Diagnosability of Discrete-Event Systems with Uncertain Observations

Xingyu Su[1,2] and **Marina Zanella**[3] and **Alban Grastien**[2,1]
[1]Artificial Intelligence Group, Australian National University, Australia
[2]Optimisation Research Group, NICTA/Data61, Australia
[3]Department of Information Engineering, University of Brescia, Italy
u4383016@anu.edu.au, marina.zanella@unibs.it, alban.grastien@nicta.com.au

Abstract

Diagnosability is the property that a Discrete-Event System (DES) exhibits if every fault can be detected and isolated within a finite number of (observable) events that have taken place after its occurrence. In the literature, diagnosability of DESs relies on the availability of a certain observation, which equals the sequence of observable events that have taken place in the DES. But can diagnosability be achieved even if the observation is uncertain? The present paper provides an answer to this question when the observation is temporally or logically uncertain, that is, when the order of the observed events or their (discrete) values are partially unknown. The original notion of compound observable event enables a smooth extension of both the definition of DES diagnosability in the literature and the twin plant method to check such a property. The intuition is to deal with a compound observable event the same way as with a single event. In case a DES is diagnosable even if its observation is uncertain, the diagnosis task can be performed (without any loss in the ability to identify every fault) although the available measuring equipment cannot get a certain observation.

1 Introduction

A DES is a conceptual model of a dynamical system, where the system behavior is described by transitions over a finite set of states and each transition is associated with an event out of a finite set of events [Cassandras and Lafortune, 2008]. Model-based diagnosis of DESs is a task that takes as input the DES model of a (natural or man-made) system along with a relevant observation and produces as output a *diagnosis*, i.e. some pieces of information explaining whether what has been observed is consistent either with a normal behavior or an abnormal one. There are several notions of diagnosis of DESs in the literature featuring different levels of abstraction. According to a common notion, the diagnosis of a DES is a set of *candidates*, each candidate being a set of *faults*, where a fault is an undesired state transition. The definition of a candidate requires that the faults included in a candidate are consistent with both the DES model and the given observation. However, distinct candidates may bring conflicting information. This is the case, for instance, when according to a candidate the system is free of faults while according to another it is affected by faults. A DES that is repeatedly diagnosed while it is being monitored (that is, a new set of candidates is produced every time a new observable event is processed) is *diagnosable* if such ambiguity can be removed once a finite sequence of observable events have taken place. Diagnosability is very desirable and system designers often want to enforce it.

DES diagnosability was introduced by the diagnoser approach [Sampath *et al.*, 1995], where a necessary and sufficient condition is proposed to check diagnosability based on the construction of a so-called *diagnoser*. The problem of deciding diagnosability was then proved to be polynomial by using the *twin plant* method [Jiang *et al.*, 2001]. Similar approaches to diagnosability checking can be found in [Yoo and Lafortune, 2002; Cimatti *et al.*, 2003]. Recently, there has been an increasing interest in applying DES techniques to the diagnosability analysis of hybrid systems [Bayoudh and Travé-Massuyès, 2014]. Existing works are focused on how to verify the intrinsic diagnosability of a DES and assume that candidates are computed by an *exact* diagnostic algorithm that takes as input a completely *certain* observation. Exceptions include diagnosability under imperfect conditions for modular structures [Contant *et al.*, 2006], decentralised analysis [Sengupta and Tripakis, 2004], and approximate diagnosers [Su and Grastien, 2014]. As remarked in this latest paper, the diagnosability property can be exhibited even when some *incomplete* or *approximate* diagnostic algorithms are used, i.e. algorithms that do not perform a complete search of the behavioral space of the DES. However, this work still relies on a completely certain observation while in the real world the observation may be uncertain, as remarked by some contributions on diagnosis of DESs [Lamperti and Zanella, 2002; Grastien *et al.*, 2007]. In a broader perspective, one can see that the ability to remove ambiguities in candidates depends not only on the DES and the diagnostic algorithm at hand but also on the available observations.

This paper investigates whether the ability to disambiguate DES candidates, i.e. the diagnosability property, holds for a diagnosable system with uncertain observations. The uncertainty is measured by a parameter, which allows to study the

level of noise that can affect the observation without impacting the performance of diagnosis. The remaining of this paper is organized as follows. The next section presents the relevant literature review on DES diagnosability. Section 3 introduces uncertain observations along with the notions of compound observable event and uncertainty measure. Section 4 extends the original definition of DES diagnosability to the case when an uncertain observation is considered. It also extends the twin plant method so as to check diagnosability of DESs with uncertain observations. Finally, Section 5 draws conclusions and hints at directions for future research.

2 Background

A DES diagnosis problem consists in a DES D and a (finite) observation O, the latter representing what has been observed while D was running during a time interval of interest.

2.1 Discrete Event Systems

A (partially observable) DES D is a 4-tuple $(\Sigma, L, obs, \mathit{flt})$, where Σ is the finite set of events that can take place in the system; $L \subseteq \Sigma^*$ is the *behavior space*, which is a prefix-closed and live, i.e. deadlock-free, language that models all (and only) the possible sequences of events, or *traces*, that can take place in the system. Function obs associates each trace τ with an observation $obs(\tau) \in \Sigma_o^*$ and is defined as the projection of τ on the subset $\Sigma_o \subseteq \Sigma$ of observable events, i.e. $obs(\tau)$ is a copy of τ, where all non-observable events have been removed. The length of the sequence of events in $obs(\tau)$ is denoted $|obs(\tau)|$. $obs(L)$ is the prefix-closed and live observable language relevant to L [1]. The set of unobservable *faulty events*, or *faults*, is denoted as Σ_f, where $\Sigma_f \subseteq \Sigma \setminus \Sigma_o$. Function *flt* associates each trace τ with the sequence $\mathit{flt}(\tau) \in \Sigma_f^*$ of faulty events that appear in the trace itself.

Language L of DES $D = (\Sigma, L, obs, \mathit{flt})$ can be represented by a finite automaton (FA) $G = (X, \Sigma, \delta, x_0)$, called the *behavioral model*, where X is the set of states and $\delta \subseteq X \times \Sigma \times X$ is the set of state transitions. Each $x \in X$ represents a state that D can be in and each triple $(x, \sigma, x') \in \delta$ represents a possible state change. State $x_0 \in X$ is the *initial* one, i.e. the state of the system at the moment when we have started to observe its evolution. A *path* in automaton G is a sequence of transitions starting from the initial state, concisely represented as $x_0 \xrightarrow{\sigma_1} x_1 \xrightarrow{\sigma_2} \cdots \xrightarrow{\sigma_n} x_n$, where $n \geq 1$. A trace is a projection of a path on Σ, e.g. $\sigma_1.\cdots.\sigma_n$. Figure 1 displays the behavioral model G of a DES D that will be used as a running example throughout this paper. Such a model encompasses one faulty event f, another unobservable event u, and seven observable events (a–e, g, and h). A possible path is $0 \xrightarrow{h} 8 \xrightarrow{g} 9 \xrightarrow{e} 3 \xrightarrow{f} 4 \xrightarrow{c} 4$, corresponding to the trace $h.g.e.f.c$, where . is the concatenation operator.

Given a diagnosis problem (D, O), a diagnosis *candidate* is a pair $(x, \varphi) \in X \times 2^{\Sigma_f}$, where x represents the state that system D has reached by a path generating O and φ represents the set of faults of this path. The *diagnosis* is the set of all the candidates relevant to the diagnosis problem (D, O). The diagnosis relevant to our sample system D in Figure 1 and observation $O = h.g.e.c$ is $\{(4, \{f\})\}$. Such a diagnosis consists of just one candidate, meaning that, once observation O has been perceived, the state of D is certainly 4 and fault f has necessarily occurred.

[1] Note that the fact that L is assumed to be live does not imply that $obs(L)$ is live. However, following the diagnoser approach [Sampath *et al.*, 1995], we also assume that $obs(L)$ is live.

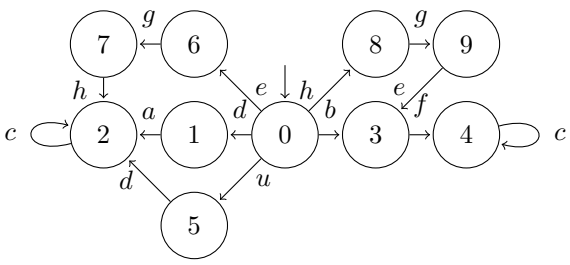

Figure 1: A $||^{//2}$-diagnosable DES model that is not $||^{//3}$-diagnosable (and it is not $||^{\#2}$-diagnosable)

2.2 Diagnosability

Following [Sampath *et al.*, 1995], a DES D exhibits the diagnosability property as far as a fault $f \in \Sigma_f$ is concerned if the occurrence of such a fault can always be detected and isolated without any ambiguity once a finite sequence of observable events has been recorded. Given an observation, an exact diagnostic algorithm is able to draw all the sets of faults relevant to all the traces consistent with such an observation. If, for whichever path that has preceded the occurrence of the fault, and for whichever sequence of transitions (generating k observable events) that has followed it, all the traces that are consistent with such an observation include the fault, then such a fault is certain (and it is said to be diagnosable) as it belongs to the intersection of all the candidate sets of faults. The system is said to be diagnosable if all its faults are diagnosable. We denote $L_f = (\Sigma^* f \Sigma^*) \cap L$ the set of traces that include fault f and $\bar{L}_f = (\Sigma^* f) \cap L$ the set of traces that end with fault f.

Definition 1 (Diagnosability [Sampath *et al.*, 1995])**.** *Given a DES $D = (\Sigma, L, obs, \mathit{flt})$ whose set of faults is $\Sigma_f \subseteq \Sigma$, a fault $f \in \Sigma_f$ is* diagnosable *if*

$$\forall \tau_1 \in \bar{L}_f, \exists k \in \mathbf{N}, \forall \tau_2 : \tau_1.\tau_2 \in L, |obs(\tau_2)| \geq k \Rightarrow$$
$$(\forall \tau \in L), (obs(\tau) = obs(\tau_1.\tau_2) \Rightarrow (\tau \in L_f)).$$

System D is diagnosable *if all its faults are diagnosable.*

DES D of our example in Figure 1 is diagnosable with $k = 1$ since the occurrence of fault f is precisely detected once the occurrence of observable event c has been perceived immediately after having perceived either b or $h.g.e$. One can appreciate that such a notion of diagnosability relies on the function obs, which provides the sequence of observable events that have occurred in the system during its evolution, where such a sequence reflects the chronological order of the occurrence of events within a trace. The above definition of diagnosability implicitly assumes that, if a DES follows a trace u, the observation O processed by the diagnostic engine equals *obs(u)*. An observation like this is *certain*.

3 Temporal and Logical Uncertainty of Observations

In the literature, diagnosability has so far been confined to certain observations. However, observation are uncertain in many applications. We present two types of uncertainties, i.e. temporal and logical, and for each of them, a measure of how uncertain the observation is. These measures are by no means the only ones possible.

3.1 Temporally Uncertain Observations

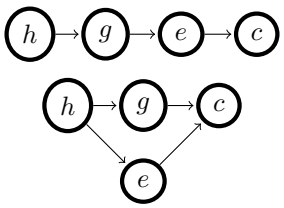

Figure 2: Certain (top) and temporally uncertain (bottom) observations

In observation $O = h.g.e.c$ used above, the occurrence order of the observable events is known. This observation is depicted in the top graph of Figure 2, where the order is represented by the arrows between observed events. Implicit arrows, e.g. from h to e, are not displayed. We say that the observation is *temporally certain*. However, the temporal order of the observable events that have occurred within the DES is not always known, in particular when they occur in a short time span. The bottom graph of Figure 2 shows a *temporally uncertain* observation O', where the order between observable events g and e is unknown. Since we do not know which sequence, i.e. either $h.g.e.c$ or $h.e.g.c$, actually occurred, an exact diagnostic algorithm has to consider both of them. The pair of observable events e and g can altogether be considered as a *temporally compound event* $e//g$, which cumulatively represents both sequences $e.g$ and $g.e$. We can describe the uncertain observation as a sequence $O' = h.e//g.c$.

Definition 2 (Temporally compound observable event)**.** *A* temporally compound observable event *of level ℓ (with $\ell \geq 1$) is a multiset of ℓ reciprocally temporally unrelated instances of observable events. When $\ell > 1$, not all the ℓ instances are identical. A temporally compound event of level* 1 *is a* single *observable event.*

We use $\left(\!\!\binom{\Sigma_o}{k}\!\!\right)$ and $\left(\!\!\binom{\Sigma_o}{\leq k}\!\!\right)$ to denote the collection of multisets of Σ_o of cardinality k and of cardinality k or less, respectively. Notice that $\left(\!\!\binom{\Sigma_o}{\leq k}\!\!\right) = \bigcup_{i \leq k} \left(\!\!\binom{\Sigma_o}{i}\!\!\right)$. Although a temporally compound event is univocally identified by writing the values of all the instances that it includes, independently of their order, using // as a separator, we put such values in alphabetical order in this paper.

Definition 3 (Temporal uncertainty level)**.** *A* temporally uncertain observation *is a sequence of temporally compound observable events. The* temporal uncertainty level *of a temporally uncertain observation O is the maximum level of the compound observable events that O includes.*

The lowest temporal uncertainty level of an observation is 1 corresponding to a certain observation. The temporal uncertainty level of the observation in the bottom graph of Figure 2 instead is 2, since events e and g are reciprocally temporally unrelated. Notice that the temporally uncertain observations defined above do not encompass all the temporally uncertain observations as defined in [Lamperti and Zanella, 2002]. However, the class of temporally uncertain observation we are addressing is meaningful. If an exact diagnostic algorithm is adopted to diagnose a DES in a monitoring context, the diagnosis output is *monotonic* [Lamperti and Zanella, 2011] for whichever temporally uncertain observation that is a sequence of temporally compound events, provided that a new set of candidates is output only after all the observable events in a temporally compound event have been processed.

3.2 Logically Uncertain Observations

A temporally uncertain observation is a certain observation, where some temporal constraints have been relaxed. Similarly, a logically uncertain observation is a *logical* relaxation of a certain one. The so-called logical content [Lamperti and Zanella, 2002] of an observed event is its (discrete) value. If such a value is not known with certainty, the relevant observation is logically uncertain.

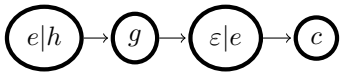

Figure 3: Logically uncertain observation

Figure 3 shows a logically uncertain observation, where the logical uncertainty comes from the fact that i) the first observed event is not known with certainty, i.e. it could be either e or h, and ii) whether the third observed event (e) actually occurred is not certain, which is represented by ε. Since we do not know which sequence (either $h.g.e.c$ or $h.g.c$ or $e.g.e.c$ or $e.g.c$) actually occurred, an exact diagnostic algorithm has to consider all of them.

Because logically uncertain observations may include ε, we use the notation $\Sigma_{o+} = \Sigma_o \cup \{\varepsilon\}$. We define a logically compound observable event as a set of events belonging to Σ_{o+}. The *degree* of this compound event, tantamount to the level of a temporally compound observable event, is here defined as the maximal *distance* according to a specified distance matrix (increased by 1 for normalization) between any pair of events included in the compound event.

Definition 4 (Distance matrix and logically compound observable event)**.** *The* distance matrix M *is a map that associates any pair in $\Sigma_o \times \Sigma_{o+}$ with a (possibly infinite) non-negative integer while respecting these constraints, i.e. $\forall (e_1, e_2) \in \Sigma_o \times \Sigma_{o+}$, $M(e_1, e_2) = 0$ if $e_1 = e_2$, $M(e_1, e_2) > 0$, if $e_1 \neq e_2$, $M(e_2, e_1) = M(e_1, e_2)$, if $e_2 \neq \varepsilon$. A* logically compound observable event *o of degree d (with $d \geq 1$) is a non-empty subset of elements from Σ_{o+}, that is not the singleton $\{\varepsilon\}$, such that $d = \max\{M(e_1, e_2) \mid \{e_1, e_2\} \subseteq o)\}$*

+ 1. A logically compound event of degree 1 *is a* single *observable event.*

Given the system D in Figure 1, we assume that observable events b and d are hard to distinguish. We also assume that a, e, and h are less difficult to distinguish, and sometimes it is difficult to find out whether what has been perceived is either pure noise (that is, no observable event has occurred in the DES) or observable event e. This can be modeled by $M(b,d) = 1$; $M(a,e) = M(a,h) = M(e,h) = 2$; $M(e,\varepsilon) = 3$; and $M(\cdot) = \infty$ for any other pair of distinct elements.

We use $2^{\Sigma_{o+},d}$ and $2^{\Sigma_{o+},\leq d}$ to denote the collection of subsets of Σ_{o+}, where each subset represents a logically compound observable event of degree d, and d or less, respectively. Notice that $2^{\Sigma_{o+},\leq d} = \bigcup_{i\leq d} 2^{\Sigma_{o+},i}$. We use the symbol $\#$ as a separator to represent the logically compound observable event, e.g. $e\#h$. Although a logically compound event is univocally identified by writing all the values that are included, independently of their order, we put such values in an order in this paper so that ε precedes any other event and all the other events are in alphabetical order.

Definition 5 (Logical uncertainty degree)**.** *A* logically uncertain observation *is a sequence of logically compound observable events. The* logical uncertainty degree *of a logically uncertain observation is the maximum degree of the logically compound events that are included.*

The logical uncertainty degree of observation $e\#h.\,g.\,\varepsilon\#e.\,c$ depicted in Figure 3 is 4 because the distance between ε and e is 3.

3.3 Unifying Uncertainty Representations

The examples presented in this paper use either pure temporal uncertainty or pure logical uncertainty. However, a combination of both uncertainties could be adopted. To make the next definitions independent of the specific type of the considered uncertainty and of its measure (since several measures can be envisaged for the same uncertainty type), we introduce the *extension* of an observation. Such a notion encapsulates both the specific kind of uncertainty and its value according to a specific measure.

Definition 6 (Extension)**.** *Given a type of uncertainty $\|$, the value m of a specific measure of this uncertainty, and a certain observation O, the* extension $||O||^{\|m}$ *of the observation is the set of certain and uncertain observations that O could produce according to the given uncertainty type and up to the given uncertainty measure, where $O \in ||O||^{\|m}$.*

We now talk about $\|^m$ as the uncertainty that can affect the observation produced by the system. For instance, we denote the extension up to temporal uncertainty of level ℓ as $||O||^{//\ell}$ and denote the extension up to logical uncertainty of degree d as $||O||^{\#d}$. In our example, given the trace τ whose certain observation is $obs(\tau) = h.\,g.\,e.\,c$, the extension of such an observation to the second temporal uncertainty level is $||obs(\tau)||^{//2} = \{h.\,g.\,e.\,c, h.\,g.\,c//e, h.\,e//g.\,c, g//h.\,e.\,c, g//h.\,c//e\}$, while its extension to the third logical uncertainty degree based on the distance matrix provided in Section 3.2 is $||obs(\tau)||^{\#3} = \{x.\,g.\,y.\,c\}$, which is a set including sixteen sequences, where $x \in \{h, a\#h, e\#h, a\#e\#h\}$ and $y \in \{e, a\#e, e\#h, a\#e\#h\}$. Notice that $||obs(\tau)||^{//1} = ||obs(\tau)||^{\#1} = \{h.\,g.\,e.\,c\}$, i.e. these extensions give a certain observation. This is a general property, i.e. for any trace τ, $||obs(\tau)||^{//1} = ||obs(\tau)||^{\#1} = \{obs(\tau)\}$ since both $||^{//1}$ and $||^{\#1}$ comprise no uncertainty. Given an uncertain observation O_{u}, the fact $O_{\mathrm{u}} \in ||O_1||^{\|m} \cap ||O_2||^{\|m}$ for certain observations O_1 and O_2 means that observable behavior O_1 can be mistaken for observable behavior O_2 if the observation is affected by uncertainty $\|^m$.

4 Diagnosability with Uncertain Observations

This section proposes a definition of diagnosability with an observation affected by a (generic) uncertainty $\|^m$. According to this generalized definition, a faulty behavior should always eventually produce an observation that cannot be mistaken for an observation produced by a nominal behavior.

Definition 7 (Diagnosability under uncertainty)**.** *Given a DES $D = (\Sigma, L, obs, flt)$ with a set of faults $\Sigma_f \subseteq \Sigma$ and an uncertainty $\|^m$, a fault $f \in \Sigma_f$ is* $\|^m$-diagnosable *if*

$$\forall \tau_1 \in \bar{L}_f, \exists k \in \boldsymbol{N}, \forall \tau_2 : \tau_1.\,\tau_2 \in L, |obs(\tau_2)| \geq k \Rightarrow (\forall \tau \in L),$$
$$\left(||obs(\tau_1.\,\tau_2)||^{\|m} \cap ||obs(\tau)||^{\|m} \neq \emptyset \Rightarrow (\tau \in L_f)\right).$$

System D is $\|^m$-diagnosable *if every fault $f \in \Sigma_f$ is $\|^m$-diagnosable.*

Comparing Definition 1 with Definition 7, it is easy to see that the latter one is a generalization of the former since $||O||^{\|m}$ is a singleton when $\|^m$ comprises no uncertainty. System D in Figure 1 is $||^{//2}$-diagnosable. Indeed, fault f is identified by observing either $b.\,c^*$ or $e.\,c^*$; changing the order of two consecutive observed events does not eliminate the fact that b will be observed; a temporally uncertain observation with level $\ell \leq 2$ will not modify the order between h and e. However, the system is not $||^{//3}$-diagnosable since observation $e//g//h.\,c^*$ cannot be precisely diagnosed as it is relevant both to a normal and a faulty trace.

Given the distance matrix provided in Section 3.2, let us now consider the degree of logical uncertainty as 2. Hence, only events whose distance value between them is up to 1 need to be considered, i.e. the only uncertainty lies in event b, which may be confused with d. If the logically uncertain observation $b\#d.\,c^*$ is perceived, the diagnosis task cannot find out whether fault f has occurred or not, which proves that D is not $||^{\#2}$-diagnosable.

Notice how the definition of diagnosability is well-behaved w.r.t. increasing uncertainty. If uncertainty $||''$ is stronger than $||'$, i.e. $||O||'' \supseteq ||O||'$ for any certain observation O, then $||''$-diagnosability implies $||'$-diagnosability. Given a sequence $||^1, ||^2, \ldots$ of increasingly stronger uncertainties, the maximum index i such that the system is $||^i$-diagnosable (or 0, if the DES is not diagnosable even for certain observations, or $+\infty$, if there does not exist any upper bound for i) defines the robustness of the system w.r.t. uncertainty. Since temporal uncertainty is increasingly stronger for increasing values

of the uncertainty level and logical uncertainty is increasingly stronger for increasing values of the uncertainty degree (for any given distance matrix), we can conclude that the sample DES D is not $||^{//\ell}$-diagnosable for any $\ell > 2$ and it is not $||^{\#d}$-diagnosable for any $d > 1$.

4.1 Diagnosability and Temporal Uncertainty

The most popular approach to diagnosability analysis is the twin plant method [Jiang *et al.*, 2001], which synchronizes two completely observable FAs, called *verifiers*, to search for non-diagnosable faulty behaviors. We now present the $||^{//\ell}$-verifier, which is the verifier that incorporates temporal uncertainty.

Definition 8 ($||^{//\ell}$-Verifier)**.** *Let $D = (\Sigma, L, obs, flt)$ be a DES, where $\Sigma_o \subseteq \Sigma$ and $\Sigma_f \subseteq \Sigma$ are the sets of observable and faulty events, respectively. Let $G = (X, \Sigma, \delta, x_0)$ be the FA generating L. The $||^{//\ell}$-verifier relevant to a fault $f \in \Sigma_f$ is the FA $G^{//\ell} = (X^{//\ell}, \Sigma^{//\ell}, \delta^{//\ell}, x_0^{//\ell})$ defined as follows:*

- $X^{//\ell} = X \times \{N, F\}$ *and* $x_0^{//\ell} = (x_0, N)$*;*
- $\Sigma^{//\ell} = \left(\!\!\binom{\Sigma_o}{\leq \ell}\!\!\right)$*; and*
- $\delta^{//\ell} = \{((x,\phi), w, (x',\phi')) \in X^{//\ell} \times \Sigma_o^{//\ell} \times X^{//\ell} \mid \exists x \xrightarrow{\sigma_1} \dots \xrightarrow{\sigma_n} x'.\ w \in ||obs(\sigma_1.\cdots.\sigma_n)||^{//\ell} \wedge (\phi' = N \Leftrightarrow \phi = N \wedge f \notin \{\sigma_1, \dots, \sigma_n\})\}$.

The size of the $||^{//\ell}$-verifier relevant to a fault and the computational complexity of its construction is $O(|X|^2|\Sigma^{//\ell}|) = O(|X|^2|\Sigma_o|^\ell)$.

Once $G^{//\ell}$ has been built, it has to be synchronized with itself, which results in the twin plant. A state of the twin plant is *ambiguous* if it matches the pattern $((x, N), (x', F))$ or $((x, F), (x', N))$. Diagnosability holds if no loop includes ambiguous states, as stated in Theorem 1. Notice that if a state in a loop is ambiguous, then all the states in the same loop are ambiguous.

Theorem 1. *Given a DES D whose behavior is represented by FA $G = (X, \Sigma, \delta, x_0)$ and the $||^{//\ell}$-verifier $G^{//\ell}$, fault f in D is $||^{//\ell}$-diagnosable iff $G^{//\ell} \otimes G^{//\ell}$ contains no loop of ambiguous states.*

Proof outline: The proof is similar to the corresponding one in the classical twin plant approach [Jiang *et al.*, 2001]. A loop of ambiguous states proves that there is an infinite ambiguous path in the twin plant. By construction, an infinite ambiguous path in the twin plant betrays the existence of two infinite behaviors of the DES, a nominal one and a faulty one, that can indefinitely generate the same uncertain observation, which shows that the finite delay k in Definition 7 after which the fault can be diagnosed does not exist. □

The complexity of the whole method to check the $||^{//\ell}$-diagnosability of a fault is $O(|X|^4|\Sigma_o|^\ell)$.

The $||^{//2}$-verifier for our sample DES D in Figure 1 is depicted in Figure 4. Instead of displaying all the transitions having the same source and target nodes, just one is shown, which is labeled by all the events triggering these transitions, where $+$ is a separator.

4.2 Diagnosability and Logical Uncertainty

Logical uncertainty requires a more involved verifier. The main issue stems from the fact that an unbounded number of observation fragments such as $\varepsilon\#e$ could be generated without any transition actually taking place in the system; we shall call them *interrupting fragments*. However, the condition specified in the definition of diagnosability only applies to system paths of non-trivial length, i.e. the k parameter in the definition. Therefore, sequences of interrupting fragments, regardless how long, need to be ignored as they do not represent arbitrary long paths in the system.

The purpose of the twin plant is to exhibit an infinite faulty path on the system, every prefix of which generates an observation similar to that of a non-faulty path. The idea of the verifier is to create copies $\langle x, b, x'\rangle$ of transition $\langle x, a, x'\rangle$ whenever $M(a, b) + 1 \leq d$. As usual, the states are actually augmented with a label N or F that records whether a fault has occurred. In order to account for interrupting fragments, we also define *interruption transitions* δ_3 in Definition 9, which are loops labeled by ε. The semantics of such transitions is that nothing happened on the system but the sensors wrongly detected an observable event.

However, diagnosability cannot be checked with such verifier because the twin plant may now include cycles of interruption transitions. In order to prevent the inclusion of those cycles, we record the state flag F if an observable event has just occurred; otherwise, we record F'. We then search for cycles that contain at least one F state (cf. Theorem 2).

Definition 9 ($||^{\#d}$-Verifier)**.** *Let $D = (\Sigma, L, obs, flt)$ be a DES, where $\Sigma_o \subseteq \Sigma$ and $\Sigma_f \subseteq \Sigma$ are the sets of observable and faulty events, respectively. Let $G = (X, \Sigma, \delta, x_0)$ be the FA generating L. Let M be the distance matrix. The $||^{\#d}$-verifier relevant to a fault $f \in \Sigma_f$ is the FA $G^{\#d} = (X^{\#d}, \Sigma^{\#d}, \delta^{\#d}, x_0^{\#d})$ defined as follows:*

- $X^{\#d} = X \times \{N, F, F'\}$ *and* $x_0^{\#d} = (x_0, N)$*;*
- $\Sigma^{\#d} = \Sigma_o \cup \{\varepsilon\}$*; and*
- $\delta^{\#d} = \delta_1 \cup \delta_2 \cup \delta_3$*, where*
  - $\delta_1 = \{((x,\phi), e, (x',\phi')) \in X^{\#d} \times \Sigma^{\#d} \times X^{\#d} \mid \exists e' \in \Sigma_o.\ (x, e', x') \in \delta \wedge M(e, e') + 1 \leq d \wedge (\phi' \in \{N, F\}) \wedge (\phi' = N \Leftrightarrow \phi = N)\}$ *;*
  - $\delta_2 = \{((x,\phi), \varepsilon, (x',\phi')) \in X^{\#d} \times \Sigma^{\#d} \times X^{\#d} \mid \exists e' \in \Sigma \setminus \Sigma_o.\ (x, e', x') \in \delta \wedge (\phi' \in \{N, F'\}) \wedge (\phi' = N \Leftrightarrow \phi = N \wedge e \neq f)\}$ *;*
  - $\delta_3 = \{((x,\phi), \varepsilon, (x,\phi')) \in X^{\#d} \times \Sigma^{\#d} \times X^{\#d} \mid (\phi' \in \{N, F'\}) \wedge (\phi' = N \Leftrightarrow \phi = N)\}$.

The set of transitions of the verifier is partitioned into δ_1, the transitions corresponding to an observable event; δ_2, the transitions corresponding to a non-observable event; and δ_3, the interruption transitions.

The size of the $||^{\#d}$-verifier relevant to a fault is $O(|X|^2|\Sigma_o|)$.

Theorem 2. *Given a DES D whose behavior is represented by FA $G = (X, \Sigma, \delta, x_0)$, a distance matrix M, and the $||^{\#d}$-verifier $G^{\#d}$, fault f in D is $||^{\#d}$-diagnosable iff $G^{\#d} \otimes G^{\#d}$ contains no loop with an ambiguous state, i.e. a state $((x, N), (x', F))$ or $((x, F), (x', N))$.*

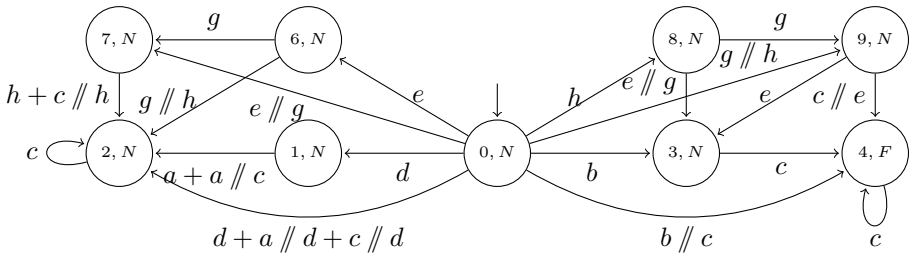

Figure 4: $||^{//2}$-verifier for the example of Figure 1

Proof outline: The proof is similar to that of Theorem 1. The only difference is that it suffices for a loop to include an ambiguous state (instead of including ambiguous states only) and conclude that an infinite behavior after the fault is possible along which the diagnosis task cannot discriminate whether the fault has occurred. □

The complexity of the whole method to check the $||^{\#d}$-diagnosability of a fault is $O(|X|^4|\Sigma_o|)$.

Although checking diagnosability when the observation is both temporally and logically uncertain is beyond the scope of this paper, we briefly mention it here. If we want to find out whether a fault is ($||^{\#d}$ and $||^{//\ell}$)-diagnosable, we first transform G into $G_{\#} = (X, \Sigma, \delta_{\#}, x_0)$, where $\delta_{\#}$ is initially set to δ, i.e. $\forall e_1 \in \Sigma_o, \forall e_2 \in \Sigma_{o+}$ such that $M(e_1, e_2) \leq d-1$, $\forall (x, e_1, x') \in \delta$, we add (x, e_2, x') to $\delta_{\#}$. Then, we apply the method described in Section 4.1 to $G_{\#}$. If the relevant twin plant does not include any loop of ambiguous states, we can conclude that the fault is diagnosable for whichever observation that mixes $||^{\#d}$ uncertainty and $||^{//\ell}$ uncertainty.

5 Conclusions

This paper investigates how uncertainty in observations can affect the diagnosability of a DES, i.e. the ability of detecting a fault without any ambiguity within a finite number of observable events after the fault has occurred. The analysis is carried out in a scenario, where the considered DES is diagnosable according to the original definition of DES diagnosability in the literature (that is, it is diagnosable given a certain observation) and the diagnostic algorithm is exact. In particular, the paper deals with the above topic in the context of event-based approaches to fault modeling [Jéron *et al.*, 2006] and a relaxation of either the temporal constraints or the logical constraints between observed events is considered.

In the former case, the observation becomes a sequence of compound temporal events. If the maximum cardinality of the considered temporally compound events is i (which is called the *temporal uncertainty level* of the observation), this means that, after i (single) observable events have been recorded, we may be unable to find out in which temporal order they were produced by the DES. This is the case, for instance, when the observable events are conveyed to the observer through distinct channels, having distinct clocks or delays, and the synchronization error of these clocks (or the—possibly varying—length of these delays) is such that at most i events can be received without the observer being able to disclose their reciprocal temporal order.

In the latter case, the observation becomes a sequence of compound logical events. If the degree of logical uncertainty is i, each observable event occurred in the DES may be confused with some other observable event(s) or even with pure noise, provided that its distance from them is less than i. This is the case, for instance, when the observable events are conveyed to the observer through channels affected by noise. Hence, both temporal and logical relaxations are quite meaningful and representative of real world situations.

This paper provides a definition of DES diagnosability that extends the original definition [Sampath *et al.*, 1995] in the literature, as well as a method to check whether the newly defined property holds for a given DES, that extends the original twin plant method [Jiang *et al.*, 2001] considering temporal and logical uncertainty. If a DES is diagnosable even if the observation has a temporal uncertainty level of value $i > 1$ or a logical uncertainty degree $i > 1$, the diagnosis task can be performed without any loss in the ability to disambiguate candidates although the available measuring equipment cannot get a certain observation. The higher the uncertainty level/degree that still guarantees diagnosability, the less expensive the needed measuring equipment and its design.

Future research can follow two orthogonal directions, one focused on the distribution and the other on the extension of the proposed conceptual framework. Such a framework is currently based on a global model of the DES at hand and on its monolithic processing. Instead, the model can be compositional and a distributed processing method can be adopted. As to the second research direction, the new definition of DES diagnosability and the proposed method to check it could be adapted to state-based approaches of fault modeling. In addition, all kinds of temporal uncertainty should be addressed including the relaxations of temporal constraints that are not sequences of temporally compound events but bring to uncertain observations. A further challenge is to define diagnosability in the frame of temporal uncertainty, logical uncertainty, and approximate diagnostic algorithms altogether.

Acknowledgements

NICTA is funded by the Australian Government through the Department of Communications and by the Australian Research Council through the ICT Centre of Excellence Program.

The authors thank the reviewers for their comments.

References

[Bayoudh and Travé-Massuyès, 2014] M. Bayoudh and L. Travé-Massuyès. Diagnosability analysis of hybrid systems cast in a discrete-event framework. *Journal of Discrete Event Dynamical Systems*, 24(3):309–338, 2014.

[Cassandras and Lafortune, 2008] C. Cassandras and S. Lafortune. *Introduction to Discrete Event Systems (2nd ed.)*. Springer, New York, N.Y., 2008.

[Cimatti *et al.*, 2003] A. Cimatti, C. Pecheur, and R. Cavada. Formal verification of diagnosability via symbolic model checking. In *Proceedings of the 18th International Joint Conference on Artificial Intelligence*, pages 363–369, 2003.

[Contant *et al.*, 2006] O. Contant, S. Lafortune, and D. Teneketzis. Diagnosability of discrete event systems with modular structure. *Journal of Discrete Event Dynamical Systems*, 16:9–37, 2006.

[Grastien *et al.*, 2007] A. Grastien, Anbulagan, J. Rintanen, and E. Kelareva. Diagnosis of discrete-event systems using satisfiability algorithms. In *Proceedings of the 22nd Conference on Artificial Intelligence*, pages 305–310, 2007.

[Jéron *et al.*, 2006] T. Jéron, H. Marchand, S. Pinchinat, and M.-O. Cordier. Supervision patterns in discrete-event systems diagnosis. In *Proceedings of the 17th International Workshop on Principles of Diagnosis*, pages 117–124, 2006.

[Jiang *et al.*, 2001] S. Jiang, Z. Huang, V. Chandra, and R. Kumar. A polynomial algorithm for testing diagnosability of discrete event systems. *IEEE Transactions on Automatic Control*, 46(8):1318–1321, 2001.

[Lamperti and Zanella, 2002] G. Lamperti and M. Zanella. Diagnosis of discrete-event systems from uncertain temporal observations. *Artificial Intelligence*, 137(1–2):91–163, 2002.

[Lamperti and Zanella, 2011] G. Lamperti and M. Zanella. Monitoring of active systems with stratified uncertain observations. *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans*, 41(2):356–369, 2011.

[Sampath *et al.*, 1995] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis. Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, 40(9):1555–1575, 1995.

[Sengupta and Tripakis, 2004] R. Sengupta and S. Tripakis. Decentralized diagnosability of regular languages is undecidable. In *Proceedings of the 43rd IEEE Conference on Decision and Control*, pages 423–428, 2004.

[Su and Grastien, 2014] X. Su and A. Grastien. Verifying the precision of diagnostic algorithms. In *Proceedings of the 21st European Conference on Artificial Intelligence*, pages 861–866, 2014.

[Yoo and Lafortune, 2002] T. Yoo and S. Lafortune. Polynomial-time verification of diagnosability of partially observed discrete-event systems. *IEEE Transactions on Automatic Control*, 47(9):1491–1495, 2002.