



**HAL**  
open science

# Functional Diagnosability of Possibly Uncertain Systems

Carine Jauberthie, Nathalie Verdière, Louise Travé-Massuyès

► **To cite this version:**

Carine Jauberthie, Nathalie Verdière, Louise Travé-Massuyès. Functional Diagnosability of Possibly Uncertain Systems. *IEEE Control Systems Letters*, 2024, 8, pp.2181-2186. 10.1109/LC-SYS.2024.3456230 . hal-04703936

**HAL Id: hal-04703936**

**<https://laas.hal.science/hal-04703936v1>**

Submitted on 29 Oct 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.

# Functional diagnosability of possibly uncertain systems

Carine Jauberthie, Nathalie Verdière, Louise Travé-Massuyès

**Abstract**—Diagnosability is a crucial attribute of systems and their instrumentation, ensuring that specified faults can be uniquely identified using the available sensors. In a model-based context, diagnosability is evaluated through analytical redundancy relations derived from the model by eliminating unknown variables. These relations, evaluated from sensor data, yield residuals, which indicate the system's normal or faulty state. Ideally, residuals exhibit distinct values for different faults, generating unique fault signatures that facilitate fault discrimination and affirm system diagnosability.

This paper presents a sufficient condition for the functional diagnosability of nonlinear dynamical systems, based on the functional linear independence of fault signatures. Unlike conventional diagnosability analysis, which focuses on residuals evaluated in a binary manner, 0 when not sensitive to a fault and 1 otherwise, functional diagnosability emphasizes the system's behavior by evaluating the functional expressions of residuals defined as functional fault signatures. Evaluated from sensor data, functional signatures allow for an analysis of the whole residual trajectories. This advantageously increases the discriminating power. This approach leverages the symbolic framework of differential algebra, accommodating both deterministic and bounded uncertain systems without the need for a set-membership framework.

**Index Terms**—Diagnosability, nonlinear dynamical systems, uncertain systems, fault functional signatures, functional linear independence, differential algebra.

## I. INTRODUCTION

Verifying diagnosability is an important task to be carried out before putting a system into operation. Diagnosability guarantees that the set of measures delivered by the available sensors can be processed into an appropriate set of symptoms that discriminate different faulty situations. This property must be checked in the design phase so that the designer knows beforehand which faults the diagnoser will be able to discriminate during the operational life of the system. Although diagnosability analysis has been a topic of research for a long time in the diagnostic community [6], [12], [17], [19], [21], this theme is still active today and is giving rise to new results in both model-based and data-based frameworks [5], [9]–[12].

In a model-based framework, diagnosability is evaluated through analytical redundancy relations (ARRs) derived from

the model by eliminating unknown variables. These relations, evaluated from sensor data, yield residuals, which indicate the system's normal or faulty state. Residuals possess both computational and internal forms, with only the internal form explicitly reflecting the impact of different faults. Ideally, residuals exhibit distinct values for different faults, generating unique fault signatures that facilitate fault discrimination and affirm system diagnosability.

Unlike conventional diagnosability analysis, which focuses on residuals evaluated from their computational form in a binary manner, 0 when not sensitive to a fault and 1 otherwise, functional diagnosability introduced in [22] emphasizes the system's behavior through the formal internal form of residuals under various faults, defined as functional fault signatures. Evaluated from sensor data, functional signatures allow for an analysis of the whole residual trajectories, which advantageously increases the discriminating power.

A sufficient condition for functional diagnosability was previously proved as the identifiability of the faults modeled as additional parameters impacting the system's behavior [22]. A drawback of this approach is its sensitivity to experimental conditions, particularly to the class of admissible input functions applied to the system. The approach assumes persistently exciting inputs [18]. Indeed, input functions that fail to sufficiently "excite" the system may prevent to determine certain faults. Consequently, a requirement is that the class of admissible inputs includes such persistently exciting functions.

Hence, the fault parameter identifiability condition offers a sufficient condition for functional diagnosability, though it can be overly restrictive in certain cases.

This paper provides a new sufficient condition for functional diagnosability of non linear possibly uncertain dynamical systems. The approach relies on ARRs, obtained through variable elimination theory in the context of differential algebra, and leverages the fact that each ARR is sensitive to different subsets of faults. It considers functional fault signatures defined from the formal internal form of residuals under various faults, and states a condition based on their linear functional independence. In addition to being simpler to implement than the identifiability condition, this approach has several advantages: first, functional signatures, evaluated from sensor data, allow for a time-based analysis; second, it accommodates both deterministic and bounded uncertain systems without requiring a set-membership framework.

This paper is organized as follows: Section II formulates the problem, Section III presents functional diagnosability and the different concepts attached to it. Section IV develops the

C. Jauberthie and L. Travé-Massuyès are with LAAS-CNRS, Université de Toulouse, CNRS, UPS, 7 avenue du Colonel Roche, 31400 Toulouse, France.

N. Verdière is with University of Normandie, UNIHAVRE, LMAH, FR-CNRS-3335, ISCN, 76600, Le Havre, France  
(Corresponding author: carine.jauberthie@laas.fr).

results that lead to the new condition of functional diagnosability. The Bernoulli equation is issued as a running example, then Section V illustrates the method with a two water tanks model. Finally, Section VI concludes the paper and draws perspectives for future work.

## II. PROBLEM FORMULATION

The systems considered are possibly uncertain, in which case their parameters and initial state are set-valued and bounded (in intervals in this paper). Let us denote the set of real intervals by  $\mathbb{IR} \triangleq \{\underline{x}, \bar{x} : \underline{x}, \bar{x} \in \mathbb{R}, \underline{x} \leq \bar{x}\}$  and the set of  $k$ -dimensional real interval vectors by  $\mathbb{IR}^{k1}$ . The considered systems are of the following form in which a fault vector  $f$  has been explicitly introduced:

$$\begin{cases} \dot{x}(t) = g(x(t), u(t), f, p), & x(t_0) = x_0, \\ y(t) = h(x(t), u(t), f, p), \end{cases} \quad (1)$$

where  $x(t) \in \mathbb{IR}^n$ ,  $y(t) \in \mathbb{IR}^m$  denote the state variables and the outputs, respectively and  $u(t) \in \mathbb{IR}^l$  is the input vector, which may be equal to 0 in case of an uncontrolled system.  $p$  denotes the interval parameter vector included in a connected set  $P \subset \mathcal{U}_p$ , where  $\mathcal{U}_p$  is an open set of  $\mathbb{IR}^p$ .  $f$  is the fault vector such that  $f \subset \mathcal{F}_{SYS} \subset \mathbb{IR}^e$ , where  $\mathcal{F}_{SYS}$  is an exhaustive set defining the fault domain. This means that faults may also suffer uncertainty, in which case their magnitude is represented by a bounded set of nonzero measure and the faults are called "bounded faults" [14]. Let us denote by  $f_j$  the  $j$ th component of the fault vector  $f$  and by  $f^j$  the vector derived from  $f$  by setting all the components equal to zero except the  $j$ th component.

The functions  $g$  and  $h$  are interval nonlinear functions and can be viewed as two families of real functions, each of them being real, rational and analytic <sup>2</sup> in  $x$ ,  $u$ ,  $f$  and  $p$  on an open set  $M$  of  $\mathbb{R}^n$  such that for all  $\tilde{x}(t) \in \mathbb{R}^n$ , if  $\tilde{x}(t) \in x(t)$ , then  $\tilde{x}(t) \in M$  for every  $t \in [t_0, T]$ .

The set of outputs, solution of (1) with input  $u$  (resp. without input), parameter vector  $p$ , and fault vector  $f$ , is denoted  $y(p, f, u)$  (resp.  $y(p, f)$ ), where the dependency on time is omitted to lighten the notations.

Given that real numbers can be considered as degenerated intervals, note that (1) may as well represent a deterministic system (no uncertainty) or a system of which some but not all quantities are uncertain.

This paper seeks to analyse diagnosability for the class of systems of the form (1). In other words, the goal is to assess whether two faults  $f_i$  and  $f_j$  are diagnosable or not, i.e., whether the input-output behavior of the system allows us to discriminate the two faulty situations. We also want to check whether the system as a whole is diagnosable, i.e., whether all the considered faults forming the vector  $f$  are mutually diagnosable. For this purpose, we propose to rely on functional diagnosability as introduced in [22], for

<sup>1</sup>A  $k$ -dimensional real interval vector is a vector whose components are real intervals. Each component interval represents a range of possible values within the real numbers, thus defining a multi-dimensional box or hyperrectangle in the  $k$ -dimensional space.

<sup>2</sup>This assumption is not restrictive since lots of models can be reduced to a rational and analytical model by a change of variables [1].

it advantageously increases the discriminating power versus standard diagnosability.

## III. FUNCTIONAL DIAGNOSABILITY

This section summarizes the notion of functional diagnosability which is defined thanks to the functional signatures of the faults [22]. As detailed below, functional signatures are defined from a set of residuals that can be generated from analytical redundancy relations (ARRs).

### A. Analytical Redundancy Relations

For any vector  $\vartheta$ , let us define  $\tilde{\vartheta}$  as the vector composed of  $\vartheta$  and its time derivatives up to some (unspecified) order. An ARR is a relation of the form  $w_i(\tilde{y}, \tilde{u}, f, p) = 0$  deduced from the model of the system by eliminating unknown variables, i.e., state variables  $x(t)$ .

According to the assumptions on the system functions  $g$  and  $h$  and using an elimination algorithm with a specific order, ARRs can be put in the following form [20], [22]:

$$\begin{aligned} w_i(\tilde{y}, \tilde{u}, f, p) &= m_{0,i}(\tilde{y}, \tilde{u}, p) - \sum_{k=1}^{n_i} \gamma_k^i(f, p) m_{k,i}(\tilde{y}, \tilde{u}) \\ &= w_{0,i}(\tilde{y}, \tilde{u}, p) - w_{1,i}(\tilde{y}, \tilde{u}, f, p) = 0 \end{aligned} \quad (2)$$

where  $i$  is an index identifying the ARR,  $(\gamma_k^i(f, p))_{1 \leq k \leq n_i}$  are rational in  $f$  and  $p$ ,  $\gamma_v^i \neq \gamma_w^i$  ( $v \neq w$ ) and  $(m_{k,i}(y, u))_{1 \leq k \leq n_i}$  are differential polynomials with respect to  $\tilde{y}$  and  $\tilde{u}$ . Let  $r_i = w_{0,i}(\tilde{y}, \tilde{u}, p)$ , where  $r_i$  is called the *residual* and  $w_{0,i}(\tilde{y}, \tilde{u}, p)$ , which is fault-free, is the *residual computation form*. It only involves known variables and can be evaluated from sensor data.  $w_{1,i}(\tilde{y}, \tilde{u}, f, p)$ , which depends on the faults, is the *residual internal form*.

From (2), the following is always true:

$$w_{0,i}(\tilde{y}, \tilde{u}, p) = w_{1,i}(\tilde{y}, \tilde{u}, f, p) \quad (3)$$

In the ideal case of no noise nor disturbances, when no fault is acting on the system, i.e.,  $f = 0$ ,  $w_{1,i}(\tilde{y}, \tilde{u}, 0, p) = 0$  and hence, from (3) the residual  $r_i = w_{0,i}(\tilde{y}, \tilde{u}, p) = 0$  for any triple  $(\tilde{y}, \tilde{u}, p)$  that satisfies (1).

ARRs can be designed to react to different faults and this is why, when put together, the corresponding residuals can provide a different signature for every fault. ARRs can hence be used to detect, isolate, and estimate a fault acting on the system [13], [22].

The polynomials  $w_i(\tilde{y}, \tilde{u}, f, p)$  are input-output polynomials that can be obtained using elimination theory. In the last decade, algorithms have been developed and implemented in softwares like Maple [3]. They are based on differential algebra [16] and the procedure consists in eliminating unknown state variables from the model in order to obtain the ARRs.

*Example 3.1:* Consider the Bernoulli equation:

$$\dot{y}(t) = \beta_1 y(t) + \beta_2 y(t)^2, \quad \text{for } t \in [0, 10], \quad y(0) = -1 \quad (4)$$

whose solution is  $y(t) = \frac{\beta_1 e^{\beta_1 t}}{\beta_2 - \beta_1 - \beta_2 e^{\beta_1 t}}$ .

The residual computational form reads:  $w_{0,1}(\tilde{y}, p) = \dot{y}(t) - \beta_1 y(t) - \beta_2 y(t)^2$ . If some positive single faults  $f_1$  and  $f_2$  impact additively the two parameters  $\beta_1$  and  $\beta_2$  respectively, then the residual internal form is:  $w_{1,1}(\tilde{y}, f, p) = f_1 y(p, f) + f_2 y(p, f)^2$  where  $p = (\beta_1, \beta_2)^T$ ,  $f = (f_1, f_2)^T$  ( $T$  denotes the transpose operation).

## B. Signature and functional signature of a fault

Formally speaking, the *signature* of a fault is a function  $Sig$  which associates to a fault a set of indicators corresponding to the residuals associated to the ARR's being used. The internal form of the residuals indicates which faults should activate which residuals.

*Definition 3.1 (Signature of a fault):* Assume that  $m$  ARR's are used, then the fault signature  $Sig(f_j)$  of  $f_j$  is the binary  $m$ -vector where the  $i^{th}$  component of the  $f_j$ 's signature is evaluated "1" when the fault  $f_j$  may act on the residual  $r_i$ , otherwise it is evaluated 0.

Classically, residual vectors are binary and two faults are said *diagnosable* if their signatures are different. A system is qualified *diagnosable* if all the fault signatures are pairwise different [6]. To increase the discrimination power, [22] has proposed the concept of *functional signature*. The functional signature of a fault is a function  $FSig$  which associates to  $f_j$  the vector formed by the internal form of the  $m$  residuals by considering that only the fault  $f_j$  is acting on the system.

*Definition 3.2 (Functional signature of a fault):* The functional signature  $FSig(f_j)$  of a fault  $f_j$  is the vector whose  $i$ th component is  $w_{1,i}(\tilde{y}, \tilde{u}, f^j, p)$ , that is the polynomial obtained from  $w_{1,i}(\tilde{y}, \tilde{u}, f, p)$  by considering all the components of  $f$  equal to zero but the  $j$ th component equal to  $f_j$ .

$FSig(f_j)$  is a vector of functions of the form (cf. (2):

$$FSig(f_j) = \left( \sum_{k=1}^{n_i} \gamma_k^i(f_j, p) m_{k,i}(\tilde{y}, \tilde{u}) \right)_{i=1, \dots, m}.$$

Comparing functional signatures hence accounts for comparing functional vectors. This comparison is of course finer than comparing classical binary fault signatures as defined in Definition 3.1, hence higher diagnosability power is obtained.

The  $i^{th}$  component of  $FSig(f_j)$ , which corresponds to an interval function, is written  $FSig_i(f_j)$ .  $FSig_i(f_j)$  consists of a set of trajectories generated in the presence of  $f_j$  and can be viewed as a tube of trajectories, or an envelope, on the time interval  $[t_0, T]$ . Note that if  $f_j$  is reduced to a real number,  $FSig_i(f_j)$  is composed of one single trajectory. The term *functional signature* is used independently of the bounded nature of the fault.

(Functional) fault signatures can be collected in a table, called the *(functional) signature matrix*, for which the cell intersecting the  $i^{th}$  line and  $j^{th}$  column contains the  $i^{th}$  residual for the fault  $f_j$ , i.e.,  $r_i(f_j) = w_{1,i}(\tilde{y}, \tilde{u}, f^j, p)$  [14].

*Example 3.2:* Continuing the Bernoulli equation example, the functional signatures are constructed based on the internal form of the residual. From  $w_{1,1}(\tilde{y}, f, p)$ , we get  $FSig(f_1) = f_1 y(p, f_1)$  and  $FSig(f_2) = f_2 y(p, f_2)^2$ . Each functional signature defines a set of trajectories when  $t \in [t_0, T]$ . For uncertain systems, in particular when  $f_1$  and  $f_2$  are bounded, functional fault signature discriminability is not straightforward and meets three possible cases, as illustrated by the following numerical examples.

Let us consider the time interval  $[0, T] = [0, 10]$  and assume that  $f_1$  and  $f_2$  occur at time point  $t_f = 4.6$  seconds. In this scenario, let us assume that  $f_1$  has interval value  $[0.5, 1]$  and  $f_2$  has interval value  $[0.55, 0.6]$  for the three following cases.

- Case 1: for  $\beta_1 = 0.5$ , and  $\beta_2 = -0.2$ , the intersection of  $FSig(f_1)$  and  $FSig(f_2)$  is empty on the interval  $]4.6; 10]$ , as shown in Figure 1a.
- Case 2: for  $\beta_1 = 0.5$ , and  $\beta_2 = -0.3$ , the intersection of  $FSig(f_1)$  and  $FSig(f_2)$  is not empty on the time interval  $]4.6; 10]$ , as shown in Figure 1b.
- Case 3: for  $\beta_1 = 0.5$ , and  $\beta_2 = -0.35$ ,  $FSig(f_2)$  is included in  $FSig(f_1)$  on the time interval  $]4.6; 10]$ , as shown in Figure 1c.

Note that in the classical sense, this model is not diagnosable because the signatures of  $f_1$  and  $f_2$  are both equal to 1 (the residuals are non zero for the two faulty situations). However, case 1 and case 2 show that  $f_1$  and  $f_2$  can be discriminated, what can be assessed by functional diagnosability.

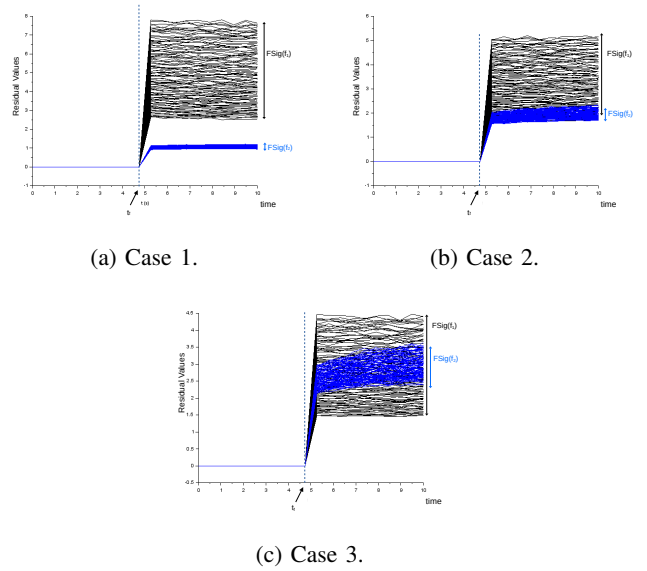


Fig. 1: Three cases for the Bernoulli equation example illustrating disjoint, intersecting and included fault signature trajectory sets.

The above scenario illustrates three possible cases of fault functional diagnosability whose formal definitions are given in the following section.

## C. Diagnosability and functional diagnosability

Several definitions of diagnosability have been proposed around the use of ARR's. The classical diagnosability definition is based on binary residual fault signatures. Two faults  $f_i$  and  $f_j$  are diagnosable if they have different fault signatures [6].

[7] considers that a system is diagnosable if each fault  $f_j$  can be written as the solution of a polynomial equation in  $f_j$  and a finite number of time derivatives of inputs and outputs. This definition is close to the one of identifiability proposed in [18]. However, the definition of diagnosability proposed in [7] is based on obtaining particular differential polynomials which may require many manipulations of the model equations. In case of complex models, it is often impossible to obtain such polynomials even using dedicated symbolic software. Furthermore, the order of derivatives is so high that they are



hardly suitable in practice.

In [22], the authors propose to relax the constraints of [7] and to use ARRs involving one or more faults for studying diagnosability, the advantage being to obtain ARRs with derivatives of lower order. Obtaining such ARRs is based on the work of [8]. In practice, ARRs are obtained from the Rosenfeld-Groebner algorithm implemented in Maple [3]. The definition of functional diagnosability as proposed in [22] is based on these particular ARRs. It was shown that, if a deterministic model is identifiable with respect to the faults, then the residuals of the ARRs forming the *functional signature* have distinct trajectories.

In the general case of bounded faults, one must deal with sets of trajectories or *tubes*. Distinguishing sets of trajectories leads to the following definition of functional diagnosability and strong-functional diagnosability.

*Definition 3.3:* Two faults  $f_1$  and  $f_2$  are *functionally diagnosable* over the time interval  $[t_0, T]$  if  $FSig(f_1)$  and  $FSig(f_2)$  are distinct in the sense that there exists at least one component  $i^*$  and a time interval  $[t_1, t_2] \subseteq [t_0, T]$  such that for all  $t \in [t_1, t_2]$ ,  $FSig_{i^*}(f_1) \not\subseteq FSig_{i^*}(f_2)$  or  $FSig_{i^*}(f_2) \not\subseteq FSig_{i^*}(f_1)$ . If in addition  $FSig_{i^*}(f_1) \cap FSig_{i^*}(f_2) = \emptyset$ ,  $f_1$  and  $f_2$  are *strongly functionally diagnosable* over  $[t_0, T]$ .

Definition 3.3 means that, if a functional signature is included in another, the faults cannot be distinguished. Otherwise, if the two sets of trajectories defined by the functional signatures do not intersect, the two faults are strongly functionally diagnosable. The ambiguous case is when they strictly intersect, in which case the two faults are just functionally diagnosable. Definition 3.3 gives a numerical way to detect faults in a bounded context.

*Definition 3.4:* The model (1) is (strongly) functionally diagnosable over the time interval  $[t_0, T]$  for  $\mathcal{F}_{SYS}$  if any two faults  $f_1, f_2 \subseteq \mathcal{F}_{SYS}$  are (strongly) functionally diagnosable over  $[t_0, T]$ .

*Example 3.3:* Consider again the Bernoulli equation example.

- In case 1,  $f_1$  and  $f_2$  are strongly functionally diagnosable since  $FSig(f_1) \cap FSig(f_2) = \emptyset$  over the time interval  $]4.6, 10]$ .
- In case 2,  $f_1$  and  $f_2$  are functionally diagnosable since  $FSig(f_1) \cap FSig(f_2) \neq \emptyset$ ,  $FSig(f_1) \not\subseteq FSig(f_2)$ , and  $FSig(f_2) \not\subseteq FSig(f_1)$  over the time interval  $]4.6, 10]$ .
- In case 2,  $f_1$  and  $f_2$  are not functionally diagnosable since  $FSig(f_2) \subset FSig(f_1)$  over the time interval  $]4.6, 10]$ .

Detectability is a specific form of diagnosability that only requires the ability to distinguish a fault from the absence of faults. Functional detectability can hence also be defined based on functional signatures as follows.

*Definition 3.5:* The fault  $f_j$  is functionally detectable if the functional signature  $FSig(f_j)$  is not equal to the null vector over  $[t_0, T]$ .

Definition 3.4 is given for uncontrolled systems. If the system is controlled, i.e.,  $u(t) \neq 0$ , we can distinguish the case in which the property is true for at least one input or for all inputs. The faults  $f_1$  and  $f_2$  are said (strongly) *input-functionally diagnosable*. The distinction between (strongly) functionally

detectable and (strongly) *input-functionally detectable* faults can also be done.

#### IV. A NEW CONDITION FOR FUNCTIONAL DIAGNOSABILITY

This section presents a theoretical result for determining the functional diagnosability of potentially bounded faults based on the formal expressions of functional signatures, which are actually the observable manifestations of faults.

Functional signatures  $FSig(f_j), j \in [1, e]$  are function vectors where each component  $FSig_i(f_j), i \in [1, m]$ , represents the  $i$ -th residual internal form among the  $m$  considered residuals, assuming that only the fault  $f_j$  is affecting the system.

*Proposition 4.1:* Two faults  $f_i$  and  $f_j, f_i \neq f_j$  are functionally diagnosable over the time interval  $[t_0, T]$  if there exists at least one  $k$  such that the components  $k$  of their functional signatures, i.e.,  $FSig_k(f_i)$  and  $FSig_k(f_j)$ , are linearly functionally independent over  $[t_0, T]$ .

*Proof–* By contrapositive, it is clear that if two distinct faults are not functionally diagnosable, all the components of their functional signatures are equal over the time interval  $[t_0, T]$  and consequently, all the components of their functional signatures are linearly functionally dependent on some subinterval of  $[t_0, T]$ .

In the following, we leverage the fact that linear functional independence of vectors is implied by linear functional independence of at least one of their components. When we talk about the functional independence of a vector, it will be in relation to one of its components, in particular with regard to fault signatures.

The following proposition links the functional linear independence of any two fault signatures with model diagnosability.

*Proposition 4.2:* If the functional signatures of any couple of faults are linearly functionally independent over the time interval  $[t_0, T]$ , then the model is functionally diagnosable over the time interval  $[t_0, T]$ .

*Proof–* Functional linear independence of any two fault signatures over  $[t_0, T]$  implies, by Proposition 4.1, that any pair of faults is functionally diagnosable over  $[t_0, T]$ . By definition, the model is then functionally diagnosable over  $[t_0, T]$ .

It has been shown that a set of differentiable functions is linearly independent on a time interval if their Wronskian does not vanish identically [2]. In addition, linear independence of a set of functions implies that the functions are pairwise linearly independent, which is, from Propositions 4.1 and 4.2, the condition sought to prove the functional diagnosability of the system.

*Definition 4.1:* Consider a set of faults  $\mathcal{F} \subseteq \mathcal{F}_{SYS}, |\mathcal{F}| \geq 2$  and the functions given by the  $i$ th component  $FSig_i(\mathcal{F})$  of their fault signatures, and define the Wronskian  $W_i(\mathcal{F})$  as the determinant constructed by placing the functions  $FSig_i(f_j), f_j \in \mathcal{F}$ , in the first row and the 1-st to the  $(|\mathcal{F}| - 1)$ -th derivatives of the functions in the subsequent

rows, thus forming the square matrix:

$$\begin{vmatrix} FSig_i(f_1) & \dots & \dots & FSig_i(f_{|\mathcal{F}|}) \\ FSig_i(f_1)' & \dots & \dots & FSig_i(f_{|\mathcal{F}|})' \\ \vdots & \vdots & \vdots & \vdots \\ FSig_i(f_1)^{(|\mathcal{F}|-1)} & \dots & \dots & FSig_i(f_{|\mathcal{F}|})^{(|\mathcal{F}|-1)} \end{vmatrix} \quad (5)$$

Propositions 4.3 and 4.4 below are based on the properties of the Wronskian, in particular the link between the vanishing of the Wronskian and linear dependance as proved in [2].

*Proposition 4.3:* Consider a set of faults  $\mathcal{F} \subseteq \mathcal{F}_{SYS}$ ,  $|\mathcal{F}| \geq 2$ . If  $W_i(\mathcal{F}) \neq 0$  over the time interval  $[t_0, T]$ , i.e., is of full rank, then the faults in  $\mathcal{F}$  are functionally diagnosable over  $[t_0, T]$ .

*Proof-*  $W_i(\mathcal{F}) \neq 0$  implies that the fault signatures of the faults in  $\mathcal{F}$  are linearly functionally independent, as well as any subset of fault signatures within this set. Proposition 4.1 then implies the result.

*Proposition 4.4:* If the following conditions are satisfied:

- 1) there exists a set  $\mathcal{K}$  of sets of faults  $\mathcal{F}_k \subseteq \mathcal{F}_{SYS}$ ,  $|\mathcal{F}_k| \geq 2$ , such that the Wronskians  $W_i(\mathcal{F}_k) \neq 0$  over the time interval  $[t_0, T]$ , i.e., are of full rank, and  $\bigcup_k \mathcal{F}_k = \mathcal{F}_{SYS}$ ,
- 2)  $\bigcap_k \mathcal{F}_k \neq \emptyset$ ,

then the system (1) is functionally diagnosable over  $[t_0, T]$ , i.e., all the faults in  $\mathcal{F}_{SYS}$  are functionally diagnosable over  $[t_0, T]$ , as well as any subset of faults within this set.

*Proof-* From Proposition 4.3, condition 1) implies that the set of faults in the  $\mathcal{F}_k$ 's,  $k \in \mathcal{K}$ , are functionally diagnosable over  $[t_0, T]$  and that the  $\mathcal{F}_k$ 's cover all the faults in  $\mathcal{F}_{SYS}$ . Condition 2) guarantees the same property for all the pairs of faults of  $\mathcal{F}_{SYS}$  that are not covered by the  $\mathcal{F}_k$ 's, hence the result.

Note that the Wronskians  $W_i(-)$  of Propositions 4.3 and 4.4 are differential expressions with respect to inputs, outputs, parameters, and faults of system (1). They can be estimated using the function "Determinant" in Maple 19. The result indicates whether the determinant is identically equal to zero or not.

Interestingly, Propositions 4.3, and 4.4 allow to deal naturally with uncertain systems and unbounded or bounded faults because the Wronskians are calculated in a formal way.

*Example 4.1:* Consider again the Bernoulli equation example where  $f = (f_1, f_2)$ . To test if  $f_1$  and  $f_2$  are functionally diagnosable over the time interval  $[4.6, 10]$ , we consider the functional signatures  $FSig(f_1)$  and  $FSig(f_2)$  that have, in this simple example, only one component, and form the following Wronskian for the only possible set of faults of cardinal superior or equal to 2  $\mathcal{F} = \{f_1, f_2\}$ :

$$W_1(\mathcal{F}) = \begin{vmatrix} FSig(f_1) & FSig(f_2) \\ FSig(f_1)' & FSig(f_2)' \end{vmatrix} = \begin{vmatrix} f_1 y & f_2 y^2 \\ f_1 \dot{y} & 2 f_2 \dot{y} y \end{vmatrix}.$$

$W_1(\mathcal{F})$  is equal to  $f_1 f_2 \dot{y} y^2 \neq 0$ . Therefore, by Proposition 4.4, the model is functionally diagnosable over  $[4.6, 10]$ .

## V. EXAMPLE: TWO-WATER-TANK MODEL

Consider the two coupled water tanks shown in Figure 2 and modeled by:

$$\begin{cases} \dot{x}_1(t) = p_1(u(t) + f_1) - p_2(1 - f_4)z_1(t), \\ \dot{x}_2(t) = p_3(1 - f_4)z_1(t) - p_4z_2(t), \\ z_1(t)^2 = x_1(t), \quad z_2(t)^2 = x_2(t), \\ y_1(t) = p_5(1 - f_4)z_1(t) + f_2, \\ y_2(t) = p_6z_2(t) + f_3, \end{cases} \quad (6)$$

where  $p = (p_i)_{i=1,\dots,6}$ ,  $p_i \neq 0$ , is the parameter vector,  $x = (x_1, x_2)^T$  represents the state vector and corresponds to the level in each tank,  $z_1(t) = \sqrt{x_1(t)}$  and  $z_2(t) = \sqrt{x_2(t)}$  are auxiliary variables introduced to rewrite the model in the form (1) and  $u \neq 0$  is the input vector. The water level in the tanks can vary between 0 and 10.

$f_1$  denotes an unknown additive fault on the actuator signal,  $f_2$  and  $f_3$  are additive faults referring to the two sensors on the output of each of the water tanks, and  $f_4$  is a clogging fault.

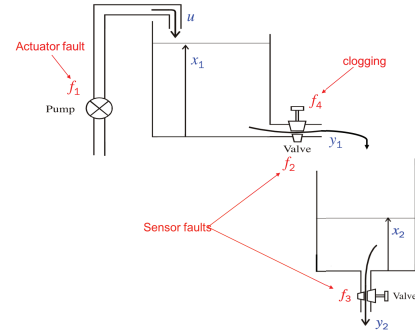


Fig. 2: Two coupled water tanks

According to the Rosenfeld-Groebner algorithm, the two ARR are:

$$\begin{aligned} w_1(\tilde{y}, \tilde{u}, f, p) &= w_{0,1}(\tilde{y}, \tilde{u}, p) - w_{1,1}(\tilde{y}, \tilde{u}, f, p) \\ w_2(\tilde{y}, \tilde{u}, f, p) &= w_{0,2}(\tilde{y}, \tilde{u}, p) - w_{1,2}(\tilde{y}, \tilde{u}, f, p) \end{aligned} \quad (7)$$

where:

$$\begin{aligned} w_{0,1}(\tilde{y}, \tilde{u}, p) &= -up_1p_5^2 + (p_2p_5 + 2\dot{y}_1)y_1, \\ w_{1,1}(\tilde{y}, \tilde{u}, f, p) &= 2\dot{y}_1f_2 - (f_4^2p_2p_5 - 2f_4p_2p_5)y_1 \\ &\quad - (-f_4^2p_1p_5^2 + 2f_4p_1p_5^2)u \\ &\quad + f_4^2f_2p_2p_5 + f_4^2f_1p_1p_5^2 - 2f_4f_2p_2p_5 \\ &\quad - 2f_4f_1p_1p_5^2 + f_2p_2p_5 + f_1p_1p_5^2, \\ w_{0,2}(\tilde{y}, \tilde{u}, p) &= 2p_5\dot{y}_2y_2 - p_3p_6^2y_1 + p_4p_5p_6y_2, \\ w_{1,2}(\tilde{y}, \tilde{u}, f, p) &= 2\dot{y}_2f_3p_5 + f_3p_4p_5p_6 - f_2p_3p_6^2. \end{aligned} \quad (8)$$

Hence,

$$\begin{aligned} FSig(f_1) &= (f_1p_1p_5^2, 0)^T \\ FSig(f_2) &= (2\dot{y}_1f_2 + f_2p_3p_6^2)^T \\ FSig(f_3) &= (0, 2\dot{y}_2f_3p_5 + f_3p_4p_5p_6)^T \\ FSig(f_4) &= (-y_1f_4^2p_2p_5 + 2y_1f_4p_2p_5 \\ &\quad + u f_4^2p_1p_5^2 - 2u f_4p_1p_5^2, 0)^T. \end{aligned} \quad (9)$$

For the subset of faults  $\mathcal{F}_1 = \{f_1, f_2, f_4\}$  and the first component of  $FSig(\mathcal{F}_1)$  we obtain the following expression for the Wronskian  $W_1(\mathcal{F}_1)$ :

$$2f_1f_4(f_4 - 2)p_1p_5^3(\dot{y}_1(\ddot{u}p_1p_5 - \dot{y}_1p_2) - \ddot{y}_1(\dot{u}p_1p_5 - \dot{y}_1p_2)).$$

Using Maple 19, we verify that this determinant is not identically equal to zero. Thus, by Propositions 4.3, the faults  $f_1$ ,  $f_2$  and  $f_4$  are functionally diagnosable.

For the subset of faults  $\mathcal{F}_2 = \{f_2, f_3\}$  and the second component of  $FSig(\mathcal{F}_2)$  we obtain the following expression for the Wronskian  $W_2(\mathcal{F}_2)$ :

$$2f_2f_3p_3p_5p_6^2\ddot{y}_2$$

and assess that it is not identically equal to zero. Thus, by Propositions 4.3, the faults  $f_2$  and  $f_3$  are functionally diagnosable. We can verify that  $\mathcal{F}_1 \cup \mathcal{F}_2 = \mathcal{F}_{SYS}$  and that  $\mathcal{F}_1 \cap \mathcal{F}_2 \neq \emptyset$ , hence the two conditions of Proposition 4.4 are satisfied and the system (6) is functionally diagnosable.

The above theoretical results are confirmed numerically for faults valued by the interval  $[0.4, 0.6]$  and introduced at  $t = 20$ s. Fig. 3 shows the trajectory envelopes of bounded fault functional signatures computed by means of interval analysis [15]. These are obviously zero before  $t = 20$ s. After  $t = 20$ s, time intervals in which their intersections are empty can be identified, hence indicating functional diagnosability. For the first component of the fault functional signatures (left figure), empty intersection of pairs of envelopes for faults in  $\mathcal{F}_1 = \{f_1, f_2, f_4\}$  is visible on  $]20.8, 28.7[$ , while the other ones remain zero. For the second component (right figure), there is empty intersection of pairs of envelopes for faults in  $\mathcal{F}_2 = \{f_2, f_3\}$  until the end of the simulation, while the other ones remain zero.

Note that in the classical sense, System (6) is not diagnosable because the signatures of  $f_1$  and  $f_4$  are both equal to  $(1, 0)^T$ .

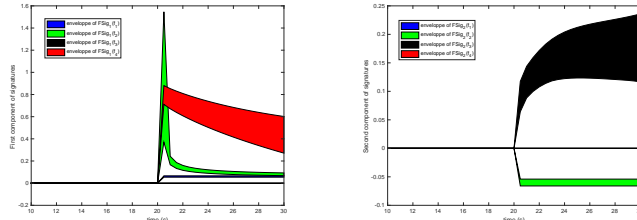


Fig. 3: First (left) and second (right) component of the fault functional signatures of  $f_1$ ,  $f_2$ ,  $f_3$ , and  $f_4$  identified by different colors. Note that  $FSig(f_3)$  and  $FSig(f_1)$ ,  $FSig(f_4)$  in the left and right figure, respectively, are constant at 0.

## VI. CONCLUSION

In this paper, an operational sufficient condition for the functional diagnosability of nonlinear dynamical systems is proposed. The condition is based on the functional linear independence of fault functional signature vectors which is brought back to a rank condition. A two-water-tanks example is used to illustrate the approach and confirm the relevance of this result.

Following this work, it would be of interest to determine theoretically the intervals of time on which faults are discriminable or undiscriminable based on the time at which the Wronskians of Proposition 4.3 and 4.4 in section IV vanish or the opposite. This could be done by evaluating them on small subsequent time intervals  $[t, t + \gamma]$ , by using,

for example, contractors that avoid wrapping effects but still provide guaranteed results, i.e., that enclose all real results [4]. In this way, one would be able to identify the time intervals for which the system is functionally diagnosable or not.

## REFERENCES

- [1] S. Audoly, G. Bellu, L. D'Angio, M. P. Saccomani, and C. Cobelli. Global identifiability of nonlinear models of biological systems. *IEEE Trans. Biomed. Eng.*, 48:55–65, 2001.
- [2] M. Bôcher. Certain cases in which the vanishing of the wronskian is a sufficient condition for linear dependence. *Transactions of the American Mathematical Society*, 2:139–149, 1901.
- [3] F. Boulrier, D. Lazard, F. Ollivier, and M. Petitot. Computing representation for radicals of finitely generated differential ideals. *Technical report, IT-306, Université Lille I, LIFL, 59655, Villeneuve d'Ascq*, 1997.
- [4] G. Chabert and L. Jaulin. Contractor programming. *Artificial Intelligence*, 173(11):1079–1100, 2009.
- [5] A. Chouchane, M. Ghazel, and A. Boussif. K-diagnosability analysis of bounded and unbounded petri nets using linear optimization. *Automatica*, 147:110689, 2023.
- [6] M.O. Cordier, L. Travé-Massuyès, and X. Pucel. Comparing diagnosability in continuous and discrete-event systems. In *Proceedings of the 17th International Workshop on Principles of Diagnosis, DX'06*, pages 55–60, 2006.
- [7] J.C. Cruz-Victoria, R. Martinez-Guerra, and J.J. Rincon-Pasaye. On linear systems diagnosis using differential and algebraic methods. *Journal of the Franklin Institute*, 345:102–118, 2008.
- [8] L. Denis-Vidal, G. Joly-Blanchard, and C. Noiret. Some effective approaches to check identifiability of uncontrolled nonlinear systems. *Mathematics and Computers in Simulation*, 57:35–44, 2001.
- [9] F. Fu, D. Wang, L. Li, W. Li, and Z. Wu. Data-driven method for the quantitative fault diagnosability analysis of dynamic systems. *IET Control Theory & Applications*, 13(8):1197–1203, 2019.
- [10] F. Fu, D. Wang, W. Li, D. Zhao, and Z. Wu. Overall fault diagnosability evaluation for dynamic systems: A quantitative–qualitative approach. *Automatica*, 146:110591, 2022.
- [11] X. Gu and X. Shi. A review of research on diagnosability of control systems. *Energy Reports*, 11:2174–2188, 2024.
- [12] F. Hashemniya, B. Caillaud, E. Frisk, M. Krysander, and M. Malandain. Fault diagnosability analysis of multi-mode systems. In *[2024] IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, arXiv preprint arXiv:2312.14030*, 2024.
- [13] C. Jauberthie, N. Verdière, and L. Travé-Massuyès. Fault detection and identification relying on set-membership identifiability. *Annual Reviews in Control*, 37:129–136, 2013.
- [14] C. Jauberthie, N. Verdière, and L. Travé-Massuyès. Set-membership diagnosability: definitions and analysis. In *Proceedings of International Conference on Control and Fault-Tolerant Systems, Barcelona, Spain*, pages 1–6, 2016.
- [15] L. Jaulin, M. Kieffer, O. Didrit, and E. Walter. *Applied Interval Analysis, with examples in parameter and state estimation, Robust control and robotics*. Springer, Londres, 2001.
- [16] E.R. Kolchin. *Differential algebra and algebraic groups*. Academic Press, New York, 1973.
- [17] S. Lafortune, F. Lin, and C. N. Hadjicostis. On the history of diagnosability and opacity in discrete event systems. *Annual Reviews in Control*, 45:257–266, 2018.
- [18] L. Ljung and T. Glad. On global identifiability for arbitrary model parametrizations. *Automatica*, 30:265–276, 1994.
- [19] R. Seliger and P.M. Frank. Fault-diagnosis by disturbance decoupled nonlinear observers. In *[1991] Proceedings of the 30th IEEE Conference on Decision and Control*, pages 2248–2253 vol.3, 1991.
- [20] Marcel Staroswiecki and G. Comtet-Varga. Analytical redundancy relations for fault detection and isolation in algebraic dynamic systems. *Automatica*, 37(5):687–699, 2001.
- [21] L. Travé-Massuyès, T. Escobet, and X. Olive. Diagnosability analysis based on component-supported analytical redundancy relations. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 36(6):1146–1160, 2006.
- [22] N. Verdière, C. Jauberthie, and L. Travé-Massuyès. Functional diagnosability and detectability of nonlinear models based on analytical redundancy relations. *Journal of Process Control*, 35:1–10, 2015.