A Sufficient Condition for Diagnosability of Large-Scale Discrete Event Systems

Shigemasa Takai
Department of Information Science, Kyoto Institute of Technology
Matsugasaki, Sakyo-ku, Kyoto 606-8585, Japan
E-mail : takai@kit.ac.jp

Abstract: In this paper, we study the diagnosability property of a large-scale discrete event system that is modeled by the synchronous composition of \( n \) subsystems. In order to verify the necessary and sufficient condition for the diagnosability property, we have to perform operations over the entire system model, which suffers from the state space explosion problem. Motivated by this, we present a sufficient condition for the diagnosability property that can be tested by using only the subsystem models.

1. Introduction

Failure diagnosis of discrete event systems (DESs) has received considerable attention. A language-based approach for failure diagnosis was proposed by Sampath et al. [1], [2]. In their approach, the problem of diagnosis is detecting the occurrence of an unobservable failure event within a uniformly bounded number of steps. A notion of diagnosability was introduced in [1], and polynomial-time algorithms for verifying diagnosability were developed [3], [4]. Further, these results have been extended to decentralized diagnosis where the system is diagnosed by a set of local diagnosers [5], [6], [7], [8].

In this paper, we study the diagnosability property of a large-scale DES that is modeled by the synchronous composition of \( n \) subsystems. The algorithms for testing the necessary and sufficient condition for diagnosability require operations over the entire system model [3], [4], [6]. In the worst case, the number of states in the entire system grows exponentially with respect to the number of subsystems. Thus, verifying diagnosability using the algorithms of [3], [4], [6] suffers from the state space explosion problem. Motivated by this, we present a sufficient condition for diagnosability of the entire system under the assumption that an unobservable failure event is not shared by two or more subsystems. Note that this assumption is not imposed in this paper.

2. Preliminaries

We consider a finite automaton

\[ G = (X, \Sigma, \delta, x_0), \]

where \( X \) is the finite state set, \( \Sigma \) is the finite event set, \( \delta : \Sigma \times X \rightarrow X \) is the transition function, and \( x_0 \in X \) is the initial state. Let \( \Sigma^* \) be the set of all finite strings of elements of \( \Sigma \), including the empty string \( \varepsilon \). For each \( s \in \Sigma^* \), \(|s|\) denotes its length. The notation \( \sigma \in s \) means that \( \sigma \in \Sigma \) is an event contained in a string \( s \in \Sigma^* \). Also the notation \( \sigma \notin s \) means that \( \sigma \in \Sigma \) is not contained in \( s \in \Sigma^* \). The transition function \( \delta \) is extended to \( \delta : \Sigma^* \times X \rightarrow X \) in the usual way. The notation \( \delta(s,x) \) denotes that \( \delta(s,x) \) is defined for any \( s \in \Sigma^* \) and \( x \in X \). The generated language \( L(G) \) of \( G \) is defined as

\[ L(G) = \{ s \in \Sigma^* \mid \delta(s,x_0) \}. \]

For each \( s \in L(G) \), the postlanguage of \( L(G) \) after \( s \) is defined as

\[ L(G) \setminus s = \{ t \in \Sigma^* \mid st \in L(G) \}. \]

For each \( \sigma \in \Sigma \), the set of strings of \( L(G) \) that end in \( \sigma \) is denoted by \( \Psi_{L(G)}(\sigma) \), that is,

\[ \Psi_{L(G)}(\sigma) = \{ s \in L(G) \mid \exists t \in \Sigma^* ; s = ts \}. \]

A finite automaton \( G \) is said to be live if for each \( x \in X \), there exists \( \sigma \in \Sigma \) such that \( \delta(\sigma,x) \). A path \( p \) in \( G \) is a finite sequence of transitions \( (x_1, \sigma_1, x_2, \cdots, x_{m-1}, \sigma_{m-1}, x_m) \) such that \( \delta(\sigma_i, x_i) = x_{i+1} (i = 1, 2, \cdots, m-1) \). \( p \) is called a cycle if \( x_1 = x_m \).

3. Diagnosability Property

In this paper, we study the diagnosability property of a large-scale DES that consists of \( n \) subsystems \( G_i (i \in I = \{1, 2, \cdots, n\}) \) which operate concurrently.

3.1 Diagnosability of Subsystems

Each subsystem \( G_i \) is modeled by a live finite automaton

\[ G_i = (X_i, \Sigma_i, \delta_i, x_{i0}). \]

The event set \( \Sigma_i \) is partitioned into the observable event set \( \Sigma_{io} \) and the unobservable event set \( \Sigma_{iuo} \). The natural projection map \( P_i : \Sigma_i^* \rightarrow \Sigma_{io}^* \) is inductively defined as follows:

- \( P_i(\varepsilon) = \varepsilon \)
- \( \forall s_i \in \Sigma_i^*, \sigma_i \in \Sigma_i ; \)
  \[ P_i(s_i) = \begin{cases} P_i(s_i)\sigma_i, & \text{if } \sigma_i \in \Sigma_{io} \\ P_i(s_i), & \text{otherwise} \end{cases} \]

For each string \( s_i \in \Sigma_i^* \), \( P_i(s_i) \) is obtained by erasing all events of \( \Sigma_{iuo} \) from \( s_i \). If \( s_i \in L(G_i) \) is executed by \( G_i \), \( P_i(s_i) \) is observed by a diagnoser for \( G_i \). Also, the inverse projection map \( P_i^{-1} : \Sigma_{io}^* \rightarrow 2^{\Sigma_i^*} \) is defined as

\[ P_i^{-1}(s_{io}) = \{ s_i \in \Sigma_i^* \mid P_i(s_i) = s_{io} \}. \]

In this paper, we consider a diagnosis problem to detect the occurrence of an unobservable event. The diagnosability
property of $G_i$ with respect to an unobservable event $\sigma_f \in \Sigma_{uo}$ is defined as follows.

**Definition 1:** [1] The subsystem $G_i$ ($i \in I$) is said to be diagnosable with respect to an unobservable event $\sigma_f \in \Sigma_{uo}$ if

\[
(\exists n_i \in N)(\forall s_i \in \Psi_{L(G_i)}(\sigma_f))(\forall t_i \in L(G_i) \setminus s_i)
\]

\[
|t_i| \geq n_i \Rightarrow \forall u_i \in P^{-1}_iP_i(s_i,t_i) \cap L(G_i); \quad \sigma_f \in u_i,
\]

where $N$ is the set of all nonnegative integers.

The above condition for diagnosability requires the existence of a nonnegative integer $n_i$ such that for any string $s_i \in \Psi_{L(G_i)}(\sigma_f)$ whose last event is $\sigma_f$, if $s_i$ is extended by a string $t_i \in L(G_i) \setminus s_i$ with $|t_i| \geq n_i$, then any string $u_i \in L(G_i)$ that is indistinguishable from $s_i,t_i$ also contains the event $\sigma_f$. If $G_i$ is diagnosable with respect to $\sigma_f \in \Sigma_{uo}$, the occurrence of $\sigma_f$ can be detected within $n_i$ steps.

### 3.2 Diagnosability of Entire System

The entire system $G$ is modeled by the synchronous composition $||_{i \in I}G_i$ of $n$ subsystems $G_i$ ($i \in I$) as follows:

\[
G = ||_{i \in I}G_i = (X, \Sigma, \delta, x_0),
\]

where $X = X_1 \times X_2 \times \cdots \times X_n$, $\Sigma = \bigcup_{i \in I} \Sigma_i$, and $x_0 = (x_{10}, x_{20}, \cdots, x_{n0})$. For each $\sigma \in \Sigma$, let $I(\sigma) = \{i \in I \mid \sigma \in \Sigma_i\}$. The transition function $\delta : \Sigma \times X \to X$ is defined as

\[
\delta(\sigma, (x_1, x_2, \cdots, x_n)) = \begin{cases} (x_1', x_2, \cdots, x_n') & \text{if } \forall i \in I(\sigma) : \delta_i(\sigma, x_i) \text{ is defined}, \\ x_i & \text{otherwise}. \end{cases}
\]

where for each $i \in I$,

\[
x_i' = \begin{cases} \delta_i(\sigma, x_i) & \text{if } i \in I(\sigma) \\ x_i & \text{otherwise}. \end{cases}
\]

In this paper, we assume that the entire system $G$ is also live.

**Remark 1:** Even if all subsystems $G_i$ are live, the entire system $G$ is not necessarily live. In this paper, we do not address the issue of verification of liveness of the entire system.

The observable event set $\Sigma_o$ and the unobservable event set $\Sigma_{uo}$ are defined as

\[
\Sigma_o = \bigcup_{i \in I} \Sigma_{io},
\]

\[
\Sigma_{uo} = \Sigma - \Sigma_o,
\]

respectively. The natural projection map $P : \Sigma^* \to \Sigma^*_o$ and its inverse projection map $P^{-1} : \Sigma^*_o \to 2^{\Sigma^*}$ are defined in the same way as $P_i : \Sigma_i^* \to \Sigma_{io}$ and $P_i^{-1} : \Sigma_{io}^* \to 2^{\Sigma_i^*}$, respectively.

As in the subsystems $G_i$, the diagnosability property of the entire systems $G$ with respect to an unobservable event $\sigma_f \in \Sigma_{uo}$ is defined as follows.

**Definition 2:** [1] The entire system $G$ is said to be diagnosable with respect to an unobservable event $\sigma_f \in \Sigma_{uo}$ if

\[
(\exists n \in N)(\forall s \in \Psi_{L(G)}(\sigma_f))(\forall t \in L(G) \setminus s)
\]

\[
|t| \geq n \Rightarrow \forall u \in P^{-1}(P(st) \cap L(G)); \quad \sigma_f \in u.
\]

For each $i \in I$, a map $\pi_i : \Sigma^* \to \Sigma_i^*$ is inductively defined as follows:

- $\pi_i(\varepsilon) = \varepsilon$,
- $\forall s \in \Sigma_i^* \ni \sigma \in \Sigma$,

\[
\pi_i(s) = \begin{cases} \pi_i(s)\sigma & \text{if } \sigma \in \Sigma_i \\ \pi_i(s), & \text{otherwise.} \end{cases}
\]

For each string $s \in \Sigma_i^*$, $\pi_i(s)$ is obtained by erasing all events of $\Sigma - \Sigma_i$ from $s$. Then, the generated language $L(G)$ of the entire system $G$ satisfies the following equation [10]:

\[
L(G) = \{s \in \Sigma^* \mid \forall i \in I ; \pi_i(s) \in L(G_i)\}.
\]

When a string $s$ is executed in $G$, $\pi_i(s)$ is executed in each subsystem $G_i$.

### 4. Sufficient Condition for Diagnosability

Using the verification algorithm presented in [6], diagnosability of the entire system $G$ (respectively, the subsystem $G_i$) is tested in $O(|X|^2 \cdot |\Sigma|^2)$ (respectively, $O(|X|^2 \cdot |\Sigma_i|^2)$). In the worst case, the number of states in the entire system grows exponentially with respect to the number of subsystems. Motivated by this, we present a sufficient condition for diagnosability of the entire system $G$ that can be tested by using only the subsystem models.

**Theorem 1:** The entire system $G$ is diagnosable with respect to an unobservable event $\sigma_f \in \Sigma_{uo}$ if there exists $I' \subseteq I(\sigma_f)$ satisfying the following two conditions:

- In each subsystem $G_i$ ($i \in I$), every cycle contains an event of $\Sigma_f^i := \bigcup_{i \in I'} \Sigma_i$.
- For each $i \in I'$, $G_i$ is diagnosable with respect to $\sigma_f$.

**Proof:** Assume that there exists $I' \subseteq I(\sigma_f)$ satisfying the two conditions of Theorem 1. By the second condition, for each $i \in I'$, the subsystem $G_i$ is diagnosable with respect to $\sigma_f$. Let $n_i \in N$ be a nonnegative integer such that $n_i$ is the diagnosability condition of $G_i$ holds, and $n := \max_{i \in I'} n_i$.

We prove that the diagnosability condition of the entire system $G$ holds for the nonnegative integer $n \cdot |I'| \cdot |X|$. Consider any $s \in \Psi_{L(G)}(\sigma_f)$ and any $t \in L(G) \setminus s$ with $|t| \geq n \cdot |I'| \cdot |X|$. By executing the string $t$, $G$ goes through cycles at least $n \cdot |I'|$ times. When a cycle is executed in $G$, a cycle is executed in at least one subsystem. By the first condition of the theorem, in each subsystem, every cycle contains an event of $\Sigma_f^i$. Thus, the string $t$ contains at least $n \cdot |I'|$ events of $\Sigma_f$. For each $i \in I'$, $\pi_i(t)$ be the number of events of $\Sigma_i$ contained in $t$. Then, we have $\sum_{i \in I'} \pi_i(t) \geq n \cdot |I'|$, which implies that there exists $i' \in I'$ such that $\pi_i(t) \geq n_i$. It follows that $|\pi_{i'}(t)| = |\pi_i(t)| \geq n \geq n_i$. Also, we have $\pi_{i'}(s) \in L(G_{i'})$, and $\sigma_f \in \Sigma_{i'}$. So we have $\pi_{i'}(s) \in \Psi_{L(G_{i'})}(\sigma_f)$. Further, since $\pi_{i'}(s)\pi_{i'}(t) \in L(G_{i'})$, we have $\pi_{i'}(t) \in L(G_{i'})\pi_{i'}(s)$.
Consider any $u \in P^{-1}P(st) \cap L(G)$. $P_\tau(\pi_\tau(u))$ is the string obtained by erasing all events of $\Sigma = \Sigma^{\tau \alpha}$ from $u$, and the same as the string obtained by erasing all events of $\Sigma = \Sigma^{\tau \alpha}$ from $P(u)$. In the same way, $P_\tau(\pi_\tau(st))$ is the same as the string obtained by erasing all events of $\Sigma = \Sigma^{\tau \alpha}$ from $P(st)$. Since $P(u) = P(st)$, we have

$$P_\tau(\pi_\tau(u)) = P_\tau(\pi_\tau(st)) = P_\tau(\pi_\tau(s)\pi_\tau(t)).$$

Further, since $\pi_\tau(u) \in L(G_\tau)$, we have

$$\pi_\tau(u) \in P_\tau^{-1}P_\tau(\pi_\tau(s)\pi_\tau(t)) \cap L(G_\tau).$$

Since $G_\tau$ is diagnosable with respect to $\sigma_f$, we have $\sigma_f \in \pi_\tau(u)$, which implies that $\sigma_f \in u$. Therefore, $G$ is diagnosable with respect to $\sigma_f$.

The sufficient condition of Theorem 1 requires that in each subsystem, every cycle must contain an event of diagnosable subsystems. This requirement is needed to ensure that at least one diagnosable subsystem, a sufficiently long string is executed after the occurrence of $\sigma_f \in \Sigma^{\tau \alpha}$.

**Remark 2:** The first condition of Theorem 1 can be tested in the following way. In each subsystem $G_i$ ($i \in I$), we first remove all transitions labeled by an event of $\Sigma_\tau$. Then, the first condition holds if and only if there is no cycle in the remaining transition structures.

Next, we show that under the sufficient condition of Theorem 1, the occurrence of $\sigma_f \in \Sigma^{\tau \alpha}$ can be detected in a decentralized fashion. Let $I' \subseteq I(\sigma_f)$ be a subset satisfying the two conditions of Theorem 1. For each subsystem $G_i$ ($i \in I'$), a local diagnoser $D_i$ is formally defined as a map $D_i : P_i(L(G_i)) \rightarrow \{1, 0, \phi\}$. For a local observation string, a local diagnoser issues a diagnosis decision either “1”, “0”, or “ϕ”, where “1” means that $\sigma_f$ was occurred, “0” means that $\sigma_f$ was not occurred, and “ϕ” means that the occurrence of $\sigma_f$ is not known. We consider local diagnosers $D_i : P_i(L(G_i)) \rightarrow \{1, 0, \phi\}$ ($i \in I'$) given by

$$D_i(P_i(s)) = \begin{cases} 1, & \text{if } \forall u_i \in P_i^{-1}P_i(s) \cap L(G_i); \sigma_f \in u_i \\ 0, & \text{if } \forall u_i \in P_i^{-1}P_i(s) \cap L(G_i); \sigma_f \notin u_i \quad (1) \\ \phi, & \text{otherwise.} \end{cases}$$

As in the proof of Theorem 1, we consider any $s \in \Psi_{L(G)}(\sigma_f)$ and any $t \in L(G) \setminus s$ with $|t| \geq n \cdot |I'| \cdot |X|$. As shown in the proof of Theorem 1, there exists $i' \in I'$ such that $\pi_{\tau}(s) \in \Psi_{L(G),\tau}(\sigma_f), \pi_{\tau}(t) \in L(G_i) \setminus \pi_{\tau}(s)$, and $|\pi_{\tau}(t)| \geq n_{i'}$. By diagnosability of $G_i$ with respect to $\sigma_f$, we have

$$\forall u_{i'} \in P_{i'}^{-1}P_{i'}(\pi_{\tau}(s)\pi_{\tau}(t)) \cap L(G_i); \sigma_f \in u_{i'}.\]$$

It follows from (1) that $D_i(P_i(\pi_{\tau}(s)\pi_{\tau}(t))) = 1$. Note that when $st$ is executed in $G$, $P_i(\pi_\tau(s)\pi_\tau(t))$ is observed by $D_i$. So the occurrence of $\sigma_f$ is detected by at least one local diagnoser within $n \cdot |I'| \cdot |X|$ steps. This means that there is no missed detection under the decentralized diagnosis performed by $D_i$.

We further show that there is no false decision under the decentralized diagnosis performed by $D_i$. Consider any $s' \in L(G)$. We first consider the case that $\sigma_f \in s'$. Since $\pi_{\tau}(s')$ contains $\sigma_f$ for any $i' \in I'$, it follows from (1) that $D_i(P_i(\pi_{\tau}(s'))) \neq 0$. We next consider the case that $\sigma_f \notin s'$. Since $\pi_{\tau}(s)$ does not contain $\sigma_f$ for any $i' \in I'$, it follows from (1) that $D_i(P_i(\pi_{\tau}(s'))) = 1$.

**Example 1:** We consider the entire system $G$ that is modeled by the synchronous composition of three subsystems $G_1$, $G_2$, $G_3$ shown in Fig. 1. The entire system $G$ is shown in Fig. 2. Let $\Sigma_{1\alpha} = \{a, c_1\}, \Sigma_{1\alpha} = \{f, d_1\}, \Sigma_{2\alpha} = \{b, c_2\}, \Sigma_{2\alpha} = \{f, d_2\}, \Sigma_{3\alpha} = \{a\}, \Sigma_{3\alpha} = \{b\}$ in each subsystem.

We consider the problem of detecting the occurrence of the unobservable event $f \in \Sigma^{\tau \alpha}$, which is shared by $G_1$ and $G_2$. Both $G_1$ and $G_2$ are diagnosable with respect to $f$. There are two cycles in $G_3$. One contains $a \in \Sigma_1$, and the other contains $b \in \Sigma_2$. Thus, for $I' = \{1, 2\} = I(f)$, the two conditions of Theorem 1 are satisfied. By using only the subsystem models, we can verify that the entire system $G$ is diagnosable with respect to $f$.

By (1), the local diagnosers $D_i : P_i(L(G_i)) \rightarrow \{1, 0, \phi\}$ ($i = 1, 2$) are constructed as follows:

$$D_1(P_1(s_1)) = \begin{cases} 1, & \text{if } c_1 \in P_1(s_1) \\ \phi, & \text{otherwise,} \end{cases}$$

$$D_2(P_2(s_2)) = \begin{cases} 1, & \text{if } c_2 \in P_2(s_2) \\ \phi, & \text{otherwise.} \end{cases}$$

$D_1$ and $D_2$ can detect the occurrence of $f$ by observing $c_1$ and $c_2$, respectively. In the entire system $G$, if $G$ executes the cycle $(2, 2, 0), c_1, (3, 2, 0), a, (2, 2, 0)$ repeatedly after the occurrence of $f$, only $D_1$ can detect the occurrence of $f$. Also, if $G$ executes the cycle $(2, 2, 0), c_2, (2, 3, 0), b, (2, 2, 0)$ repeatedly, only $D_2$ can detect the occurrence of $f$. Therefore, in this example, both $D_1$ and $D_2$ are needed to perform the
5. Conclusion

In this paper, we present a sufficient condition for diagnosability of a large-scale DES modeled by the synchronous composition of subsystems. In contrast to the necessary and sufficient condition given in [3], [4], [6], our sufficient condition has an advantage that it can be tested by using only the subsystem models. Further, under our sufficient condition, the task of diagnosis can be performed in a decentralized fashion.

Acknowledgments

This research was supported in part by MEXT under Grant-in-Aid for Scientific Research (C) 18560433.

References


