ARTICLE IN PRESS

Journal of Complexity ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Journal of Complexity

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

Effective differential Nullstellensatz for ordinary DAE systems with constant coefficients[☆]

Lisi D'Alfonso[a], Gabriela Jeronimo[b], Pablo Solernó[b,*]

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

[b] Departamento de Matemática and IMAS, UBA-CONICET, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, 1428, Buenos Aires, Argentina

ARTICLE INFO

Article history:
Received 27 May 2013
Accepted 23 January 2014
Available online xxxx

Keywords:
Differential algebra
Differential Hilbert Nullstellensatz
Differential elimination
DAE systems

ABSTRACT

We give upper bounds for the differential Nullstellensatz in the case of ordinary systems of differential algebraic equations over any field of constants K of characteristic 0. Let $\mathbf{x}$ be a set of n differential variables, $\mathbf{f}$ a finite family of differential polynomials in the ring $K\{\mathbf{x}\}$ and $f \in K\{\mathbf{x}\}$ another polynomial which vanishes at every solution of the differential equation system $\mathbf{f} = 0$ in any differentially closed field containing K. Let $d := \max\{\deg(\mathbf{f}), \deg(f)\}$ and $\epsilon := \max\{2, \operatorname{ord}(\mathbf{f}), \operatorname{ord}(f)\}$. We show that f^M belongs to the algebraic ideal generated by the successive derivatives of $\mathbf{f}$ of order at most $L = (n\epsilon d)^{2^{c(n\epsilon)^3}}$, for a suitable universal constant $c > 0$, and $M = d^{n(\epsilon+L+1)}$. The previously known bounds for L and M are not elementary recursive.

© 2014 Elsevier Inc. All rights reserved.

1. Introduction

In 1890, D. Hilbert states his famous result, currently known as Hilbert's Nullstellensatz: if k is a field and $f_1, \ldots, f_s, h$ are multivariate polynomials such that every zero of the f_i's, in an algebraic closure of k, is a zero of h, then some power of h is a linear combination of the f_i's with polynomial coefficients. In particular if $f_1, \ldots, f_s$ have no common zeros, then there exist polynomials $h_1, \ldots, h_s$ such that $1 = h_1 f_1 + \cdots + h_s f_s$. The classical proofs give no information about the polynomials h_i, for

☆ Partially supported by the following grants: UBACYT 20020110100063 (2012–2015)/Math-AmSud SIMCA "Implicit Systems, Modelling and Automatic Control" (2013–2014)/Subsidio para Investigador CONICET 4541/12 (2013) (P.S).

* Corresponding author.
E-mail addresses: lisi@cbc.uba.ar (L. D'Alfonso), jeronimo@dm.uba.ar (G. Jeronimo), psolerno@dm.uba.ar (P. Solernó).

http://dx.doi.org/10.1016/j.jco.2014.01.001
0885-064X/© 2014 Elsevier Inc. All rights reserved.

Please cite this article in press as: L. D'Alfonso, et al., Effective differential Nullstellensatz for ordinary DAE systems with constant coefficients, Journal of Complexity (2014), http://dx.doi.org/10.1016/j.jco.2014.01.001

instance, they give no bound for their degrees. The knowledge of such bounds yields a simple way of determining whether the algebraic variety $\{f_1 = 0, \dots, f_s = 0\}$ is empty. G. Hermann, in 1925, first addresses this question in [9] where she obtains a bound for the degrees of the h_i's double exponential in the number of variables. In the last 25 years, several authors have shown bounds single exponential in the number of variables (for a survey of the first results see [1] and for more recent improvements see [10]).

In 1932, J.F. Ritt in [21] introduces for the first time the differential version of Hilbert's Nullstellensatz in the ordinary context: *let $f_1, \dots, f_k, h$ be multivariate differential polynomials with coefficients in an ordinary differential field $\mathcal{F}$. If every zero of the system $f_1, \dots, f_k$ in any extension of $\mathcal{F}$ is a zero of h, then some power of h is a linear combination of the f_i's and a certain number of their derivatives, with polynomials as coefficients. In particular if the f_i's do not have common zeros, then a combination of $f_1, \dots, f_k$ and their derivatives of various orders equals unity*.

In fact, Ritt considers only the case of differential polynomials with coefficients in a differential field $\mathcal{F}$ of meromorphic functions in an open set of the complex plane. Later, H.W. Raudenbush, in [20], proves this result for polynomials with coefficients in any abstract ordinary differential field of characteristic 0. In 1952, A. Seidenberg gives a proof for arbitrary characteristic (see [22]) and, in 1973, E. Kolchin, in his book [12], proves the generalization of this result to differential polynomials with coefficients in an arbitrary, not necessarily ordinary, differential field.

None of the proofs mentioned above gives a constructive method for obtaining admissible values of the power of the polynomial h that is a combination of the f_i's and their derivatives, or for the number of these derivatives. A bound for these orders of derivation allows us to work in a polynomial ring in finitely many variables and invoke the results of the algebraic Nullstellensatz in order to determine whether or not a differential system has a solution. A first step in this direction was given by R. Cohn in [2], where he proves the existence of the power of the polynomial h through a process that it is known to have only a finite number of steps. In [23], Seidenberg studies this problem in the case of ordinary and partial differential systems, proving the existence of functions in terms of the parameters of the input polynomials which describe the order of the derivatives involved; however, no bounds are explicitly shown there. The first known bounds on this subject are given by O. Golubitsky et al. in [5], by means of rewriting techniques. Their general upper bounds are stated in terms of the Ackermann function and, in particular, they are not primitive recursive (see [5, Theorem 1]). If the number of derivations is fixed (for instance, in the case of ordinary differential equations), the bounds become primitive recursive; however, they are not elementary recursive, growing faster than any tower of exponentials of fixed height.

The present paper deals with effective aspects of the *ordinary* differential Nullstellensatz over the field $\mathbb{C}$ of complex numbers or, more generally, over arbitrary fields of constants of characteristic 0. Our main result, which can be found in Corollary 21 (see also Section 6 for the general case) states a doubly exponential upper bound for the number of required differentiations:

Theorem. *Let $\mathbf{x} := x_1, \dots, x_n$ and $\mathbf{f} := f_1, \dots, f_s$ be differential polynomials in $\mathbb{C}\{\mathbf{x}\}$. Suppose that $f \in \mathbb{C}\{\mathbf{x}\}$ is a differential polynomial such that every solution of the differential system $\mathbf{f} = 0$ in any differentially closed field containing $\mathbb{C}$ satisfies also $f = 0$. Let $d := \max\{\deg(\mathbf{f}), \deg(f)\}$ and $\epsilon := \max\{2, \mathrm{ord}(\mathbf{f}), \mathrm{ord}(f)\}$. Then $f^M \in (\mathbf{f}, \dots, \mathbf{f}^{(L)})$ where $L \leq (n\epsilon d)^{2^{c(n\epsilon)^3}}$, for a universal constant $c > 0$, and $M = d^{n(\epsilon+L+1)}$.*

In particular, this theorem, combined with known degree bounds for the polynomial coefficients in a representation of 1 as a linear combination of given generators of trivial algebraic ideals, allows the construction of an algorithm to decide whether a differential system has a solution with a triple exponential running time. From a different approach, an algorithm for this decision problem, with similar complexity, can be deduced as a particular case of the quantifier elimination method for ordinary differential equations proposed by D. Grigoriev in [6].

Our approach focuses mainly on the consistency problem for *first order semiexplicit ordinary systems over* $\mathbb{C}$, namely differential systems of the type of the system (4) introduced in Section 4. An iterative process of prolongation and projection, together with several tools from effective commutative algebra and algebraic geometry, is applied in such a way that in each step the dimension of the algebraic

Please cite this article in press as: L. D'Alfonso, et al., Effective differential Nullstellensatz for ordinary DAE systems with constant coefficients, Journal of Complexity (2014), http://dx.doi.org/10.1016/j.jco.2014.01.001

constraints decreases until a reduced, zero-dimensional situation is reached. The bounds for this particular case are computed directly. Then, by means of a recursive reconstruction, we are able to obtain a representation of 1 as an element of the differential ideal associated to the original system. The results for any arbitrary ordinary DAE system over $\mathbb{C}$ are deduced through the classical method of reduction of order, the algebraic Nullstellensatz, and the Rabinowitsch trick. The generalization from $\mathbb{C}$ to an arbitrary field of constants of characteristic 0 is achieved by means of standard arguments of field theory.

This paper is organized as follows. In Section 2 we introduce some basic tools and previous results from effective commutative algebra and algebraic geometry and some basic notions and notations from differential algebra. In Section 3 we address the case of semiexplicit systems with reduced 0-dimensional algebraic constraints. In Section 4 we show the process that reduces the arbitrary dimensional case to the reduced 0-dimensional one and then recover the information for the original system. In Section 5, the general case of an arbitrary ordinary DAE system over $\mathbb{C}$ is considered. Finally, in Section 6 we extend the previous results to any arbitrary base field K of characteristic 0 considered as a field of constants.

2. Preliminaries

In this section we recall some definitions and results from effective commutative algebra and algebraic geometry and introduce the notation and basic notions from differential algebra used throughout the paper.

2.1. Some tools from effective commutative algebra and algebraic geometry

Throughout the paper we will need several results from effective commutative algebra and algebraic geometry. We recall them here in the precise formulations we will use.

Before proceeding, we introduce some notation. Let $\mathbf{x} = x_1, \ldots, x_n$ be a set of variables and $\mathbf{f} = f_1, \ldots, f_s$ polynomials in $\mathbb{C}[\mathbf{x}]$. We will write $V(\mathbf{f})$ for the algebraic variety in $\mathbb{C}^n$ defined by $\{\mathbf{f} = 0\} = \{x \in \mathbb{C}^n : f_1(x) = 0, \ldots, f_s(x) = 0\}$. If $V \subset \mathbb{C}^n$ is an algebraic variety, $I(V)$ will denote the vanishing ideal of the variety V, that is $I(V) = \{f \in \mathbb{C}[\mathbf{x}] : f(x) = 0\ \forall x \in V\}$.

One of the results we will apply is an effective version of the strong Hilbert's Nullstellensatz (see for instance [10, Theorem 1.3]):

Proposition 1. *Let $f_1, \ldots, f_s \in \mathbb{C}[x_1, \ldots, x_n]$ be polynomials of degrees bounded by d, and let $I = (f_1, \ldots, f_s) \subset \mathbb{C}[x_1, \ldots, x_n]$. Then $(\sqrt{I})^{d^n} \subset I$.*

In addition, we will need estimates for the degrees of generators of the (radical) ideal of an affine variety $V \subset \mathbb{C}^n$.

A classical result due to Kronecker [16] states that any algebraic variety in $\mathbb{C}^n$ can be defined by $n + 1$ polynomials in $\mathbb{C}[x_1, \ldots, x_n]$. Moreover, these $n + 1$ polynomials can be chosen to be $\mathbb{Q}$-linear combinations of any finite set of polynomials defining the variety. In [7, Proposition 3], a refined version of Kronecker's theorem is proved for irreducible affine varieties. In this version the degree of the $n+1$ defining polynomials is bounded by the *degree* of the variety. We recall that the degree of an irreducible algebraic variety is defined as the number of points in the intersection of the variety with a generic linear variety of complementary dimension; for an arbitrary algebraic variety, it is defined as the sum of the degrees of its irreducible components (see [7]).

Kronecker's theorem with degree bounds can be extended straightforwardly to an arbitrary (not necessarily irreducible) algebraic variety $V \subset \mathbb{C}^n$ by considering equations of degree $\deg(C)$ for each irreducible component C of V and multiplying them in order to obtain a finite family of polynomials of degree $\sum_C \deg(C) = \deg(V)$ defining V:

Proposition 2. *Let $V \subset \mathbb{C}^n$ be an algebraic variety. Then, there exist $n+1$ polynomials of degrees at most $\deg(V)$ whose set of common zeros in $\mathbb{C}^n$ is V.*

In order to obtain upper bounds for the number and degrees of generators of the ideal of V, we will apply the following estimates, which follow from the algorithm for the computation of the radical of

Please cite this article in press as: L. D'Alfonso, et al., Effective differential Nullstellensatz for ordinary DAE systems with constant coefficients, Journal of Complexity (2014), http://dx.doi.org/10.1016/j.jco.2014.01.001

an ideal presented in [17, Section 4] (see also [14,15]) and estimates for the number and degrees of polynomials involved in Gröbner basis computations (see, for instance, [3,19,4]):

Proposition 3. *Let $I = (f_1, \ldots, f_s) \subset \mathbb{C}[x_1, \ldots, x_n]$ be an ideal generated by s polynomials of degrees at most d that define an algebraic variety of dimension r and let $\nu = \max\{1, r\}$. Then, the radical ideal $\sqrt{I}$ can be generated by $(sd)^{2^{O(\nu n)}}$ polynomials of degrees at most $(sd)^{2^{O(\nu n)}}$.*

Combining Propositions 2 and 3, we have:

Proposition 4. *Let $V \subset \mathbb{C}^n$ be an algebraic variety of dimension r and degree D and $\nu = \max\{1, r\}$. Then, the vanishing ideal of V can be generated by $(nD)^{2^{O(\nu n)}}$ polynomials of degrees at most $(nD)^{2^{O(\nu n)}}$.*

Finally, in order to use the bounds in the previous proposition, we will need to compute upper bounds for the degrees of algebraic varieties. To this end, we will apply the following Bézout type bound, taken from [8, Proposition 2.3]:

Proposition 5. *Let $V \subset \mathbb{C}^n$ be an algebraic variety of dimension r and degree D, and let $f_1, \ldots, f_s \in \mathbb{C}[x_1, \ldots, x_n]$ be polynomials of degree at most d. Then,*

$$\deg(V \cap V(f_1, \ldots, f_s)) \leq Dd^r.$$

2.2. Basic notions from differential algebra

If $\mathbf{z} := z_1, \ldots, z_\alpha$ is a set of α indeterminates, the ring of differential polynomials is denoted by $\mathbb{C}\{z_1, \ldots, z_\alpha\}$ or simply $\mathbb{C}\{\mathbf{z}\}$ and is defined as the commutative polynomial ring $\mathbb{C}[z_j^{(p)}, 1 \leq j \leq \alpha, p \in \mathbb{N}_0]$ (in infinitely many indeterminates), with the derivation $\delta(z_j^{(i)}) = z_j^{(i+1)}$, that is, $z_j^{(i)}$ stands for the ith derivative of z_j (as usual, the first derivatives are also denoted by $\dot{z}_j$). We write $\mathbf{z}^{(p)} := \{z_1^{(p)}, \ldots, z_\alpha^{(p)}\}$ and $\mathbf{z}^{[p]} := \{\mathbf{z}^{(i)}, 0 \leq i \leq p\}$ for every $p \in \mathbb{N}_0$.

For a differential polynomial h lying in the differential polynomial ring $\mathbb{C}\{\mathbf{z}\}$ the *successive total derivatives of h* are:

$$h^{(0)} := h$$
$$h^{(p)} := \sum_{i\in\mathbb{N}_0, 1\leq j\leq\alpha} \frac{\partial h^{(p-1)}}{\partial z_j^{(i)}} z_j^{(i+1)}, \quad \text{for } p \geq 1.$$

The *order of* $h \in \mathbb{C}\{\mathbf{z}\}$ *with respect to* z_j is $\mathrm{ord}(h, z_j) := \max\{i \in \mathbb{N}_0 : z_j^{(i)} \text{ appears in } h\}$, and the *order of h* is $\mathrm{ord}(h) := \max\{\mathrm{ord}(h, z_j) : 1 \leq j \leq \alpha\}$.

Given a finite set of differential polynomials $\mathbf{h} = h_1, \ldots, h_\beta \in \mathbb{C}\{\mathbf{z}\}$, we write $[\mathbf{h}]$ to denote the smallest *differential* ideal of $\mathbb{C}\{\mathbf{z}\}$ containing $\mathbf{h}$ (i.e. the smallest ideal containing the polynomials $\mathbf{h}$ and all their derivatives of arbitrary order). For every $i \in \mathbb{N}$, we write $\mathbf{h}^{(i)} := h_1^{(i)}, \ldots, h_\beta^{(i)}$ and $\mathbf{h}^{[i]} := \mathbf{h}, \mathbf{h}^{(1)}, \ldots, \mathbf{h}^{(i)}$.

3. The case of ODE's with 0-dimensional reduced algebraic constraint

3.1. An introductory case: univariate ODE's

We start by considering the simple case of trivial *univariate* differential ideals contained in $\mathbb{C}\{x\}$ where x is a single differential variable.

Suppose that the trivial ideal is presented by two generators $\dot{x} - f(x)$ and $g(x)$, without common differential solutions, where f and g are polynomials in $\mathbb{C}[x]$.

Since we assume that there exists a representation of 1 as a combination of $\dot{x} - f(x)$ and $g(x)$ and suitable derivatives of them, by replacing in such a representation all derivatives $x^{(i)}$ by 0 for $i \geq 1$, we deduce that the univariate polynomials f and g are relatively prime in $\mathbb{C}[x]$.

Let $1 = pf + qg$ be an identity in $\mathbb{C}[x]$; therefore, we have

$$1 = -p(x)(\dot{x} - f(x)) + q(x)g(x) + p(x)\dot{x}. \quad (1)$$

Please cite this article in press as: L. D'Alfonso, et al., Effective differential Nullstellensatz for ordinary DAE systems with constant coefficients, Journal of Complexity (2014), http://dx.doi.org/10.1016/j.jco.2014.01.001

On the other hand, if we *assume that* g *is square-free*, from a relation $1 = a(x)g(x) + b(x)\frac{\partial g}{\partial x}(x)$ we deduce $\dot{x} = \dot{x}a(x)g(x) + b(x)\dot{x}\frac{\partial g}{\partial x}(x) = \dot{x}a(x)g(x) + b(x)\dot{g}$. Thus, replacing $\dot{x}$ in (1) we have:

$$1 = -p(x)(\dot{x} - f(x)) + (q(x) + p(x)\dot{x}a(x))g(x) + p(x)b(x)\dot{g}.$$

In other words, we need at most one derivative of g in order to write 1 as a combination of the derivatives of the generators $\dot{x} - f(x)$ and $g(x)$.

Let us remark that a similar argument can be applied also if g is not assumed square-free with the aid of the Faà di Bruno formula (see for instance [11]) which describes each differential polynomial $g^{(i)}$ as a $\mathbb{Q}$-linear combination of products of $x^{(j)}, j \le i$, and successive derivatives $\frac{\partial^k g}{\partial x^k}$ up to order i. In this case it is not difficult to show that the maximum number of derivatives of the input equations which allow us to write 1 can be bounded *a priori* by the smallest k such that the first k derivatives of g are relatively prime and, moreover, no derivatives of $\dot{x} - f$ of positive order are needed. Since we do not make use of this result, we have not included a complete proof here.

3.2. *The multivariate case*

Now we consider the case of an arbitrary number of variables. Suppose that $\mathbf{x} = x_1, \dots, x_n$ and $\mathbf{u} = u_1, \dots, u_m$ are independent differential variables. Let $\mathbf{f} = f_1, \dots, f_n \in \mathbb{C}[\mathbf{x}, \mathbf{u}]$ and $\mathbf{g} = g_1, \dots, g_s \in \mathbb{C}[\mathbf{x}, \mathbf{u}]$ be polynomials such that the (polynomial) ideal $(\mathbf{g}) \subseteq \mathbb{C}[\mathbf{x}, \mathbf{u}]$ is *radical and* 0*-dimensional*.

Suppose that the differential ideal generated by the $n + s$ polynomials $\dot{\mathbf{x}} - \mathbf{f}$ and $\mathbf{g}$ is the whole differential ring $\mathbb{C}\{\mathbf{x}, \mathbf{u}\}$ (i.e. $1 \in [\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}]$). The goal of this subsection is to show that the order of derivatives of the generators which allows us to write 1 as a combination of them is at most 1 (see Proposition 6).

Under these assumptions, as in the previous section, we deduce that the polynomial ideal $(\mathbf{f}, \mathbf{g})$ is the ring $\mathbb{C}[\mathbf{x}, \mathbf{u}]$; hence, we have an algebraic identity $1 = \mathbf{p} \cdot \mathbf{f} + \mathbf{q} \cdot \mathbf{g}$ for suitable $n + s$ polynomials $\mathbf{p}, \mathbf{q} \in \mathbb{C}[\mathbf{x}, \mathbf{u}]$. Thus,

$$1 = -\mathbf{p} \cdot (\dot{\mathbf{x}} - \mathbf{f}) + \mathbf{q} \cdot \mathbf{g} + \mathbf{p} \cdot \dot{\mathbf{x}}. \tag{2}$$

Since the polynomial ideal $(\mathbf{g})$ is assumed to be radical and 0-dimensional, for each variable x_j there exists a nonzero square-free univariate polynomial $h_j \in \mathbb{C}[x_j]$ such that $h_j(x_j) \in (\mathbf{g}) \subseteq \mathbb{C}[\mathbf{x}, \mathbf{u}]$. The square-freeness of h_j implies that the relation $1 = a_j h_j + b_j \frac{\partial h_j}{\partial x_j}$ holds in the ring $\mathbb{C}[x_j]$ for suitable polynomials $a_j, b_j \in \mathbb{C}[x_j]$ and then, after multiplying by $\dot{x}_j$ we obtain the identities

$$\dot{x}_j = a_j \dot{x}_j h_j + b_j \dot{h}_j, \quad \text{for } j = 1, \dots, n. \tag{3}$$

On the other hand, each polynomial h_j can be written as a linear combination of the polynomials $\mathbf{g}$ with coefficients in $\mathbb{C}[\mathbf{x}, \mathbf{u}]$, which induces by derivation a representation of its derivative $\dot{h}_j$ as a linear combination of $\mathbf{g}, \dot{\mathbf{g}}$ with coefficients in $\mathbb{C}[\mathbf{x}, \mathbf{u}, \dot{\mathbf{x}}, \dot{\mathbf{u}}]$. Replacing h_j and $\dot{h}_j$ in (3) by these combinations and then replacing $\dot{\mathbf{x}}$ in (2), we conclude:

Proposition 6. *With the previous notations and assumptions we have*

$$1 \in [\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}] \subseteq \mathbb{C}\{\mathbf{x}, \mathbf{u}\} \quad \text{if and only if} \quad 1 \in (\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}, \dot{\mathbf{g}}) \subseteq \mathbb{C}[\mathbf{x}, \mathbf{u}, \dot{\mathbf{x}}, \dot{\mathbf{u}}].$$

In other words, in order to obtain a (differential) representation of 1 *it suffices to derive once the algebraic reduced equations* $\mathbf{g}$. ■

4. The main case: ODE's with arbitrary algebraic constraint

We will now consider semiexplicit differential systems with no restrictions on the dimension of the algebraic variety of constraints.

Let $\mathbf{x} = x_1, \dots, x_n$ and $\mathbf{u} = u_1, \dots, u_m$ be differential variables, and let $\mathbf{f} = f_1, \dots, f_n$ and $\mathbf{g} = g_1, \dots, g_s$ be polynomials in $\mathbb{C}[\mathbf{x}, \mathbf{u}]$. We consider the differential first order semiexplicit system

$$\begin{cases} \dot{\mathbf{x}} - \mathbf{f}(\mathbf{x}, \mathbf{u}) = 0 \\ \mathbf{g}(\mathbf{x}, \mathbf{u}) = 0. \end{cases} \tag{4}$$

Please cite this article in press as: L. D'Alfonso, et al., Effective differential Nullstellensatz for ordinary DAE systems with constant coefficients, Journal of Complexity (2014), http://dx.doi.org/10.1016/j.jco.2014.01.001

Suppose that the differential system (4) has no solution (or equivalently, $1 \in [\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}] \subseteq \mathbb{C}\{\mathbf{x}, \mathbf{u}\}$). Our goal is to find bounds for the order of a representation of 1 as a combination of the polynomials $\dot{\mathbf{x}} - \mathbf{f}$, $\mathbf{g}$ and their derivatives. Without loss of generality we will suppose *that the purely algebraic system* $\mathbf{g} = 0$ *is consistent*, because if it is not, it suffices to write 1 as a combination of the polynomials $\mathbf{g}$ and no derivatives are required.

The following theorem will be proved at the end of this section:

Theorem 7. *Let $\mathbf{x} = x_1, \ldots, x_n$ and $\mathbf{u} = u_1, \ldots, u_m$ be differential variables, and let $\mathbf{f} = f_1, \ldots, f_n$ and $\mathbf{g} = g_1, \ldots, g_s$ be polynomials in $\mathbb{C}[\mathbf{x}, \mathbf{u}]$. Let $V \subset \mathbb{C}^{n+m}$ be the variety defined as the set of zeros of the ideal $(\mathbf{g})$, $0 \le r := \dim(V)$, $\nu := \max\{1, r\}$ and D be an upper bound for the degrees of $\mathbf{f}, \mathbf{g}$ and V. Then,*

$$1 \in [\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}] \iff 1 \in (\dot{\mathbf{x}} - \mathbf{f}, \ldots, \mathbf{x}^{(L+1)} - \mathbf{f}^{(L)}, \mathbf{g}, \ldots, \mathbf{g}^{(L)}),$$

where $L \le ((n+m)D)^{2^{c\nu^2(n+m)}}$ for a universal constant $c > 0$.

In what follows we will show how it is possible to obtain a system related to the original inconsistent input system (4) but whose algebraic variety of constraints has dimension 0. To do this, we consider a sequence of auxiliary inconsistent differential systems such that their algebraic constraints define varieties with decreasing dimensions. Once this descending dimension process is done, we will be able to apply the results of Section 3.2. Finally, we will estimate the order of derivatives of the equations which enable us to write 1 as an element of the differential ideal by means of an ascending dimension process associated to the same sequence of auxiliary systems.

4.1. The dimension descending process

Let us begin by introducing some notation related to the differential part $\dot{\mathbf{x}} - \mathbf{f} = 0$ of the system (4) that will be used throughout this section.

Notation 8. If $\mathbf{h} = h_1, \ldots, h_\beta$ is a set of polynomials in $\mathbb{C}[\mathbf{x}, \mathbf{u}]$, we define

$$\widetilde{h_i} := \sum_{j=1}^{n} \frac{\partial h_i}{\partial x_j} f_j + \sum_{k=1}^{m} \frac{\partial h_i}{\partial u_k} \dot{u}_k \in \mathbb{C}[\mathbf{x}, \mathbf{u}, \dot{\mathbf{u}}]$$

for $i = 1, \ldots, \beta$. In other words,

$$\widetilde{\mathbf{h}} := \frac{\partial \mathbf{h}}{\partial \mathbf{x}} \cdot \mathbf{f} + \frac{\partial \mathbf{h}}{\partial \mathbf{u}} \cdot \dot{\mathbf{u}}.$$

Note that the polynomials $\widetilde{\mathbf{h}}$ belong to the polynomial ideal $(\dot{\mathbf{x}} - \mathbf{f}, \dot{\mathbf{h}}) \cap \mathbb{C}[\mathbf{x}, \mathbf{u}, \dot{\mathbf{u}}]$.

If $I \subset \mathbb{C}[\mathbf{x}, \mathbf{u}]$ is an ideal, we denote by $\widetilde{I} \subset \mathbb{C}[\mathbf{x}, \mathbf{u}, \dot{\mathbf{u}}]$ the ideal generated by I and the polynomials $\widetilde{h}$ with $h \in I$. Note that if a set of polynomials $\mathbf{h}$ generates the ideal I, then the polynomials $\mathbf{h}, \widetilde{\mathbf{h}}$ generate the ideal $\widetilde{I}$ in $\mathbb{C}[\mathbf{x}, \mathbf{u}, \dot{\mathbf{u}}]$ and that $\widetilde{I} \subset (\dot{\mathbf{x}} - \mathbf{f}, \mathbf{h}, \dot{\mathbf{h}}) \cap \mathbb{C}[\mathbf{x}, \mathbf{u}, \dot{\mathbf{u}}]$.

The key point to our dimension descending process is the following geometric lemma.

Lemma 9. *Let $\pi : \mathbb{C}^{n+2m} \to \mathbb{C}^{n+m}$ be the projection $(\mathbf{x}, \mathbf{u}, \dot{\mathbf{u}}) \mapsto (\mathbf{x}, \mathbf{u})$ and suppose that the ideal $(\mathbf{g}) \subset \mathbb{C}[\mathbf{x}, \mathbf{u}]$ is radical.*

If the system (4) has no solution, then no irreducible component of $V(\mathbf{g})$ is contained in the Zariski closure $\overline{\pi(V(\mathbf{g}, \widetilde{\mathbf{g}}))}$ and, in particular, since $\pi(V(\mathbf{g}, \widetilde{\mathbf{g}})) \subseteq V(\mathbf{g})$, we have that $\dim \overline{\pi(V(\mathbf{g}, \widetilde{\mathbf{g}}))} < \dim V(\mathbf{g})$.

Proof. Throughout the proof, for a set of variables $\mathbf{z}$ and a set of polynomials $\mathbf{h}$ in $\mathbb{C}[\mathbf{z}]$, if $\bar{\mathbf{z}} \subset \mathbf{z}$ and $\bar{\mathbf{h}} \subset \mathbf{h}$, we will denote by $\frac{\partial \bar{\mathbf{h}}}{\partial \bar{\mathbf{z}}}$ the $\#(\bar{\mathbf{h}}) \times \#(\bar{\mathbf{z}})$ Jacobian matrix of the polynomials $\bar{\mathbf{h}}$ with respect to the variables $\bar{\mathbf{z}}$.

Suppose that there is an irreducible component C of $V(\mathbf{g})$ included in $\overline{\pi(V(\mathbf{g}, \widetilde{\mathbf{g}}))}$. We will construct a solution for the system (4).

Since the Zariski algebraic closed set $\overline{\pi(V(\mathbf{g}, \widetilde{\mathbf{g}}))}$ is contained in $V(\mathbf{g})$, there exists at least one irreducible component Z of $V(\mathbf{g}, \widetilde{\mathbf{g}})$ such that $C = \overline{\pi(Z)}$. From Chevalley's Theorem (see e.g. [18, Chapter 2, Section 6]) there exists a nonempty Zariski open subset $\mathcal{U}$ of C contained in the image

$\pi(Z) \subseteq \pi(V(\mathbf{g}, \widetilde{\mathbf{g}}))$. Moreover, since the ideal $(\mathbf{g})$ is assumed to be radical, shrinking the open set $\mathcal{U}$ if necessary, we may also suppose that all points $p \in \mathcal{U}$ are regular points of C and then, the Jacobian matrix $\frac{\partial \mathbf{g}}{\partial(\mathbf{x},\mathbf{u})}(p)$ has rank $n + m - \dim C$.

Similarly, we may suppose also that for all $p \in \mathcal{U}$ the equality

$$\mathrm{rk}\frac{\partial \mathbf{g}}{\partial \mathbf{u}}(p) = \max\left\{\mathrm{rk}\frac{\partial \mathbf{g}}{\partial \mathbf{u}}(x, u) : (x, u) \in C\right\}$$

holds, and that the first columns of $\frac{\partial \mathbf{g}}{\partial \mathbf{u}}(p)$ are a $\mathbb{C}$-basis of the column space of this matrix.

Set $l := \mathrm{rk}\frac{\partial \mathbf{g}}{\partial \mathbf{u}}(p)$. If $\widehat{\mathbf{u}} = u_1, \ldots, u_l$ and $\overline{\mathbf{u}} = u_{l+1}, \ldots, u_m$, then there exists a subset $\widehat{\mathbf{x}} \subseteq \mathbf{x}$ of cardinality $k := n + m - \dim C - l$ such that $\mathrm{rk}\frac{\partial \mathbf{g}}{\partial(\widehat{\mathbf{x}},\widehat{\mathbf{u}})}(p) = \mathrm{rk}\frac{\partial \mathbf{g}}{\partial(\mathbf{x},\mathbf{u})}(p) = k + l$. For simplicity assume that $\widehat{\mathbf{x}} = x_1, \ldots, x_k$. We denote $\overline{\mathbf{x}} = x_{k+1}, \ldots, x_n$.

Claim. *For every $p \in \mathcal{U}$ there exists a unique $\widehat{\eta} \in \mathbb{C}^l$ (depending on p) such that $(p, \widehat{\eta}, 0) \in V(\mathbf{g}, \widetilde{\mathbf{g}})$.*

Proof of the claim. Fix $p \in \mathcal{U}$. Since $\mathcal{U} \subseteq \pi(V(\mathbf{g}, \widetilde{\mathbf{g}}))$ there exists $(a, b) \in \mathbb{C}^l \times \mathbb{C}^{m-l}$ (not necessarily unique) such that $(p, a, b) \in V(\mathbf{g}, \widetilde{\mathbf{g}})$. Thus

$$\frac{\partial \mathbf{g}}{\partial \mathbf{x}}(p) \cdot \mathbf{f}(p) + \frac{\partial \mathbf{g}}{\partial \widehat{\mathbf{u}}}(p) \cdot a + \frac{\partial \mathbf{g}}{\partial \overline{\mathbf{u}}}(p) \cdot b = 0.$$

In particular, the linear system in the unknowns $(\mathbf{y}, \mathbf{z}) \in \mathbb{C}^l \times \mathbb{C}^{m-l}$:

$$\frac{\partial \mathbf{g}}{\partial \widehat{\mathbf{u}}}(p) \cdot \mathbf{y} + \frac{\partial \mathbf{g}}{\partial \overline{\mathbf{u}}}(p) \cdot \mathbf{z} = -\frac{\partial \mathbf{g}}{\partial \mathbf{x}}(p) \cdot \mathbf{f}(p)$$

has a solution, or equivalently, the columns of $\frac{\partial \mathbf{g}}{\partial \mathbf{x}}(p) \cdot \mathbf{f}(p)$ belong to the linear subspace generated by the columns of the matrix $\frac{\partial \mathbf{g}}{\partial \mathbf{u}}(p)$. By our choice of the variables $\widehat{\mathbf{u}}$, the columns of the matrix $\frac{\partial \mathbf{g}}{\partial \widehat{\mathbf{u}}}(p)$ are a basis of this subspace. Then, the linear system $\frac{\partial \mathbf{g}}{\partial \widehat{\mathbf{u}}}(p) \cdot \mathbf{y} = -\frac{\partial \mathbf{g}}{\partial \mathbf{x}}(p) \cdot \mathbf{f}(p)$ has a unique solution $\widehat{\eta} \in \mathbb{C}^l$, which means that $(p, \widehat{\eta}, 0) \in V(\mathbf{g}, \widetilde{\mathbf{g}})$. This finishes the proof of the claim.

Now we go back to the proof of the lemma. We are looking for a solution of the system (4) when the irreducible component C of the variety $V(\mathbf{g})$ lies in $\overline{\pi(V(\mathbf{g}, \widetilde{\mathbf{g}}))}$.

Fix a point $(x_0, u_0) = (\widehat{x}_0, \overline{x}_0, \widehat{u}_0, \overline{u}_0) \in \mathcal{U}$. From the Implicit Function Theorem around (x_0, u_0), shrinking the open set $\mathcal{U}$ in the strong topology if necessary, there exists a neighborhood $\mathcal{V}_0 \subset \mathbb{C}^{(n-k)+(m-l)}$ of the point $(\overline{x}_0, \overline{u}_0)$ (also in the strong topology) and differentiable functions $\varphi_1 : \mathcal{V}_0 \to \mathbb{C}^k$ and $\varphi_2 : \mathcal{V}_0 \to \mathbb{C}^l$ such that for any $(x, u) = (\widehat{x}, \overline{x}, \widehat{u}, \overline{u}) \in \mathcal{U}$, the equality $(\widehat{x}, \widehat{u}) = (\varphi_1(\overline{x}, \overline{u}), \varphi_2(\overline{x}, \overline{u}))$ holds and in particular we have

$$(x, u) = (\varphi_1(\overline{x}, \overline{u}), \overline{x}, \varphi_2(\overline{x}, \overline{u}), \overline{u}) \quad \text{for all } (x, u) \in \mathcal{U}. \tag{5}$$

For $i = k+1, \ldots, n$, we write $\overline{\psi_i}(\overline{\mathbf{x}}, \overline{\mathbf{u}}) = f_i(\varphi_1(\overline{\mathbf{x}}, \overline{\mathbf{u}}), \overline{\mathbf{x}}, \varphi_2(\overline{\mathbf{x}}, \overline{\mathbf{u}}), \overline{\mathbf{u}})$ and $\overline{\psi} = \overline{\psi}_{k+1}, \ldots, \overline{\psi}_n$.

Let us consider the following ODE with initial condition in the $n - k$ unknowns $\overline{\mathbf{x}}$:

$$\begin{cases} \dot{\overline{\mathbf{x}}} = \overline{\psi}(\overline{\mathbf{x}}, \overline{u}_0) \\ \overline{\mathbf{x}}(0) = \overline{x}_0 \end{cases} \tag{6}$$

and let $\gamma(t) = (\gamma_{k+1}(t), \ldots, \gamma_n(t))$ be a solution of the system (6) in a neighborhood of 0.

From this solution γ we define

$$\Gamma(t) = (\varphi_1(\gamma(t), \overline{u}_0), \gamma(t), \varphi_2(\gamma(t), \overline{u}_0), \overline{u}_0)$$

in a neighborhood of 0. From (6) we have that $(\gamma(0), \overline{u}_0) = (\overline{x}_0, \overline{u}_0)$; therefore, the continuity of γ ensures that for all t in a neighborhood of 0, $(\gamma(t), \overline{u}_0)$ belongs to the open set $\mathcal{V}_0$ and then Γ is well defined.

It suffices to prove that $\Gamma(t)$ is a solution of the original system (4), which leads to a contradiction since that system has no solution.

First of all, by (5) we deduce that $\Gamma(t) \in \mathcal{U} \subseteq C$ for all t small enough and so, $\mathbf{g}(\Gamma(t)) = 0$. In other words, $\Gamma(t)$ satisfies the algebraic constraint of the system (4). In order to show that $\Gamma(t)$ also satisfies the differential part of (4) we observe that its coordinates $k+1,\dots,n$ are simply $\gamma(t)$, which satisfy the differential relations:

$$\frac{d}{dt}(\gamma_i(t)) = \overline{\psi}_i(\gamma(t),\overline{u}_0)$$

for $i = k+1,\dots,n$. Since $\overline{\psi}_i(\gamma(t),\overline{u}_0) = f_i(\Gamma(t))$, we conclude that Γ satisfies the last $n-k$ differential equations of (4). It remains to show that it also satisfies the first k differential equations of (4).

Taking the derivative with respect to the single variable t in the identity $\mathbf{g}(\Gamma(t)) = 0$ we obtain:

$$\frac{\partial \mathbf{g}}{\partial \widehat{\mathbf{x}}}(\Gamma(t)) \cdot \frac{d}{dt}(\varphi_1(\gamma(t),\overline{u}_0)) + \frac{\partial \mathbf{g}}{\partial \overline{\mathbf{x}}}(\Gamma(t)) \cdot \frac{d}{dt}(\gamma(t)) + \frac{\partial \mathbf{g}}{\partial \widehat{\mathbf{u}}}(\Gamma(t)) \cdot \frac{d}{dt}(\varphi_2(\gamma(t),\overline{u}_0)) = 0,$$

and then

$$-\frac{\partial \mathbf{g}}{\partial \overline{\mathbf{x}}}(\Gamma(t)) \cdot \frac{d}{dt}(\gamma(t)) = \frac{\partial \mathbf{g}}{\partial (\widehat{\mathbf{x}},\widehat{\mathbf{u}})}(\Gamma(t)) \cdot \frac{d}{dt}(\varphi(\gamma(t),\overline{u}_0)), \tag{7}$$

where $\varphi = (\varphi_1,\varphi_2)$.

On the other hand, since for all t in a neighborhood of 0 we have $\Gamma(t) \in \mathcal{U} \subseteq \pi(V(\mathbf{g},\widetilde{\mathbf{g}}))$, the previous *Claim* implies that there exists a unique $\widehat{\eta}(t) \in \mathbb{C}^l$ such that $(\Gamma(t),\widehat{\eta}(t),0) \in V(\mathbf{g},\widetilde{\mathbf{g}})$ and then, if we write $\widehat{\mathbf{f}} = f_1,\dots,f_k$ and $\bar{\mathbf{f}} = f_{k+1},\dots,f_n$,

$$\frac{\partial \mathbf{g}}{\partial \widehat{\mathbf{x}}}(\Gamma(t)) \cdot \widehat{\mathbf{f}}(\Gamma(t)) + \frac{\partial \mathbf{g}}{\partial \overline{\mathbf{x}}}(\Gamma(t)) \cdot \bar{\mathbf{f}}(\Gamma(t)) + \frac{\partial \mathbf{g}}{\partial \widehat{\mathbf{u}}}(\Gamma(t)) \cdot \widehat{\eta}(t) = 0.$$

Hence,

$$-\frac{\partial \mathbf{g}}{\partial \overline{\mathbf{x}}}(\Gamma(t)) \cdot \bar{\mathbf{f}}(\Gamma(t)) = \frac{\partial \mathbf{g}}{\partial (\widehat{\mathbf{x}},\widehat{\mathbf{u}})}(\Gamma(t)) \cdot (\widehat{\mathbf{f}}(\Gamma(t)),\widehat{\eta}(t)). \tag{8}$$

Since $\frac{d}{dt}(\gamma(t)) = \overline{\psi}(\gamma(t),\overline{u}_0) = \bar{\mathbf{f}}(\Gamma(t))$ and the matrix $\frac{\partial \mathbf{g}}{\partial(\widehat{\mathbf{x}},\widehat{\mathbf{u}})}(\Gamma(t))$ has a $(k+l)\times(k+l)$ invertible minor, comparing (7) and (8), we infer that

$$\frac{d}{dt}(\varphi(\gamma(t),\overline{u}_0)) = (\widehat{\mathbf{f}}(\Gamma(t)),\widehat{\eta}(t)).$$

In particular $\frac{d}{dt}(\varphi_1(\gamma(t),\overline{u}_0)) = \widehat{\mathbf{f}}(\Gamma(t))$. Thus Γ verifies also the first k differential equations in (4) and the lemma is proved. ■

Before we begin the descending process, let us remark that the new differential system induced by the construction underlying Lemma 9 trivially inherits the inconsistency from the input system (4):

Remark 10. Let notations be as in Lemma 9 and $\mathbf{g}_1$ be a set of generators of the (radical) ideal $I(\overline{\pi(V(\mathbf{g},\widetilde{\mathbf{g}}))})$. If the system (4) has no solution, neither does the differential system

$$\begin{cases} \dot{\mathbf{x}} - \mathbf{f}(\mathbf{x},\mathbf{u}) = 0 \\ \mathbf{g}_1(\mathbf{x},\mathbf{u}) = 0. \end{cases}$$

This is a consequence of the inclusion of algebraic ideals $(\mathbf{g}) \subset \sqrt{(\mathbf{g})} \subset (\mathbf{g}_1)$, which implies the inclusion of differential ideals $[\mathbf{g}] \subset [\mathbf{g}_1]$; hence, $1 \in [\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}_1]$.

We will now begin to present the descending dimension process induced by Lemma 9.

Definition 11. From the system (4), we define recursively an increasing chain of radical ideals $I_0 \subset I_1 \subset \cdots$ in the polynomial ring $\mathbb{C}[\mathbf{x},\mathbf{u}]$ as follows:

- $I_0 = \sqrt{(\mathbf{g})}$.
- Assuming that I_i is defined, consider the ideal $\widetilde{I}_i \subseteq \mathbb{C}[\mathbf{x},\mathbf{u},\dot{\mathbf{u}}]$ introduced in Notation 8 and suppose that $1 \notin \widetilde{I}_i$. We define $I_{i+1} = \sqrt{\widetilde{I}_i \cap \mathbb{C}[\mathbf{x},\mathbf{u}]}$.

Let us observe some basic facts about this definition. First, note that $I_0 = I(V(\mathbf{g}))$ and, for $i \geq 1$, if $\pi : \mathbb{C}^{n+2m} \to \mathbb{C}^{n+m}$ is the projection $(\mathbf{x},\mathbf{u},\dot{\mathbf{u}}) \mapsto (\mathbf{x},\mathbf{u})$, then $I_{i+1} = I(\overline{\pi(V(\widetilde{I}_i))})$ (we have that

$V(\widetilde{I_i}) \subset \mathbb{C}^{n+2m}$ is nonempty since we assume $1 \notin \widetilde{I_i}$). Second, from Lemma 9, it follows that the chain of ideals defined is strictly increasing since the inequality $\dim(V(I_{i+1})) < \dim(V(I_i))$ holds. We can estimate the length of this chain: if we define

$$\rho := \min\{i \in \mathbb{Z}_{\geq 0} : \dim(V(I_i)) \leq 0\}$$

we have that $0 \leq \rho \leq r$ (recall that we assume that the ideal I_0 is a proper ideal with $\dim(V(I_0)) = r \geq 0$). Notice also that if $\rho > 0$, then $\dim(V(I_\rho)) = 0$ or -1 and $\dim(V(I_{\rho-1})) > 0$.

Any system of generators $\mathbf{g}_\rho$ of the last ideal I_ρ allows us to exhibit a new ODE system, related to the original one, with no solutions and such that 1 can be easily written as a combination of the generators of the associated differential ideal. More precisely,

Proposition 12. *Fix $i = 0, \ldots, \rho$ and let $\mathbf{g}_i \subset \mathbb{C}[\mathbf{x}, \mathbf{u}]$ be any system of generators of the radical ideal I_i. Then the DAE system*

$$\begin{cases} \dot{\mathbf{x}} - \mathbf{f}(\mathbf{x}, \mathbf{u}) = 0 \\ \mathbf{g}_i(\mathbf{x}, \mathbf{u}) = 0 \end{cases}$$

has no solution. In the particular case $i = \rho$, we also have that 1 belongs to the polynomial ideal $(\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}_\rho, \dot{\mathbf{g}}_\rho) \subset \mathbb{C}[\mathbf{x}, \dot{\mathbf{x}}, \mathbf{u}, \dot{\mathbf{u}}]$.

Proof. The first assertion follows from the iterated application of Remark 10. If $i = \rho$ and $\dim(I_\rho) = -1$ (i.e. if $I_\rho = \mathbb{C}[\mathbf{x}, \mathbf{u}]$) we have $1 \in (\mathbf{g}_\rho) \subset (\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}_\rho, \dot{\mathbf{g}}_\rho)$. Otherwise, if $\dim(I_\rho) = 0$, since the ideal $I_\rho = (\mathbf{g}_\rho)$ is radical, the proposition follows from the 0-dimensional case considered in Proposition 6. ■

In the following lemma we will estimate bounds for the degree and the number of polynomials in suitable families $\mathbf{g}_i$ which generate the ideals I_i, for each $i = 1, \ldots, \rho$. It will be a consequence of Proposition 4.

Lemma 13. *Consider the DAE system (4), and let $r := \dim(V(\mathbf{g}))$, $\nu := \max\{1, r\}$ and $D := \max\{\deg(\mathbf{f}), \deg(\mathbf{g}), \deg(V(\mathbf{g}))\}$. There exists a universal constant $c > 0$ such that for each $0 \leq i \leq \rho$, the ideal I_i can be generated by a family of polynomials $\mathbf{g}_i$ whose number and degrees are bounded by $((n+m)D)^{2^{c(i+1)\nu(n+m)}}$. Moreover, if $r > 0$, this is also an upper bound for the degrees of the polynomials $\widetilde{\mathbf{g}}_i$.*

Proof. First, notice that, if $r = 0$, then $\rho = 0$. Since $\mathbf{g}_0$ is a set of generators of $\sqrt{(\mathbf{g})}$, the bound is a direct consequence of Proposition 4. Let us now suppose that $r > 0$.

From Proposition 4, since $V(\mathbf{g}) \subset \mathbb{C}^{n+m}$ is an algebraic variety of dimension $r_0 := r$ and degree at most $D_0 := D$, the radical ideal $I_0 = I(V(\mathbf{g}))$ can be generated by a set $\mathbf{g}_0$ of $\delta_0 := ((n+m)D)^{2^{c_0 r_0 (n+m)}}$ polynomials of degrees at most δ_0, where c_0 is an adequate positive constant. By modifying the constant c_0 if necessary, we may suppose that δ_0 is also an upper bound for the degrees of the polynomials $\widetilde{\mathbf{g}}_0$ introduced in Notation 8.

Following [7, Lemma 2], the degree of the variety $\overline{\pi(V(\widetilde{I_0}))} = \overline{\pi(V(\mathbf{g}_0, \widetilde{\mathbf{g}}_0))}$ is at most $\deg(V(\mathbf{g}_0, \widetilde{\mathbf{g}}_0))$ and then, from Proposition 5 and the previous bounds we infer that

$$\deg(\overline{\pi(V(\widetilde{I_0}))}) \leq \deg(V(\mathbf{g}_0, \widetilde{\mathbf{g}}_0)) \leq D_0 \delta_0^{r_0} = (n+m)^{r_0 2^{c_0 r_0 (n+m)}} D^{1 + r_0 2^{c_0 r_0 (n+m)}} =: D_1.$$

Applying again the estimate stated in Proposition 4, we have that the ideal $I_1 = I(\overline{\pi(V(\widetilde{I_0}))})$ can be generated by a set $\mathbf{g}_1$ consisting of at most

$$\delta_1 := ((n+m)D_1)^{2^{c_0 r_1 (n+m)}} = ((n+m)D)^{2^{c_0 r_1 (n+m)} (1 + r_0 2^{c_0 r_0 (n+m)})}$$

polynomials of degrees bounded by δ_1, where $r_1 := \dim(V(I_1)) < r_0$. By the choice of c_0, δ_1 is also an upper bound for the degrees of the polynomials $\widetilde{\mathbf{g}}_1$.

Proceeding in the same way, it can be proved inductively that, for every $0 \leq i \leq \rho - 1$,

$$\deg(\overline{\pi(V(\widetilde{I_i}))}) \leq \deg(V(\mathbf{g}_i, \widetilde{\mathbf{g}}_i)) \leq D_i \delta_i^{r_i} = \frac{1}{n+m} ((n+m)D)^{\prod_{j=0}^{i} (1 + r_j 2^{c_0 r_j (n+m)})} =: D_{i+1}$$

and, therefore, the radical ideal $I_{i+1} = I(\overline{\pi(V(\widetilde{I}_i))})$ can be generated by a system of polynomials $\mathbf{g}_{i+1}$ whose number and degrees are bounded by

$$\delta_{i+1} := ((n+m)D_{i+1})^{2^{c_0 r_{i+1}(n+m)}} = ((n+m)D)^{2^{c_0 r_{i+1}(n+m)} \prod_{j=0}^{i}(1+r_j 2^{c_0 r_j(n+m)})},$$

which is also an upper bound for the degrees of the polynomials $\widetilde{\mathbf{g}}_i$.

The result follows by choosing a universal constant c such that $1 + r2^{c_0 r(n+m)} \leq 2^{cr(n+m)}$ for every $r > 0$. ■

We introduce the following invariants associated to the chain of ideals $I_0 \subset I_1 \subset \cdots \subset I_\rho$ and the generators $\mathbf{g}_i$, $i = 0, \dots, \rho$, considered in Lemma 13, that we will use in the next section.

Definition 14. With the previous notations, for each $i = 0, \dots, \rho$, we define ε_i as follows:

$$\varepsilon_0 := \min\{\varepsilon \in \mathbb{N} : I_0^\varepsilon \subseteq (\mathbf{g})\},$$
$$\varepsilon_i := \min\{\varepsilon \in \mathbb{N} : I_i^\varepsilon \subseteq (\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}_{i-1}, \dot{\mathbf{g}}_{i-1})\} \quad \text{for } i > 0.$$

Observe that by definition, $\varepsilon_i > 0$ for all i. Moreover, they are well defined (i.e. finite) since I_i is the radical of the ideal $\widetilde{I}_{i-1} \cap \mathbb{C}[\mathbf{x}, \mathbf{u}]$ and $\widetilde{I}_{i-1} = (\mathbf{g}_{i-1}, \widetilde{\mathbf{g}}_{i-1}) \subseteq (\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}_{i-1}, \dot{\mathbf{g}}_{i-1})$ (see the final remark in Notation 8). In fact, we can obtain upper bounds for these integer numbers in terms of the parameters of the input system (4):

Proposition 15. *As in Lemma 13, let $D := \max\{\deg(\mathbf{f}), \deg(\mathbf{g}), \deg(V(\mathbf{g}))\}$. We have the inequalities:*

$$\varepsilon_0 \leq D^{n+m} \quad \textit{and} \quad \varepsilon_i \leq ((n+m)D)^{2^{cir(n+m)}} \quad \textit{for } i = 1, \dots, \rho,$$

where $c > 0$ is a universal constant.

Proof. If $i = 0$ the bound follows from Proposition 1 applied to $I = (\mathbf{g})$ and $I_0 = \sqrt{I}$ in the polynomial ring $\mathbb{C}[\mathbf{x}, \mathbf{u}]$: we have that $I_0^{\deg(\mathbf{g})^{n+m}} \subset (\mathbf{g})$ and then, $\varepsilon_0 \leq D^{n+m}$.

Now, fix an index $i = 1, \dots, \rho$. From Definition 11, it follows that I_i is contained in $\sqrt{(\mathbf{g}_{i-1}, \widetilde{\mathbf{g}}_{i-1})} \subset \mathbb{C}[\mathbf{x}, \mathbf{u}, \dot{\mathbf{u}}]$. Thus, applying Proposition 1 to the ideal $I = (\mathbf{g}_{i-1}, \widetilde{\mathbf{g}}_{i-1})$, with the estimations of Lemma 13, we conclude that $I_i^\varepsilon \subset (\mathbf{g}_{i-1}, \widetilde{\mathbf{g}}_{i-1})$ for $\varepsilon := (((n+m)D)^{2^{cir(n+m)}})^{n+2m} = ((n+m)D)^{(n+2m)2^{cir(n+m)}}$, since in this case $r > 0$ and then $\nu = r$.

The proposition follows from the fact that $(\mathbf{g}_{i-1}, \widetilde{\mathbf{g}}_{i-1}) \subset (\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}_{i-1}, \dot{\mathbf{g}}_{i-1})$ changing the constant c by another one c' such that the inequality $(n+2m)2^{cir(n+m)} \leq 2^{c' ir(n+m)}$ holds for any n, m. ■

4.2. Going back to the original system

We follow the notations and keep the hypotheses of the previous section.

The aim of this section is to prove the main Theorem 7, roughly speaking, an upper bound for the number of derivations needed to obtain a representation of 1 as an element of the differential ideal $[\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}]$ introduced in formula (4).

Let $\mathbf{g}_i$, $i = 0, \dots, \rho$, be the polynomials in $\mathbb{C}[\mathbf{x}, \mathbf{u}]$ introduced in Lemma 13. From Proposition 12, the differential Nullstellensatz asserts that $1 \in [\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}_i]$ for $i = 0, \dots, \rho$. Thus for each i there exists a non negative integer k (depending on i) such that $1 \in ((\dot{\mathbf{x}} - \mathbf{f})^{[k]}, \mathbf{g}_i^{[k]}) \subseteq \mathbb{C}[\mathbf{x}^{[k+1]}, \mathbf{u}^{[k]}]$.

For $i = 0, \dots, \rho$, we define:

$$k_i := \min\{k \in \mathbb{N}_0 : 1 \in ((\dot{\mathbf{x}} - \mathbf{f})^{[k]}, \mathbf{g}_i^{[k]})\}. \tag{9}$$

Observe that, since $(\mathbf{g}_i) = I_i \subset I_{i+1} = (\mathbf{g}_{i+1})$, the sequence k_i is decreasing and that Proposition 12 ensures that $k_\rho \leq 1$.

The following key lemma allows us to bound recursively each k_{i-1} in terms of k_i with the help of the sequence ε_i introduced in Definition 14:

Lemma 16. *Suppose that the finite sequence k_i introduced in (9) is not identically zero and let $\mu := \max\{0 \leq i \leq \rho : k_i \neq 0\}$. Then:*

1. *the inequality $k_{i-1} \leq 1 + \varepsilon_i k_i$ holds for every $1 \leq i \leq \mu$.*

2. $k_\mu = 1$ *and* $k_i = 0$ *for every* $i > \mu$.
3. $k_0 \le (\mu + 1)\prod_{i=1}^{\mu} \varepsilon_i$.

Proof. Obviously, $k_i = 0$ for all $i > \mu$ from the definition of μ.

Consider now $1 \le i \le \mu + 1$. From Definition 14, any $g \in I_i = (\mathbf{g}_i)$ satisfies

$$g^{\varepsilon_i} \in (\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}_{i-1}, \dot{\mathbf{g}}_{i-1}). \tag{10}$$

For any $j \ge 1$, if we differentiate $j\varepsilon_i$ times the polynomial g^{ε_i}, by means of Leibniz's Formula, we have

$$(g^{\varepsilon_i})^{(j\varepsilon_i)} = \sum_{r_1+r_2+\cdots r_{\varepsilon_i}=j\varepsilon_i} \binom{j\varepsilon_i}{r_1 \ldots r_{\varepsilon_i}} g^{(r_1)} \ldots g^{(r_{\varepsilon_i})},$$

where $r_1, \ldots, r_{\varepsilon_i}$ are nonnegative integers and $\binom{j\varepsilon_i}{r_1 \ldots r_{\varepsilon_i}} := \frac{(j\varepsilon_i)!}{r_1! \ldots r_{\varepsilon_i}!}$. In the formula above, the term with $r_1 = \cdots = r_{\varepsilon_i} = j$ equals $\frac{(j\varepsilon_i)!}{(j!)^{\varepsilon_i}}(g^{(j)})^{\varepsilon_i}$ and, since the sum of all the r_l, with $l = 1, \ldots, \varepsilon_i$, must be $j\varepsilon_i$, in all the other terms there is at least one $g^{(r_l)}$ with $r_l < j$. Thus, for every $j = 0, \ldots, k_i$, there exist polynomials $p_{j,0}, \ldots, p_{j,j-1}$, such that the equality

$$(g^{\varepsilon_i})^{(j\varepsilon_i)} = \frac{(j\varepsilon_i)!}{(j!)^{\varepsilon_i}} (g^{(j)})^{\epsilon_i} + \sum_{l=0}^{j-1} p_{j,l}\, g^{(l)}$$

holds; moreover, from (10), by differentiating $j\varepsilon_i$ times we deduce that

$$\frac{(j\varepsilon_i)!}{(j!)^{\varepsilon_i}} (g^{(j)})^{\varepsilon_i} + \sum_{l=0}^{j-1} p_{j,l}\, g^{(l)} \in ((\dot{\mathbf{x}} - \mathbf{f})^{[j\varepsilon_i]}, \mathbf{g}_{i-1}^{[1+j\varepsilon_i]}).$$

From these relations we deduce recursively that a common zero of the polynomials $(\dot{\mathbf{x}}-\mathbf{f})^{[k_i\varepsilon_i]}$ and $\mathbf{g}_{i-1}^{[1+k_i\varepsilon_i]}$ is also a zero of the polynomials $g, \dot{g}, \ldots, g^{(k_i)}$ for every $g \in I_i = (\mathbf{g}_i)$; in particular, it is a common zero of $(\dot{\mathbf{x}} - \mathbf{f})^{[k_i]}, \mathbf{g}_i^{[k_i]}$ (recall that, by definition, ε_i is at least 1 and then $k_i\varepsilon_i \ge k_i$ for all i). This contradicts the definition of k_i (see (9)).

Therefore, $1 \in ((\dot{\mathbf{x}} - \mathbf{f})^{[k_i\varepsilon_i]}, \mathbf{g}_{i-1}^{[1+k_i\varepsilon_i]})$ and then, $k_{i-1} \le 1 + k_i\varepsilon_i$, which proves the first part of the lemma.

In particular, if $\mu < \rho$, taking $i = \mu + 1$ in the previous inequality, we have $0 < k_\mu \le 1 + k_{\mu+1}\varepsilon_{\mu+1} = 1$, hence $k_\mu = 1$. In the case $\mu = \rho$, Proposition 12 implies that $k_\rho \le 1$ and then, since k_μ is assumed nonzero, we have $k_\mu = k_\rho = 1$. This proves the second assertion.

Finally, the last statement is an easy consequence of the previous ones: it follows from the fact that $k_\mu = 1$, applying recursively the inequality $k_{i-1} \le 1 + k_i\varepsilon_i$ for $i = \mu, \mu - 1, \ldots, 1$. ■

We are now ready to prove Theorem 7 stated at the beginning of this subsection as a corollary of the previous lemma and its proof:

Proof of Theorem 7. We must estimate an upper bound for the minimum integer L such that

$$1 \in ((\dot{\mathbf{x}} - \mathbf{f})^{[L]}, \mathbf{g}^{[L]}).$$

By Definition 14 the inclusion $(\mathbf{g}_0)^{\varepsilon_0} \subseteq (\mathbf{g})$ holds. We can repeat the same argument as in the proof of Lemma 16 and prove that, for any $g \in (\mathbf{g}_0) = I_0 = \sqrt{(\mathbf{g})}$ and for $j = 0, \ldots, k_0$, there exist polynomials $p_{j,0}, \ldots, p_{j,j-1}$ such that

$$(g^{\varepsilon_0})^{(j\varepsilon_0)} = \frac{(j\varepsilon_0)!}{(j!)^{\varepsilon_0}} (g^{(j)})^{\varepsilon_0} + \sum_{l=0}^{j-1} p_{j,l}\, g^{(l)} \in (\mathbf{g}^{[j\varepsilon_0]}).$$

As before, this implies that a common zero of the polynomials $(\dot{\mathbf{x}} - \mathbf{f})^{[k_0\varepsilon_0]}$ and $\mathbf{g}^{[k_0\varepsilon_0]}$ is also a zero of $g, \ldots, g^{(k_0)}$ for an arbitrary element $g \in (\mathbf{g}_0)$; in particular, taking into account that $\varepsilon_0 \ge 1$, it follows

Please cite this article in press as: L. D'Alfonso, et al., Effective differential Nullstellensatz for ordinary DAE systems with constant coefficients, Journal of Complexity (2014), http://dx.doi.org/10.1016/j.jco.2014.01.001

that it is a common zero of $(\dot{\mathbf{x}} - \mathbf{f})^{[k_0]}$, $\mathbf{g}_0^{[k_0]}$, contradicting the definition of k_0 (see (9)). We conclude then that

$$1 \in ((\dot{\mathbf{x}} - \mathbf{f})^{[k_0\varepsilon_0]}, \mathbf{g}^{[k_0\varepsilon_0]}).$$

Thus, the inequality $L \leq k_0\varepsilon_0$ holds.

If $r = 0$, from Proposition 6, we have that $k_0 = 1$ and then, from Proposition 15, $L \leq \varepsilon_0 \leq D^{n+m}$. On the other hand, if $r > 0$, from Proposition 15 and Lemma 16, taking into account that $\mu \leq r$, we have that there is a constant c such that

$$\begin{aligned} L &\leq k_0\varepsilon_0 \leq D^{n+m}(\mu+1)\prod_{i=1}^{\mu}((n+m)D)^{2^{cir(n+m)}} \\ &= (\mu+1)((n+m)D)^{\sum_{i=0}^{\mu} 2^{cir(n+m)}} \\ &\leq (\mu+1)((n+m)D)^{2^{1+c\mu r(n+m)}} \\ &\leq (r+1)((n+m)D)^{2^{1+cr^2(n+m)}}. \end{aligned}$$

The desired bound follows taking a new constant c', in such a way that the inequality $(r+1)((n+m)D)^{2^{1+cr^2(n+m)}} \leq ((n+m)D)^{2^{c'r^2(n+m)}}$ holds. Finally, since $\nu = \max\{1, r\}$, it is easy to see that D^{n+m} and $((n+m)D)^{2^{c'r^2(n+m)}}$ are both bounded by $((n+m)D)^{2^{c''\nu^2(n+m)}}$ for a suitable universal constant $c'' > 0$.

The converse is obvious. ■

As we have observed in the previous proof, if we assume $r = 0$ (i.e. the algebraic constraint $\mathbf{g} = 0$ of the DAE system (4) defines a 0-dimensional algebraic variety in $\mathbb{C}^{n+m}$), the constant L can be bounded directly by ε_0. This estimation is optimal for this kind of DAE systems as it is shown by the following example extracted from [5, Example 5]:

Example 17. In the DAE system (4) suppose $n = 1$, $\mathbf{x} = x_1$, $\mathbf{u} = u_1, \ldots, u_m$, $\mathbf{f} = 1$, and $\mathbf{g}(\mathbf{x}, \mathbf{u}) = u_m - x_1^2, u_{m-1} - u_m^2, \ldots, u_1 - u_2^2, u_1^2$.
As it is shown in [5, Example 5], this system has no solutions and $1 \in ((\dot{\mathbf{x}} - \mathbf{f})^{[L]}, \mathbf{g}^{[L]})$ if and only if $L \geq 2^{m+1}$. On the other hand, the inequality $\varepsilon_0 \leq 2^{m+1}$ holds from Proposition 1. Hence $\varepsilon_0 = 2^{m+1}$ and the upper bound is reached.

5. The general case

The well-known method of reducing the order of a system of differential equations will enable us to apply the results of the previous section to the general case.

Let $\mathbf{x} = x_1, \ldots, x_n$ and $\mathbf{f} = f_1, \ldots, f_s$ be differential polynomials in $\mathbb{C}[\mathbf{x}, \ldots, \mathbf{x}^{(e)}]$, with $e \geq 1$. We consider the differential system

$$\begin{cases} f_1(\mathbf{x}, \ldots, \mathbf{x}^{(e)}) = 0 \\ \vdots \\ f_s(\mathbf{x}, \ldots, \mathbf{x}^{(e)}) = 0. \end{cases} \tag{11}$$

Theorem 7 yields the following:

Theorem 18. *Let $\mathbf{x} = x_1, \ldots, x_n$ and $\mathbf{f} = f_1, \ldots, f_s$ be differential polynomials in $\mathbb{C}[\mathbf{x}, \ldots, \mathbf{x}^{(e)}]$. Let $V \subset \mathbb{C}^{n(e+1)}$ be the algebraic variety defined by $\{\mathbf{f} = 0\}$, and let $\nu := \max\{1, \dim(V)\}$ and $D := \max\{\deg(\mathbf{g}), \deg(V)\}$. Then*

$$1 \in [\mathbf{f}] \iff 1 \in (\mathbf{f}, \ldots, \mathbf{f}^{(L)})$$

where $L \leq (n(e+1)D)^{2^{c\nu^2 n(e+1)}}$ for a universal constant $c > 0$.

Proof. As usual, the introduction of the new variables $z_{i,j} := x_i^{(j)}$, for $i = 1, \ldots, n$ and $j = 0, \ldots, e$, and $\mathbf{z}_j = z_{1,j}, \ldots, z_{n,j}$, allows us to transform the implicit system (11) into the following first order system with a set of polynomial constraints:

$$\begin{cases} \dot{\mathbf{z}}_0 = \mathbf{z}_1 \\ \vdots \\ \dot{\mathbf{z}}_{e-1} = \mathbf{z}_e \\ \bar{\mathbf{f}} = 0 \end{cases} \tag{12}$$

where $\bar{\mathbf{f}} = f_1(\mathbf{z}_0, \dots, \mathbf{z}_e), \dots, f_s(\mathbf{z}_0, \dots, \mathbf{z}_e)$. It is clear that

$$1 \in [\mathbf{f}] \iff 1 \in [\dot{\mathbf{z}}_0 - \mathbf{z}_1, \dots, \dot{\mathbf{z}}_{e-1} - \mathbf{z}_e, \bar{\mathbf{f}}].$$

The differential part of the system (12) is given by an ODE consisting of ne equations in $n(e+1)$ variables and the constraints are given by polynomials in $n(e+1)$ variables, that is, $\bar{\mathbf{f}} \in \mathbb{C}[\mathbf{z}_0, \dots, \mathbf{z}_e]$. Then, Theorem 7 applied to this system implies that

$$1 \in [\dot{\mathbf{z}}_0 - \mathbf{z}_1, \dots, \dot{\mathbf{z}}_{e-1} - \mathbf{z}_e, \bar{\mathbf{f}}] \iff 1 \in ((\dot{\mathbf{z}}_0 - \mathbf{z}_1)^{[L]}, \dots, (\dot{\mathbf{z}}_{e-1} - \mathbf{z}_e)^{[L]}, \bar{\mathbf{f}}^{[L]})$$

where $L \le (n(e+1)D)^{2^{c\nu^2(n(e+1))}}$, with $c > 0$ a universal constant. Going back to the original variables, replacing $z_{i,j}^{(k)}$ by $x_i^{(j+k)}$ for $i = 1, \dots, n$, $j = 0, \dots, e$ and $k = 0, \dots, L$, we get that

$$1 \in [\mathbf{f}] \iff 1 \in (\mathbf{f}, \dots, \mathbf{f}^{(L)})$$

and the theorem follows. ■

Applying the trivial bound $\dim(V) \le n(e+1)$ and Bézout's inequality, which implies that $\deg(V) \le d^{n(e+1)}$, we deduce the following purely syntactic upper bound for the order in the differential Nullstellensatz:

Corollary 19. *Let $\mathbf{f} \subset \mathbb{C}\{\mathbf{x}\}$ be a finite set of differential polynomials in the variables $\mathbf{x} = x_1, \dots, x_n$, whose degrees and orders are bounded by d and e respectively. Then,*

$$1 \in [\mathbf{f}] \iff 1 \in (\mathbf{f}, \dots, \mathbf{f}^{(L)})$$

where $L \le (n(e+1)d)^{2^{c(n(e+1))^3}}$ for a universal constant $c > 0$. ■

Now, once the order is bounded, as a straightforward consequence of the classical effective Nullstellensatz (see for instance [10, Theorem 1.1]), we can estimate the degrees of the polynomials involved in the representation of 1 as an element of the ideal $[\mathbf{f}]$.

Corollary 20. *Let $\mathbf{f} = \{f_1, \dots, f_s\} \subset \mathbb{C}\{\mathbf{x}\}$ be a finite set of differential polynomials in the variables $\mathbf{x} = x_1, \dots, x_n$, whose degrees and orders are bounded by d and e respectively. Let $\epsilon := \max\{2, e\}$. Then $1 \in [\,\mathbf{f}\,]$ if, and only if, there exist polynomials $p_{ij} \in \mathbb{C}[\mathbf{x}^{[\epsilon+L]}]$ such that $1 = \sum_{i=1}^{s} \sum_{j=0}^{L} p_{ij} f_i^{(j)}$, where*

$$L \le (n\epsilon d)^{2^{c(n\epsilon)^3}} \quad \text{and} \quad \deg(p_{ij} f_i^{(j)}) \le d^{(n\epsilon d)^{2^{c(n\epsilon)^3}}},$$

for a universal constant $c > 0$.

Proof. This corollary is an immediate consequence of the result in [10, Theorem 1.1] applied to the polynomials $\mathbf{f}^{[L]}$ of Corollary 19, once we notice that all the polynomials $\mathbf{f}^{[L]}$ have degree bounded by d, since differentiation does not increase the degree, and that $N := n(e+L+1)$ is the number of variables used. Thus $\deg(p_{ij} f_i^{(j)}) \le 2d^N$, and we only need to change the constant c for a new constant $c' > 0$ such that $(n(e+1)d)^{2^{c(n(e+1))^3}} \le (n\epsilon d)^{2^{c'(n\epsilon)^3}}$ and, for $d \ge 2$, $2d^{n(e+(n(e+1)d)^{2^{c(n(e+1))^3}}+1)} \le d^{(n\epsilon d)^{2^{c'(n\epsilon)^3}}}$. For $d = 1$, we can take $p_{ij} \in \mathbb{C}$ and so, the degree upper bound also holds. ■

We remark that Corollary 20 allows us to construct an algorithm which decides if an ordinary DAE system $\mathbf{f} = 0$ over $\mathbb{C}$ has a solution or not. It suffices to consider the coefficients of the polynomials p_{ij} as indeterminates (finitely many, since orders and degrees are bounded *a priori*) and obtain them by solving a non homogeneous linear system over $\mathbb{C}$. It is easy to see that the complexity of this procedure becomes triply exponential in the parameters n and e. Another algorithm of the same hierarchy of complexity (i.e. triply exponential) can be deduced as a particular case of the quantifier elimination method of ordinary differential equations proposed by D. Grigoriev in [6].

In the usual way, we can deduce an effective strong differential Nullstellensatz from Corollary 19 and the well-known Rabinowitsch trick:

Corollary 21. *Let* $\mathbf{f} \subset \mathbb{C}\{\mathbf{x}\}$ *be a finite set of differential polynomials in the variables* $\mathbf{x} = x_1, \ldots, x_n$. *Suppose that* $f \in \mathbb{C}\{\mathbf{x}\}$ *is a differential polynomial such that every solution of the differential system* $\mathbf{f} = 0$ *is a solution of the differential equation* $f = 0$. *Let* $d := \max\{\deg(\mathbf{f}), \deg(f)\}$ *and* $\epsilon := \max\{2, \mathrm{ord}(\mathbf{f}), \mathrm{ord}(f)\}$. *Then* $f^M \in (\mathbf{f}^{[L]}) \subset [\,\mathbf{f}\,]$ *where* $M = d^{n(\epsilon+L+1)}$ *and* $L \leq (n\epsilon d)^{2^{c(n\epsilon)^3}}$ *for a universal constant* $c > 0$.

Proof. We start with the Rabinowitsch trick: since every solution of the system $\mathbf{f} = 0$ is a solution of $f = 0$, if we introduce a new differential variable y, the differential system $\mathbf{f} = 0$, $1 - yf = 0$ has no solution. Hence, 1 belongs to the differential ideal $[\mathbf{f}, 1 - yf] \subseteq \mathbb{C}\{\mathbf{x}, y\}$.

Therefore, Corollary 19 implies that 1 belongs to the polynomial ideal $(\mathbf{f}^{[L]}, (1 - yf)^{[L]})$, with $L \leq ((n+1)(\epsilon+1)(d+1))^{2^{c((n+1)(\epsilon+1))^3}} \leq (n\epsilon d)^{2^{c'(n\epsilon)^3}}$, for suitable universal constants $c, c' > 0$. Taking any representation of 1 as a linear combination of the generators $\mathbf{f}^{[L]}, (1 - yf)^{[L]}$ with polynomial coefficients and replacing each variable $y^{(i)}$ by the corresponding $(f^{-1})^{(i)}$ for $0 \leq i \leq L$, we deduce that a suitable power of f belongs to the polynomial ideal $(\mathbf{f}^{[L]})$ or, equivalently, $f \in \sqrt{(\mathbf{f}^{[L]})}$ in the polynomial ring $\mathbb{C}[\mathbf{x}^{[\epsilon+L]}]$.

Now, applying [10, Theorem 1.3] stated in Proposition 1, we conclude that $f^{d^N} \in (\mathbf{f}^{[L]})$ for $N := n(\epsilon + L + 1)$, the number of variables of the ground polynomial ring $\mathbb{C}[\mathbf{x}^{[\epsilon+L]}]$, and the corollary is proved. ■

With the same notation and assumptions as in Corollary 21, we can obtain upper bounds for the degrees of the polynomials involved in a representation of a power of f as an element of the differential ideal $[\mathbf{f}]$. Applying [13, Corollary 1.7], we have that, if $\mathbf{f} = f_1, \ldots, f_s$ are differential polynomials of *degrees at least* 3, there are polynomials $p_{ij} \in \mathbb{C}[\mathbf{x}^{[\epsilon+L]}]$ such that $f^M = \sum_{i=1}^{s} \sum_{j=0}^{L} p_{ij} f_i^{(j)}$ with $\deg(p_{ij} f_i^{(j)}) \leq (1 + d)M$, where $M = d^{n(\epsilon+L+1)}$. For differential polynomials with *arbitrary degrees*, following the proof of the first part of Corollary 21 and taking into account the bounds in Corollary 20, we get a representation $f^{\widetilde{M}} = \sum_{i=1}^{s} \sum_{j=0}^{L} \widetilde{p}_{ij} f_i^{(j)}$, where $\widetilde{M} = 2(L + 1)d^{n(\epsilon+L+1)+1} \leq d^{(n\epsilon d)^{2^{c(n\epsilon)^3}}}$, with $\deg(\widetilde{p}_{ij}) \leq d^{(n\epsilon d)^{2^{c(n\epsilon)^3}}}$ for a suitable universal constant $c > 0$.

6. The case of an arbitrary field of constants

In the previous sections the assumption of taking the complex numbers as the ground field is only essential in the proof of Lemma 9 because the Implicit Function Theorem is applied. Even if the statement of this lemma makes sense in any field, we are not able to prove it in the more general case of any field of constants. However, it is not difficult to prove that if K is an arbitrary field of characteristic 0 (with the trivial derivation) the following analogue of Theorem 7 remains true for K. More precisely:

Theorem 22. *Let* K *be an arbitrary field of characteristic* 0 *with the trivial derivation,* $\mathbf{x} = x_1, \ldots, x_n$ *and* $\mathbf{u} = u_1, \ldots, u_m$ *differential variables over* K, $\mathbf{f} = f_1, \ldots, f_n$ *and* $\mathbf{g} = g_1, \ldots, g_s$ *polynomials in* $K[\mathbf{x}, \mathbf{u}]$. *If* $d > 0$ *is an upper bound for the degrees of* $\mathbf{f}$ *and* $\mathbf{g}$ *we have:*

$$1 \in [\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}] \subseteq K\{\mathbf{x}, \mathbf{u}\} \iff 1 \in (\dot{\mathbf{x}} - \mathbf{f}, \ldots, \mathbf{x}^{(L+1)} - \mathbf{f}^{(L)}, \mathbf{g}, \ldots, \mathbf{g}^{(L)}),$$

where $L \leq ((n + m)d)^{2^{c(n+m)^3}}$ *for a suitable universal constant* $c > 0$.

Proof. We prove only the non trivial implication. Suppose that

$$1 \in [\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}] \subseteq K\{\mathbf{x}, \mathbf{u}\}$$

holds. Let $\mathbf{k} \subseteq K$ be the subfield of K which is generated over $\mathbb{Q}$ by the coefficients of the finitely many polynomials involved in a decomposition of 1 as an element of the ideal $[\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}]$. Obviously, we have $1 \in [\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}]$ in the differential ring $\mathbf{k}\{\mathbf{x}, \mathbf{u}\}$.

Since $\mathbf{k}$ is a finitely generated extension of $\mathbb{Q}$ and $\mathbb{C}$ is algebraically closed having infinite transcendence degree over $\mathbb{Q}$, there exists a field $\mathbb{Q}$-embedding $\sigma : \mathbf{k} \to \mathbb{C}$. This morphism can be extended to an embedding of the ring $\mathbf{k}\{\mathbf{x}, \mathbf{u}\}$ into $\mathbb{C}\{\mathbf{x}, \mathbf{u}\}$, simply by applying σ to the coefficients of the polynomials. Moreover, by considering $\mathbf{k}$ and $\mathbb{C}$ as fields of constants, σ defines a monomorphism of differential rings. In particular, the condition $1 \in [\dot{\mathbf{x}} - \mathbf{f}, \mathbf{g}] \subseteq \mathbf{k}\{\mathbf{x}, \mathbf{u}\}$ implies that $1 \in [\dot{\mathbf{x}} - \sigma(\mathbf{f}), \sigma(\mathbf{g})] \subseteq \sigma(\mathbf{k})\{\mathbf{x}, \mathbf{u}\} \subseteq \mathbb{C}\{\mathbf{x}, \mathbf{u}\}$.

Now, applying Theorem 7 to the polynomials $\sigma(\mathbf{f}), \sigma(\mathbf{g})$ we conclude that the relation

$$1 \in (\dot{\mathbf{x}} - \sigma(\mathbf{f}), \dots, \mathbf{x}^{(L+1)} - \sigma(\mathbf{f})^{(L)}, \sigma(\mathbf{g}), \dots, \sigma(\mathbf{g})^{(L)}) \tag{13}$$

holds in an algebraic polynomial ring $\mathbb{C}[\mathbf{x}^{[L+1]}, \mathbf{u}^{[L]}]$ with $L \leq ((n+m)D)^{2^{c\nu^2(n+m)}}$, where D is the degree of the variety $V \subset \mathbb{C}^{n+m}$ defined by $\sigma(\mathbf{g})$ and $\nu := \max\{1, \dim(V)\}$. Using Bézout's inequality we may replace D by d^{n+m} and then, changing the constant c if necessary, we may suppose $L \leq ((n+m)d)^{2^{c(n+m)^3}}$. Moreover, we can also replace $\mathbb{C}$ by the subfield $\sigma(\mathbf{k})$, because the coefficients of the polynomial combination underlying (13) may be chosen as solutions of a linear system with coefficients in that field. The theorem follows by taking σ^{-1} in that polynomial relation. ■

Using Theorem 22 we can replace $\mathbb{C}$ by an arbitrary base field of constants K of characteristic 0 and the results in Corollaries 19–21 of Section 5 remain true: the general version of Corollary 19 follows by a standard reduction to a first order system as in the proof of Theorem 18 and replacing the bound for the order L in Theorem 7 by the one in Theorem 22. The proofs of Corollaries 20 and 21 rely on the bound stated in Corollary 19 and on known results that hold over any field of characteristic 0.

Acknowledgments

The authors thank Michael Wibmer (RWTH Aachen University) for pointing out a way of extending the results from the field of complex numbers to an arbitrary field of constants of characteristic zero.

References

[1] C. Berenstein, D. Struppa, Recent improvements in the complexity of the effective Nullstellensatz, Linear Algebra Appl. 157 (1991) 203–215.
[2] R. Cohn, On the analogue for differential equations of the Hilbert–Netto theorem, Bull. Amer. Math. Soc. 47 (4) (1941) 268–270.
[3] T. Dubé, The structure of polynomial ideals and Gröbner bases, SIAM J. Comput. 19 (4) (1990) 750–775.
[4] M. Giusti, Some effectivity problems in polynomial ideal theory, in: EUROSAM 84 (Cambridge, 1984), in: Lecture Notes in Comput. Sci., vol. 174, Springer, Berlin, 1984, pp. 159–171.
[5] O. Golubitsky, M. Kondratieva, A. Ovchinnikov, A. Szanto, A bound for orders in differential Nullstellensatz, J. Algebra 322 (11) (2009) 3852–3877.
[6] D. Grigoriev, Complexity of quantifier elimination in the theory of ordinary differential equations, in: EUROCAL '87 (Leipzig, 1987), in: Lecture Notes in Comput. Sci., vol. 378, Springer, Berlin, 1989, pp. 11–25.
[7] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, Theoret. Comput. Sci. 24 (3) (1983) 239–277.
[8] J. Heintz, C. Schnorr, Testing polynomials which are easy to compute, in: Logic and Algorithmic (Zurich, 1980), in: Monograph. Enseign. Math., vol. 30, Univ. Genève, 1982, pp. 237–254.
[9] G. Hermann, Die Frage der endlich vielen Schritte in der theorie der polynomideale, Math. Ann. 95 (1926) 736–788.
[10] Z. Jelonek, On the effective Nullstellensatz, Invent. Math. 162 (1) (2005) 1–17.
[11] W. Johnson, The curious history of Faà di Bruno's formula, Amer. Math. Monthly 109 (3) (2002) 217–234.
[12] E. Kolchin, Differential Algebra and Algebraic Groups, Academic Press, New York, 1973.
[13] J. Kollár, Sharp effective Nullstellensatz, J. Amer. Math. Soc. 1 (4) (1988) 963–975.
[14] T. Krick, A. Logar, An algorithm for the computation of the radical of an ideal in the ring of polynomials, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (New Orleans, LA, 1991), in: Lecture Notes in Comput. Sci., vol. 539, Springer, Berlin, 1991, pp. 195–205.
[15] T. Krick, A. Logar, Membership problem, representation problem and the computation of the radical for one-dimensional ideals, in: Effective Methods in Algebraic Geometry (Castiglioncello, 1990), in: Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 203–216.
[16] L. Kronecker, Grundzüge einer arithmetischen theorie der algebraischen Grössen, J. Reine Angew. Math. 92 (1882) 1–123.
[17] S. Laplagne, An algorithm for the computation of the radical of an ideal, in: ISSAC 2006, ACM, New York, 2006, pp. 191–195.

[18] H. Matsumura, Commutative Algebra, second ed., The Benjamin/Cummings Publ. Company, 1980.
[19] M. Möller, F. Mora, Upper and lower bounds for the degree of Groebner bases, in: EUROSAM 84 (Cambridge, 1984), in: Lecture Notes in Comput. Sci., vol. 174, Springer, Berlin, 1984, pp. 172–183.
[20] H. Raudenbush, Ideal theory and algebraic differential equations, Trans. Amer. Math. Soc. 36 (1934) 361–368.
[21] J. Ritt, Differential Equations from the Algebraic Standpoint, in: Amer. Math. Soc. Colloq. Publ., vol. XIV, New York, 1932.
[22] A. Seidenberg, Some basic theorems in differential algebra (characteristic p arbitrary), Trans. Amer. Math. Soc. 73 (1952) 174–190.
[23] A. Seidenberg, An elimination theory for differential algebra, Univ. Calif. Publ. Math. (N.S.) 3 (1956) 31–65.