Verification of Robust Diagnosability for Partially Observed Discrete Event Systems

Shigemasa Takai

Abstract

In this paper, we study robust failure diagnosis of discrete event systems. Given a set of possible models, each of which has its own nonfailure specification, we consider the existence of a single diagnoser such that, for all possible models, it detects any occurrence of a failure within a uniformly bounded number of steps. We call such a diagnoser a robust diagnoser. We introduce a notion of robust diagnosability, and prove that it serves as a necessary and sufficient condition for the existence of a robust diagnoser. We then present an algorithm for verifying the robust diagnosability condition.

Key words: Discrete event system; Failure diagnosis; Robust diagnoser; Robust diagnosability.

1 Introduction

A language based framework for failure diagnosis of partially observed discrete event systems (DESs) was proposed by Sampath et al. (1995). In this framework, a failure is represented by the occurrence of an unobservable failure event, and the task of a diagnoser is to detect any occurrence of a failure event within a uniformly bounded number of steps. The diagnosability property introduced by Sampath et al. (1995) plays an important role in failure diagnosis. In Jiang et al. (2001) and Yoo and LaFortune (2002), polynomial algorithms for verifying diagnosability were developed. Qiu and Kumar (2006) studied decentralized failure diagnosis in a general case where a nonfailure specification language is specified, and a failure is modeled by violation of the specification language. A notion of codiagnosability was defined to characterize a class of diagnosable systems in the decentralized setting (Qiu and Kumar, 2006). Further, an algorithm for verifying co-diagnosability was developed by Qiu and Kumar (2006).

In some situations, a set of possible models, instead of a single model, is given for control/diagnosis of systems with multiple configurations such as flexible manufacturing systems. Robust supervisory control and failure diagnosis schemes where a single supervisor/diagnoser works for all possible models are useful for such situations (Lin, 1993; Bourdon et al., 2005; Saboori and Hashtrudi Zad, 2006). For example, it is expected that implementation and maintenance costs for supervisors/diagnosers may be reduced. In the context of supervisory control of DESs initiated by Ramadge and Wonham (1987), a robust supervisory control problem was formulated by Lin (1993). This problem requires synthesizing a single supervisor that achieves legal behavior for all possible models. The result of Lin (1993) has been extended by Takai (2000), Park and Lim (2002), Bourdon et al. (2005), and Saboori and Hashtrudi Zad (2006) in several ways. In particular, a problem of synthesizing a single supervisor that works for all possible models, each of which has its own control specification, has been studied in Bourdon et al. (2005), Saboori and Hashtrudi Zad (2006).

To the best of our knowledge, most prior work on failure diagnosis of DESs assumes that a single model of a system to be diagnosed is given. In this paper, we assume that a set of possible models, each of which has its own nonfailure specification, is given, as in Bourdon et al. (2005), Saboori and Hashtrudi Zad (2006), and consider a robust failure diagnosis problem. We first introduce a notion of diagnosability for a set of possible models, called robust diagnosability, with respect to a set of nonfailure specification languages, and compare it with the existing notion of diagnosability. We then prove that robust diagnosability is a necessary and sufficient condi-
A diagnoser for prefixes of strings in $L$ defined as $F$ or each $\alpha$ negation of $G$ describes nonfailure behavior of the system $\forall s \in \Sigma \star | \alpha(s) \in M(\sigma)$. Strings $s, s' \in L(G)$ are said to be indistinguishable (under $M$) if $M(s) = M(s')$. Further, for any language $K \subseteq \Sigma^*$, $M(K) \subseteq \Delta^*$ is defined as $M(K) = \{M(s) \in \Delta^* | s \in K\}$. Also, for any $\tau \in \Delta^*$, $M^{-1}(\tau) \subseteq \Sigma^*$ is defined as $M^{-1}(\tau) = \{s \in \Sigma^* | M(s) = \tau\}$. A diagnoser is formally defined as a function $D : \Delta^* \to \{0, 1\}$. If $D$ is certain that a failure has occurred, then it issues the decision “1”. Otherwise, the decision “0” is issued by $D$.

Let $K \subseteq L(G)$ be a nonempty closed sublanguage that describes nonfailure behavior of the system $G$. Failure behavior of $G$ is represented by the execution of a string in $L(G) - K$. A diagnoser $D : \Delta^* \to \{0, 1\}$ is required to satisfy the following condition:

$$\exists m \in N \forall s \in L(G) - K \exists t \in L(G)/s \exists M(\sigma) = M(s).$$

where $N$ is the set of all nonnegative integers. The condition C1) means that there exists $m \in N$ such that the occurrence of any failure is detected by $D$ within $m$ steps. Further, $D$ is required to issue the decision “1” only after the occurrence of a failure. That is, $D$ should also satisfy the following condition:

$$\forall s \in K \exists M(\sigma) \neq 1.$$  

The system $G$ is said to be diagnosable with respect to $K$ (Sampath et al., 1995; Qiu and Kumar 2006) if

$$\exists m \in N \forall s \in L(G) - K \exists t \in L(G)/s \exists M(\sigma) = M(s).$$

There exists a diagnoser $D$ satisfying C1) and C2) if and only if $G$ is diagnosable with respect to $K$.

### 3 Robust Diagnosability

In this section, we assume that we only know that an exact model of a system to be diagnosed belongs to a set of $n$ possible DES models $\{G_i \mid i \in I\}$ over a common event set $\Sigma$, where $I \equiv \{1, 2, \ldots, n\}$ is an index set. Each possible model $G_i (i \in I)$ has its own nonfailure behavior described by a nonempty closed sublanguage $K_i \subseteq L(G_i)$.

**Example 1** We consider a simple manufacturing line with two configurations C1 and C2 shown in Fig. 1 (a) and (b), respectively. The configuration C1 (respectively, C2) consists of two machines $M_A$ and $M_B$ (respectively,
The initial state is identified by \( \downarrow \) to a circle.) Automata models \( G_{B_1} \) and \( G_{B_2} \) of the buffers \( B_1 \) and \( B_2 \) are shown in Fig. 3 (a) and (b), respectively. For each configuration, we consider a nonfailure specification that the overflow and underflow of the buffer do not occur. We describe behaviors of the configurations \( C_1 \) and \( C_2 \) by the synchronous compositions \( C_1 = G_{M_A} \parallel G_{M_a} \) and \( C_2 = G_{M_B} \parallel G_{M_B} \), respectively. Also, the nonfailure specifications for \( C_1 \) and \( C_2 \) are modeled by \( G_{K_1} = G_{M_A} \parallel G_{M_a} \parallel G_{B_1} \) and \( G_{K_2} = G_{M_B} \parallel G_{M_B} \parallel G_{B_2} \), respectively. Note that, for example, a string \( a_1 b_1 a_1 b_1 \) is a nonfailure one of \( G_1 \) but it is a failure one of \( G_2 \). Thus, in this example, for each configuration, its own nonfailure specification language \( K_i (i \in \{1, 2\}) \) has to be specified.

We consider a problem of synthesizing a robust diagnoser \( D : \Delta^* \rightarrow \{0, 1\} \) satisfying the following two conditions:

C3. \( (\forall i \in I ) (\exists m_i \in N ) (\exists s \in L(G_i) - K_i ) (\forall t \in L(G_i)/s) \ [ |t| \geq m_i \lor s \in L_d(G_i) ] \Rightarrow D(M(st)) = 1 \),

C4. \( (\forall i \in I ) (\exists s \in K_i ) D(M(s)) \neq 1 \).

That is, a robust diagnoser satisfying C3 and C4 correctly detects the occurrence of any failure in any possible model. In order to characterize the existence of such a robust diagnoser, we introduce a notion of robust diagnosability.

**Definition 2** The set \( \{ G_i \mid i \in I \} \) of possible models is said to be robustly diagnosable with respect to a set of nonempty closed languages \( \{ K_i \subseteq L(G_i) \mid i \in I \} \) if

\[
(\forall i \in I ) (\exists m_i \in N ) (\exists s \in L(G_i) - K_i ) (\forall t \in L(G_i)/s) \ [ |t| \geq m_i \lor s \in L_d(G_i) ] \Rightarrow (\forall j \in I ) : M^{-1}M(st) \cap L(G_j) \subseteq L(G_j) - K_j).
\]

Robust diagnosability of \( \{ G_i \mid i \in I \} \) with respect to \( \{ K_i \subseteq L(G_i) \mid i \in I \} \) requires that, for each possible model \( G_i (i \in I) \), there exists a nonnegative integer \( m_i \in N \) such that, for any failure string \( s \in L(G_i) - K_i \) and any extension \( t \in L(G_i)/s \) with \( |t| \geq m_i \) or \( s \in L_d(G_i) \), any string \( u \in M^{-1}M(st) \cap L(G_j) \) indistinguishable from \( s \) in \( G_j \) is also a failure string in \( L(G_j) - K_j \) for all possible models \( G_j (j \in I) \). Note that, if \( j \neq i \), it is possible that the set \( M^{-1}M(st) \cap L(G_j) \) of indistinguishable strings is the empty set. On the other hand, diagnosability of \( G_i \) with respect to \( K_i \) only requires that strings indistinguishable from \( s \) in \( G_i \) be failure ones in \( L(G_i) - K_i \). Thus, the following proposition holds.

**Proposition 3** If the set \( \{ G_i \mid i \in I \} \) of possible models is robustly diagnosable with respect to a set of nonempty closed languages \( \{ K_i \subseteq L(G_i) \mid i \in I \} \), then, for each \( i \in I \), \( G_i \) is diagnosable with respect to \( K_i \).

As shown in Example 2 of Takai (2010), however, the converse relation of Proposition 3 does not hold in general.

We also compare robust diagnosability of \( \{ G_i \mid i \in I \} \) with diagnosability of an aggregated model \( G^* \) such that \( L(G^*) = \bigcup_{i \in I} L(G_i) \). The following proposition shows that robust diagnosability of \( \{ G_i \mid i \in I \} \) is stronger than diagnosability of \( G^* \).

**Proposition 4** Let \( G^* \) be an aggregated model such that \( L(G^*) = \bigcup_{i \in I} L(G_i) \). If the set \( \{ G_i \mid i \in I \} \) of possible models is robustly diagnosable with respect to a set of nonempty closed languages \( \{ K_i \subseteq L(G_i) \mid i \in I \} \), then the aggregated model \( G^* \) is diagnosable with respect to \( \bigcup_{i \in I} K_i \).

![Fig. 1. Two configurations C1 and C2 of the manufacturing line.](image1)

![Fig. 2. Automata models of the machines M_A, M_a, and M_B.](image2)

![Fig. 3. Automata models of the buffers B_1 and B_2.](image3)
PROOF. Suppose for contradiction that $G^*$ is not diagnostable with respect to $\bigcup_{i \in I} K_i$. Then, for any $m \in N$, there exist $s \in \Delta^*(G^*) - \bigcup_{i \in I} K_i$ and $t \in \Delta^*(G^*)/s$ such that

$$[[t] \geq m \vee st \in \Delta^*(G^*)]$$

$$\land M^{-1}M(st) \cap \Delta^*(G^*) \subseteq \Delta^*(G^*) - \bigcup_{i \in I} K_i.$$ 

Since $M^{-1}M(st) \cap \Delta^*(G^*) \subseteq \Delta^*(G^*) - \bigcup_{i \in I} K_i$, there exists $u \in \bigcup_{i \in I} K_i$ such that $M(st) = M(u)$. Also, since $st \in \Delta^*(G^*)$ and $u \in \bigcup_{i \in I} K_i$, there exist $i, j \in I$ such that $s \in L(G_i)$ and $u \in L(G_i) - K_j$. We have $s \in L(G_i) - K_i$, $t \in L(G_i)/s$, $[[t] \geq m \vee st \in \Delta^*(G_i)]$, and $M^{-1}M(st) \cap L(G_i) \subseteq L(G_i) - K_j$. This contradicts robust diagnosability of $\{G_i \mid i \in I\}$ with respect to $\{K_i \subseteq L(G_i) \mid i \in I\}$. \qed

However, the converse relation of Proposition 4 does not necessarily hold. The following proposition shows that if nonfailure behavior and deadlocking behavior are consistent among all possible models, that is, if a string is a nonfailure (respectively, deadlocking) string in some possible model, then it is also a nonfailure (respectively, deadlocking) string if it is feasible in other possible models, then robust diagnosability of $\{G_i \mid i \in I\}$ with respect to $\{K_i \subseteq L(G_i) \mid i \in I\}$ is equivalent to diagnosability of an aggregated model $G^*$ with respect to $\bigcup_{i \in I} K_i$.

**Proposition 5** Let $G^*$ be an aggregated model such that $L(G^*) = \bigcup_{i \in I} L(G_i)$. Assume that, for each $i \in I$, a nonempty closed language $K_i \subseteq L(G_i)$ is specified as $K_i = K \cap L(G_i)$ by a nonempty closed language $K \subseteq \Sigma^*$, and $L_d(G_i) = \Delta^*(G^*) \cap L(G_i)$. Then, the set $\{G_i \mid i \in I\}$ of possible models is robustly diagnosable with respect to $\{K_i \subseteq L(G_i) \mid i \in I\}$ if and only if the aggregated model $G^*$ is diagnosable with respect to $\bigcup_{i \in I} K_i$.

**PROOF.** By Proposition 4, it suffices to show that if $G^*$ is diagnosable with respect to $\bigcup_{i \in I} K_i$, then $\{G_i \mid i \in I\}$ is robustly diagnosable with respect to $\{K_i \subseteq L(G_i) \mid i \in I\}$. Since $G^*$ is diagnosable with respect to $\bigcup_{i \in I} K_i$, there exists $m \in N$ such that

$$(\forall s \in \Delta^*(G^*) - K^*)[[t] \geq m \vee st \in \Delta^*(G^*)]$$

$$\land M^{-1}M(st) \cap \Delta^*(G^*) \subseteq \Delta^*(G^*) - K^*,$$

where $K^* = \bigcup_{i \in I} K_i$.

For each $i \in I$, we consider $s \in L(G_i) - K_i$ and $t \in L(G_i)/s$ such that $[[t] \geq m \vee st \in \Delta^*(G_i)]$. Since $s \in L(G_i) - K_i$ and $K_j = K \cap L(G_j)$ for each $j \in I$, we have $s \in L(G_j) - K^*$. Also, since $L_d(G_j) = \Delta^*(G^*) \cap L(G_j)$ for each $j \in I$, if $st \in L_d(G_i)$ then $st \in L_d(G^*)$. Thus, we have $M^{-1}M(st) \cap \Delta^*(G^*) \subseteq \Delta^*(G^*) - K^*$. For any $j \in I$ and any $s_j \in M^{-1}M(st) \cap L(G_i) \subseteq M^{-1}M(st) \cap \Delta^*(G^*) \subseteq \Delta^*(G^*) - K^*$, we have $s_j \in L(G_j) - K^* \subseteq L(G_j) - K_j$. We can conclude that $\{G_i \mid i \in I\}$ is robustly diagnosable with respect to $\{K_i \subseteq L(G_i) \mid i \in I\}$. \qed

The following theorem shows that robust diagnosability characterizes the existence of a robust diagnoser satisfying C3) and C4).

**Theorem 6** There exists a robust diagnoser $D : \Delta^* \rightarrow \{0, 1\}$ satisfying the conditions C3) and C4) for a set of nonempty closed languages $\{K_i \subseteq L(G_i) \mid i \in I\}$ if and only if the set $\{G_i \mid i \in I\}$ of possible models is robustly diagnosable with respect to $\{K_i \subseteq L(G_i) \mid i \in I\}$.

**PROOF.** We first prove the sufficiency part. We consider a diagnoser $D : \Delta^* \rightarrow \{0, 1\}$ given as

$$D(\tau) = \begin{cases} 1, & \text{if } \forall i \in I : M^{-1}(\tau) \cap L(G_i) \subseteq L(G_i) - K_i \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

We show that this diagnoser $D$ satisfies C3). Consider any $i \in I$. Since $\{G_i \mid i \in I\}$ is robustly diagnosable with respect to $\{K_i \subseteq L(G_i) \mid i \in I\}$, there exists $m_i \in N$ such that

$$(\forall s \in L(G_i) - K_i)\, ([[\tau] \geq m_i \vee st \in L_d(G_i)]$$

$$\land \forall j \in I : M^{-1}M(st) \cap L(G_j) \subseteq L(G_j) - K_j).$$

For any $s \in L(G_i) - K_i$ and $t \in L(G_i)/s$ such that $[[\tau] \geq m_i \vee st \in L_d(G_i)]$, we have $M^{-1}M(st) \cap L(G_j) \subseteq L(G_j) - K_j$ for all $j \in I$, which implies together with (1) that $D(M(st)) = 1$. It remains to show that $D$ satisfies C4). For each $i \in I$ and each $s \in K_i$, since $s \in M^{-1}M(st) \cap L(G_i)$, we have $D(M(st)) = 0$. Thus, C4) holds.

We next prove the necessity part. Since $D$ satisfies C3), for each $i \in I$, there exists $m_i \in N$ such that

$$(\forall s \in L(G_i) - K_i)\, ([[\tau] \geq m_i \vee st \in L_d(G_i)] \Rightarrow D(M(st)) = 1).$$

For any $s \in L(G_i) - K_i$ and $t \in L(G_i)/s$ such that $[[\tau] \geq m_i \vee st \in L_d(G_i)$, we consider any $j \in I$ and any $s_j \in M^{-1}M(st) \cap L(G_j)$. Since $D(M(st)) = D(M(st)) = 1$, we have by C4) that $s_j \in K_j$, that is, $s_j \in L(G_j) - K_j$. Thus, $\{G_i \mid i \in I\}$ is robustly diagnosable with respect to $\{K_i \subseteq L(G_i) \mid i \in I\}$. \qed
with respect to $K$ can be written as
$$\emptyset \subseteq \mathcal{M}_2 \subseteq \mathcal{G}_1 \cap \{ \tau \in \Delta \mid \tau \in \alpha_{K_i}(q_{K_i}, q_{K_i}) \},$$
for Example 7. We consider two possible models $G_1$ and $G_2$ shown in Fig. 4 (a) and (b), respectively, where $\Sigma = \{a, b, c, d, e, f\}$. Let $\Delta = \{a, b, c, d\}$. We assume that an observation mask $M : \Delta \to \Delta \cup \{\varepsilon\}$ is given as
$$M(\sigma) = \begin{cases} \sigma, & \text{if } \sigma \in \{a, b, c, d\} \\ \varepsilon, & \text{otherwise.} \end{cases}$$

Nonfailure specification languages $K_1$ and $K_2$ are assumed to be described by automata $G_{K_1}$ and $G_{K_2}$ shown in Fig. 5 (a) and (b), respectively. We have $L(G_1) = K_1 = \{ b^k a c^l \mid k, l \geq 0 \} \cup \{ b^k a d^l \mid k, l \geq 0 \}$ and $L(G_2) = K_2 = \{ d^k a e^l \mid k, l \geq 0 \} \cup \{ d^k a f^l \mid k, l \geq 0 \}$.

Since $G_1$ and $G_2$ are deadlock-free, $L_d(G_1) = L_d(G_2) = \emptyset$. We first show that
$$(\forall s \in L(G_1) - K_1) (\forall t \in L(G_1)/s \mid |t| \geq 1 \Rightarrow (\forall j \in I : M^{-1}(s) \cap L(G_j) \subseteq L(G_j) - K_j)).$$

For any $s \in L(G_1) - K_1$ and $t \in L(G_1)/s$ with $|t| \geq 1$, $st$ can be written as $b^k a c^l$ or $b^k a d^l$, where $k \geq 0$ and $l \geq 1$. We consider the case that $st = b^k a c^l$. Then, we have $M^{-1}(s) \cap L(G_1) = \{ c^l \mid l \geq 1 \} \subseteq L(G_1) - K_1$. Also, if $k = 0$ then $M^{-1}(s) \cap L(G_2) = \{ d^l \mid l \geq 1 \} \subseteq L(G_2) - K_2$; otherwise $M^{-1}(s) \cap L(G_2) = \emptyset \subseteq L(G_2) - K_2$. We consider the case that $st = b^k a d^l$. Then, we have $M^{-1}(s) \cap L(G_1) = \{ b^k a c^l \} \subseteq L(G_1) - K_1$ and $M^{-1}(s) \cap L(G_2) = \emptyset \subseteq L(G_2) - K_2$. Thus, the above condition holds. Analogously, we can verify that
$$(\forall s \in L(G_2) - K_2) (\forall t \in L(G_2)/s \mid |t| \geq 1 \Rightarrow (\forall j \in I : M^{-1}(s) \cap L(G_j) \subseteq L(G_j) - K_j)).$$

We can conclude that $(G_i \mid i \in I)$ is robustly diagnosable with respect to $\{ K_i \subseteq L(G_i) \mid i \in I \}$. By (1), a robust diagnoser $D : \Delta^* \to \{0, 1\}$ is given as
$$D(\tau) = \begin{cases} 0, & \text{if } \tau \in b^* + b^* a + d^* + d^* a \\ 1, & \text{otherwise.} \end{cases}$$

4 Verification of Robust Diagnosability

In this section, we present an algorithm for verifying robust diagnosability by generalizing the result of Qiu and Kumar (2006) (in the centralized setting). Hereafter, we assume that each possible model $G_i = (Q_i, \Sigma, \alpha_i, q_{0_i})$ ($i \in I$) has a finite state set, and a nonfailure specification language $K_i \subseteq L(G_i)$ is generated by a finite automaton $G_{K_i} = (Q_{K_i}, \Sigma, \alpha_{K_i}, q_{K_i})$. We augment the automaton $G_{K_i}$ by adding a dump state $q_{d_i} \notin Q_{K_i}$. Formally, the augmented automaton is defined as $G_{K_i} = (Q_{K_i}, \Sigma, \alpha_{K_i}, q_{K_i}, s)$, where $Q_{K_i} = Q_i \cup \{ q_{d_i} \}$, and the state transition function $\alpha_{K_i} : Q_{K_i} \times \Sigma \to Q_{K_i}$ is defined as
$$\alpha_{K_i}(q_{K_i}, \sigma) = \begin{cases} \alpha_{K_i}(q_{K_i}, \sigma), & \text{if } q_{K_i} \in Q_i, \text{ and } \alpha_{K_i}(q_{K_i}, \sigma) \neq q_{d_i} \\ q_{d_i}, & \text{otherwise.} \end{cases}$$

We have $L(G_{K_i}) = \Delta^*$. Further, for any $s \in \Delta^*$, $s \notin K$ if and only if $\alpha_{K_i}(q_{K_i}, s) = q_{d_i}$.

For each $i \in I$, we construct a testing automaton $T_i = (R_i, \Sigma, \alpha_T, r_{0_i})$ that consists of $G_i$, two copies of $G_{K_i}$, and $n - 1$ automata $G_{K_j}$ ($j \neq i$) as follows:

Algorithm 1 Construction of the testing automaton $T_i$:

(1) Define the state set $R_i$ and the initial state $r_{0_i} \in R_i$ as $R_i = (Q_i \times Q_{K_i} \times Q_{K_i} \times \cdots \times Q_{K_i})$ and $r_{0_i} = (q_{0_i}, q_{K_i}, q_{K_i}, \ldots, q_{K_i})$, respectively.

(2) Define the event set $\Sigma_T$ as
$$\Sigma_T = \left( \bigcup_{\varepsilon} \right) \times \left( \bigcup_{\varepsilon} \right) \times \cdots \times \left( \bigcup_{\varepsilon} \right)$$
$$(n + 1) \text{ times}$$
$- \left\{ (\varepsilon, \varepsilon, \ldots, \varepsilon) \right\}.$

(3) Define the state transition function $\alpha_{\Sigma} : R_i \times \Sigma_T \to R_i$ as follows: For each $r_i = (q_{0_i}, q_{K_i}, q_{K_i}, \ldots, q_{K_i}) \in R_i$ and $\sigma_T = (\sigma_1, \sigma_2, \ldots, \sigma_n) \in \Sigma_T$, $\alpha_{\Sigma}(r_i, \sigma_T)$ if and only if
- $\exists j \in I : q_{K_i} \neq q_{d_j} \land [\sigma_j \neq \varepsilon \Rightarrow \alpha_{K_i}(q_{K_i}, \sigma_j) \neq q_{d_j}]$,
- $\sigma \neq \varepsilon \Rightarrow \alpha_{T_i}(q_{K_i}, \sigma)$,
- $\forall l \in I : M(\sigma) = M(\sigma_l)$.

If $\alpha_{T_i}(r_i, \sigma_T)$, then
$$\alpha_{T_i}(r_i, \sigma_T) = (q_{0_i}, q_{K_i}^*, q_{K_i}^*, \ldots, q_{K_i}^*),$$
where
\[
q_i^* = \begin{cases} 
\alpha_i(q_i, \sigma), & \text{if } \sigma \neq \varepsilon \\
q_i, & \text{otherwise,}
\end{cases}
\]
\[
\hat{q}_K^* = \begin{cases} 
\hat{\alpha}_K(q_K, \sigma), & \text{if } \sigma \neq \varepsilon \\
\hat{q}_K, & \text{otherwise,}
\end{cases}
\]
\[
\check{q}_K^* = \begin{cases} 
\check{\alpha}_K(q_K, \sigma), & \text{if } \sigma_j \neq \varepsilon \\
\check{q}_K, & \text{otherwise. (}\forall j \in I\text{).}
\end{cases}
\]

For strings in $\Sigma_T^{+}$, projection functions $P : \Sigma_T^{+} \rightarrow \Sigma^*$ and $P_j : \Sigma_T^{+} \rightarrow \Sigma^*$ ($j \in I$) are defined as follows 2:

1. $P(\varepsilon) = \varepsilon, P_j(\varepsilon) = \varepsilon$,
2. $(\forall s_T \in \Sigma_T^{+})P(s_T) = (\sigma, \sigma_1, \sigma_2, \ldots, \sigma_n) \in \Sigma_T$,
3. $P(s_T\sigma_T) = P(s_T)\sigma_j$,
4. $(\forall i \in I, \forall j \in I)$.

By the definition of $\alpha_T$, we have, for any $s_{T_i} \in L(T_i)$,
\[
\alpha_T(r_i, 0, s_{T_i}) = (q_i, \hat{q}_K, \hat{q}_K, \ldots, \hat{q}_K),
\]
(2)

where $\alpha_i(q_i, 0, P(s_{T_i})) = q_i, \hat{\alpha}_K(q_K, 0, P(s_{T_i})) = \hat{q}_K$, and, for all $j \in I, \check{\alpha}_K(q_K, 0, P_j(s_{T_j})) = \check{q}_K$. Also, we have $M(P(s_{T_i})) = M(P_j(s_{T_j}))$ for any $j \in I$. Thus, $T_i$ traces all strings $s \in L(G)$ and $s_1, s_2, \ldots, s_n \in \Sigma^*$ such that

1. $(\forall i \in I)$ $M(s) = M(s_i)$,
2. $(\exists j \in I)$ $s_j \in K_j$.

A path $\pi_i$ in the testing automaton $T_i$ is a sequence of transitions such that $r_i^{(1)} \xrightarrow{\sigma_1} r_i^{(2)} \xrightarrow{\sigma_2} \ldots \xrightarrow{\sigma_{p-1}} r_i^{(p-1)} \xrightarrow{\sigma_{p}} r_i^{(p+1)}$ ($p \geq 1$), where, for each $k \in \{1, 2, \ldots, p\}, r_i^{(k+1)} = \alpha_T(r_i^{(k)}, \sigma_i^{(k)}). \pi_i$ is called a cycle if $r_i^{(1)} = r_i^{(p+1)}$.

Intuitively, the existence of a failure string $s \in L(G_i) - K_i$ (which is traced by the first two components $G$ and $G_K$) such that any extension of $s$ cannot be distinguished from a nonfailure string in some nonfailure specification language $K_j$ (which is traced by the $2 + j$th component $G_K$) is characterized by the existence of a reachable cycle $\pi_i$ of the testing automaton $T_i$ such that it contains an event $\sigma_{T_i} \in \Sigma_T$, whose first coordinate is not $\varepsilon$ and a state $r_i \in R_i$, whose second coordinate is the dump state $q_{d_i}$ of $G_{K_i}$. Also, the existence of a deadlocking failure string $s' \in L(G_i) - K_i$ that cannot be distinguished from a nonfailure string in some nonfailure specification language $K_j$ is characterized by the existence of a reachable state of $T_i$ such that its first coordinate is a deadlocking state of $G_i$ and its second coordinate is the dump state of $G_{K_i}$.

\* The projection functions $P$ and $P_j$ ($j \in I$) are used to extract the 1st and $1 + j$th coordinates of a string in $\Sigma_T$, respectively.

**Theorem 8** The set $\{G_i \mid i \in I\}$ of possible models is not robustly diagnosable with respect to $\{K_i \subseteq L(G_i) \mid i \in I\}$ if and only if there exists $i \in I$ such that, in the testing automaton $T_i$,

1. there exists a reachable cycle $r_i^{(1)} \xrightarrow{\sigma_i^{(1)}} r_i^{(2)} \xrightarrow{\sigma_i^{(2)}} \ldots \xrightarrow{\sigma_i^{(p)}} r_i^{(p+1)}$ such that
   \[
   (\exists k \in \{1, 2, \ldots, p\}) \sigma_i^{(k)} \neq \varepsilon \wedge q_{d_i},
   \]
   (3)
   where $\sigma_i^{(k)} = (\sigma_i^{(1)}, \sigma_i^{(2)}, \ldots, \sigma_i^{(k)})$, and $r_i^{(k)} = (q_{K_i}, q_{K_i}, q_{K_i}, \ldots, q_{K_i})$,
   or
   2. there exists a reachable state $(\check{q}_i, \check{q}_K, \check{q}_K, \ldots, \check{q}_K)$ such that $q_i \in Q_{i,d}$ and $\check{q}_K = q_{d_i}$, where $Q_{i,d}$ is the set of deadlocking states of $G_i$ defined as $Q_{i,d} = \{q_i \in Q_i \mid \forall s \in \Sigma : \neg \alpha_i(q_i, s)\}$.

**PROOF.** First, we prove the sufficiency part. We consider the case that, in the testing automaton $T_i$ ($i \in I$), there exists a reachable cycle $r_i^{(1)} \xrightarrow{\sigma_i^{(1)}} r_i^{(2)} \xrightarrow{\sigma_i^{(2)}} \ldots \xrightarrow{\sigma_i^{(p)}} r_i^{(p+1)}$ satisfying (3). Then, there exists $s_{T_i} \in L(T_i)$ such that $\alpha_T(r_i, 0, s_{T_i}) = r_i^{(1)}$. Note that, for all $j \in I$, once $G_K$ reaches the dump state $q_{d_i}$, it remains there. Since there exists $k \in \{1, 2, \ldots, p\}$ such that the second coordinate $\hat{q}_K$ of $r_i^{(k)}$ is $q_{d_i}$, the second coordinate $\check{q}_K$ of $r_i^{(1)}$ is $q_{d_i}$. Also, since $r_i^{(1)} = \alpha_T(r_i, 0, s_{T_i}) = r_i^{(1)}$, we have by the definition of $\alpha_T$ that there exists $j \in I$ such that $\check{q}_K \neq q_{d_i}$. It follows from $P(s_{T_j}) \in L(G_i)$ and $\check{\alpha}_K(q_K, 0, P(s_{T_j})) = \check{q}_K, \check{q}_K, \ldots, \check{q}_K)$, we have $s_j := P_j(s_{T_j}) \in K_j$. Also, since $\check{\alpha}_K(q_K, 0, P_j(s_{T_j})) = \check{q}_K \neq q_{d_i}$, we have

For any nonnegative integer $m_i \in N$, consider $t_{m_i}^{(k)} \in \Sigma_T^{\star}$ where $t_{m_i}^{(k)} := \alpha_i^{(1)}(\sigma_i^{(2)}), \ldots, \sigma_i^{(k)}$. Since there exists $\sigma_i^{(k)}$ whose first coordinate $\sigma_i^{(k)}$ is not $\varepsilon$, we have $|t_{m_i}^{(k)}| \geq m_i$, where $t := P(t_{m_i}^{(k)}).$ Also, since $t_{m_i}^{(k)} \in L(T_i)$, we have $s = P(t_{m_i}^{(k)}) \in L(G_i).$ Moreover, since $\check{\alpha}_K(q_K, 0, P_j(s_{T_j})) = \check{q}_K \neq q_{d_i}$, we have $u_{j} := P_j(s_{T_j}) \in K_j \subseteq L(G_i)$. It follows that

We also consider the case that there exists a reachable state $r_i = (q_i, \check{q}_K, \check{q}_K, \check{q}_K^2, \ldots, \check{q}_K^n) \in T_i$ such that $q_i \in Q_{i,d}$ and $\check{q}_K = q_{d_i}$. There exists $s_{T_i} \in L(T_i)$ such that $\alpha_T(r_i, 0, s_{T_i}) = r_i$. We have $s' := P(s_{T_j}) \in L(G_j)$.

Therefore, we can conclude that $\{G_i \mid i \in I\}$ is not robustly diagnosable with respect to $\{K_i \subseteq L(G_i) \mid i \in I\}$. We also consider the case that there exists a reachable state $r_i = (q_i, \check{q}_K, \check{q}_K, \check{q}_K^2, \ldots, \check{q}_K^n) \in T_i$ such that $q_i \in Q_{i,d}$ and $\check{q}_K = q_{d_i}$. Since $\alpha_T(q_i, s') = q_i$, and $\check{\alpha}_K(q_K, 0, s') = \check{q}_K = q_{d_i}$, we have
We also consider the case that for any state reachable from $\tilde{q}_K$, there exists $\tilde{q}_d \neq q_d$. Since $\tilde{q}_K \neq q_d$, we have $s_i' := P(s_{T_i}') \in K_i$. It follows that $s_i' \in L(G_i) - K_i$, $\varepsilon \in L(G_i)/s'$, $s_i' \in L_d(G_i)$, $s_j' \in M^{-1}(s') \cap L(G_i)$, and $s_j' \in K_j$. Thus, $\{G_i \mid i \in I\}$ is not robustly diagnosable with respect to $\{K_i \subseteq L(G_i) \mid i \in I\}$. 

Next, we suppose that $\{G_i \mid i \in I\}$ is not robustly diagnosable with respect to $\{K_i \subseteq L(G_i) \mid i \in I\}$. Then, there exists $i \in I$ such that, for any $m_i \in N$,

$$\exists s \in L(G_i) - K_i, \exists t \in L(G_i)/s$$

$$\bigl[[|t| \geq m_i \lor st \in L_d(G_i)\bigr]$$

$$\land \exists j \in I : M^{-1}(st) \cap L(G_i) \subseteq L(G_i) - K_j.$$ 

Consider any $m_i > |R_i|$, where $|R_i|$ denotes the number of states of $T_i$. We pick up an index $j \in I$ such that $M^{-1}(st) \cap L(G_i) \not\subseteq L(G_i) - K_j$. For this index $j$, there exists $u_j \in K_j$ such that $M(st) = M(u_j)$. Also, for any $l \in I$ with $l \neq j$, let $u_l \in \Sigma^*$ be any string such that $M(st) = M(u_l)$. Note that, for any $v_j \in pr\{u_j\}$, we have $\tilde{q}_K(q_K, v_j) \neq q_d$. By the construction of the testing automaton $T_i$, there exists $s_T \in L(T_i)$ such that $P(s_T) = st$, $P(s_T) = u_l$ for all $l \in I$, and $\alpha_T(v_i, s_T) = q_i$, $\tilde{q}_K(q_K, v_i, st) = q_d$, and $\tilde{q}_K(q_K, u_i) = q_d$, for all $i \in I$.

There exists a prefix $s_T'$ of $s_T$, such that $P(s_T') = s$. Let $\tilde{q}_K'$ be the second coordinate of $\alpha_T(v_i, s_T')$. Then, we have $\tilde{q}_K'(q_K, v_i, s) = q_d$. Since $s \in L(G_i) - K_i$, we have $\tilde{q}_K'(q_K, s) = q_d$. This means that the second coordinate of any state reachable from $\alpha_T(v_i, s_T')$ is $q_d$. We can write $s_T = s_T', t_{T_i}$. Then, we have $P(t_{T_i}) = t$.

We consider the case that $|t| \geq m_i$. Since $|t| \geq m_i > |R_i|$, $t_{T_i}$ contains more than $|R_i|$ events in $\Sigma^*$ whose first coordinates are not $\varepsilon$. Thus, there exists a cycle $r_{i_1}^{(1)} \sigma r_{i_1}^{(2)} \cdots \sigma r_{i_1}^{(p-1)} \sigma r_{i_1}^{(p)} \cdots \sigma r_{i_1}' \cdots \sigma r_{i_1}'$ satisfying (3) along the string $t_{T_i}$. Since $s_T = s_T', t_{T_i} \in L(T_i)$, this cycle is reachable from $r_{i_1}$.

We also consider the case that $st \in L_d(G_i)$. Then, for $\alpha_T(v_i, st) = q_i, q_K, q_K, q_K, \ldots, q_K$, we have $\alpha_T(v_i, st) = q_i$, and $\tilde{q}_K(q_K, v_i, st) = q_d$. Thus, the second condition of the theorem holds. $\square$

**Remark 9** For each $i \in I$, the number of states of the testing automaton $T_i$ is at most $|Q_i| \times (|Q_K| + 1)^2 \times \prod_{j \neq i}(|Q_j| + 1)$. Since $|\Sigma^*| = (|\Sigma| + 1)^{n+1} - 1$, there are at most $|Q_i| \times (|Q_K| + 1)^2 \times \prod_{j \neq i}(|Q_j| + 1) \times ((|\Sigma| + 1)^{n+1} - 1)$ transitions in $T_i$. Therefore, for each $T_i$, the complexity of verifying the conditions of Theorem 8 is $O(|Q_i| \times |Q_K|^2 \times \prod_{j \neq i}(|Q_j|) \times |\Sigma|^{n+1})$.

Fig. 6. Possible models $G_1$ and $G_2$ for Example 10.

![Fig. 6](image URL)

Fig. 7. Nonfailure specifications $G_{K_1}$ and $G_{K_2}$ for Example 10.

![Fig. 7](image URL)

Fig. 8. Augmented nonfailure specifications $\tilde{G}_{K_1}$ and $\tilde{G}_{K_2}$ for Example 10.

**We consider the special case that the specification model $G_{K_i}$ is a subautomaton of the system model $G_i$ for each $i \in I$. By Remark 4 of Qiu and Kumar (2006), we can show that, for each $T_i$, the complexity of testing the conditions of Theorem 8 is $O(|Q_i|^2 \times \prod_{j \neq i}(|Q_j|) \times |\Sigma|^{n+1})$ for this special case.

The following example illustrates the verification result of Theorem 8.

**Example 10** We consider two possible models $G_1$ and $G_2$ shown in Fig. 6 (a) and (b), respectively, where $\Sigma = \{a, b, c\}$. Let $\Delta = \{a, b\}$. We assume that an observation mask $M : \Sigma \rightarrow \Delta \cup \{\varepsilon\}$ is given as

$$M(\sigma) = \begin{cases} \sigma, & \text{if } \sigma \in \{a, b\} \\ \varepsilon, & \text{otherwise.} \end{cases}$$

Nonfailure specification languages $K_1$ and $K_2$ are described by automata $G_{K_1}$ and $G_{K_2}$ shown in Fig. 7 (a) and (b), respectively. The augmented automata $\tilde{G}_{K_1}$ and $\tilde{G}_{K_2}$ are shown in Fig. 8 (a) and (b), respectively.

To verify robust diagnosability of $\{G_i \mid i \in I\}$ with respect to $\{K_i \subseteq L(G_i) \mid i \in I\}$, we construct the testing automata $T_1$ and $T_2$, which are shown in Figs. 9 and 10, respectively. Since there exists a reachable state $(q_{1.1}, q_{4.1}, q_{4.1})$ such that the first coordinate $q_{1.1} \in Q_{4.1}$ is a deadlocking state of $G_1$ and the second coordinate $q_{4.1}$ is the dump state of $G_{K_1}$, we can conclude that $\{G_i \mid i \in I\}$ is not robustly diagnosable with respect to $\{K_i \subseteq L(G_i) \mid i \in I\}$. This reachable state indicates that the occurrence of a deadlocking failure string $c^b$.
also be verified by using the testing automaton that detects any occurrence of a failure within a uniformly bounded number of steps for all possible models. Instead of an exact single model, it is formally bounded number of steps for all possible models.

$$I K 0 \epsilon, c, c \epsilon \in (T) \in \{q_{2,1}, q_{d_1}, K_1, \phi, q_{d_2}\}$$

satifying (3).

5 Conclusions

In this paper, we considered a situation where a set of possible models, instead of an exact single model, is given, and studied the existence of a robust diagnoser that detects any occurrence of a failure within a uniformly bounded number of steps for all possible models. We introduced a notion of robust diagnosability to characterize the existence of a robust diagnoser. We then presented a verification algorithm for robust diagnosability.

Recently, failure diagnosis under dynamic event observation has been studied by Wang et al. (2011). Extension of the obtained results to the setting of dynamic observation is future work.

References


