On Approximate Diagnosability of Nonlinear Systems

Elena De Santis, Giordano Pola and Maria Domenica Di Benedetto

Abstract—This paper deals with diagnosability of discrete-time nonlinear systems with unknown inputs and quantized outputs. We propose a novel notion of diagnosability that we term approximate diagnosability, corresponding to the possibility of detecting within a finite delay and within a given accuracy if a set of faulty states is reached or not. Addressing diagnosability in an approximate sense is primarily motivated by the fact that system outputs in concrete applications are measured by sensors that introduce measurement errors. Consequently, it is not possible to detect exactly if the state of the system has reached or not the set of faulty states. In order to check approximate diagnosability on the class of nonlinear systems we use tools from formal methods. We first derive a symbolic model approximating the original system within any desired accuracy. This step allows us to check approximate diagnosability of the symbolic model. We then establish the relation between approximate diagnosability of the symbolic model and of the original nonlinear system.

keywords: approximate diagnosability, nonlinear systems, quantized systems, symbolic models.

I. INTRODUCTION

The increasing complexity in real-world engineered systems requires great attention to performance degradation, safety hazards and occurrence of faults, which must be detected as soon as possible to possibly restore nominal behavior of the system. The notion of diagnosability plays a key role in this regard, since it corresponds to the possibility of detecting within a finite delay if a fault, or in general a hazardous situation, occurred. This notion has been extensively studied both in the Discrete–Event Systems (DES) community and control systems community, and the related literature is very broad. Within the DES community, after the seminal work [1], several results have been achieved, see e.g. [2], [3], [4], [5], [6], [7], [8], [9] and the references therein. An excellent review of recent advances on diagnosis methods can be found in [10]. More recently, a unifying framework for the study of observability and diagnosability of DES has been also proposed in [11]. Within the control systems community, for fault–tolerant control, an early review paper was presented in [12], which introduced the basic concepts of fault–tolerant control and analyzed the applicability of artificial intelligence to fault–tolerant control systems. Subsequent overviews appeared in [13], [14]. Reconfigurable fault–tolerant control systems are reviewed in [15], [16], [17] and some results on fault–tolerant control for nonlinear systems in [18]. A recent comprehensive survey on diagnosability of continuous systems is reported in [19]. Extensions to hybrid systems, featuring both discrete and continuous dynamics, are also present in the literature. For example, [20] addressed diagnosability for timed automata, [21] diagnosability for hybrid systems, [22], [23], [24] propose abstraction techniques for diagnosability of hybrid automata. Apart from differences in the class of systems considered and in the way faults are modeled, to the best of our knowledge, existing papers, except for [25], [26], either assume that state variables are available, or assume the exact knowledge of output variables. This is rather limiting in concrete applications where state variables cannot be directly measured, or output variables are measured by sensors that introduce measurement errors. The papers [25] and [26] study diagnosability for quantized systems. They both model faults as additional inputs to the system. The former considers continuous–time nonlinear systems and the detection is done in a stochastic setting, by assuming an appropriate description of the occurrence of faults. The latter analyzes discrete–time linear systems and the faults are detected, provided that they belong to an appropriate class of functions. In this paper, we introduce a new notion of diagnosability, that we term approximate diagnosability, for discrete–time nonlinear systems with unknown inputs and quantized output measurements. Given an accuracy $\rho \geq 0$ and a set of faulty states $F$, approximate diagnosability corresponds to the possibility of detecting, within a finite time delay:

- if the system’s state reached the set $F + B_\rho(0)$, obtained by adding to $F$ a closed ball $B_\rho(0)$ centered at the origin and with radius $\rho$, and
- if the system’s state has never reached the set $F$.

This ambiguity around the set $F$ reflects uncertainties introduced by measurement errors. When the accuracy $\rho = 0$, approximate diagnosability translates to dynamical systems the notion of diagnosability investigated in [11] for DES.

In order to check this property on the class of nonlinear systems we use tools from formal methods. Under an assumption of incremental stability of the nonlinear system we first derive a symbolic model approximating the original system within any desired accuracy. We recall that a symbolic model is an abstract description of the control system where each state corresponds to an aggregate of continuous states and each control label corresponds to an aggregate of continuous inputs. We then extend the classical notion of diagnosability given for DES to metric symbolic models and in an approximate sense. Algorithms for checking this property can be easily obtained by naturally extending those
proposed in [11] to an approximate sense. We finally show how to check approximate diagnosability of the original nonlinear system by analyzing the same property on the obtained symbolic model. Computational complexity of the proposed approach is also discussed.

This paper is organized as follows. Section II introduces notation and preliminary definitions. Section III introduces the notion of approximate diagnosability for the class of discrete–time nonlinear systems. In Section IV we first derive symbolic models approximating the nonlinear system in the sense of approximate bisimulation, then we extend the notion of diagnosability given for DES to metric symbolic systems and in an approximate sense, and then establish connections between approximate diagnosability of the symbolic model and approximate diagnosability of the original nonlinear system. Some concluding remarks are offered in Section V.

II. Notation and Preliminary Definitions

The symbols N, Z, R, R+ and R0+ denote the set of non-negative integer, integer, real, positive real, and nonnegative real numbers, respectively. The symbol 0 denotes the origin in Rn. Given a, b ∈ Z, we denote [a; b] = [a, b] ∩ Z. Given a set X, the symbol 2X denotes the power set of X. Given a pair of sets X and Y and a relation R ⊆ X × Y, the symbol R−1 denotes the inverse relation of R, i.e. R−1 = \{ (y, x) ∈ Y × X \mid (x, y) ∈ R \}. Given X ⊆ X and Y ⊆ Y, we denote R(X′) = { y ∈ Y \mid ∃ x ∈ X \text{s.t.} (x, y) ∈ R } and R−1(Y′) = { x ∈ X \mid ∃ y ∈ Y \text{s.t.} (x, y) ∈ R }. Given a function f : X → Y and X′ ⊆ X the symbol f(X′) denotes the image of X′ through f, i.e. f(X′) = \{ y ∈ Y \mid ∃ x ∈ X \text{s.t.} f(x) = y \} and the symbol f|X′ denotes the restriction of f to X′ that is f|X′ : X′ → Y such that f|X′(x′) = f(x′) for all x′ ∈ X′. A continuous function γ : R+ → R+ is said to belong to class K if it is strictly increasing and γ(0) = 0; γ is said to belong to class K∞ if γ ∈ K and γ(r) → ∞ as r → ∞. A continuous function β : R+ × R+ → R+ is said to belong to class KL if for each fixed s, the map β(r, s) belongs to class K∞ with respect to r and, for each fixed r, the map β(r, s) is decreasing with respect to s and β(r, s) → 0 as s → ∞. Symbol I, denotes the identity matrix in Rn. Given a vector x ∈ Rn we denote by x(i) the i-th element of x and by ∥x∥ the infinity norm of x. Given a ∈ R and X ⊆ Rn, the symbol aX denotes the set \{ y ∈ Rn \mid ∃ x ∈ X \text{s.t.} y = ax \}. Given θ ∈ R+ and x ∈ Rn, we denote

\[ B_0(x) = \{ y ∈ R^n \mid \|x - y\| ≤ \theta \}; \]
\[ B_{[−\theta,\theta]}(x) = \{ y ∈ R^n \mid y(i) ∈ [−\theta + x(i), \theta + x(i)], i \in [1; n] \}. \]

Note that for any θ ∈ R+, the collection of B_{[−\theta,\theta]}(x) with x ranging in 2θZn is a partition of Rn. Given a set X ⊆ Rn we denote by B_0(X) the set \{ x ∈ X \mid B_0(x) \}. We now define the quantization function.

Definition 1: Given a positive n ∈ N and a quantization parameter θ ∈ R+, the quantizer in Rn with accuracy θ is a function |. |_θ : R^n → 2θZn.

\[ u(t) \rightarrow \Sigma \quad y(t) \rightarrow \left[ \begin{array}{c} \eta \end{array} \right] \]

Fig. 1. Nonlinear system with quantized output measurements.

associating to any x ∈ Rn the unique vector |x|_θ ∈ 2θZn such that x ∈ R^n_{[−\theta,\theta]}(|x|_θ).

Definition above naturally extends to sets X ⊆ R^n when |X|_θ is interpreted as the image of X through function |. |_θ.

III. Nonlinear Systems and Approximate Diagnosability

The class of nonlinear systems that we consider in this paper is described by

\[ \Sigma : \left\{ \begin{array}{l}
  x(t+1) = f(x(t), u(t)), \\
  y(t) = \left[ \begin{array}{c} I_p \\ 0 \end{array} \right] x(t), \\
  x(0) ∈ X_0, x(t) ∈ R^n, u(t) ∈ U, y(t) ∈ R^p, t ∈ N,
\end{array} \right. \]

(1)

where:

- \( x(t), u(t) \) and \( y(t) \) denote, respectively, the state, the input and the output, at time \( t ∈ N \);
- \( \mathbb{R}^n \) is the state space;
- \( X_0 ⊆ \mathbb{R}^n \) is the set of initial states;
- \( U ⊆ \mathbb{R}^m \) is the input set;
- \( \mathbb{R}^p \) is the output space with \( p < n \);
- \( f : \mathbb{R}^n × \mathbb{R}^m → \mathbb{R}^n \) is the vector field.

In this paper we make the following:

Assumption 1:

set \( X_0 \) is compact;
set \( U \) is compact and contains the origin \( 0_m \);
function \( f \) is continuous in its arguments and satisfies \( f(0_n, 0_m) = 0_n \).

We denote by \( U \) the collection of input functions from \( N \) to \( U \). Given \( t_f ∈ N \), a function

\[ x : [0; t_f] → \mathbb{R}^n \]

(2)

is said to be a state trajectory of \( \Sigma \) if \( x(0) ∈ X_0 \) and there exists \( u ∈ U \) satisfying \( x(t+1) = f(x(t), u(t)) \), for all \( t ∈ [0; t_f] \). Given \( t_f ∈ N \), a function \( y : [0; t_f] → \mathbb{R}^p \) is said to be an output trajectory of \( \Sigma \) if \( y(t) = \left[ \begin{array}{c} I_p \\ 0 \end{array} \right] x(t) \) for all \( t ∈ [0; t_f] \). Given \( t_f ∈ N \), we denote by \( \mathcal{Y}_{t_f} \) the collection of output trajectories of \( \Sigma \) with domain \([0; t_f] \).

Remark 1: The choice in the output function in nonlinear system \( \Sigma \) is motivated by many concrete applications where the output variables correspond to a selection of the state variables. However, it is easy to see that there is no loss of generality in considering output function in \( \Sigma \) in the form of \( y(t) = Cx(t), t ∈ N \), for some matrix \( C ∈ \mathbb{R}^{p × n} \), instead of \( y(t) = \left[ \begin{array}{c} I_p \\ 0 \end{array} \right] x(t), t ∈ N \). General nonlinear output
functions are not considered in this paper and will be the object of future investigations.

Throughout the paper we will make the following assumptions.

Assumption 2: Inputs \( u(.) \) are available through output runs. \( \forall t \in \mathbb{N} \), where \( \eta \in \mathbb{R}^+ \) is the quantization parameter, see Fig. 1.

Assumption 3: Output \( y(t) \) of \( \Sigma \) at time \( t \in \mathbb{N} \) is only available through its quantization \( y(t)_{\eta}^\rho \), where \( \eta \in \mathbb{R}^+ \) is the quantization parameter, see Fig. 1.

Given the quantization parameter \( \eta \in \mathbb{R}^+ \) and \( t_f \in \mathbb{N} \), we denote by \( Y^\eta_{t_f} \) the collection of quantized output trajectories generated by \( \Sigma \) with domain \([0; t_f]\), i.e. the collection of functions

\[ y_{t_f, \eta} : [0; t_f] \rightarrow [\mathbb{R}^+]_{\eta}^\rho, \]

such that there exists \( y_{t_f, \eta} \in Y^\eta_{t_f} \) for which:

\[ y_{t_f, \eta}(t) = [y_{t_f}(t)]_{\eta}^\rho, \forall t \in [0; t_f]. \]

We also set

\[ Y^\eta = \bigcup_{t_f \in \mathbb{N}} Y^\eta_{t_f}, \]
corresponding to the collection of all quantized output trajectories of \( \Sigma \). We can now define the notion of approximate diagnosability for nonlinear systems.

Definition 2: (Approximate diagnosability of nonlinear systems) Given a desired accuracy \( \rho \in \mathbb{R}^+_0 \) and a set of faulty states \( F \subseteq \mathbb{R}^n \) with

\[ F \cap X_0 = \emptyset, \]

nonlinear system \( \Sigma \) in [1] is \((\rho, F)\)-diagnosable if there exists a finite delay \( \Delta \in \mathbb{N} \), and

\[ D : Y^\eta \rightarrow \{0, 1\}, \]
called the diagnoser, such that

\[ D(y_{0, \eta}) = 0, \]

and whenever for some time \( t > 0 \)

\[ (x(t) \in F) \land (x(t) \notin F, \forall t \in [0; t-1]) \]

we have

\[ D(y_{t+\Delta, \eta}) = 1. \]

Conversely, whenever for some time \( t' > 0 \)

\[ (D(y_{t', \eta}) = 1) \land (D(y_{t, \eta}) = 0, \forall t \in [0; t'-1]) \]

we have

\[ x(t) \in B_{\rho}(F), \]

for some \( t \in [\max \{(t' - \Delta), 0\}; t'] \).

Remark 2: Definition above is a natural extension of the notion of diagnosability given in [11] for DES (with finite set of states), along two directions. First, it applies to nonlinear systems, hence dynamical systems with infinite set of states. Second, it is given in an approximate sense. Motivation for addressing approximate diagnosability primarily stems from the fact that outputs of nonlinear systems in concrete applications are measured by sensors that introduce measurement errors. Consequently, it is not possible to detect in general, with arbitrary small precision if the state of the system is or is not within the set of faulty states. When accuracy \( \rho = 0 \) definition above coincides with the one of [11], when rewritten for nonlinear systems.

IV. CHECKING APPROXIMATE DIAGNOSABILITY

The approach that we follow to check approximate diagnosability of \( \Sigma \) is based on the use of formal methods and in particular, of symbolic models. Symbolic models are abstract descriptions of control systems where each state corresponds to an aggregate of continuous states and each label to an aggregate of control inputs [27]. This section is organized as follows. In Subsection IV-A we review the notion of systems, approximate relations and extend the notion of diagnosability of [11] to metric symbolic systems and in an approximate sense. In Subsection IV-B we give the main result of the paper: after having approximated the nonlinear system \( \Sigma \) through a symbolic model, we establish connections between approximate diagnosability of the original nonlinear system \( \Sigma \) and approximate diagnosability of the obtained symbolic model; computational complexity of the approach taken is also discussed.

A. Systems, approximate relations and exact diagnosability

We start by recalling the notion of systems that we use to approximate the nonlinear system \( \Sigma \).

Definition 3: [27] A system is a tuple

\[ S = (X, X_0, U, \xrightarrow{r_N}, Y, H), \]

consisting of

- a set of states \( X \),
- a set of initial states \( X_0 \subseteq X \),
- a set of inputs \( U \),
- a transition relation \( \rightarrow \subseteq X \times U \times X \),
- a set of outputs \( Y \) and,
- an output function \( H : X \rightarrow Y \).

A transition \((x, u, x') \in \rightarrow\) of \( S \) is denoted by \( x \xrightarrow{u} x' \).

The evolution of systems is captured by the notions of state, input and output runs. Given a sequence of transitions of \( S \)

\[ x_0 \xrightarrow{u_0} x_1 \xrightarrow{u_1} \ldots x_{l-1} \xrightarrow{u_{l-1}} x_l \quad (3) \]

with \( x_0 \in X_0 \), the sequences

\[ r_N : x_0 x_1 \ldots x_l, \]
\[ r_U : u_0 u_1 \ldots u_{l-1}, \quad (4) \]
\[ r_Y : H(x_0) H(x_1) \ldots H(x_l), \quad (5) \]

are called a state run, an input run and an output run of \( S \), respectively.

The accessible part of a system \( S \), denoted \( Ac(S) \), is the collection of states of \( S \) that are reached by state runs of \( S \). System \( S \) is said to be:

- symbolic, if \( Ac(S) \) and \( U \) are finite sets;
- metric, if \( X \) is equipped with a metric \( d : X \times X \rightarrow \mathbb{R}^+_0 \);
- deterministic, if for any \( x \in X \) and \( u \in U \) there exists at most one transition \( x \xrightarrow{u} x' \) and nondeterministic, otherwise.
In order to provide approximations of $\Sigma$ we need to recall the following notions of approximate simulation and bisimulation relations.

**Definition 4:** [28] Consider a pair of metric systems

$$S_i = (X_i, X_{0,i}, U_i, \quad i \quad Y_i, H_i),$$

with $X_1$ and $X_2$ subsets of some metric set $X$ equipped with metric $d$, and let $\varepsilon \in \mathbb{R}_0^+$ be a given accuracy. Consider a relation

$$\mathcal{R} \subseteq X_1 \times X_2$$

satisfying the following conditions:

(i) $\forall x_1 \in X_{0,1}$ $\exists x_2 \in X_{0,2}$ such that $(x_1, x_2) \in \mathcal{R}$;

(ii) $\forall (x_1, x_2) \in \mathcal{R}$, $d(x_1, x_2) \leq \varepsilon$.

Relation $\mathcal{R}$ is an $\varepsilon$-approximate ($\varepsilon\mathcal{A}$) simulation relation from $S_1$ to $S_2$ if it enjoys conditions (i)–(ii) and the following one:

(iii) $\forall (x_1, x_2) \in \mathcal{R}$ if $x_1 \xrightarrow{u_1} x'_1$ then there exists $x_2 \xrightarrow{u_2} x'_2$ such that $(x'_1, x'_2) \in \mathcal{R}$.

System $S_1$ is $\varepsilon$-simulated by $S_2$, if there exists an $\varepsilon$-approximate simulation relation from $S_1$ to $S_2$.

Relation $\mathcal{R}$ in (6) is an $\varepsilon$-approximate ($\varepsilon\mathcal{A}$) bisimulation relation between $S_1$ and $S_2$ if

- $\mathcal{R}$ is an $\varepsilon\mathcal{A}$ simulation relation from $S_1$ to $S_2$, and
- $\mathcal{R}^-$ is an $\varepsilon\mathcal{A}$ simulation relation from $S_2$ to $S_1$.

Systems $S_1$ and $S_2$ are $\varepsilon$-bisimilar, denoted $S_1 \equiv_\varepsilon S_2$, if there exists an $\varepsilon$-approximate bisimulation relation between $S_1$ and $S_2$.

We conclude this section with the following

**Definition 5:** (Approximate diagnosability of metric systems) Consider a metric system $S = (X, X_0, U, \quad \quad Y, H)$, with metric $d$, and a set $\hat{F} \subseteq X$ of faulty states with

$$\hat{F} \cap X_0 = \varnothing.$$ 

Denote by $X$ and $Y$ the collection of state runs and of output runs of $S$, respectively. Denote by $\hat{B}_\rho(\hat{x})$ the closed ball induced by metric $\hat{d}$ centered at $\hat{x} \in X$ and with radius $\hat{\rho}$, i.e.

$$\hat{B}_\rho(\hat{x}) = \{ x \in X | \hat{d}(x, \hat{x}) \leq \hat{\rho} \}.$$ 

Given $\hat{X} \subseteq X$, denote by $\hat{B}_\rho(\hat{X})$ the set

$$\bigcup_{\hat{x} \in \hat{X}} \hat{B}_\rho(\hat{x}).$$

Given a desired accuracy $\hat{\rho} \in \mathbb{R}_0^+$, system $S$ is $(\hat{\rho}, \hat{F})$-diagnosable if there exists a finite delay $\hat{\Delta} \in \mathbb{N}$, and

$$\hat{D} : Y \rightarrow \{0, 1\},$$

called the diagnoser, with

$$\hat{D}(y_0) = 0,$$

where $y_0$ is any output run of $S$ with length 1, such that for any state run $x_0 x_1 \ldots x_t \in X$ and corresponding output run $y_0 y_1 \ldots y_t \in Y$ of $S$, whenever for some $t > 0$

$$\left( x_t \in \hat{F} \right) \land \left( x_i \notin \hat{F}, \forall t \in [0; t - 1] \right),$$

we have

$$\hat{D} \left(y_{t+\hat{\Delta}} \right) = 1.$$

Conversely, whenever for some $t' > 0$

$$\left( \hat{D}(y_{t'}) = 1 \right) \land \left( \hat{D}(y_t) = 0, \forall t \in [0; t' - 1] \right)$$

we have

$$x_t \in \hat{B}_{\hat{\rho}}(\hat{F}),$$

for some $t \in \max\{ (t' - \hat{\Delta}), 0 \}; t'$.

**Remark 3:** Definition above extends the notion of diagnosability of [11], to metric systems in the sense of Definition [3] In [11], diagnosability with accuracy $\hat{\rho} = 0$ of DES has been characterized in a set membership framework, and it is shown that both space and time computational complexities in checking this property are polynomial in the cardinality of the set of states of the DES. Since, the conditions of [11] rely upon the set $\hat{F}$ and its complement (see Theorem 20), the generalization of such conditions to $(\hat{\rho}, \hat{F})$-diagnosability with $\hat{\rho} \geq 0$ can simply be obtained by replacing the complement of $\hat{F}$ with the complement of $\hat{B}_{\hat{\rho}}(\hat{F})$; obtained algorithms remain of polynomial computational complexity.

**B. Main result**

We start by defining a symbolic system that approximates $\Sigma$ in the sense of approximate bisimulation for any desired accuracy. For convenience, we reformat the nonlinear system $\Sigma$ by using the formalism given in Definition [5]

**Definition 6:** Given $\Sigma$, define the system

$$S(\Sigma) = (X, X_0, U, \quad \quad X_m, Y, H)$$

where

- $X = \mathbb{R}^n$;
- $X_0 = X_0$;
- $U$ coincides with the set $U$ in [14];
- $x \xrightarrow{u} x^+$, if $x^+ = f(x, u)$;
- $Y = \mathbb{R}^m$;
- $H(x) = \left[ I_p \quad 0 \right] x$, for all $x \in X$.

System $S(\Sigma)$ is metric because set $X = \mathbb{R}^n$ can be equipped with a metric $d; \text{ in the sequel we choose metric}$

$$d(x, x') = ||x - x'||, x, x' \in \mathbb{R}^n.$$ 

System $S(\Sigma)$ will be approximated by means of a system that we now introduce.

**Definition 7:** Given $\Sigma$, a state and output quantization parameter $\eta \in \mathbb{R}^+$ and an input quantization parameter $\mu \in \mathbb{R}^+$, define the system

$$S_{\eta, \mu}(\Sigma) = (X_{\eta, \mu}, X_{\eta, \mu, 0}, U_{\eta, \mu}, \quad \quad Y_{\eta, \mu}, H_{\eta, \mu}),$$

where:

- $X_{\eta, \mu} = [\mathbb{R}^n]_\eta$;
- $X_{\eta, \mu, 0} = [X_0]_\eta$;
- $U_{\eta, \mu} = [U]_\eta$;
- $\xi \xrightarrow{\mu} \xi^+$, if $\xi^+ = [f(\xi, v)]_\eta$;
- $Y_{\eta, \mu} = [\mathbb{R}^m]_\eta.$
• $H_{\eta,\mu}(\xi) = [I_\rho \ 0] \xi$, for all $\xi \in X_{\eta,\mu}$.

The basic idea in the construction above is to replace each state $x$ in $\Sigma$ by its quantized value $\xi = [x]_\eta$ and each input $u$ in $U$ by its quantized value $v = [u]_\mu$ in $S_{\eta,\mu}(\Sigma)$. Accordingly, evolution of system $\Sigma$ with initial state $x$ and input $v$ to state $x' = f(\xi, v)$, is captured by the transition $\xi \xrightarrow{\mu} \xi'$ in system $S_{\eta,\mu}(\Sigma)$, where $\xi$ and $\xi'$ are the quantized values of $x$ and $x'$, respectively, i.e., $\xi = [x]_\eta$ and $\xi' = [x']_\eta$. System $S_{\eta,\mu}(\Sigma)$ is metric; in the sequel we use the metric $d$ in (9); this choice is allowed because $X_{\eta,\mu} \subset X$. Moreover, by definition of the transition relation $\xrightarrow{\eta,\mu}$, system $S_{\eta,\mu}(\Sigma)$ is countable. We now consider the following

**Assumption 4:** A locally Lipschitz function

$$ V : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}_0^+ $$

exists for nonlinear system $\Sigma$, which satisfies the following inequalities for some $\kappa_\infty$ functions $\alpha$, $\beta$, $\gamma$ and $\lambda$ function $\sigma$:

(i) $\alpha(|x - x'|) \leq V(x, x') \leq \beta(|x - x'|)$, for any $x, x' \in \mathbb{R}^n$;
(ii) $V(f(x, u), f(x', u')) - V(x, x') \leq -\lambda(V(x, x')) + \sigma(|u - u'|)$, for any $x, x' \in \mathbb{R}^n$ and any $u, u' \in U$.

Function $V$ is called an incremental input–to–state stable (δ–ISS) Lyapunov function [29], [30] for nonlinear system $\Sigma$. Assumption 4 has been shown in [30] to be a sufficient condition for $\Sigma$ to fulfill the δ–ISS stability property [29], [30].

We now have all the ingredients to present the following

**Proposition 1:** Suppose that Assumption 4 holds and let $L$ be a Lipschitz constant of function $V$ in $\mathbb{R}^n \times \mathbb{R}^n$. Then, for any desired accuracy $\varepsilon \in \mathbb{R}^+$ and for any quantization parameters $\eta, \mu \in \mathbb{R}^+$ satisfying the following inequalities

$$ L\eta + \beta(\mu) \leq (\lambda \circ \alpha)(\varepsilon), $$

relation $\mathcal{R}_\varepsilon \subseteq \mathbb{R}^n \times X_{\eta,\mu}$ specified by

$$ (x, \xi) \in \mathcal{R}_\varepsilon \Leftrightarrow V(x, \xi) \leq \alpha(\varepsilon) \tag{10} $$

is an $\varepsilon$–approximation bisimulation between $S(\Sigma)$ and $S_{\eta,\mu}(\Sigma)$. Consequently, systems $S(\Sigma)$ and $S_{\eta,\mu}(\Sigma)$ are $\varepsilon$–bisimilar.

**Proof:** Direct consequence of Proposition 1 in [31].

We now show that under Assumption 4 system $S_{\eta,\mu}(\Sigma)$ is not only countable but also symbolic.

**Proposition 2:** Suppose that Assumption 4 holds. Then, for any quantization parameters $\eta, \mu \in \mathbb{R}^+$, system $S_{\eta,\mu}(\Sigma)$ is symbolic.

**Proof:** Under Assumption 4 the nonlinear system $\Sigma$ is δ–ISS [30]. Given $\eta, \mu \in \mathbb{R}^+$, select $\varepsilon \in \mathbb{R}^+$ satisfying the inequality in (10). By Proposition 1 for any $t_f \in \mathbb{N}$ and for any state run

$$ \xi(0), \xi(1), \ldots, \xi(t_f) $$

of $S_{\eta,\mu}(\Sigma)$ there exists a state trajectory $x : [0; t_f] \rightarrow \mathbb{R}^n$ of $\Sigma$ such that:

$$ (\xi(t), x(t)) \in \mathcal{R}_\varepsilon, \forall t \in [0; t_f]. $$

By definition of $\mathcal{R}_\varepsilon$ in (10), the δ–ISS property and Assumption 1 we get for any $t \in [0, t_f]$ and for any $t_f \in \mathbb{N}$:

$$ \|\xi(t)\| \leq \|\xi(t) - x(t)\| + \|x(t)\| \leq \varepsilon + \beta(\|x(0)\|, t) + \gamma(\sup_{u \in [a, b]} \|u(t')\|) \leq \varepsilon + \max_{x_0 \in X, \alpha}(\|x(0)\|, 0) + \gamma(\sup_{u \in U} \|u\|), $$

for some $K\mathcal{C}$ function $\beta$ and $K$ function $\gamma$ [30]. Hence,

$$ (\xi(t) \in B_\varepsilon(0), t \in \mathbb{N}, $$

with $r = \varepsilon + \max_{x_0 \in X, \alpha}(\|x(0)\|, 0) + \gamma(\sup_{u \in U} \|u\|)$, and since $\xi(t) \in X_{\eta,\mu}$ for all $t \in \mathbb{N}$, we get

$$ \text{Acc}(S_{\eta,\mu}(\Sigma)) \subseteq B_\varepsilon(0) \cap X_{\eta,\mu} $$

that is a finite set. Finally, since $U$ is compact then $[U]_\mu^n$ is finite from which, the result follows.

Computational complexity in constructing $S_{\eta,\mu}(\Sigma)$ is discussed in the following

**Proposition 3:** Space and time computational complexities in computing $S_{\eta,\mu}(\Sigma)$ are exponential with the dimension $n$ of state space and with the dimension $m$ of the input space of $\Sigma$.

One way to mitigate computational complexity above is in constructing only the accessible part of $S_{\eta,\mu}(\Sigma)$; similar ideas were explored in [32] by following on–the–fly techniques studied in e.g. [33], [34] for efficient formal verification and control design of transition systems. We now have all the ingredients to present the main result of this paper establishing connections between approximate diagnosability of $S_{\eta,\mu}(\Sigma)$ and approximate diagnosability of the original nonlinear system $\Sigma$.

Given a set $F \subseteq \mathbb{R}^n$ and an accuracy $\varepsilon \in \mathbb{R}^+$, consider the sets

$$ F_\varepsilon = B_\varepsilon(F) \cap [\mathbb{R}^n]_\eta^n, $$

$$ F'_\varepsilon = \{ x \in F : B_\varepsilon(x) \subseteq F \} \cap [\mathbb{R}^n]_\eta^n. $$

By construction above, we get:

$$ F'_\varepsilon \subseteq (F \cap [\mathbb{R}^n]_\eta^n) \subseteq F_\varepsilon. $$

**Theorem 1:** Consider nonlinear system $\Sigma$ in (1) satisfying Assumption 4 and a set $F \subseteq \mathbb{R}^n$. Consider a triplet $\varepsilon, \eta, \mu \in \mathbb{R}^+$ of parameters satisfying (9). The following statements hold:

i) If $S_{\eta,\mu}(\Sigma)$ is $(k_\eta, F_\varepsilon)$–diagnosable, for some $k \in \mathbb{N}$, then $\Sigma$ is $(\rho, F)$–diagnosable, for any $\rho > 2\varepsilon + k_\eta$.

ii) Suppose that set $F$ is with interior and parameter $\varepsilon \in \mathbb{R}^+$ is such that

$$ F'_\varepsilon \neq \emptyset. \tag{11} $$

1Since $F$ is with interior there always exists $\varepsilon \in \mathbb{R}^+$ satisfying (11).
If $\Sigma$ is $(\rho, F)$-diagnosable, for some $\rho \in \mathbb{R}_0^+$, then $S_{\eta, \mu}(\Sigma)$ is $(k', \eta, F')$-diagnosable, for any integer

$$k' > \min\{h \in \mathbb{N} : (\rho + 2 \varepsilon) \leq h\eta\}.$$

**Proof:** (Proof of i.) By contradiction, suppose that $S_{\eta, \mu}(\Sigma)$ is $(k', \eta, F')$-diagnosable, but $\Sigma$ is not $(\rho, F)$-diagnosable, with $\rho > 2 \varepsilon + k' \eta$. Then $\forall \Delta \in \mathbb{N}$ there exists a state trajectory $x_f$ of $\Sigma$ such that for some $t > 0$

$$(x_f(t) \in F) \wedge (x(t) \notin F, \forall t \in [0; t-1])$$

and a state trajectory $x_s$ of $\Sigma$ such that

$$B_\rho(x^s(t)) \cap [R^n]_\eta \subseteq F_s.$$ (12)

and, by denoting by $y_{t+\Delta, \eta}^f$ and $y_{t+\Delta, \eta}^s$ the quantized output trajectories associated to $x_f|_{[0; t+\Delta]}$ and to $x_s|_{[0; t+\Delta]}$, respectively, we have

$$y_{t+\Delta, \eta}^f = y_{t+\Delta, \eta}^s.$$

Since $S(\Sigma) \cong \varepsilon S_{\eta, \mu}(\Sigma)$, for any state trajectory $x$ of $\Sigma$ there exists a state run $\xi(0) \xi(1) \ldots$ of $S_{\eta, \mu}(\Sigma)$, such that

$$||\xi(t) - x(t)|| \leq \varepsilon, \forall t \in \mathbb{N}$$

By construction of $F_\varepsilon$, if $x_f(t) \in F$ then

$$B_\varepsilon(x_f(t)) \cap [R^n]_\eta \subseteq F_\varepsilon.$$ (12)

Moreover, since $\rho > 2 \varepsilon + k' \eta$ and condition (12) holds, then

$$B_\varepsilon(x^s(t)) \cap F_s = \emptyset.$$ (12)

Therefore $\forall \Delta \in \mathbb{N}$ there exist two state runs $\xi'(0) \xi'(1) \ldots$ and $\xi''(0) \xi''(1) \ldots$ of $S_{\eta, \mu}(\Sigma)$, the first one such that for some $t' \in [0; t]$

$$(\xi'(t') \in F') \wedge ((t' = 0) \vee (\xi'(t') \notin F', \forall t \in [0; t'-1]))$$

and the other one such that

$$\xi''(t) \notin B_{k' \eta}(F'), \forall t \in [0; t'+\Delta]$$

with the same corresponding output runs, i.e.

$$y_{t+\Delta, \eta}^f = y_{t+\Delta, \eta}''.$$ (13)

Therefore $S_{\eta, \mu}(\Sigma)$ is not $(k', \eta, F')$-diagnosable, and the first statement follows.

(Proof of ii.) Again by contradiction, suppose that $\Sigma$ is $(\rho, F)$-diagnosable, but $S_{\eta, \mu}(\Sigma)$ is not $(k', \eta, F')$-diagnosable, with $\varepsilon, \eta, \mu$ satisfying (9), $\varepsilon$ such that $F' \neq \emptyset$, and $k' > \min_{h \in \mathbb{N}} h \eta : (\rho + 2 \varepsilon) \leq h\eta$. Then $\forall \Delta \in \mathbb{N}$ there exists a state run $\xi'_f$ of $S_{\eta, \mu}(\Sigma)$ such that for some $t > 0$

$$(\xi'_f(t) \in F'), \wedge (x_f(t) \notin F', \forall t \in [0; t-1])$$

and a state run $x_s$ of $S_{\eta, \mu}(\Sigma)$ such that

$$B_{k' \eta}(\xi'_f(t)) \cap F' = \emptyset, \forall t \in [0; t+\Delta]$$ (13)

and, by denoting with $y_{t+\Delta, \eta}^f$ and $y_{t+\Delta, \eta}^s$ the output runs associated to $\xi'_f|_{[0; t+\Delta]}$ and to $\xi'_s|_{[0; t+\Delta]}$, respectively, we have

$$y_{t+\Delta, \eta}^f = y_{t+\Delta, \eta}^s.$$ (13)

Since $S(\Sigma) \cong \varepsilon S_{\eta, \mu}(\Sigma)$, for any state run $\xi(0) \xi(1) \ldots$ of $S_{\eta, \mu}(\Sigma)$ there exists a state trajectory $x$ of $\Sigma$, such that

$$||\xi(t) - x(t)|| \leq \varepsilon, \forall t \in \mathbb{N}.$$ (13)

By construction of $F'_\varepsilon$, if $\xi'_f(t) \in F'_\varepsilon$ then

$$B_\varepsilon(\xi'_f(t)) \subseteq F'_\varepsilon.$$ (13)

Moreover, since $k' > \min_{h \in \mathbb{N}} h \eta : (\rho + 2 \varepsilon) \leq h\eta$, and since condition (13) holds, then $B_{k' \eta}(\xi'_f(t)) \cap F = \emptyset$. Therefore $\forall \Delta \in \mathbb{N}$ there exist two state trajectories $x'$ and $x''$ of $\Sigma$, the first one such that for some $t' \in [0; t]$

$$(x'(t') \in F) \wedge (x'(t') \notin F', \forall t \in [0; t'-1])$$

and the other one such that

$$x''(t) \notin B_{k' \eta}(F'), \forall t \in [0; t'+\Delta]$$

with the same corresponding quantized output trajectories, i.e.

$$y_{t+\Delta, \eta}^f = y_{t+\Delta, \eta}''.$$ (13)

Therefore $\Sigma$ is not $(k', \eta, F')$-diagnosable. Since $k' \eta \geq (\rho + 2 \varepsilon)$, then $k' \eta > \rho$, $\Sigma$ is not $(\rho, F)$-diagnosable and the proof is complete.

Remark 4: While statement i) of Theorem 1 is useful to check if $\Sigma$ is $(\rho, F)$-diagnosable, statement ii) can be used in its logical negation form as a tool to check if $\Sigma$ is not $(\rho, F)$-diagnosable.

We conclude this section with a computational complexity analysis of the approach proposed. By combining Remark 3 and Proposition 3 we get

Theorem 2: Space and time computational complexities in checking $(\rho, F)$-diagnosability of $\Sigma$ are exponential with the dimension $n$ of state space and with the dimension $m$ of the input space of $\Sigma$.

V. CONCLUSIONS

In this paper we proposed a novel notion of diagnosability, termed approximate diagnosability, for discrete-time nonlinear systems with unknown inputs and quantized output measurements. Under an assumption of incremental stability of the nonlinear system we first derived a symbolic model. We extended the classical notion of diagnosability given for DES to metric symbolic systems. We then established the relation between approximate diagnosability of the nonlinear system and approximate diagnosability of the symbolic model. Computational complexity of the approach taken is also discussed.

REFERENCES

[1] M. Sampath, R. Sengupta, S. LaFortune, K. Sinnamohideen, and D. Tenekeetzis, “Diagnosability of discrete-event systems,” IEEE Transactions of Automatic Control, vol. 40, no. 9, pp. 1555–1575, 1995.
[2] W. Wang, S. LaFortune, A. Girard, and F. Lin, “Optimal sensor activation for diagnosing discrete event systems,” Automatica, vol. 46, pp. 1165–1175, 2010.
[3] W. Wang, A. Girard, S. LaFortune, and F. Lin, “On codiagnosability and coobservability with dynamic observations,” IEEE Transactions on Automatic Control, vol. 56, no. 7, pp. 1551–1566, 2011.
