Automatica 81 (2017) 115–122

Contents lists available at ScienceDirect

Automatica

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

Brief paper

Observability and diagnosability of finite state systems: A unifying framework[☆]

Elena De Santis, Maria Domenica Di Benedetto

University of L'Aquila, DISIM, Department of Information Engineering, Computer Science and Mathematics, Center of Excellence DEWS, 67100 L'Aquila, Italy

ARTICLE INFO

Article history:
Received 22 December 2014
Received in revised form
8 February 2017
Accepted 10 February 2017

Keywords:
Observability
Diagnosability
Finite state systems

ABSTRACT

In this paper, a general framework is proposed for the analysis and characterization of observability and diagnosability of finite state systems. Observability corresponds to the reconstruction of the system's discrete state, while diagnosability corresponds to the possibility of determining the past occurrence of some particular states, for example faulty states. A unifying framework is proposed where observability and diagnosability properties are defined with respect to a critical set, i.e. a set of discrete states representing a set of faults, or more generally a set of interest. These properties are characterized and the involved conditions provide an estimation of the delay required for the detection of a critical state, of the precision of the delay estimation and of the duration of a possible initial transient where the diagnosis is not possible or not required. Our framework makes it possible to precisely compare some of the observability and diagnosability notions existing in the literature with the ones introduced in our paper, and this comparison is presented.

1. Introduction

Reconstructing the internal behavior of a dynamical system on the basis of the available measurements is a central problem in control theory. Starting from the seminal paper (Kalman, 1959), state observability has been investigated both in the continuous domain (see e.g. the fundamental papers Luenberger, 1971 for the linear case and Griffith & Kumar, 1971 for the nonlinear case), in the discrete state domain (see e.g. Ozveren & Willsky, 1990 and Ramadge, 1986), and more recently for hybrid systems (see e.g. the special issue (De Santis, 2009) on observability and observer-based control of hybrid systems and the references therein, Babaali & Pappas, 2005; Balluchi, Benvenuti, Di Benedetto, & Sangiovanni-Vincentelli, 2002; Balluchi, Benvenuti, Di Benedetto, & Sangiovanni-Vincentelli, 2013; Bemporad, Ferrari-Trecate, & Morari, 2000; Collins & van Schuppen, 2007; De Santis, Di Benedetto, & Pola, 2003; Tanwani, Shim, & Liberzon, 2013; Vidal, Chiuso, Soatto, & Sastry, 2003). In some references dealing with discrete event systems, e.g. in Lafortune (2007), the notion of observability is related to state disambiguation, which is the property of distinguishing unambiguously among certain pairs of states in the state space. We will use here the term observability in the traditional meaning used in Zaytoon and Lafortune (2013) where observability corresponds to the reconstruction of the system's discrete state. Diagnosability, a property that is closely related to observability but is more general, corresponds to the possibility of detecting the occurrence of some particular state, for example a faulty state, on the basis of the observations. An excellent survey of recent advances on diagnosis methods for discrete systems can be found in Zaytoon and Lafortune (2013). The formal definition and analysis of observability and diagnosability depend on the model, on the available output information, and on the objective for which state reconstruction is needed, e.g. for control purposes, for detection of critical situations, and for diagnosis of past system evolutions. It is therefore hard, in general, to understand the precise relationships that exist between the different notions that exist in the literature.

In this paper, we propose a unifying framework where observability and diagnosability are defined with respect to a subset of the state space, called critical set. A state belonging to the critical set is called critical state. This idea comes from safety critical applications, e.g. Air Traffic Management (De Santis, Di Benedetto, Di Gennaro, D'Innocenzo, & Pola, 2006; Di Benedetto, Di Gennaro, & D'Innocenzo, 2005b), where the critical set of discrete states represents dangerous situations that must be

[☆] The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Jan Komenda under the direction of Editor Ian R. Petersen.

E-mail addresses: elena.desantis@univaq.it (E. De Santis), mariadomenica.dibenedetto@univaq.it (M.D. Di Benedetto).

http://dx.doi.org/10.1016/j.automatica.2017.02.042
0005-1098/© 2017 Elsevier Ltd. All rights reserved.

detected to avoid unsafe or even catastrophic behavior of the system. However, the critical set can represent a set of faults, or more generally any set of interest. We define and characterize observability and diagnosability in a uniform set-membership-based formalism. The set-membership formalism and the derived algorithms are very simple and intuitive, and allow checking the properties without constructing an observer, thereby avoiding the exponential complexity of the observer design. The definitions of observability and diagnosability are given in a general form that is parametric with respect to the delay required for the detection of a critical state, and the precision of the delay estimation. Using the proposed conditions that characterize those properties, we can check diagnosability of a critical event, such as a faulty event, and at the same time compute the delay of the diagnosis with respect to the occurrence of the event, the uncertainty about the time at which that event occurred, and the duration of a possible initial transient where the diagnosis is not possible or not required. These evaluations are useful to better understand the characteristics of the system and can be used in the implementation of the diagnoser.

While in the literature on discrete event systems a transition-based model is used, we adopt a state-based approach, similarly to what was done in Lin (1994) where an on-line diagnosability problem for a deterministic Moore automaton with partial state observation was solved, in Hashtrudi Zad, Kwong, and Wonham (1971) where the focus was on the complexity reduction in the diagnoser design, and in Takai and Ushio (2012) where verification of codiagnosability is performed. Because of the different formalism used in the transition-based and state-based approaches, a comparison between our definitions and those existing in the literature on discrete event systems is very hard to achieve without a unifying framework where the different notions can all be formulated and compared. We show that, using our formalism, we are able to understand the precise relationships that exist between the properties we analyze and some of the many diagnosability concepts that exist in the literature.

The paper is organized as follows. After introducing the main definitions in Section 2, Section 3 is devoted to establishing some geometrical tools that are instrumental in proving our results. In Section 4, observability and diagnosability properties are completely characterized. The proofs are omitted for space reason and are available in De Santis and Di Benedetto (2016), where also examples are provided to better understand our results. The proofs of the main theorems are constructive and show how a diagnoser can be determined.

Notations: The symbol $\mathbb{Z}$ denotes the set of nonnegative integer numbers. For $a, b \in \mathbb{Z}$, $[a, b] = \{x \in \mathbb{Z} : a \leq x \leq b\}$. For a set X, the symbol $|X|$ denotes its cardinality. For a set $Y \subset X$, where the symbol $\subset$ has to be understood as "subset", not necessarily strict, the symbol $\overline{Y}$ denotes the complement of Y in X, i.e. $\overline{Y} = \{x \in X : x \notin Y\}$. For $W \subset X \times X$, the symbol W^{-} denotes the symmetric closure of W, i.e. $W^{-} = \{(x_1, x_2) : (x_1, x_2) \in W \text{ or } (x_2, x_1) \in W\}$. The null event is denoted by ϵ. For a string σ, $|\sigma|$ denotes its length, $\sigma(i)$, $i \in \{1, 2, \ldots, |\sigma|\}$, denotes the ith element, and $|\sigma|_{[a,b]}$ is the string $\sigma(a)\sigma(a+1)\ldots\sigma(b)$. $P(\sigma)$ is the projection of the string σ, i.e. the string obtained from σ by erasing the symbol ϵ (see e.g. Ramadge & Wonham, 1989).

2. Diagnosability properties and their relationships

We consider a Finite State Machine (FSM)

$$M = (X, X_0, Y, H, \Delta)$$

where X is the finite set of states; $X_0 \subset X$ is the set of initial states; Y is the finite set of outputs; $H : X \to Y$ is the output function; $\Delta \subset X \times X$ is the transition relation.

For $i \in X$, define $succ(i) = \{j \in X : (i, j) \in \Delta\}$ and $pre(i) = \{j \in X : (j, i) \in \Delta\}$.

We make the following standard assumption:

Assumption 1 (*Liveness*). $succ(i) \neq \emptyset, \forall i \in X$.

Any finite or infinite string x with symbols in X that satisfies the condition $x(1) \in X$ and $x(k+1) \in succ(x(k))$, $k = 1, 2, \ldots, |x| - 1$ is called a state execution (or state trajectory or state evolution) of the FSM M. The singleton $\{i \in X\}$ is an execution.

Let $\mathcal{X}^*$ be the set of all the state executions of M. Then, for a given $\Psi \subset X$, we can define the following subsets of $\mathcal{X}^*$:

- $\mathcal{X}_\Psi$ is the set of state executions $x \in \mathcal{X}^*$ with $x(1) \in \Psi$
- $\mathcal{X}_{\Psi,\infty}$ is the set of infinite state executions $x \in \mathcal{X}^*$ with $x(1) \in \Psi$. For simplicity, the set $\mathcal{X}_{X_0,\infty}$ will be denoted by $\mathcal{X}$
- $\mathcal{X}^\Psi$ is the set of finite state executions $x \in \mathcal{X}^*$ with last symbol in Ψ.

Obviously, $\mathcal{X}_X = \mathcal{X}^*$ and $\mathcal{X}_{\Psi,\infty} \subset \mathcal{X}_\Psi \subset \mathcal{X}^*$.

Let $\mathcal{Y}$ be the set of strings with symbols in $\widehat{Y} = \{y \in Y : y \neq \epsilon\}$. Define $\mathbf{y} : \mathcal{X}^* \to \mathcal{Y}$, the function that associates to a state execution the corresponding output execution, as $\mathbf{y}(x) = P(\sigma)$ where $\sigma = H(x(1)) \ldots H(x(n))$, $n = |x|$ if $|x|$ is finite. Otherwise $\mathbf{y}(x) = P(\sigma_\infty)$ where σ_∞ is an infinite string recursively defined as $\sigma_1 = H(x(1))$, $\sigma_{k+1} = \sigma_k H(x(k+1))$, $k = 1, 2, \ldots$. Finally, $\mathbf{y}^{-1}(\mathbf{y}(x)) = \left\{\widehat{x} \in \mathcal{X}_{X_0} : \mathbf{y}(\widehat{x}) = \mathbf{y}(x)\right\}$, $x \in \mathcal{X}_{X_0}$.

We now propose a framework where observability and diagnosability are defined with respect to a subset of the state space $\Omega \subset X$ called critical set. The set Ω may represent unsafe states, faulty states, or more generally any set of states of interest.

For a string $x \in \mathcal{X}$, two cases are possible: $x(k) \notin \Omega, \forall k \in \mathbb{Z}$ or $x(k) \in \Omega$, for some $k \in \mathbb{Z}$. If the second condition holds, let k_x be the minimum value of k such that $x(k) \in \Omega$. Otherwise set $k_x = \infty$.

The next definition describes the capability of inferring, from the output execution, that the state belongs to the set Ω, at some step during the execution, after a finite transient or after a finite delay or with some uncertainty in the determination of the step. The precise meaning of the parameters used to describe those characteristics will be discussed after the definition.

Definition 1. The FSM M is parametrically diagnosable with respect to a set $\Omega \subset X$ (shortly parametrically Ω-diag) if there exist τ and $\delta \in \mathbb{Z}$, and $T \in \mathbb{Z} \cup \{\infty\}$ such that for any string $x \in \mathcal{X}$ with finite k_x, whenever $x(k) \in \Omega$ and $k \in [\max\{k_x, (\tau+1)\}, k_x + T]$, it follows that for any string $\widehat{x} \in \mathbf{y}^{-1}\left(\mathbf{y}\left(x|_{[1,k+\delta]}\right)\right)$, $\widehat{x}(h) \in \Omega$, for some $h \in [\max\{1, (k-\gamma_1)\}, k+\gamma_2]$ and for some $\gamma_1, \gamma_2 \in \mathbb{Z}$, $\gamma_2 \leq \delta$.

If $x(k) \in \Omega$ for some $k \in \mathbb{Z}$, in what follows the condition $x(k) \in \Omega$ is called *crossing event*, and k is the step at which the crossing event occurs.

The value $\gamma = \max\{\gamma_1, \gamma_2\}$ is the uncertainty radius in the reconstruction of the step at which the crossing event occurred. The parameter δ corresponds to the delay of the crossing event detection while τ corresponds to an initial time interval where the crossing event is not required to be detected.

The detection of the crossing event is required whenever it occurs in the interval defined by the parameter T.

To better understand the role of these parameters, consider the examples in Fig. 1. For fixed values τ, T, δ and γ, we have represented three possible cases, corresponding to three different executions, and hence with different values for k_x. In the first case $\max\{k_x, (\tau+1)\} = (\tau+1)$. Hence, any crossing event occurring in $[(\tau+1), k_x + T]$ has to be detected, with maximum delay δ and with maximum uncertainty γ. Crossing events occurring in $[1, \tau]$ are not needed to be detected. In the second case,