



**HAL**  
open science

# Computing all identifiable functions of parameters for ODE models

Alexey Ovchinnikov, Anand Pillay, Gleb Pogudin, Thomas Scanlon

► **To cite this version:**

Alexey Ovchinnikov, Anand Pillay, Gleb Pogudin, Thomas Scanlon. Computing all identifiable functions of parameters for ODE models. *Systems and Control Letters*, 2021, 157, pp.105030. 10.1016/j.sysconle.2021.105030 . hal-04460638

**HAL Id: hal-04460638**

**<https://hal.science/hal-04460638v1>**

Submitted on 15 Feb 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Computing all identifiable functions of parameters for ODE models

Alexey Ovchinnikov<sup>a</sup>, Anand Pillay<sup>b</sup>, Gleb Pogudin<sup>c</sup>, Thomas Scanlon<sup>d</sup>

<sup>a</sup>*CUNY Queens College, Department of Mathematics, 65-30 Kissena Blvd, Queens, NY 11367, USA*  
*CUNY Graduate Center, Mathematics and Computer Science, 365 Fifth Avenue, New York, NY 10016, USA*

<sup>b</sup>*University of Notre Dame, Department of Mathematics, Notre Dame, IN 46556, USA*

<sup>c</sup>*LIX, CNRS, École Polytechnique, Institut Polytechnique de Paris, 1 rue Honoré d'Estienne d'Orves, 91120, Palaiseau, France*

<sup>d</sup>*University of California, Berkeley, Department of Mathematics, Evans Hall, Berkeley, CA 94720-3840, USA*

---

## Abstract

Parameter identifiability is a structural property of an ODE model for recovering the values of parameters from the data (i.e., from the input and output variables). This property is a prerequisite for meaningful parameter identification in practice. In the presence of nonidentifiability, it is important to find all functions of the parameters that are identifiable. The existing algorithms check whether a given function of parameters is identifiable or, under the solvability condition, find all identifiable functions. However, this solvability condition is not always satisfied, which presents a challenge. Our first main result is an algorithm that computes all identifiable functions without any additional assumptions, which is the first such algorithm as far as we know. Our second main result concerns the identifiability from multiple experiments (with generically different inputs and initial conditions among the experiments). For this problem, we prove that the set of functions identifiable from multiple experiments is what would actually be computed by input-output equation-based algorithms (whether or not the solvability condition is fulfilled), which was not known before. We give an algorithm that not only finds these functions but also provides an upper bound for the number of experiments to be performed to identify these functions. We provide an implementation of the presented algorithms.

*Keywords:* parameter identifiability, multiple experiments, input-output equations, differential algebra, characteristic sets

---

## 1. Introduction

In this paper, we study structural parameter identifiability of rational ODE systems. Roughly speaking, a parameter is structurally identifiable if its value can be recovered from the observations assuming continuous noise-free measurements and sufficiently exciting inputs (also referred to as the persistence of excitation, see [21, 43]). If not all of the parameters of a model are identifiable, the next question usually is what rational functions  $h(\bar{\mu}) \in \mathbb{C}(\bar{\mu})$  of the parameters  $\bar{\mu}$  are identifiable. The knowledge of identifiable functions can be used in these ways:

- If the functions of interest to the modeler are identifiable, then the lack of identifiability of some parameters is not an issue (sometimes, this is even an advantage [38]).
- Identifiable functions can be used to find an identifiable reparametrization of the model [1, 23, 24], which is a way of improving the model.
- Knowledge of identifiable functions can be used to discover parameter transformations that preserve the input-output behavior and thus could provide additional insights to the modeler (see Section 5.2).

To the best of our knowledge, all existing approaches to computing identifiable functions extract them from the coefficients of input-output equations (going back to [29]; for a concise summary, we refer to [31, Introduction and Algorithm II.1]). To conclude that the coefficients of an input-output equation are identifiable, one can, for example,

---

*Email addresses:* aovchinnikov@qc.cuny.edu (Alexey Ovchinnikov), Anand.Pillay.3@nd.edu (Anand Pillay), gleb.pogudin@polytechnique.edu (Gleb Pogudin), scanlon@math.berkeley.edu (Thomas Scanlon)

<sup>1</sup>During the preparation of this manuscript, G. Pogudin also worked at the Courant Institute of Mathematical Sciences, New York University, New York, NY 10012, USA and at the Higher School of Economics, Faculty of Computer Science, Moscow, 109028, Russia

verify if the solvability condition [35, Remark 3] holds for the equation. The condition can be checked by an algorithm (see [8, Section 4.1] and [28, Section 3.4]) and holds for some classes of models [31]. If the condition does not hold, then this approach of finding identifiable functions of parameters is not applicable but is still used by some of the existing software packages, including DAISY and COMBOS. This is a reason why these tools may miss the non-identifiability of some of the parameters in such systems. For a simple example of a system for which this condition does not hold, see [16, Example 2.14] (see also Sections 5.2 and 5.3).

Therefore, we are not aware of any prior algorithm that can compute all identifiable functions (e.g., by computing generators of the field of identifiable functions). Note that some existing software can, for any fixed rational function of parameters, check whether it is identifiable [32, Remark 1]. However, looking for all identifiable functions, it is not known in advance what functions of parameters to test for identifiability, so this approach cannot be used as an algorithm.

The above issues motivate the following questions (which remained unanswered as far as we know) we study in this paper:

(Q1) How to find the identifiable functions of a model even if the solvability condition does not hold?

(Q2) If the solvability condition does not hold, what is the meaning of the coefficients of the input-output equations?

Our main results are the following answers to these questions:

- We answer (Q1) by providing Algorithm 1 for computing generators of the field of identifiable functions. This is the first such algorithm and is based on our theory established in Theorem 11.
- We show in Theorem 19 that the coefficients of the input-output equations are generators of the field of functions identifiable from multiple experiments (with generically different inputs and initial conditions among the experiments [20]), thus answering (Q2). To the best of our knowledge, this natural interpretation of the coefficients of the input-output equations has not been known before despite the popularity of this method. Furthermore, we use this to derive the first upper bound for the number of such experiments, which can be used further for experimental design (e.g., for protocols such as [10, Section 7]). The multi-experiment setup is natural, for example, for models involving constant inputs [42].

The theoretical basis for this work uses differential algebra and commutative algebra. We employ characteristic sets, a tool from computational algebra. The key difference with the prior algorithms based on characteristic sets is that we provide a mathematically sound way to treat a typically ignored case in which the solvability condition is not satisfied. To achieve this, we analyze the Wronskians of the monomials of characteristic sets using methods from linear algebra. Our results are informed by model theory in the sense of mathematical logic, though this does not appear explicitly in our presentation. We elaborate on this connection in a follow-up work [30]. Additional related results on identifiability using input-output equations and differential algebra include [3, 7, 14, 17, 25–27, 34–36].

The rest of the paper is organized as follows. Section 2 contains definitions and notation that we use. In Section 3, we give our algorithm for computing the generators of the field of identifiable functions, which is based on the theory we present in this section as well. Section 4 is on theory for multi-experimental identifiability. We illustrate our methods with examples in Section 5. We prove our main results in Appendix A. In the other remaining appendices, we present and prove correctness of two algorithms that are used in our main algorithmic contributions and also provide a mathematical discussion, illustrated with examples, on our main theorems.

We have implemented Algorithm 1 and an algorithm for computing the bound from Theorem 19 (as in Remark 23) in Maple. A MAPLE implementation together with the examples from Section 5 is available at <https://github.com/pogudingleb/AllIdentifiableFunctions>. This implementation has recently been incorporated into a freely available web app <https://maple.cloud/app/5710317752942592/SIAN>.

## 2. Basic notions and notation

In this section, we will present the basic notions and notation from differential algebra and parameter identifiability that are essential for our main results.

### 2.1. Background and notation from differential algebra

Differential algebra has been a standard theory behind identifiability, and we will simply fix the basic notation. General references include [19, 33]. For other presentations of these concepts in the context of control theory, see [11,

18, 21, 35].

**Notation 1 (Differential rings and ideals).**

- (a) A *differential ring*  $(R, ')$  is a commutative ring with a derivation  $' : R \rightarrow R$ , that is, a map such that, for all  $a, b \in R$ ,  $(a + b)' = a' + b'$  and  $(ab)' = a'b + ab'$ . A *differential field* is a differential ring that is a field. For  $i > 0$ ,  $a^{(i)}$  denotes the  $i$ -th order derivative of  $a \in R$ .  $\text{Const}(K)$  denotes the field of constants of a differential field  $K$ .
- (b) The *ring of differential polynomials* in the variables  $z_1, \dots, z_n$  over a differential field  $(K, ')$  is the ring

$$K[z_j^{(i)} \mid i \geq 0, 1 \leq j \leq n]$$

with a derivation defined on the ring by  $(z_j^{(i)})' := z_j^{(i+1)}$ . This differential ring is denoted by  $K\{z_1, \dots, z_n\}$ .

- (c) For differential fields  $F \subset L$  and  $a_1, \dots, a_n \in L$ , the smallest differential subfield of  $L$  that contains  $F$  and  $a_1, \dots, a_n$  is denoted by  $F\langle a_1, \dots, a_n \rangle$ .
- (d) For a commutative ring  $R$  and a subset  $F \subset R$ , the smallest ideal containing  $F$  is denoted by  $(F)$ .
- (e) An ideal  $I$  of a differential ring  $(R, ')$  is called a *differential ideal* if, for all  $a \in I$ ,  $a' \in I$ . For  $F \subset R$ , the smallest differential ideal containing  $F$  is denoted by  $[F]$ .
- (f) For an ideal  $I$  and element  $a$  in a ring  $R$ , we denote  $I : a^\infty = \{r \in R \mid \exists n : a^n r \in I\}$ . This set is also an ideal in  $R$ . This will be useful for dealing with ODE systems in which (non-polynomial) rational functions appear.
- (g) For  $a_1, \dots, a_n$  in a differential ring  $R$ , we denote the  $n \times n$  matrix with  $(i, j)$ -entry  $a_j^{(i-1)}$  by  $\text{Wr}(a_1, \dots, a_n)$  and call it the *Wronskian* of  $a_1, \dots, a_n$ . For example,

$$\text{Wr}(a_1, a_2) = \begin{pmatrix} a_1 & a_2 \\ a_1' & a_2' \end{pmatrix}.$$

The rest of the definitions in this section generalize Gaussian elimination to systems of non-linear ODEs. Differential rankings are analogous to ordering of variables in Gaussian elimination; characteristic sets and presentations are analogous to row echelon form and reduced row echelon forms, respectively.

**Definition 2.** A *differential ranking* is a total order  $>$  on  $Z := \{z_j^{(i)} \mid i \geq 0, 1 \leq j \leq n\}$  satisfying:

$$\forall x \in Z \quad x' > x \quad \text{and} \quad \forall x, y \in Z \quad (x > y \implies x' > y').$$

**Notation 3.** For  $f \in K\{z_1, \dots, z_n\} \setminus K$  and a differential ranking,

- $\text{lead}(f)$  is the element of  $\{z_j^{(i)} \mid i \geq 0, 1 \leq j \leq n\}$  of the highest rank appearing in  $f$ . This is partly analogous to the leading variable in Gaussian elimination.
- The leading coefficient of  $f$  viewed as a polynomial in  $\text{lead}(f)$  is called the *initial* of  $f$ . This is similar to the leading coefficient in Gaussian elimination.
- The *separant* of  $f$  is  $\frac{\partial f}{\partial \text{lead}(f)}$ . One can show that it is equal to the leading coefficient of any derivative of  $f$ .
- The *rank* of  $f$  is  $\text{rank}(f) = \text{lead}(f)^{\text{deg}_{\text{lead}(f)} f}$ . The ranks are compared first by lead, and in the case of equality, by deg. This is analogous to the leading variable in Gaussian elimination/leading term in Gröbner bases.
- For  $S \subset K\{z_1, \dots, z_n\} \setminus K$ , the product of initials and separants of  $S$  is denoted by  $H_S$ . This is used in handling division with remainder algebraically.

**Definition 4 (Characteristic sets).**

- For  $f, g \in K\{z_1, \dots, z_n\} \setminus K$ ,  $f$  is said to be *reduced* w.r.t.  $g$  if no proper derivative of  $\text{lead}(g)$  appears in  $f$  and  $\text{deg}_{\text{lead}(g)} f < \text{deg}_{\text{lead}(g)} g$ .
- A subset  $\mathcal{A} \subset K\{z_1, \dots, z_n\} \setminus K$  is called *autoreduced* if, for all  $p \in \mathcal{A}$ ,  $p$  is reduced w.r.t. every element of  $\mathcal{A} \setminus \{p\}$ . Every autoreduced set is finite [19, Section I.9].
- Let  $\mathcal{A} = A_1 < \dots < A_r$  and  $\mathcal{B} = B_1 < \dots < B_s$  be autoreduced sets ordered by their ranks (see Notation 3). We say that  $\mathcal{A} < \mathcal{B}$  if
  - $r > s$  and  $\text{rank}(A_i) = \text{rank}(B_i)$ ,  $1 \leq i \leq s$ , or
  - there exists  $q$  such that  $\text{rank}(A_q) < \text{rank}(B_q)$  and, for all  $i$ ,  $1 \leq i < q$ ,  $\text{rank}(A_i) = \text{rank}(B_i)$ .

- An autoreduced subset of the smallest rank of a differential ideal  $I \subset K\{z_1, \dots, z_n\}$  is called a *characteristic set* of  $I$ . One can show that every non-zero differential ideal in  $K\{z_1, \dots, z_n\}$  has a characteristic set.

**Definition 5 (Characteristic presentation).** (cf. [5, Definition 3]) A polynomial is said to be *monic* if at least one of its coefficients is 1. This is how monic is typically used in identifiability analysis and not how it is used in [5]. A set of polynomials is said to be monic if each polynomial in the set is monic.

Let  $C$  be a monic characteristic set of a prime differential ideal  $P \subset K\{z_1, \dots, z_n\}$ . Let  $N(C)$  denote the set of non-leading variables of  $C$ . Then  $C$  is called a *characteristic presentation* of  $P$  if all initials of  $C$  belong to  $K[N(C)]$  and none of the elements of  $C$  has a factor in  $K[N(C)]$ .

## 2.2. Parameter identifiability for ODE models

Consider an ODE system of the form

$$\Sigma = \begin{cases} \bar{x}' = \bar{f}(\bar{x}, \bar{\mu}, \bar{u}), \\ \bar{y} = \bar{g}(\bar{x}, \bar{\mu}, \bar{u}), \end{cases} \quad (1)$$

where  $\bar{x}$ : a vector of state variables,  $\bar{y}$ : a vector of output variables,  $\bar{\mu}$ : a vector of time-independent parameters,  $\bar{u}$ : a vector of input variables, and  $\bar{f}$  and  $\bar{g}$ : tuples of elements of  $\mathbb{C}(\bar{x}, \bar{\mu}, \bar{u})$ .

Bringing  $\bar{f}$  and  $\bar{g}$  to the common denominator, write  $\bar{f} = \bar{F}/Q$  and  $\bar{g} = \bar{G}/Q$ , for  $F_1, \dots, F_n, G_1, \dots, G_m, Q \in \mathbb{C}[\bar{x}, \bar{\mu}, \bar{u}]$ . Consider the (prime, see [16, Lemma 3.2]) differential ideal

$$I_\Sigma := [Qx'_i - F_i, Qy_j - G_j, 1 \leq i \leq n, 1 \leq j \leq m]: Q^\infty.$$

Note that every solution of (1) is a zero of every element of  $I_\Sigma$ .

**Definition 6 (Generic solution, cf. [12, 13]).** The image of  $(\bar{x}, \bar{y}, \bar{u})$  under the canonical homomorphism

$$\mathbb{C}(\bar{\mu})\{\bar{x}, \bar{y}, \bar{u}\} \rightarrow \mathbb{C}(\bar{\mu})\{\bar{x}, \bar{y}, \bar{u}\}/I_\Sigma$$

is called the *generic solution* of (1).

Rigorously written definitions of identifiability in analytic terms can be found in [31, Definition 1] and [16, Definition 2.5]. [16, Proposition 3.4] implies that the following is an equivalent definition of identifiability, which we will use.

**Definition 7 (Identifiability).** A function  $h \in \mathbb{C}(\bar{\mu})$  is said to be (*single-experiment, or SE-*) *identifiable* for (1) if, for every generic solution  $(\bar{x}^*, \bar{y}^*, \bar{u}^*)$  of (1), we have  $h \in \mathbb{C}\langle \bar{y}^*, \bar{u}^* \rangle$ .

**Definition 8 (Input-output equations, cf. [9, Definition 4.1]).** For a fixed differential ranking  $>$  on  $(\bar{y}, \bar{u})$ , the set of *input-output equations (IO-equations)* of the system  $\Sigma$  from (1) is the characteristic presentation of  $I_\Sigma \cap \mathbb{C}\langle \bar{y}, \bar{u} \rangle$ .

It can be computed by computing the characteristic presentation  $C$  of  $I_\Sigma$  with respect to the differential ranking that is compatible with  $>$  and in which any derivative from  $\bar{x}$  is greater than any derivative from  $(\bar{y}, \bar{u})$ , and returning  $C \cap \mathbb{C}\langle \bar{y}, \bar{u} \rangle$  (e.g., by the Rosenfeld-Gröbner algorithm [6]).

In the Sections 3 and 4, we will present our two main results, Theorem 11 and Theorem 19. The former is the main theoretical ingredient for our Algorithm 1 to find all single-experiment identifiable functions of parameters. The latter is a key to calculating a bound for a sufficient number of experiments to check identifiability of multi-experiment identifiable functions of parameters. Both main results are used in our software implementations referenced in the introduction. We prove our main results in Appendix A.

## 3. Main result: Single-experiment identifiability

In this section, we give an algorithm to compute all functions of the parameters that are identifiable from a single experiment for system (1). We begin with a construction in Section 3.1, which is a refinement of considering Wronskians of monomials (cf. [8, 12, 28, 31]). Using this, we give an algebraic characterization, Theorem 11 (our first main result), of the identifiable functions, which we turn into Algorithm 1. The proof of Theorem 11 can be found in Appendix A.1.

### 3.1. Preparation for Theorem 11

To find the identifiable functions, we will begin with a new construction. Let  $K$  be a differential field and  $k$  a constant subfield such that  $\mathbb{C} \subset k$  and let  $\bar{a} = (a_1, \dots, a_n) \in K^n$ . For  $p \in k\{\bar{z}\}$ , where  $\bar{z} = (z_1, \dots, z_n)$ , such that  $p(\bar{a}) = 0$ , we construct a subfield  $F(p) \subset K$  as follows:

1. Let  $W_p$  denote the Wronskian (see Notation 1(g)) of the monomials of  $p$  evaluated at  $\bar{a}$ .
2. Define  $F(p)$  to be the field generated over  $\mathbb{C}$  by (the nonleading) entries in the reduced row echelon form of  $W_p$ .

**Example 9.** Let  $K = \mathbb{C}(x)$ ,  $n = 2$ ,  $\bar{a} = (x + 1, 2/(x + 1))$ , and  $p = z_1' - 2z_1z_2 + 3$ . Then the monomials of  $p$  are  $z_1'$ ,  $z_1z_2$ , and 1, their Wronskian and its evaluation at  $\bar{a}$  are

$$\begin{pmatrix} z_1' & z_1z_2 & 1 \\ z_1'' & (z_1z_2)' & 0 \\ z_1''' & (z_1z_2)'' & 0 \end{pmatrix} \quad \text{and} \quad W_p = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

which is already in reduced row echelon form, and so  $F(p) = \mathbb{C}(1, 2, 1) = \mathbb{C}$ . For examples in which  $F(p)$  is strictly greater than  $\mathbb{C}$ , see Example 14 and Section 5.2. There, evaluation of the Wronskian at a point is by differential ideal calculations.

For a tuple  $\bar{p} \subset k\{\bar{z}\}$  of differential polynomials,

$$F(\bar{p}) := \mathbb{C}(F(p) \mid p \in \bar{p}).$$

**Lemma 10.** For every  $p \in k\{\bar{z}\}$  such that  $p(\bar{a}) = 0$ , we have  $F(p) \subset \mathbb{C}\langle\bar{a}\rangle$ .

*Proof.* Follows from all entries of  $W_p$  being from  $\mathbb{C}\langle\bar{a}\rangle$ . □

### 3.2. Statement of main result

We will now show that the problem of finding the field of identifiable functions is reduced to computing the intersection of fields of constants defined by their generators. This is a key step in Algorithm 1 to find the field of all identifiable functions.

**Theorem 11** (Single-experiment identifiability). For system (1), the field of identifiable functions is equal to

$$\mathbb{C}(\bar{\mu}) \cap F(\bar{p}),$$

where  $\bar{p}$  is a set of input-output equations of (1) (Definition 8).

**Remark 12.** Similarly to Theorem 19, the statement of Theorem 11 remains true if, in the calculation of  $F(\bar{p})$ , for each  $p$ , one replaces the Wronskian of the monomials evaluated at  $\bar{a}$  by the Wronskian of any  $q_1, \dots, q_n \in \mathbb{C}\{z\}$  evaluated at  $\bar{a}$  such that  $p = \sum_{i=1}^n c_i q_i$  for some  $c_1, \dots, c_n \in k$ .

### 3.3. An algorithm for computing all identifiable functions

In this section, we present an algorithm that computes generators of the field of all identifiable functions of system (1). We also give an example following the algorithm step by step.

---

**Algorithm 1** Computing all identifiable functions

---

**Input** System  $\Sigma$  as in (1)

**Output** Generators of the field of identifiable functions of  $\Sigma$

- (Step 1)** Compute a set  $\bar{p}$  of input-output equations of  $\Sigma$  (see Definition 8).
- (Step 2)** For each  $p \in \bar{p}$ , compute  $\widetilde{W}_p$  the Wronskian of the monomials of  $p$ . Compute  $W_p$  by replacing each  $y_i^{(j)}$  in  $\widetilde{W}_p$  with the  $j$ -th Lie derivative of  $g_i$  with respect to  $\Sigma$  ( $g_i$ 's are the same as in (1)).
- (Step 3)** For each  $p \in \bar{p}$ , calculate the reduced row echelon form of the matrix  $W_p$  and let  $F(\bar{p})$  be the field generated over  $\mathbb{C}$  by all non-leading coefficients of all matrices  $W_p$ . By [16, Lemma 3.1] and Remark 25, the generators of  $F(\bar{p})$  belong to  $\mathbb{C}(\bar{\mu}, \bar{x})$ .
- (Step 4)** Apply Algorithm 2 to find generators of  $\mathbb{C}(\bar{\mu}) \cap F(\bar{p})$ . Return these generators.
- 

**Remark 13.** In practice, the runtime of the algorithm depends on the chosen ranking, and it would be interesting to have a way to choose the ranking based on the problem.

**Example 14 (Computing identifiable functions – illustration).** To illustrate, we will follow Algorithm 1 for the system:

$$\Sigma = \begin{cases} x_1' = 0, \\ x_2' = x_1 x_2 + a x_1 u + b u, \\ y = x_2 \end{cases}$$

where  $\bar{x} = (x_1, x_2)$ ,  $\bar{y} = (y)$ ,  $\bar{\mu} = (a, b)$ ,  $\bar{u} = (u)$ . This system is a variant of the example from [30, Section 5].

**(Step 1)** For the elimination differential ranking with  $x_1 > x_2 > y > u$ , a calculation shows that

$$x_1 y - a x_1 u - y' - b u, \quad x_2 - y, \quad y y'' - a u y'' - y'^2 + a u' y' - b u y' + b u' y$$

is a monic characteristic presentation for  $I_\Sigma$ . Therefore,  $\bar{p} = (p)$ , where  $p = y y'' - a u y'' - y'^2 + a u' y' - b u y' + b u' y$ .

**(Step 2)** The Wronskian  $\widetilde{W}_p = \text{Wr}(u' y, u y', u' y', y'^2, u y'', y y'')$  is computed (too large to be displayed here). Then, to compute  $W_p$ , all derivatives of  $y$  are replaced with the corresponding Lie derivatives of  $x_2$ , for example:

$$\begin{aligned} y &\rightarrow x_2, & y' &\rightarrow x_1 x_2 + a x_1 u + b u, \\ y'' &\rightarrow x_1(x_1 x_2 + a x_1 u + b u) + a x_1 u' + b u'. \end{aligned}$$

**(Step 3)** A calculation shows that the corresponding reduced row echelon form is:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & -x_1 & -a x_1 - b \\ 0 & 1 & 0 & 0 & x_1 & a x_1 + b \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Therefore,  $F(\bar{p}) = \mathbb{C}(a x_1 + b, x_1)$ .

**(Step 4)** By Theorem 11, the field of identifiable functions is

$$\mathbb{C}(a, b) \cap \mathbb{C}(a x_1 + b, x_1).$$

Applying Algorithm 2, we find that

$$\mathbb{C}(a, b) \cap \mathbb{C}(a x_1 + b, x_1) = \mathbb{C}, \tag{2}$$

so there are no nontrivial identifiable functions in this model.

#### 4. Main result: Multi-experiment identifiability

In this section, we show that the coefficients input-output equations generate the field of multi-experiment identifiable function and derive a generally *tight* upper bound for the number of independent experiments for system (1) sufficient to recover the field of multi-experiment identifiable functions of parameters. These results are stated in Section 4.1 and proven in Appendix A.2. We apply them to specific examples from the literature in Section 5. The tightness of the bound from the mathematical point of view is discussed in the appendix.

##### 4.1. Preparation for Theorem 19

**Definition 15 (Input-output identifiable functions).** A function of parameters  $h \in \mathbb{C}(\bar{\mu})$  in system (1) is said to be *input-output (IO) identifiable* if  $h$  can be expressed as a rational function of the coefficients of the IO-equations of system (1) (see Definition 8), see also [31, Definition 2] and [32, Corollary 1].

As shown in [32, Section 4.1], every identifiable function is input-output identifiable but not every input-output identifiable function is necessarily identifiable.

**Definition 16 (Multi-experiment identifiability, cf. [20]).** A function of parameters  $h \in \mathbb{C}(\bar{\mu})$  in system (1) is said to be *multi-experiment identifiable (ME-identifiable)* if there exists  $N \geq 1$  such that  $h$  is identifiable in the following “ $N$ -experiment” system

$$\Sigma_N := \begin{cases} \bar{x}'_i = f(\bar{x}_i, \bar{\mu}, \bar{u}_i), \\ y_i = g(\bar{x}_i, \bar{\mu}, \bar{u}_i), \end{cases} \quad 1 \leq i \leq N. \quad (3)$$

We also say that  $h$  is  $N$ -experiment identifiable in this case.

**Example 17 (Illustrating the definition).** Consider the system (intentionally simple to illustrate the definition)

$$\begin{cases} x'_1 = 0 \\ y_1 = x_1 \\ y_2 = \theta x_1 + \theta^2, \end{cases} \quad (4)$$

in which  $\theta$  is the unknown parameter. By [16, Example 2.14],  $\theta$  is not (globally) identifiable. Consider now the corresponding 2-experiment system

$$\begin{cases} x'_{1,1} = x'_{2,1} = 0 \\ y_{1,1} = x_{1,1} \\ y_{1,2} = \theta x_{1,1} + \theta^2 \\ y_{2,1} = x_{2,1} \\ y_{2,2} = \theta x_{2,1} + \theta^2; \end{cases}$$

now  $\theta = \frac{y_{2,2} - y_{1,2}}{y_{2,1} - y_{1,1}}$  and so is identifiable.

**Remark 18.** SIAN [15] (see also [32, Remark 2.3]) is software that can check (SE-) global and local identifiability of any given function  $h \in \mathbb{C}(\bar{\mu})$  of parameters of an ODE model  $\Sigma$ . If  $h$  is globally ME-identifiable, then, running SIAN on models of the form  $\Sigma_N$  (see (3)) for  $N = 1, 2, \dots$ , one will in principle eventually find this out. However, if  $h$  is not globally ME-identifiable, one will not be able to conclude this from assessing SE-identifiability of  $\Sigma_N$  without a bound on the number of experiments (provided by Theorem 19).

On the other hand, one could use SIAN to find the sufficient number of experiments **given** a set of generators of the field of ME-identifiable functions. Indeed, for each of these generators, there is an  $N$  such that the generator is SE-identifiable in  $\Sigma_N$ , so the sufficient number of experiments can be taken as the maximum of these  $N$ s. However, this approach works only if generators of the field of ME-identifiable functions are known in advance. Theorem 19 and an algorithm to compute IO-equations (Definition 8) yield an algorithm to find such generators.



#### 4.2. Statement of main result

**Theorem 19** (Multi-experiment identifiability). *A function of parameters  $h \in \mathbb{C}(\bar{\mu})$  in system (1) is multi-experiment identifiable if and only if it is input-output identifiable in system (1).*

*Moreover, if  $h$  is multi-experiment identifiable, then, for all*

$$N \geq \max_{1 \leq i \leq m} (s_i - r_i + 1),$$

*$h$  is identifiable in the  $N$ -experiment system, where  $s_i$  and  $r_i$  are defined by the following:*

- $\bar{p} = p_1, \dots, p_m$  is a set of input-output equations of system (1), and for all  $i$ ,  $1 \leq i \leq m$ ,
- we write

$$p_i = f_{i,s_i+1} + \sum_{j=1}^{s_i} c_{i,j} f_{i,j}, \quad (5)$$

*where  $f_{i,j} \in \mathbb{C}\{\bar{y}, \bar{u}\}$  and linearly independent over  $\mathbb{C}$  (so,  $s_i$  is the length of such a presentation of  $p_i$  minus 1),*

- $r_i := \text{rank Wr}(f_{i,1}(\bar{y}, \bar{u}), \dots, f_{i,s_i}(\bar{y}, \bar{u}))$  modulo  $I_\Sigma$ .

**Example 20 (Degenerate Wronskian).** The goal of this intentionally simple example is to demonstrate that the Wronskians in the theorem can indeed be singular. Consider system (4) again. A calculation shows that

$$\bar{p} = \{y_1', y_2 - \theta y_1 - \theta^2\}$$

is a set of IO-equations for (4). Then  $m = 2$ ,  $s_1=0$ , and  $s_2 = 2$ . We have

$$\text{Wr}(y_1, 1) = \begin{pmatrix} y_1 & 1 \\ y_1' & 0 \end{pmatrix} \text{ mod } I_\Sigma = \begin{pmatrix} x_1 & 1 \\ 0 & 0 \end{pmatrix},$$

and so  $r_2 = 1$ . From [16, Example 2.14],  $\theta$  is not (globally) identifiable (so, we cannot take  $N = 1$ ). By Theorem 19, for all

$$N \geq 2 - 1 + 1 = 2,$$

the field of ME-identifiable functions  $\mathbb{C}(\theta, \theta^2) = \mathbb{C}(\theta)$  is  $N$ -experiment identifiable.

**Remark 21.** In some works (e.g., [2, Section 3.1]), it was suggested that the Wronskians of monomials in a characteristic set be always of corank one ( $r_i = s_i$  in the notation of Theorem 19). As Example 20 (see also Sections 5.2 and 5.3) shows, this is not the case.

#### 4.3. Computational aspects

**Remark 22 (Dependence on decomposition (5)).** For fixed input-output equations  $p_1, \dots, p_m$ , the bound given by Theorem 19 may depend on the choice of decomposition (5). In Appendix D, we give an algorithm to compute a representation yielding the best possible bound (compared to other representations). We use this algorithm in our implementation.

**Remark 23 (Computing the bound).** The rank of the Wronskian matrix from Theorem 19 can be found by:

1. Calculating the Wronskian matrix in  $\bar{y}, \bar{u}$ ,
2. For each matrix entry, computing its differential remainder [19, Section I.9] with respect to the characteristic set defined by  $\Sigma$ , and
3. Applying a (symbolic) algorithm for rank computation.

The correctness follows from [16, Lemma 3.1]. Before computing the rank, one can evaluate the Wronskian at a point. Since the rank cannot increase after an evaluation, the resulting bound will always be correct although might be larger than the bound from Theorem 19.

**Remark 24.** The bound for  $N$  from Theorem 19 can be improved if some of the output variables are constant as discussed in Section 5.3. Constant outputs arise, e.g., to encode the case of constant inputs, which is common in some application domains [42]. The general idea of the refinement is first to treat the constant outputs as parameters, apply Theorem 19 to the rest of the outputs, and then use simultaneous rational interpolation to extract the coefficients with respect to the constant outputs.

## 5. Examples

We illustrate our results with 3 examples. In Section 5.1, Lotka-Volterra model with control, we show that the SE-identifiable and ME-identifiable functions coincide, so one can find the generators of the field of identifiable functions from the coefficients of the IO-equations. The second example (Section 5.2) is a chemical reaction exhibiting the slow-fast ambiguity [41]. Here, the bound from Theorem 19 is exact, and yields that all parameters are identifiable from 2 experiments. In Section 5.3, we show another Lotka-Volterra model, for which some of the parameters become identifiable only after 2 experiments. For other models with more ME-identifiable functions than SE-identifiable ones, we refer to [42, Section III]. Finally, in Section 5.4, we apply our results to the SEIR epidemiological model studied in [40].

All the computations for the examples in this section can be performed automatically using our implementation. The corresponding files can be found in the `examples` folder in the repository <https://github.com/pogudingleb/AllIdentifiableFunctions>.

### 5.1. Lotka-Volterra model with control

Consider the following system

$$\Sigma = \begin{cases} x_1' = ax_1 - bx_1x_2, \\ x_2' = -cx_2 + dx_1x_2 + eu, \\ y = x_1, \end{cases}$$

in which  $a, b, c, d, e$  are the unknown parameters and  $u$  is the input (control). With Theorem 19, we show that, for this model, the fields of SE-identifiable and of ME-identifiable functions coincide. A computation shows that the IO-equation is:

$$\bar{p} = (yy'' - y'^2 - dy^2y' + cyy' + ady^3 - beuy^2 - acy^2),$$

so, in the notation of Theorem 19,  $m = 1$  and, for  $f_1 = y^2y'$ ,  $f_2 = yy'$ ,  $f_3 = y^3$ ,  $f_4 = uy^2$ ,  $f_5 = y^2$ , and  $f_6 = yy'' - y'^2$ , we have  $s_1 = 5$ . A computation shows that

$$r_1 := \text{rank}(\text{Wr}(f_1, f_2, f_3, f_4, f_5) \bmod I_\Sigma) = 5.$$

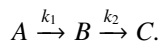
By Theorem 19, for any

$$N \geq 5 - 5 + 1 = 1$$

the ME-identifiable functions are identifiable from  $N$  experiments (cf. [31, Main Results 1 and 2]). In particular, 1 experiment is sufficient. Hence, by Theorem 19, the field of SE-identifiable functions is  $\mathbb{C}(d, c, ad, be, ac) = \mathbb{C}(a, be, c, d)$ .

### 5.2. Slow-fast ambiguity in chemical reactions

In this example, we consider the system [15, Section A.1, equation (3)]. This system originates from the following chemical reaction network [41, equation (1.1)]:



Then the quantities  $x_A, x_B$ , and  $x_C$  of species satisfy the system:

$$\begin{cases} x_A' = -k_1x_A, \\ x_B' = k_1x_A - k_2x_B, \\ x_C' = k_2x_B. \end{cases} \quad (6)$$

The observed quantities will be

- $y_1 = x_C$ , the concentration of  $C$ ;
- $y_2 = \varepsilon_A x_A + \varepsilon_B x_B + \varepsilon_C x_C$ , which may represent a property of the mixture, e.g. absorbance or conductivity [41, p. 701].

As explained in [41, p. 701], in practice,  $x_B$  might be hard to isolate, so  $\varepsilon_B$  is also an unknown parameter, while the values  $\varepsilon_A$  and  $\varepsilon_C$  can be assumed to be known but could depend on  $A$ ,  $C$ , and the details of the experimental setup. The assumption that  $\varepsilon_A$  and  $\varepsilon_C$  are known can be encoded into the ODE system by making them state variables with zero derivatives and adding outputs to make them observable. This will yield the following final ODE model (the same as [15, Section A.1, equation (3)]):

$$\Sigma = \begin{cases} x'_A = -k_1 x_A, \\ x'_B = k_1 x_A - k_2 x_B, \\ x'_C = k_2 x_B, \\ \varepsilon'_A = \varepsilon'_C = 0, \\ y_1 = x_C, \\ y_2 = \varepsilon_A x_A + \varepsilon_B x_B + \varepsilon_C x_C, \\ y_3 = \varepsilon_A, \\ y_4 = \varepsilon_C, \end{cases} \quad (7)$$

where  $\bar{x} = (x_A, x_B, x_C, \varepsilon_A, \varepsilon_C)$ ,  $\bar{y} = (y_1, y_2, y_3, y_4)$ , and  $\bar{\mu} = (k_1, k_2, \varepsilon_B)$ . As noted in [41] (see also [15, Section A.1]), this model has slow-fast ambiguity: it is possible to recover a pair of numbers  $\{k_1, k_2\}$  from the observations but impossible to know which one is  $k_1$  and which one is  $k_2$ . A similar phenomenon occurs in epidemiological models, see [40, Proposition 2].

We start with assessing the **SE-identifiability** of the model (7) using Algorithm 1 to find the field of identifiable functions. For (Step 1), a calculation in MAPLE shows that the following set  $\bar{p} = \{p_1, p_2, p_3, p_4\}$  is a set of IO-equations of (7):

$$\begin{aligned} p_1 &= k_1 k_2 (y_2 - y_1 y_4) - \varepsilon_B k_1 y'_1 - k_2 y'_1 y_3 - y'_1 y_3, \\ p_2 &= y'''_1 + (k_1 + k_2) y''_1 + k_1 k_2 y'_1, \quad p_3 = y'_3, \quad p_4 = y'_4. \end{aligned}$$

In (Step 2) and (Step 3), we compute the reduced row echelon forms of  $W_{p_1} = \text{Wr}(y_2, y_1 y_4, y'_1, y'_1 y_3, y''_1 y_3)$  and  $W_{p_2} = \text{Wr}(y'''_1, y'_1, y''_1)$  modulo the equations  $\Sigma$  and obtain the matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 & k_1 k_2 \\ 0 & 1 & 0 & 0 & -k_1 k_2 \\ 0 & 0 & 1 & \varepsilon_A & -(\varepsilon_A k_2 + \varepsilon_B k_1) \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & -k_1 k_2 \\ 0 & 1 & -(k_1 + k_2) \\ 0 & 0 & 0 \end{pmatrix},$$

respectively.  $W_{p_3}$  and  $W_{p_4}$  are  $1 \times 1$  matrices with the reduces row echelon form (1). Therefore,

$$F(\bar{p}) = \mathbb{C}(k_1 + k_2, k_1 k_2, \varepsilon_A, \varepsilon_A k_2 + \varepsilon_B k_1).$$

Before going to (Step 4), we show that this intermediate result of computation can provide additional insights, for example, recover the parameter transformation corresponding to the slow-fast ambiguity [41, equation (1.3)]. From the proof of Theorem 11,  $F(\bar{p})$  consists of identifiable constants. So, any parameter transformation induces an automorphism  $\alpha$  of the constants over  $F(\bar{p})$ . Since  $k_1 + k_2$  and  $k_1 k_2$  are identifiable,  $\alpha(k_1) = k_1$  and  $\alpha(k_2) = k_2$  or  $\alpha(k_1) = k_2$  and  $\alpha(k_2) = k_1$ . Consider the latter case. Since  $\varepsilon_A \in F(\bar{p})$ , we have  $\alpha(\varepsilon_A) = \varepsilon_A$ . Hence,

$$\varepsilon_A k_2 + \varepsilon_B k_1 = \alpha(\varepsilon_A k_2 + \varepsilon_B k_1) = \varepsilon_A k_1 + k_2 \alpha(\varepsilon_B),$$

so  $\alpha(\varepsilon_B) = \varepsilon_A + \frac{k_1(\varepsilon_B - \varepsilon_A)}{k_2}$ , giving the transformation [41, (1.3)]:

$$k_1 \rightarrow k_2, \quad k_2 \rightarrow k_1, \quad \varepsilon_A \rightarrow \varepsilon_A, \quad \varepsilon_B \rightarrow \varepsilon_A + \frac{k_1(\varepsilon_B - \varepsilon_A)}{k_2}. \quad (8)$$

Finally, in (Step 4), we compute

$$\mathbb{C}(k_1, k_2, \varepsilon_B) \cap F(\bar{p}) = \mathbb{C}(k_1 k_2, k_1 + k_2).$$

Now we will consider model (7) in the **multi-experiment setup** in which one is allowed to perform several

experiments with the same  $k_1, k_2, \varepsilon_B$  but different initial concentrations and  $\varepsilon_A, \varepsilon_C$ . We will show that, in this setup, the ambiguity can be resolved by one extra experiment. The first part of Theorem 19 implies that the field of ME-identifiable functions is generated by the coefficients of  $\bar{p}$ , so it equals

$$\mathbb{C}(k_1 k_2, \varepsilon_B k_1, k_2, k_1 + k_2) = \mathbb{C}(k_1, k_2, \varepsilon_B).$$

Therefore, *all* the parameters can be identified from several experiments. Now we use the bound from Theorem 19 to find the number of experiments sufficient to make all the parameter identifiable. In the notation of the theorem, for  $i = 1$ , we take

$$f_{1,1} = y_2 - y_1 y_4, \quad f_{1,2} = y'_1, \quad f_{1,3} = y'_1 y_3, \quad f_{1,4} = y''_1 y_3,$$

and so  $s_1 = 3$ . A calculation in MAPLE shows that

$$r_1 = \text{rank Wr}(f_{1,1}, f_{1,2}, f_{1,3}) \pmod{I_\Sigma} = 2.$$

so the Wronskian does not always have full rank in practical examples either. For  $i = 2$ ,  $f_{2,1} = y''_1, f_{2,2} = y'_1$ , so  $s_2 = 2$ , and

$$r_2 = \text{rank Wr}(f_{2,1}, f_{2,2}) \pmod{I_\Sigma} = 2.$$

Finally,  $f_{3,1} = y'_3$  and  $f_{4,1} = y'_4$ , and so  $s_3 = s_4 = 0$ . Thus, all parameters are  $N$ -identifiable for all

$$N \geq \max(3 - 2 + 1, 2 - 2 + 1, 0 - 0 + 1, 0 - 0 + 1) = 2.$$

This bound is tight because, as we demonstrated earlier, neither of the parameter is identifiable from a single experiment.

### 5.3. Lotka-Volterra model with “mixed” output

In this example, we will illustrate the refinement of the bound on the number of experiments mentioned in Remark 24 on the following variant of the Lotka-Volterra model:

$$\Sigma = \begin{cases} x'_1 = ax_1 - x_1 b x_2, \\ x'_2 = -cx_2 + dx_1 x_2, \\ y = ex_1 + f x_2, \end{cases}$$

where we assume that  $a, b, c, d, e$  are unknown parameters and  $f$  is a known parameter that takes different values if multiple experiments are conducted. In the context of our differential algebra setup, this can be encoded as follows:

$$\Sigma = \begin{cases} x'_1 = ax_1 - bx_1 x_2, \\ x'_2 = -cx_2 + dx_1 x_2, \\ f' = 0, \\ y_1 = ex_1 + f x_2, \\ y_2 = f \end{cases} \quad (9)$$

Our implementation shows that the field of ME-identifiable functions is

$$\mathbb{C}(a, b, c, d/e). \quad (10)$$

In particular,  $a, b, c$  are ME-identifiable,  $d$  and  $e$  are not but their ratio is.

We now discuss the number of experiments for globally identifying the functions (10). A straightforward application of Theorem 19 yields a bound 35 (Wronskian of dimension 51 and rank 17). 35 could be viewed as a rather high number of experiments and is far from the actual number (2, as shown below).

We can get a better bound equal to 4 using the same Theorem 19 as follows. Observe that, since  $y_2$  is constant, then there will be the following input-output equations for the model:  $y'_2 = 0$  and  $p = 0$ , where  $p$  is a differential polynomial  $y_1$  and  $y_2$  over  $\mathbb{C}(\bar{\mu})$  of zero order in  $y_2$ . We observe that, if one replaces  $y_2$  in  $p = 0$  with  $f$ , the resulting equations will be the input-output equations for the following simplified model, in which  $f$  is considered as a scalar

parameter:

$$\Sigma = \begin{cases} x'_1 = ax_1 - bx_1x_2, \\ x'_2 = -cx_2 + dx_1x_2, \\ y = ex_1 + fx_2, \end{cases} \quad (11)$$

Our implementation shows that the bound for this model is one, so SE-identifiable and ME-identifiable functions for this model are the same. In particular the coefficients of the monic input-output equation of (11) are identifiable from a single experiment. These coefficients are rational function in  $f$  over  $\mathbb{C}(a, b, c, d, e)$ . We write them as  $C_1/C, \dots, C_s/C$ , where  $C, C_1, \dots, C_s$  are polynomials in  $f$  over  $\mathbb{C}(a, b, c, d, e)$ , and  $C$  is monic. We denote the number coefficients not belonging to  $\mathbb{C}$  in  $C, C_1, \dots, C_s$  by  $n, n_1, \dots, n_s$ , respectively. Then these coefficients can be determined uniquely from

$$\max \left( n + \min_{1 \leq i \leq s} n_i, \max_{1 \leq i \leq s} n_i \right).$$

evaluations for different values of  $f$ . To show this, assume that  $n_1 = \min_{1 \leq i \leq s} n_i$ . Then  $n + n_1$  evaluations are sufficient to reconstruct coefficients of  $C_1/C$  as a rational function in  $f$ . Then, once the coefficients of  $C$  are known, evaluations of  $C_2/C, \dots, C_s/C$  can be used to find the coefficients of  $C_2, \dots, C_s$  via polynomial interpolation. In this example,  $n = 2$ ,  $\min_{1 \leq i \leq s} n_i = 2$ , and  $\max_{1 \leq i \leq s} n_i = 4$ , so four evaluations (that is, four experiments with different known values of  $f$  will be enough).

The obtained bound 4 is close to the exact bound 2, which can be obtained using Theorem 19 and SIAN as follows. Using SIAN, we obtain that  $a, b, c, d/e$  are only locally identifiable (from one experiment), so  $N > 1$ . Running SIAN for 2 experiments shows that the functions (10) are 2-experiment globally identifiable. Since from Theorem 19 we know that these functions generate all ME-identifiable functions, we conclude that  $N = 2$ . Replication of the system makes it substantially more challenging for SIAN, so this approach might be impractical if  $N$  is large, while computing the bound above may be feasible.

#### 5.4. SEIR epidemiological model

Structural identifiability of the following epidemiological model has been considered in [40, Equation 2.2]

$$\begin{cases} S' = -\beta \frac{SI}{N}, \\ E' = \beta \frac{SI}{N} - \eta E, \\ I' = \eta E - \alpha I, \\ R' = \alpha I, \end{cases} \quad (12)$$

where  $N$  is the total population which is constant and known. The following two setups are considered in [40]:

- *Prevalence observation.* In this case, these is an output  $y_1 = I$ . We also add  $y_2 = N$  to account for the fact that  $N$  is known. Our implementation shows that the bound from Theorem 19 is equal to one, so the fields of ME-identifiable and SE-identifiable functions coincide. It also finds that these fields are equal to  $\mathbb{C}(\alpha\eta, \alpha + \eta, \beta, N)$ .
- *Cumulative incidence observation.* In this case, the observed quantity is  $\int \eta E dt$ . This can be encoded by introducing a new state variable  $C$  with  $C' = \eta E$  and the outputs  $y_1 = C$  and  $y_2 = N$ . Our algorithm again shows that the fields of ME-identifiable and SE-identifiable functions coincide and that they equal  $\mathbb{C}(\alpha, \beta, \eta, N)$ , so all of the parameters are globally identifiable.

These results confirm the findings of [40] obtained from analysis of input-output equations (that is, for ME-identifiability) and show that they are valid for SE-identifiability as well.

#### Acknowledgments

We are grateful to Julio Banga and Alejandro Villaverde for learning from them about the importance of multi-experiment parameter identifiability at the AIM workshop ‘‘Identifiability problems in systems biology’’. We thank the editors and referees for their useful comments and suggestions. This work was partially supported by the

NSF grants CCF-1564132, CCF-1563942, DMS-1760448, DMS-1760413, DMS-1853650, DMS-1665035, DMS-1760212, DMS-1853482, and DMS-1800492, and by the Paris Ile-de-France Region.

## References

- [1] J. Baaijens and J. Draisma. On the existence of identifiable reparametrizations for linear compartment models. *SIAM Journal on Applied Mathematics*, 76(4), 2016. URL <https://doi.org/10.1137/15M1038013>.
- [2] D. J. Bearup, N. D. Evans, and M. J. Chappell. The input-output relationship approach to structural identifiability analysis. *Computer Methods and Programs in Biomedicine*, 109(2):171–181, 2013. URL <https://doi.org/10.1016/j.cmpb.2012.10.012>.
- [3] G. Bellu, M. P. Saccomani, S. Audoly, and L. D’Angiò. DAISY: A new software tool to test global identifiability of biological and physiological systems. *Computer Methods and Programs in Biomedicine*, 88(1):52–61, 2007. URL <https://doi.org/10.1016/j.cmpb.2007.07.002>.
- [4] A. K. Binder. *Algorithms for Fields and an Application to a Problem in Computer Vision*. PhD thesis, Technische Universität München, 2009. URL <https://pdfs.semanticscholar.org/e8f3/bba89b1f1c524d55914cf930562ac8432041.pdf>.
- [5] F. Boulier and F. Lemaire. Computing canonical representatives of regular differential ideals. In *Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 38–47. ACM, 2000. URL <https://doi.org/10.1145/345542.345571>.
- [6] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Computing representations for radicals of finitely generated differential ideals. *Applicable Algebra in Engineering, Communication and Computing*, 20:73–121, 2009. URL <https://doi.org/10.1007/s00200-009-0091-7>.
- [7] F. Boulier, F. Lemaire, M. Rosenkranz, R. Ushirobira, and N. Verdière. On symbolic approaches to integro-differential equations. In *Algebraic and Symbolic Computation Methods in Dynamical Systems*, pages 161–182. Springer International Publishing, 2020. URL [https://doi.org/10.1007/978-3-030-38356-5\\_6](https://doi.org/10.1007/978-3-030-38356-5_6).
- [8] L. Denis-Vidal, G. Joly-Blanchard, C. Noiret, and M. Petitot. An algorithm to test identifiability of non-linear systems. *IFAC Proceedings Volumes*, 34(6):197–201, 2001. URL [https://doi.org/10.1016/S1474-6670\(17\)35173-X](https://doi.org/10.1016/S1474-6670(17)35173-X).
- [9] M. Eisenberg. Input-output equivalence and identifiability: some simple generalizations of the differential algebra approach. 2019. URL <https://arxiv.org/abs/1302.5484>.
- [10] M. Fink and M. Noble. Markov models for ion channels: Versatility versus identifiability and speed. *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, 367(1896):2161–2179, 2009. URL <https://doi.org/10.1098/rsta.2008.0301>.
- [11] K. Forsman and M. Jirstrand. Some finiteness issues in differential algebraic systems theory. In *Proceedings of 1994 33rd IEEE Conference on Decision and Control*. URL <https://doi.org/10.1109/cdc.1994.411295>.
- [12] S. Glad. Nonlinear input output relations and identifiability. In *Proceedings of the 31st IEEE Conference on Decision and Control*, volume 4, pages 3673–3675, Tucson, AZ, USA, 1992. URL <https://doi.org/10.1109/CDC.1992.370965>.
- [13] S. Glad and L. Ljung. Model structure identifiability and persistence of excitation. In *Proceedings of the 29th IEEE Conference on Decision and Control*, volume 6, pages 3236–3240, Honolulu, HI, USA, 1990. URL <https://doi.org/10.1109/CDC.1990.203389>.
- [14] E. Gross, H. A. Harrington, N. Meshkat, and A. Shiu. Linear compartmental models: input-output equations and operations that preserve identifiability. *SIAM Journal on Applied Mathematics*, 79(4):1423–1447, 2019. URL <https://doi.org/10.1137/18M1204826>.
- [15] H. Hong, A. Ovchinnikov, G. Pogudin, and C. Yap. SIAN: software for structural identifiability analysis of ODE models. *Bioinformatics*, 35(16):2873–2874, 2019. URL <https://doi.org/10.1093/bioinformatics/bty1069>.
- [16] H. Hong, A. Ovchinnikov, G. Pogudin, and C. Yap. Global identifiability of differential models. *Communications on Pure and Applied Mathematics*, 73(9):1831–1879, 2020. URL <https://doi.org/10.1002/cpa.21921>.
- [17] R. Jain, S. Narasimhan, and N. Bhatt. A priori parameter identifiability in models with non-rational functions. *Automatica*, 109(11):108513, 2019. URL <https://doi.org/10.1016/j.automatica.2019.108513>.
- [18] Z. Jiafan and L. Xiang. Diagnosability test for nonlinear systems using the characteristic set. In *2009 Asia-Pacific Conference on Information Processing*, 2009. URL <https://doi.org/10.1109/apcip.2009.59>.
- [19] E. Kolchin. *Differential Algebra and Algebraic Groups*. Academic Press, New York, 1973.
- [20] T. S. Ligon, F. Fröhlich, O. T. Chiş, J. R. Banga, E. Balsa-Canto, and J. Hasenauer. GenSSI 2.0: multi-experiment structural identifiability analysis of SBML models. *Bioinformatics*, 34(8):1421–1423, 2017. URL <https://doi.org/10.1093/bioinformatics/btx735>.
- [21] L. Ljung and T. Glad. On global identifiability for arbitrary model parametrizations. *Automatica*, 30(2):265–276, 1994. URL [https://doi.org/10.1016/0005-1098\(94\)90029-9](https://doi.org/10.1016/0005-1098(94)90029-9).
- [22] D. Marker. *Model Theory of Differential Fields*, volume 5 of *Lecture Notes in Logic*, pages 38–113. Springer-Verlag, Berlin, 1996. URL <https://doi.org/10.1017/9781316716991.003>.
- [23] N. Meshkat and S. Sullivant. Identifiable reparametrizations of linear compartment models. *Journal of Symbolic Computation*, 63:46–67, 2014. URL <https://doi.org/10.1016/j.jsc.2013.11.002>.
- [24] N. Meshkat, M. Eisenberg, and J. DiStefano. An algorithm for finding globally identifiable parameter combinations of nonlinear ODE models using Gröbner bases. *Mathematical Biosciences*, 222(2):61–72, 2009. URL <https://doi.org/10.1016/j.mbs.2009.08.010>.
- [25] N. Meshkat, C. Kuo, and J. DiStefano. On finding and using identifiable parameter combinations in nonlinear dynamic systems biology models and COMBOS: A novel web implementation. *PLoS ONE*, 9(10):e110261, 2014. URL <https://doi.org/10.1371/journal.pone.0110261>.
- [26] N. Meshkat, S. Sullivant, and M. Eisenberg. Identifiability results for several classes of linear compartment models. *Bulletin of Mathematical Biology*, 77:1620–1651, 10 2014. URL <https://doi.org/10.1007/s11538-015-0098-0>.
- [27] N. Meshkat, Z. Rosen, and S. Sullivant. Algebraic tools for the analysis of state space models. In T. Hibi, editor, *The 50th Anniversary of Gröbner Bases, July 1–10, 2015, Osaka, Japan*, volume 77 of *Advances in Pure Mathematics*, pages 171–205, Tokyo, Japan, 2018. Mathematical Society of Japan. URL <https://doi.org/10.2969/aspm/07710171>.
- [28] H. Miao, X. Xia, A. S. Perelson, and H. Wu. On identifiability of nonlinear ODE models and applications in viral dynamics. *SIAM Review*, 53(1):3–39, 2011. URL <https://doi.org/10.1137/090757009>.

- [29] F. Ollivier. *Le problème de l'identifiabilité structurelle globale: approche théorique, méthodes effectives et bornes de complexité*. PhD thesis, École polytechnique, 1990. URL <https://www.theses.fr/1990EPXX0009>.
- [30] A. Ovchinnikov, A. Pillay, G. Pogudin, and T. Scanlon. Multi-experiment parameter identifiability of ODEs and model theory. 2020. URL <https://arxiv.org/abs/2011.10868>.
- [31] A. Ovchinnikov, G. Pogudin, and P. Thompson. Input-output equations and identifiability of linear ODE models. 2020. URL <https://arxiv.org/abs/1910.03960>.
- [32] A. Ovchinnikov, G. Pogudin, and P. Thompson. Parameter identifiability and input-output equations. *Applicable Algebra in Engineering, Communication and Computing*, 2021. URL <https://doi.org/10.1007/s00200-021-00486-8>.
- [33] J. F. Ritt. *Differential Algebra*, volume 33 of *Colloquium Publications*. American Mathematical Society, 1950.
- [34] M. Saccomani and L. D'Angiò. Examples of testing global identifiability with the DAISY software. *IFAC Proceedings Volumes*, 42(10): 48–53, 2009. URL <https://doi.org/10.3182/20090706-3-FR-2004.00007>.
- [35] M. Saccomani, S. Audoly, and L. D'Angiò. Parameter identifiability of nonlinear systems: the role of initial conditions. *Automatica*, 39: 619–632, 2003. URL [https://doi.org/10.1016/S0005-1098\(02\)00302-3](https://doi.org/10.1016/S0005-1098(02)00302-3).
- [36] M. P. Saccomani and G. Bellu. DAISY: An efficient tool to test global identifiability. Some case studies. In *2008 16th Mediterranean Conference on Control and Automation*, pages 1723–1728, 2008. URL <https://doi.org/10.1109/MED.2008.4602152>.
- [37] A. Seidenberg. The prime ideals of a polynomial ideal under extension of the base field. *Annali di Matematica Pura ed Applicata*, 102(1): 57–59, 1975. URL <https://doi.org/10.1007/bf02410595>.
- [38] E. D. Sontag. Dynamic compensation, parameter identifiability, and equivariances. *PLOS Computational Biology*, 13(4):1–17, 2017. URL <https://doi.org/10.1371/journal.pcbi.1005447>.
- [39] G. W. Stewart. *Matrix Algorithms: I. Basic Decompositions*. SIAM, 1998.
- [40] N. Tuncer and T. T. Le. Structural and practical identifiability analysis of outbreak models. *Mathematical Biosciences*, 299:1–18, 2018. URL <https://doi.org/10.1016/j.mbs.2018.02.004>.
- [41] S. Vajda and H. Rabitz. Identifiability and distinguishability of first-order reaction systems. *Journal of Physical Chemistry*, 92:701–707, 1988. URL <https://doi.org/10.1021/j100314a024>.
- [42] A. Villaverde, N. Evans, M. Chappell, and J. Banga. Input-dependent structural identifiability of nonlinear systems. *IEEE Control Systems Letters*, 3(2):272–277, 2019. URL <https://doi.org/10.1109/LCSYS.2018.2868608>.
- [43] A. F. Villaverde, N. D. Evans, M. J. Chappell, and J. R. Banga. Sufficiently exciting inputs for structurally identifiable systems biology models. *IFAC-PapersOnLine*, 51(19):16–19, 2018. URL <https://doi.org/10.1016/j.ifacol.2018.09.015>.

## Appendix A. Proofs of the main results

### Appendix A.1. Single-experiment identifiability

In this section, we will prove our first main result, Theorem 11.

**Remark 25** ( $F(p)$  is generated by first integrals). Lemma 26 implies that  $F(\bar{p})$  consists of constants (that is, first integrals). [31, Lemma 2] implies that  $F(\bar{p}) \subset \mathbb{C}(\bar{\mu}, \bar{x})$ .

**Lemma 26.** *In the setup of Section 3.1,  $F(p) \subset \text{Const}(K)$ .*

*Proof.* We will show that the space of linear relations between columns of  $W_p$  is defined over  $\text{Const}(K)$ . This will imply that all the entries in the reduced row echelon form of  $W_p$  are constants. Let  $X$  be a maximal set of linearly independent columns of  $W_p$ , and let  $Y$  denote the rest of the columns. The monomials corresponding to  $X$  are linearly independent over  $\text{Const}(K)$  because any such dependence would yield a dependence of  $X$ . For each  $v \in Y$ , there exists a column dependence of  $X \cup \{v\}$ , unique up to scaling. These dependencies span the space of column dependencies of  $W_p$ . [19, Chapter II, Section 1, Theorem 1] implies that the monomials corresponding to  $X \cup \{v\}$  are dependent over  $\text{Const}(K)$ . Therefore, the corresponding column dependence can be chosen to be over  $\text{Const}(K)$  as well.  $\square$

*Proof of Theorem 11.* To prove the theorem, we will show that, for all differential fields  $k \subset K$  with  $\mathbb{C} \subset k \subset \text{Const}(K)$  and  $k$  being algebraically closed in  $K$ , every  $n$ , and every tuple  $\bar{a} \in K^n$ ,

$$k \cap F(\bar{p}) = k \cap \mathbb{C}(\bar{a}),$$

where  $\bar{p} := \{p_1, \dots, p_m\} \subset k\{z_1, \dots, z_n\}$  is a characteristic set of the prime ideal of all differential polynomials vanishing at  $\bar{a}$ . This is then applied to  $k = \mathbb{C}(\bar{\mu})$  and the differential field  $K$  generated over  $k$  by the  $(\bar{y}, \bar{u})$ -components (denoted by  $\bar{a}$ ) of a generic solution of (1).

Lemma 10 implies that  $k \cap F(\bar{p}) \subset k \cap \mathbb{C}(\bar{a})$ . Assume that

$$k \cap \mathbb{C}(\bar{a}) \supsetneq k \cap F(\bar{p})$$

and let  $b \in k \cap \mathbb{C}(\bar{a}) \setminus k \cap F(\bar{p})$ .

Recall (see [22, Section 2]) that a differential field  $K$  is differentially closed if: for all  $m$  and finite  $G \subset K\{w_1, \dots, w_m\}$ , if there exists  $L \supset K$  such that  $G = 0$  has a solution in  $L$ , then  $G = 0$  has a solution in  $K$ . Let  $K^{\text{diff}}$  be a differential closure of  $K$ , that is, a differentially closed field containing  $K$  that embeds into any other differentially closed field containing  $K$ .

We have  $K^{\text{diff}} \supset k^{\text{acl}}$ , the algebraic closure of  $k$ , and  $k^{\text{acl}} \cap K = k$ . Since  $b \notin F(\bar{\rho})$ , there exists an automorphism  $\alpha: \text{Const}(K^{\text{diff}}) \rightarrow \text{Const}(K^{\text{diff}})$  such that  $\alpha|_{F(\bar{\rho})} = \text{id}$  and  $\alpha(b) \neq b$ . We pick such an  $\alpha$  and extend it to a differential automorphism of  $K^{\text{diff}}$  and denote the extension by  $\alpha$  as well.

For a vector  $K$ -subspace  $V$  of  $K^n$  with  $\mathbb{C} \subset K$ , we denote the field of definition of the subspace over  $\mathbb{C}$  by  $\text{FD}(V)$ . Recall that  $V$  has a  $K$ -basis  $e_1, \dots, e_\ell$  of  $V$  such that  $e_1, \dots, e_\ell \in \text{FD}(V)^n$ .

Fix  $1 \leq i \leq m$ . Let  $V_{p_i}$  denote the right kernel of  $W_{p_i}$ . Note that  $V_{p_i}$  is defined over  $\text{Const}(K)$ . Since  $p_i(\bar{a}) = 0$ , the vector of coefficients of  $p_i$  belongs to  $V_{p_i}$ . Note that  $\text{FD}(V_{p_i}) = F(p_i)$ . By the preceding paragraph, there exist  $r_{i,1}, \dots, r_{i,N_i} \in \text{FD}(V_{p_i})\{z_1, \dots, z_n\}$  such that

- for every  $1 \leq j \leq N_i$ , the vector of the coefficients of  $r_{i,j}$  belongs to  $V_{p_i}$  (in particular,  $r_{i,j}(\bar{a}) = 0$ );
- $p_i$  is a  $K$ -linear combination of  $r_{i,1}, \dots, r_{i,N_i}$ .

Since  $b \in \mathbb{C}(\bar{a})$ , there exist differential polynomials  $R_1, R_2 \in \mathbb{C}\{\bar{z}\}$  such that  $b = \frac{R_1(\bar{a})}{R_2(\bar{a})}$ . We write  $H = S_1 \cdot \dots \cdot S_m \cdot I_1 \cdot \dots \cdot I_m$ , where  $I_i$  and  $S_i$  are the initial and separant of  $p_i$ . Since  $b \in k$ ,  $bR_2 - R_1 \in k\{\bar{x}\}$ . Since additionally  $bR_2(\bar{a}) - R_1(\bar{a}) = 0$ ,

$$H(bR_2 - R_1) \in \sqrt{[\bar{\rho}]}$$

Since, for every  $1 \leq i \leq \ell$ ,  $p_i \in [r_{i,1}, \dots, r_{i,N_i}]$ , we have

$$H(bR_2 - R_1) \in \sqrt{[r_{1,1}, \dots, r_{m,N_m}]} \tag{A.1}$$

We apply  $\alpha$  to (A.1) and use that  $r_{i,j}$ 's are invariant under  $\alpha$ :

$$\alpha(H)(\alpha(b)R_2 - R_1) \in \sqrt{[r_{1,1}, \dots, r_{m,N_m}]} \tag{A.2}$$

We multiply (A.1) by  $\alpha(H)$  and (A.2) by  $H$ , and subtract. We obtain

$$H\alpha(H)R_2(\alpha(b) - b) \in \sqrt{[r_{1,1}, \dots, r_{m,N_m}]}$$

Every element of  $\sqrt{[r_{1,1}, \dots, r_{m,N_m}]}$  vanishes at  $\bar{a}$  since every  $r_{i,j}$  vanishes at  $\bar{a}$ . Since  $H(\bar{a}) \neq 0$  and  $R_2(\bar{a})(\alpha(b) - b) \neq 0$ , it is sufficient to show that  $\alpha(H)(\bar{a}) \neq 0$  to arrive at contradiction.

Assume there are  $1 \leq i \leq m$  and  $h \in \{S_i, I_i\}$  such that  $\alpha(h)(\bar{a}) = 0$ . Consider the sets  $M_0$  and  $M_1$  of monomials of  $\alpha(h)(\bar{a})$  (or, equivalently, of  $h(\bar{a})$ ) and  $p_i(\bar{a})$ , respectively. Observe that there is a monomial  $A$  in  $\bar{a}$  with  $AM_0 \subset M_1$  because

- if  $h = S_i$ , take  $A$  to be lead  $p_i(\bar{a})$ ;
- if  $h = I_i$ , take  $A$  to be the appropriate power of lead  $p_i(\bar{a})$ .

As  $AM_0 \subset M_1$ , we have  $F(AM_0) \subset F(p_i)$ . Kernels of Wronskians are defined over the constants by Lemma 26, so the kernel of the Wronskian of a tuple does not change if the tuple is multiplied by a nonzero element. Hence,  $F(AM_0) = F(M_0) = F(\alpha(h))$ , and so  $F(\alpha(h)) \subset F(p_i)$ . Since  $\alpha(h)(\bar{a}) = 0$ , there are  $r_1, \dots, r_s \in F(\alpha(h))\{\bar{z}\} = F(h)\{\bar{z}\} \subset K\{\bar{z}\}$  and  $\lambda_1, \dots, \lambda_s \in K$  such that

$$\alpha(h) = \lambda_1 r_1 + \dots + \lambda_s r_s \text{ and } r_1(\bar{a}) = \dots = r_s(\bar{a}) = 0.$$

Applying  $\alpha^{-1}$ , we get

$$h = \alpha^{-1}(\lambda_1)r_1 + \dots + \alpha^{-1}(\lambda_s)r_s,$$

so  $h(\bar{a}) = 0$ , which is impossible, hence the contradiction.  $\square$

## Appendix A.2. Multi-experiment identifiability

*Proof of Theorem 19.* For simplicity of notation, we denote the tuple of variables  $\bar{y}, \bar{u}$  by  $\bar{w}$ . Note that, for every  $N \geq 1$ , the set

$$\bar{p}(\bar{w}_1), \dots, \bar{p}(\bar{w}_N) \subset k\{\bar{w}_1, \dots, \bar{w}_N\}$$



is a set of IO-equations of  $\Sigma_N$ . The coefficients of  $\bar{p}(\bar{w}_1), \dots, \bar{p}(\bar{w}_N)$  are also  $c_{1,1}, \dots, c_{m,s_m}$ . Hence, as in [32, Corollary 1 and Theorem 1], the field of  $N$ -experiment identifiable functions is contained in  $\mathbb{C}(c_{1,1}, \dots, c_{m,s_m})$ .

For the reverse inclusion, let  $p \in \bar{p}$ ,

$$p = \sum_{i=1}^s b_i f_i + f_{s+1},$$

where, for each  $i$ ,  $f_i \in \mathbb{C}\{\bar{w}\}$  and  $f_1, \dots, f_s$  are linearly independent over  $\mathbb{C}$ . By dividing  $p$  by an element of  $k$ , we may assume that  $\deg f_{s+1} = \deg p$ . Let

$$A := \begin{pmatrix} f_1(\bar{a}_1) & \dots & f_s(\bar{a}_1) \\ \vdots & \ddots & \vdots \\ f_1(\bar{a}_s) & \dots & f_s(\bar{a}_s) \end{pmatrix},$$

where, for each  $i$ ,  $\bar{a}_i$  is the image of  $\bar{w}_i$  modulo  $I_{\Sigma_N}$ . We will first show that  $\det A \neq 0$ . For this, let  $M$  be a minimal (by size) zero minor of  $A$ . Let, for some  $i$  and  $\ell$ ,  $f_i(\bar{a}_\ell)$  appear in  $M$  and  $q \in k\{\bar{w}\}$  be the differential polynomial obtained from  $M$  by replacing  $f_j(\bar{a}_\ell)$  with  $f_j(\bar{w})$ ,  $1 \leq j \leq s$ . By the minimality of  $M$  and linear independence of  $f_1, \dots, f_s$ ,  $q(\bar{w}) \neq 0$ . Since  $q(\bar{a}_\ell) = 0$ , there exist  $q_{i,j} \in k\{\bar{w}_j\}$  such that

$$\forall i \ q_{i,1}(\bar{w}) \in I_\Sigma \text{ or } \dots \text{ or } q_{i,s}(\bar{w}) \in I_\Sigma \quad \text{and}$$

$$q = \sum_i q_{i,\ell}(\bar{w}) \cdot \prod_{\substack{j=1 \\ j \neq \ell}}^s q_{i,j}(\bar{a}_j).$$

Hence, there exist  $\alpha$ , and  $q_1, \dots, q_\alpha \in I_\Sigma$ , and  $b_1, \dots, b_\alpha \in k\langle \bar{a}_1, \dots, \bar{a}_{\ell-1}, \bar{a}_{\ell+1}, \dots, \bar{a}_s \rangle$  such that  $q = \sum_{i=1}^\alpha b_i q_i$  and, for each  $i$ , every monomial that appears in  $q_i$  also appears in  $q$  (and, therefore, in  $p$ ). Let  $\tilde{q}$  be the primitive part of  $q_1$  considered as a polynomial in its leader. Since  $I_\Sigma$  is prime,  $\tilde{q} \in I_\Sigma$ . Since  $\bar{p}$  is autoreduced and  $\tilde{q}$  divides a linear combination of the monomials of  $p$ , the characteristic set  $\tilde{\bar{p}}$  of  $\bar{p} \setminus \{p\} \cup \{\tilde{q}\}$  satisfies  $\text{rank } \tilde{\bar{p}} \leq \text{rank } \bar{p}$ . Hence,  $\tilde{\bar{p}}$  is a characteristic set of  $J$ , and so

$$\tilde{\bar{p}} = \bar{p} \setminus \{p\} \cup \{\tilde{q}\}.$$

Thus,  $\tilde{\bar{p}}$  is a characteristic presentation of  $I_\Sigma$ . If  $\tilde{q} \neq q$ , then  $\deg \tilde{q} < \deg q$ . If  $\tilde{q} = q$ , then  $\tilde{q}$  has fewer monomials than  $p$  does. Thus, in either case,  $p/\tilde{q} \notin k$ . However, [5, Theorem 3] implies that  $p/\tilde{q} \in k$ , which is a contradiction. This shows that  $\det A \neq 0$ . Thus, the rows of  $A$  are linearly independent.

Let  $r = \text{rank } \text{Wr}(f_1(\bar{a}), \dots, f_s(\bar{a}))$  and the rows  $i_1 = 0, i_2, \dots, i_r$  of the Wronskian be linearly independent. Since the rows of  $A$  form a basis of  $\mathbb{C}\langle \bar{a}_1, \dots, \bar{a}_s \rangle^s$ , there exist rows  $j_1, \dots, j_{s-r}$  of  $A$  such that they together with the rows  $i_1, \dots, i_r$  of the Wronskian form a basis of  $\mathbb{C}\langle \bar{a}_1, \dots, \bar{a}_s \rangle^s$  as well. Hence,

$$B := \begin{pmatrix} f_1(\bar{a}_1) & \dots & f_s(\bar{a}_1) \\ f_1^{(i_2)}(\bar{a}_1) & \dots & f_s^{(i_2)}(\bar{a}_1) \\ \vdots & \ddots & \vdots \\ f_1^{(i_r)}(\bar{a}_1) & \dots & f_s^{(i_r)}(\bar{a}_1) \\ f_1(\bar{a}_{j_1}) & \dots & f_s(\bar{a}_{j_1}) \\ \vdots & \ddots & \vdots \\ f_1(\bar{a}_{j_{s-r}}) & \dots & f_s(\bar{a}_{j_{s-r}}) \end{pmatrix},$$

is invertible. Replacing  $\bar{a}_1, \bar{a}_{j_1}, \dots, \bar{a}_{j_{s-r}}$  in  $\det B$  by the indeterminates  $\bar{w}_1, \dots, \bar{w}_{s-r+1}$ , we obtain a differential polynomial with coefficients in  $\mathbb{C}$  that does not belong to the vanishing ideal of  $\bar{a}_1, \bar{a}_{j_1}, \dots, \bar{a}_{j_{s-r}}$ . Since this ideal is the same

as the vanishing ideal of  $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_{s-r+1}$ , we conclude that the matrix

$$C := \begin{pmatrix} f_1(\bar{a}_1) & \dots & f_s(\bar{a}_1) \\ f_1^{(i_2)}(\bar{a}_1) & \dots & f_s^{(i_2)}(\bar{a}_1) \\ \vdots & \ddots & \vdots \\ f_1^{(i_r)}(\bar{a}_1) & \dots & f_s^{(i_r)}(\bar{a}_1) \\ f_1(\bar{a}_2) & \dots & f_s(\bar{a}_2) \\ \vdots & \ddots & \vdots \\ f_1(\bar{a}_{s-r+1}) & \dots & f_s(\bar{a}_{s-r+1}) \end{pmatrix}$$

is invertible. Thus,

$$\begin{pmatrix} b_1 \\ \vdots \\ b_s \end{pmatrix} = C^{-1} \begin{pmatrix} f_{s+1}(\bar{a}_1) \\ f_{s+1}^{(i_2)}(\bar{a}_1) \\ \vdots \\ f_{s+1}^{(i_r)}(\bar{a}_1) \\ f_{s+1}(\bar{a}_2) \\ \vdots \\ f_{s+1}(\bar{a}_s) \end{pmatrix},$$

which is in  $\mathbb{C}\langle \bar{a}_1, \dots, \bar{a}_{s-r+1} \rangle^s$  and so is  $(s-r+1)$ -experiment identifiable. Thus, the field of IO-identifiable functions is  $N$ -experiment identifiable.  $\square$

## Appendix B. Intersection for rational function fields

In this section, we will describe how [4, Algorithm 2.38] can be used to compute the intersection  $L_1 \cap L_2$ , where  $L_1 = \mathbb{C}(\bar{\mu})$  and  $L_2 = F(\bar{\rho})$ , as required by Algorithm 1.

Algorithm 2 below is a version of [4, Algorithm 2.38]. It was shown [4, p. 37-38] that the output of the algorithm is correct if the algorithm terminates. Termination was proved only if both input fields are algebraically closed in the ambient rational function field. To use the algorithm in our applications, we relax this condition to requiring only one of the fields to be algebraically closed ( $\mathbb{C}(\bar{\mu})$  in  $\mathbb{C}(\bar{\mu}, \bar{x})$ ) in Proposition 27.

---

**Algorithm 2** Intersection of fields (a version of [4, Algorithm 2.38])
 

---

**Input** Tuples  $\bar{f} := (f_1, \dots, f_s)$  and  $\bar{g} := (g_1, \dots, g_\ell)$  such that  $f_1, \dots, f_s, g_1, \dots, g_\ell \in K(\bar{x})$ , where  $\bar{x} := (x_1, \dots, x_n)$ ;

**Output** If terminates, returns generators of  $K(\bar{f}) \cap K(\bar{g})$ .

**Notation:** Introduce new variables  $\bar{X} := (X_1, \dots, X_n)$ . In the algorithm, for a set  $S \subset K(\bar{x})[\bar{X}]$ ,  $\langle S \rangle$  will denote the ideal generated by  $S$  in  $K(\bar{x})[\bar{X}]$ .

**(Step 1)** For every  $1 \leq i \leq s$ , write  $f_i(\bar{x}) = \frac{n_i(\bar{x})}{d_i(\bar{x})}$  so that  $n_i, d_i \in K[\bar{x}]$ , and set  $D(\bar{x}) := d_1 \cdot \dots \cdot d_s$ ;

**(Step 2)** Set  $i := 1$ ,  $I_1 := \langle 1 \rangle$  and

$$J_1 := \langle n_1(\bar{X}) - f_1(\bar{x})d_1(\bar{X}), \dots, n_s(\bar{X}) - f_s(\bar{x})d_s(\bar{X}) \rangle : D(\bar{X})^\infty;$$

**(Step 3)** While  $I_i \neq J_i$  do

- (a)  $I_{i+1} := \langle J_i \cap K(\bar{g})[\bar{X}] \rangle$ ;
- (b)  $J_{i+1} := \langle I_{i+1} \cap K(\bar{f})[\bar{X}] \rangle$ ;
- (c)  $i := i + 1$ ;

**(Step 4)** Compute any reduced Gröbner basis of  $J_i$  and return its coefficients.

---

**Proposition 27** (Termination of Algorithm 2). *In the notation of Algorithm 2, if  $K(\bar{f})$  is algebraically closed in  $K(\bar{x})$  or  $K(\bar{g})$  is algebraically closed in  $K(\bar{x})$ , then Algorithm 2 terminates.*

**Lemma 28.** *Let  $I_0, I_1, \dots, I_s \subset K[\bar{x}]$ , where  $\bar{x} = (x_1, \dots, x_n)$ , be ideals such that  $I_0 = I_1 \cap \dots \cap I_s$ , and let  $L \subset K$  be a subfield. For  $0 \leq j \leq s$ , we define  $J_j$  to be the ideal in  $K[\bar{x}]$  generated by  $I_j \cap L[\bar{x}]$ . Then  $J_0 = J_1 \cap \dots \cap J_s$ .*

*Proof.* Since  $I_0 \cap L[\bar{x}] = (I_1 \cap L[\bar{x}]) \cap \dots \cap (I_s \cap L[\bar{x}])$ , we have  $J_0 \subset J_1 \cap \dots \cap J_s$ .

Now we prove the reverse inclusion. Let  $\{a_\lambda\}_{\lambda \in \Lambda}$  be an  $L$ -basis of  $K$ . Consider  $b \in J_1 \cap \dots \cap J_s$ . We write  $b = \sum_{\lambda \in \Lambda} b_\lambda a_\lambda$ , where  $b_\lambda \in L[\bar{x}]$  for every  $\lambda \in \Lambda$  and only finitely many of them are not zeroes. Consider any  $1 \leq j \leq s$ . Since  $J_j$  has a set of generators with coefficients in  $L$ , the inclusion  $b \in J_j$  implies that  $b_\lambda \in I_j \cap L[\bar{x}]$  for every  $\lambda \in \Lambda$ . Therefore,  $b_\lambda \in I_0 \cap L[\bar{x}]$  for every  $\lambda \in \Lambda$ . Thus,  $b \in J_0$ .  $\square$

*Proof of Proposition 27.* We will assume that  $K(\bar{f})$  is algebraically closed in  $K(\bar{x})$ . The proof for the case of  $K(\bar{g})$  being algebraically closed in  $K(\bar{x})$  is analogous. Assume that the algorithm does not terminate. By the construction,  $I_j \supset J_j$  for every  $j \geq 1$ . The ideals  $I_1$  and  $J_1$  are radical (the latter is due to [4, Definition 2.16 and Proposition 2.21] and since the intersection of a radical ideal with a subring is radical and the extension of a radical ideal is radical). It follows then that all  $I_i$ 's and  $J_i$ 's are radical. For every  $i \geq 1$ , we define  $d_i$  to be the minimum of the dimensions of the prime components  $P$  of  $J_i$  such that  $P \not\supset I_i$ . We will show that the sequence  $d_i$  is strictly increasing thus arriving at a contradiction.

Fix  $i \geq 1$ . Let  $P_1, \dots, P_m$  be the prime components of  $J_i$  so that  $P_1, \dots, P_r$  are the components of the dimension  $< d_i$  and  $P_{r+1}, \dots, P_m$  are the components of the dimension  $\geq d_i$ . By the construction,  $J_i$  is defined over  $K(\bar{f})$ . [4, Proposition 2.37] implies that  $P_1, \dots, P_m$  are also defined over  $K(\bar{f})$ .

Since  $I_i \supset J_i$ , and  $P_1, \dots, P_r$  contain  $I_i$ ,  $P_1, \dots, P_r$  are exactly the prime components of  $I_i$  of dimension  $< d$ , so  $Q := P_1 \cap \dots \cap P_r$  is the intersection of the equidimensional components of  $I_i$  of dimensions  $< d$ . Therefore, since  $I_i$  is defined over  $K(\bar{g})$ ,  $Q$  is defined over  $K(\bar{g})$ . Hence,

$$Q = \langle Q \cap K(\bar{g})[\bar{X}] \rangle = \langle Q \cap K(\bar{f})[\bar{X}] \rangle \supset I_{i+1}. \tag{B.1}$$

Consider

$$C := \{C \mid C \text{ is a prime component of } \langle P_j \cap K(\bar{g})[\bar{X}] \rangle \text{ for } j > r\}$$

[37] implies that, for every  $j > r$ , all prime components of  $\langle P_j \cap K(\bar{g})[\bar{X}] \rangle$  are of the same dimension, so, for all  $C \in \mathcal{C}$ ,  $\dim C \geq d_j$ . For every  $C \in \mathcal{C}$ , denote  $C' := \langle C \cap K(\bar{f})[\bar{X}] \rangle$ . [4, Proposition 2.37] implies that  $C'$  is prime. If  $C \neq C'$ , then  $\dim C' > d_i$ . Otherwise,  $C' = C \supset I_{i+1}$ . Therefore, due to Lemma 28, we have:

$$J_{i+1} = \langle I_{i+1} \cap K(\bar{f})[\bar{X}] \rangle = \underbrace{\left( \langle Q \cap K(\bar{f})[\bar{X}] \rangle \cap \bigcap_{C \in \mathcal{C}, C=C'} C' \right)}_{=:A} \cap \underbrace{\left( \bigcap_{C \in \mathcal{C}, C \neq C'} C' \right)}_{=:B}$$

Since  $\langle Q \cap K(\bar{f})[\bar{X}] \rangle \supset I_{i+1}$  (see (B.1)), we have  $A \supset I_{i+1}$ . Since every component of  $B$  has dimension at least  $d_i + 1$ , we deduce that  $d_{i+1} > d_i$ .  $\square$

### Appendix C. Mathematical discussion for Theorems 11 and 19

**Example 29 (Ranking dependency of  $F(\bar{p})$  in Theorem 11).** We show that the field  $F(\bar{p})$  from Theorem 11 can depend on the ranking although  $\mathbb{C}(\bar{\mu}) \cap F(\bar{p})$  cannot. Consider the following input-output equations

$$p_1 := y_1^2 + y_2^2 + y_3, \quad p_2 := y_2' - 1, \quad p_3 := y_3' - 1.$$

For the elimination differential ranking  $y_1 > y_2 > y_3$ ,  $p_1, p_2, p_3$  is the characteristic presentation of the prime differential ideal  $P := \sqrt{[p_1, p_2, p_3]}$ . A calculation in MAPLE shows that  $F(p_1) = F(p_2) = F(p_3) = \mathbb{C}$ , and so  $F(\bar{p}) = \mathbb{C}$ . However, a calculation in MAPLE shows that  $\bar{q} := \{q_1, q_2, q_3\}$ ,

$$\begin{aligned} q_1 &:= 2y_2 + 2y_1y_1' + 1, \\ q_2 &:= 4y_1^2y_1'^2 + 4y_1y_1' + 4y_1^2 + 4y_3 + 1, \\ q_3 &:= y_3' - 1, \end{aligned}$$

is the characteristic presentation of  $P$  with respect to the elimination differential ranking  $y_2 > y_1 > y_3$  and that  $F(q_2) = \mathbb{C}(y_1y_1' + y_3)$  and  $F(q_1) = F(q_3) = \mathbb{C}$ , and so  $F(\bar{q}) \supsetneq F(\bar{p})$ .

**Example 30 (Achieving the bound in Theorem 19).** A natural mathematical question about a bound is whether it is tight in the sense that the equality can be reached for all the values of the parameters appearing in the bound. We will give an indication of the tightness of the bound from Theorem 19 by providing, for every positive integers  $h \leq n$ , a model with  $n+1$  monomials in the IO-equations and the corresponding Wronskian having rank  $h$  so that every element of the field of IO-identifiable functions is  $(n-h+1)$ -identifiable but not necessarily  $(n-h)$ -identifiable. Fix  $h \leq n$  and consider the system

$$\Sigma = \begin{cases} x_1' = c_1 + \sum_{i=2}^n c_i x_i, \\ x_i^{(h)} = 0, & 2 \leq i \leq h \\ x_i' = 0, & h+1 \leq i \leq n \\ y_i = x_i, & 1 \leq i \leq n \end{cases} \quad (\text{C.1})$$

with unknown parameters  $\{c_i, 1 \leq i \leq n\}$ . By a calculation,

$$\bar{p} = \left\{ y_1' - c_1 - \sum_{i=2}^n c_i y_i, y_i^{(h)}, 2 \leq i \leq h, y_i', h+1 \leq i \leq n \right\}$$

is a set of IO-equations of (C.1). We have modulo  $I_\Sigma$ :

$$\text{Wr}(y_2, \dots, y_n, 1) = \begin{pmatrix} y_2 & \dots & y_h & y_{h+1} & \dots & y_n & 1 \\ y_2' & \dots & y_h' & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ y_2^{(h-1)} & \dots & y_h^{(h-1)} & 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 \end{pmatrix},$$

whose rank is  $r_1$ . On the one hand  $r_1 \leq h$  because the matrix has only  $h$  non-zero rows. On the other hand,  $\det \text{Wr}(y_2, \dots, y_h, 1) \notin I_\Sigma$  since  $\text{Wr}(y_2, \dots, y_h, 1)$  is not reducible (to zero) by  $\bar{p}$ . Thus,  $r_1 = h$ . Also,  $s_1 = n$  and, for all  $i \geq 2$ ,  $s_i = 0$ . So, by Theorem 19, for all

$$N \geq s_1 - r_1 + 1 = n - h + 1,$$

the field of IO-identifiable functions  $\mathbb{C}(c_1, \dots, c_n)$  is  $N$ -experiment identifiable. We will show that it is not  $(n - h)$ -experiment identifiable, thus showing the desired tightness of the bound in Theorem 19. For this, consider the following set of IO-equations for the  $(n - h)$ -experiment system  $\Sigma_{n-h}$ :

$$\bigcup_{j=1}^{n-h} \left\{ y_{j,1}' - c_1 - \sum_{i=2}^n c_i y_{j,i}, \begin{array}{l} y_{j,i}^{(h)}, 2 \leq i \leq h \\ y_{j,i}', h+1 \leq i \leq n \end{array} \right\}$$

Let  $a_{j,i}$  denote the image of  $y_{j,i}$  modulo  $I_{\Sigma_{n-h}}$ . Since, for all  $i$  and  $j$ ,  $h+1 \leq i \leq n$ ,  $1 \leq j \leq n-h$ ,  $a_{j,i}$  is constant, we can define a differential field automorphism  $\varphi$  of  $\mathbb{C}\langle \bar{a}_1, \dots, \bar{a}_{n-h} \rangle(c_1, \dots, c_n)$  over  $\mathbb{C}\langle \bar{a}_1, \dots, \bar{a}_{n-h} \rangle$  by

$$\varphi(c_1, c_2, \dots, c_h, c_{h+1}, \dots, c_n) := (c_1 + b_{n-h+1}, c_2, \dots, c_h, c_{h+1} + b_1, \dots, c_n + b_{n-h}),$$

where  $(b_1, \dots, b_{n-h+1}) \in \mathbb{C}\langle a_{j,i} \mid 1 \leq j \leq n-h, h+1 \leq i \leq n \rangle$  is a non-zero linear dependence among the columns of the  $(n-h) \times (n-h+1)$  matrix

$$\begin{pmatrix} a_{1,h+1} & \dots & a_{1,n} & 1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{n-h,h+1} & \dots & a_{n-h,n} & 1 \end{pmatrix}.$$

Thus, there exists  $i \in \{1, h+1, \dots, n\}$  such that  $c_i \notin \mathbb{C}\langle \bar{a}_1, \dots, \bar{a}_{n-h} \rangle$ , and so the IO-identifiable parameter  $c_i$  is not  $(n-h)$ -experiment identifiable.

#### Appendix D. Computing an optimal representation (5) in Theorem 19

In this section, we prove Lemma 31 providing a sufficient condition for a decomposition (5) to yield the optimal (compared to other decompositions) bound in Theorem 19. Then we give Algorithm 3 to compute such a decomposition, which basically computes an LU-decomposition of a matrix in the language of polynomials (see the proof of Lemma 31).

**Lemma 31.** *Let  $p(\bar{z}) \in \mathbb{C}(\bar{\mu})\{\bar{z}\}$  be a differential polynomial over a constant field  $\mathbb{C}(\bar{\mu})$  in  $\bar{z} = (z_1, \dots, z_n)$ , where  $\bar{\mu} = (\mu_1, \dots, \mu_m)$  are transcendental constants. Let  $I \subset \mathbb{C}(\bar{\mu})\{\bar{z}\}$  be a prime differential ideal containing  $p$ . Consider two representations of  $p$*

$$p = f_{s+1} + \sum_{j=1}^s c_j f_j \quad \text{and} \quad p = \tilde{f}_{\tilde{s}+1} + \sum_{j=1}^{\tilde{s}} \tilde{c}_j \tilde{f}_j$$

*such that  $f_1, \dots, f_{s+1}, \tilde{f}_1, \dots, \tilde{f}_{\tilde{s}+1} \in \mathbb{C}\{\bar{z}\}$ ,  $c_1, \dots, c_s, \tilde{c}_1, \dots, \tilde{c}_{\tilde{s}} \in \mathbb{C}(\bar{\mu})$ ,  $f_1, \dots, f_{s+1}$  are  $\mathbb{C}$ -linearly independent, and  $1, c_1, \dots, c_s$  are  $\mathbb{C}$ -linearly independent. We define  $r$  and  $\tilde{r}$  to be the ranks of  $\text{Wr}(f_1, \dots, f_s)$  and  $\text{Wr}(\tilde{f}_1, \dots, \tilde{f}_{\tilde{s}})$  modulo  $I$ , respectively. Then*

$$s - r \leq \tilde{s} - \tilde{r} \quad \text{and} \quad s \leq \tilde{s}.$$

*Proof.* Viewing  $\mathbb{C}(\bar{\mu})\{\bar{z}\}$  as a tensor product of  $\mathbb{C}$ -vector spaces  $\mathbb{C}(\bar{\mu}) \otimes_{\mathbb{C}} \mathbb{C}\{\bar{z}\}$ , we can consider  $p$  as an element of this tensor product. Then the linear independence of  $1, c_1, \dots, c_s$  and of  $f_1, \dots, f_{s+1}$  implies that

$$1 \otimes f_{s+1} + c_1 \otimes f_1 + \dots + c_s \otimes f_s$$

is a full-rank factorization of  $p$  [39, Theorem 3.13]. Since  $1 \otimes \tilde{f}_{\tilde{s}+1} + \tilde{c}_1 \otimes \tilde{f}_1 + \dots + \tilde{c}_{\tilde{s}} \otimes \tilde{f}_{\tilde{s}}$  is another rank-one factorization of the same tensor, the proof of [39, Theorem 3.13] implies that  $1, c_1, \dots, c_s$  belong to the  $\mathbb{C}$ -span of  $1, \tilde{c}_1, \dots, \tilde{c}_{\tilde{s}}$  and  $f_1, \dots, f_{s+1}$  belong to the  $\mathbb{C}$ -span of  $\tilde{f}_1, \dots, \tilde{f}_{\tilde{s}+1}$ . The former inclusion implies  $s \leq \tilde{s}$ . The latter implies that there exists a full-rank  $\mathbb{C}$ -matrix  $M$  such that  $(f_1, \dots, f_{s+1}) = (\tilde{f}_1, \dots, \tilde{f}_{\tilde{s}+1})M$ . Therefore, any nontrivial linear dependence of the images of  $f_1, \dots, f_{s+1}$  in  $\mathbb{C}(\bar{\mu})\{\bar{z}\}/I$  over the constants of the fraction field of  $\mathbb{C}(\bar{\mu})\{\bar{z}\}/I$  yields (after multiplying by  $M$ ) such a relation for the images of  $\tilde{f}_1, \dots, \tilde{f}_{\tilde{s}+1}$ . Therefore, the proof of Lemma 26 implies that the corank of  $\text{Wr}(f_1, \dots, f_s)$  modulo  $I$ ,  $r - s$ , does not exceed the corank of  $\text{Wr}(\tilde{f}_1, \dots, \tilde{f}_{\tilde{s}})$  modulo  $I$ ,  $\tilde{r} - \tilde{s}$ .  $\square$

---

**Algorithm 3** Computing optimal representation for Theorem 19

---

**Input** a monic polynomial  $p(\bar{x}) \in \mathbb{C}(\bar{\mu})[\bar{x}]$  (see Definition 5), where  $\bar{x} = (x_1, \dots, x_n)$  and  $\bar{\mu} = (\mu_1, \dots, \mu_m)$  are independent indeterminates;

**Output** A representation of  $p$  of the form

$$p = f_{s+1} + \sum_{j=1}^s c_j f_j$$

in which  $f_1, \dots, f_{s+1} \in \mathbb{C}[\bar{x}]$  are  $\mathbb{C}$ -linearly independent and  $1, c_1, \dots, c_s \in \mathbb{C}(\bar{\mu})$  are  $\mathbb{C}$ -linearly independent.

Fix an arbitrary ordering on the monomials in  $\bar{\mu}$ . The leading monomial and leading coefficient of a polynomial  $f$  w.r.t. this ordering will be denoted by  $\text{lm } f$  and  $\text{lc } f$ , respectively.

**(Step 1)** Compute the LCM  $q(\bar{\mu}) \in \mathbb{C}[\bar{\mu}]$  of the denominators of the coefficients of  $p$ . Set  $P(\bar{\mu}, \bar{x}) := q \cdot p \in \mathbb{C}[\bar{\mu}, \bar{x}]$ .

**(Step 2)** Write  $P$  as  $\sum_{i=1}^{\ell} C_i(\bar{\mu})M_i(\bar{x})$ , where  $M_1, \dots, M_{\ell}$  are distinct monomials in  $\bar{x}$  and  $C_1, \dots, C_{\ell} \in \mathbb{C}[\bar{\mu}]$ , and  $C_1 = q$  (possible since  $p$  is monic).

**(Step 3)** Let  $S$  be a list of pairs from  $\mathbb{C}[\bar{\mu}] \times \mathbb{C}[\bar{x}]$  initialized to be empty.

**(Step 4)** For every  $i = 1, \dots, \ell$ , do

(a) for every  $(A, B) \in S$ , where  $A \in \mathbb{C}[\bar{\mu}], B \in \mathbb{C}[\bar{x}]$

$$C_i := C_i - \frac{c}{\text{lc}(A)}A, \quad B := B + \frac{c}{\text{lc}(A)}M_i, \tag{D.1}$$

where  $c$  is the coefficient in front of  $\text{lm}(A)$  in  $C_i$ .

(b) if  $C_i \neq 0$ , append  $(C_i, M_i)$  to  $S$ .

**(Step 5)** Let  $S = [(A_0, B_0), (A_1, B_1), \dots, (A_s, B_s)]$ . Return  $f_{s+1} = B_0$  and  $f_i = B_i$  and  $c_i = \frac{A_i}{q}$  for every  $1 \leq i \leq s$ .

---

**Lemma 32.** *Algorithm 3 is correct.*

*Proof.* First we will show that  $p = \sum_{i=1}^s \frac{A_i}{q} B_i + B_0$ . By the construction, we will have  $A_0 = Q$ , so this is equivalent to proving  $p = \sum_{i=0}^s \frac{A_i}{q} B_i$ . To prove this, we observe that the transformation (D.1) preserves the value

$$\sum_{(A,B) \in S} A \cdot B + C_i M_i.$$

Therefore, after the  $i$ -th iteration of the loop in **(Step 4)**, the value  $\sum_{(A,B) \in S} AB$  is increased by  $C_i M_i$ . Since it starts with zero, it will be equal to  $\sum_{j=1}^{\ell} C_j M_j = P$  after **(Step 4)**. Therefore,  $\sum_{i=0}^s \frac{A_i}{q} B_i = \frac{P}{q} = p$ .

To prove the  $\mathbb{C}$ -linear independence of  $B_j$ 's, for each  $1 \leq j \leq s$ , consider the pair  $(C_i, M_i)$  that was the  $j$ -th appended pair for **(Step 4)b)**. Then  $M_i$  will not appear in any of  $B_{j+1}, \dots, B_s$ , so  $B_1, \dots, B_s$  are  $\mathbb{C}$ -linearly independent.

The linear independence of  $A_0, \dots, A_s$  follows from the fact that,  $\text{Im}(A_j)$  does not appear in  $A_{j+1}, \dots, A_s$  for every  $0 \leq j \leq s$ , and this property is due to the reduction procedure **(D.1)**.  $\square$