Hindawi
Complexity
Volume 2020, Article ID 4306261, 17 pages
https://doi.org/10.1155/2020/4306261

Research Article

Minimal Diagnosis and Diagnosability of Discrete-Event Systems Modeled by Automata

Xiangfu Zhao,[1] **Gianfranco Lamperti**,[2] **Dantong Ouyang**,[3] **and Xiangrong Tong**[1]

[1]*School of Computer and Control Engineering, Yantai University, Yantai 264005, China*
[2]*Department of Information Engineering, University of Brescia, Brescia 25123, Italy*
[3]*College of Computer Science and Technology, Jilin University, Changchun 130012, China*

Correspondence should be addressed to Xiangfu Zhao; xiangfuzhao@gmail.com and Xiangrong Tong; txr@ytu.edu.cn

Received 13 September 2019; Revised 13 December 2019; Accepted 7 January 2020; Published 18 February 2020

Guest Editor: Viet-Thanh Pham

In the last several decades, the model-based diagnosis of discrete-event systems (DESs) has increasingly become an active research topic in both control engineering and artificial intelligence. However, in contrast with the widely applied minimal diagnosis of static systems, in most approaches to the diagnosis of DESs, all possible candidate diagnoses are computed, including nonminimal candidates, which may cause intractable complexity when the number of nonminimal diagnoses is very large. According to the principle of parsimony and the principle of joint-probability distribution, generally, the minimal diagnosis of DESs is preferable to a nonminimal diagnosis. To generate more likely diagnoses, the notion of the minimal diagnosis of DESs is presented, which is supported by a minimal diagnoser for the generation of minimal diagnoses. Moreover, to either strongly or weakly decide whether a minimal set of faulty events has definitely occurred or not, two notions of minimal diagnosability are proposed. Necessary and sufficient conditions for determining the minimal diagnosability of DESs are proven. The relationships between the two types of minimal diagnosability and the classical diagnosability are analysed in depth.

1. Introduction

In recent years, several disasters, including the nuclear leakage that occurred in Fukushima (Japan) in 2011 and the blackout that occurred in nearly the entire country of India in 2012, have greatly threatened the safety of society and even the lives of many people. To prevent such disasters, determining faulty events/components is a very important topic. To this end, model-based fault diagnosis techniques may be very effective.

Nonlinear science is a new interdisciplinary subject which studies the common problems proposed by nonlinear interaction widely existing in various disciplines, especially in complex networks [1–4], system control [5–7], secure communication [8–10], chaotic systems [11], random number generators [12, 13], discrete-event systems (DESs) [14], and other fields. The creative work on the diagnosis/diagnosability of DESs, presented in [15, 16], with the originally proposed concept of a diagnoser, model-based diagnosis, and diagnosability have attracted more and more attention, as indicated by the large number of methods and techniques proposed in the literature, including [17–26]. Because of the intractable complexity of reasoning of the global DES model and the corresponding centralized diagnoser, decentralized approaches were proposed in [27–29]. More recently, fuzzy diagnoser/diagnosability [30, 31] or the stochastic diagnoser/diagnosability/prognosability [32–35] has been studied, with fuzzy or stochastic information being injected into an automaton that models a DES. In addition to diagnoser-based approaches for the diagnosis of DESs, a history-based approach [36, 37] and a consistency-based approach [38] to the diagnosis of DESs have also been presented.

However, as far as we know, one of the current main problems is that, in most approaches to diagnosing DESs, all possible candidate diagnoses are derived, even if many candidates are proper supersets of some other candidates. In other words, nonminimal (redundant) diagnoses are generated.

In this paper, we extend the idea of a minimal diagnosis, first presented in [39], via additional theoretical analyses, formal proofs, examples, and comparisons with related work.

Example 1. Among candidate diagnoses (sets of possible faulty events) $\{f_1\}$, $\{f_2, f_3\}$, $\{f_1, f_2, f_3\}$, $\{f_1, f_3, f_4\}$, and $\{f_2, f_3, f_4\}$, only $\{f_1\}$ and $\{f_2, f_3\}$ are minimal according to the set-inclusion relationship, as all other candidates contain $\{f_1\}$ or $\{f_2, f_3\}$ and include additional faults (f_2 and/or f_3 and/or f_4). Minimal diagnosis differs from minimal-cardinality diagnosis. In our example, the only minimal-cardinality diagnosis is $\{f_1\}$. In this paper, we focus on minimal diagnosis rather than minimal-cardinality diagnosis. In addition, in our example, even if we cannot definitely know whether f_4 has occurred or not, we know that minimal diagnoses $\{f_1\}$ and $\{f_2, f_3\}$ are generally more probable than others.

In theory, all possible fault sets need to be diagnosed. However, considering a scenario like Example 1, although there are a large number of possible candidate diagnoses that can explain the current observation sequence, there may exist set-inclusion relationships among some of them.

The two principles of parsimony and joint-probability distribution, which are briefly described as follows:

(i) The principle of parsimony: also called "Occam's razor" [40], parsimony is a principle of succinctness often adopted in logic and problem solving which states that, among competing hypotheses, the hypothesis with the fewest assumptions should be selected. The principle of parsimony has also been introduced for the minimal diagnosis of static systems [41].

(ii) The principle of joint-probability distribution: a widely used assumption in the literature, in this paper, a joint-probability distribution means that each fault is independent of one another and that the prior probability of each fault is equal.

Minimal diagnoses (based on the set-inclusion relationship (for instance, we assume that there are three candidate diagnoses $\{f_1\}$, $\{f_1, f_2\}$, and $\{f_2, f_3, f_4, f_5\}$. Then, $\{f_1\}$ and $\{f_2, f_3, f_4, f_5\}$ are minimal diagnoses, even if $\{f_2, f_3, f_4, f_5\}$ has a bigger cardinality than $\{f_1, f_2\}$ but without a set-inclusion relationship between them.)) are more likely than the corresponding nonminimal ones. As a result, just like the minimal diagnosis of static systems [41, 42], determining only the minimal diagnoses of DESs is bound to reduce the complexity, as additional nonminimal diagnoses are not considered.

The benefit of a minimal diagnosis is related to both cognition and computation. Cognition is relevant to the human who is responsible for the monitoring of the DES. Consider, for instance, the operator in the control room of a power network, who is responsible for the correct behaviour of the network. When a misbehaviour occurs, such as a short circuit on a transmission line, several actions can be triggered by the protection system to isolate the shorted line, e.g., opening breakers and reconfiguring the power load to avoid a blackout. If the reaction of the protection system is abnormal, a possibly large number of alarms and messages will be generated. Since the operator is expected to activate specific recovery actions, it is essential that the (possibly overwhelming) stream of information generated by the system, namely, the observation, be interpreted correctly under stringent time constraints. This is why automated diagnosis becomes a key factor in supporting the operator in performing his/her critical job. To this end, the diagnosis engine may generate diagnosis information in a relatively short amount of time. Specifically, a set of candidate diagnoses are presented to the operator, who is expected to make critical decisions regarding the safety of the involved population. However, if the number of candidates is large, the operator may be confused about which diagnoses should deserve more attention. Choosing minimal diagnoses is a good heuristic, as they are more probable and, as such, more worthy of attention.

Computation involves the efficient generation of candidate diagnoses. Since a key factor in real applications of automated diagnosis is the time response, that is, the delay between the occurrence of a faulty event and the generation of candidate diagnoses, it is of paramount importance that the diagnosis engine is not only effective but also efficient. Being free of the burden of nonminimal candidates, minimal diagnosis allows the diagnosis engine to be more efficient compared with nonminimal diagnosis with respect to both processing speed and memory space.

In summary, the main contribution of the paper is that the theoretical concepts of minimal diagnosis and minimal diagnosability of DESs are proposed, and meanwhile, the minimal diagnosis of DESs is not a purely academic exercise; it may drive attention to the actual cause of a misbehaviour effectively (cognition) and efficiently (computation).

The rest of the paper is organized as follows. The terminology and preliminary concepts related to the model-based diagnosis of DESs are given in Section 2. Several novel concepts, including minimal diagnosis, minimal diagnoser, and minimal diagnosability of DESs, are presented in Section 3. Related work is discussed in Section 4. Conclusions and future work are presented in Section 5.

2. Background

In this section, the classical notions of the diagnosis, diagnoser, and diagnosability of DESs [16] are recalled.

2.1. Classical Diagnosis of DESs. A DES is a deterministic finite state machine (FSM), namely, $G = (Q, \Sigma, T, q_0)$, where

Q is the set of states.

Σ is the set of events, including two disjoint sets of observable events (Σ_o) and unobservable events (Σ_{uo}); $\sum_f = \{f_1, f_2, \ldots, f_m\}$(for the sake of simplicity, the classification (types) of faults in [16] is disregarded in this paper), with $\sum_f \subseteq \sum_{uo}$, is the set of faulty events to be inferred, while $(\Sigma_{uo} - \Sigma_f)$ is the set of events that are both unobservable and nonfaulty.

$T \subseteq Q \times \Sigma \times Q$ is the set of transitions, where a transition from state q to state q', when event e is activated on state q, is equivalently denoted by $(q, e, q') \in T$, $q \xrightarrow{e} q'$, or $T(q, e) = q'$.

$q_0 \in Q$ denotes the initial state of the system.

The behaviour of G consists of all possible traces generated from q_0 to some state in G, which form a prefix-closed language $L(G)$, abbreviated as L, with $L \subseteq \Sigma^*$ (Σ^* is the set of all possible strings composed of events in Σ, including the empty string ε). For simplicity, we assume that language L is live, that is,

For each state $q \in Q$, there exists at least one event $\sigma \in \Sigma$ such that $q \xrightarrow{\sigma} q'$ holds, where $q' \in Q$ (with q' being nonnecessarily different from q).

In addition, similar to [16], we assume that there does not exist any cycle of unobservable events, that is,

For any cycle $q_1 \xrightarrow{\sigma_1} q_2 \xrightarrow{\sigma_2} \cdots q_{k-1} \xrightarrow{\sigma_{k-1}} q_k \xrightarrow{\sigma_k} q_1$ ($k \geq 1$), $q_i \in Q$, and $\sigma_i \in \Sigma$ ($i \in [1 \cdots k]$), there exists at least one event σ_j ($j \in [1 \cdots k]$) such that $\sigma_j \in \Sigma_o$.

Example 2. Outlined in Figure 1(a) is the diagrammatic representation of a DES model G, where $\Sigma_o = \{\alpha, \beta, \gamma, \theta, \rho\}$, $\Sigma_f = \{f_1, f_2\}$, and $\Sigma_{uo} = \{\sigma_{uo1}, \sigma_{uo2}\} \cup \Sigma_f$.

We denote the empty trace as ε and extend one transition event to a string of transition events as follows:

$q \xrightarrow{\varepsilon} q$ always holds

For $s \in \Sigma^*$ and $\sigma \in \Sigma$, $q \xrightarrow{s\sigma} q'$ holds whenever $q \xrightarrow{s} q''$ and $q'' \xrightarrow{\sigma} q'$ hold for $q'' \in Q$

Denoting a transition in which the entered state is missing, $q \xrightarrow{s}$ indicates that, for $s \in \Sigma^*$, there exists at least one state $q' \in Q$ such that $q \xrightarrow{s} q'$ holds.

The notation L/s represents the postlanguage of L after string $s \in L$, that is, $L/s = \{t \mid t \in \Sigma^*, st \in L\}$.

Two types of projection are given: Prj_{Σ_o} (on observation) and P_{Σ_f} (on faults). Assuming that $\sigma \in \Sigma$ and $s \in \Sigma^*$, $\mathrm{Prj}_{\Sigma_o}: \Sigma^* \longrightarrow \Sigma_o^*$ represents how a trace is projected onto a sequence of observable events:

$$\mathrm{Prj}_{\Sigma_o}(s\sigma) = \mathrm{Prj}_{\Sigma_o}(s)\mathrm{Prj}_{\Sigma_o}(\sigma). \tag{1}$$

Conversely, $\mathrm{Prj}_{\Sigma_o}^{-1}(s_o) = \{s \mid s \in L, \mathrm{Prj}_{\Sigma_o}(s) = s_o\}$ denotes the set of traces whose projection equals s_o (note here that $\mathrm{Prj}_{\Sigma_o}^{-1}(\mathrm{Prj}_{\Sigma_o}(s_o))$ may not equal s_o).

$P_{\Sigma_f}: \Sigma^* \longrightarrow 2^{\Sigma_f}$ denotes how a (possibly empty) trace $s \in \Sigma^*$ is mapped onto a set of faults:

$$P_{\Sigma_f}(s) = \{f_i \mid f_i \in \Sigma_f, f_i \in s\}. \tag{2}$$

Example 3. Let $s = af_1bcf_2$, $\{f_1, f_2\} \subseteq \Sigma_f$, and $\{a, b, c\} \subseteq \Sigma_o$. We have $\mathrm{Prj}_{\Sigma_o}(s) = abc$ and $P_{\Sigma_f}(s) = \{f_1, f_2\}$.

Let s_e denote the last event of a nonempty trace $s \in \Sigma^+$, where $\Sigma^+ = \Sigma^* - \{\varepsilon\}$, and $F \subseteq \Sigma_f$. Then, $S_F = \{s \mid s \in L, P_{\Sigma_f}(s) = F, s_e \in F\}$ denotes the set of all traces ending with one fault of F and containing all the faulty events of F.

We use $L(G, q)$ to denote all traces in G starting from state q. Let $L_o(G, q) = \{s \mid s \in L(G, q), s = u\sigma, u \in \Sigma_{uo}^*, \sigma \in \Sigma_o\}$ denote all traces starting from state q up to the first observable event and $L_\sigma(G, q) = \{s \mid s \in L_o(G, q), s_e = \sigma\}$ denote all traces starting from q up to the first observable event σ.

Based on $G = (Q, \Sigma, T, q_0)$, an FSM $G^o = (Q^o, \Sigma_o, T^o, q_0)$ (in general, nondeterministic (a nondeterministic FSM is a state in G which may reach more than one state via the same transition event. Accordingly, in Figure 1(b), state 1 can reach four different states (2, 7, 14, and 18) via the same observation α)) is defined as follows:

$Q^o = \{q_0\} \cup \{q' \mid q \xrightarrow{\sigma} q' \in T, \sigma \in \Sigma_o\}$ denotes both q_0 and all observable states.

$T^o \subseteq Q^o \times \Sigma_o \times Q^o$ denotes the set of transitions, defined as follows:

$$\left(q^o, \sigma, q^{o'}\right) \in T^o, \quad \text{iff } T(q^o, s) = q^{o'}, s \in L_\sigma(G, q^o). \tag{3}$$

As such, $L(G^o) = \{t \mid t = \mathrm{Prj}_{\Sigma_o}(s), s \in L\}$.

Example 4. With reference to Example 2, Figure 1(b) presents a diagrammatic representation of G^o, with G being displayed in Figure 1(a).

Based on the abovementioned notions, the notion of the diagnosis of a DES is given in Definition 1.

Definition 1. Let $G = (Q, \Sigma, T, q_0)$ be a DES, L be the corresponding language of G, and obs $\in \Sigma_o^*$ be the current observation sequence for G. A subset $F \subseteq \Sigma_f$ is called a candidate diagnosis (or just a diagnosis) of a DES for observation sequence obs (written as $F \rightsquigarrow$ obs) iff there is a string of events $s \in L$ with $s_e \in \Sigma_o$ such that $P_{\Sigma_f}(s) = F \wedge \mathrm{Prj}_{\Sigma_o}(s) = \text{obs}$.

In other words, a diagnosis of a DES is a set of faulty events (unlike the diagnosis of static systems (e.g., [41, 42]), where a diagnosis is defined as a set of faulty components.) in a trace whose mapping onto observable events equals only the current observation sequence obs. Note that the condition $s_e \in \Sigma_o$ must be satisfied in the definition, as we generally use the currently received observation sequences immediately after the DES fails to work properly to infer a set of faults to explain observation obs (this is also a fundamental principle of finding the diagnosis of DESs).

Example 5. With reference to Example 2, for the DES G displayed in Figure 1(a), if we get the current observation sequence obs = $\alpha\beta\theta$, then all candidate diagnoses are $\varnothing$, $\{f_1\}$, and $\{f_1, f_2\}$, with $\alpha\beta\theta$, $f_1\alpha\beta\theta$, and $f_1\alpha\beta f_2\theta$ being the corresponding traces of events, respectively.

2.2. Classical Diagnoser for DESs. To generate candidate diagnoses, the diagnoser-based approach introduced in [16] is used.

Let $\Delta = 2^{\Sigma_f \cup \{A\}}$ be all possible fault labels, with each label being a set of faulty events. N is used as an alias for the empty fault set (to indicate a normal state). A is interpreted as

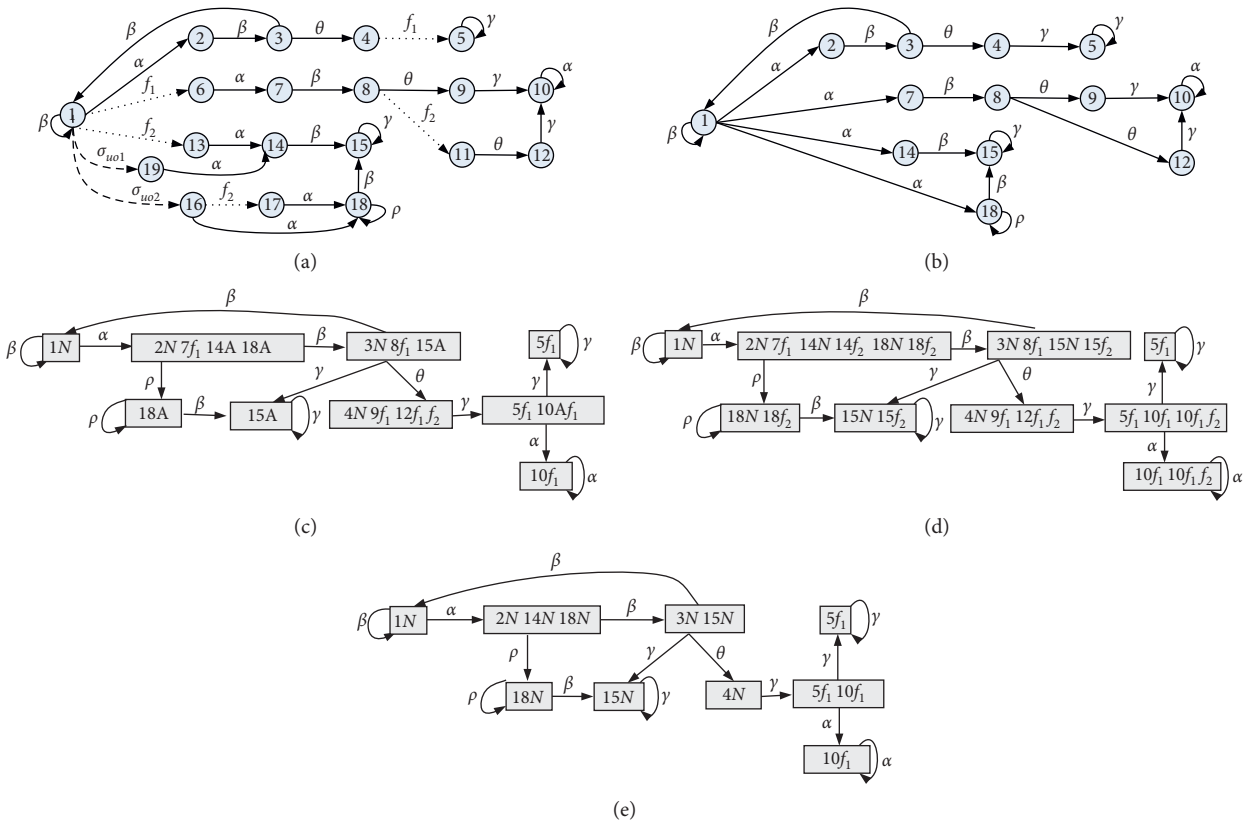

Figure 1: A DES and its related variant diagnosers: (a) DES model G. (b) Nondeterministic FSM G^o for G. (c) Classical diagnoser G_d for G. (d) Revised diagnoser G^d for G. (e) Minimal diagnoser G^m for G.

"ambiguous" (that is, we cannot be sure that some faults have definitely occurred).

Starting from $G^o = (Q^o, \Sigma_o, T^o, q_0)$, the classical diagnoser G_d for G is a deterministic FSM:

$$G_d = \left(q_d, \Sigma_o, T_d, q_d^0\right), \tag{4}$$

where

$q_d \subseteq 2^{(Q^o \times \Delta)}$ is the set of states.

$q_d^0 = \{(q_0, N)\}$ (since the fault label associated with q_0 is N, G is assumed to be normal at the initial state.) Any state $q_d \in q_d$ is reachable from q_d^0 via transitions in T_d, written as $q_d = \{(q_1^o, l_1), \ldots, (q_n^o, l_n)\}$, where $q_i^o \in Q^o$ and $l_i \in \Delta$ (that is, l_i is in the form of either N or a nonempty subset of $\Sigma_f \cup \{A\}$). In subsequent set-theoretic operations in the minimal diagnoser, we replace N with the empty set $\varnothing$.

The range function R: $q_d \times \Sigma_o \longrightarrow q_d$ is defined as follows:

$$R(q_d, \sigma) = \bigcup_{(q^o, l) \in q_d} \left(\bigcup_{s \in L_\sigma (G, q^o)} \left\{ \left(T(q^o, s), \mathrm{LP}(q^o, l, s) \right) \right\} \right), \tag{5}$$

where LP: $Q^o \times \Delta \times \Sigma^* \longrightarrow \Delta$ denotes the fault label propagation function. Given $q^o \in Q^o, l \in \Delta$, and $s \in L_o(G, q^o)$, fault label l is propagated by LP over string s from q^o in the following way:

$$\mathrm{LP}(q^o, l, s) = \left\{ f_i \,\middle|\, f_i \in l \vee f_i \in s \right\}. \tag{6}$$

Then, the label correction function LC: $q_d \longrightarrow q_d$ is defined as follows:

$$\begin{aligned} \mathrm{LC}(q_d) = \Big\{ (q^o, l) \,\Big|\, (q^o, l) \in q_d, \text{ and } \nexists (q^o, l') \in q_d \text{ with } l' \neq l \Big\} \cup \Big\{ \Big(q^o, \{A\} \cup \left(l_{i_1} \cap \cdots \cap l_{i_k} \right) \Big) \mid \left(q^o, l_{i_1} \right), \ldots, \left(q^o, l_{i_k} \right) \\ \in q_d, l_v \neq l_w, v, w \in \{i_1, \ldots, i_k\}, v \neq w, k \geq 2 \Big\}. \end{aligned} \tag{7}$$

The label correction function LC and the label A can be explained as follows. When the system moves along trace s and transitions from some state into a state q^o with at least two different fault labels, we cannot be sure that some faults

have definitely occurred; therefore, we use label A to refer to this scenario.

The transition function T_d: $q_d \times \Sigma_o \longrightarrow q_d$ is defined as follows:

$$q_d^2 = T_d\left(q_d^1, \sigma\right) \Longleftrightarrow q_d^2 = \mathrm{LC}\left(R\left(q_d^1, \sigma\right)\right). \tag{8}$$

In other words, assuming that the current state in diagnoser G_d is q_d^1, while the next observable event is σ, we generate the new state q_d^2 of G_d in the following way:

(1) For each $(q^o, l) \in q_d^1$, compute the set $S(q^o, \sigma)$ of reachable states of G from q^o using observation σ:

$S(q^o, \sigma) = \{T(q^o, u\sigma) \mid u \in \Sigma_{uo}^*$, and $\sigma \in \Sigma_o\}$(note here that $S(q^o, \sigma)$ is a finite set of observable states, as we have made an assumption (in Section 2.1) that there does not exist any cycle of unobservable events [16]).

(2) Given $q^{o'} \in S(q^o, \sigma)$ with $T(q^o, u\sigma) = q^{o'}$, propagate label l associated with q^o to label l' associated with $q^{o'}$ according to the following rules:

(a) If $l = N$ and s contains no faulty events, then label l' is kept as N.
(b) If $l = \{A\}$ and s contains no faulty events, then label l' is kept as $\{A\}$.
(c) If $l = \{A\} \cup F$ with $F \subseteq \Sigma_f$ and s contains no faulty events, then label l' is updated to F.
(d) If $l = N$ or $\{A\}$ and s contains a set F of faulty events, then label l' is updated to F.
(e) If either $l = F$ or $\{A\} \cup F$ with $F \subseteq \Sigma_f$ and s contains a set F' of faulty events, then label l' is updated to $F \cup F'$(in cases (c), (d), and (e) above, we do not propagate label A from one state to the next. As noted in [16], while this leads to a reduction in the state space of the diagnoser, no information necessary for either determining the diagnosability properties of a language or for implementing diagnostics is lost).

(3) Let q_d^2 be the set of all pairs $(q^{o'} l')$ generated by (1) and (2) above for each $(q^o, l) \in q_d^1$. Replace all $(q^{o'}, l')$, $(q^{o'}, l'') \in q_d^2$ $(l' \neq l'')$ with $(q^{o'}, \{A\} \cup l' \cup l'')$. That is, if the same state $q^{o'}$ appears more than once in q_d^2 with different labels, then associate all the common faults with $q^{o'}$ as well as the ambiguous label A with $q^{o'}$.

Example 6. With reference to Example 2 and Example 4, Figure 1(c) presents the classical diagnoser G_d relevant to DES G displayed in Figure 1(a) (where pairs (q, l) are written as ql, while "{}" is omitted for each nonempty fault label l for simplicity). According to G_d in Figure 1(c), we can easily obtain the definite diagnosis $\{f_1\}$, for a given observation sequence $\alpha\beta\theta\gamma\gamma$, online by synchronizing diagnoser G_d with the sequence.

2.3. Classical Diagnosability of DESs. To decide whether or not a faulty event in a DES has definitely occurred, the classical notion of diagnosability presented by [16] is rephrased in Definition 2 (Definition 2 is slightly different from the original definition of diagnosability in [16]. Specifically, "$\exists n_i (n_i \in \mathbb{N})$" is placed after "$\forall s (s \in L, s_e = f_i)$", while n_i in [16] becomes the greatest n_i for all s in Definition 2. This adjustment, while not affecting the virtual meaning of diagnosability, allows us to provide a formalization that is more consistent with the notions of minimal diagnosability introduced below).

Definition 2. A prefix-closed and live language L is said to be diagnosable iff, for any fault $f_i \in \Sigma_f$, we have

$$\begin{aligned} &\forall s\left(s \in L, s_e = f_i\right) \exists n_i \left(n_i \in \mathbb{N}\right), \\ &\forall t\left(t \in L/s, t_e \in \Sigma_o\right), \\ &\left(\|t\| \geq n_i \Longrightarrow D\right), \end{aligned} \tag{9}$$

where the diagnosability condition D is defined as follows:

$$\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(st)\right) \Longrightarrow f_i \in \omega. \tag{10}$$

In other words, if a DES G is diagnosable, then any faulty event f_i of G will definitely be detected after its occurrence, provided that the observation sequence after f_i is long enough.

Example 7. From Definition 2, we know that DES G in Figure 1(a) is not diagnosable, since for observation sequences $\alpha\rho^k$, $k \in \mathbb{N}$, we cannot decide whether fault f_2 has definitely occurred or not.

3. Minimal Diagnosis of DESs

In this section, in a way similar to the minimal diagnosis of static systems [41, 42], a notion of the "minimal diagnosis" of DESs is proposed. Then, the related "minimal diagnoser" for DESs is presented to generate all minimal diagnoses. Finally, the relevant "minimal diagnosability" is put forward and compared with classical diagnosability.

3.1. Minimal Diagnosis of DESs. Based on Definition 1 and Example 5, for a given observation sequence, there are three possible candidate diagnoses. Generally, given a DES G with language L, there is usually more than one string in L, with each string having a projection on the set of observable events equal to the current observation sequence obs. Hence, there may be more than one candidate diagnosis set according to the different strings. However, as noted above, minimal diagnoses are very valuable. For example, for a batch of new products from a factory, the qualification rate is usually very high (generally required to be more than 95%). The probability of a product with a fault is very low (less than 5%). According to the principles of joint probability distribution (usually, in the literature, it is assumed that faults are independent of one another and have equal probability of occurrence), the probability of a product with two or more faults is significantly lower.

To obtain more likely candidates and to reduce the space complexity (with less space to store diagnoses with fewer faults), we provide a definition below to formalize the

concept of the minimal diagnosis of DESs based on set-inclusion relationship.

Let F_1 and F_2 be two candidate diagnoses for an observation sequence obs, namely, $(F_1 \rightsquigarrow \text{obs}) \wedge (F_2 \rightsquigarrow \text{obs})$. The following notation is defined:

$F_1 \preccurlyeq F_2$ if $F_1 \subseteq F_2$

$F_1 \prec F_{2\text{ss}}$ if $F_1 \subset F_2$

$F_1 \prec\succ F_2$ if $(F_1 \not\subseteq F_2) \wedge (F_2 \not\subseteq F_1)$

Definition 3. Let $G = (Q, \Sigma, T, q_0)$ be a DES, obs be a relevant observation sequence, and F be a candidate diagnosis for obs. Candidate F is called a minimal diagnosis of G for obs, also written as $F \rightsquigarrow_{\min} \text{obs}$, if there is no other candidate diagnosis F' for obs such that $F' \prec F$. The family of all minimal candidate diagnoses for obs is $\{F \mid F \rightsquigarrow_{\min} \text{obs}\}$.

In other words, if a fault set F is a minimal diagnosis of G, then none of its proper subsets is a diagnosis. Furthermore, according to the principle of joint-probability distribution, a minimal diagnosis (with fewer number of faults) is more probable than the corresponding nonminimal diagnosis (with additional faults). As a result, some faulty events may not appear in the minimal diagnosis, although they can also be used to explain the current observation sequence. The following example explicitly verifies this conclusion.

Example 8. With reference to Example 5, for the DES G displayed in Figure 1(a), when the current observation sequence is obs = $\alpha\beta\theta$, we find that all the possible candidate diagnoses are $\varnothing$ (or N), $\{f_1\}$, and $\{f_1, f_2\}$. Then, we get the minimal diagnosis N, i.e., the system is probably working normally. Although two fault sets $\{f_1\}$ and $\{f_1, f_2\}$ can also be used to explain the current observation sequence, they are not minimal diagnoses.

3.2. Minimal Diagnoser for DESs. In this section, we propose a type of minimal diagnoser based on a revised diagnoser.

3.2.1. Revised Diagnoser. In order to properly and briefly define the concept of a minimal diagnoser, we first introduce a revised diagnoser G^d based on the classical notion of diagnoser G_d presented in [16].

Starting from $G^o = (Q^o, \Sigma_o, T^o, q_0)$, a revised diagnoser G^d for G is a deterministic FSM:

$$G^d = \left(Q^d, \Sigma_o, T^d, q_0^d\right), \tag{11}$$

where

$Q^d \subseteq 2^{(Q^o \times \Delta)}$ is the set of states.

$q_0^d = \{(q_0, N)\}$. Any state $Q^d \in Q^d$ is reachable from q_0^d via transitions in T^d, written as $Q^d = \{(q_1^o, l_1), \ldots, (q_n^o, l_n)\}$, where $q_i^o \in Q^o$ and $l_i \in \Delta$ (that is, l_i is in the form of either N or a nonempty subset of Σ_f).

The transition function T^d: $Q^d \times \Sigma_o \longrightarrow Q^d$ is defined as follows:

$$T^d\left(Q^d, \sigma\right) = \bigcup_{(q^o,l)\in Q^d} \left(\bigcup_{s\in L_\sigma(G,q^o)} \{(T(q^o, s), \text{LP}(q^o, l, s))\} \right). \tag{12}$$

In other words, assume that q_1^d is the current state in the revised diagnoser G^d and that σ is the next observable event. The new state q_2^d of G^d is generated in the following way (the revised diagnoser can also be computed by performing a parallel composition between G and the label automaton Al, as suggested in the book by Cassandras and Lafortune [14], where Al is an automaton whose initial state is N, whose remaining (2^{p-1}) states are nonempty subsets of $\{f_1, f_2, \ldots, f_p\}$, with p being the number of faulty events, and whose transition events are $f_1, f_2, \ldots, f_p$ when appropriate):

(1) For each $(q^o, l) \in q_1^d$, compute the set $S(q^o, \sigma)$ of reachable states of G from q^o over observable event σ:

$$S\left(q^o, \sigma\right) = \left\{T\left(q^o, u\sigma\right) \mid u \in \Sigma_{uo}^*, \text{ and } \sigma \in \Sigma_o\right\}. \tag{13}$$

(2) Given $q^{o'} \in S(q^o, \sigma)$ with $T(q^o, u\sigma) = q^{o'}$, propagate fault label l related to q^o to fault label l' related to $q^{o'}$ as follows: $l' = l \cup \{f_i \mid f_i \in u\}$.

(3) Let q_2^d be the set of all pairs $(q^{o'}, l')$, generated by the above steps (1) and (2), for each $(q^o, l) \in q_1^d$.

According to the definitions of G^d and G_d, we can find that for each state in G^d, there is a corresponding state in G_d; the contrary, however, is not always the case. In addition, an important difference between G^d and G_d is that the symbol A is not introduced in G^d. Hence, we can retain more relevant fault information (for obtaining the minimal diagnosis). For example, if one state $Q^d \in G^d$ is $\{(q_i, f_i), (q_j, f_j)\}$, then the two minimal diagnoses $\{f_i\}$ and $\{f_j\}$ are both kept, that is, clearer fault information is provided compared with G_d. In fact, the fault information in G_d is denoted only as A in this situation, and the necessary fault information is missing (e.g., states {(18, {A})} and {(15, {A})} in Figure 1(c)). Additionally, some relevant fault information is again missing for all possible diagnoses, according to rules (c), (d), and (e) when propagating fault label l, including A, into l' because the ambiguous symbol A is omitted (see Section 2.2 and the transition from state {(5, $\{f_1\}$), (10, {A, f_1})} to state {(10, $\{f_1\}$)} in Figure 1(c)). In contrast, all possible fault information is preserved in the revised diagnoser G^d.

Example 9. With reference to Example 2 and Example 4, Figure 1(d) presents the revised diagnoser G^d relevant to the DES G displayed in Figure 1(a) (similar to Example 6, each pair (q, l) is written as ql, while, for the sake of simplicity, "{}" is omitted for each nonempty fault label l).

Notice how all possible fault information is maintained in G^d, which can be conveniently exploited by a minimal diagnoser for the minimization of fault sets.

3.2.2. Minimal Diagnoser. To efficiently generate all minimal diagnoses of a DES online, we propose a novel notion of minimal diagnoser, which can be generated offline.

Definition 4. Given a DES $G = (Q, \Sigma, T, q_0)$, the related $G^o = (Q^o, \Sigma_o, T^o, q_0)$, and the revised diagnoser $G^d = (Q^d, \Sigma_o, T^d, q_0^d)$, a minimal diagnoser for G is an FSM:

$$G^m = \left(Q^m, \Sigma_o, T^m, q_0^m\right), \tag{14}$$

where

$Q^m \subseteq 2^{(Q^o \times \Delta)}$ is the set of states.

$q_0^m = \{(q_0, N)\}$. Any state $q^m \in Q^m$ is reachable from q_0^m via transitions in T^m, written as $q^m = \{(q_1^o, l_1), \ldots, (q_n^o, l_n)\}$, where $q_i^o \in Q^o$ and $l_i \in \Delta$ (that is, l_i is in the form of either N or a nonempty subset of Σ_f).

T^m: $Q^m \times \Sigma_o \longrightarrow Q^m$ is the transition function.

More specifically, T^m and Q^m are generated as follows:

(1) For each $q_i^d \in Q^d$, there exists a corresponding minimized state $q_i^m \in Q^m$, obtained as follows: initially, $q_i^m = q_i^d$; then, for each $(q^o, l) \in q_i^d$, any other $(q^{o'}, l') \in q_i^d$ with $l \prec l'$ will be removed from q_i^m(in particular, state $q^{o'}$ may equal q^o). In other words, all the pairs labelled with nonminimal fault labels will be dropped.

(2) For each transition $(q_i^d \xrightarrow{\sigma} q_j^d) \in T^d$ (where $\sigma \in \Sigma_o$ and $q_i^d, q_j^d \in Q^d$), there is a corresponding transition $(q_i^m \xrightarrow{\sigma} q_j^m) \in T^m$ (where $q_i^m, q_j^m \in Q^m$).

(3) All states and transitions in G^m are generated by the abovementioned steps (1) and (2).

(4) Trim operation: if any two minimal states share not only the same contents but also the same transitions from them (to the same states), they will be seen as the same state and be merged into one state. Otherwise, they will not be merged even if they have the same contents.

From the definition of minimal diagnoser, any state in the revised G^d is transformed into a state in the minimal diagnoser G^m, though generally with the same or fewer labels (there may be several different states in G^d that have been transformed into one state in G^m).

In other words, the minimal diagnoser G^m, with the same number of states and the same isomorphic transition structure as those of the classical diagnoser G_d, is a deterministic (and trim) FSM, where each state is generally smaller than the corresponding state in G_d (although the space complexity of G^m is still exponential regarding the number of states of the system model, since only the minimal fault labels are retained, less space is required. Although, for simplicity, the theoretical definition of minimal diagnoser is based on that of the revised diagnoser G^d, we would actually like to consider some algorithms that generate a minimal diagnoser based only on the DES G in some special situations, without the need to generate G^d again. This is an interesting topic that should be analysed in future research).

Remark 1. Based on the definition of a "minimal diagnoser," it seems that some nonminimal diagnoses will be lost as well as the diagnosis completeness of the requirement in model-based diagnosis. As a matter of fact, the property of minimal-diagnosis completeness is indeed preserved by the minimal diagnoser, that is, most probable diagnoses are retained in the diagnosis results.

Remark 2. Like the classical diagnoser, the minimal diagnoser can generally be built offline and used for online efficient diagnosis.

Example 10. Figures 2(a) and 2(b) show two different DESs and their different diagnosers G_d, G^d, and G^m. We can see that G^m is isomorphic to the corresponding G_d. Also, note that in Figure 2(a), two states of G^d, namely, $(3N\ 3f_1)$ and $(3N\ 3f_2)$, are merged into one state $(3N)$ in G^m after minimization. By contrast, in Figure 2(b), two states of G^d, namely, $(4N\ 5f_1)$ and $(4N\ 6f_2)$, are not merged into one state $(4N)$ in G^m, as they have different transitions from themselves (to different states).

According to Definition 4, a number of relevant properties of minimal diagnoser G^m are given below (which will be used to prove the subsequent related lemmas/propositions):

(P_1) Let $q_i^m \in Q^m$. For each $(q_i^o, l_i) \in q_i^m$, there is at least a state $q_i^d \in Q^d$ in G^d such that $(q_i^o, l_i) \in q_i^d$.

(P_2) Let $q^m \in Q^m$. If $(q^o, l), (q^{o'}, l') \in q^m$, then there exist $s, s' \in L$ with $s_e, s_e' \in \Sigma_o$ such that $T(q_0, s) = q^o$, $T(q_0, s') = q^{o'}$, $\mathrm{Prj}_{\Sigma_o}(s) = \mathrm{Prj}_{\Sigma_o}(s')$, $P_{\Sigma_f}(s) = l$, $P_{\Sigma_f}(s') = l'$, and either $l = l'$ or $l \prec\succ l'$.

(P_3) Let $q^m \in Q^m$. There may exist $(q^o, l), (q^o, l') \in q^m$, that is, the system might reach the same observable state q^o with different minimal fault labels $(l \neq l')$.

(P_4) For each $q^m \in Q^m$ and for each $(q^o, l), (q^{o'}, l') \in q^m$, we have

$$l = l' \Longleftrightarrow l \subseteq l'$$
$$l \neq l' \Longleftrightarrow l \prec\succ l'$$

(P_5) Let $(q_i^m \xrightarrow{\sigma} q_j^m) \in T^m$. For each $(q_j^o, l_j) \in q_j^m$, there exists $(q_i^o, l_i) \in q_i^m$ such that $l_i \subseteq l_j$.

After (offline) building the minimal diagnoser G^m for DES G and assuming that the current observation is obs, we can (online) synchronize obs with G^m to reach the corresponding state in G^m to directly obtain the minimal diagnoses within the state.

Example 11. Consider the DES G outlined in Figure 1(a) and assume obs = $\alpha\beta\theta$. According to the minimal diagnoser G^m outlined in Figure 1(e), we obtain the current minimal diagnosis N, that is, no fault is produced by $(4, N)$. In addition, when we receive the additional observation γ, we obtain the new minimal diagnosis $\{f_1\}$ (while the nonminimal diagnosis $\{f_1, f_2\}$ in label $(10, \{f_1, f_2\})$ of G^d is avoided).

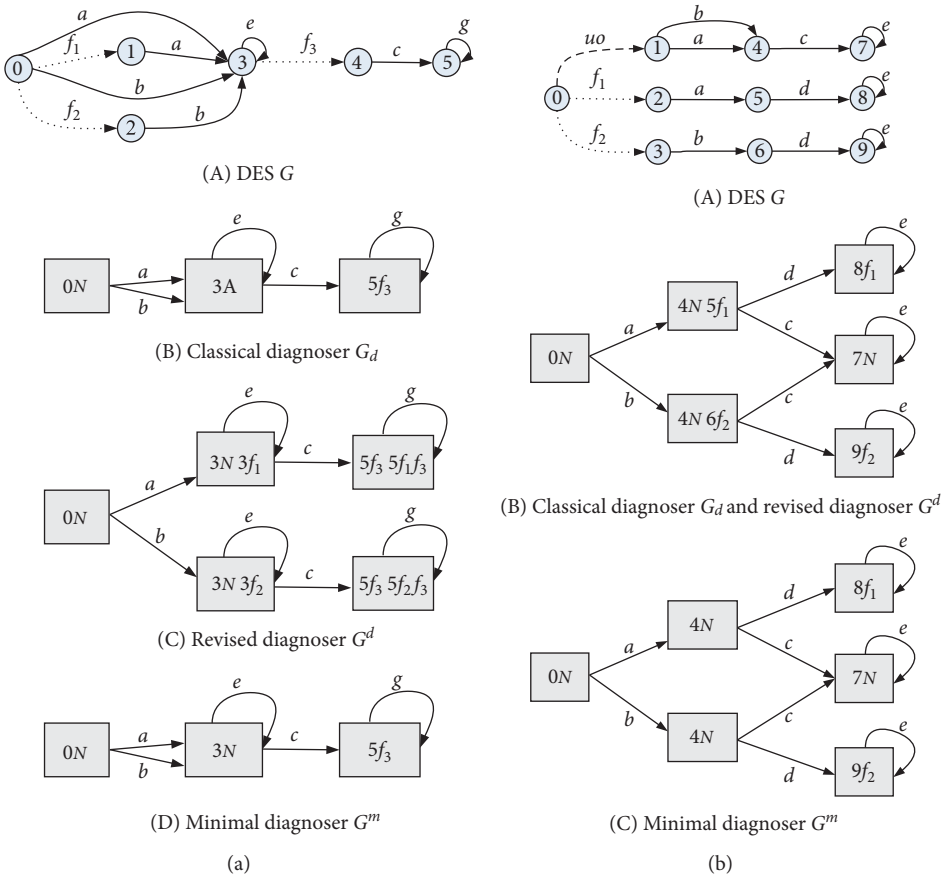

Figure 2: Two DESs and their minimal diagnosers: (a) the first DES and (b) the second DES.

3.3. Minimal Diagnosability of DESs. Just as the classical diagnosability was defined to determine whether a classical diagnosis has definitely occurred or not, it is natural to define minimal diagnosability to determine whether a set of faults has definitely occurred or not.

In this section, to either strongly or weakly determine whether a set of faults has definitely occurred or not, two notions (strong and weak) of the minimal diagnosability of DESs are proposed.

To introduce the formalizations for the minimal diagnosability of a DES G, we define the domain $\mathscr{F}_L$ to denote the collection of all possible fault sets of G (with behaviour L) as follows:

$$\mathscr{F}_L = \bigcup_{s\in L\wedge s_e\in\Sigma_o} \left\{\left\{f_i \mid f_i \in s\right\}\right\}. \tag{15}$$

Obviously, $\mathscr{F}_L = \cup_{s\in L\wedge s_e\in\Sigma_o}\left\{P_{\Sigma_f}(s)\right\}$.

3.3.1. Strong Minimal Diagnosability of DESs

Definition 5. A prefix-closed and live language L is said to be strongly minimally diagnosable if, for any fault set $F \in \mathscr{F}_L$ and for any string $s \in S_F$, the following properties hold:

(i) $\forall t\,(t \in L/s, t_e \in \Sigma_o, P_{\Sigma_f}(t) \subseteq F)\,\exists t'\,(t' \in L/(st),\ (tt')_e \in \Sigma_o, P_{\Sigma_f}(t') \subseteq F)\,((F \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(st)) \Longrightarrow D_m^1)$

(ii) $\exists n\,(n \in \mathbb{N})\,\forall t\,(t \in L/s, t_e \in \Sigma_o)\,(\|t\| \geq n \Longrightarrow ((F \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(st)) \Longrightarrow D_m^2))$

where the strong minimal diagnosability conditions D_m^1 and D_m^2 are defined as follows:

$$\begin{aligned} D_m^1&: \left(\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(stt')\right)\right) \Longrightarrow \left(F \lesssim P_{\Sigma_f}(\omega)\right), \\ D_m^2&: \left(\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(st)\right)\right) \Longrightarrow \left(F \lesssim P_{\Sigma_f}(\omega)\right). \end{aligned} \tag{16}$$

In other words, assume that s is a trace in G ending with one fault of F and containing exactly the faulty events of F:

(i) For any continuation t of string s without any new fault, the DES will always reach an observable state after a continuation t' of t (i.e., $(tt')_e \in \Sigma_o$), also without any new fault, such that if F is a minimal fault set for st, then F will be the unique minimal diagnosis for any trace with the same observation sequence in stt' (here, we make an implicit assumption that a faulty event may be triggered by a string many times. In other words, if all faulty events in F have been triggered by string s, then some faults in F may still be triggered again in a suffix string t after s).

(ii) In addition, it is required that there is always a natural number n such that when any continuation t

of s is long enough (i.e., the length of t is not less than n), if F is a minimal fault set for st, then F will be the unique minimal diagnosis for any trace with the same observation sequence in st.

Note: in contrast with the notion of classical diagnosability (Definition 2), here, we add two additional conditions, namely, $P_{\Sigma_f}(t) \subseteq F$ and $P_{\Sigma_f}(t') \subseteq F$, to restrict later subsequences, after the complete occurrence of F, such that they do not contain any new fault, except those in F, to ensure that F is still retained as a candidate diagnosis.

In [16], the notion of classical diagnosability is proposed for checking any single fault f_i of G (Definition 2), whereas our notion of minimal diagnosability is proposed for a set F of faulty events of G, which must be minimal (compared to other related candidates). Both require that any fault f_i or any minimal fault set F must be definitely detected after their occurrences (within a finite delay).

However, there is no logic entailment between the classical diagnosability and our strong minimal diagnosability, as shown in the following example.

Example 12. According to Definition 2 and Definition 5, DES G in Figure 1(a) is strongly minimally diagnosable yet not diagnosable (we can verify the strong minimal diagnosability of the DES in Figure 1(a) based on Proposition 1 below. That is, we can check the minimal diagnoser in Figure 1(e). It is much easier to find that the minimal diagnoser satisfies the following two conditions in Proposition 1: (1) there is no F-indeterminate cycle and (2) there is no F-incomparable state. Thus, the DES in Figure 1(a) is strongly minimally diagnosable). By contrast, DES G_3 in Figure 3(e) is diagnosable yet not strongly minimally diagnosable.

Before introducing the necessary and sufficient conditions for the strong minimal diagnosability of DESs, a number of related definitions and relevant lemmas are provided below.

Definition 6. A state $q^m \in Q^m$ is said to be F-certain if, for any two pairs (q^o, l), $(q^{o'}, l') \in q^m$ (where $q^{o'}$ can possibly equal q^o), we always have $l' = l$.

A state $q^m \in Q^m$ is said to be F-incomparable if there exist two pairs (q^o, l), $(q^{o'}, l') \in q^m$ (where $q^{o'}$ can possibly equal q^o) such that $l \prec\succ l'$.

For instance, the state exactly labelled with $\{4f_1, 5f_2\}$ in Figure 3 is F-incomparable, whereas other states of minimal diagnosers in Figure 3 are all F-certain. The basic properties of the two types of states are described by the following lemma.

Lemma 1. *For the minimal diagnoser G^m of DES G, the following properties hold.*

Let $T^m(q_0^m, s) = q^m$, $s \in \Sigma_o^*$. If state q^m with fault label l is F-certain, then for each $\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}(s)$, we have $l \preccurlyeq P_{\Sigma_f}(\omega)$.

If a state $q^m \in Q^m$ is F-incomparable, then for any two pairs (q^o, l), $(q^{o'}, l') \in q^m$ with $l \neq l'$, there exist two strings $t, t' \in L$ with $t_e, t'_e \in \Sigma_o$ such that $T(q_0, t) = q^o$, $T(q_0, t') = q^{o'}$, $\mathrm{Prj}_{\Sigma_o}(t) = \mathrm{Prj}_{\Sigma_o}(t')$, $T^m(q_0^m, \mathrm{Prj}_{\Sigma_o}(t)) = q^m$, $l = P_{\Sigma_f}(t)$, $l' = P_{\Sigma_f}(t')$, and $l \prec\succ l'$.

In other words, if a state q^m is F-certain, then any trace ω with the same observation projection as observation sequence s will necessarily contain fault set l. Otherwise, if a state q^m is F-incomparable, then there exist at least two different traces t and t' having the same observation projection but with two incomparable fault sets l and l'.

Definition 7. A set of F-incomparable states $q_1^m, q_2^m, \ldots, q_n^m \in Q^m$ is said to form an F-indeterminate cycle if $T^m(q_i^m, \sigma_i) = q^m_{(i+1) \bmod n}$ (here, "$(i+1) \bmod n$" represents the modulus of $(i+1)$ divided by n.), where $\sigma_i \in \Sigma_o$, $i \in [1 \cdots n]$.

Based on Definition 7, an interesting lemma is given below.

Lemma 2. *Assume that $q_1^m, q_2^m, \ldots, q_n^m \in Q^m$ are a set of F-incomparable states forming an F-indeterminate cycle, where*

$$\begin{aligned} q_i^m &= \left\{\left(q^o_{i_1}, l_{i_1}\right), \left(q^o_{i_2}, l_{i_2}\right), \ldots, \left(q^o_{i_{len\_i}}, l_{i_{len\_i}}\right)\right\}, \\ q_j^m &= \left\{\left(q^o_{j_1}, l_{j_1}\right), \left(q^o_{j_2}, l_{j_2}\right), \ldots, \left(q^o_{j_{len\_j}}, l_{j_{len\_j}}\right)\right\}, \end{aligned} \tag{17}$$

with $i, j \in [1 \cdots n]$ and len_i, len_j denoting the number of pairs in q_i^m and q_j^m, respectively. Then, we have

$$\left\{l_{i_1}, l_{i_2}, \ldots, l_{i_{\mathrm{len\_}i}}\right\} = \left\{l_{j_1}, l_{j_2}, \ldots, l_{j_{\mathrm{len\_}j}}\right\}. \tag{18}$$

In other words, in an F-indeterminate cycle, any state has the same set of different fault labels. Intuitively, on the one hand, a fault in the current state will stay in the next state (we assume that the faults are persistent); on the other hand, since all states form a cycle, the previous state of the current one can also be seen as the next state. Therefore, all states share the same faults (in fact, Lemma 2 is true for all kinds of cycles. That is, the conclusion is much clearer when all states in the cycle are F-certain).

Lemma 3. *Given a prefix-closed language L, if $F \rightsquigarrow_{\min} Prj_{\Sigma_o}(s)$ holds for a fault set $F \in \mathscr{F}_L$ and a string $s \in L$ with $s_e \in \Sigma_o$ and $P_{\Sigma_f}(s) = F$, then for any string $t \in L/s$ with $t_e \in \Sigma_o$ and $P_{\Sigma_f}(t) \subseteq F$, we have $F \rightsquigarrow_{\min} Prj_{\Sigma_o}(st)$.*

In other words, if a fault set F of a trace s is a minimal diagnosis for the observation projection of s, then F is still a minimal diagnosis for any subsequent longer trace from s, provided there is no new fault in the subsequent trace.

Lemma 4. *Given a prefix-closed language L, $F \rightsquigarrow_{\min} Prj_{\Sigma_o}(s)$ holds for a fault set $F \in \mathscr{F}_L$ and a string $s \in L$ with $s_e \in \Sigma_o$ and $P_{\Sigma_f}(s) = F$. If F is the unique minimal diagnosis for observation $Prj_{\Sigma_o}(s)$, i.e.,*

$$\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(s)\right) \Longrightarrow F \preccurlyeq P_{\Sigma_f}(\omega), \tag{19}$$

then for each string $t \in L/s$ with $t_e \in \Sigma_o$, the following holds:

$$\omega' \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(st)\right) \Longrightarrow F \preccurlyeq P_{\Sigma_f}(\omega). \tag{20}$$

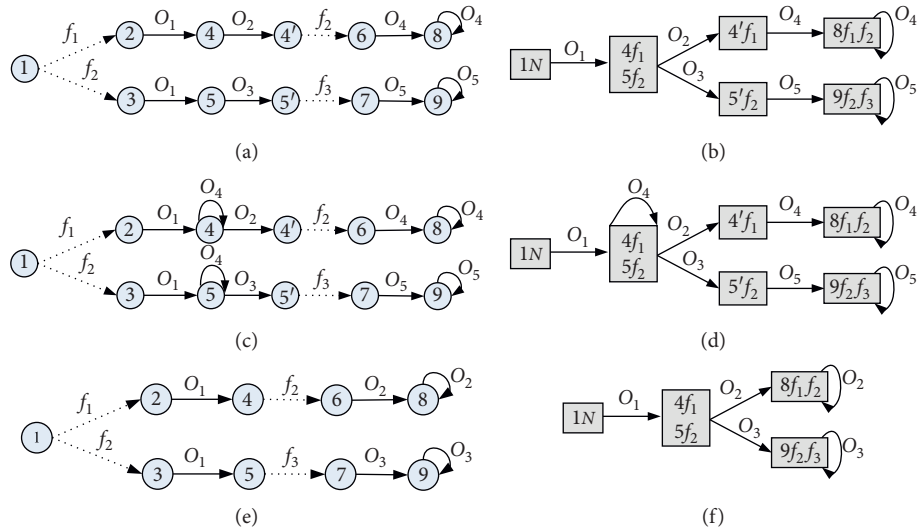

Figure 3: DES models and minimal diagnosers. (a) DES model G_1. (b) Minimal diagnoser G_m^1 for G_1. (c) DES model G_2. (d) Minimal diagnoser G_m^2 for G_2. (e) DES model G_3. (f) Minimal diagnoser G_m^3 for G_3.

In other words, if F is the unique minimal diagnosis for a string s (and its projection on the observation is $\mathrm{Prj}_{\Sigma_o}(s)$), then any trace with the same observation $\mathrm{Prj}_{\Sigma_o}(st)$ will still contain all the faults in F.

Given the definitions and lemmas introduced above, we now present the necessary and sufficient conditions for the strong minimal diagnosability of a DES G in Proposition 1, based on its minimal diagnoser G^m.

Proposition 1. *A language L generated by an FSM G is strongly minimally diagnosable iff its minimal diagnoser G^m satisfies the following two conditions:*

(C_1) *There is no F-indeterminate cycle in G^m*

(C_2) *For each F-incomparable state $q^m \in Q^m$ and for each pair $(q^o, l) \in q^m$, there exist a state $q^{m'} \in Q^m$ and a nonempty observation sequence $s_o \in \Sigma_o^+$ such that $T^m(q^m, s_o) = q^{m'}$, and for each pair $(q^{o'}, l')$, we have $l' = l$, that is, $q^{m'}$ (after q^m) is an F-certain state with the unique minimal fault label l*

Remark 3. Condition (C_1) is almost identical to the first condition for checking the classical diagnosability in [16], with the exception that "F_i-indeterminate cycle" is replaced by "F-indeterminate cycle". However, Condition (C_2) is more complex than the corresponding one for checking the classical diagnosability (where only one statement is needed, namely, "No state $q \in q_d$ is ambiguous"), as the strong minimal diagnosability is conceptually more complex.

Example 13. Consider the three DES models G_1, G_2, and G_3 in Figure 3, where f_1, f_2, and f_3 are faults, while the other events are observable. Their minimal diagnosers G_1^m, G_2^m, and G_3^m are also depicted in Figure 3. According to the three minimal diagnosers, we can find that only G_1 is strongly minimally diagnosable. G_2 is not strongly minimally diagnosable because it does not fulfil Condition (C_1): there does exist an F-indeterminate cycle including state $\{(4, \{f_1\}), (5, \{f_2\})\}$ and the cyclic transition event o_4 in G_2^m. G_3 is also not strongly minimally diagnosable because it does not fulfil Condition (C_2): there does exist an F-incomparable state $q^m = \{(4, \{f_1\}), (5, \{f_2\})\}$ in G_3^m, but there are no states such as $\{(4', \{f_1\})\}$ or $\{(5', \{f_2\})\}$ after q^m in G_3^m.

3.3.2. Weak Minimal Diagnosability of DESs. As mentioned above, according to Definition 5, it is required that any minimal fault set F be the unique minimal diagnosis after a finite delay but before a new faulty event (not in F) occurs. In theory, the condition is very strong. Therefore, we provide the following notion of the weak minimal diagnosability of a DES.

Definition 8. A prefix-closed and live language L is weakly minimally diagnosable if the following condition holds:

$$\begin{aligned} &\forall F\left(F \in \mathscr{F}_L\right), \\ &\forall s\left(s \in S_F\right), \\ &\exists n\left(n \in \mathbb{N}\right), \\ &\forall t\left(t \in L/s, t_e \in \Sigma_o\right), \\ &\left(t \geq n \Longrightarrow D_m\right), \end{aligned} \tag{21}$$

where the minimal diagnosability condition D_m is defined in the following way:

$$\left(F \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(st)\right) \Longrightarrow \left(\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(st)\right) \Longrightarrow F \preccurlyeq P_{\Sigma_f}(\omega)\right). \tag{22}$$

In other words, assume that s is a trace of G ending with a set F of faulty events. For each continuation trace t of s, there always exists a natural number n such that when the length of trace t is greater than or equal to n, and if F is still the minimal fault set for st, then fault set F will be the unique minimal diagnosis for any trace with the same observation projection on st.

If the language of a DES has the property of weakly minimal diagnosability, when a trace is long enough (i.e., the length of its continuation t is not less than a given integer n), and if the set of faulty events in the trace is still minimal, then it will definitely be the unique minimal diagnosis. According to the above analysis, the condition of Definition 8 is weaker than that provided in Definition 5 and Definition 2. The following proposition shows the relations between the representation of classical diagnosability and our two representations of minimal diagnosability.

Proposition 2. *Let G be a DES with language L. If L is strongly minimally diagnosable, then L is also weakly minimally diagnosable. If L is diagnosable, then L is also weakly minimally diagnosable.*

However, based on the following example, we can show that the contrary of Proposition 2 does not hold.

Example 14. According to our definitions, we can see that DES G_3 in Figure 3(e) is weakly minimally diagnosable yet not strongly diagnosable. In contrast, the DES G in Figure 1(a) is weakly minimally diagnosable yet not diagnosable.

Remark 4. The notion of minimal diagnosability allows missed detection. That is, it is possible that some of the failures are not detected by a minimal diagnoser. For example, the occurrence of f_2 cannot be detected in the DES model shown in Figure 1(a), although the DES is also weakly minimally diagnosable. After all, only subset-minimal diagnoses are taken into account in our framework.

In the following, we give the necessary and sufficient conditions for the weak minimal diagnosability of a DES.

Proposition 3. *A language L generated by an FSM G is weakly minimally diagnosable iff its minimal diagnoser G^m does not include any F-indeterminate cycle.*

Remark 5. Compared with the necessary and sufficient conditions for the strong minimal diagnosability of DESs in Proposition 1, the conditions for weak minimal diagnosability for the DESs in Proposition 3 are much weaker.

Example 15. Consider the three DESs and the related minimal diagnosers shown in Figure 3. Based on the three minimal diagnosers, we conclude that both G_1 and G_3 are weakly minimally diagnosable. Instead, G_2 is not weakly minimally diagnosable, as there is an F-indeterminate cycle that includes the only state $\{(4, \{f_1\}), (5, \{f_2\})\}$ and the corresponding cyclic transition event o_4 in G_2^m.

4. Related Work and Comparison

Several works aimed at finding only the minimal diagnosis of DESs are based on either AI planning [43, 44] or SAT approaches [45]. Significantly, they require first to transform a diagnosis problem description into the corresponding knowledge representation, generally with the bottleneck of quickly solving planning or SAT problems for online diagnosis. However, we generate minimal diagnoses by minimal diagnoser only, which is the main advantage of our approach.

In addition, we compared our method with many other related approaches for diagnosis in different views:

(1) Minimal diagnosis of static systems vs. minimal diagnosis of DESs: Similarity: Like the minimal diagnosis of static systems [41, 42], the minimal diagnosis of DESs is also quite valuable.
   (a) First, a diagnosis with fewer faults is more probable than one with more faults
   (b) Second, some space is saved by a minimal diagnosis than corresponding superset diagnoses with very large sizes

   Difference: a superset diagnosis of the static system is still a diagnosis, but a superset may not be a diagnosis for a given observation sequence of a DES.

(2) Minimal diagnosis vs. diagnosis with probability:
   (a) Minimal diagnosis does not need probability information, which sometimes cannot present quite precise diagnoses.
   (b) Diagnosis with explicit fault probability based on Bayesian/probabilistic reasoning [32–35] can offer precise diagnoses in a mathematically rigorous way. However, the shortcomings of these approaches may be twofold.
      (i) First, the prior probability of each faulty event is required, which may be difficult to obtain in practice
      (ii) Second, adding the probability of each faulty event will possibly make the diagnosis process more complex

5. Conclusions

In this paper, to focus on the more likely diagnoses, a notion of minimal diagnosis of DESs is proposed, where only subset-minimal fault sets are considered as the most probable explanations for the given observation sequences. Then, the notion of a minimal diagnoser is proposed for the online minimal diagnosis of DESs. Moreover, two sorts of minimal diagnosability are presented for deciding whether a DES is strongly/weakly minimally diagnosable or not, along with necessary and sufficient conditions for testing the minimal diagnosability, which are based on the notion of a minimal diagnoser. Finally, the basic relationships among the three types of diagnosability (classical diagnosability and the two novel notions of minimal diagnosability) are presented.

However, since the generation of the minimal diagnoser requires the availability of the whole DES model, a problem of complexity may arise if the DES is large (which is normal for real, possibly distributed systems). To cope with this problem, as in previous approaches to developing decentralized diagnosers, a challenging goal for future research is the decentralization/distribution of minimal diagnoses.

The paper is conceived to provide a theoretical/formal foundation for the minimal diagnosis and minimal diagnosability of DESs. Unfortunately, as far as we know, although there are several real case studies on the diagnosis of DESs (e.g., the hydraulic circuit case [46]), there are still no widely used artificially well-designed or widely used real-application benchmarks for the diagnosis of DESs to be applied for testing the diagnosis approaches. Accordingly, practical applications are one interesting subject for future research as well as an effective/efficient algorithm for constructing a minimal diagnoser of a DES with a sound space complexity.

A polynomial "twin-plant" approach has been proposed in [47, 48] for efficiently testing the diagnosability of DESs. Designing similar polynomial approaches to check the minimal diagnosability of DESs is also an interesting future topic.

Still, a number of important issues must be considered in future research. An essential assumption of this paper is the independence of faults. Although this may be reasonable in a wide variety of contexts, the question remains: how will the notion of the minimal diagnosis of DESs change when fault dependence actually occurs? Another challenging task is the injection of minimal diagnosis into other approaches for the diagnosis of DESs, including those that do not require the generation of a diagnoser (which may be impractical in real-application domains), such as the diagnosis of active systems [21]. Like our model-based distributed minimal diagnosis of static systems [49] or the decentralized/distributed diagnosis of DESs [27–29, 50], the decentralized/distributed minimal diagnosis of DESs is also an interesting and challenging topic. Eventually, only the application of minimal diagnosis to real DESs will provide evidence of its practical utility.

Appendix

Proofs for Properties, Lemmas, and Propositions

Properties of minimal diagnoser G^m:

(P_1) Let $q_i^m \in Q^m$. For each $(q_i^o, l_i) \in q_i^m$, there is at least a state $q_i^d \in Q^d$ in G^d such that $(q_i^o, l_i) \in q_i^d$.

(P_2) Let $q^m \in Q^m$. If $(q^o, l), (q^{o'}, l') \in q^m$, then there exist s, $s' \in L$ with $s_e, s_e' \in \Sigma_o$ such that $T(q_0, s) = q^o$, $T(q_0, s') = q^{o'}$, $\mathrm{Prj}_{\Sigma_o}(s) = \mathrm{Prj}_{\Sigma_o}(s')$, $P_{\Sigma_f}(s) = l$, $P_{\Sigma_f}(s') = l'$, and either $l = l'$ or $l \prec\succ l'$.

(P_3) Let $q^m \in Q^m$. There may exist $(q^o, l), (q^o, l') \in q^m$, that is, the system might reach the same observable state q^o while having different minimal fault labels ($l \neq l'$).

(P_4) For each $q^m \in Q^m$ and for each (q^o, l), $(q^{o'}, l') \in q^m$, we have

(i) $l = l' \Longleftrightarrow l \subseteq l'$
(ii) $l \neq l' \Longleftrightarrow l \prec\succ l'$

(P_5) Let $\left(q_i^m \xrightarrow{\sigma} q_j^m\right) \in T^m$. For each $(q_j^o, l_j) \in q_j^m$, there exists $(q_i^o, l_i) \in q_i^m$ such that $l_i \subseteq l_j$.

Proof.

(P_1) According to case (1) of the definition (Definition 4) of a minimal diagnoser, for each $q_i^d \in Q^d$, there exists a state $q_i^m \in Q^m$ with $(q^o, l) \in q_i^d$, with l being the minimal fault label in q_i^d. On the contrary, for each $q_i^m \in Q^m$, we can apply a backforward process to G^d to find at least a state q_i^d with $(q^o, l_i) \in q_i^d$, as well as for any other $(q^{o'}, l_i') \in q_i^d$ (if they exist), such that $l_i \prec l_i'$.

(P_2) According to the definitions of the revised diagnoser (especially the two functions S and T^d) and the minimal diagnoser, for $(q^o, l), (q^{o'}, l') \in q^m$, we can find two corresponding traces $s, s' \in L$, with $s_e, s_e' \in \Sigma_o$, such that $T(q_0, s) = q^o$ (i.e., to reach the observable state q^o), $T(q_0, s') = q^{o'}$, $\mathrm{Prj}_{\Sigma_o}(s) = \mathrm{Prj}_{\Sigma_o}(s')$ (since s and s' reach the same state q^m, they may have the same observation sequence), and $P_{\Sigma_f}(s) = l$ and $P_{\Sigma_f}(s') = l'$. Because q^o may equal $q^{o'}$, then $l = l'$ may hold; otherwise, $l \not\subset l'$ and $l' \not\subset l$ (i.e., $l \prec\succ l'$). If, for example, $l \subset l'$, then l' will not be a minimal diagnosis. Hence we get the conclusion.

(P_3) As in (P_2), when $q^o = q^{o'}$, i.e., s and s' reach the same observable state, but with $l = P_{\Sigma_f}(s) \neq P_{\Sigma_f}(s') = l'$ and $l \prec\succ l'$, then $l \neq l'$.

(P_4) Because q^m is a minimal state, any two fault labels l and l' in q^m are minimal. Then,

(a) If $l \subseteq l'$, then $l = l'$, since otherwise, if, for instance, $l \subseteq l'$ but $l \neq l'$, then $l \subset l'$, that is, l is the minimal fault set. However, l' is not, which contradicts the idea that l' is in q^m. On the contrary, if $l = l'$, then obviously $l \subseteq l'$. Thus, $l = l' \Longleftrightarrow l \subseteq l'$ holds.
(b) If $l \neq l'$, then suppose that $l \subset l'$ or $l' \subset l$. In the former case, l' is not minimal, which contradicts the idea that l' is in q^m; in the latter case, l is not minimal, which also contradicts the idea that l is in q^m. Thus, $l \prec\succ l'$ holds. On the contrary, if $l \prec\succ l'$, then according to the definition of $\prec\succ$, obviously $l \neq l'$. Therefore, $l \neq l' \Longleftrightarrow l \prec\succ l'$ holds.

(P_5) According to the method for the propagation of labels using T^d (i.e., case (2) of the definition of T^d, where $l' = l \cup \{f_i \mid f_i \in u\}$), l' in the next state is a superset of the label l in the previous state. Accordingly, l_j in q_j^m is a superset of the label l_i in the previous state q_i^m. Thus, $l_i \subseteq l_j$ holds. □

Lemma A.1. *For the minimal diagnoser G^m of DES G, the following properties hold:*

(i) Let $T^m(q_0^m, s) = q^m$, $s \in \Sigma_o^*$. If state q^m with fault label l is F-certain, then for each $\omega \in Prj_{\Sigma_o}^{-1}(s)$, we have $l \preccurlyeq P_{\Sigma_f}(\omega)$.

(ii) If a state $q^m \in Q^m$ is F-incomparable, then for any two pairs (q^o, l), $(q^{o'}, l') \in q^m$ with $l \neq l'$, there exist two strings $t, t' \in L$ with $t_e, t_e' \in \Sigma_o$ such that $T(q_0, t) = q^o$, $T(q_0, t') = q^{o'}$, $Prj_{\Sigma_o}(t) = Prj_{\Sigma_o}(t')$, $T^m(q_0^m, Prj_{\Sigma_o}(t)) = q^m$, $l = P_{\Sigma_f}(t)$, $l' = P_{\Sigma_f}(t')$, and $l \prec\succ l'$.

Proof.

(i) For property (i)

In the revised diagnoser G^d for DES G, consider any pair $(q^o, P_{\Sigma_f} \mid \omega)$ with $Q^d \in Q^d$ and $T^d(q_0, s) = Q^d$.

(a) On the one hand, if $(q^o, P_{\Sigma_f}(\omega))$, then either $l = P_{\Sigma_f}(\omega)$ or $l \prec\succ P_{\Sigma_f}(\omega)$ holds. However, if $l \prec\succ P_{\Sigma_f}(\omega)$ holds, that is, there exist at least two different fault labels in q^m, then it contradicts the idea that q^m is F-certain. Therefore, only $l = P_{\Sigma_f}(\omega)$ holds, which is also consistent with property (P_1) of a "minimal diagnoser".

(b) On the other hand, if $(q^o, P_{\Sigma_f}(\omega))$, according to the first condition in Definition 4, we obtain $l \prec P_{\Sigma_f}(\omega)$. In other words, $P_{\Sigma_f}(\omega)$ is not a minimal diagnosis for observation $\mathrm{Prj}_{\Sigma_o}(s)$.

Based on the above analysis, we have $l \prec P_{\Sigma_f}(\omega)$.

(b) For property (ii)

It is easy to draw a conclusion from property (P_2) of a "minimal diagnoser." □

Lemma A.2. *Assume that $q_1^m, q_2^m, \ldots, q_n^m \in Q^m$ are a set of F-incomparable states forming an F-indeterminate cycle, where*

$$\begin{aligned} q_i^m &= \left\{\left(q_{i_1}^o, l_{i_1}\right), \left(q_{i_2}^o, l_{i_2}\right), \ldots, \left(q_{i_{\mathrm{len}\_i}}^o, l_{i_{\mathrm{len}\_i}}\right)\right\}, \\ q_j^m &= \left\{\left(q_{j_1}^o, l_{j_1}\right), \left(q_{j_2}^o, l_{j_2}\right), \ldots, \left(q_{j_{\mathrm{len}\_j}}^o, l_{j_{\mathrm{len}\_j}}\right)\right\}, \end{aligned} \tag{A.1}$$

with $i, j \in [1 \cdots n]$ and len_i and len_j denotes the number of pairs in q_i^m and q_j^m, respectively. Then, we have

$$\left\{l_{i_1}, l_{i_2}, \ldots, l_{i_{\mathrm{len}\_i}}\right\} = \left\{l_{j_1}, l_{j_2}, \ldots, l_{j_{\mathrm{len}\_j}}\right\}. \tag{A.2}$$

Proof. For any two adjacent states q_i^m and $q_{(i+1)}^m$ in the F-indeterminate cycle, according to property (P_5) of a "minimal diagnoser," we have the following.

For any pair $(q^o_{(i+1)_{j_{(i+1)}}}, l_{(i+1)_{j_{(i+1)}}}) \in q^m_{(i+1)}$ $(1 \le j_{(i+1)} \le \mathrm{len}\_(i+1))$, there exists $(q_{i_{j_i}}, l_{i_{j_i}}) \in q_i^m$ such that $l_{i_{j_i}} \subseteq l_{(i+1)_{j_{(i+1)}}}$.

Then, we have

$$l_{1_{j_1}} \subseteq l_{2_{j_2}}, l_{2_{j_2}} \subseteq l_{3_{j_3}}, \ldots, l_{(n-1)_{j_{(n-1)}}} \subseteq l_{n_{j_n}}, \tag{A.3}$$

and then we obtain

$$l_{1_{j_1}} \subseteq l_{2_{j_2}} \subseteq \cdots \subseteq l_{(n-1)_{j_{(n-1)}}} \subseteq l_{n_{j_n}}. \tag{A.4}$$

Because $q_1^m, q_2^m, \ldots, q_n^m$ form a cycle, then for a pair $(q_{1_{j_1}}, l_{1_{j_1}}) \in q_1^m$, according to property (P_5) of a "minimal diagnoser," there exists a pair $(q_{n_{k_n}}, l_{n_{k_n}}) \in q_n^m$ such that

$$l_{n_{k_n}} \subseteq l_{1_{j_1}}. \tag{A.5}$$

From formula (A.4), we obtain

$$l_{1_{j_1}} \subseteq l_{n_{j_n}}. \tag{A.6}$$

From formulas (A.5) and (A.6), we obtain

$$l_{n_{k_n}} \subseteq l_{n_{j_n}}. \tag{A.7}$$

From property (P_4) of a "minimal diagnoser," we have

$$l_{n_{k_n}} = l_{n_{j_n}}. \tag{A.8}$$

From formulas (A.5), (A.6), and (A.8), we obtain

$$l_{1_{j_1}} = l_{n_{j_n}}. \tag{A.9}$$

From formulas (A.4) and (A.8), we obtain

$$l_{1_{j_1}} = l_{2_{j_2}} = \cdots = l_{n_{j_n}}. \tag{A.10}$$

That is, for any pair with label l_i in any state q_i^m, there exists the same label in each of the other states. Therefore, we have the following conclusion:

$$\left\{l_{i_1}, l_{i_2}, \ldots, l_{i_{\mathrm{len}\_i}}\right\} = \left\{l_{j_1}, l_{j_2}, \ldots, l_{j_{\mathrm{len}\_j}}\right\}. \tag{A.11}$$

□

Lemma A.3. *Given a prefix-closed language L, if $F \rightsquigarrow_{\min} Prj_{\Sigma_o}(s)$ holds for a fault set $F \in \mathcal{F}_L$ and a string $s \in L$ with $s_e \in \Sigma_o$ and $P_{\Sigma_f}(s) = F$, then for any string $t \in L/s$ with $t_e \in \Sigma_o$ and $P_{\Sigma_f}(t) \subseteq F$, we have $F \rightsquigarrow_{\min} Prj_{\Sigma_o}(st)$.*

Proof. According to the definition of a "minimal diagnosis" (Definition 1 and Definition 3), to prove that $F \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(st)$, we have to prove the following two statements:

(i) $F \rightsquigarrow \mathrm{Prj}_{\Sigma_o}(st)$

(ii) $\nexists F'' \subseteq \Sigma_f$ such that $F'' \rightsquigarrow \mathrm{Prj}_{\Sigma_o}(st) \wedge F'' \prec F$

For the first statement, because $P_{\Sigma_f}(s) = F$ and $P_{\Sigma_f}(t) \subseteq F$, then $F = \mathrm{Prj}_{\Sigma_f}(st)$, that is, $F \rightsquigarrow \mathrm{Prj}_{\Sigma_o}(st)$.

For the second statement, by contradiction, assume that there exists $F'' \subseteq \Sigma_f$ such that $F'' \rightsquigarrow \mathrm{Prj}_{\Sigma_o}(st) \wedge F'' \prec F$ (i.e., $F'' \subset F$). That is, there exists a string $s'' \in L$ with $\mathrm{Prj}_{\Sigma_o}(s'') = \mathrm{Prj}_{\Sigma_o}(st)$ and $F'' = P_{\Sigma_f}(s'')$.

Let $s'' = s't'$ such that $s' \in S_F$, that is, $s'_e \in \Sigma_o \wedge \mathrm{Prj}_{\Sigma_o}(s') = \mathrm{Prj}_{\Sigma_o}(s)$.

Since $F \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(s)$, we have $F \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(s')$.

Then, we have two possible cases regarding the relations between F and $P_{\Sigma_f}(s')$:

(A) $F \precsim P_{\Sigma_f}(s')$ (also $F \subseteq P_{\Sigma_f}(s')$)

(B) $F \prec\succ P_{\Sigma_f}(s')$

For case (A), since $F \subseteq P_{\Sigma_f}(s') \subseteq P_{\Sigma_f}(s't') = P_{\Sigma_f}(s'') = F''$, we get $F \subseteq F''$, which contradicts the assumption that $F'' \subset F$.

For case (B), from $F \prec\succ P_{\Sigma_f}(s')$, we get $P_{\Sigma_f}(s') \notin F$, and then $P_{\Sigma_f}(s't') \notin F$, that is, $P_{\Sigma_f}(s'') \notin F$; thus, we get $F'' \notin F$, which also contradicts the assumption that $F'' \subset F$.

Therefore, the second statement also holds.

Hence, we get the conclusion. □

Lemma A.4. *Given a prefix-closed language L, $F \rightsquigarrow_{\min} Prj_{\Sigma_o}(s)$ holds for a fault set $F \in \mathcal{F}_L$ and a string $s \in L$ with $s_e \in \Sigma_o$ and $P_{\Sigma_f}(s) = F$. If F is the unique minimal diagnosis for observation $Prj_{\Sigma_o}(s)$, i.e.,*

$$\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(s)\right) \Longrightarrow F \lesssim P_{\Sigma_f}(\omega), \tag{A.12}$$

then for each string $t \in L/s$ with $t_e \in \Sigma_o$, and the following holds:

$$\omega' \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(st)\right) \Longrightarrow F \lesssim P_{\Sigma_f}(\omega'). \tag{A.13}$$

Proof. For each $\omega' \in \mathrm{Prj}_{\Sigma_o}^{-1}(\mathrm{Prj}_{\Sigma_o}(st))$, we have $\mathrm{Prj}_{\Sigma_o}(\omega') = \mathrm{Prj}_{\Sigma_o}(st)$.

Let $\omega' = s't'$ with $\mathrm{Prj}_{\Sigma_o}(t') = \mathrm{Prj}_{\Sigma_o}(t)$ and $\mathrm{Prj}_{\Sigma_o}(s') = \mathrm{Prj}_{\Sigma_o}(s)$ with $s'_e \in \Sigma_o$; thus, $s' \in \mathrm{Prj}_{\Sigma_o}^{-1}(\mathrm{Prj}_{\Sigma_o}(s))$, and then $F \lesssim P_{\Sigma_f}(s')$ (i.e., $F \subseteq P_{\Sigma_f}(s')$).

Then, $F \subseteq P_{\Sigma_f}(s') \subseteq P_{\Sigma_f}(s't') = P_{\Sigma_f}(\omega')$; thus, we get $F \lesssim P_{\Sigma_f}(\omega')$.

Therefore, we obtain the following conclusion: $\omega' \in \mathrm{Prj}_{\Sigma_o}^{-1}(\mathrm{Prj}_{\Sigma_o}(st)) \Longrightarrow F \lesssim P_{\Sigma_f}(\omega')$. □

Proposition A.1. *A language L generated by an FSM G is strongly minimally diagnosable iff its minimal diagnoser G^m satisfies the following two conditions:*

(C_1) There is no F-indeterminate cycle in G^m

(C_2) For each F-incomparable state $q^m \in Q^m$ and for each pair $(q^o, l) \in q^m$, there exist a state $q^{m'} \in Q^m$ and a nonempty observation sequence $s_o \in \Sigma_o^+$ such that $T^m(q^m, s_o) = q^{m'}$, and for each pair $(q^{o'}, l')$, we have $l' = l$, that is, $q^{m'}$ (after q^m) is an F-certain state with the unique minimal fault label l.

Proof. Necessity: firstly, we prove that if L is strongly minimally diagnosable, then it satisfies condition (C_1). By contradiction, assume there exist $q_1^m, q_2^m, \ldots, q_n^m \in Q^m$ such that they form an F-indeterminate cycle, and let $T^m(q_i^m, \sigma_i) = q_{(i+1) \bmod n}^m$, $\sigma_i \in \Sigma_o$. According to Lemma A.2, let $q_i^m = \{(q_{i_1}^{o_1}, l_{i_1}^1), (q_{i_1}^{o_2}, l_{i_1}^2), \ldots, (q_{i_1}^{o_{\mathrm{len}-i_1}}, l_{i_1}^{\mathrm{len}-i_1}), \ldots, (q_{i_k}^{o_1}, l_{i_k}^1), (q_{i_k}^{o_2}, l_{i_k}^2), \ldots, (q_{i_k}^{o_{\mathrm{len}-i_k}}, l_{i_k}^{\mathrm{len}-i_k})\}$, $(1 \le i \le n)$, where k is the number of different fault labels in q_i^m, and

$$\begin{aligned} &l_{i_j}^1 = l_{i_j}^2 = \cdots = l_{i_j}^{\mathrm{len}-i_j} \ (1 \le j \le k), \\ &l_{i_r}^1 \prec\succ l_{i_s}^1 \ (1 \le r, s \le k, r \ne s), \\ &l_{x_j}^1 = l_{y_j}^1 \ (1 \le x, y \le n, 1 \le j \le k). \end{aligned} \tag{A.14}$$

For any two pairs $(q_{1_j}^{o_1}, l_{1_j}^1), (q_{1_m}^{o_1}, l_{1_m}^1) \in q_1^m$ $(1 \le j, m \le k)$ with $l_{1_j}^1 \prec\succ l_{1_m}^1$, since q_1^m is F-incomparable, according to Lemma A.1-(ii), there exist two strings $s, s' \in L$ with $s_e, s'_e \in \Sigma_o$ such that $l_{1_j}^1 = P_{\Sigma_f}(s)$, $l_{1_m}^1 = P_{\Sigma_f}(s')$, $T(q_0, s) = q_{1_j}^{o_1}$, $T(q_0, s') = q_{1_m}^{o_1}$, and $T^m(q_0^m, \mathrm{Prj}_{\Sigma_o}(s)) = q_1^m$. Then, $l_{1_j}^1 \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(s)$ and $l_{1_m}^1 \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(s')$.

Consider the following two traces:

$$\begin{aligned} \omega &= s\left(s_1\sigma_1 s_2\sigma_2 \cdots s_z\sigma_z\right)^p; \\ \omega' &= s'\left(s'_1\sigma_1 s'_2\sigma_2 \cdots s'_z\sigma_z\right)^p; \end{aligned} \tag{A.15}$$

with $p \in \mathbb{N}$ and $p \ge 1$ being arbitrarily large, $s_q, s'_q \in \Sigma_{uo}^*$, and $\sigma_q \in \Sigma_o$ $(q = [1 \cdots z])$.

Let $P_{\Sigma_f}(s_q) \subseteq l_{1_j}^1$ and $P_{\Sigma_f}(s'_q) \subseteq l_{1_m}^1$ for each q $(q \in [1 \cdots z])$. Then, we have

$$\begin{aligned} \mathrm{Prj}_{\Sigma_o}(\omega) &= \mathrm{Prj}_{\Sigma_o}(\omega'), \\ P_{\Sigma_f}(\omega) &= l_{1_j}^1, \\ P_{\Sigma_f}(\omega') &= l_{1_m}^1. \end{aligned} \tag{A.16}$$

Let $F = l_{1_j}^1$ and $t \in L/s$ such that $\omega = st$; then, $t = (s_1\sigma_1 s_2\sigma_2 \cdots s_z\sigma_z)^p$, $t_e \in \Sigma_o$, and $P_{\Sigma_f}(t) \subseteq F$. By choosing p to be arbitrarily large, we can obtain $\|t\| \ge n$ for any given $n \in \mathbb{N}$, and then we have: $\omega' \in \mathrm{Prj}_{\Sigma_o}^{-1}(\mathrm{Prj}_{\Sigma_o}(st))$ and $l_{1_j}^1 \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(st)$ (according to Lemma A. $3 l_{1_j}^1 \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(s)$, $l_{1_j}^1 = P_{\Sigma_f}(s)$, and $P_{\Sigma_f}(t) \subseteq l_{1_j}^1$.) but $l_{1_j}^1 \not\lesssim P_{\Sigma_f}(\omega') = l_{1_m}^1$ (because $l_{1_j}^1 \prec\succ l_{1_m}^1$), which contradicts condition D_m^2 of the definition of a "strong minimal diagnosability" (Definition 5).

Thus, for two such traces, according to Definition 5, L is not strongly minimally diagnosable.

Therefore, condition (C_1) must be satisfied.

Then, we prove that if L is strongly minimally diagnosable, then it satisfies condition (C_2). By contradiction, assume that there exists an F-incomparable state $q^m \in Q^m$ and that there also exists a pair $(q^o, l) \in q^m$ but there does not exist a state $q^{m'} \in Q^m$ such that $T^m(q^m, s_o) = q^{m'}$ (where $s_o \in \Sigma_o^+$), and for each $(q^{o'}, l') \in q^{m'}$, $l' = l$. Then, for each $q^{m'}$, there exist only two possible distinct cases:

(1) For each $(q^{o'}, l') \in q^{m'}$, $l' \ne l$

(2) There exist $(q_1^{o'}, l_1')$, $(q_2^{o'}, l_2') \in q^{m'}$ such that $l_1' = l$ and $l_2' \ne l$

For case (1), because $(q^o, l) \in q^m$, according to property (P_2) of a "minimal diagnoser," there exists $s' \in \Sigma^*$ with $s'_e \in \Sigma_o$ such that $T(q_0, s') = q^o$ and $P_{\Sigma_f}(s') = l$.

Let $s' = st$ with $s_e \in \Sigma_f$, $P_{\Sigma_f}(s) = l$ (i.e., $s \in s_l$), $t_e = s'_e \in \Sigma_o$, and $P_{\Sigma_f}(t) = \varnothing$ $(\subseteq l)$.

Then, for condition (i) of Definition 5, we cannot find a trace $t' \in L/(st)$, $(tt')_e \in \Sigma_o$, and $P_{\Sigma_f}(t') \subseteq l$ such that $(l \rightsquigarrow_{min} \mathrm{Prj}_{\Sigma_o}(st)) \Longrightarrow D_m^1$.

By contradiction, assume that there exist $t' \in L/(st)$, $(tt')_e \in \Sigma_o$, and $P_{\Sigma_f}(t') \subseteq l$ (then, according to Lemma A.3, $l \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(s't'))$. Let $s_o = \mathrm{Prj}_{\Sigma_o}(t')$ and $T^m(q^m, s_o) = q^{m'}$; then, there must exist a pair $(q^{o'}, l') \in q^{m'}$ with $l' = l$ (because $l \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(s't'))$, which contradicts case (1), in which $\forall (q^{o'}, l') \in q^{m'}, l' \ne l$. Even if s_o (i.e., $\mathrm{Prj}_{\Sigma_o}(t')$) is ε, the condition D_m^1 of Definition 5 will not be satisfied, or else q^m will be F-certain with the unique fault label l, which contradicts the assumption that q^m is F-incomparable.

For case (2), as in case (1), there also exists $s' \in \Sigma^*$ with $s'_e \in \Sigma_o$ such that $T(q_0, s') = q^o$ and $P_{\Sigma_f}(s') = l$.

Let $s' = st$ with $s_e \in \Sigma_f$, $P_{\Sigma_f}(s) = l$ (i.e., $s \in S_l$), $t_e = s'_e \in \Sigma_o$, and $P_{\Sigma_f}(t) = \varnothing$ $(\subseteq l)$.

For each $t' \in L/(st)$ with $P_{\Sigma_f}(t') \subseteq l$ (and subsequently $P_{\Sigma_f}(stt') \subseteq l$) and $\mathrm{Prj}_{\Sigma_o}(t') = s_o$, according to Case (2), we have $T(q_0, stt') = q_1^{o'}$, $l_1'(= l) \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(stt')$, and $l_2' \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(stt')$, but $l_1' \not\prec\succ l_2'$, which contradicts the definition of a "strong minimal diagnosability" (condition D_m^1). Even if s_o (i.e., $\mathrm{Prj}_{\Sigma_o}(t')$) is ε, as in case (1), condition D_m^1 of Definition 5 is not satisfied.

Therefore, condition (C_2) must be satisfied.

Sufficiency: assume that the minimal diagnoser G^m satisfies conditions (C_1) and (C_2). For any fault set $F \in \mathscr{F}_L$, pick any $s \in L$ with $s \in S_F$. Pick any $t \in L/s$ with $t_e \in \Sigma_o$ (based on the assumption that there is no infinite sequence of unobservable events in L, we let a natural number n_0 denote the maximum length of any sequence of unobservable events; thus, $t \leq (n_0 + 1)$).

Let $T(q_0, st) = q_i^o$, and then we get the corresponding state $q_j^m = T^m(q_0^m, \mathrm{Prj}_{\Sigma_o}(st))$ in G^m. Since $P_{\Sigma_f}(st) = F$, according to the conditions of Definition 5, we suppose that $F \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(st)$, and then we get $(q_i^o, F) \in q_j^m$. Then, we have two distinct cases to consider:

(a) q_j^m is F-certain

(b) q_j^m is F-incomparable

For case (a), in which q_j^m is F-certain, according to Lemma A.1-(i), we have

$$\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(st)\right) \Longrightarrow F \lesssim P_{\Sigma_f}(\omega). \tag{A.17}$$

Thus, there exists $t' = \varepsilon$ such that $t' \in L/(st)$, $(tt')_e \in \Sigma_o$ (because $tt' = t$ and $t_e \in \Sigma_o$), and $P_{\Sigma_f}(t') \subseteq F$. If $F \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(st)$, then D_m^1 of Definition 5 holds:

$$\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(stt')\right) \Longrightarrow F \lesssim P_{\Sigma_f}(\omega). \tag{A.18}$$

Thus, the first condition (i) of Definition 5 holds $(F \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(st)) \Longrightarrow D_m^1$.

According to Lemma A.4, for each $t'' \in L/(st)$ with $t_e'' \in \Sigma_o$,

$$\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(stt'')\right) \Longrightarrow F \lesssim P_{\Sigma_f}(\omega). \tag{A.19}$$

Then, for the second condition (ii) of Definition 5, let $n = t$; for each string u with $u \in L/s$ and $u_e \in \Sigma_o$, when $u \geq n$, we have the following:

If $F \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(su)$, then

$$\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(su)\right) \Longrightarrow F \lesssim P_{\Sigma_f}(\omega), \quad \left(\text{i.e., } D_m^2 \text{ holds}\right). \tag{A.20}$$

Thus, the second condition (ii) of Definition 5 holds.

For case (a), since the conclusion is true for any $F \in \mathscr{F}_L$, L is strongly minimally diagnosable.

For case (b), if q_j^m is F-incomparable, according to condition (C_1) (there is no F-indeterminate cycle), there must exist $m \in \mathbb{N}$ and $r \in \Sigma_o^+$. When $r \geq m$, the diagnoser will reach the first F-certain state $q_j^{m'}$ with the unique fault label F' via observation sequence r only in two possible distinct scenarios:

(b1) $F \subset F'$ for each $(q_i^{o'}, F') \in q_j^{m'}$

(b2) $F = F'$ for each $(q_i^{o'}, F') \in q_j^{m'}$

For scenario (b1), because F is no longer a minimal diagnosis, we do not care about this scenario.

Scenario (b2) is just condition (C2). According to (C2), there exists $s_o \in \Sigma_o^+$ such that $T^m(q_j^m, s_o) = q_j^{m'}$; then, there exists $t' \in L/(st)$ with $\mathrm{Prj}_{\Sigma_o}(t') = s_o$, $P_{\Sigma_f}(t') \subseteq F$, and $t_e' \in \Sigma_o$ (also $(tt')_e \in \Sigma_o$) such that $T(q_0, stt') = q_i^{o'}$ and $(q_i^{o'}, F) \in q_j^{m'}$. By Lemma A.1-(i), we have

$$\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(stt')\right) \Longrightarrow F \lesssim P_{\Sigma_f}(\omega). \tag{A.21}$$

That is, D_m^1 of Definition 5 holds.

Thus, the first condition (i) of Definition 5 holds.

For any $t'' \in L/(stt')$ with $t_e'' \in \Sigma_o$, according to Lemma A.4, we have

$$\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(stt't'')\right) \Longrightarrow F \lesssim P_{\Sigma_f}(\omega). \tag{A.22}$$

In other words, $\exists n = tt'$, $\forall u (u \in L/s, u_e \in \Sigma_o)$. When $u \geq n$, we have the following. If $F \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(su)$, then

$$\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(su)\right) \Longrightarrow F \lesssim P_{\Sigma_f}(\omega). \tag{A.23}$$

That is, the second condition (ii) of Definition 5 holds.

Hence, L is strongly minimally diagnosable. □

Proposition 3.18. *Let G be a DES with language L. If L is strongly minimally diagnosable, then L is also weakly minimally diagnosable. If L is diagnosable, then L is also weakly minimally diagnosable.*

Proof.

(1) From the second condition (ii) of Definition 5 ("strong minimal diagnosability") and the condition of Definition 8 ("weak minimal diagnosability"), we can clearly see that the former condition is just the latter one. Therefore, if G is strongly minimally diagnosable, then G is necessarily weakly minimally diagnosable.

(2) Let a DES G with language L be diagnosable. Pick any fault set $F \in \mathscr{F}_L$, with $F = \{f_1, f_2, \ldots, f_p\}$. According to Definition 2, for each $f_i \in F$ and for each $s \in L, s_e = f_i$, there exists $n \in \mathbb{N}$ such that

$$\forall t \left(t \in L/s, t_e \in \Sigma_o\right), \quad (\|t\| \geq n \Longrightarrow D), \tag{A.24}$$

where the diagnosability condition D is defined as follows:

$$\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(st)\right) \Longrightarrow f_i \in \omega. \tag{A.25}$$

Hence,

$$\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(st)\right) \Longrightarrow f_i \in \omega \Longrightarrow f_i \in P_{\Sigma_f}(\omega). \tag{A.26}$$

Thus, we obtain

$$\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(st)\right) \Longrightarrow F \subseteq P_{\Sigma_f}(\omega) \Longrightarrow F \lesssim P_{\Sigma_f}(\omega). \tag{A.27}$$

Thus,

$$\left(F \rightsquigarrow_{\min} \mathrm{Prj}_{\Sigma_o}(st)\right) \Longrightarrow \left(\omega \in \mathrm{Prj}_{\Sigma_o}^{-1}\left(\mathrm{Prj}_{\Sigma_o}(st)\right) \Longrightarrow F \lesssim P_{\Sigma_f}(\omega)\right). \tag{A.28}$$

Therefore, if G is diagnosable, then G is also weakly minimally diagnosable. □

Proposition 3.20. *A language L generated by an FSM G is weakly minimally diagnosable iff its minimal diagnoser G^m does not include any F-indeterminate cycle.*

Proof. (sketch)Based on the proof of Proposition 3.15, we can see that condition (C_1) is only required by the second case (ii) of "strong minimal diagnosability" (Definition 5), which is the same as "weak minimal diagnosability" (Definition 8). Therefore, only condition (C_1) of Proposition 3.15 is required for the current proposition. That is, a language L generated by an FSM G is weakly minimally diagnosable iff its minimal diagnoser G^m does not include any F-indeterminate cycle. □

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant no. 61972360).

References

[1] F. Yu, L. Li, B. He et al., "Design and FPGA implementation of a pseudorandom number generator based on a four-wing memristive hyperchaotic system and bernoulli map," *IEEE Access*, vol. 7, pp. 181884–181898, 2019.

[2] L. Zhou, F. Tan, and F. Yu, "A robust synchronization-based chaotic secure communication scheme with double-layered and multiple hybrid networks," *IEEE Systems Journal*, pp. 1–12, 2019.

[3] X. Yang, Q. Zhu, and C. Huang, "Lag stochastic synchronization of chaotic mixed time-delayed neural networks with uncertain parameters or perturbations," *Neurocomputing*, vol. 74, no. 10, pp. 1617–1625, 2011.

[4] J. Jin, L. Zhao, M. Li, F. Yu, and Z. Xi, "Improved zeroing neural networks for finite time solving nonlinear equations," *Neural Computing and Applications*, pp. 1–10, 2019.

[5] Q. Xie, X. Wang, Z. Han, Y. Zuo, and M. Tang, "Immersion and invariance control of a class of nonlinear cascaded discrete systems," *Neurocomputing*, vol. 171, pp. 1661–1665, 2016.

[6] Y.-S. Huang and Z.-Y. Wang, "Decentralized adaptive fuzzy control for a class of large-scale MIMO nonlinear systems with strong interconnection and its application to automated highway systems," *Information Sciences*, vol. 274, no. 8, pp. 210–224, 2014.

[7] Y.-S. Huang and M. Wu, "Robust decentralized direct adaptive output feedback fuzzy control for a class of large-sale nonaffine nonlinear systems," *Information Sciences*, vol. 181, no. 11, pp. 2392–2404, 2011.

[8] M. Long, Y. Chen, and F. Peng, "Simple and accurate analysis of BER performance for DCSK chaotic communication," *IEEE Communications Letters*, vol. 15, no. 11, pp. 1175–1177, 2011.

[9] L. Zhou, F. Tan, F. Yu, and W. Liu, "Cluster synchronization of two-layer nonlinearly coupled multiplex networks with multi-links and time-delays," *Neurocomputing*, vol. 359, pp. 264–275, 2019b.

[10] F. Peng, X. W. Zhu, and M. Long, "An ROI privacy protection scheme for H.264 video based on FMO and chaos," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 10, pp. 1688–1699, 2013.

[11] F. Yu, L. Li, Q. Tang, S. Cai, Y. Song, and Q. Xu, "A survey on true random number generators based on chaos," *Discrete Dynamics in Nature and Society*, vol. 2019, Article ID 2545123, 10 pages, 2019.

[12] F. Yu, L. Liu, B. He et al., "Analysis and FPGA realization of a novel 5D hyperchaotic four-wing memristive system, active control synchronization, and secure communication application," *Complexity*, vol. 2019, Article ID 4047957, 18 pages, 2019.

[13] F. Yu, L. Liu, L. Xiao, K. Li, and S. Cai, "A robust and fixed-time zeroing neural dynamics for computing time-variant nonlinear equation using a novel nonlinear activation function," *Neurocomputing*, vol. 350, pp. 108–116, 2019.

[14] C. G. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2008.

[15] F. Lin, "Diagnosability of discrete event systems and its applications," *Discrete Event Dynamic Systems: Theory and Applications*, vol. 4, no. 2, pp. 197–212, 1994.

[16] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis, "Diagnosability of discrete-event systems," *IEEE Transactions on Automatic Control*, vol. 40, no. 9, pp. 1555–1575, 1995.

[17] X. Zhao and D. Ouyang, "Model-based diagnosis of discrete event systems with an incomplete system model," in *Proceedings of the 18th European Conference on Artificial Intelligence (ECAI-08)*, pp. 189–193, IOS Press, Patras, Greece, July 2008.

[18] R. H. Kwong and D. L. Yonge-Mallo, "Fault diagnosis in discrete-event systems with incomplete models: learnability and diagnosability," *IEEE Transactions on Cybernetics*, vol. 45, no. 7, pp. 1236–1249, 2015.

[19] S. Takai and R. Kumar, "A generalized framework for inference-based diagnosis of discrete event systems capturing both disjunctive and conjunctive decision-making," *IEEE Transactions on Automatic Control*, vol. 62, no. 6, pp. 2778–2793, 2017.

[20] X. Yin, J. Chen, Z. Li, and S. Li, "Robust fault diagnosis of stochastic discrete event systems," *IEEE Transactions on Automatic Control*, vol. 64, no. 10, pp. 4237–4244, 2019.

[21] G. Lamperti, M. Zanella, and X. Zhao, *Introduction to Diagnosis of Active Systems*, Springer, Basel, Switzerland, 2018.

[22] N. Kanagawa and S. Takai, "Diagnosability of discrete event systems subject to permanent sensor failures," *International Journal of Control*, vol. 88, no. 12, pp. 2598–2610, 2015.

[23] C. Keroglou and C. N. Hadjicostis, "Distributed fault diagnosis in discrete event systems via set intersection refinements," *IEEE Transactions on Automatic Control*, vol. 63, no. 10, pp. 3601–3607, 2018.

[24] F. Liu, "Predictability of failure event occurrences in decentralized discrete-event systems and polynomial-time verification," *IEEE Transactions on Automation Science and Engineering*, vol. 16, no. 1, pp. 498–504, 2019.

[25] G. S. Viana, M. V. Moreira, and J. C. Basilio, "Codiagnosability analysis of discrete-event systems modeled by weighted automata," *IEEE Transactions on Automatic Control*, vol. 64, no. 10, pp. 4361–4368, 2019.

[26] G. Zhu, Z. Li, and N. Wu, "Model-based fault identification of discrete event systems using partially observed petri nets," *Automatica*, vol. 96, pp. 201–212, 2018.

[27] R. Debouk, S. Lafortune, and D. Teneketzis, "On the effect of communication delays in failure diagnosis of decentralized

discrete event systems," *Discrete Event Dynamic Systems*, vol. 13, no. 3, pp. 263–289, 2003.

[28] Y. Pencolé and M.-O. Cordier, "A formal framework for the decentralised diagnosis of large scale discrete event systems and its application to telecommunication networks," *Artificial Intelligence*, vol. 164, no. 1-2, pp. 121–170, 2005.

[29] W. Qiu and R. Kumar, "Decentralized failure diagnosis of discrete event systems," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 36, no. 2, pp. 384–395, 2006.

[30] F. Liu and D. Qiu, "Diagnosability of fuzzy discrete-event systems: a fuzzy approach," *IEEE Transactions on Fuzzy Systems*, vol. 17, no. 2, pp. 372–384, 2009.

[31] M. Luo, Y. Li, F. Sun, and H. Liu, "A new algorithm for testing diagnosability of fuzzy discrete event systems," *Information Sciences*, vol. 185, no. 1, pp. 100–113, 2012.

[32] D. Thorsley and D. Teneketzis, "Diagnosability of stochastic discrete-event systems," *IEEE Transactions on Automatic Control*, vol. 50, no. 4, pp. 476–492, 2005.

[33] J. Chen and R. Kumar, "Failure detection framework for stochastic discrete event systems with guaranteed error bounds," *IEEE Transactions on Automatic Control*, vol. 60, no. 6, pp. 1542–1553, 2015.

[34] J. Chen, C. Keroglou, C. N. Hadjicostis, and R. Kumar, "Revised test for stochastic diagnosability of discrete-event systems," *IEEE Transactions on Automation Science and Engineering*, vol. 15, no. 1, pp. 404–408, 2018.

[35] X. Geng, D. Ouyang, X. Zhao, and S. Hao, "Probabilistic logical approach for testing diagnosability of stochastic discrete event systems," *Engineering Applications of Artificial Intelligence*, vol. 53, pp. 53–61, 2016.

[36] G. Lamperti and M. Zanella, "Flexible diagnosis of discrete-event systems by similarity-based reasoning techniques," *Artificial Intelligence*, vol. 170, no. 3, pp. 232–297, 2006.

[37] G. Lamperti and X. Zhao, "Diagnosis of active systems by semantic patterns," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 44, no. 8, pp. 1028–1043, 2014.

[38] A. Grastien, P. Haslum, and S. Thiébaux, "Conflict-based diagnosis of discrete event systems: theory and practice," in *Proceedings of the 13th International Conference on the Principles of Knowledge Representation and Reasoning (KR-12)*, pp. 489–499, AAAI Press, Rome, Italy, June 2012.

[39] X. Zhao, G. Lamperti, and D. Ouyang, "Minimal diagnosis of discrete-event systems," in *Proceedings of the 24th International Workshop on Principles of Diagnosis (DX-13)*, pp. 154–159, Jerusalem, Israel, October 2013.

[40] Wikipedia, "Occam's razor," 2016, https://en.wikipedia.org/wiki/Occam%27s_razor.

[41] R. Reiter, "A theory of diagnosis from first principles," *Artificial Intelligence*, vol. 32, no. 1, pp. 57–95, 1987.

[42] J. de Kleer and B. C. Williams, "Diagnosing multiple faults," *Artificial Intelligence*, vol. 32, no. 1, pp. 97–130, 1987.

[43] S. Sohrabi, J. Baier, and S. McIlraith, "Diagnosis as planning revisited," in *Proceedings of the 12th International Conference on the Principles of Knowledge Representation and Reasoning (KR-10)*, pp. 26–36, AAAI Press, Toronto, Canada, May 2010.

[44] P. Haslum and Al. Grastien, "Diagnosis as planning: two case studies," in *Proceedings of the 5th Scheduling and Planning Applications Workshop (SPARK-11)*, pp. 37–44, Cambridge, UK, December 2011.

[45] A. Grastien, A. Anbulagan, J. Rintanen, and E. Kelareva, "Diagnosis of discrete-event systems using satisfiability algorithms," in *Proceedings of the 22nd AAAI Conference on Artificial Intelligence (AAAI-07)*, pp. 305–310, AAAI Press, Vancouver, Canada, July 2007.

[46] M. Cerrada, L. Ferarini, and A. Dedè, "Modular fault diagnosis using temporized analysis for a class of discrete event systems," in *Proceedings of the 12th IFAC Symposium on Large Scale Systems: Theory and Applications*, pp. 180–185, Villeneuve-d'Ascq, France, July 2010.

[47] S. Jiang, Z. Huang, V. Chandra, and R. Kumar, "A polynomial algorithm for testing diagnosability of discrete-event systems," *IEEE Transactions on Automatic Control*, vol. 46, no. 8, pp. 1318–1321, 2001.

[48] T.-S. Yoo and S. Lafortune, "Polynomial-time verification of diagnosability of partially observed discrete-event systems," *IEEE Transactions on Automatic Control*, vol. 47, no. 9, pp. 1491–1495, 2002.

[49] X. Zhao and D. Ouyang, "Deriving all minimal hitting sets based on join relation," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 7, pp. 1063–1076, 2015.

[50] R. Su and W. M. Wonham, "Global and local consistencies in distributed fault diagnosis for discrete-event systems," *IEEE Transactions on Automatic Control*, vol. 50, no. 12, pp. 1923–1935, 2005.