Some Finiteness Issues in Differential Algebraic Systems Theory

Krister Forsman and Mats Jirstrand
Department of Electrical Engineering
Linköping University
S-581 83 Linköping
Sweden

email: {krister,matsj}@isy.liu.se

1994-02-24

REGLERTEKNIK

AUTOMATIC CONTROL

LINKÖPING

Some Finiteness Issues in Differential Algebraic Systems Theory

Krister Forsman and Mats Jirstrand
Department of Electrical Engineering, Linköping University
S-581 83 Linköping, Sweden
email: {krister,matsj}@isy.liu.se

Abstract. The elimination problem in differential algebraic systems theory is discussed. The focus is on finiteness questions, such as conditions for the elimination ideal to be finitely generated.

Keywords: nonlinear systems, differential algebra, elimination

1 Introduction

In this paper a few algorithmic problems relating to differential algebraic systems theory are addressed. We will point out some problems arising as one treats systems of polynomial differential equations using the language of differential algebra. In particular we will see what happens when we search for the input-output equations, which are possible to derive from the original system. Most of the problems are related to computational difficulties, e.g. the existence of a finite set of differential equations describing the system.

Differential algebra made its way into systems theory via the discoveries of Michel Fliess in the mid 80's and has now grown quite extensive. A very good survey is given in [3]. Several authors have studied how the algorithms of differential algebra, mostly elimination theory, can be used in systems theory. Let us here mention [1, 7, 8, 14, 19].

The paper is organized as follows: section 2 presents an example which serves as a background for later sections. Sections 3 and 4 display some properties of this example, which are probably rather surprising and counter-intuitive to the non-expert. Section 5, 6 and 7 explain how most of the problems that arose can be resolved. Section 8 describes some problems that are still open, and section 9 summarizes the results of the paper.

1.1 Basic Definitions and Notation

We suppose that the reader is familiar with some basic concepts from commutative and differential algebra, such as ring, ideal, prime ideal and characteristic sets. Some references are [11, 12, 21, 22]. Here follow a few definitions and theorems we use.

k denotes an arbitrary field of characteristic zero.

The ring of polynomials in the variables $x_1, \ldots, x_n$ with coefficients from k is written $k[x_1, \ldots, x_n]$.

The ideal generated by a set P of polynomials is denoted $\langle P \rangle$.

The ring of differential polynomials in the differential indeterminates $x_1, \ldots, x_n$ is denoted $k\{x_1, \ldots, x_n\}$.

We will consider variables which are time dependent and denote derivation with respect to time with a dot or $\frac{d}{dt}$. Higher order derivatives is denoted with superscripts within parentheses in the usual way, i.e.

$$x,\, \dot{x},\, \ddot{x},\, x^{(3)},\, x^{(4)},\, \ldots$$

The *leader* of a differential polynomial is the highest ranked derivative that appears in the differential polynomial. The *initial* I_g of a differential polynomial g is the (polynomial) coefficient of the highest power of the leader and the *separant* S_g of a differential polynomial g is the partial derivative of g w.r.t. the leader.

If $H_{\mathbf{A}}$ is a differential polynomial the ideal $[\mathbf{A}] : H_{\mathbf{A}}^{\infty}$ is defined by

$$[\mathbf{A}] : H_{\mathbf{A}}^{\infty} \;=\; \{f \;:\; H_{\mathbf{A}}^{r} f \in [\mathbf{A}] \;\mathit{for\ some}\; r \in \mathbb{N}\}. \tag{1}$$

This notation, which is rather unfortunate from commutative algebraic point of view, stems from differential algebra [11, 21].

Consider the class of systems that can be represented by a classical state space description:

$$\begin{aligned} \dot{x}_1 &= f_1(\bar{x}, u) \\ &\vdots \\ \dot{x}_n &= f_n(\bar{x}, u) \\ y &= h(\bar{x}, u), \end{aligned} \tag{2}$$

where $\bar{x} = (x_1, \ldots, x_n)$ and $f_1, \ldots, f_n, h \in k[x_1, \ldots, x_n, u]$, i.e. all nonlinearities are polynomial. If we allow derivatives of the input in the right hand sides, as is often done in differential algebraic systems theory, nothing will change for the issues discussed in this paper.

To a given state space description (2) we associate a differential ideal

$$\Sigma \;:=\; [\dot{x}_1 - f_1, \ldots, \dot{x}_n - f_n, \, y - h], \tag{3}$$

called the *state space differential ideal* of system (2).

Our main question is: which differential equations in y and u only that belong to Σ? I.e. which input-output equations can we derive from the state space description (2). Mathematically speaking this means that we look for the differential ideal

$$\Sigma^c \;:=\; \Sigma \cap k\{u, y\} \tag{4}$$

2 An Interesting Example

We now consider an example of a system whose input-output ideal Σ^c has some interesting properties. The system is:

$$\dot{x}_1 = x_1 x_2, \quad \dot{x}_2 = 0, \quad y = x_1 \tag{5}$$

The equations can be seen as a state space description of all systems, which is described by a linear, first order differential equation with constant coefficient.

The equations generate the following differential ideal

$$\Sigma \;=\; [\dot{x}_1 - x_1 x_2, \dot{x}_2, y - x_1] \tag{6}$$

which we now will study more in detail.

In the ideal Σ we are especially interested in the equations that only involve y and its derivatives, since these describe the output behaviour of the system. In other words: what does Σ^c look like? If we denote $y = y_0, \dot{y} = y_1, \ddot{y} = y_2$, *etc.* we get

$$y_0 = x_1, \quad y_1 = \dot{x}_1 = x_1 x_2, \quad y_2 = \dot{x}_1 x_2 + x_1 \dot{x}_2 = x_1 x_2^2.$$

Eliminating x_1 and x_2 from these gives

$$p := y_2 y_0 - y_1^2 = 0 \tag{7}$$

Clearly it is not possible to construct a differential polynomial in the variable y of lower order than this from the above equations. This means that there are no differential polynomials of lower order than p in Σ^c.

We can now pose a variety of interesting questions concerning the differential ideal description of the above system, such as

- Is $[p] = \Sigma^c$? In that case we have a simple description of the system, namely one differential equation $p = 0$.
- How is Σ^c generated? We will see that Σ^c in this example is not even (differentially) finitely generated despite the fact that Σ is generated by a finite set.

We will also see that Σ^c is a prime ideal. Naturally one may ask the question:

- Is $[p]$ prime? The answer is negative and hence $\Sigma^c \neq [p]$, which answers the first question.

3 The Differential Ideal $[y_0 y_2 - y_1^2]$ is Not Prime

In section 6 we show that the differential ideal Σ can be considered as a non-differential graph ideal. This implies that Σ is prime and hence Σ^c is prime too.

We use the convenient notation $y_i := y^{(i)}$. Let $p := y_0 y_2 - y_1^2$ as in the previous section and consider the differential ideal $P := [p]$.

The polynomial p has a special property that we are going to exploit. The following definitions come from [11].

Definition 3.1 Let $M \in k\{y\}$ be a differential monomial.Then, $M = y_{\mu_1}^{\nu_1} y_{\mu_2}^{\nu_2} \ldots y_{\mu_m}^{\nu_m}$ is said to have *weight* $wt(M) = \sum_{i=1}^{m} \mu_i \nu_i$. □

Definition 3.2 A differential polynomial p in one variable is said to be *isobaric* of weight w if all its monomials have the same weight w. We then use the notation $wt(p) = w$. □

Lemma 3.1 *The derivative $\dot{p}$ of an isobaric polynomial p is isobaric and $wt(\dot{p}) = wt(p) + 1$*

Proof. See [9]. □

Lemma 3.2 *Let f and g be isobaric polynomials, then fg is isobaric with weight $wt(f) + wt(g)$.*

Proof. See [9]. □

The differential ideal $[y_0y_2 - y_1^2]$ is generated by the isobaric polynomial $p := y_0y_2 - y_1^2$. The isobaric property of p can help us solve the membership problem for such an ideal. Let $P_j = \langle\, p, \dot{p}, \ldots, p^{(j)}\,\rangle$ in $k[y_0, \ldots, y_{wt(p)+j}]$.

Theorem 3.1 *Let $P = [p] \subset k\{y\}$, where p is isobaric of weight $wt(p)$ and $f \in k\{y\}$. If the monomials of f have weight less than or equal to w then*

$$f \in P \quad \Leftrightarrow \quad f \in P_{w-wt(p)}.$$

Proof. See [9]. □

Let $f := y_1y_3 - y_2^2,\ \ g := y_1$ and $p := y_0y_2 - y_1^2$. With aid of the above theorem we can show that $fg = y_1^2y_3 - y_1y_2^2 \in P$ but $f \notin P$ and $g \notin P$. Hence $P = [p]$ is not prime!

We know that Σ^c is prime but $[p]$ is not and hence $\Sigma^c \neq [p]$.

4 Σ^c Does Not Have to Be Finitely Generated

In this section we will show the somewhat surprising result that there are systems described by the finitely generated differential ideal Σ that have a Σ^c which is not (differentially) finitely generated. The combinatorial techniques employed in this section are not entirely different from those in [15, 16].

As before we consider the differential ideal

$$\Sigma := [\dot{x}_1 - x_1x_2, \dot{x}_2, y_0 - x_1].$$

If we differentiate the last generator w.r.t. time and substitute $\dot{x}_1$ and $\dot{x}_2$ by the first two equations or equivalently use the Lie-derivative we get $y_1 = x_1x_2$. Repeating this a number of times results in the expression $y_k := x_1x_2^k$. This expression can now be used to determine if a polynomial $f \in k\{y\}$ is a member of Σ^c. Since the elements in Σ^c is formed by elimination in the differential ideal Σ, which includes the elements $y_k - x_1x_2^k$ the substitution $y_k = x_1x_2^k$ in an element of Σ^c must yield zero.

We will now study how an arbitrary element of Σ^c can be constructed.

Definition 4.1 A monomial $M \in k[y_0, y_1, \ldots]$ is said to be of *type* (i, j), where $i = \mathrm{tdeg}\,(M)$ is the total degree and $j = wt(M)$ is the weight of M. □

By the notation $\mathrm{tdeg}\,(M)$ we here mean the sum of the powers of all variables in M.

Lemma 4.1 *Let $M \in k[y_0, y_1, \ldots]$ be a monomial and type$(M) = (i, j)$. Then $M = x_1^i x_2^j$ under the substitution rule $y_k = x_1x_2^k$.*

Proof. See [9]. □

The lemma tells us that monomials of the same type in $k[y_0, y_1, \ldots]$ will be reduced to the same monomial in $k[x_1, x_2]$ under the substitution $y_k = x_1x_2^k$.

Let $f \in \Sigma^c$. A consequence of the discussion just before definition 4.1 and of lemma 4.1 is that the coefficients of monomials of same type in f have to sum up to zero.

We now generalize these thoughts. Every polynomial in $k[y_0, y_1, \ldots]$ can be written as a sum of homogeneous polynomials, i.e. polynomials the monomials of which are of the same total degree. Further, every polynomial can be divided into isobaric polynomials. These two observations implies that we always have the following composition of a polynomial $P \in k[y_0, y_1, \ldots]$

$$P = \sum_{i=0}^{N} \sum_{j=0}^{L_i} P_i^j, \tag{8}$$

where N is the largest total degree of a monomial in P and L_i is the highest weight of any of the monomials in P_i^j. Further, $\operatorname{tdeg}(P_i^j) = i$, P_i^j are isobaric of weight j and $P_i^j = \sum_{k=1}^{S_{ij}} \alpha_k^{ij} M_k^{ij}$,where $M_k^{ij}, k = 1, \ldots, S_{ij}$ are monomials of type (i, j) and $\alpha_k^{ij} \in k$.

From the above discussion we know that $P \in \Sigma^c$ if and only if $\sum_{k=1}^{S_{ij}} \alpha_k^{ij} = 0$.

We now concentrate on the pieces P_i^j in which we can divide P if $P \in \Sigma^c$. Which monomials can then P_i^j be built of? The following theorem gives us the answer:

Theorem 4.1

$$P \in \Sigma^c \iff P = \sum_{i=2}^{N} \sum_{j=2}^{L} P_i^j,$$

where P_i^j is a linear combination of the isobaric polynomials

$$q_k^{ij} = y_0 \ldots y_0 y_j - y_{l_1} y_{l_2} \ldots y_{l_i},$$

where $\sum_{r=1}^{i} l_r = j$ and N is the largest total degree of any monomial in P. The index k is an enumeration of the possible l_i-tuples $(l_1, \ldots, l_i)$, where $l_1 \leq \ldots \leq l_i$.

The polynomials q_k^{ij} can be considered as base vectors in a vector space and the coefficients α_k^{ij} as coordinates.

Lemma 4.2 *Let $\mathcal{S} = \{p \in k[y_0, y_1, \ldots] : p = \sum_{i=1}^{N} \alpha_i f_i,\ \alpha_i \in k,\ f_i \in k[y_0, y_1, \ldots]\}$. Then,*

$$\langle\, \mathcal{S} \,\rangle = \langle\, f_1, \ldots, f_N \,\rangle.$$

Proof. See [9]. □

If we allow derivation of the elements in $\mathcal{S}$ as well one can show that $[\mathcal{S}] = [f_1, \ldots, f_N]$ in a similar way.

We can now attack the original question: Is Σ^c (differentially) finitely generated? The answer is negative despite the fact that Σ is!

Theorem 4.2 *Let $\Sigma = [\dot{x}_1 - x_1 x_2, \dot{x}_2, y - x_1]$. The ideal $\Sigma^c = \Sigma \cap k\{y\}$ is not finitely generated.*

Proof. We introduce the notation

$$\Sigma^c_{wt \leq L} = \{P \in \Sigma^c : \textit{The monomials } M \textit{ of } P \textit{ have } wt(M) \leq L\}. \tag{9}$$

Suppose that Σ^c is finitely generated. This means that there are polynomials $g_1, \ldots, g_K \in \Sigma^c$ such that $\Sigma^c = [g_1, \ldots, g_K]$. Since K is finite there is a monomial in one of the generators which has higher or equal weight as all the other monomials of the generators.This means that $\{g_1, \ldots, g_K\} \in \Sigma^c_{wt \leq L}$ if L is chosen big enough.

We have that $\Sigma^c_{wt\leq L} \subset \Sigma^c$ which implies $[\Sigma^c_{wt\leq L}] \subseteq \Sigma^c$. If we for every fixed L are able to construct a polynomial g with the properties $g \in \Sigma^c$ but $g \notin [\Sigma^c_{wt\leq L}]$ then Σ^c has to be non finitely generated. We claim that

$$f_{L+1} := y_{\frac{L-1}{2}} y_{\frac{L+3}{2}} - y^2_{\frac{L+1}{2}}, \quad L \; odd \;\; \in \Sigma^c \; but \; f_{L+1} \notin [\Sigma^c_{wt\leq L}], \tag{10}$$

i.e. f_{L+1} is the kind of polynomial we are searching for.

By theorem 4.1 we know that an element in $\Sigma^c_{wt\leq L}$ always can be written on the form $P = \sum_{r=1}^{M} \gamma_r f_r$ since

$$P = \sum_{i=2}^{N} \sum_{j=2}^{L} P_i^j = \sum_{i=2}^{N} \sum_{j=2}^{L} \sum_{k=1}^{S_{ij}} \alpha_k^{ij} q_k^{ij} =: \sum_{r=1}^{M} \gamma_r f_r, \tag{11}$$

where γ_r are all the α_k^{ij} and f_r are all the q_k^{ij}.

By the differential variant of lemma 4.2 we have that $[\Sigma^c_{wt\leq L}] = [f_1, \ldots, f_N]$, i.e. $[\Sigma^c_{wt\leq L}]$ is finitely generated of the isobaric polynomials $f_r := q_k^{ij}$ of weight equal to or less than L.

We now know that

$$\Sigma^c_{wt\leq L} = [y_0y_2 - y_1^2, \ldots, y_0y_L - y_1y_{L-1}, \ldots, y_0y_L - y_{\frac{L-1}{2}} y_{\frac{L+1}{2}}, y_0y_0y_2 - y_0y_1^2, \ldots], \tag{12}$$

where the last dots denote a finite number of generators of total degree higher than or equal to three. This differential ideal can be viewed as an non finitely generated ideal where the generators are the above generators and their derivatives.

We observe that the total degree of a generator remains constant as one differentiate it. This means that if $f_{L+1} \in [\Sigma^c_{wt\leq L}]$ then it has to be constructed of generators of total degree two and their derivatives.

Since f_{L+1} is an isobaric polynomial of weight $L+1$ and all the generators are isobaric, f_{L+1} has to be constructed of generators of weight $L+1$. The only polynomials which can be used to construct f_{L+1} is the first derivative of the generators of weight L, i.e.

$$\frac{d}{dt}(y_0y_L - y_jy_{L-j}) = y_0y_{L+1} + y_1y_L - y_jy_{L-j+1} - y_{j+1}y_{L-j}, \tag{13}$$

where $j = 1, 2, \ldots, \frac{L-1}{2}$ and L is odd. The polynomial f_{L+1} has to be a linear combination over k of these derivatives since this is the only construction that keeps the weight and total degree constant. It is easy to show that this is not the case and thus $f_{L+1} \notin [\Sigma^c_{wt\leq L}]$, which completes the proof. $\square$

5 Chains of Graph Ideals

When we want to apply some non-differential algebraic results, such as Gröbner bases to state space differential ideals in differential rings, we have to develop some preliminary results concerning rings of infinitely many variables.

Definition 5.1 A *graph ideal* is an ideal of the form

$$\langle z_1 - f_1, \ldots, z_s - f_s \rangle,$$

where z_i are variables and $f_i \in k[x_1, \ldots, x_n]$. $\square$

The usefulness of graph-ideals is to study relations of dependency between $f_1, \ldots, f_s$, which are supposed to be known. By dependency we mean *algebraic dependency.* The polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ is said to be algebraically dependent if there is a non-zero $P \in k[z_1, \ldots, z_m]$ such that $P(f_1, \ldots, f_m) = 0$. The relations can be found by using e.g. Gröbner bases and elimination theory. An alternative to this appraoch is suggested in [18].

We will now consider chains of graph ideals and will therefore need a notation for rings of variable size. Let

$$R_j := k[x_1, \ldots, x_n, z_1, \ldots, z_j], \tag{14}$$

(where n is fixed) and

$$G_j := \{z_1 - f_1, \ldots, z_j - f_j\}, \tag{15}$$

where as before z_i are variables and $f_1, \ldots, f_j \in k[x_1, \ldots, x_n]$.

Definition 5.2 Let $I_{j,N}$ be the graph ideal generated by G_j in R_N, i.e.

$$I_{j,N} := \{f \in R_N : f = \sum_{\alpha \in R_N, p \in G_j} \alpha p\}.$$

$\square$

Lemma 5.1 *Let $p = p(x_1, \ldots, x_n, z_1, \ldots, z_N) \in R_N$, then*

$$p \in I_{j,N} \iff p(x_1, \ldots, x_n, f_1, \ldots, f_j, z_{j+1}, \ldots, z_N) = 0.$$

Proof. There is a special representation of polynomials in R_N, from which the lemma immediately follows.

Consider the polynomial $h(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0$ and make the substitution $x \to x + c$ in h. We get

$$h(x + c) = \alpha(x)x + h(c). \tag{16}$$

This is easily generalized to polynomials in several variables, i.e. if $h \in k[x_1, \ldots, x_n]$ then

$$h(x_1 + c_1, \ldots, x_n + c_n) = \alpha_1(x_1, \ldots, x_n)x_1 + \ldots + \alpha_n(x_n)x_n + h(x_1, \ldots, x_n), \tag{17}$$

or in a slightly more compact form:

$$h(x_1 + c_1, \ldots, x_n + c_n) = q(x_1, \ldots, x_n) + h(c_1, \ldots, c_n), \tag{18}$$

where $q \in \langle x_1, \ldots, x_n \rangle$.

Take a polynomial $p \in R_N$ and observe that the identity $z_i = (z_i - f_i) + f_i$ is a composition of the above form. If we now use what we just have shown we can rewrite p in the following manner

$$p(x_1, \ldots, x_n, z_1, \ldots, z_N) = p(x_1, \ldots, x_n, (z_1 - f_1) + f_1, \ldots, (z_j - f_j) + f_j, z_{j+1}, \ldots, z_N) =$$

$$q(x_1,\ldots,x_n,z_1,\ldots,z_N)+p(x_1,\,\ldots,\,x_n,\,f_1,\,\ldots,\,f_j,\,z_{j+1},\ldots,z_N),$$

where $q \in I_{j,N} = \langle\, z_1 - f_1,\ldots,z_j - f_j\,\rangle$. From this representation it immediately follows that

$$p \in I_{j,N} \quad \Leftrightarrow \quad p(x_1,\ldots,x_n,f_1,\ldots,f_j,z_{j+1},\ldots,z_N) = 0.$$

□

Lemma 5.2 *Let $I_{j,N}$ be the graph ideal defined in definition 5.2, then*

i) $I_{j,N}$ is a prime ideal.

ii) $I_{j,N} \cap k[x_1,\ldots,x_n] = 0$.

iii) For all j,s,N where $j \le s \le N$ we have that

$$I_{N,N} \cap k[z_1,\,\ldots,\,z_j] \;=\; I_{s,N} \cap k[z_1,\,\ldots,\,z_j].$$

Proof. We start by showing that $I_{j,N}$ is a prime ideal.

Suppose that $fg \in I_{j,N}$. We know, by lemma 5.1 that this is equivalent to

$$f(x_1,\,\ldots,\,x_n,\,f_1,\,\ldots,\,f_j,z_{j+1},\ldots,z_N)g(x_1,\,\ldots,\,x_n,f_1,\,\ldots,\,f_j,z_{j+1},\ldots,z_N) \;=\; 0. \tag{19}$$

Now both $f(x_1,\ldots,x_n,f_1,\ldots,f_j,z_{j+1},\ldots,z_N)$ and $g(x_1,\ldots,x_n,f_1,\ldots,f_j,z_{j+1},\ldots,z_N)$ are polynomials in the ring $k[x_1,\ldots,x_n,z_{j+1},\ldots,z_N]$, since $f_i \in k[x_1,\ldots,x_n]$. The product of two polynomials cannot be zero unless one of them are zero. This forces at least one of $f(x_1,\ldots,x_n,f_1,\ldots,f_j,z_{j+1},\ldots,z_N)$ or $g(x_1,\ldots,x_n,f_1,\ldots,f_j,z_{j+1},\ldots,z_N)$ to be zero, i.e. at least one of f or g belongs to $I_{j,N}$ according to lemma 5.1. This shows that $I_{j,N}$ is prime.

Suppose that $p \in I_{j,N}$. According to lemma 5.1 this is equivalent to

$$p(x_1,\,\ldots,\,x_n,\,f_1,\,\ldots,\,f_j,\,z_{j+1},\ldots,z_N) \;=\; 0 \tag{20}$$

If in addition $p \in k[x_1,\ldots,x_n]$ then $p = q(x_1,\ldots,x_n)$ and

$$0 = p(x_1,\,\ldots,\,x_n,\,f_1,\ldots,f_j,z_{j+1},\ldots,z_N) = q(x_1,\ldots,x_n) \tag{21}$$

This shows that p has to be the zeropolynomial. Thus we have shown

$$I_{j,N} \cap k[x_1,\ldots,x_n] = 0$$

We have that $I_{s,N} \subseteq I_{N,N}$ and hence

$$I_{s,N} \cap k[z_1,\ldots,z_j] \subseteq I_{N,N} \cap k[z_1,\ldots,z_j] \tag{22}$$

Now suppose $p \in I_{N,N} \cap k[z_1,\ldots,z_j]$ but $p \notin I_{s,N} \cap k[z_1,\ldots,z_j]$.
The assumptions give

$$p \in k[z_1,\,\ldots,\,z_j] \quad \Rightarrow \quad p(x_1,\,\ldots,\,x_n,\,z_1,\,\ldots,\,z_N) = q(z_1,\,\ldots,\,z_j) \tag{23}$$

and

$$p \in I_{N,N} \iff p(x_1,\,\dots,\,x_n,\,f_1,\dots,f_j,\dots,f_N) = 0. \tag{24}$$

Together this leads to $p(x_1,\,\dots,\,x_n,f_1,\dots,f_j,\dots,f_N) = q(f_1,\,\dots,\,f_j) = 0$.

Next we notice that

$$p \notin I_{s,N} \iff 0 \neq p(x_1,\,\dots,\,x_n,f_1,\dots,f_j,\dots,f_s,z_{s+1},\dots,z_N) = q(f_1,\dots,f_j). \tag{25}$$

This is a contradiction and hence the last part of the lemma follows. □

Remark: Part *i)* and *ii)* of the above lemma can be proved very elegantly using a little more abstract reasoning: Consider the quotient ring $R_N/I_{j,N}$. Obviously we have that

$$R_N/I_{j,N} \simeq k[x_1,\,\dots,\,x_n,\,z_{j+1},\,\dots,\,z_N] \tag{26}$$

i.e. the quotient ring is the *free* polynomial ring in the variables

$$x_1,\,\dots,\,x_n,\,z_{j+1},\,\dots,\,z_N \tag{27}$$

So in particular it is an integral domain, so $I_{j,N}$ is prime. Since the quotient ring is free claim *ii)* follows. The authors have not found an equally elegant proof of claim *iii)*.

The concept of graph ideals is very useful when considering differential ideals as (3), i.e. differential ideals generated by the state equations. These differential ideals can be considered as graph ideals in infinitely many variables.

6 Truncations of Graph Ideals

The question now is if we can get a grip on differential ideals with non differential tools? One way is to consider only the elements of a differential ideal up to a certain order, which we will call the truncation of that differential ideal.

Our main interest will be in differential ideals of one variable y and truncations of those differential ideals, i.e. subsets of elements up to a certain order. We will use the notation y_i for the variable representing the ith derivative of y and $y_0 = y$.

Definition 6.1 The *Lie-derivative operator* is defined by

$$L_f = \sum_{i=1}^{n} f_i \frac{\partial}{\partial x_i} + \sum_{i=1}^{\infty} u^{(i)} \frac{\partial}{\partial u^{(i-1)}}.$$

□

All derivatives of y can be obtained by repeated use of the Lie-derivative operator and the result is a function of the state variables and u and its derivatives.

Definition 6.2 Let $h_j = L_f^j h(\bar{x},\bar{u})$, where $\bar{x} = (x_1,\,\dots,\,x_n)$ and $\bar{u} = (u_0,\dots,u_N)$, i.e. u and its N first derivatives. We define the graph ideal

$$\mathcal{O}_j := \langle\, y_0 - h_0(\bar{x},\bar{u}),\dots,y_j - h_j(\bar{x},\bar{u})\,\rangle \subseteq k[y_0,\dots,y_j,\bar{x},\bar{u}]$$

□

Theorem 6.1 *$\mathcal{O}_n \cap k[y_0, \ldots, y_n, \bar{u}]$ contains an input-output equation for (2).*

Proof. See [4] or [5]. □

The input-output equation is easily found by using Gröbner bases and elimination theory.

How much information does one get about the truncated differential ideal $\Sigma^c \cap k[y_0, \ldots, y_j, \bar{u}]$ by considering truncations of the graph ideal $\mathcal{O}_j$?

Theorem 6.2 *We have that $\Sigma^c \cap k[y_0, \ldots, y_j] = \mathcal{O}_j \cap k[y_0, \ldots, y_j]$.*

Proof. By changing point of view we can consider a differential ring as a ring of infinitely many variables, i.e.

$$k\{x_1, \ldots, x_n, y\} \to k[x_1, \ldots, x_n, y, \dot{x}_1, \ldots, \dot{x}_n, \dot{y}, \ldots],$$

where the superscripts together with the subscripts are now nothing more than labels for the variables. A finitely generated differential ideal as $[A, B, C]$ then becomes

$$\langle A, \dot{A}, \ldots, B, \dot{B}, \ldots, C, \dot{C}, \ldots \rangle \tag{28}$$

i.e. an infinitely generated ideal.

Consider the differential ideal $\Sigma = [\dot{x}_1 - f_1, \ldots, \dot{x}_n - f_n, y - h]$. If we now rename the variables according to

$$z_0 = y_0, \ldots, z_j = y_j, \tag{29}$$

$$z_{j+1} = \dot{x}_1, \ldots, z_{j+n} = \dot{x}_n, \quad z_{j+1+n} = y_{j+1}, \tag{30}$$

$$z_{j+2+n} = \ddot{x}_1, \ldots, z_{j+1+2n} = \ddot{x}_n, \quad z_{j+2+2n} = y_{j+2}, \ldots \tag{31}$$

we get the ideal

$$\langle z_0 - h_0, \ldots, z_j - h_j, z_{j+1} - f_1, \ldots, z_{j+n} - f_n, \ldots \rangle \tag{32}$$

This is a graph ideal of infinitely many z_i. Since the proofs in section 5 are completely independent of the number N of the variables z_i, lemma 5.1 and 5.2 are true even when $N = \infty$.

With the non-differential description of Σ it now follows from *iii*) of lemma 5.2 that

$$\begin{gathered}\langle z_0 - h_0, \ldots, z_j - h_j, z_{j+1} - f_1, \ldots \rangle \cap k[z_0, \ldots, z_j] = \\ \langle z_0 - h_0, \ldots, z_j - h_j \rangle \cap k[z_0, \ldots, z_j]\end{gathered} \tag{33}$$

or in the old names of the variables

$$\Sigma \cap k[y_0, \ldots, y_j] = \langle y_0 - h_0, \ldots, y_j - h_j \rangle \cap k[y_0, \ldots, y_j] \tag{34}$$

that is

$$\Sigma^c \cap k[y_0, \ldots, y_j] = \mathcal{O}_j \cap k[y_0, \ldots, y_j]$$

which completes the proof. □

Note that the input u does not appear anywhere in the proof. The theorem holds equally well if we adjoin u and its derivatives to k, i.e. if we let $k\langle u \rangle$ be the field of coefficients instead of k.

Another way of computing $\Sigma^c \cap k[y_0, \ldots, y_j]$ is provided by theorem 7.3.

7 Description of Σ^c with Characteristic Sets

In section 3 we showed that if p is a polynomial of lowest order in Σ^c then in general $\Sigma^c \neq [p]$. An interesting question now is: Are there cases when we have equality and in that case which conditions do we then have to pose on p?

Consider a system described by state space equations of the form (2) but without an input, i.e. $u = 0$. This equations corresponds to the differential ideal

$$\Sigma := [\dot{x}_1 - f_1(\bar{x}), \ldots, \dot{x}_n - f_n(\bar{x}), y - h(x)] \subseteq k\{x_1, \ldots, x_n, y\} \tag{35}$$

We now want to know which differential equations the output y satisfies, i.e. we are interested in $\Sigma^c := \Sigma \cap k\{y\}$. We are especially interested in the differential equation of lowest order $p = 0$ that y satisfies.

The differential polynomial p can be found using a method built on Gröbner bases presented in [4]. It can also be showed that when the process stops we get one polynomial, which is unique.

This polynomial p has some interesting properties. Since $p \in \Sigma$ is the polynomial of lowest order in the single variable y in Σ it is also of lowest order in Σ^c. Now Σ^c is a set of differential ideals in one variable and because p is a polynomial of lowest order it has to be a characteristic set of Σ^c (two differential polynomials in one variable cannot be reduced w.r.t. each other so the characteristic set has only one element).

Theorem 7.1 *If* $\mathbf{A}$ *is a characteristic set of a prime differential ideal* I *then* $I = [\mathbf{A}] : H_{\mathbf{A}}^{\infty}$.

Proof. See [11]. □

From the preceding chapters we now that Σ can be interpreted as a graph ideal and hence is a prime differential ideal. That Σ is prime implies that Σ^c is prime. We have the characteristic set $\{p\}$ of the prime differential ideal Σ^c and consequently the theorem gives

$$\Sigma^c = [p] : H_p^{\infty} \tag{36}$$

We notice that since $p \in \Sigma^c$ we have that

$$[p] \subseteq \Sigma^c \tag{37}$$

and from the expressions (36) and (37) we get the following limits on Σ^c:

$$[p] \subseteq \Sigma^c = [p] : H_p^{\infty} \tag{38}$$

We will now examine the relationship between $[p]$ and the differential ideal $[p] : H_p^{\infty}$.

If $f \in [p]$ then $f = fH_p^0 \in [p]$ which shows that

$$[p] \subseteq [p] : H_p^{\infty} \tag{39}$$

Suppose that $[p]$ is prime and that $\{p\}$ is a characteristic set of $[p]$. Let $f \in [p] : H_p^{\infty}$, then $fH_p^r \in [p]$ for some r. Since $[p]$ is prime either f or H_p^r has to be in $[p]$. According to the definition of H_p it has lower order than p. Since $\{p\}$ is a characteristic set of $[p]$ there are no element of lower order than p in $[p]$, hence $H_p \notin [p]$. The product $H_p^2 = H_pH_p \notin [p]$, since

$[p]$ is prime and none of the factors of H_p^2 are in $[p]$. By induction one realizes that $H_p^r \notin [p]$. Thus we have a product $f H_p^r \in [p]$, where the factor $H_p^r \notin [p]$. Since $[p]$ is prime then f has to be in $[p]$. Thus we have showed that if p is the characteristic set of the prime differential ideal $[p]$ then

$$[p] : H_p^\infty \subseteq [p] \tag{40}$$

Combining the inclusions (39) and (40) gives the equality

$$[p] = [p] : H_p^\infty, \tag{41}$$

when p is the characteristic set of the prime differential ideal $[p]$. This discussion is in fact the proof of theorem 7.1 in the case when the characteristic set consist of only one element.

We now observe the fact that since $\{p\}$ is a characteristic set of Σ^c it is also a characteristic set of $[p]$, since $[p] \subseteq \Sigma^c$.

Notice that if $\Sigma^c = [p]$ then $[p]$ have to be prime since Σ^c is prime. The discussion above is summed up in the following theorem:

Theorem 7.2 *If $p \in k\{y\}$ is the polynomial of lowest order in Σ^c then*

$$[p] \textit{ is prime} \iff \Sigma^c = [p]$$

Despite this characterization of Σ^c it can be of limited use, since it can be a very difficult task to decide if $[p]$ is prime or not. There is one case when it is easy, namely if the initial I_p and separant S_p of p belong to k. Then $H_p \in k$ and $[p] = [p] : H_p$, which is prime.

We also note that Σ^c can be finitely generated without being equal to $[p]$. An example is provided by

$$[\, y_1^2 - y_0 \,] : y_1 = [\, y_1^2 - y_0,\, 2y_2 - 1 \,] \tag{42}$$

The ideal $[y_1^2 - y_0]$ has a simple interpretation in mechanics and it has also been discussed by Pommaret [20].

We conclude with an alternative theorem describing the structure of the ideal Σ^c. This theorem is merely a reformulation of a well known result by Ritt.

Theorem 7.3 *Let $p \in K\{y\}$ be a differential polynomial of differential order γ in y and H the product of the separant and initial of p. Then for all i we have that*

$$\Sigma^c \cap K[y_0, \ldots, y_i] = \langle\, p, \partial p, \ldots, \partial^{i-\gamma} p \,\rangle : H^\infty$$

Here $\partial = \frac{d}{dt}$.

Proof. Let $f \in K\{y\}$. According to [21, p. 115] we have that

$$\mathrm{prem}(f, p) = 0 \iff f \in [p] : H^\infty \tag{43}$$

where $\mathrm{prem}(f,p)$ denotes the pseudo-remainder of f w.r.t. p. Ritt and Kolchin use the term remainder, but this terminology seems a little old-fashioned; cf. [10]. But the way the pseudo-remainder is constructed we realize that (43) is equivalent to

$$f \in [p] : H^\infty \iff f \in \langle\, p, \partial p, \ldots, \partial^{i-\gamma} p \,\rangle : H^\infty \tag{44}$$

which proves the theorem. □

To do calculations in ideals of the type $I : H^\infty$ one uses the so called Rabinovich trick. More about this can be found in e.g. [6].

8 Extensions

The results were obtained by examining a system written in polynomial state space form without an input. It would be interesting to examine the possibility to construct an example with nonzero input, which has similar consequences as the one treated. The input-output differential ideal $\Sigma^c \in k\{u, y\}$ is then a differential ideal in two variables.

How "bad" can the ideal $[p]$ behave? Are there examples of systems, where $[p]$ is not even a radical differential ideal? If this is the case, then there are elements in the ideal with the property $f \notin [p]$ but $f^r \in [p]$ for some r. Translated into differential equations this means that $[p]$ only contains the differential equation $f^r = 0, r > 1$ and not the simpler description $f = 0$. A candidate of a non-radical ideal is $P := [y_1^2 - y_0]$. It can be shown that $y_3^2 \in P$. To show that P is not radical, one have to show that $y_3 \notin P$.

The differential ideal $[y_0 y_2 - y_1]$ considered as an ideal in infinitely many variables has some similarities with a graph ideal. Is it prime? If this is the case we have an example of a prime differential ideal generated by a single differential polynomial whose initial and separant are nontrivial.

To use the method of Gröbner bases in differential algebraic calculations we had to interpret the differential algebraic problem in algebraic terms. This interpretation is possible due to the fact that we found a restriction of the problem to a ring of finitely many variables. In the general case this is not trivial or even possible, since there are differential ideals, which is not (differential) finitely generated as in section 4. An interesting subject is the concept of differential Gröbner bases. Some references on this topic are [2],[13] and [17].

9 Conclusions

We have considered systems described by polynomial differential equations, i.e.

$$\begin{aligned} \dot{x}_1 - f_1(\bar{x}, u) &= 0 \\ &\vdots \\ \dot{x}_n - f_n(\bar{x}, u) &= 0 \\ y - h(\bar{x}, u) &= 0, \end{aligned} \tag{45}$$

where $\bar{x} = x_1, \ldots, x_n$ are the state variables, u is the input, y is the output and $f_1, \ldots, f_n$ are polynomials. In the language of differential algebra we can formulate this system description as a differential ideal generated by the left hand sides of (45), i.e.

$$[\dot{x}_1 - f_1, \ldots, \dot{x}_n - f_n, y - h].$$

We have studied the set $\Sigma^c = \Sigma \cap k\{u, y\}$, i.e. all input-output differential equations that the systems input and output variables have to satisfy. In particular we have considered the case of no input, that is $\Sigma \subset k\{\bar{x}, y\}$ and $\Sigma^c \subset k\{y\}$, which corresponds to the transient behavior of the system.

There is a method for obtaining the unique input-output equation of lowest order of the system represented by (45). We call the left hand side of this differential equation p. The results are

- $\Sigma^c \neq [p]$ in general
- Σ^c might not even be generated by a finite number of differential polynomials

- $\Sigma^c = [p]$ iff $[p]$ is prime
- Σ^c is always prime but $[p]$ does not have to be prime

These results were obtained by the study of a parameterized version of a first order system, namely

$$\dot{x}_1 - x_1 x_2 = 0, \quad \dot{x}_2 = 0, \quad y - x_1 = 0 \tag{46}$$

so they are not anomalies from some non physical system.

These results shows the fact that despite the structure of the original system of polynomial differential equations is captured in the finitely generated differential ideal Σ we do not have a simple differential algebraic description of the input-output ideal Σ^c other than in special cases. This means that one has to be careful in the study of such ideals and that the ideal description problem for them is highly non-trivial. It is also an indication that it could be more convenient to consider a system as described by solutions (time-trajectories) rather than equations. This is also one of the ideas in the behavioral framework of Willems, see e.g. [23]. There is also a close analogy with the duality between algebraic geometry and commutative algebra, i.e. zero manifolds vs. equations, as in the spirit of [14].

Acknowledgement

This work was financially supported by the Swedish Council for Technical Research (TFR).

References

[1] S. Diop. Elimination in control theory. *Math. Control Signals Systems*, 4(1):17–32, 1991.

[2] G. Carrà Ferro. Gröbner bases and differential algebra. In L. Huguet and A. Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 356 of *Lecture Notes Comp. Sci.*, pages 129–140. Springer, 1989. Proc. AAECC-5, Menorca.

[3] M. Fliess and T. Glad. An algebraic approach to linear and nonlinear control. In H.L. Trentelman and J.C. Willems, editors, *Essays on Control: Perspectives in the Theory and Its Applications*, volume 14 of *Progress in Systems and Control Theory*, pages 223–268. Birkhäuser, 1993. From the 2nd European Control Conf.

[4] K. Forsman. *Constructive Commutative Algebra in Nonlinear Control Theory.* PhD thesis, Dept. of Electrical Engineering, Linköping University, S-581 83 Linköping, Sweden, 1991. Linköping Studies in Science and Technology. Dissertations. No 261.

[5] K. Forsman. Some generic results on algebraic observability and connections with realization theory. In J.W. Nieuwenhuis, C. Praagman, and H.L. Trentelman, editors, *Proc. 2nd European Control Conf.*, volume 3, pages 1185–1190, Groningen, July 1993.

[6] P. Gianni, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. In L. Robbiano, editor, *Computational Aspects of Commutative Algebra*, pages 15–33. Academic Press, 1989. From J. Symbolic Computation Vol. 6, nr. 2-3.

[7] S.T. Glad. Nonlinear state space and input output descriptions using differential polynomials. In J. Descusse et al., editor, *New Trends in Nonlinear Control Theory*, volume 122 of *Lect. Notes Control Inf. Sci.*, pages 182–189. Springer, 1988.

[8] S.T. Glad. Nonlinear regulators and Ritt's remainder algorithm. In *Colloque international sur l'analyse des systèmes dynamiques controllés*, volume 2, July 1990. Lyon, France.

[9] M. Jirstrand. Differential algebraic systems theory – some finiteness problems. Master's thesis, Dept. of Electrical Engineering, Linköping University, S-581 83 Linköping, Sweden, January 1994. LiTH-ISY-EX-1434.

[10] D.E. Knuth. *The Art of Computer Programming. Vol. 2: Seminumerical Algorithms.* Addison-Wesley, second edition, 1981.

[11] E.R. Kolchin. *Differential Algebra and Algebraic Groups.*, volume 54 of *Pure and Applied Mathematics.* Academic Press, 1973.

[12] S. Lang. *Algebra.* Addison-Wesley, second edition, 1984.

[13] E.L. Mansfield. Diffgrob2: A symbolic algebra package for analysing systems of PDE using Maple. Technical report, Department of Mathematics, University of Exeter, Exeter, U.K., 1993.

[14] J. Michalik and J.C. Willems. The elimination problem in differential algebraic systems. In *Proc. MTNS*, Regensburg, Germany, 1993.

[15] K.B. O'Keefe. A property of the differential ideal $[y^p]$. *Trans. Amer. Math. Soc.*, 94:483–497, March 1960.

[16] K.B. O'Keefe. Unusual power products and the ideal $[y^2]$. *Proc. Amer. Math. Soc.*, 17(3):757–758, June 1966.

[17] F. Ollivier. Standard bases of differential ideals. In S. Sakata, editor, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 508 of *Lecture Notes Comp. Sci.*, pages 304–321. Springer, 1990. Proc. AAECC-8, Tokyo.

[18] F. Ollivier. Canonical bases: Relations with standard bases, finiteness conditions and application to tame automorphisms. In T. Mora and C. Traverso, editors, *Effective Methods in Algebraic Geometry*, volume 94 of *Progress in Mathematics*, pages 379–400. Birkhäuser, 1991. From the Symposium MEGA 90, Castiglioncello, Italy, 1990.

[19] F. Ollivier. Generalized standard bases with applications to control. In *Proc. First European Control Conf.*, volume 1, pages 170–176, Grenoble, France, July 1991. Hermès.

[20] J.F. Pommaret. *Differential Galois Theory.* Gordon and Breach, 1983.

[21] J.F. Ritt. *Differential Algebra.* Dover, 1950.

[22] R.Y. Sharp. *Steps in Commutative Algebra*, volume 19 of *London Mathematical Society Student Texts.* Cambridge University Press, 1990.

[23] J.C. Willems. Puzzles and paradigms in the theory of dynamical systems. *IEEE Trans. Aut. Contr.*, AC-36(3):259–294, March 1991.