{\pi}$ is unramified.

Let us denote by $\underline{\mathcal{O}}$ the dense Zariski open subset $\underline{\mathcal{Q}_0} \cap \{p_0 \neq 0\}$ of $\underline{\mathcal{S}}$, where p_0 denotes the polynomial in $\mathbb{K}[U, \upsilon]$ introduced in Notation 12. Note that, since all the points in $\underline{\mathcal{S}}$ satisfy that $B(U)\frac{\partial q}{\partial \upsilon}(U, \upsilon) \neq 0$, the morphism $\Phi : \mathcal{H} \to \mathcal{S}$ is an isomorphism between the set $\widetilde{\pi}(\underline{\mathcal{O}})$ (denoted by $\underline{\mathcal{Q}_1}$ in the sequel) and its image. Let us denote by $\mathcal{O}$ the set $\mathcal{Q} \cap (\pi_1 \circ \Phi)(\underline{\mathcal{Q}_1})$. We have then the following situation:

$$\begin{array}{ccccccc} \mathcal{V} & \supset & \Phi(\underline{\mathcal{Q}_1}) & \xleftarrow[\cong]{\Phi} & \underline{\mathcal{Q}_1} & \subset & \mathcal{H} \\ & & \pi_1 \downarrow & & \uparrow \widetilde{\pi} & & \\ \mathcal{S} & \supset & \mathcal{O} & & \underline{\mathcal{O}} & \subset & \underline{\mathcal{S}} \end{array}$$

Let $\mathcal{X}$ be the point $(\mathcal{X}_0, \ldots, \mathcal{X}_e)$ in the set $\mathcal{O} \subset \mathcal{Q}$. By Theorem 20, there exist a real $\varepsilon > 0$, an open neighborhood $\mathcal{O}_{\mathcal{X}}$ of $\mathcal{X}$, $\mathcal{O}_{\mathcal{X}} \subset \mathcal{O} \subset \mathcal{S}$, and a unique analytic solution $\varphi_{\mathcal{X}} : (-\varepsilon, \varepsilon) \to \mathbb{C}^n$ of Σ such that the image $\big(\varphi_{\mathcal{X}}, \ldots, {\varphi_{\mathcal{X}}}^{(e)}\big)(-\varepsilon, \varepsilon)$ is in $\mathcal{O}_{\mathcal{X}}$ and the relation $\big(\varphi_{\mathcal{X}}(0), \ldots, {\varphi_{\mathcal{X}}}^{(e-1)}(0)\big) = (\mathcal{X}_0, \ldots, \mathcal{X}_{e-1})$ holds.

Since the point $\mathcal{X}$ is in $\pi_1 \circ \Phi(\underline{\mathcal{Q}_1})$, there exists a point ξ in $\mathbb{A}^{(\sigma-e)n+\mathrm{ord}[F]}$ such that $(\mathcal{X}_0, \ldots, \mathcal{X}_e, \xi)$ is in $\Phi(\underline{\mathcal{Q}_1}) \subset \mathcal{V}$. Then, there is a point $(\mathcal{U}_0, \upsilon_0)$ in $\underline{\mathcal{Q}_1}$ such that $\Phi(\mathcal{U}_0, \upsilon_0) = (\mathcal{X}_0, \ldots, \mathcal{X}_e, \xi)$ and, since $\underline{\mathcal{Q}_1} = \widetilde{\pi}(\underline{\mathcal{O}})$, the relation $(\mathcal{U}_0, \upsilon_0) = \widetilde{\pi}(\mathcal{U}_0, \upsilon_0, \dot{\mathcal{U}}_0, \dot{\upsilon}_0)$ holds for some point $\mathcal{P} =$

$(\mathcal{U}_0, \upsilon_0, \dot{\mathcal{U}}_0, \dot{\upsilon}_0)$ in $\underline{\mathcal{O}}$. Recalling that $\underline{\mathcal{O}}$ is a subset of $\underline{\mathcal{Q}_0}$, by Remark 4, there exist a real $\underline{\varepsilon} > 0$, an open neighborhood $\underline{\mathcal{Q}_{\mathcal{P}}} \subset \underline{\mathcal{O}}$ of $\mathcal{P}$ and an analytic solution $\underline{\varphi} : (-\underline{\varepsilon}, \underline{\varepsilon}) \to \mathbb{C}^{1+\mathrm{ord}[F]}$ of $(\underline{\Sigma})$ with initial conditions $\underline{\varphi}(0) = (\mathcal{U}_0, \upsilon_0)$ such that the image $(\underline{\varphi}, \dot{\underline{\varphi}})(-\underline{\varepsilon}, \underline{\varepsilon})$ is in $\underline{\mathcal{Q}_{\mathcal{P}}}$. Then, for every $t \in (-\underline{\varepsilon}, \underline{\varepsilon})$, the point $\underline{\varphi}(t)$ is in the subset $\widetilde{\pi}(\underline{\mathcal{O}})$ of $\mathcal{G}_0$, where $\mathcal{G}_0$ is the dense Zariski open subset of $\mathcal{H}$ from Notation 12.

Now, Theorem 13 implies that the relation $\pi_1 \circ \Phi(\underline{\varphi}(t)) = (\varphi(t), \ldots, \varphi^{(e)}(t))$ holds for $t \in (-\varepsilon, \varepsilon)$, where $\varphi : (-\varepsilon, \varepsilon) \to \mathbb{C}^n$ is a solution of Σ. Since $\pi_1 \circ \Phi(\underline{\varphi}(0)) = \pi_1 \circ \Phi(\mathcal{U}_0, \upsilon_0) = \pi_1(\mathcal{X}_0, \ldots, \mathcal{X}_e, \xi) = \mathcal{X}$, which lies in $\mathcal{O}$, taking a smaller ε if necessary, we get that for every $t \in (-\varepsilon, \varepsilon)$ the point $\big(\varphi(t), \ldots, \varphi^{(e)}(t)\big)$ is in $\pi_1 \circ \Phi(\underline{\mathcal{Q}_1}) \cap \mathcal{Q} = \mathcal{O}$. Moreover, as $(\varphi(0), \ldots, \varphi^{(e-1)}(0)) = (\mathcal{X}_0, \ldots, \mathcal{X}_{e-1})$, if we denote $\min\{\underline{\varepsilon}, \varepsilon\}$ by ϵ, using the uniqueness statement of Theorem 20, we conclude that $\varphi_{\mathcal{X}}(t) = \varphi(t)$ for every $t \in (-\epsilon, \epsilon)$. $\square$

5. Conclusion

In this paper, we presented a new index reduction method for a class of implicit DAE systems which is based on a characterization of the differentiation index from an algebraic point of view. We proved that any of these systems is generically equivalent to a first order differential Kronecker representation with differentiation index 1 and we described a probabilistic algorithm to compute the index and the new DAE system by using the Kronecker solver for polynomial equations.

Our results rely on some *a priori* hypotheses on the considered differential system, for example the primality of the ideal $[F]$, which seems natural in practice, and the primality of the prolongation ideals, which in general we are not able to test. Assuming an admissible initial condition for our system to be known, polynomial time numerical methods of resolution, such as the one described in Corless and Ilie (2008) or power series computations (Bostan et al., 2007), may be used in order to obtain a solution. Since it is always possible to test, by simple substitution in the input equations, if a solution of the new system is actually a solution of the original DAE, one can attempt to use our method even if all our requirements on the considered system are not guaranteed.

A next step in a future work would be to generalize the method to positive differential dimension and to regular components of systems, without any extra technical hypothesis.

Urbs Romæ non uno die condita fuit.

Acknowledgements

D'Alfonso, Jeronimo and Solernó were partially supported by UBACyT X211 (2008–2010) and ANPCyT PICT2007-816. Jeronimo was partially supported by UBACyT X847 (2006–2009) and UBACyT 1069 (2010–2012). The work of Ollivier and Sedoglavic is supported by French Agence Nationale de la Recherche, Grant ANR-10-BLAN-0109.

Appendix A. On the specialization of free variables in a regular sequence

This appendix deals with Bertini-type results from Commutative Algebra that justify the random evaluation of suitable free variables made in Proposition 4. We have decided to include them for the sake of completeness and the lack of adequate references.

Throughout the appendix, $\mathbb{K}$ denotes a field of characteristic 0 and $\mathbb{K}[X]$ the ring of polynomials in the variables $X := \{x_1, \ldots, x_n\}$ with coefficients in $\mathbb{K}$.

We start recalling a well-known result concerning the behavior of radical ideals under field extensions of $\mathbb{K}$ (see Matsumura (1970, Section 27,(27.2), Lemma 2) and Hodge and Pedoe (1994, Volume 2, Chapter 10, Section 11)):

Theorem 15. *Let $\mathbb{K} \subseteq \mathbb{K}^\star$ be a field extension and let I be a radical equidimensional ideal in $\mathbb{K}[X]$. Then, the subset $I^\star := I \otimes \mathbb{K}^\star$ of $\mathbb{K}^\star[X]$ is also a radical equidimensional ideal. Furthermore, if I is a prime ideal and Y is a subset of the variables X such that $\mathbb{K}[Y] \hookrightarrow \mathbb{K}[X]/I$, then $\mathbb{K}^\star[Y] \hookrightarrow \mathbb{K}^\star[X]/\mathfrak{p}$ for any prime* *ideal $\mathfrak{p}$ in $\mathtt{Ass}\, I^\star$ (in other words, the transcendence of the variables modulo I is preserved modulo any primary component of $I^\star$).*

Notation 16. *For an ideal $I \subset \mathbb{K}[X]$, a subset $W \subset X$ of cardinality s and any $\mathcal{W} \in \mathbb{K}^s$, we denote by $I|_{\mathcal{W}}$ the ideal of $\mathbb{K}[X \setminus W]$ obtained after the specialization $W \mapsto \mathcal{W}$ in the polynomials of I.*

Lemma 2. *Let I be a radical equidimensional ideal in $\mathbb{K}[X]$ of dimension s. Let W be a subset of s variables in X such that the canonical morphism $\mathbb{K}[W] \to \mathbb{K}[X]/I$ is injective. Then, there exists a nonempty $\mathbb{K}$-definable Zariski open set $\mathcal{O}$ in $\mathbb{A}^s$ such that $I|_{\mathcal{W}}$ is a radical 0-dimensional ideal in $\mathbb{K}[X \setminus W]$ for any point $\mathcal{W}$ in $\mathcal{O} \cap \mathbb{K}^s$.*

Proof. Let $\widetilde{I}$ denote the ideal $I \otimes \mathbb{K}(W)$ in $\mathbb{K}(W)[Y]$ where Y stands for the set of variables $X \setminus W$. From the hypotheses and Theorem 15, this ideal is a radical 0-dimensional ideal in the polynomial ring $\mathbb{K}(W)[Y]$.

Then, the Shape Lemma implies that there exists a square-free polynomial $q(W, \upsilon)$ in $\mathbb{K}[W][\upsilon]$, where υ is a new single indeterminate, polynomials p_y in $\mathbb{K}[W][\upsilon]$ for each variable $y \in Y$, and a $\mathbb{K}$-linear form ℓ in the variables Y such that the equality of ideals

$$\widetilde{I} = \left(q(W, \ell), \left(\frac{\partial q}{\partial \upsilon}(W, \ell)y - p_y(W, \ell)\right)_{y \in Y}\right) \tag{11}$$

holds in $\mathbb{K}(W)[Y]$. Moreover, we may assume that the polynomials q, $\frac{\partial q}{\partial \upsilon}y - p_y$ have trivial content in $\mathbb{K}[W]$. From identity (11), it follows that there exists a nonzero denominator g in $\mathbb{K}[W]$ such that the relation $I\,\mathbb{K}[X]_g = \big(q(W, \ell), (\frac{\partial q}{\partial \upsilon}(W, \ell)y - p_y(W, \ell))_{y \in Y}\big)\,\mathbb{K}[X]_g$ holds.

Finally, let $\mathcal{O}$ be the Zariski open subset of $\mathbb{A}^s$, where the product $\big(g\,\frac{\partial q}{\partial \upsilon}\mathrm{discr}_\upsilon q\big)(W, \ell)$ is nonzero. Clearly, for any point $\mathcal{W}$ in $\mathcal{O}$, we have

$$I|_{\mathcal{W}} = \big(q(\mathcal{W}, \ell), (\tfrac{\partial q}{\partial \upsilon}(\mathcal{W}, \ell)y - p_y(\mathcal{W}, \ell))_{y \in Y}\big),$$

that is a 0-dimensional radical ideal in $\mathbb{K}[Y]$. □

The previous lemma can be generalized as follows.

Lemma 3. *Let I be a radical equidimensional ideal in $\mathbb{K}[X]$ and W be a subset of s variables in X such that the natural morphism $\mathbb{K}[W] \to \mathbb{K}[X]/I$ is injective (in particular, the relation $s \le \dim I$ holds). Then, there exists a nonempty $\mathbb{K}$-definable Zariski open set $\mathcal{O}$ in $\mathbb{A}^s$ such that, for any point $\mathcal{W}$ in $\mathcal{O} \cap \mathbb{K}^s$, the ideal $I|_{\mathcal{W}}$ has dimension $\dim I - s$ and its primary components of maximal dimension are prime ideals.*

Proof. Let us denote $\dim I$ by d. If $d = s$, the result follows from Lemma 2. Suppose now that $s < d$. Let us denote by $\mathtt{A}$ the set of primary components $\mathfrak{p}$ of I such that $\mathbb{K}[W] \to \mathbb{K}[X]/\mathfrak{p}$ is a monomorphism. Since the canonical map $\mathbb{K}[W] \to \mathbb{K}[X]/I$ is assumed to be injective, the set $\mathtt{A}$ is a nonempty subset in $\mathtt{Ass}\, I$. If we consider the canonical projection $\pi : \mathbb{A}^n \to \mathbb{A}^s$ the prime ideals in $\mathtt{A}$ correspond exactly with the components $V(\mathfrak{p})$ of $V(I)$ such that $\overline{\pi(V(\mathfrak{p}))} = \mathbb{A}^s$. Therefore, the set $\bigcup_{\mathfrak{p} \notin \mathtt{A}} \overline{\pi(V(\mathfrak{p}))}$ is a proper closed subset of $\mathbb{A}^s$; let $\mathcal{O}_0$ denote its complement in $\mathbb{A}^s$ (that is a nonempty Zariski open set).

Let U denote a set of $d - s$ $\mathbb{K}$-linear combinations of the variables $X \setminus W$ such that the natural morphism $\mathbb{K}[U, W] \to \mathbb{K}[X]/\mathfrak{p}$ is a monomorphism for all $\mathfrak{p}$ in $\mathtt{A}$. After a change of variables we may suppose without loss of generality that U is a subset of $X \setminus W$. Let Y be the set of the $n - d$ many remaining variables $X \setminus \{U, W\}$.

By Theorem 15, the ideal $\widetilde{I} := I \otimes \mathbb{K}(U)$ is a radical equidimensional ideal in $\mathbb{K}(U)[W, Y]$. Moreover, if $\mathfrak{p}$ is in $\mathtt{A}$, we have that $\mathfrak{p} \otimes \mathbb{K}(U)$ is a prime ideal of dimension $d - \mathrm{card}\, U = s$ and so, $\widetilde{I}$ is also s-dimensional. Therefore, the ideal $\widetilde{I} \subset \mathbb{K}(U)[W, Y]$ and the variables W meet the hypotheses of Lemma 2 and then, there exists a Zariski nonempty open set $\mathcal{G}$ in $\mathbb{A}^s_{\overline{\mathbb{K}(U)}}$, definable over $\mathbb{K}(U)$, such that $\widetilde{I}|_{\mathcal{W}}$ is a radical 0-dimensional ideal in $\mathbb{K}(U)[Y]$ for every $\mathcal{W}$ in $\mathcal{G} \cap \mathbb{K}(U)^s$. Let $\mathcal{O}_1$ be a Zariski nonempty open set in $\mathbb{A}^s$ definable over $\mathbb{K}$ such that $\mathcal{O}_1$ is a subset of $\mathcal{G}$. Then, if $\mathcal{W}$ is a point in $\mathcal{O}_1 \cap \mathbb{K}^s$, the primary components of $I|_{\mathcal{W}}$ in $\mathbb{K}[U, Y]$ with no nonzero polynomial pure in the variables U are $(d - s)$-dimensional prime ideals.

On the other hand, since the projection $\pi : \mathbb{A}^n \to \mathbb{A}^s$ induces a dominant regular morphism of varieties $\pi : V(I) \to \mathbb{A}^s$, by the theorem on the dimension of the fibers (see, for instance Shafarevich (1994, Chapter I, Section 6.3, Theorem 7), suitably adapted to the case of a ground field not necessarily algebraically closed), there exists a $\mathbb{K}$-definable Zariski nonempty open subset $\mathcal{O}_2$ of $\mathbb{A}^s$ such that for every point $\mathcal{W}$ in $\mathcal{O}_2$ the fiber $\pi^{-1}(\mathcal{W})$ is $\mathbb{K}$-definable and geometrically equidimensional of dimension equal to $\dim V(I) - \dim \mathbb{A}^s = d - s$.

Summarizing, if the point $\mathcal{W}$ is in $\mathcal{O}_0 \cap \mathcal{O}_1 \cap \mathcal{O}_2 \cap \mathbb{K}^s$, then the ideal $I + (W - \mathcal{W})$ satisfies:

1. Any of its primary components of maximal dimension contains an isolated prime $\mathfrak{p}$ in $\mathtt{A}$ (that is a subset of $\mathtt{Ass}\, I$) such that $\mathbb{K}[U, W] \hookrightarrow \mathbb{K}[X]/\mathfrak{p}$ (since $\mathcal{W}$ is in $\mathcal{O}_0 \cap \mathcal{O}_2$ and due to the choice of the variables U).
2. Its primary components of maximal dimension which contain no nonzero polynomials in $\mathbb{K}[U]$ are prime (because $\mathcal{W}$ is in $\mathcal{O}_1$).
3. It is geometrically equidimensional of dimension $d - s$ (since $\mathcal{W}$ is in $\mathcal{O}_2$).

From condition (2), the lemma will be proved if we are able *to exhibit a $\mathbb{K}$-definable Zariski nonempty open set contained in $\mathcal{O}_0 \cap \mathcal{O}_1 \cap \mathcal{O}_2$ such that, for any point $\mathcal{W}$ lying in this open set, all the isolated components of $I + (W - \mathcal{W})$ contain no nonzero polynomials of* $\mathbb{K}[U]$. The remaining part of the proof is devoted to showing this fact.

Let $\mathfrak{p}$ be a prime ideal in $\mathtt{A}$. We have the following injections $\mathbb{K}[W] \hookrightarrow \mathbb{K}[U, W] \hookrightarrow \mathbb{K}[X]/\mathfrak{p}$, and each variable y_i in Y, with $i = 1, \ldots, n - d$, verifies a polynomial equation $p_i(y_i) = 0$ modulo $\mathfrak{p}$, where p_i is a nonzero element in $\mathbb{K}[U, W][T]$ with $\deg_T p_i > 0$ (here T denotes a new variable). We denote by $\mathrm{lc}(p_i)$ the leading coefficient of p_i in $\mathbb{K}[U, W]$.

Claim. *There exists a $\mathbb{K}$-definable nonempty Zariski open subset $\mathcal{O}_{i,\mathfrak{p}}$ in $\mathcal{O}_0 \cap \mathcal{O}_1 \cap \mathcal{O}_2$ such that for any point $\mathcal{W}$ in $\mathcal{O}_{i,\mathfrak{p}} \cap \mathbb{K}^s$ and for any irreducible component $\mathcal{C}$ of $\pi^{-1}(\mathcal{W}) \cap V(\mathfrak{p})$ (necessarily of dimension $d - s$), we have that* $\mathrm{lc}(p_i)$ *does not vanish identically over $\mathcal{C}$.*

Let us prove this claim. To do so, consider the set $V(\mathfrak{p}) \cap V(\mathrm{lc}(p_i))$ in $\mathbb{A}^n$. If this set is empty there is no component of $\pi^{-1}(\mathcal{W}) \cap V(\mathfrak{p})$ contained in $V(\mathrm{lc}(p_i))$ and the claim follows. On the other hand, if the set $V(\mathfrak{p}) \cap V(\mathrm{lc}(p_i))$ is nonempty, since we have the injection $\mathbb{K}[U, W] \hookrightarrow \mathbb{K}[X]/\mathfrak{p}$, then $\mathrm{lc}(p_i)$ is not a zero divisor modulo $\mathfrak{p}$ and so this algebraic set must be an equidimensional algebraic variety of dimension $\dim V(\mathfrak{p}) - 1 = d - 1$. We consider two cases:

- If the relation $\overline{\pi(V(\mathfrak{p}) \cap V(\mathrm{lc}(p_i)))} = \mathbb{A}^s$ holds: from the theorem on the dimension of fibers applied to the restriction of the projection π to $V(\mathfrak{p}) \cap V(\mathrm{lc}(p_i))$, there exists a $\mathbb{K}$-definable nonempty Zariski open $\mathcal{O}_{i,\mathfrak{p}}$ in $\mathbb{A}^s$, that can be assumed contained in $\mathcal{O}_0 \cap \mathcal{O}_1 \cap \mathcal{O}_2$, such that, for any point $\mathcal{W}$ in $\mathcal{O}_{i,\mathfrak{p}} \cap \mathbb{K}^s$, any component of the fiber $\pi^{-1}(\mathcal{W}) \cap V(\mathfrak{p}) \cap V(\mathrm{lc}(p_i))$ has dimension $\dim V(\mathfrak{p}) \cap V(\mathrm{lc}(p_i)) - s = d - 1 - s$.

  Now, if $\mathcal{C}$ is an irreducible component of $\pi^{-1}(\mathcal{W}) \cap V(\mathfrak{p})$, since $\mathcal{W}$ is in $\mathcal{O}_2$ the relation $\dim \mathcal{C} = d - s$ holds. If $\mathrm{lc}(p_i)$ vanishes identically over $\mathcal{C}$, then $\mathcal{C}$ is contained in $\pi^{-1}(\mathcal{W}) \cap V(\mathfrak{p}) \cap V(\mathrm{lc}(p_i))$ that is a $(d - 1 - s)$-dimensional variety. So $\mathcal{C}$ is not contained in $V(\mathrm{lc}(p_i))$.
- If $\overline{\pi(V(\mathfrak{p}) \cap V(\mathrm{lc}(p_i)))}$ is a proper subset of $\mathbb{A}^s$: define the set $\mathcal{O}_{i,\mathfrak{p}}$ to be the open Zariski set $\mathcal{O}_0 \cap \mathcal{O}_1 \cap \mathcal{O}_2 \cap \overline{\pi(V(\mathfrak{p}) \cap V(\mathrm{lc}(p_i)))}^{\mathrm{C}}$. Clearly, $\pi^{-1}(\mathcal{W}) \cap V(\mathfrak{p}) \cap V(\mathrm{lc}(p_i))$ is empty and so $\mathcal{O}_{i,\mathfrak{p}}$ works.

Hence, our claim is proved. In order to finish the proof of the lemma, consider the nonempty Zariski open set $\mathcal{O} := \bigcap_{i,\mathfrak{p}\in\mathtt{A}} \mathcal{O}_{i,\mathfrak{p}}$. It suffices to prove that for any $\mathcal{W}$ in $\mathcal{O}$ and any isolated primary component $\mathfrak{q}$ of $I + (W - \mathcal{W}) \subset \mathbb{K}[X]$, the relation $\mathbb{K}[U] \cap \mathfrak{q} = \{0\}$ holds. The primary ideal $\mathfrak{q}$ defines an irreducible component $\mathcal{C}$ of the fiber $\pi^{-1}(\mathcal{W}) \cap V(I)$; therefore, $\mathcal{C}$ is a subset of $V(\mathfrak{p})$ for some $\mathfrak{p}$ in $\mathtt{A}$ (since $\mathcal{W}$ is in $\mathcal{O}_0$) and the relation $\dim \mathfrak{q} = d - s$ holds because $\mathcal{W}$ is in $\mathcal{O}_2$. Hence we have the sequence of natural morphisms

$$\mathbb{K}[U, W] \hookrightarrow \mathbb{K}[X]/\mathfrak{p} \to \mathbb{K}[X]/\sqrt{\mathfrak{q}} = \mathbb{K}[\mathcal{C}],$$

where the last morphism is the projection to the quotient; in particular, if we call ϕ the composition of the morphisms we have $\phi(W) = \mathcal{W}$ and the coordinate ring $\mathbb{K}[\mathcal{C}]$ is generated as a $\mathbb{K}$-algebra by $\phi(U)$ and the class of the variables Y. From the definition of $\mathcal{O}$ and the previous claim, it follows that the class of each y_i is algebraic over the subring $\mathbb{K}[\phi(U)]$ of $\mathbb{K}[\mathcal{C}]$ and so, the relation $d - s = \dim \mathcal{C} \leq \operatorname{card} U = d - s$ holds. Hence ϕ is a monomorphism, and in particular $\mathfrak{q}$ does not contain polynomials in $\mathbb{K}[U] \setminus \{0\}$. $\square$

Corollary 17. *Let I be a radical equidimensional ideal in $\mathbb{K}[X]$, and let U and W be two disjoint subsets of variables such that the natural morphism $\mathbb{K}[U, W] \to \mathbb{K}[X]/I$ is injective. Then, there exists a nonempty $\mathbb{K}$-definable Zariski open set $\mathcal{O}$ in $\mathbb{A}^s$, where s is the cardinality of W, verifying the previous lemma and such that, for every point $\mathcal{W}$ in $\mathcal{O} \cap \mathbb{K}^s$, the morphism $\mathbb{K}[U] \to \mathbb{K}[X]/(I + (W - \mathcal{W}))$ is injective.*

Proof. From Theorem 15 we are able to apply Lemma 3 to the field $\widetilde{\mathbb{K}} := \mathbb{K}(U)$ and the ideal $\widetilde{I} := I \otimes \widetilde{\mathbb{K}} \subset \widetilde{\mathbb{K}}[X \setminus U]$. Therefore, we obtain a nonempty Zariski open subset $\widetilde{\mathcal{O}}$ of $\mathbb{A}^s_{\widetilde{\mathbb{K}}}$. On the other hand, we may also apply Lemma 3 to the ideal I and the variables W over the ground field $\mathbb{K}$, obtaining an open set $\mathcal{O}_0$.

Now take $\mathcal{O}$ an arbitrary $\mathbb{K}$-definable nonempty Zariski open set contained in $\widetilde{\mathcal{O}} \cap \mathcal{O}_0$. It suffices to see that $\mathbb{K}[U]$ is included in the ring $\mathbb{K}[X]/(I + (W - \mathcal{W}))$ for $\mathcal{W}$ in $\mathcal{O}$, which is immediate from the fact that $\mathcal{W}$ is in $\widetilde{\mathcal{O}}$ and, in particular, there exists a component of maximal dimension of $I + (W - \mathcal{W})$ which contains no nonzero polynomial pure in the variables U. $\square$

If the ideal I is prime, the proof of Lemma 3 allows us to show a more precise version of the previous corollary.

Corollary 18. *Let I be a prime ideal in $\mathbb{K}[X]$, and let U and W be two disjoint subsets of variables such that $\{U, W\}$ is a transcendence basis of the fraction field of $\mathbb{K}[X]/I$. Then, there exists a nonempty $\mathbb{K}$-definable Zariski open set $\mathcal{O} \subset \mathbb{A}^s$ such that, for every point $\mathcal{W}$ in $\mathcal{O} \cap \mathbb{K}^s$, the ideal $I|_{\mathcal{W}}$ has dimension $\dim I - s$ and its primary components of maximal dimension are prime ideals containing no nonzero polynomial pure in the variables U.*

Proof. Simply observe that in the proof of Lemma 3 the subset of associated primes $\mathtt{A}$ is the unitary set $\{I\}$ if I is assumed to be a prime ideal. Therefore, the claim and the remaining part of the proof run *mutatis mutandis*. $\square$

Now, we can prove the main result of this appendix.

Theorem 19. *Let $n \geq 2$ and X a set of n indeterminates over a field $\mathbb{K}$ of characteristic 0. Let $\{f_1, \ldots, f_r\}$ be a reduced regular sequence in $\mathbb{K}[X]$ (that is, a regular sequence such that the ideals $(f_1, \ldots, f_i)$ in $\mathbb{K}[X]$ are radical for $i = 1, \ldots, r$). Let W be a subset of s many variables in X, with $s < n$, such that the canonical map $\mathbb{K}[W] \to \mathbb{K}[X]/(f_1, \ldots, f_r)$ is injective. Let us denote by Y the set of remaining variables $X \setminus W$.*

Then, there exists a nonempty $\mathbb{K}$-definable Zariski open set $\mathcal{O} \subset \mathbb{A}^s$ such that, for every point $\mathcal{W}$ in $\mathcal{O} \cap \mathbb{K}^s$ and all $i = 1, \ldots, r$, the polynomials $f_1(\mathcal{W}, Y), \ldots, f_i(\mathcal{W}, Y)$ form a reduced regular sequence in the polynomial ring $\mathbb{K}[Y]$.

Proof. We prove this theorem by recurrence in r.

If $r = 1$, since the polynomial f_1 is assumed to be square-free, we take $\mathcal{O}$ as the projection of $\{\mathrm{discr}_y(f_1) \neq 0\}$ to $\mathbb{A}^s$, where y is any variable in Y which appears in f_1.

Assume that the result holds for an integer $r \geq 1$. Let $f_1, \ldots, f_{r+1}$ be a regular sequence in $\mathbb{K}[X]$ such that the ideals $(f_1, \ldots, f_i)$ are radical for $i = 1, \ldots, r + 1$ and let W be a subset of X such that the canonical morphism $\mathbb{K}[W] \hookrightarrow \mathbb{K}[X]/(f_1, \ldots, f_{r+1})$ is injective. In particular, $\mathbb{K}[W] \hookrightarrow \mathbb{K}[X]/(f_1, \ldots, f_r)$ is injective too. Hence, by the induction hypothesis, there exists a nonempty $\mathbb{K}$-definable Zariski open subset $\mathcal{O}_1$ of $\mathbb{A}^s$ such that, for any point $\mathcal{P}_1$ in $\mathcal{O}_1$ and for any $i = 1, \ldots, r$, the polynomials $f_1(\mathcal{P}_1, Y), \ldots, f_i(\mathcal{P}_1, Y)$ form a regular sequence which generates a radical ideal in $\mathbb{K}[Y]$.

From Macaulay's unmixedness theorem (see, for instance Kunz (1985, Chapter VI, Section 3, Theorem 3.14)), the ideal $I := (f_1, \ldots, f_{r+1})$ is equidimensional of dimension $n - (r + 1)$ and so, the hypotheses of Lemma 3 are met for the ideal I and the variables W. Then, there exists a $\mathbb{K}$-definable nonempty Zariski open subset $\mathcal{O}_2$ of $\mathbb{A}^s$, such that for any point $\mathcal{P}_2$ in $\mathcal{O}_2 \cap \mathbb{K}^s$, the primary components of maximal dimension of $(f_1(\mathcal{P}_2, Y), \ldots, f_{r+1}(\mathcal{P}_2, Y)) \subset \mathbb{K}[Y]$ are prime ideals of dimension $\dim I - s = n - (r+1) - s$.

Take $\mathcal{O} := \mathcal{O}_1 \cap \mathcal{O}_2$. We will show that this open set verifies the statement of the theorem for $r+1$. Let $\mathcal{W}$ be a point in $\mathcal{O} \cap \mathbb{K}^s$. Since $f_1(\mathcal{W}, Y), \ldots, f_r(\mathcal{W}, Y)$ is a regular sequence that generates an equidimensional radical ideal (because $\mathcal{W}$ is in $\mathcal{O}_1$), in order to prove that $f_{r+1}(\mathcal{W}, Y)$ is not a zero divisor modulo $(f_1(\mathcal{W}, Y), \ldots, f_r(\mathcal{W}, Y))$, it suffices to show that the dimension drops by 1 when this polynomial is added. This follows directly from the fact that $\mathcal{W}$ also belongs to $\mathcal{O}_2$. Therefore $f_1(\mathcal{W}, Y), \ldots, f_{r+1}(\mathcal{W}, Y)$ is a regular sequence in $\mathbb{K}[Y]$. In particular, the generated ideal is unmixed by Macaulay's theorem, and then it is radical since $\mathcal{W} \in \mathcal{O}_2$. $\square$

Appendix B. Existence and uniqueness of solutions

Several previous articles consider the problem of the existence and uniqueness of solutions for *first order* implicit DAE systems (see, for instance Rabier and Rheinboldt, 1994; Pritchard, 2003; Pritchard and Sit, 2007; D'Alfonso et al., 2009). By adding new variables for the higher order derivatives in the usual way, these results can be extended to DAE systems of arbitrary order. For instance, let Σ be the DAE system introduced in Section 2.2 assuming that the hypotheses of Sections 2.1 and 2.4 are fulfilled and that $\mathbb{K}$ is a subfield of $\mathbb{C}$. Then we have the following generalization of D'Alfonso et al. (2009, Theorem 24):

Theorem 20. *Let $\mathcal{V}_0 \subset \mathbb{A}^{ne}$ and $\mathcal{V}_1 \subset \mathbb{A}^{n(e+1)}$ be the algebraic varieties defined by the ideals $[F] \cap \mathrm{R}^{(e-1)}$ and $[F] \cap \mathrm{R}^{(e)}$ respectively, and let $\pi : \mathcal{V}_1 \to \mathcal{V}_0$ be the projection to the first ne coordinates.*

Then, for every regular point $\mathcal{X} := (\mathcal{X}_0, \ldots, \mathcal{X}_{e-1}, \mathcal{X}_e)$ in $\mathcal{V}_1$ where the projection π is unramified, there exist $\varepsilon > 0$, a relative open neighborhood $\mathcal{O} \subset \mathcal{V}_1$ of $\mathcal{X}$ and a unique analytic function $\varphi : (-\varepsilon, \varepsilon) \to \mathbb{C}^n$ which is a solution of Σ with initial condition

$$\left(\varphi(0), \ldots, \varphi^{(e-1)}(0)\right) = (\mathcal{X}_0, \ldots, \mathcal{X}_{e-1})$$

such that $\left(\varphi(t), \ldots, \varphi^{(e-1)}(t), \varphi^{(e)}(t)\right)$ is in $\mathcal{O}$ for all t.

Proof. We make a straightforward change of variables in order to obtain an equivalent first order system: for each $i \in \{0, \ldots, e-1\}$, consider a new set Z_i of variables $(z_{i,1}, \ldots, z_{i,n})$ representing the derivatives $X^{(i)}$, and let Γ be the first order DAE system

$$\Gamma := \begin{cases} z_{i,j} - \dot{z}_{i-1,j} = 0, & i = 1, \ldots, e-1, \quad j = 1, \ldots, n, \\ f_1(Z, \dot{Z}) = 0, & \\ \quad\vdots & \\ f_n(Z, \dot{Z}) = 0, & \end{cases} \tag{12}$$

where Z denotes $Z_0, \ldots, Z_{e-1}$. We apply now to this system the existence and uniqueness result in D'Alfonso et al. (2009, Theorem 24), which holds in the case $e = 1$. In order to do so, let us verify that the required assumptions hold.

Denote by $\mathfrak{A}$ the differential ideal associated with the system Γ and consider the map $\Upsilon : \mathbb{K}\{X\} \to \mathbb{K}\{Z\}$ defined by

$$\Upsilon(x_i^{(j)}) = \begin{cases} z_{i,j} & \text{if } i < e, \\ {z_{e-1,j}}^{(i-e+1)} & \text{if } i \geq e. \end{cases}$$

Note that Υ is an injection that maps $[F] = [f_1, \ldots, f_n]$ to $\mathfrak{A}$. For each differential polynomial f in $\mathbb{K}\{X\}$, the expression $\Upsilon(\dot{f}) - (\Upsilon(f))'$ belongs to the differential ideal $[z_{i,j} - \dot{z}_{i-1,j}\,;\ 1 \leq i \leq e-1,\ 1 \leq j \leq n]$.

This implies that the relation $\mathfrak{A} = \Upsilon([F]) + [z_{i,j} - \dot{z}_{i-1,j}\,;\ 1 \leq i \leq e-1, 1 \leq j \leq n]$ holds. In particular, we have the isomorphism $\mathbb{K}\{X\}/[F] \simeq \mathbb{K}\{Z\}/\mathfrak{A}$ and then, if $[F]$ is a prime ideal, then so is $\mathfrak{A}$.

Moreover, we have the identities:

$$\begin{aligned} \mathfrak{A} \cap \mathbb{K}[Z] &= \Upsilon\left([F] \cap \mathrm{R}^{(e-1)}\right), \\ \mathfrak{A} \cap \mathbb{K}[Z, \dot{Z}] &= (z_{i,j} - \dot{z_{i-1,j}}\,;\ 1 \le i \le e-1,\ 1 \le j \le n) + \Upsilon\left([F] \cap \mathrm{R}^{(e)}\right). \end{aligned}$$

Therefore, if the polynomials $\mathtt{F}_{e-1}$ in $\mathrm{R}^{(e-1)}$ and $\mathtt{F}_e$ in $\mathrm{R}^{(e)}$ are generators of $[F] \cap \mathrm{R}^{(e-1)}$ and $[F] \cap \mathrm{R}^{(e)}$ respectively, then $\Upsilon(\mathtt{F}_{e-1})$ and

$$\mathtt{G} := \{z_{1,1} - \dot{z_{0,1}}, \dots, z_{1,n} - \dot{z_{0,n}}, \dots, \dot{z_{e-2,1}} - z_{e-1,1}, \dots, \dot{z_{e-2,n}} - z_{e-1,n}\} \cup \Upsilon(\mathtt{F}_e)$$

are generators of $\mathfrak{A} \cap \mathbb{K}[Z]$ and $\mathfrak{A} \cap \mathbb{K}[Z, \dot{Z}]$, respectively.

In particular, the Jacobian submatrix $\frac{\partial \mathtt{G}}{\partial \dot{Z}}$ has the block form

$$\begin{pmatrix} -\mathrm{Id}_{(e-1)n} & 0 \\ 0 & \Upsilon\left(D_{X^{(e)}} \mathtt{F}_e\right) \end{pmatrix}.$$

Thus, if $V(\mathfrak{A} \cap \mathbb{K}[Z, \dot{Z}])$ in $\mathbb{A}^{2ne}$ and $V(\mathfrak{A} \cap \mathbb{K}[Z])$ in $\mathbb{A}^{ne}$ are the varieties defined by the specified ideals, and $\widetilde{\mathcal{X}}$ is the point in $V(\mathfrak{A} \cap \mathbb{K}[Z, \dot{Z}])$ corresponding to $\mathcal{X} \in \mathcal{V}_1$, the unramifiedness of the projection $\pi : \mathcal{V}_1 \to \mathcal{V}_0$ at $\mathcal{X}$ is equivalent to the unramifiedness of the projection $\widetilde{\pi} : V(\mathfrak{A} \cap \mathbb{K}[Z, \dot{Z}]) \to V(\mathfrak{A} \cap \mathbb{K}[Z])$ at $\widetilde{\mathcal{X}}$. Similarly, the fact that $\mathcal{X}$ is a regular point of $\mathcal{V}_1$ implies that $\widetilde{\mathcal{X}}$ is a regular point of $V(\mathfrak{A} \cap \mathbb{K}[Z, \dot{Z}])$. $\square$

Remark 4. In the case of first order DAE systems, the existence and uniqueness of solutions as stated in D'Alfonso et al. (2009, Theorem 24) can also be extended to the case when the ideal $[F]$ is not prime, but the system Σ is quasi-regular. The result follows as in the proof of D'Alfonso et al. (2009, Theorem 24): if $\mathfrak{p}$ denotes a minimal prime differential ideal of $[F]$, then $\mathfrak{p}$ plays the same role as the ideal $\mathfrak{Q}$ in that proof and we can take $d = \mathrm{ord}(\mathfrak{p})$.

References

Bostan, A., Chyzak, F., Ollivier, F., Schost, É., Salvy, B., Sedoglavic, A., Fast computation of power series solutions of systems of differential equations, In: Proceedings of the 18th ACM-SIAM Symposium on Discrete Algorithms, New Orleans, Louisiana, USA, 2007, pp. 1012–1021.

Boulier, F., Lazard, D., Ollivier, F., Petitot, M., 2009. Computing representation for radicals of finitely generated differential ideals. AAECC 20 (1), 73–121.

Brenan, K.E., Stability and convergence for higher index differential algebraic equations with applications to trajectory control. Ph.D. Thesis, Department of Mathematics, University of California, 1983.

Brenan, K.E., Campbell, S.L.V., Petzold, L.R., 1996. Numerical Solution of Initial-Value Problems in Differential-Algebraic Equations. In: SIAM Classics in Applied Mathematics, vol. 14. Society for Industrial and Applied Mathematics.

Campbell, S.L.V., Gear, C.W., 1995. The index of general nonlinear DAEs. Numerische Mathematik 72 (2), 173–196.

Cluzeau, T., Hubert, E., 2003. Resolvent representation for regular differential ideals. Appl. Algebra Eng. Commun. Comput. 13 (5), 395–425.

Cluzeau, T., Hubert, E., 2008. Probabilistic algorithms for computing resolvent representations of regular differential ideals. Appl. Algebra Eng. Commun. Comput. 19 (5), 365–392.

Corless, R.M., Ilie, S., 2008. Polynomial cost for solving IVP for high-index DAE. BIT Numerical Mathematics 48, 29–49.

Dahan, X., Jin, X., Moreno Maza, M., Schost, E., 2008. Change of order for regular chains in positive dimension. Theoretical Computer Science 392, 37–65.

D'Alfonso, L., Jeronimo, G., Massaccesi, G., Solernó, P., 2009. On the index and the order of quasi-regular implicit systems of differential equations. Linear Algebra and its Applications 430 (8–9), 2102–2122.

D'Alfonso, L., Jeronimo, G., Solernó, P., 2006. On the complexity of the resolvent representation of some prime differential ideals. Journal of Complexity 22 (3), 396–430.

D'Alfonso, L., Jeronimo, G., Solernó, P., 2008. A linear algebra approach to the differentiation index of generic DAE systems. Applicable Algebra in Engineering, Communication and Computing 19 (6), 441–473.

Durvye, C., Lecerf, G., 2007. A concise proof of the kronecker polynomial system solver from scratch. Expositiones Mathematicae 26 (2), doi:10.1016/j.exmath.2007.07.001.

Eisenbud, D., 1995. Commutative algebra. In: Graduate Texts in Mathematics, vol. 150. Springer-Verlag, New York, With a view toward algebraic geometry.

Fliess, M., Lévine, J., Martin, Ph, Rouchon, P., Implicit differential equations and Lie-Bäcklund mappings. In: Proceedings of the 34th IEEE Conference on Decision and Control, New Orleans, Louisiana, USA, Dec. 1995, vol. 3, pp. 2704–2709.

Gear, C.W., 1988. Differential-algebraic equation index transformations. SIAM Journal on Scientific and Statistical Computing 9 (1), 39–47.

Gear, C.W., 1989. DAEs: ODEs with constraints and invariants. In: Numerical Methods for Ordinary Differential Equations. L'Aquila, Italy, Sept. 1989. In: Lecture Notes in Mathematics, vol. 1386. Springer, pp. 54–68.

Giusti, M., Lecerf, G., Salvy, B., 2001. A Gröbner free alternative for polynomial system solving. Journal of Complexity 17 (1), 154–211.

Hodge, W.V.D., Pedoe, D., 1994. Methods of Algebraic Geometry, vol. 2. Cambridge University Press.
Jacobi, C.G.J., 1865. De investigando ordine systematis aequationum differentialum vulgarium cujuscunque. Borchardt Journal für die reine und angewandte Mathematik LXIV 4, 297–320. English translation in Jacobi (2009).
Jacobi, C.G.J., 2009. Looking for the order of a system of arbitrary ordinary differential equations. Applicable Algebra in Engineering, Communication and Computing 20 (1), 7–32. Translated from the Latin by F. Ollivier.
Johnson, J., 1978. Systems of n partial differential equations in n unknown functions: the conjecture of M. Janet. Transactions of the American Mathematical Society 242, 329–334.
Kolchin, E.R., 1973. Differential algebra and algebraic groups. In: Pure and Applied Mathematics, vol. 54. Academic Press, New York.
Kondratieva, M.V., Mikhalev, A.V., Pankratiev, E.V., 1982. On Jacobi's bound for systems of differential polynomials. Algebra 79, 75–85.
Kondratieva, M.V., Mikhalev, A.V., Pankratiev, E.V., 2009. Jacobi's bound for independent systems of algebraic partial differential equations. AAECC 20 (1), 65–71.
Kunkel, P., Mehrmann, V.L., 2006. Differential-Algebraic Equations. Analysis and Numerical Solution. European Mathematical Society.
Kunz, E., 1985. Introduction to Commutative Algebra and Algebraic Geometry. Birkhäuser.
Lang, S., 2002. Algebra, 3rd ed. In: Graduate Texts in Mathematics, vol. 211. Springer.
Le Vey, G., 1994. Differential algebraic equations a new look at the index. Tech. Rep. 808, Institut de Recherche en Informatique et en Automatique.
Lecerf, G., 2003. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. Journal of Complexity 19 (4), 564–596.
Lötstedt, P., Petzold, L.R., 1986. Numerical solution of nonlinear differential equations with algebraic constraints I: convergence results for backward differentiation formulas. Mathematics of Computation 46 (174), 491–516.
Matera, G., Sedoglavic, A., 2003. Fast computation of discrete invariants associated to a differential rational mapping. Journal of Symbolic Computation 36 (3–4), 473–499.
Matsumura, H., 1970. Commutative Algebra, 2nd ed. In: Mathematics Lecture Note, vol. 56. WA Benjamin.
Mattsson, S.E., Söderlind, G., 1993. Index reduction in differential-algebraic equations using dummy derivatives. SIAM Journal of Scientific Computing 14 (3), 677–692.
Mishra, B., 1993. Algorithmic algebra. Springer-Verlag New York, Inc., New York, NY, USA.
Ollivier, F., Sadik, B., 2007. La borne de Jacobi pour une diffiété définie par un système quasi régulier. Comptes Rendus de l'Académie des Sciences 345 (3), 139–144.
Pantelides, C.C., 1988. The consistent initialization of differential–algebraic systems. SIAM Journal on Scientific and Statistical Computing 9 (2), 213–231.
Petzold, L.R., Lötstedt, P., 1986. Numerical solution of nonlinear differential equations with algebraic constraints II: practical implications. SIAM Journal on Scientific and Statistical Computing 7 (3), 720–733.
Poulsen, M.Z., 2001. Structural analysis of DAEs. PhD thesis, Informatics and Mathematical Modelling, Technical University of Denmark.
Pritchard, F.L., 2003. On implicit systems of differential equations. Journal of Differential Equations 194 (2), 328–363.
Pritchard, F.L., Sit, W.Y., 2007. On initial value problems for ordinary differential–algebraic equations. In: Gröbner Bases in Symbolic Analysis. In: Radon Ser. Comput. Appl. Math., vol. 2. Walter de Gruyter, Berlin, pp. 283–340.
Pryce, J.D., 2001. A simple structural analysis method for DAEs. BIT Numerical Mathematics 41, 364–394.
Rabier, P.J., Rheinboldt, W.C., 1994. A geometric treatment of implicit differential–algebraic equations. Journal of Differential Equations 109 (1), 110–146.
Reid, G.J., Lin, P., Wittkopf, A.D., 2001. Differential elimination-completion algorithms for DAE and PDAE. Studies in Applied Mathematics 106 (1), 1–45.
Ritt, J.F., 1950. Differential Algebra. In: American Mathematical Society Colloquium Publications, vol. 33. American Mathematical Society, New York, NY, USA.
Ritt, J.P., 1932. Differential equations from the algebraic standpoint. In: Amer. Math. Soc. Colloq. Publ., vol. 14. Walter De Gruyter Inc.
Schost, É., 2003. Computing parametric geometric resolutions. Applicable Algebra in Engineering, Communication and Computing 13 (5), 349–393.
Schwartz, J.T., 1980. Fast probabilistic algorithms for verification of polynomial identities. Journal of the ACM 27 (4), 701–717.
Seidenberg, R.A., 1952. Some basic theorems in differential algebra (characteristic p arbitrary). Transactions of the American Mathematical Society 73, 174–190.
Seiler, W.M., 1999. Indices and solvability of general systems of differential equations. In: Ghanza, V.G., Mayr, E.W., Vorozhtsov, E.V. (Eds.), Computer Algebra in Scientific Computing, vol. 99. Springer, pp. 365–386.
Shafarevich, I.R., 1994. Basic Algebraic Geometry, 2nd ed. vol. 1. Springer.
von zur Gathen, J., Gerhard, J., 1999. Modern Computer Algebra. Cambridge University Press, New York.
Zippel, R., 1979. Probabilistic algorithms for sparse polynomials. In: Symbolic and Algebraic Computation (EUROSAM'79, Internat. Sympos., Marseille, 1979). In: Lecture Notes in Comput. Sci., vol. 72. Springer, Berlin, pp. 216–226.