Kalpa Publications in Computing

Volume 4, 2018, Pages 78–93

28th International Workshop on
Principles of Diagnosis (DX'17)

Asymmetric Diagnosability Analysis of Discrete-Event Systems

Marina Zanella

Department of Information Engineering, University of Brescia, Brescia, Italy
e-mail: marina.zanella@unibs.it

Abstract

The twin plant method is central in every research whose focus is checking the diagnosability of discrete-event systems (DESs). Although the property of diagnosability has been extended over time, and several proposals have been advanced to perform a distributed analysis, diagnosability checking still relies on the exploitation of the twin plant method. However, the twin plant structure is redundant, which is a drawback, above all if the considered DES observation is uncertain: in such a case, several distinct twin plants have to be built in order to check the diagnosability for increasing levels of uncertainty. A higher uncertainty level requires a twin plant of larger size. The paper first gives some preliminary thoughts to the reduction of the twin plant size. Next, on the ground that no contribution in the literature has altered the original state-based representation of the twin plant, the paper shows how to transform such a representation into a transition-based one. Finally, it reports some investigations aimed at reducing the effort needed to produce each twin plant: a twin plant inherent to a higher uncertainty level can be produced by incrementing the twin plant relevant to the lower level.

1 Introduction

A Discrete-Event System (DES) [1] 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. Some state transitions are observable outside the system, that is, the DES usually exhibits a partial observability. Model-based diagnosis of DESs is a task that takes as input the complete DES model (i.e. a model encompassing both normal and abnormal state changes) of a (natural or man-made) system along with a relevant observation. The task 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 some 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 an ambiguity can be removed once a finite sequence of observable events have taken place.

The property of diagnosability of DESs was defined in the diagnoser approach [2], where a necessary and sufficient condition is proposed to check diagnosability based on the construction of a so-called *diagnoser*. However, the most famous approach to checking whether this property holds for a given DES is the *twin plant* method [3], whose time complexity is polyomial. A similar approach to diagnosability checking, whose complexity is still polynomial, is presented in [4]. Finding out whether the condition for diagnosability expressed by the twin plant method holds was formulated also as a model-checking problem [5, 6] or a satisfiability problem [7].

Research on diagnosability of DESs has been quite active for several years, and the interest in the topic is going to increase, possibly for DES techniques can be applied to the diagnosability analysis of hybrid systems [8]. Moreover, while both the original notion of DES diagnosability and the traditional twin plant method assume that faults are permanent, a new definition of diagnosability relevant to intermittent faults and a consequent adaptation of the twin plant method can be found in [9]. Another research line is aimed at performing distributed diagnosability analysis [10, 11], based on a distributed modeling of the considered DES.

Most of 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. As remarked in [12], 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. The ability to disambiguate DES candidates for a diagnosable system with uncertain observations is discussed in [13]. 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 diagnosability analysis is still performed by adopting the twin plant method (or a variant).

The twin plant is a finite automaton (FA), resulting from the product of an FA, representing the DES observable behavior, by itself. The two operands can be regarded as a pair of twin FAs, say the left one and the right one. The result of such a synchronization is redundant as a pair of distinct observationally identical paths are synchronized twice, that is, both assigning the former path to the left twin and the latter to the right twin and vice versa. The claim here is that an *asymmetric* handling, such that a faulty path is assigned just to the left twin, would reduce the size of the twin plant.

In all the contributions in the literature, the representation of the twin plant is state-based: a DES model is represented in a state-based fashion if the set of its states is explicitly partitioned into two parts, one containing the *normal* states, the other the *faulty* ones. When faults are assumed to be persistent, a state-based representation of a DES can equivalently be replaced by a transition-based (or event-based) one [6]. This paper transforms the notion of the twin plant in a transition-based one, and updates the condition for diagnosability straightforwardly. Finally, it reports some investigations aimed at reducing the effort needed to produce each transition-based twin-plant. The considered scenario assumes that faults are persistent, the DES model is monolithic and is endowed with a single initial state, the observations are temporally uncertain, and the diagnostic processing is exact.

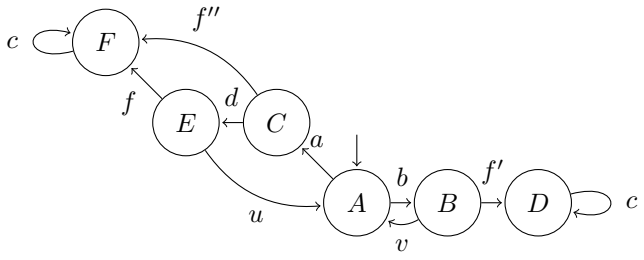

Figure 1: DES behavioral model

2 Background

2.1 Diagnosis of Discrete-Event Systems

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. 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. The length of the sequence of events in $obs(\tau)$ is denoted $|obs(\tau)|$. The prefix-closed observable language relevant to L, denoted as $obs(L)$, is assumed to be live. 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 at 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 three faulty events (f, f', and f''), two further unobservable events (u and v), and four observable ones (a–d). A possible path is $A \xrightarrow{b} B \xrightarrow{v} A \xrightarrow{a} C \xrightarrow{d} E \xrightarrow{f} F \xrightarrow{c} F$, corresponding to the trace $b.v.a.d.f.c$, 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 along 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 $O = b.a.d.c$ is $\{(F, \{f\})\}$. Such a diagnosis consists of just one candidate, meaning that, once observation O has been perceived, the state of D is certainly F and fault f has necessarily occurred.

2.2 Temporally Uncertain Observations

In observation $O = b.a.d.c$ used in the previous section 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 b to d, are not displayed. We say that the observation is *certain*. However, the temporal order of the observable events that have occurred within the DES is not always known [14], 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 a and d is unknown. Since we do not know which sequence, i.e. either $b.a.d.c$ or $b.d.a.c$, actually occurred, an exact diagnostic algorithm has to take into account both of them. The pair of observable events a and d can altogether be considered as a *temporally compound event* $a//d$, which cumulatively represents both sequences $a.d$ and $d.a$. We can describe the temporally uncertain observation as a sequence $O' = b.a//d.c$.

Definition 1 (Temporally compound observable event [13])**.** *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.*

The collection of multisets of Σ_o of cardinality ℓ and of cardinality ℓ or less are denoted as $\left(\!\binom{\Sigma_o}{\ell}\!\right)$ and $\left(\!\binom{\Sigma_o}{\leq \ell}\!\right)$, respectively. Notice that $\left(\!\binom{\Sigma_o}{\leq \ell}\!\right) = \bigcup_{i \leq \ell} \left(\!\binom{\Sigma_o}{i}\!\right)$.

Definition 2 (Temporal uncertainty level [13])**.** *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 a and d are reciprocally temporally unrelated.

Definition 3 (Extension of a certain observation [13])**.** *Given a value ℓ of the temporal uncertainty level, and a certain observation O, the* extension $||O||^{//\ell}$ *of the observation is the set of certain and temporally uncertain observations that O could produce up to the given level, where $O \in ||O||^{//\ell}$.*

In our example, given the trace τ whose certain observation is $obs(\tau) = b.a.d.c$, the extension of such an observation to the second temporal uncertainty level is $||obs(\tau)||^{//2} =$

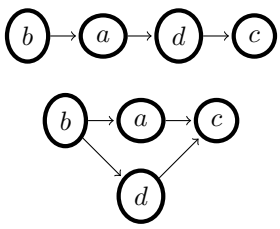

Figure 2: Certain (top) and temporally uncertain (bottom) observations

$\{b.a.d.c, b.a.c//d, b.a//d.c, a//b.d.c, a//b.c//d\}$. In other words, $||obs(\tau)||^{//2}$ includes all the ways the sequence $obs(\tau)$ of observable events generated by the DES can be perceived if the occurrence order of whichever pair of consecutive observable events may be unknown.

2.3 Diagnosability under Uncertainty

Following [2], if, for whichever path that has preceded the occurrence of the fault, and for whichever sequence of transitions (generating k observable events or more) 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. 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 4 (Diagnosability [2]). *Given a DES $D = (\Sigma, L, obs, flt)$ whose set of faults is $\Sigma_f \subseteq \Sigma$, a fault $f \in \Sigma_f$ is* diagnosable *if*

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

$$(\forall \tau \in L), (obs(\tau) = obs(\tau_1.\tau_2) \Rightarrow (\tau \in L_f)).$$

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 faults f, f', and f'' is precisely detected once event c has been perceived after having perceived either d or b or a, respectively.

The above definition of diagnosability implicitly assumes that, if a DES follows a trace τ, the observation O processed by the diagnostic engine is certain, that is, it equals *obs(τ)*. Such a limitation is overcome by the following definition of diagnosability [13] relevant to a DES with an observation affected by a temporal uncertainty up to level ℓ, denoted $\|^{//\ell}$. According to this generalized definition, that subsumes the former, a faulty behavior, in order to be diagnosable, should always eventually produce an observation that cannot be mistaken for an observation produced by a nominal behavior.

Definition 5 ($\|^{//\ell}$-Diagnosability [13]). *Given a DES $D = (\Sigma, L, obs, flt)$ with a set of faults $\Sigma_f \subseteq \Sigma$ and temporal uncertainty $\|^{//\ell}$, a fault $f \in \Sigma_f$ is* $\|^{//\ell}$-diagnosable *if*

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

$$(\forall \tau \in L), \left(||obs(\tau_1.\tau_2)||^{//\ell} \cap ||obs(\tau)||^{//\ell} \neq \emptyset \Rightarrow (\tau \in L_f) \right).$$

System D is $\|^{//\ell}$-diagnosable *if every fault $f \in \Sigma_f$ is $\|^{//\ell}$-diagnosable.*

System D in Figure 1 is $||^{//2}$-diagnosable. Indeed, fault f is identified by observing d and c; changing the order of two consecutive observed events does not eliminate the fact that d will be observed. Analogously, fault f' is identified if events b and c are observed, whichever their order. Finally, fault f'' is identified if a and c are observed, independently of their order. However, the system is not $||^{//3}$-diagnosable since observation $a//b//d.c^*$ is relevant to a pair of distinct faulty traces, one including fault f and the other fault f'.

Notice how the generalized definition of diagnosability is well-behaved w.r.t. increasing uncertainty. If uncertainty $||''$ is more permissive than $||'$, i.e. $||O||'' \supseteq ||O||'$ for any certain observation O, then $||''$-diagnosability implies $||'$-diagnosability. Since temporal uncertainty is increasingly more permissive for increasing values of the uncertainty level, we can conclude that the sample DES D in Figure 1 is not $||^{//\ell}$-diagnosable for any $\ell > 2$.

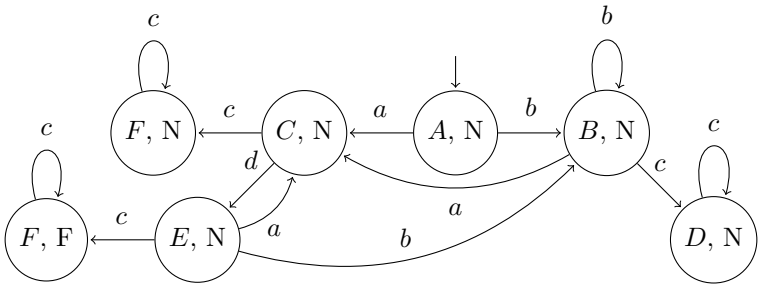

Figure 3: (State-based) verifier of level 1 for fault f of the DES in Figure 1

2.4 Twin Plant Method

The most popular approach to DES diagnosability analysis is the so-called *twin plant* method [3], which was originally conceived for permanent faults and certain observations, assuming an exact diagnostic processing.

Given a (nondeterministic) FA $G = (X, \Sigma, \delta, x_0)$, representing the behavioral model of a DES, where $\Sigma_f \subseteq \Sigma$ is the set of faulty events and $\Sigma_o \subseteq \Sigma$ is the set of observable events, the twin plant method draws from G a completely observable (nondeterministic) FA G_o, whose set of events is Σ_o. Each state of G_o is a pair (x, ϕ), where x is either the initial state x_0 of G or a state in G that is the target of an observable transition, and ϕ is a set of faults. If $x = x_0$, then $\phi = \emptyset$, that is, it is assumed that G is initially free of faults, the same as in the diagnoser approach [2]. Each transition from a pair (x, ϕ) to a pair (x_1, ϕ_1) in G_o represents a path in G from state x to state x_1, where the only observable transition in such a path is the last one. Set ϕ_1 is the set-theoretic union of ϕ with all the faults corresponding to the transitions on the path from x to x_1 in G. Thus the constraint holds that $\phi_1 \supseteq \phi$.

Intuitively G_o is a (nondeterministic) FA generating the observable language of G, hence each state (x, ϕ) in G_o includes the set ϕ of all the faults that manifest themselves along a path (at least) in G that produces the same sequence of observable events as a path in G_o from the initial state $(x_0, \emptyset)$ to state (x, ϕ).

Once G_o is available, the product [1] of G_o by itself ($G_o \otimes G_o$) is computed, and denoted G_d. Thus each state in G_d is a pair of pairs, $((x_1, \phi_1); (x_2, \phi_2))$.

Finally, an algorithm checks whether in G_d there exists a cycle that includes an *ambiguous* state $((x_1, \phi_1); (x_2, \phi_2))$, that is, a state such that ϕ_1 does not equal ϕ_2: if this condition holds, G is not diagnosable.

As already remarked, given a transition $(x, \phi) \rightarrow (x_1, \phi_1)$ in G_o, the constraint holds that $\phi_1 \supseteq \phi$. Hence, in G_o the set of failure types is the same for all the states belonging to the same cycle. Consequently, in G_d, if a cycle includes a state $((x_1, \phi_1); (x_2, \phi_2))$, all the other states in the same cycle are $((-, \phi_1); (-, \phi_2))$, that is, they include the same sets of faults. Thus, if in a state in a cycle in G_d such sets are different from each other, the system is not diagnosable since it may indefinitely produce the observable events relevant to the cycle, in which case we cannot decide within a finite delay which faults have occurred.

The complexity of the whole method is $O(|X|^4 2^{4|\Sigma_f|}|\Sigma_o|)$, which is exponential in the number of faults. However, it can be reduced to $O(|X|^4|\Sigma_o||\Sigma_f|)$, which is polynomial in the number of faults, by noticing that a system is diagnosable with respect to all the faults if and only if it is diagnosable with respect to each individual fault. In other words, one can apply the

algorithm iteratively (a number of times that equals the number of distinct failures), for testing the diagnosability with respect to each singleton set of faults. In case an individual fault $f \in \Sigma_f$ is considered (and every transition in G that is affected by any other type of fault is simply reckoned as an unobservable transition), the set of faults within each pair (x, ϕ) of G_o is either $\phi = \{f\}$, which can conveniently be denoted as F, or $\phi = \emptyset$, which is denoted as N. Automaton G_o can be referred to as the *verifier* of fault f. A state of the twin plant G_d is *ambiguous* if it matches the pattern $((x, N); (x', F))$ or $((x, F); (x', N))$. As already remarked, if a state in a loop is ambiguous, then all the states in the same loop are ambiguous. A loop of ambiguous states betrays the existence of a *critical pair*, this being a pair of evolutions of the DES, one normal and the other faulty, that are indefinitely observationally identical.

Figure 3 represents the verifier relevant to fault f of the DES whose behavioral model is shown in Figure 1.

In [13], the twin plant method was adapted to DESs with temporally uncertain observations. The $||^{//\ell}$-verifier relevant to fault f is nothing but the classical twin plant verifier where the alphabet of observable events, instead of being Σ_o, is $\Sigma_o^{//\ell} = \left(\!\!\left(\begin{matrix}\Sigma_o \\ \leq \ell\end{matrix}\right)\!\!\right)$, i.e. the alphabet of all temporally compound observable events up to a given level ℓ. Hence $\Sigma_o^{//1} = \Sigma_o$ and the $||^{//1}$-verifier is G_o.

Once the $||^{//1}$-verifier has been built, it has to be synchronized with itself, which results in the twin plant of level 1. $||^{//1}$-diagnosability of fault f holds if no loop in such a twin plant includes ambiguous states. If $||^{//1}$-diagnosability of fault f holds, as it is the case in the running example, we can assess the successive level of diagnosability. This requires building the verifier of level 2 relevant to fault f, then synchronizing it with itself, controlling whether the diagnosability condition holds, and so on.

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 marking these transitions, where + is a separator. So, for instance, label $c + b//c$ from state (B, N) to state (D, N) means that, when the DES is in state B and fault f has never occurred and either c or $b//c$ is perceived, then the DES has reached state D and fault f has not occurred. In fact, in the behavioral model in Figure 1, if c is perceived starting at state B, this means that path $B \xrightarrow{f'} D \xrightarrow{c} D$ has been followed. If, instead, $b//c$ is perceived starting at state B, this means that path $B \xrightarrow{v} A \xrightarrow{b} B \xrightarrow{f'} D \xrightarrow{c} D$ has been followed.

3 Twin Plant Method Revisited

The previous sections have briefly surveyed the original twin plant method and its generalization in order to deal with temporally uncertain observation of any level. Since a temporally uncertain observation of level 1 is actually a certain observation, and the $||^{//1}$-verifier is indeed a verifier for certain observation (that is, the traditional G_o), the generalized twin plant method for temporally uncertain observations subsumes the original one, and any remark relevant to the former applies also to the latter.

3.1 State-based Representation

The first remark is about the size of the twin plant. The original construction of the twin plant is such that (i) each path represents a pair of evolutions of the considered DES (and, consequently, of the relevant candidate diagnoses) that can produce the same (possibly uncertain)

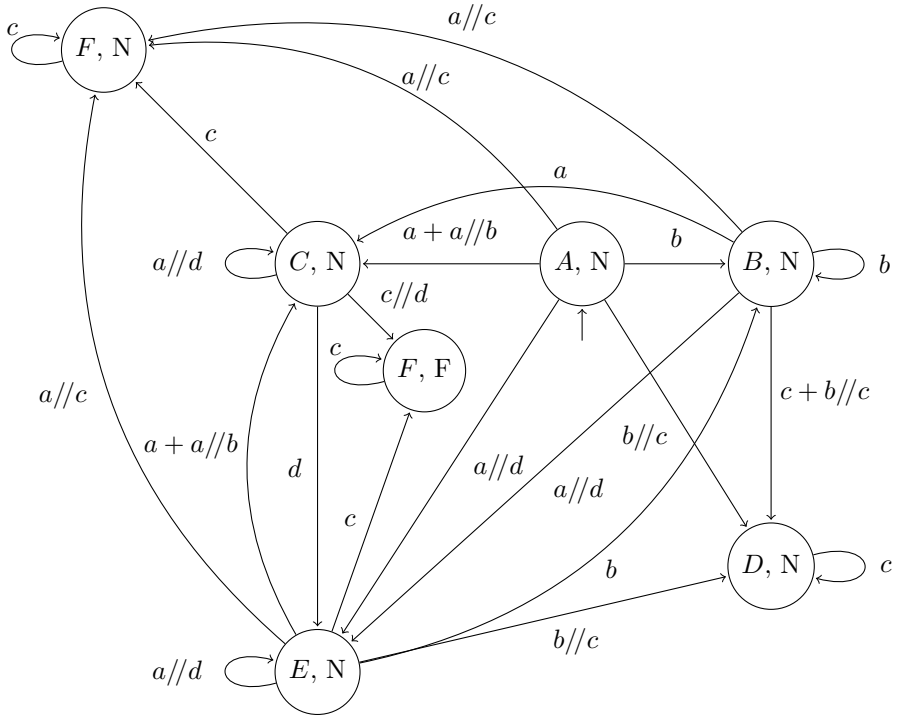

Figure 4: (State-based) $||^{//2}$-verifier for fault f of the DES in Figure 1

observation, and (*ii*) every pair of distinct evolutions that can produce the same (possibly uncertain) observation is represented by a path in the twin plant. Point (*i*) can be understood by observing that (*a*) the initial state of the twin plant is a pair of candidate diagnoses according to which the DES is in its initial state and it is free of faults, and (*b*) each transition in the twin plant brings to a new pair of candidate diagnoses, relevant to a pair of evolutions that are driven by the same perception of a new (compound) observable event. Such an evolution is compliant with the $||^{//\ell}$-verifier, which in turn is compliant with the behavioral model of the DES.

The twin plant representation is not only complete but also redundant, as the same pair of distinct evolutions t_1 and t_2 of the $||^{//\ell}$-verifier (that is, of G_o in the original twin plant method) is compared in the twin plant both as a sequence of pair of states where the former belongs to t_1 and the latter to t_2 and, vice versa, as a sequence of pair of states where the former belongs to t_2 and the latter to t_1. We can say that the twin plant method is *symmetric*.

A reduction of the number of pairs to be compared can be achieved by replacing the product of two identical verifiers of level ℓ with the product of such a verifier (called *bad twin* as it allows also for abnormal behaviors) with a *good twin*, this being the verifier deprived of any abnormal behavior.

Definition 6 (Bad twin of level ℓ)**.** *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 an FA generating L. The* bad twin of level ℓ *relevant to a fault $f \in \Sigma_f$ is the* $||^{//\ell}$-verifier *relevant to*

the same fault. In [13] such a verifier is defined as an FA $B^{//\ell} = (X^{//\ell}, \Sigma^{//\ell}, \delta^{//\ell}, x_0^{//\ell})$*, where:*

- $X^{//\ell} = X \times \{N, F\}$ *and* $x_0^{//\ell} = (x_0, N)$*;*
- $\Sigma^{//\ell} = \Sigma_o^{//\ell}$*; and*
- $\delta^{//\ell} = \{((x,\phi), w, (x',\phi')) \in X^{//\ell} \times \Sigma^{//\ell} \times X^{//\ell} \mid \exists$ *a path in* $G : x \xrightarrow{\sigma_1} \ldots \xrightarrow{\sigma_n} x'$, $n \geq 1, \sigma_n \in \Sigma_o, w \in ||obs(\sigma_1.\cdots.\sigma_n)||^{//\ell}, (\phi' = N \Leftrightarrow \phi = N \wedge f \notin \{\sigma_1, \ldots, \sigma_n\})\}$.

The *good twin* $G^{//\ell}$ of level ℓ is obtained by removing from $B^{//\ell}$ all the faulty states, along with their entering and exiting transitions.

Definition 7 (Good twin of level ℓ)**.** *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 an FA generating* L*. The* good twin of level ℓ *relevant to a fault* $f \in \Sigma_f$ *is an FA* $G^{//\ell} = (\bar{X}^{//\ell}, \Sigma^{//\ell}, \bar{\delta}^{//\ell}, x_0^{//\ell})$ *defined as follows:*

- $\bar{X}^{//\ell} = X \times \{N\}$ *and* $x_0^{//\ell} = (x_0, N)$*;*
- $\Sigma^{//\ell} = \Sigma_o^{//\ell}$*; and*
- $\bar{\delta}^{//\ell} = \{((x,\phi), w, (x',\phi')) \in \bar{X}^{//\ell} \times \Sigma^{//\ell} \times \bar{X}^{//\ell} \mid \exists$ *a path in* $G : x \xrightarrow{\sigma_1} \ldots \xrightarrow{\sigma_n} x'$, $n \geq 1, \sigma_n \in \Sigma_o, w \in ||obs(\sigma_1.\cdots.\sigma_n)||^{//\ell}, f \notin \{\sigma_1, \ldots, \sigma_n\}\}$.

Notice that the set of states and the set of transitions of the good twin of level ℓ are subsets of those of the bad twin of the same level, that is, $\bar{X}^{//\ell} \subseteq X^{//\ell}$ and $\bar{\delta}^{//\ell} \subseteq \delta^{//\ell}$.

The product of the bad twin by the good twin will generate an FA with a reduced number of paths with respect to the product of the bad twin by itself. In particular, each pair of observationally identical evolutions, the former including some faulty states, the latter no faulty state, will be represented by just one path in $B^{//\ell} \otimes G^{//\ell}$, while it is represented by two in $B^{//\ell} \otimes B^{//\ell}$. We can summarize this difference by saying that the product of the bad twin by the good twin is an *asymmetric twin plant*. In the following we will consider just asymmetric twin plants. Notice that the (necessary and sufficient) condition for $\|^{//\ell}$-diagnosability relevant to the asymmetric twin plant is the same as for the symmetric twin plant. In fact, a fault is diagnosable if there are no critical pairs in the symmetric twin plant. Each critical pair is replicated in the symmetric twin plant while there is just one instance of it in the asymmetric twin plant. However, in both cases the property of $\|^{//\ell}$-diagnosability holds iff there are no (infinite) critical pairs.

Another remark is worthwhile here. In the diagnosability check, we have to take into account only infinite paths of the twin plant, while the paths relevant to the product of two FAs can also be finite. Let us denote as *Live()* an operator that, as applied to an FA, removes from it all the parts that generate a language that is not live.

Theorem 1. *Let* $BG^{//\ell} = B^{//\ell} \otimes G^{//\ell}$ *be the asymmetric twin plant of level* ℓ *relevant to a fault* f*, and* $Live(BG^{//\ell})$ *be its live part. Fault* f *is* $\|^{//\ell}$*-diagnosable iff* $Live(BG^{//\ell})$ *does not include any ambiguous state.*

Proof outline: $Live(BG^{//\ell})$ represents all the observationally identical infinite evolutions of the considered DES, since, by construction, all of them are represented by the asymmetric twin plant $BG^{//\ell}$. The liveliness of $Live(BG^{//\ell})$ guarantees that each state in it either belongs to a loop or is followed (within a finite number of transitions) by a loop.

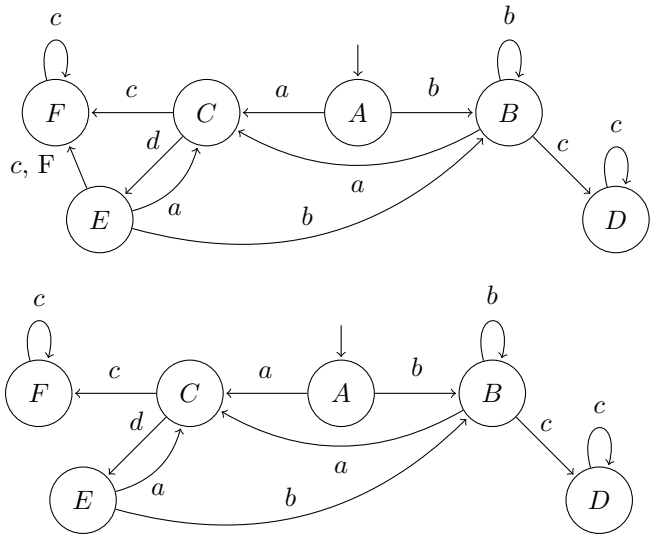

Figure 5: TB bad twin (top) and TB good twin (bottom) of level 1 for fault f of the DES in Figure 1

($\rightarrow$) The assumption that f is $\|^{//\ell}$-diagnosable implies (according to the necessary and sufficient condition for $\|^{//\ell}$-diagnosability) that there are no cycles of ambiguous states in the symmetric twin plant $BB^{//\ell} = B^{//\ell} \otimes B^{//\ell}$. This in turn implies that there are no ambiguous states within any cycle in $B^{//\ell} \otimes G^{//\ell}$, and, hence, within any cycle in $Live(BG^{//\ell})$. Moreover, this implies that $Live(BG^{//\ell})$ does not include any ambiguous state outsides its cycles. In fact, assume, by contradiction, that $Live(B^{//\ell} \otimes G^{//\ell})$ includes an ambiguous state that does not belong to a loop, then such a state is necessarily followed by an ambiguous loop, which contradicts the hypothesis.

($\leftarrow$) If $Live(BG^{//\ell})$ does not include any ambiguous state, then it does not include any cycle of ambiguous states, which implies that the asymmetric twin plant $BG^{//\ell}$ does not include any cycle of ambiguous states, which in turn implies that the symmetric twin $BB^{//\ell} = B^{//\ell} \otimes B^{//\ell}$ does not include any cycle of ambiguous states, hence the fault is $\|^{//\ell}$-diagnosable since the condition for $\|^{//\ell}$-diagnosability of the symmetric twin plant holds. □

The purport of this theorem is that the (necessary and sufficient) condition for diagnosability to be checked in a live asymmetric twin plant is weaker than the condition to be checked in an asymmetric twin plant whose observational language is not live. However, the saving involved in assessing a weaker condition may be paid beforehand in handling the asymmetric twin plant so as to remove from it all the parts that generate a language of the observations that is not live. In case an algorithmic implementation is adopted, if the algorithm that generates the asymmetric twin plant (which is indeed an algorithm for computing the strict product of two FAs) can instead be replaced with an algorithm that generates a live FA without any additional temporal burden, or such that the total time needed to build the live asymmetric twin plant and to check the diagnosability is less than the total time needed when the asymmetric twin plant is not live, this option could be interesting.

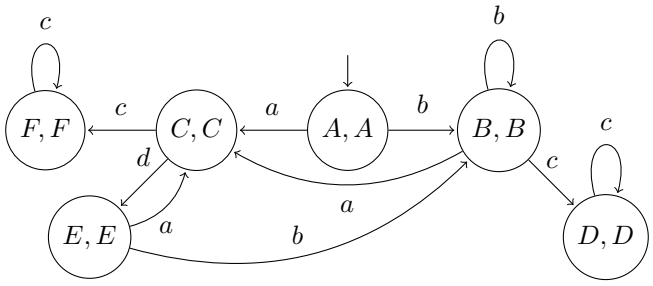

Figure 6: TB asymmetric twin plant of level 1 resulting from the synchronization of the twins in Figure 5

3.2 Transition-Based Representation

While the previous section has introduced the notions of bad twin, good twin, and asymmetric twin plant by adopting a state-based representation (as in the original method), in this section the corresponding transition-based (TB) concepts are presented.

Definition 8 (TB Bad twin of level ℓ)**.** *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 an FA generating L. The* TB bad twin of level ℓ *relevant to a fault $f \in \Sigma_f$ is an FA $B_\ell = (X^{B_\ell}, \Sigma^{B_\ell}, \delta^{B_\ell}, x_0^{B_\ell})$ defined as follows:*

- $X^{B_\ell} = X$ *and* $x_0^{B_\ell} = x_0$ *and* $\Sigma^{B_\ell} = \Sigma_o^{//\ell}$*; and*
- $\delta^{B_\ell} = \{(x, w, \phi, x') \in X^{B_\ell} \times \Sigma^{B_\ell} \times \{N, F\} \times X^{B_\ell} \mid \exists$ *a path in* $G : x \xrightarrow{\sigma_1} \ldots \xrightarrow{\sigma_n} x'$, $n \geq 1, \sigma_n \in \Sigma_o, w \in ||obs(\sigma_1.\cdots.\sigma_n)||^{//\ell}, (\phi = N \Leftrightarrow f \notin \{\sigma_1, \ldots, \sigma_n\})\}$.

Notice that the number of states of the TB bad twin is lower than that of the state-based bad twin (and hence also of the verifier of the original method), it can possibly be reduced to a half. In our running example, the TB bad twin of level 1 (top of Figure 5) includes 6 states while the state-based bad twin (Figure 3) includes 7 states.

According to the next definition, the TB good twin of level ℓ is obtained by removing from the TB bad twin of level ℓ all the faulty transitions (and all the states that become unreachable).

Definition 9 (TB Good twin of level ℓ)**.** *Let $B_\ell = (X^{B_\ell}, \Sigma^{B_\ell}, \delta^{B_\ell}, x_0^{B_\ell})$ be the TB bad twin of level ℓ relevant to a fault $f \in \Sigma_f$. The TB good twin G_ℓ of level ℓ relevant to the same fault is the accessible part of an FA $(X^{G_\ell}, \Sigma^{G_\ell}, \delta^{G_\ell}, x_0^{G_\ell})$ defined as follows:*

- $X^{G_\ell} \subseteq X^{B_\ell}$ *and* $x_0^{G_\ell} = x_0^{B_\ell}$ *and* $\Sigma^{G_\ell} = \Sigma^{B_\ell}$*; and*
- $\delta^{G_\ell} = \delta^{B_\ell} \setminus \{(x, w, \phi, x') \in \delta^{B_\ell} \mid \phi = F\}$.

The TB good twin of level 1 relevant to fault f of the DES in Figure 1 is shown on the bottom of Figure 5.

Definition 10 (TB Asymmetric twin plant of level ℓ)**.** *Let B_ℓ and G_ℓ be the TB bad and good twin of level ℓ, respectively, relevant to a fault $f \in \Sigma_f$. The* TB asymmetric twin plant of level ℓ *relevant to the same fault, denoted BG_ℓ, is given by the product $B_\ell \otimes G_\ell$ on the set of temporally*

compound observable events $\Sigma_o^{//\ell}$*, where the value of parameter* ϕ *of each transition ranges over the set* $\{N, A\}$*, value* N *being assigned to a transition resulting from the synchronization of two normal transitions, value* A *being assigned to a transition resulting from the synchronization of a faulty transition (of* B_ℓ*) with a normal transition (of* G_ℓ*).*

In the asymmetric TB twin plant, a transition whose value of parameter ϕ is A is *ambiguous*. Figure 6 displays the TB asymmetric twin plant of level 1 relevant to fault f of the sample DES. The value of parameter ϕ (which is omitted from the figure) is N for all its transitions.

Theorem 2. *A fault* f *is* $||^{//\ell}$*-diagnosable iff the relevant TB asymmetric twin plant of level* ℓ *contains no ambiguous transition that either precedes a cycle or belongs to a cycle.*

Proof outline: ($\rightarrow$) If fault f is $||^{//\ell}$-diagnosable, then the state-based (a)symmetric twin plant of level ℓ does not include any ambiguous cycle. This implies that in the TB asymmetric twin plant neither there is any cycle that includes an ambiguous transition nor any cycle that is preceded by an ambiguous transition (as such a cycle would correspond to a cycle of ambiguous states in the state-based representation).

($\leftarrow$, by contradiction) Every path t relevant to the TB asymmetric twin plant of level ℓ has a corresponding path t' relevant to the state-based asymmetric twin plant of the same level. We consider separately the case when a path t contains an ambiguous transition that precedes a cycle and the case when t contains an ambiguous transition that belongs to a cycle.

If path t contains an ambiguous transition that precedes a cycle, in t' the target of such a transition is an ambiguous state and all its following states in t' are ambiguous too as in t there is no transition that results from the synchronization of two faulty transitions. Hence, all the states in the cycle in t' are ambiguous.

If path t contains an ambiguous transition that belongs to a cycle, then in t' the target of such a transition is an ambiguous state and all its following states in t' are ambiguous too. Since there is a cycle in t, there is a corresponding cycle also in t' whose states are all ambiguous (since they belong to the same cycle as the ambiguous state).

In both the above cases the condition for $||^{//\ell}$-diagnosability relevant to the state-based (a)symmetric twin plant does not hold, hence fault f is not $||^{//\ell}$-diagnosable, which contradicts the hypothesis. □

Theorem 2 expresses a necessary and sufficient condition for $||^{//\ell}$-diagnosability, which, unfortunately, is heavier to check than the necessary and sufficient condition relevant to the state-based twin plant. The following ones are instead three sufficient conditions for $||^{//\ell}$-diagnosability.

Condition 1. *The TB asymmetric twin plant of level* ℓ *does not include any ambiguous transition.*

Condition 1 trivially comes from Theorem 2. It holds for the TB asymmetric twin plant of level 1 in Figure 6.

Condition 2. *The TB bad twin of level* ℓ *is observationally deterministic, that is, all the transitions exiting from the same state are marked with a distinct (compound) observable event.*

(Notice that, if the TB bad twin of level ℓ includes a pair of transitions exiting from the same source and marked with the same compound observable event, one with ϕ = N and the other with ϕ = F, then such a bad twin is not observationally deterministic). Condition 2 can be understood by considering that, it the TB bad twin of level ℓ is observationally deterministic, then also the TB good twin of level ℓ is deterministic. The resulting TB asymmetric twin

plant of level ℓ is such that each state is a pair of identical states and each transition is the composition of two transitions that are not only observationally identical but also identical as far as parameter ϕ is concerned. Therefore, no transition is the result of the synchronization of an F transition with an N transition, hence there is no ambiguous transition in the asymmetric twin plant of level ℓ, that is, sufficient Condition 1 holds. Condition 2 holds for the TB bad twin of level 1 in Figure 5 (and, in fact, the TB asymmetric twin plant in Figure 6 does not include any ambiguous transition).

Condition 3. $\nexists((x, w, \phi, x') \in \delta^{B_\ell}, (x_1, w, \phi_1, x'_1) \in \delta^{B_\ell})$ *s.t.* $(\phi = N \wedge \phi_1 = F)$.

Condition 3 requires normal and faulty transitions of the TB bad twin of level ℓ not to share any (compound) observable event. The rationale is that, if this condition holds, no ambiguous transition can be created in the TB twin plant of level ℓ as no faulty transition of the TB bad twin of level ℓ can be synchronized with a normal transition of the TB bad twin of level ℓ. Hence, the fulfillment of this condition implies that sufficient Condition 1 holds. Condition 3 does not hold for the bad twin on the top of Figure 5, as observable event c is shared.

The following properties are quite interesting for the construction of the TB bad twin.

Property 1. *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 an FA generating L. Let $B_\ell = (X^{B_\ell}, \Sigma^{B_\ell}, \delta^{B_\ell}, x_0^{B_\ell})$ be the TB bad twin of level ℓ relevant to a fault $f \in \Sigma_f$. For the TB bad twin of level $\ell+1$, $B_{\ell+1} = (X^{B_{\ell+1}}, \Sigma^{B_{\ell+1}}, \delta^{B_{\ell+1}}, x_0^{B_{\ell+1}})$, relevant to the same fault, the following equalities hold:*

1. $X^{B_{\ell+1}} = X^{B_\ell}$ *and* $x_0^{B_{\ell+1}} = x_0^{B_\ell}$;
2. $\Sigma^{B_{\ell+1}} = \Sigma^{B_\ell} \cup \left(\!\!\binom{\Sigma_o}{\ell+1}\!\!\right)$; *and*
3. $\delta^{B_{\ell+1}} = \delta^{B_\ell} \cup \{(x, w, \phi, x') \in X^{B_\ell} \times \left(\!\!\binom{\Sigma_o}{\ell+1}\!\!\right) \times \{N, F\} \times X^{B_\ell} \mid \exists$ *a path in* $G : x \xrightarrow{\sigma_1} \ldots \xrightarrow{\sigma_n} x',\ n \geq 1, \sigma_n \in \Sigma_o, w \in ||obs(\sigma_1.\cdots.\sigma_n)||^{//\ell+1}, (\phi = N \Leftrightarrow f \notin \{\sigma_1, \ldots, \sigma_n\})\}$.

Proof outline: Equality 1 trivially comes from Definition 8. As to equality 2, based on Definition 8, $\Sigma^{B_\ell} = \left(\!\!\binom{\Sigma_o}{\leq \ell}\!\!\right)$ and $\Sigma^{B_{\ell+1}} = \left(\!\!\binom{\Sigma_o}{\leq (\ell+1)}\!\!\right)$. Since $\left(\!\!\binom{\Sigma_o}{\leq (\ell+1)}\!\!\right) = \left(\!\!\binom{\Sigma_o}{\leq \ell}\!\!\right) \cup \left(\!\!\binom{\Sigma_o}{\ell+1}\!\!\right)$, the equality is proven. Equality 3 is drawn from the definition of the transition function in Definition 8. Since $||obs(\sigma_1.\cdots.\sigma_n)||^{//\ell+1} \supseteq ||obs(\sigma_1.\cdots.\sigma_n)||^{//\ell}$, then $\delta^{B_{\ell+1}} \supseteq \delta^{B_\ell}$. All the transitions to be added to δ^{B_ℓ} in order to obtain $\delta^{B_{\ell+1}}$ are necessarily relevant to compound events of level $\ell+1$, which proves the equality. □

Lemma 1. $\delta^{B_{\ell+1}} = \delta^{B_\ell} \cup \{(x, w, \phi, x') \in X^{B_\ell} \times \left(\!\!\binom{\Sigma_o}{\ell+1}\!\!\right) \times \{N, F\} \times X^{B_\ell} \mid \exists$ *a path in* $B_\ell : x \xrightarrow{w_1, \phi_1} x_1 \xrightarrow{w_2, \phi_2} x', \left(w_1 \in \left(\!\!\binom{\Sigma_o}{m}\!\!\right), w_2 \in \left(\!\!\binom{\Sigma_o}{\ell+1-m}\!\!\right)\right), m \in [1 \ldots \ell], w = w_1 // w_2,$ $(\phi = N \Leftrightarrow (\phi_1 = N \wedge \phi_2 = N))\}$.

Proof outline: This lemma just asserts that each transition marked with a temporally compound observable event of level $\ell+1$ to be added to δ^{B_ℓ} in order to obtain $\delta^{B_{\ell+1}}$ can be obtained by considering a sequence of two transitions in B_ℓ, one marked with a temporally compound

observable event $w_1 \in \left(\!\!\binom{\Sigma_o}{m}\!\!\right)$ and the other with a temporally compound observable event $w_2 \in \left(\!\!\binom{\Sigma_o}{\ell+1-m}\!\!\right)$. In fact, the composition of w_1 and w_2 yields a temporally compound event of level $\ell+1$. □

According to Property 1, given the TB bad twin B_ℓ of level ℓ relevant to a fault, the TB bad twin of level $\ell+1$ relevant to the same fault can be obtained by adding to B_ℓ all (and only) the transitions relevant to the temporally compound observable events of level $\ell+1$. The above lemma underlines that, starting at each state of B_ℓ, each transitions to be added in order to build $B_{\ell+1}$ can be obtained by considering a sequence of two transitions in B_ℓ. This opens the way to an incremental construction of the TB bad twin and consequently of the TB asymmetric twin plant, as asserted by the next lemmas.

Lemma 2. *Let $G_{\ell+1}$ be the TB good twin of level $\ell+1$ relevant to a fault. The TB asymmetric twin plant of level $\ell+1$ relevant to the same fault can be obtained by adding to the TB asymmetric twin plant of level ℓ, $BG_\ell = B_\ell \otimes G_\ell$, all (and only) the following transitions:* $\{((x_B, x_G), w, \phi, (x'_B, x'_G)) \in (X^{B_\ell} \times X^{G_\ell}) \times \left(\!\!\binom{\Sigma_o}{\ell+1}\!\!\right) \times \{N, A\} \times (X^{B_\ell} \times X^{G_\ell}) \mid \exists$ *a transition in* $B_{\ell+1} : x_B \xrightarrow{w,\phi_B} x'_B, \exists$ *a transition in* $G_{\ell+1} : x_G \xrightarrow{w,\phi_G} x'_G, w \in \left(\!\!\binom{\Sigma_o}{\ell+1}\!\!\right), (\phi = N \Leftrightarrow \phi_B = N)\}$.

Proof outline: According to Property 1, the TB bad twin of level $\ell+1$ can be obtained by adding to B_ℓ all (and only) the transitions relevant to the compound observable events of level $\ell+1$. Analogously, the TB good twin of level $\ell+1$ can be obtained by adding to G_ℓ all (and only) the normal transitions relevant to the compound observable events of level $\ell+1$. By definition, the TB asymmetric twin plant of level $\ell+1$ is given by the product $B_{\ell+1} \otimes G_{\ell+1}$. The TB asymmetric twin plant of level ℓ includes all the synchronizations of the transitions of the twins relevant to compound observable events up to level ℓ, and the twins of level $\ell+1$ do no include any new transition relevant to compound observable events up to level ℓ w.r.t. the twins of level ℓ. Hence, the only new transitions in the TB asymmetric twin plant of level $\ell+1$ w.r.t. those included in the TB asymmetric twin plant of level ℓ are those obtained by synchronizing the transitions marked with compound observable events of level $\ell+1$ in the twins of level $\ell+1$. □

Lemma 2 states that, in order to build the TB asymmetric twin plant of level $\ell+1$, we have to add to the TB twin plant of level ℓ the transitions obtained by synchronizing the pair of transitions marked with compound events of level $\ell+1$ in the TB twins of level $\ell+1$. The next lemma gets us free from building such twins. In other words, the only TB asymmetric twin plant to be built as a product is that of level 1, while any other TB asymmetric twin plant of increasing level can be build by incrementally adding some transitions, where such transitions can be built by exploiting the information already included in the twin plant of level ℓ.

Lemma 3. *The TB asymmetric twin plant of level $\ell+1$ can be obtained by adding to the TB asymmetric twin plant BG_ℓ of level ℓ all (and only) the following transitions:* $\{((x_B, x_G), w, \phi, (x'_B, x'_G)) \in (X^{B_\ell} \times X^{G_\ell}) \times \left(\!\!\binom{\Sigma_o}{\ell+1}\!\!\right) \times \{N, A\} \times (X^{B_\ell} \times X^{G_\ell}) \mid \exists$ *a path in* $BG_\ell : (x_B, \cdot) \xrightarrow{w_1,\phi_1} (x^1_B, \cdot) \xrightarrow{w_2,\phi_2} (x'_B, \cdot), \left(w_1 \in \left(\!\!\binom{\Sigma_o}{m}\!\!\right), w_2 \in \left(\!\!\binom{\Sigma_o}{\ell+1-m}\!\!\right)\right), m \in [1 \dots \ell], w = w_1 // w_2, \exists$ *a path in* $BG_\ell : (\cdot, x_G) \xrightarrow{\bar{w_1},\bar{\phi_1}} (\cdot, x^1_G) \xrightarrow{\bar{w_2},\bar{\phi_2}} (\cdot, x'_G), \left(\bar{w_1} \in \left(\!\!\binom{\Sigma_o}{\mu}\!\!\right), \bar{w_2} \in \left(\!\!\binom{\Sigma_o}{\ell+1-\mu}\!\!\right)\right), \mu \in [1 \dots \ell],$

$w = \bar{w}_1 // \bar{w}_2, (\phi = N \Leftrightarrow (\phi_1 = N \wedge \phi_2 = N))\}$.

Proof outline: The TB asymmetric twin plant of level ℓ includes all the transitions marked with compound observable events with level from 1 to ℓ. This means that it includes all the information contained in the TB asymmetric twin plant of level 1, which in turn includes all the information contained in the verifier of level 1, from which we can draw all the TB asymmetric twin plants of higher levels. However, instead of resorting to the raw knowledge contained in the verifier of level 1, we can exploit the compiled knowledge in the TB asymmetric twin plant of level ℓ, that includes all the transitions marked with compound events up to level ℓ drawn from it. Hence, either transition in each pair of observationally identical transitions marked with events of level $\ell + 1$ belonging to the twins of level $\ell + 1$ to be synchronized is actually given by the sequence of two transitions in the TB asymmetric twin plant of level ℓ, where the sum of the levels of their compound observable events is $\ell + 1$. □

Further properties that can make the diagnosability check faster (in particular, the assessment of the sufficient conditions for diagnosability) hold, although they are not dealt with here. We also skip the equivalent of Theorem 1 for the TB representation of the twin plant; however, the reader can easily understand that a diagnosability condition weaker than that expressed by Theorem 2 is bound to exist when the TB asymmetric twin plant is live.

4 Conclusion

This paper deals with diagnosability analysis of DESs. Its goal is to provide a preliminary theoretical basis for an experimental activity. In fact, the paper shows that the size of the twin plant can be reduced by transforming it from a symmetric structure into an asymmetric one, both in its original state-based representation and in an equivalent transition-based representation. However, the necessary and sufficient condition for diagnosability relevant to the transition-based representation of the twin plant is heavier to check. The paper shows also that generating a twin plant that does not include any finite path leads to a weaker condition for diagnosability. However, the question is: does these findings pay? The answer can be given just by providing an implementation of the new version of twin plant method, and experimentally trying it.

In addition, the paper proposes to check the diagnosability of a DES for increasing levels of temporal uncertainty of the observations this way: first the (reduced) twin plant of level 1 (corresponding to no uncertainty) is built and diagnosability of level 1 is checked. If such a diagnosability holds, the twin plant of the next higher level is produced by updating the current twin plant, by exploiting only pieces of information that are already included in the current twin plant, and so on. Moreover, some sufficient conditions for diagnosability are listed. The efficiency of this incremental method, and the possible advantages brought by such sufficient conditions, should be tested via an extensive experimentation.

As to the reduction of the size of the twin plant, one could object that, in order to minimize the number of pairs to be compared in order to carry out the diagnosability analysis, we should synchronize an FA that represents the language of all (and only) the normal traces of the DES with another that represents the language of all (and only) the faulty traces. However, generating the latter FA requires performing a reachability analysis, which instead is not needed in the reduction envisaged in this paper. All the same, this is a topic for future research.

References

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

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] A. Grastien. Symbolic testing of diagnosability. In *Proceedings of the 20th International Workshop on Principles of Diagnosis*, 2009.

[7] J. Rintanen and A. Grastien. Diagnosability testing with satisfiability algorithms. In *Proceedings of the 20th International Joint Conference on Artificial Intelligence*, pages 532–537, 2007.

[8] 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.

[9] A. Boussif, B. Liu, and M. Ghazei. A twin plant based approach for diagnosablity analysis of intermittent failures. In *Proceedings of the 13th International Workshop on Discrete Event Systems*, 2016.

[10] A. Schumann and Y. Pencolé. Scalable diagnosability checking of event-driven systems. In *Proceedings of the 20th International Joint Conference on Artificial Intelligence – IJCAI-07*, pages 575–580, 2007.

[11] H. Ibrahim, P. Dague, and L. Simon. Using incremental SAT for testing diagnosability of distributed DES. In *Proceedings of the 26th International Workshop on Principles of Diagnosis*, pages 51–58, 2015.

[12] 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.

[13] X. Su, M. Zanella, and A. Grastien. Diagnosability of discrete-event systems with uncertain observations. In *Proceedings of the 25th International Joint Conference on Artificial Intelligence*, pages 1265–1271, 2016.

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