Distributed Diagnosis Under Bounded-Delay Communication of Immediately Forwarded Local Observations

Wenbin Qiu and Ratnesh Kumar (wqiu, rkumar@iastate.edu)
Department of Electrical & Computer Engineering
Iowa State University, Ames, IA 50011

Abstract

In this paper, we study distributed failure diagnosis under $k$-bounded communication delay, where each local site transmits its observations to other sites immediately after each observation, and which is received within at most $k$ more event executions of the plant. This work extends our prior work on decentralized failure diagnosis [17] that did not allow any communication among the local sites. A notion of joint $\text{iop}^k$-diagnosability is introduced so that any failure can be diagnosed within a bounded delay of its occurrence by one of the local sites using its own observations and the $k$-bounded delayed observations received from other local sites. The local sites communicate among each other using an “immediate observation passing (iop)” protocol, forwarding any observation immediately up on its occurrence. We construct models for $k$-bounded communication delay, and use them to extend the system and non-fault specification models for capturing the effect of bounded-delay communication. Using the extended system and specification models, the distributed diagnosis problem under the immediate observation passing protocol is then converted to a decentralized diagnosis problem of [17]. Results from [17] are applied for verifying joint $\text{iop}^k$-diagnosability, and for synthesizing local diagnosers. Methods by which complexity of testing joint $\text{iop}^k$-diagnosability and of on-line diagnosis can be reduced are presented. Finally, we compare the notions of diagnosability, codiagnosability, and joint $\text{iop}^k$-diagnosability.

Keywords: Discrete event systems, distributed failure diagnosis, joint-diagnosability, communication delay

1 Introduction

Failure diagnosis is an active area of research, and has received considerable attention in the literature. A failure is a deviation from an expected or desired behavior. Various

*The research was supported in part by the National Science Foundation under the grants NSF-ECS-0099851, NSF-ECS-0218207, NSF-ECS-0244732, NSF-EPNES-0323379, and NSF-ECS-0424048, and a DoD-EPSCoR grant through the Office of Naval Research under the grant N000140110621.
approaches have been proposed for failure diagnosis, including fault-trees, expert systems, neural networks, fuzzy logic, bayesian networks, and analytical redundancy [16]. These are broadly categorized into non-model based (where observed behavior is matched to known failures), and model based (where observed behavior is compared against model predictions for any abnormality). For discrete event systems (DES) a certain model based approach for failure diagnosis was proposed in [22], and extended in [21, 9, 10, 8, 4, 29]. The application of DES failure diagnosis includes heating, ventilation, and air conditioning systems [23], transportation systems [13, 5], communication networks [2, 1, 14], manufacturing systems [3, 15], digital circuits [12, 26], and power systems [6].

Failure diagnosis in DES requires that once a failure occurred, it be detected and diagnosed within bounded “delay” (bounded number of transitions). This is captured by the notion of failure diagnosability introduced in [22]. Polynomial tests for diagnosability were given in [7, 28]. In [21], the notion of active failure diagnosis was introduced where control is exercised to meet given specifications while satisfying diagnosability. In [3, 15], a template based approach was developed for failure diagnosis in timed discrete event system. [20] also studied failure diagnosis in timed DES. The above approaches can be thought to be “event-based” as failure is modeled as execution of certain “faulty events”. An equivalent “state-based” approach was considered in [12, 29], where the occurrence of a failure is modeled as reaching of certain “faulty states”.

A theory for failure diagnosis of repeatedly-occurring/intermittent failures was introduced in [10]. The notion of diagnosability was extended to $[1, \infty]$-diagnosability to allow diagnosis of a failure each time it occurred. Polynomial complexity algorithms for testing $[1, \infty]$-diagnosability as well as for off-line diagnoser synthesis were presented in [10]. Algorithms of complexity that are an order lower were reported in [27]. To facilitate generalization of failure specifications, linear-time temporal logic (LTL) based specification and diagnosis of its failure was proposed in [9]. LTL can be used to specify violations of safety as well as liveness properties, allowing diagnosis of failures that have already occurred (safety violations) as well as prognosis of failures that are inevitable in future (liveness failures). [8] extended the use of LTL based specification for representing and diagnosing repeatedly-occurring/intermittent failures.

The above mentioned work dealt with centralized failure diagnosis, where a central diagnoser is responsible for failure detection and diagnosis in the system. Many large complex systems, however, are physically distributed which introduces variable communication delays and communication errors when diagnosis information collected at physically distributed sites are sent to a centralized site for analysis. Consequently, although all diagnosis information can be gathered centrally, owing to the delayed/corrupted nature of the data, a centralized failure diagnosis approach may not always be appropriate for physically distributed systems, and instead diagnosis may need to be performed decentrally at sites where diagnosis information is collected.

The problem of decentralized diagnosis was first considered as one special case of distributed diagnosis in [4]. In that paper, “lack of fully ambiguous traces” was stated as a sufficient condition for decentralized diagnosis to be equivalent to that of centralized one, and an algorithm was presented for verifying the “lack of fully ambiguous traces”. The algorithm is based upon structural properties of global (centralized) and local (decentralized) diagnosers, and has an exponential complexity in the size of the system owing to the
exponential size of the diagnosers.

In a previous work [17], we studied distributed diagnosis involving no communication among local diagnosers. A notion of codiagnosability was introduced to capture the fact that the occurrence of any failure must be diagnosed within bounded delay by at least one local diagnoser using its own observations of the system execution. Polynomial algorithms were provided for (i) testing codiagnosability, (ii) computing the delay bound of diagnosis, (iii) off-line synthesis of diagnosers, and (iv) on-line diagnosis using them.

The problem of distributed diagnosis involving communication among multiple diagnosers over unbounded-delay channels was studied in [24], where a notion of decentralized-diagnosability was introduced as an attempt to capture a property guaranteeing the detection of each fault within a bounded delay of its occurrence by one of the diagnosers. Decentralized-diagnosability requires the existence of a detection delay bound \( n \) such that if the system executes a trace \( s \) which contains a fault at least \( n \)-steps in the past, then any other trace \( t \) that is indistinguishable from \( s \) to all diagnosers must itself contain the fault. It was proved in [24] that decentralized-diagnosability is undecidable. However, we showed in [18] that the notion of decentralized-diagnosability is not strong enough to capture diagnosis in a distributed setting involving unbounded-delay communication. Instead, a notion of \( \text{joint}_{\infty} \)-diagnosability was introduced, which was shown to be equivalent to the property of codiagnosability, and therefore decidable.

In this paper, we study the distributed failure diagnosis problem under \( k \)-bounded communication delay. To formulate the way information is exchanged among local sites, we first present a dynamic system model of a general communication protocol. We then restrict our attention to a specific protocol, the immediate observation passing (iop) protocol, where each local site transmits its observations to other sites immediately after each observation, and the transmitted observation is received within at most \( k \) more event executions of the plant. The communication channel is assumed to be lossless and first-in-first-out (FIFO), but incurs a bounded delay. A similar setting has been considered for distributed control in the work of Tripakis [25].

A notion of \( \text{joint}_{k} \)-diagnosability is introduced so that any failure can be diagnosed within a bounded delay of its occurrence by one of the local sites using its own observations and the delayed observations received from other local sites communicating among each other using a general protocol. The \( \text{joint}_{k} \)-diagnosability under the immediate observation passing protocol is denoted \( \text{joint}_{k}^{\text{iop}} \)-diagnosability. We construct models for \( k \)-bounded communication delay, and use them to extend the system and non-fault specification models for capturing the effect of bounded-delay communication. Using the extended system and specification models, the distributed diagnosis problem under the immediate observation passing protocol is then converted to a decentralized diagnosis problem of [17]. Results from [17] are applied for verifying \( \text{joint}_{k}^{\text{iop}} \)-diagnosability, and synthesizing local diagnosers. A way by which complexity of testing \( \text{joint}_{k}^{\text{iop}} \)-diagnosability and of on-line diagnosis can be reduced is presented. Finally, we compare the notions of diagnosability, codiagnosability, and \( \text{joint}_{k}^{\text{iop}} \)-diagnosability.

The rest of the paper is organized as follows. Section 2 presents preliminary notations. Section 3 discusses communication protocols for distributed failure diagnosis. In Section 4, we first present the communication delay models, and then combine them with the original system/specification models to obtain extended system/specification models. Using the extended models, Section 5 provides the definition of \( \text{joint}_{k} \)-diagnosability, and shows that
for the immediate observation passing protocol, joint$^{top}_k$-diagnosability can be reduced into an instance of codiagnosability. In Section 6, we present an algorithm for verifying joint$^{top}_k$-diagnosability. The synthesis of local diagnosers is discussed in Section 7. Section 8 compares the notions of diagnosability, codiagnosability, and joint$^{top}_k$-diagnosability. Conclusions and future work are presented in Section 9.

2 Notation and Preliminaries

In this section, we give the system model and present some necessary notations and preliminaries. For more details on DES theory, readers are referred to [19, 11].

Given an event set $\Sigma$, $\Sigma^*$ denotes the set of all finite length event sequences over $\Sigma$, including the zero length event sequence $\varepsilon$. A member of $\Sigma^*$ is a trace and a subset of $\Sigma^*$ is a language. Given a language $L \subseteq \Sigma^*$, it is said to be prefix-closed if $L = pr(L)$, where $pr(L) := \{ s \in \Sigma^* | \exists t \in \Sigma^* \text{ s.t. } st \in L \}$. A DES is modeled as a finite automaton $G = (X, \Sigma, \alpha, x_0)$, where $X$ is the set of states, $\Sigma$ is the finite set of events, $x_0 \in X$ is the initial state, and $\alpha : X \times \Sigma \rightarrow 2^X$ is the transition function with $\Sigma := \Sigma \cup \{ \varepsilon \}$. $G$ is said to be deterministic if $|\alpha(\cdot, \cdot)| \leq 1$ and $|\alpha(\cdot, \varepsilon)| = 0$; otherwise, it is called nondeterministic.

Given a state $x \in X$, the $\varepsilon$-closure of $x$, denoted $\varepsilon^*_G(x) \subseteq X$, includes all states that can be reached from state $x$ by zero or more $\varepsilon$ transitions, and is recursively defined as: $x \in \varepsilon^*_G(x)$; $x' \in \varepsilon^*_G(x) \Rightarrow \alpha(x', \varepsilon) \subseteq \varepsilon^*_G(x)$. The domain of the state transition function $\alpha$ can be extended from $X \times \Sigma$ to $X \times \Sigma^*$ recursively as follows:

$$\forall x \in X, s \in \Sigma^*, \sigma \in \Sigma : \alpha(x, \varepsilon) = \varepsilon^*_G(x); \alpha(x, s\sigma) = \varepsilon^*_G(\alpha(\alpha(x, s), \sigma)).$$

The generated language of $G$ is given by, $L(G) := \{ s \in \Sigma^* | \alpha(x_0, s) \neq \emptyset \}$, which includes all traces that can be executed in $G$ starting from its initial state. A path in $G$ is a sequence of transitions $(x_1, \sigma_1, x_2, \cdots, \sigma_{n-1}, x_n)$, where $\sigma_i \in \Sigma$ and $x_{i+1} \in \alpha(x_i, \sigma_i)$ for all $i \in \{1, \cdots, n-1\}$. Such a path is called a cycle if $x_1 = x_n$.

Given two automata $G_1 = (X_1, \Sigma_1, \alpha_1, x_{0,1})$ and $G_2 = (X_2, \Sigma_2, \alpha_2, x_{0,2})$, the synchronous composition of $G_1$ and $G_2$ is defined as, $G_1||G_2 = (X_1 \times X_2, \Sigma_1 \cup \Sigma_2, \alpha, (x_{0,1}, x_{0,2}))$, where $\forall (x_1, x_2) \in X_1 \times X_2, \sigma \in \Sigma_1 \cup \Sigma_2$,

$$\alpha((x_1, x_2), \sigma) = \begin{cases} \alpha_1(x_1, \sigma) \times \alpha_2(x_2, \sigma) & \text{if } \sigma \in \Sigma_1 \cap \Sigma_2; \\ \alpha_1(x_1, \sigma) \times \{ x_2 \} & \text{if } \sigma \in \Sigma_1 - \Sigma_2; \\ \{ x_1 \} \times \alpha_2(x_2, \sigma) & \text{if } \sigma \in \Sigma_2 - \Sigma_1. \end{cases}$$

When the system execution is observed by a global observer, we can define a global observation mask, $M : \Sigma \rightarrow \overline{\Lambda}$ with $M(\varepsilon) = \varepsilon$, where $\overline{\Lambda} := \Lambda \cup \{ \varepsilon \}$ and $\Lambda$ is the set of observed symbols. The definition of $M$ can be extended from events to event sequences inductively as follows:

$$M(\varepsilon) = \varepsilon; \forall s \in \Sigma^*, \sigma \in \Sigma, M(s\sigma) = M(s)M(\sigma).$$

Given an automaton $G$ and mask $M$, $M(G)$ is the automaton $G$ with each transition $(x, \sigma, x')$ of $G$ replaced by $(x, M(\sigma), x')$. Then, $L(M(G)) = M(L(G))$, where $M(L(G)) := \{ M(t) \mid t \in L(G) \}$. The local observation mask for a site $i$ is defined as $M_i : \overline{\Sigma} \rightarrow \overline{\Lambda}_i$ ($i \in I_M = \cdots$}
\{1, \cdots, m\}\} with \(M_i(\epsilon) = \epsilon\), where \(m\) is the number of local observers, \(\Lambda_i := \Lambda_i \cup \{\epsilon\}\) and \(\Lambda_i\) is the set of locally observed symbols.

Let \(G = (X, \Sigma, \alpha, x_0)\) and \(R = (Y, \Sigma, \beta, y_0)\) represent the plant and the specification models, respectively. Then the generated language of the plant, \(L = L(G)\), represents the feasible behavior of the system, whereas the specification language, \(K = L(R)\), represents the fault-free behavior of the system. The completed specification model \(\overline{R}\) is constructed from \(R\) by adding an additional failure state \(F\), which when reached due to the execution of a trace feasible in the system indicates the occurrence of a failure. Formally, \(\overline{R} := (Y, \Sigma, \overline{\beta}, y_0)\), where \(\overline{Y} := Y \cup \{F\}\), and \(\overline{\beta}\) is defined as: \(\forall \overline{y} \in \overline{Y}, \sigma \in \Sigma,\)

\[
\overline{\beta}(\overline{y}, \sigma) := \begin{cases} 
\beta(\overline{y}, \sigma), & \text{if } [\overline{y} \in Y] \land [\beta(\overline{y}, \sigma) \neq \emptyset], \\
F, & \text{if } [\overline{y} = F] \lor [\beta(\overline{y}, \sigma) = \emptyset].
\end{cases}
\]

The failure diagnosis problem is to detect and diagnose any failure behavior in \(L - K\) within a bounded delay of its execution. Execution of any such behavior is viewed as the occurrence of a fault. When there does not exist any communication among the local diagnoser sites, it is called a decentralized failure diagnosis problem; otherwise, it is called a distributed failure diagnosis problem. In [17], we studied the decentralized failure diagnosis problem having the system architecture as shown in Figure 1, where it is assumed without loss of any generality that there are two local diagnosers.

![Figure 1: Architecture of a decentralized failure diagnosis system](image)

The following notion of codiagnosability was introduced in [17] to capture the property of diagnosis of any fault within bounded delay of its occurrence by one of the local diagnosers in a decentralized setting.

**Definition 1** [17] Let \(L\) be the prefix-closed language generated by a system and \(K\) be a prefix-closed specification language contained in \(L\) (\(K \subseteq L\)). Assume there are \(m\) local sites with observation masks \(M_i : \Sigma^* \rightarrow \Lambda_i^*\) \((i \in I = \{1, \cdots, m\})\). \((L, K)\) is said to be codiagnosable with respect to \(\{M_i\}\) if

\[
(\exists n \in \mathbb{N})(\forall s \in L - K)(\forall st \in L, |t| \geq n \text{ or } st \text{ deadlocks}) \Rightarrow \\
(\exists i \in I)(\forall u \in L, M_i(u) = M_i(st) \Rightarrow u \in L - K).
\]
3 Communication Protocols

Figure 2 shows the architecture of a distributed failure diagnosis system with two local sites. Site $i$ contains three modules: observation mask $M_i$, communication protocol $i$, and diagnoser $i$. The observation mask module $M_i$ is a map $M_i : \Sigma^* \rightarrow \Lambda^*$. The protocol module for site $i$ decides how to share information among various diagnosers. The diagnoser module for site $i$ performs failure diagnosis based on the local observations and the communicated information received from other sites $j$ ($j \neq i$). Information is communicated among various sites over communication channels that are loss-free and order-preserving but introduce bounded delays.

![Figure 2: Architecture of a distributed failure diagnosis system](image)

A communication protocol is a causal (prefix-preserving) map from history of all information received to history of all information transmitted. The communication protocol at site $i$ can be implemented as a dynamical system as shown in Figure 3.

![Figure 3: Model of a general communication protocol](image)

The inputs to this dynamical system consist of the local observations $\lambda_i \in \Lambda_i$, and the communicated informations from each diagnoser $\{e_{ji}|j \neq i\}$. The output of this dynamical system is the information to be transmitted to other diagnosers $\{e_{ij}|j \neq i\}$. The protocol maintains an internal state $e_i$, called the protocol state. The formats of $e_i$, $e_{ji}$, and $e_{ij}$ ($j \neq i$) are specific to a protocol. Formally, a general communication protocol is given by $P_i^{\text{gen}} := \{P_i^{\text{gen}}|i \in I\}$, where each $P_i^{\text{gen}}$ is modeled by a set of maps $\{f_i, \{g_{ij}|j \neq i\}\}$ as follows:

$$P_i^{\text{gen}}: \begin{cases} e_i = f_i(e_i, \lambda_i, \{e_{ji}|j \neq i\}) & \text{(protocol state update)}, \\ e_{ij} = g_{ij}(e_i, \lambda_i, \{e_{ji}|j \neq i\}) & \text{(protocol output computation)} \end{cases}$$

(1)

$f_i$ is the protocol state update map at site $i$, which updates the protocol state based on its current value and newly received information, $\lambda_i$ or $\{e_{ji}|j \neq i\}$. Events in $\{\lambda_i\} \cup \{e_{ji}, j \neq i\}$

6
$\{e_{ij}, j \neq i\}$ occur asynchronously.) $g_{ij}$ is the protocol-output map at site $i$, which determines the information to be transmitted to site $j$ ($j \neq i$). The set of protocols of the form specified in (1) is denoted $\mathcal{P}^{\text{gen}}$. The setting of decentralized diagnosis involving no communication can be represented by a “null-communication” protocol, $\mathcal{P}^\theta$, for which the output is always null.

If a protocol allows diagnosers to transmit only their local observations, it is called an observation passing protocol, denoted $\mathcal{P}^{\text{op}} := \{P^{\text{op}}_i, i \in I\}$. The dynamic model of $P^{\text{op}}_i$ is captured by a set of maps $\{f_i, \{g_{ij}, j \neq i\}\}$ defined as follows. (“\" denotes the “after” operation.)

$$P^{\text{op}}_i : \left\{ \begin{array}{ll} e_i = e_i \lambda_i \setminus \{e_{ij}, j \neq i\} & \text{(protocol state update)}, \\
\quad e_{ij} = g_{ij}(e_i, \lambda_i) \leq e_i \lambda_i & \text{(protocol output computation)}, \end{array} \right. \quad (2)$$

where the protocol state $e_i$ is a “vector” whose $j^{\text{th}}$ entry stores observations that are not yet transmitted to site $j$, and $e_{ij}$ is the newly transmitted observation to site $j$, which is a prefix of $e_i \lambda_i$, the concatenation of the observation trace not yet transmitted and the newly arrived observation. The class of protocols of the form specified in (2) comprise the class of observation passing protocols, denoted $\mathcal{P}^{\text{op}}$.

When $g_{ij}(e_i, \lambda_i) = e_i \lambda_i = e \lambda_i = \lambda_i$ in (2), the protocol model simplifies to the one given in (3), and the corresponding protocol is called the immediate observation passing protocol, denoted $\mathcal{P}^{\text{imop}} := \{P^{\text{imop}}_i, i \in I\}$, where $P^{\text{imop}}_i$ is defined as follows:

$$P^{\text{imop}}_i : \left\{ \begin{array}{ll} e_i = \epsilon & \text{(protocol state update)}, \\
\quad e_{ij} = \lambda_i & \text{(protocol output computation)}. \end{array} \right. \quad (3)$$

In this protocol any local observation is transmitted immediately to other sites, and there is no observation that is not transmitted but stored as the protocol state. Therefore, the protocol state update map $f_i$ is trivial, and the information to be transmitted $e_{ij}$ simply equals the local observation $\lambda_i$ in the protocol output map $g_{ij}$. The distributed diagnosis architecture under the immediate observation passing protocol is shown in Figure 4(a), and a rearrangement of the same is shown in Figure 4(b).

#### 4 Communication & Extended System/Spec. Models

In this section, we model the effect of communication delay when using $\mathcal{P}^{\text{imop}}$-based distributed diagnosis, and introduce the extended system and specification models. The idea is to use the extended models to convert the $\mathcal{P}^{\text{imop}}$-based distributed failure diagnosis problem to an instance of a decentralized failure diagnosis problem, where no communication is exchanged among local diagnosers. The former problem can then be solved using the methods for the latter problem developed in [17].

In a channel with $k$-bounded communication delay, there can be at most $k$ events executed by the plant between the transmission and the reception of a message on the channel. Since the operations of masking and delaying can be interchanged, the behavior under the block diagram of Figure 4(b) is equivalent to that of Figure 5(a), which can be rearranged to obtain the block diagram of Figure 5(b).
Figure 4: Distributed diagnosis architecture under protocol $P^{iop}$

Figure 5: Equivalent system architecture under protocol $P^{iop}$
It is clear by comparing Figure 1 and Figure 5(b) that \( P_{\text{top}} \)-based distributed diagnosis can be converted to a decentralized diagnosis having an extended plant \( G^k \), and local diagnosers having the extended observation masks \( \{ M_i \} \). The extended plant is given by \( G^k = G || C^k_{12} || C^k_{21} \), where \( C^k_{ij} \) models the \( k \)-bounded delaying and masking operation. We call \( C^k_{ij} \) to be the \( k \)-delaying\&masking model. The extended plant \( G^k \) "generates" events in \( \Sigma \cup \Lambda_1 \cup \Lambda_2 \), which are observed by diagnoser \( i \) through an extended observation mask \( M_i : \Sigma \cup \Lambda_1 \cup \Lambda_2 \rightarrow \lambda_i \cup \lambda_2 \). \( M_i \) is same as \( M_i \) for events in \( \Lambda_i \), whereas it acts as an identity mask for events in \( \Lambda_j \) \( (j \neq i) \) and blocks the events in \( \Lambda_i \). Formally, it is defined as follows:

\[
M_i(\sigma) := \begin{cases} 
M_i(\sigma), & \sigma \in \Sigma; \\
\sigma, & \sigma \in \Lambda_j \ (j \neq i); \\
\epsilon, & \sigma \in \Lambda_i. 
\end{cases} \tag{4}
\]

The \( k \)-delaying\&masking model \( C^k_{ij} \) can be modeled as a finite automaton, which evolves whenever a new event occurs in the plant or a transmitted observation is delivered to a destination diagnoser, and such arrival and departure of events occur asynchronously. The state of the model is portion of the event trace executed by the plant whose observed value is pending to be delivered to a destination diagnoser. Formally, the \( k \)-delaying\&masking model from diagnoser \( i \) to diagnoser \( j \) \( (i \neq j) \) is defined as,

\[
C^k_{ij} = (Z^k_{ij}, \Sigma \cup \Lambda_i, \lambda^k_{ij}, z_0).
\]

\( Z^k_{ij} \) is the set of states, which are represented by the event traces executed in the plant but their observed values not yet received by the destination diagnoser. For \( z \in Z^k_{ij} \), \( |z| \) denotes the length of trace \( z \). Since the message arrivals and departures in a communication channel occur asynchronously, for a \( k \)-delaying\&masking model, we have \( |z| \leq k + 1 \). \( \Sigma \cup \Lambda_i \) is the event set, where \( \Sigma \) is the set of input events and \( \Lambda_i \) is the set of output events. Without loss of generality, we assume that \( \Sigma \cap \Lambda_i = \emptyset \) and \( \Lambda_i \cap \Lambda_j = \emptyset \) \( (i \neq j) \) (otherwise, we can simply rename some of the symbols). \( z_0 = \epsilon \) is the initial state. The transition function \( \lambda^k_{ij} \) is defined as follows.

- "Arrival" due to an event execution in the plant: \( \forall z \in Z^k_{ij}, \forall \sigma \in \Sigma, \text{ if } |z| \leq k, \text{ then } \lambda^k_{ij}(z, \sigma) = z\sigma, \)

- "Departure" due to a reception at the destination diagnoser: \( \forall z \in Z^k_{ij}, \forall \lambda_i \in \Lambda_i, \text{ if } M_i(\text{head}(z)) = \lambda_i, \text{ then } \lambda^k_{ij}(z, \lambda_i) = z\setminus\text{head}(z), \)

- Undefined, otherwise,

where \( \text{head}(z) \) is the first event in trace \( z \), and the after operator \( \setminus \) in \( z\setminus\text{head}(z) \) returns the trace after removing the initial event \( \text{head}(z) \) from the trace \( z \). The transition function \( \lambda^k_{ij} \) can be understood as follows. The state \( z \) is extended at the “tail” upon each plant execution \( \sigma \in \Sigma \) (provided the current length does not exceed the delay bound \( k \)), while shortened at the “head” upon each reception \( \lambda_i \in \Lambda_i \). It follows from the above definition that the \( k \)-delaying\&masking model \( C^k_{ij} \) is a subgraph of the \( (k+1) \)-delaying\&masking model \( C^{k+1}_{ij} \).
Having introduced the model $C^k_{ij}$, we next introduce several “extended” models (extended to capture the effect of $k$-delaying&masking). These extended models are obtained by performing a synchronous composition between an “unextended” original model and certain $k$-delaying&masking models.

- **extended plant model**: $G^k = G^{k}_{12} || C^k_{21}$.

- **extended specification model**: $R^k = R^{k}_{12} || C^k_{21}$, which consists of traces in extended plant $G^k$ whose projection over $\Sigma$ do not violate the original specification $R$.

- **refined extended specification model**: $\overline{R}^k = \overline{R}^{k}_{12} || C^k_{21}$, where $\overline{R}$ is the completed specification model with an additional failure state “$F$”.

- **refined extended plant model**: $\overline{G}^k = G^{k}_{12} || \overline{R}^{k}_{21}$, which generates the same language as $G^k$, but the execution of those traces that are “faulty” reaches a state with second coordinate “$F$”.

- **extended local specification model**: $R^k_{i} = R^{k}_{i} || C^k_{ji}$.

- **refined extended local specification model**: $\overline{R}^k_{i} = \overline{R}^{k}_{i} || C^k_{ji}$.

Note that in the above construction, any event in the set $\Sigma$ is synchronized among all participating components, while any event in the set $\Lambda_1 \cup \Lambda_2$ is executed asynchronously.

The following example illustrates the construction of $k$-delaying&masking models $C^k_{ij}$, extended plant model $G^k$, extended specification model $R^k$, and extended local specification models $R^k_{i}$.

**Example 1** A plant model $G$ and a specification model $R$ are shown in Figure 6(a) and Figure 6(b), respectively, with $L(G) = pr(aabc^* + baac^*)$ and $L(R) = pr(aabc^*)$. Suppose the observation masks of two local sites are defined as follows:

- $M_1(a) = a'$, $M_1(b) = M_1(c) = \epsilon$, and
- $M_2(b) = b'$, $M_2(a) = M_2(c) = \epsilon$.

For delay = 1, Figure 6(c) and Figure 6(d) show the models $C^k_{12}$ and $C^k_{21}$ respectively. The two models have the same structure and the same set of states, while some of the transitions are labeled differently. If we follow the trace $aba'$ in the first model $C^k_{12}$, the states $\epsilon$, $a$, $ab$ and $b$ are traversed sequentially. This corresponds to the situation in which site 1 sends out its observation $a'$ to site 2 after the occurrence of $ab$ in the plant, whereas event $b$ is executed in the plant but its observation is not yet received at site 2.

By taking the synchronous composition between the original system/specification models and the $k$-delaying&masking models, we obtain the refined extended plant model $\overline{G}^k = \overline{G}^k_{12} || \overline{R}^k_{12} || C^k_{12} || C^k_{21}$ and the extended specification model $\overline{R}^k = \overline{R}^k_{12} || C^k_{21}$ as shown in Figure 6(e). The extended local specification models $\overline{R}^k_{1} = \overline{R}^k_{1} || C^k_{12}$ and $\overline{R}^k_{2} = \overline{R}^k_{2} || C^k_{12}$ are shown in Figure 6(f) and Figure 6(g), respectively.

For delay = 2, the communication delay models $C^k_{12}$ and $C^k_{21}$, refined extended plant model $\overline{G}^k$, extended specification model $\overline{R}^k$, and extended local specification models $\overline{R}^k_{1}$ and $\overline{R}^k_{2}$ are shown in Figure 7.
Figure 6: Illustrating Example 1: System models with delay $k = 1$
Figure 7: Illustrating Example 1: System models with delay $k = 2$
Let us define a projection $\Pi_\Sigma : \Sigma \cup \Lambda_1 \cup \Lambda_2 \to \Sigma$ as follows:

$$
\forall \sigma \in \Sigma \cup \Lambda_1 \cup \Lambda_2, \Pi_\Sigma(\sigma) := \begin{cases} 
\sigma, & \sigma \in \Sigma; \\
\epsilon, & \sigma \in \Lambda_1 \cup \Lambda_2.
\end{cases}
$$

(5)

This projection can be inductively extended from event to event traces to obtain, $\Pi_\Sigma : (\Sigma \cup \Lambda_1 \cup \Lambda_2)^* \to \Sigma^*$, as follows:

$$
\Pi_\Sigma(\epsilon) = \epsilon; \ \forall s \in (\Sigma \cup \Lambda_1 \cup \Lambda_2)^*, \sigma \in \Sigma \cup \Lambda_1 \cup \Lambda_2, \Pi_\Sigma(s\sigma) = \Pi_\Sigma(s)\Pi_\Sigma(\sigma).
$$

The inverse projection of $\Pi_\Sigma$, $\Pi_\Sigma^{-1} : \Sigma^* \to (\Sigma \cup \Lambda_1 \cup \Lambda_2)^*$, is defined as follows:

$$
\forall u \in \Sigma^*, \Pi_\Sigma^{-1}(u) := \{s \in (\Sigma \cup \Lambda_1 \cup \Lambda_2)^* \mid \Pi_\Sigma(s) = u\}.
$$

(6)

**Lemma 1** Given a plant $G$ and a specification model $R$ with $L(R) \subseteq L(G)$, let $G^k$ and $R^k$ be the extended plant model and the extended specification model, respectively. Then,

$$
\forall s \in L(R^k), t \in (\Lambda_1 \cup \Lambda_2)^* : st \in L(G^k) \Rightarrow st \in L(R^k).
$$

**Proof:** Since $G^k = G\|C^k_{12}\|C^k_{21}, R^k = R\|C^k_{12}\|C^k_{21}$, and $L(R) \subseteq L(G)$, it follows that $L(R^k) \subseteq L(G^k)$. So, $s \in L(G^k)$ for any $s \in L(R^k)$. Since events in $\Lambda$ are only executed by $C^k_{ij}$ ($i, j \in 1, 2, i \neq j$), it follows that if $t \in (\Lambda_1 \cup \Lambda_2)^*$ is executable beyond $s$ in $G^k = G\|C^k_{12}\|C^k_{21}$, then $t$ is executable beyond $s$ in $C^k_{12}\|C^k_{21}$. Hence, $t$ is executable beyond $s$ in $R^k = R\|C^k_{12}\|C^k_{21}$ as well. 

**Proposition 1** Given a plant $G$ and a specification model $R$ with $L(R) \subseteq L(G)$, let $G^k$ and $R^k$ be the extended plant model and the extended specification model, respectively, and $\Pi_\Sigma$ and $\Pi_\Sigma^{-1}$ be the projection and the inverse projection as defined in (5) and (6), respectively. Then, the original system behaviors and the extended system behaviors have the following relationship:

- $\forall s \in L(G) : \Pi_\Sigma(s) \in L(G),$
- $\forall s \in L(R) : \Pi_\Sigma(s) \in L(R),$
- $\forall s \in L(R) : \Pi_\Sigma^{-1}(s) \cap L(G^k) \subseteq L(R^k).

**Proof:** We prove the above assertions inductively on the length of trace $s$, denoted $|s|$. For the first assertion, if $|s| = 0$, i.e., $s = \epsilon$, then it is obvious that $\Pi_\Sigma(s) = \epsilon \in L(G)$. Assume that the first assertion holds for any trace $s \in L(G^k)$ with $|s| = n$. Then, consider trace $s\sigma \in L(G^k)$ with $|s\sigma| = n$ and $\sigma \in \Sigma \cup \Lambda_1 \cup \Lambda_2$. If $\sigma \in \Lambda_1 \cup \Lambda_2$, then $\Pi_\Sigma(s\sigma) = \Pi_\Sigma(s) \in L(G)$ from the hypothesis. On the other hand, if $\sigma \in \Sigma$, then $\Pi_\Sigma(s\sigma) = \Pi_\Sigma(s)\sigma$. Since all events in set $\Sigma$ are executed synchronously in $G^k$ among $G$, $C^k_{12}$, and $C^k_{21}$, it follows that $\sigma$ is executable in $G$ after trace $\Pi_\Sigma(s)$, which implies that $\Pi_\Sigma(s\sigma) = \Pi_\Sigma(s)\sigma \in L(G)$. Thus, the first assertion holds. The second assertion can be proved similarly.

For the third assertion, if $|s| = 0$, i.e., $s = \epsilon$, then $\Pi_\Sigma^{-1}(s) \cap L(G^k) = (\Lambda_1 \cup \Lambda_2)^* \cap L(G^k) \subseteq L(R^k)$, where the last inclusion follows from Lemma 1. Assume that the third assertion holds for $|s| = n$. For any trace $s\sigma \in L(R)$ with $|s| = n$ and $\sigma \in \Sigma$, we have that

$$
\Pi_\Sigma^{-1}(s\sigma) \cap L(G^k) = \{t_1\sigma t_2 \mid t_1 \in L(R^k), \Pi_\Sigma(t_1) = s, t_2 \in (\Lambda_1 \cup \Lambda_2)^*, t_1\sigma t_2 \in L(G^k)\}.
$$
Since $L(G^k)$ is prefix-closed, it follows that $t_1\sigma \in G^k$. I.e., $\sigma$ is enabled after $t_1$ in $G^k = G[C_{12}^k][C_{21}^k]$. Since $R^k = R[C_{12}^k][C_{21}^k]$ and $\sigma$ is enabled after $\Pi(\Sigma)(t_1) = s$ in $R$, it follows from the synchronization of $s$ in $G^k$ and $R^k$ that $\sigma$ is enabled after $t_1$ in $R^k$ as well. I.e., $t_1\sigma \in L(R^k)$. Then, for any $t_1\sigma t_2 \in \Pi^{-1}(s\sigma) \cap L(G^k)$ with $t_2 \in (A_1 \cup A_2)^*$, it follows from Lemma 1 that $t_1\sigma t_2 \in L(R^k)$. This completes the proof for the third assertion.

From Proposition 1, we can get the following corollary.

**Corollary 1** Given a plant $G$ and a specification model $R$ with $L(R) \subseteq L(G)$, let $G^k$ and $R^k$ be the extended plant model and the extended specification model, respectively, and $\Pi(\Sigma)$ and $\Pi^{-1}$ be the projection and the inverse projection defined in (5) and (6), respectively. Then,

- $\forall s \in L(G) - L(R) : \Pi^{-1}(s) \cap L(G^k) \subseteq L(G^k) - L(R^k)$, and
- $\forall s \in L(G^k) - L(R^k) : \Pi(s) \in L(G) - L(R)$.

**Proof:** Suppose for the purpose of contradiction that there exist $s \in L(G) - L(R)$ and $t \in (\Sigma \cup A_1 \cup A_2)^*$ such that $t \in \Pi^{-1}(s) \cap L(G^k)$, but $t \notin L(G^k) - L(R^k)$, i.e., $t \notin L(R^k)$. It follows from the second assertion of Proposition 1 that $\Pi(\Sigma)(t) = s \in L(R)$, which contradicts the condition $s \in L(G) - L(R)$. This proves the first assertion. The second assertion can be proved similarly from the third assertion of Proposition 1.

In the following proposition, we present a relationship between languages $L(G^k)$ and $L(R^k)$, and languages $L(G^{k+1})$ and $L(R^{k+1})$.

**Proposition 2** Given a plant $G$ and a specification model $R$ with $L(R) \subseteq L(G)$, consider $G^k = G[C_{12}^k][C_{21}^k]$ and $R^k = R[C_{12}^k][C_{21}^k]$. Then, we have that

- $L(G^k) \subseteq L(G^{k+1})$, $L(R^k) \subseteq L(R^{k+1})$, $L(R^k) \subseteq L(R^{k+1})$, and
- $L(G^k) - L(R^k) \subseteq L(G^{k+1}) - L(R^{k+1})$.

**Proof:** Since $C_{ij}^k$ is a subgraph of $C_{ij}^{k+1}$, all system models obtained by composing with $\{C_{ij}^k\}$ are subgraphs of corresponding system models obtained by composing with $\{C_{ij}^{k+1}\}$, implying the correctness of the first assertion.

To show the second assertion, suppose for the sake of contradiction that

$$\exists s : [s \in L(G^k) - L(R^k)] \land [s \notin L(G^{k+1}) - L(R^{k+1})].$$

Since $s \in L(G^k) \subseteq L(G^{k+1})$, it follows that if $s \notin L(G^{k+1}) - L(R^{k+1})$, then $s \in L(R^{k+1})$, which combined with the second assertion of Proposition 1 implies that $\Pi(\Sigma)(s) \in L(R)$. This leads to a contradiction that since $s \in L(G^k) - L(R^k)$, and so it follows from the second assertion of Corollary 1 that $\Pi(\Sigma)(s) \in L(G) - L(R)$. 

\[\qed\]
5 Joint$_k$-Diagnosability

In this section, we introduce the notion of joint$_k$-diagnosability, which captures the property of a system in which any failure can be diagnosed within a bounded delay of its occurrence by one of the local sites using its own observations and the delayed observations received from other local sites communicating using a general communication protocol $P^\text{gen} \in \mathcal{P}^\text{gen}$. When the communication is $P^\text{gen}$-based, the notion of distributed diagnosability is denoted by joint$^\text{gen}$$_k$-diagnosability. The main result of the section is that joint$^\text{gen}$$_k$-diagnosability is an instance of codiagnosability.

Let $E_{ij}$ ($i \neq j, i, j \in I$) denote the set of output symbols communicated from site $i$ to site $j$. Then any symbol received at site $i$ lies in the set $\Lambda_i \cup E_{ji}$, called the set of aggregate observation symbols at site $i$. Assuming local sites commute over loss-free, FIFO, and $k$-bounded delay channels under a general communication protocol $P^\text{gen} \in \mathcal{P}^\text{gen}$, the execution of a trace $s$ by the system results in the reception at site $i$ of a sequence of observation symbols in $\Lambda_i$ interleaved with a sequence of communication symbols in $\cup_{j \neq i} E_{ji}$. Due to the asynchronous nature of the communication channels and the introduction of bounded but random delays by them, execution of a trace $s$ by the system can result in the reception of one of many possible sequences of observed and communicated symbols at site $i$. Also, any such sequence of observed and communicated symbols arrives in its entirety at site $i$ within a bounded-delay of the execution of trace $s$.

To characterize the set of sequences of aggregate observations received at site $i$ under protocol $P^\text{gen} \in \mathcal{P}^\text{gen}$ immediately at the time the system has executed a trace $s$, we define a map $O^\text{gen,k}_i : \Sigma^* \to 2^{(\Lambda_i \cup j \neq i E_{ji})^*}$, where $k$ is the communication delay bound. We call this map to be the $P^\text{gen}$-based aggregate observations map for site $i$ under $k$-bounded communication delay. Similarly, we can define $O^\text{op,k}_i$ (resp., $O^\text{gen,k}_i$ and $O^\text{gen,0}_i$) to be the $P^\text{op}$ (resp., $P^\text{op}$ and $P^\text{0}$)-based aggregate observations maps for site $i$ under $k$-bounded communication delay. Since $P^\text{0}$ represents the “null communication” protocol, it is obvious that $O^\text{gen,0}_i(s) = \{M_i(s)\}$ for any $s \in L(G)$. For protocol $P^\text{op}$, the aggregate observations map $O^\text{op,k}_i$ can be formally defined through the extended observation mask $\mathcal{M}_i$ as follows.

**Definition 2** Given a plant $G$, let $\mathcal{G}^k = G || C^k_{i2} || C^k_{21}$ be the extended plant model, where $C^k_{ij}$ ($i, j \in \{1, 2\}, i \neq j$) is the $k$-delaying&masking model from site $i$ to site $j$. Consider the extended observation mask $\mathcal{M}_i : \Sigma \cup \Lambda_1 \cup \Lambda_2 \to \overline{\Lambda}_1 \cup \overline{\Lambda}_2$ ($i \in \{1, 2\}$), and the inverse projection $\Pi_{\Sigma}^{-1} : \Sigma^* \to (\Sigma \cup \Lambda_1 \cup \Lambda_2)^*$. The $P^\text{op}$-based aggregate observations map for site $i$ under $k$-bounded communication delay, $O^\text{op,k}_i : \Sigma^* \to 2^{(\cup_{j \neq i} \Lambda_j)^*}$, is given by:

$$\forall s \in L(G) : O^\text{op,k}_i(s) := \mathcal{M}_i(\Pi_{\Sigma}^{-1}(s) \cap L(\mathcal{G}^k)).$$

Two traces $s$ and $t$ are indistinguishable if they possess a common aggregate observations sequence. This is captured by the following definition of indistinguishability predicate over the set of traces.

**Definition 3** Given a plant $G$, let $O^\text{gen,k}_i : \Sigma^* \to 2^{(\Lambda_i \cup j \neq i E_{ji})^*}$ be the aggregate observations map for site $i$. Then the $P^\text{gen}$-based indistinguishability predicate for site $i$ under $k$-bounded
communication delay is defined as follows:

\[
\forall s, t \in L(G), \mathcal{T}_i^{gen,k}(s, t) := \begin{cases} 
1 & O_i^{gen,k}(s) \cap O_i^{gen,k}(t) \neq \emptyset \\
0 & \text{otherwise.}
\end{cases} \tag{7}
\]

The \(P^{op}(\text{resp., } P^{\text{pop}} \text{ and } P^{\emptyset})\)-based indistinguishability predicate for site \(i\) under \(k\)-bounded communication delay, denoted \(\mathcal{Y}_i^{pop,k}\) (resp., \(\mathcal{Y}_i^{\emptyset}\)), are defined similarly by replacing \(O_i^{gen,k}\) in (7) with \(O_i^{op,k}\) (resp., \(O_i^{\text{pop,k}}\) and \(O_i^{\emptyset}\)).

The following proposition shows the relationship between indistinguishability predicates \(\mathcal{Y}_i^{\emptyset}\) and \(\mathcal{Y}_i^{\text{pop,k}}\), and observation masks \(\{M_i\}\) and \(\{\mathcal{M}_i\}\).

**Proposition 3** Given a plant \(G\), and the extended plant model \(G^k\), let \(\mathcal{Y}_i^{\text{pop,k}}\) (resp., \(\mathcal{Y}_i^{\emptyset}\)) be the \(P^{\text{pop}}\) (resp., \(P^{\emptyset}\))-based indistinguishability predicates for site \(i\) under \(k\)-bounded communication delay, \(M_i : \Sigma \rightarrow \mathcal{X}_i\) be the observation mask for site \(i\), and \(\mathcal{M}_i : \Sigma \cup \Lambda_1 \cup \Lambda_2 \rightarrow \mathcal{X}_1 \cup \mathcal{X}_2\) be the extended observation mask for site \(i\). Then, we have that

- \(\forall s, t \in L(G): [\mathcal{Y}_i^{\emptyset}(s, t) = 1] \iff [M_i(s) = M_i(t)],\) and
- \(\forall s, t \in L(G): [\mathcal{Y}_i^{\text{pop,k}}(s, t) = 1] \iff \exists s' \in \Pi_{\Sigma}^{-1}(s) \cap L(G^k), t' \in \Pi_{\Sigma}^{-1}(t) \cap L(G^k) : \mathcal{M}_i(s') = \mathcal{M}_i(t').\)

where \(\Pi_{\Sigma}^{-1} : \Sigma^* \rightarrow (\Sigma \cup \Lambda_1 \cup \Lambda_2)^*\) is the inverse projection defined in (6).

**Proof:** Since \(O_i^{\emptyset}(s) = \{M_i(s)\}\) for any \(s \in L(G)\), the first assertion readily follows from the definition of \(\mathcal{Y}_i^{\emptyset}\).

According to Definition 3, \(\mathcal{Y}_i^{\text{pop,k}}(s, t) = 1\) if and only if \(O_i^{\text{pop,k}}(s) \cap O_i^{\text{pop,k}}(t) \neq \emptyset\). Since \(O_i^{\text{pop,k}}(s) = \mathcal{M}_i(\Pi_{\Sigma}^{-1}(s) \cap L(G^k))\) and \(O_i^{\text{pop,k}}(t) = \mathcal{M}_i(\Pi_{\Sigma}^{-1}(t) \cap L(G^k))\), it follows that there exist \(s'\) and \(t'\) in \(L(G^k)\) such that \([\Pi_{\Sigma}(s') = s] \land [\Pi_{\Sigma}(t') = t] \land [\mathcal{M}_i(s') = \mathcal{M}_i(t')]\), proving the correctness of the second assertion.

Using the notion of indistinguishability predicate, we next give the definition of joint \(k\)-diagnosability.

**Definition 4** Let \(L\) be the prefix-closed language generated by a plant, and \(K\) be a prefix-closed specification language contained in \(L\) \((K \subseteq L)\). Assume there are \(m\) local sites \((I = \{1, \ldots, m\})\) communicating over \(k\)-bounded delay FIFO channels under protocol \(P^{\text{gen}} \in \mathcal{P}^{\text{gen}}\). Then \((L, K)\) is said to be joint \(k\)-diagnosable under \(P^{\text{gen}}\), called \(\text{joint}^{\text{gen,k}}\)-diagnosable, if

\[
(\exists n \in \mathcal{N})(\forall s \in L - K)(\forall st \in L, |t| \geq n \text{ or } st \text{ deadlocks}) \Rightarrow
(\exists i \in I)(\forall u \in L, \mathcal{Y}_i^{\text{gen,k}}(st, u) = 1 \Rightarrow u \in L - K), \tag{8}
\]

where \(\mathcal{Y}_i^{\text{gen,k}}\) is the \(P^{\text{gen}}\)-based indistinguishability predicate for site \(i\) under \(k\)-bounded communication delay defined in (7). The joint \(k\)-diagnosability with respect to protocol \(P^{\text{op}} \in \mathcal{P}^{\text{op}}\) and \(P^{\text{pop}}\), denoted \(\text{joint}^{\text{op,k}}\)-diagnosability and \(\text{joint}^{\text{pop,k}}\)-diagnosability, respectively, are defined by replacing \(\mathcal{Y}_i^{\text{gen,k}}\) in (8) with \(\mathcal{Y}_i^{\text{op,k}}\) and \(\mathcal{Y}_i^{\text{pop,k}}\), respectively.
The above definition has the following meaning. For any faulty trace \( s \) (\( s \in L - K \)) that is extended by a sufficiently long trace (\( |t| \geq n \)) or is extended to a deadlocking trace (\( st \) deadlocks), there exists at least one local site \( i \) such that any trace \( u \) in \( L \) that is indistinguishable from \( st \) at site \( i \) under protocol \( P^{gen} \) (resp., \( P^{op} \), \( P^{iop} \)) and \( k \)-bounded communication delay, i.e. \( \gamma^{k,gen}_i(st, u) = 1 \) (resp., \( \gamma^{iop}_i(st, u) = 1 \), \( \gamma^{op}_i(st, u) = 1 \)), belongs to the faulty language \( L - K \).

In the following theorem, we present the main result of this section, which reduces the \( P^{iop} \)-based distributed diagnosis problem to an instance of the decentralized diagnosis problem.

**Theorem 1** Given a plant \( G = (X, \Sigma, \alpha, x_0) \) and a specification model \( R \) with \( L(R) \subseteq L(G) \), define the extended plant and extended specification models \( \mathcal{G}^k = G \| C^k_{12} \| C^k_{21} \) and \( \mathcal{R}^k = R \| C^k_{12} \| C^k_{21} \) respectively, where \( C^k_{ij} \) \( (i, j \in \{1, 2\}, i \neq j \) is the \( k \)-delaying\&masking model from site \( i \) to site \( j \). Let \( M_i : \Sigma \to \overline{\Sigma}_i \) and \( \mathcal{M}_i : \Sigma \cup \Lambda_1 \cup \Lambda_2 \to \overline{\Lambda}_1 \cup \overline{\Lambda}_2 \) be the observation mask and the extended observation mask for site \( i \), respectively. Then,

\[
(L(G), L(R)) \text{ joint}^{iop}_k \text{-diagnosable} \iff (L(\mathcal{G}^k), L(\mathcal{R}^k)) \text{ codiagnosable with respect to } \{\mathcal{M}_i\}.
\]

**Proof:** (\( \Rightarrow \)) If \( (L(G), L(R)) \) is joint\(^{iop}_k\)-diagnosable, then

\[
(\exists n' \in \mathcal{N})(\forall s' \in L(G) - L(R))(\forall s' t' \in L(G), |t'| \geq n' \text{ or } s' t' \text{ deadlocks}) \Rightarrow
(\exists i \in \{1, 2\})(\forall u' \in L(G), \gamma^{iop}_i(s' t', u') = 1 \Rightarrow u' \in L(G) - L(R)).
\]

In order to prove the codiagnosability of \( (L(\mathcal{G}^k), L(\mathcal{R}^k)) \), we need to show the existence of a bound \( n \in \mathcal{N} \) such that

\[
(\forall s \in L(\mathcal{G}^k) - L(\mathcal{R}^k))(\forall s t \in L(\mathcal{G}^k), |t| \geq n \text{ or } st \text{ deadlocks}) \Rightarrow
(\exists i \in \{1, 2\})(\forall u \in L(\mathcal{G}^k), M_i(st) = M_i(u) \Rightarrow u \in L(\mathcal{G}^k) - L(\mathcal{R}^k)).
\]

We claim that \( n = 3n' \) can be chosen as such a bound, where \( n' \) is the diagnosis bound specified in (9).

Pick any \( s \in L(\mathcal{G}^k) - L(\mathcal{R}^k) \). By Corollary 1, \( \Pi_\Sigma(s) \in L(G) - L(R) \). For all \( st \in L(\mathcal{G}^k) \), it follows from Proposition 1 that \( \Pi_\Sigma(st) \in L(G) \). Since \( \mathcal{G}^k = G \| C^k_{12} \| C^k_{21} \) is extended from \( G \) by interleaving events in \( \Sigma \) with their observations or communicated observations in \( \overline{\Lambda}_1 \cup \overline{\Lambda}_2 \), and each observation in \( \overline{\Lambda}_1 \cup \overline{\Lambda}_2 \) occurs after its corresponding event in \( \Sigma \), if \( |t| \geq n = 3n' \) or if \( st \) deadlocks, we must have that \( |\Pi_\Sigma(t)| \geq n' \) or \( \Pi_\Sigma(st) \) deadlocks.

Then, pick any trace \( u \in L(\mathcal{G}^k) \). By Proposition 1, \( \Pi_\Sigma(u) \in L(G) \). Since \( \Pi_\Sigma(s) \in L(G) - L(R) \), and \( \Pi_\Sigma(st) \in L(G) \) with \( |\Pi_\Sigma(t)| \geq n' \) or \( \Pi_\Sigma(st) \) deadlocks, it follows from the joint\(^{iop}_k\)-diagnosability of \( (L(G), L(R)) \) that

\[
\exists i \in \{1, 2\} : \gamma^{iop}_i(\Pi_\Sigma(st), \Pi_\Sigma(u)) = 1 \Rightarrow \Pi_\Sigma(u) \in L(G) - L(R).
\]

From Proposition 3, we know that if \( M_i(st) = M_i(u) \), then \( \gamma^{iop}_i(\Pi_\Sigma(st), \Pi_\Sigma(u)) = 1 \), and thus \( \Pi_\Sigma(u) \in L(G) - L(R) \), which implies \( u \in \Pi_\Sigma^{-1}[\Pi_\Sigma(u)] \cap L(\mathcal{G}^k) \subseteq L(\mathcal{G}^k) - L(\mathcal{R}^k) \) by Corollary 1. Thus \( (L(\mathcal{G}^k), L(\mathcal{R}^k)) \) is codiagnosable with respect to \( \{\mathcal{M}_i\} \).
where \( u_2 f \) of the algorithm to verify joint respectively, where we claim that the same bound of a bound

\[ L_0^2 \geq n \text{ or } s't' \text{ deadlocks} \implies (10) \]

\[ (\exists i \in \{1, 2\})(\forall u' \in L(G^k), \mathcal{M}_i(s't') = \mathcal{M}_i(u') \implies u' \in L(G^k) - L(R^k)). \]

In order to prove the joint \( i_{op} \)-diagnosability of \((L(G), L(R))\), we need to show the existence of a bound \( n \) such that

\[ (\forall s \in L(G) - L(R))(\forall st \in L(G), |t| \geq n \text{ or } st \text{ deadlocks}) \implies (10) \]

\[ (\exists i \in \{1, 2\})(\forall s' \in L(G^k) - L(R^k), |s'| \geq n \text{ or } s't' \text{ deadlocks}) \implies \]

We claim that the same bound \( n' \) specified in (10) works for the joint \( i_{op} \)-diagnosability as well, i.e., \( n = n' \).

Pick any \( s \in L(G) - L(R) \). By Corollary 1, \( \Pi_{\Sigma}^{-1}(s) \cap L(G^k) \subseteq L(G^k) - L(R^k) \). For all \( st \in L(G) \) with \(|t| \geq n \) or \( st \) deadlocks, it follows that

\[ \exists s' \in \Pi_{\Sigma}^{-1}(s) \cap L(G^k), t' \in \Pi_{\Sigma}^{-1}(t) \cap L(G^k) : s't' \in \Pi_{\Sigma}^{-1}(st) \cap L(G^k), |t'| \geq n \text{ or } s't' \text{ deadlocks}. \]

Consider any \( u \in L(G) \). For any \( u' \in \Pi_{\Sigma}^{-1}(u) \cap L(G^k) \), it follows from the codiagnosability of \((L(G^k), L(R^k))\) that

\[ \exists i \in \{1, 2\} : \mathcal{M}_i(s't') = \mathcal{M}_i(u') \implies u' \in L(G^k) - L(R^k). \]

From Proposition 3, we know that if \( \Upsilon_{i, j}^{i_{op}, k}(st, u) = 1 \), then there exist \( s't' \in \Pi_{\Sigma}^{-1}(st) \cap L(G^k) \) and \( u' \in \Pi_{\Sigma}^{-1}(u) \cap L(G^k) \) such that \( \mathcal{M}_i(s't') = \mathcal{M}_i(u') \). This indicates that there exists \( i \in \{1, 2\} \) such that

\[ \forall u \in L(G) : (\Upsilon_{i, j}^{i_{op}, k}(st, u) = 1) \implies (\exists u' \in \Pi_{\Sigma}^{-1}(u) \cap L(G^k), u' \in L(G^k) - L(R^k)), \]

where \( u' \in L(G^k) - L(R^k) \) implies that \( u = \Pi_{\Sigma}(u') \in L(G) - L(R) \) by Corollary 1. This completes the proof.

\[ \]  

6 Verification of Joint \( i_{op} \)-Diagnosability

An implication of Theorem 1 is that the methods presented in [17] for studying decentralized diagnosis can be applied to study \( P^{i_{op}} \)-based distributed diagnosis. Before discussing the algorithm to verify joint \( i_{op} \)-diagnosability, we present the following proposition relating the extended global specification and the extended local specification models, which is used to reduce the complexity of the verification algorithm.

Proposition 4 Given a specification model \( R \), define \( R^k := R || C_{i, j}^k || C_{j, i}^k \) and \( R_i^k := R || C_{j, i}^k \) \((i, j \in \{1, 2\}, i \neq j)\), the extended specification and the extended local specification models, respectively, where \( C_{i, j}^k \) is the \( k \)-delaying\&masking model from site \( i \) to site \( j \). Let \( \mathcal{M}_i : \Sigma \cup \Lambda_1 \cup \Lambda_2 \rightarrow \Lambda_1 \cup \Lambda_2 \) be the extended observation mask for site \( i \). Then, we have that

\[ \mathcal{M}_i(L(R^k)) = \mathcal{M}_i(L(R_i^k)). \]
Proof: \((\subseteq)\) It suffices to show that for any trace \(s \in L(\mathcal{R}^k)\), there exists a trace \(s' \in L(\mathcal{R}^k_i)\) such that \(\mathcal{M}_i(s) = \mathcal{M}_i(s')\). Pick any trace \(s = a_1 \cdots a_l \in L(\mathcal{R}^k) = L(\mathcal{R}^k)\). Since \(\Lambda_1 \cap \Lambda_2 = \emptyset\), we can define a trace \(s' = a'_1 \cdots a'_l\) with

\[
\forall q \in \{1, \ldots, l\}, a'_q := \begin{cases} a_q & \text{if } a_q \in \Sigma \cup \Lambda_j; \\ \epsilon & \text{if } a_q \in \Lambda_i. \end{cases}
\]

It follows from \(\mathcal{M}_i(\Lambda_i) = \{\epsilon\}\) that \(\mathcal{M}_i(s) = \mathcal{M}_i(s')\). Since in \(\mathcal{R}^k\) and \(\mathcal{R}^k_i\), all events in \(\Sigma\) are executed synchronously, and all events in \(\Lambda_1 \cup \Lambda_2\) are executed asynchronously, and since \(\Pi_\Sigma(C^k_j) = \Sigma^*\), it follows that \(s' \in L(\mathcal{R}^k_i)\). Thus, \(\mathcal{M}_i(L(\mathcal{R}^k)) \subset \mathcal{M}_i(L(\mathcal{R}^k_i))\).

\((\supseteq)\) It suffices to show that for any trace \(s \in L(\mathcal{R}^k)\) such that \(\mathcal{M}_i(s) = \mathcal{M}_i(s')\). Pick any trace \(s = a_1 \cdots a_l \in L(\mathcal{R}^k_i)\). Let \(C^k_j = (Z^k_{ji}, \Sigma \cup \Lambda_j, \gamma^k_{ji}, z_0)\) \((i, j \in \{1, 2\}, i \neq j)\). Since \(C^k_{12}\) and \(C^k_{21}\) share the same structure and the same state space \((Z^k_{21} = Z^k_{12})\), and only transitions labeled by local observation symbols from \(\Lambda_1 \cup \Lambda_2\) are different, we can define \(s' = a'_1 \cdots a'_l\) with

\[
\forall q \in \{1, \ldots, l\}, a'_q := \begin{cases} a_q & \text{if } a_q \in \Sigma; \\ aqb_q & \text{if } a_q \in \Lambda_j, \end{cases}
\]

where \(b_q \in \Lambda_i\) and \(\gamma^k_{ji}(z, a_q) = \gamma^k_{ij}(z, b_q)\) for \(z \in Z^k_{21} = Z^k_{12}\). Since in \(\mathcal{R}^k\) and \(\mathcal{R}^k_i\), all events in \(\Sigma\) are executed synchronously, and all events in \(\Lambda_1 \cup \Lambda_2\) are executed asynchronously, and since \(\Lambda_1 \cap \Lambda_2 = \emptyset\), it follows that \(s' \in L(\mathcal{R}^k)\). Since \(\mathcal{M}_i(b_q) = \epsilon\) for \(b_q \in \Lambda_i\), we have that \(\mathcal{M}_i(s) = \mathcal{M}_i(s')\). Thus, \(\mathcal{M}_i(L(\mathcal{R}^k)) \supseteq \mathcal{M}_i(L(\mathcal{R}^k_i))\).

An algorithm for verifying the codiagnosability was given in [17], where a testing automaton \(T = (G|\overrightarrow{R}) \times R \times R\) was constructed to track a triplet of traces \(s, u_1\) and \(u_2\) with the following property:

\[
\forall i \in \{1, 2\}, \mathcal{M}_i(s) = \mathcal{M}_i(u_i), s \in L(G) \cap L(\overrightarrow{R}) = L(G), u_i \in L(R),
\]

and without loss of generality \(G\) was plant to be deadlock-free. A similar testing automaton is defined in the following verification algorithm for testing joint diagnosability, assuming again without loss of generality that \(G\) is deadlock-free.

Note that the application of codiagnosability test in [17, Algorithm 1] would result in the construction of the testing automaton \(\overrightarrow{G}^k \times \mathcal{R}^k \times \mathcal{R}^k\) that tracks a trace-triple satisfying

\[
\forall i \in \{1, 2\}, \mathcal{M}_i(s) = \mathcal{M}_i(u_i), s \in L(\overrightarrow{G}^k) = L(G), u_i \in L(\mathcal{R}^k) \quad (11)
\]

Since \(\mathcal{M}_i(L(\mathcal{R}^k)) = \mathcal{M}_i(L(\mathcal{R}^k_i))\) as shown in Proposition 4, it suffices to construct the testing automaton \(T^k = \overrightarrow{G}^k \times \mathcal{R}^k_1 \times \mathcal{R}^k_2\). The advantage is that \(T^k\) has a smaller state space than \(\overrightarrow{G}^k \times \mathcal{R}^k \times \mathcal{R}^k\).

**Algorithm 1** Given a (deadlock-free) plant \(G = (X, \Sigma, x_0)\) and a specification model \(R = (Y, \Sigma, \beta, y_0)\), consider a distributed diagnosis systems with two local sites, which communicate with each other using the immediate observation passing protocol \(P^{iop}\). Perform the following operations:

1. Construct the \(k\)-delaying&masking models \(C^k_{12}\) and \(C^k_{21}\).
is used to denote a non self-loop 

Theorem 2

3. Construct a testing automaton $T^k$ for checking joint$_{iop}^k$-diagnosability:

$$T^k = (G||R^k) \times R^k_1 \times R^k_2$$

$$= \overline{G}^k \times R^k_1 \times R^k_2$$

$$= (G||R||C^k_{12}||C^k_{21}) \times (R||C^k_{21}) \times (R||C^k_{12}).$$

Note that $(e, e, e)$-transition is allowed in the testing automaton if it is not performed as a self loop. The testing automaton $T^k$ tracks all triplet of traces $s, u_1, u_2 \in (\Sigma \cup \Lambda_1 \cup \Lambda_2)^*$ satisfying the following property:

$$\forall i \in \{1, 2\}, M_i(s) = M_i(u_i), s \in L(G^k) = L(G), u_i \in L(R^k_i).$$

4. Check the existence of any “offending” cycle in $T^k$: The system is not joint$_{iop}^k$-diagnosable if and only if any state in a cycle contains the label “F”.

Theorem 2 Algorithm 1 is correct. I.e., $(L, K)$ is joint$_{iop}^k$-diagnosable if and only if the testing automaton $T^k$ in Algorithm 1 does not contain cycles with states labeled by “F”.

Proof: By Theorem 1, $(L, K)$ is joint$_{iop}^k$-diagnosable if and only if $(L(G^k), L(R^k))$ is codiagnosable with respect to $\{M_i\}$. By [17, Theorem 1], codiagnosability of $(L(G^k), L(R^k))$ with respect to $\{M_i\}$ can be checked by checking presence of cycles containing states labeled “F” in the testing automaton $\overline{G}^k \times R^k_1 \times R^k_2$. Since $\overline{G}^k \times R^k_1 \times R^k_2$ tracks triplets of traces satisfying 11, and since $M_i(L(R^k)) = M_i(L(R^k_1))$ from Proposition 4, $T^k = \overline{G}^k \times R^k_1 \times R^k_2$ also tracks the same triplets of traces. So the correctness of Algorithm 1 follows from the correctness of codiagnosability test given in [17, Theorem 1] and Proposition 4.

To illustrate Algorithm 1, we present the following example to verify joint$_{iop}^k$-diagnosability of system discussed in Example 1.

Example 2 Consider the system introduced in Example 1. For the delay bound $k = 1$, the extended plant/specification models are shown in Figure 6. We construct the testing automaton as shown in Figure 8(a). Note at the initial state of $G$, the transition on a leads the state machine to a “good” region satisfying the specification, where no state is labeled by “F”, and there is no possibility of leaving that region. For the failure diagnosis purpose, we do not need to track traces in that “good” region. Thus we omit the corresponding part from the testing automation $T^1$. It is seen that no “offending” cycle exist in $T^1$. Thus, the system is joint$_{iop}^1$-diagnosable.

For the same system, if the delay bound is $k = 2$, then it can be verified that the system is not joint$_{iop}^2$-diagnosable. The extended plant/specification models are shown in Figure 7. We can construct the corresponding testing automaton $T^2 = \overline{G}^2 \times R^2_1 \times R^2_2$, part of which is shown in Figure 8(b), where $\epsilon$ is used to denote a non self-loop $\epsilon$ transition appearing
in $G^2$ or $R^2$. It is seen that there is an “ambiguous” cycle formed between the states $(82F, 5, 11)$ and $(82F, 5, 13)$, indicating that the system is not joint$^{\text{top}}_2$-diagnosable. Thus a larger delay results in a loss of diagnosability, which is not unexpected. Since the system is not joint$^{\text{top}}_2$-diagnosable, it can be further concluded that the system is not codiagnosable (recall codiagnosability requires no communication at all.)

7 Diagnoser Synthesis

In the setting of decentralized diagnosis of [17], a local diagnoser at site $i$ was taken to be $D_i = M_i(G || R)$. Analogously, we can define an extended local diagnoser for site $i$ to be $D^k_i := M_i(G^k || R^k) = M_i(G || R^k)$ for the diagnosis of a joint$^{\text{top}}_k$-diagnosable system. As is the case with the verification, certain complexity reduction is also possible for the synthesis of local diagnosers. We define a “reduced” diagnoser at site $i$ to be $\tilde{D}^k_i := M_i(G || R^k_i)$. We show in the following that the two diagnosers produce the same diagnosis result. I.e., diagnoser $\tilde{D}^k_i$ detects a failure if and only if diagnoser $D^k_i$ detects a failure. The following lemma shows that diagnosers $D^k_i$ and $\tilde{D}^k_i$ generate the same language.

Lemma 2 Given a plant $G$ and a specification model $R$ with $L(R) \subseteq L(G)$, let $G^k$, $R^k$, and $R^k_i$ ($i \in \{1, 2\}$) be the extended plant model, extended specification model, and extended
local specification model for site \(i\), respectively. Consider the local diagnosers for site \(i\), \(\mathcal{D}^i_k := \mathcal{M}_i(G^k||\mathcal{R}^k) = \mathcal{M}_i(G||\mathcal{R}^k)\) and \(\tilde{\mathcal{D}}^i_k := \mathcal{M}_i(G||\mathcal{R}^k)\), where \(\mathcal{M}_i : \Sigma \cup \Lambda_1 \cup \Lambda_2 \rightarrow \overline{\Lambda}_1 \cup \overline{\Lambda}_2\) is the extended observation mask for site \(i\). Then, \(\mathcal{D}^i_k\) and \(\tilde{\mathcal{D}}^i_k\) generate the same language, i.e., \(L(\mathcal{D}^i_k) = L(\tilde{\mathcal{D}}^i_k)\).

**Proof:** Since \(L(\mathcal{D}^i_k) = L(\mathcal{M}_i(G||\mathcal{R}^k)) = \mathcal{M}_i(L(G||\mathcal{R}^k))\) and \(L(\tilde{\mathcal{D}}^i_k) = L(\mathcal{M}_i(G||\mathcal{R}^k)) = \mathcal{M}_i(L(G||\mathcal{R}^k))\), we need to show that \(\mathcal{M}_i(L(G||\mathcal{R}^k)) \subseteq \mathcal{M}_i(L(G||\mathcal{R}^k))\) and \(\mathcal{M}_i(L(G||\mathcal{R}^k)) \subseteq \mathcal{M}_i(L(G||\mathcal{R}^k))\) as in Proposition 4.

The reachability set \(\text{Reach}_{\tilde{\mathcal{D}}^i_k}(\cdot)\) (resp., \(\text{Reach}_{\mathcal{D}^i_k}(\cdot)\)) denotes the set of possible states of \(\tilde{\mathcal{D}}^i_k\) (resp., \(\mathcal{D}^i_k\)) reached by an execution of a trace in \(L(\tilde{\mathcal{D}}^i_k)\) (resp., \(L(\mathcal{D}^i_k)\)). Let \(x_0^{\tilde{\mathcal{D}}^i_k}\) denote the initial state of diagnoser \(\tilde{\mathcal{D}}^i_k\), and \(\delta_{\tilde{\mathcal{D}}^i_k}\) denote its transition function. The reachability set \(\text{Reach}_{\tilde{\mathcal{D}}^i_k}(\cdot)\) is computed recursively upon each incoming information as follows.

- \(\text{Reach}_{\tilde{\mathcal{D}}^i_k}(\varepsilon) = \varepsilon_{\tilde{\mathcal{D}}^i_k}(x_0^{\tilde{\mathcal{D}}^i_k})\);

\(\forall s \in L(\tilde{\mathcal{D}}^i_k), \sigma \in \Lambda_1 \cup \Lambda_2 : \text{Reach}_{\tilde{\mathcal{D}}^i_k}(s\sigma) = \varepsilon_{\tilde{\mathcal{D}}^i_k}(\delta_{\tilde{\mathcal{D}}^i_k}(\text{Reach}_{\tilde{\mathcal{D}}^i_k}(s), \sigma))\).

The reachability set \(\text{Reach}_{\mathcal{D}^i_k}(\cdot)\) is computed similarly. Let \((\Omega_F)_{\tilde{\mathcal{D}}^i_k}\) denote the set of “failure states” of \(\tilde{\mathcal{D}}^i_k\), i.e., \((\Omega_F)_{\tilde{\mathcal{D}}^i_k} = X \times \{F\} \times \mathbb{Z}^k_{ji}\). Similarly, \((\Omega_F)_{\mathcal{D}^i_k} = X \times \{F\} \times \mathbb{Z}^k_{1i} \times \mathbb{Z}^k_{2i}\) denotes the failure states of diagnoser \(\mathcal{D}^i_k\). The equivalence of diagnosers \(\tilde{\mathcal{D}}^i_k\) and \(\mathcal{D}^i_k\) in the sense of their diagnosis capabilities is presented in the following theorem.

**Theorem 3** Given a plant \(G\) and a specification model \(R\) with \(L(R) \subseteq L(G)\), let \(G^k, \mathcal{R}^k,\) and \(\mathcal{R}^k_i \ (i \in \{1, 2\})\) be the extended plant model, extended specification model, and extended local specification model for site \(i\), respectively. Consider the local diagnosers for site \(i\), \(\mathcal{D}^i_k := \mathcal{M}_i(G^k||\mathcal{R}^k) = \mathcal{M}_i(G||\mathcal{R}^k)\) and \(\tilde{\mathcal{D}}^i_k := \mathcal{M}_i(G||\mathcal{R}^k)\), where \(\mathcal{M}_i : \Sigma \cup \Lambda_1 \cup \Lambda_2 \rightarrow \overline{\Lambda}_1 \cup \overline{\Lambda}_2\) is the extended observation mask for site \(i\). Let \((\Omega_F)_{\mathcal{D}^i_k}\) and \((\Omega_F)_{\tilde{\mathcal{D}}^i_k}\) denote the set of failure states in \(\mathcal{D}^i_k\) and \(\tilde{\mathcal{D}}^i_k\), respectively. Then,

\[
\forall s \in L(\mathcal{D}^i_k) = L(\tilde{\mathcal{D}}^i_k) : \text{Reach}_{\mathcal{D}^i_k}(s) \subseteq (\Omega_F)_{\mathcal{D}^i_k} \Leftrightarrow \text{Reach}_{\tilde{\mathcal{D}}^i_k}(s) \subseteq (\Omega_F)_{\tilde{\mathcal{D}}^i_k}.
\]

**Proof:** Pick any trace \(s \in L(\mathcal{D}^i_k) = L(\tilde{\mathcal{D}}^i_k)\). To prove the above theorem, we need to show that

\[
\forall x \in \text{Reach}_{\mathcal{D}^i_k}(s) : x \in (\Omega_F)_{\mathcal{D}^i_k} \Rightarrow \forall x' \in \text{Reach}_{\tilde{\mathcal{D}}^i_k}(s) : x' \in (\Omega_F)_{\tilde{\mathcal{D}}^i_k},
\]

and

\[
\forall x' \in \text{Reach}_{\tilde{\mathcal{D}}^i_k}(s) : x' \in (\Omega_F)_{\tilde{\mathcal{D}}^i_k} \Rightarrow \forall x \in \text{Reach}_{\mathcal{D}^i_k}(s) : x \in (\Omega_F)_{\mathcal{D}^i_k}.
\]

Since whether a state in \(\mathcal{D}^i_k\) or \(\tilde{\mathcal{D}}^i_k\) possesses a failure label or not only depends on the event trace in \(\Sigma^*\), to prove (12) and (13), it is enough to show that

\[
\Pi_{\Sigma}(\mathcal{M}^{-1}_i(s) \cap L(G||\mathcal{R}^k)) = \Pi_{\Sigma}(\mathcal{M}^{-1}_i(s) \cap L(G||\mathcal{R}^k)).
\]

22
We first show that \( \Pi_{\Sigma}(L(G\|\overline{R}^k)) = \Pi_{\Sigma}(L(G\|\overline{R}^i)) \). Since \( G\|\overline{R}^k = (G\|\overline{R}^i)\|C^k_{ij} \) \((i, j \in \{1, 2\}, i \neq j\) and events in \( \Sigma \) are synchronized among \( G\|\overline{R}^i \) and \( C^k_{ij} \), it follows that \( \Pi_{\Sigma}(L(G\|\overline{R}^k)) \subseteq \Pi_{\Sigma}(L(G\|\overline{R}^i)) \). Similarly as in Proposition 4, it can be shown that any possible transition in \( G\|\overline{R}^k \) would not be blocked by the additional component \( C^k_{ij} \) in \( G\|\overline{R}^k \).

Therefore, \( \Pi_{\Sigma}(L(G\|\overline{R}^k)) \supseteq \Pi_{\Sigma}(L(G\|\overline{R}^i)) \). From \( \Pi_{\Sigma}(L(G\|\overline{R}^k)) = \Pi_{\Sigma}(L(G\|\overline{R}^i)) \), it is easy to get that \( \Pi_{\Sigma}(\mathcal{M}_i^{-1}(s) \cap L(G\|\overline{R}^k)) = \Pi_{\Sigma}(\mathcal{M}_i^{-1}(s) \cap L(G\|\overline{R}^i)) \).

An implication of Theorem 3 is that we can use local diagnoser for site \( i \) to be \( \mathcal{D}_i^k = \mathcal{M}_i(G\|\overline{R}^k) = \mathcal{M}_i(G\|\overline{R}^i)\|C^k_{ji} \) for performing on-line diagnosis for a joint \( \text{top} \)-diagnosable system. Diagnoser \( \mathcal{D}_i^k \) computes the reachability set \( \text{Reach}_{\mathcal{D}_i^k} \) each time it observes a new event in the plant or receives a communicated observation from another diagnoser \( \mathcal{D}_j^k \) \((j \neq i)\). Whenever all states in \( \text{Reach}_{\mathcal{D}_i^k} \) contain the label “\( F \)”, diagnoser \( \mathcal{D}_i^k \) reports that a failure is detected.

The following example illustrates how to construct local diagnoser \( \mathcal{D}_i^k \), and how to perform on-line diagnosis using the reachability set \( \text{Reach}_{\mathcal{D}_i^k} \).

**Example 3** Let us revisit the system presented in Example 1. For the unit-delay case, we know from Example 2 that the system is joint \( \text{top} \)-diagnosable. Figure 9 shows the two local diagnosers \( \mathcal{D}_1^1 \) and \( \mathcal{D}_2^1 \). Each state in diagnoser \( \mathcal{D}_1^1 = \mathcal{M}_i(G\|\overline{R}^1) = \mathcal{M}_i(G\|\overline{R}^i)\|C^1_{ji} \) \((i, j \in \{1, 2\}, i \neq j\) contains three coordinates, which correspond to states in \( G, \overline{R} \), and \( C^1_{ji} \), respectively.

Assume that the plant executes a trace \( s = ba \). Diagnoser 1 observes event \( a' \) followed by a communicated observation \( b' \) from diagnoser 2 with unit-delay. Diagnoser 2 observes event \( b' \) followed by a communicated observation \( a' \) from diagnoser 1 with 0 or 1 delay. The reachability sets \( \text{Reach}_{\mathcal{D}_1^1} \) and \( \text{Reach}_{\mathcal{D}_2^1} \) are computed as follows:

- \( \text{Reach}_{\mathcal{D}_1^1}(e) = \{(0, 0, \epsilon), (4, F, b)\} \),
  - \( \text{Reach}_{\mathcal{D}_1^1}(a') = \{(1, 1, a), (1, 1, \epsilon), (5, F, ba)\} \),
  - \( \text{Reach}_{\mathcal{D}_1^1}(a'b') = \{(5, F, a), (5, F, \epsilon)\} \);

- \( \text{Reach}_{\mathcal{D}_2^1}(e) = \{(0, 0, \epsilon), (1, 1, a), (2, 2, aa)\} \),
  - \( \text{Reach}_{\mathcal{D}_2^1}(b') = \{(4, F, b), (5, F, ba), (4, F, \epsilon), (5, F, a), (6, F, aa)\} \),
  - \( \text{Reach}_{\mathcal{D}_2^1}(b'a') = \{(5, F, \epsilon), (6, F, a), (6, F, ac)\} \).

When diagnoser 1 observes event \( a' \), it cannot determine whether the plant is at a “normal” state 1 or the “failure” state 5, and thus is ambiguous about whether a failure has occurred or not. After receiving the communicated event \( b' \) from diagnoser 2, diagnoser 1 is sure that the plant is at state 5, and a failure has occurred. On the other hand, since all elements in \( \text{Reach}_{\mathcal{D}_2^1}(b') \) have their second coordinate labeled “\( F \)”, diagnoser 2 is certain about the occurrence of a failure after observing event \( b' \).

**Remark 1** Let \( |X| \) and \( |Y| \) be the number of states in plant \( G \) and specification model \( R \), respectively, and \( |\Sigma| \) be the number of events. Assume that there are \( m \) local sites \((I = \{1, \ldots, m\})\), each of them associated with a local observation mask \( M_i : \Sigma \rightarrow \overline{\Lambda}_i \). We
are summarized in Table 1. 

- $C_{ij}^k$: The number of states of a $k$-delaying&masking model $C_{ij}^k$ ($i, j \in I, i \neq j$) is at most $1 + |\Sigma| + |\Sigma|^2 + \ldots + |\Sigma|^{k+1} = O(|\Sigma|^{k+2})$. Since there are at most $1 + |\Sigma|$ possible transitions at each state, the number of transitions in $C_{ij}^k$ is $O(|\Sigma|^{k+3})$.

- $G^k$: Since there are $m(m-1)$ $k$-delaying&masking models $C_{ij}^k$ involved in constructing $G^k = \bigcap_{i,j \in I, i \neq j} C_{ij}^k$, the number of states in $G^k$ is $O(|X| \times |\Sigma|^{m(m-1)(k+2)})$. From the synchronization of events in $[\Sigma]$ among $G$ and $\{C_{ij}^k\}$, and the non-synchronization of events in $\bigcup_{i \in I} \Lambda_i$ among $\{C_{ij}^k\}$, we know that there are at most $|\Sigma|+m(m-1)$ transitions at each state of $G^k$. Thus, the number of transitions in $G^k$ is $O((|\Sigma| + m(m-1)) \times |X| \times |\Sigma|^{|m(m-1)(k+2)})$.

- $R_i^k$: Since there are $(m-1)$ $k$-delaying&masking models $\{C_{ij}^k\}$ involved in constructing $R_i^k = \bigcap_{j \in I, i \neq j} C_{ij}^k$, the number of states and transitions in $R_i^k$ are $O(|Y| \times |\Sigma|^{m+1})$ and $O((|\Sigma| + (m-1)) \times |Y| \times |\Sigma|^{m+1})$, respectively.

- $T_i^k$: Since there are $m$ local specification models $R_i^k$ ($i \in I$) involved in constructing the testing automaton $T_i^k = \bigcap_{i \in I} R_i^k$, the number of states and transitions are $O(|X| \times |Y| \times |\Sigma|^{2m(m-1)(k+2)})$, and $O((|\Sigma| + m(m-1)) \times |X| \times |Y|^m \times |\Sigma|^{2m(m-1)(k+2)})$, respectively.

- $\tilde{D}_i^k$: For the local diagnoser $\tilde{D}_i^k = \mathcal{M}_i(G \mid R_i^k)$, the number of states and transitions are $O(|X| \times |Y| \times |\Sigma|^{(m^2-1)(k+2)})$, and $O((|\Sigma| + m(m-1)) \times |X| \times |Y| \times |\Sigma|^{(m^2-1)(k+2)})$, respectively.

Figure 9: Local diagnosers in Example 3

analyze the number of states and transitions in various automata as follows, and the results are summarized in Table 1.

- $C_{ij}^k$: The number of states of a $k$-delaying&masking model $C_{ij}^k$ ($i, j \in I, i \neq j$) is at most $1 + |\Sigma| + |\Sigma|^2 + \ldots + |\Sigma|^{k+1} = O(|\Sigma|^{k+2})$. Since there are at most $1 + |\Sigma|$ possible transitions at each state, the number of transitions in $C_{ij}^k$ is $O(|\Sigma|^{k+3})$.

- $G^k$: Since there are $m(m-1)$ $k$-delaying&masking models $C_{ij}^k$ involved in constructing $G^k = \bigcap_{i,j \in I, i \neq j} C_{ij}^k$, the number of states in $G^k$ is $O(|X| \times |\Sigma|^{m(m-1)(k+2)})$. From the synchronization of events in $[\Sigma]$ among $G$ and $\{C_{ij}^k\}$, and the non-synchronization of events in $\bigcup_{i \in I} \Lambda_i$ among $\{C_{ij}^k\}$, we know that there are at most $|\Sigma|+m(m-1)$ transitions at each state of $G^k$. Thus, the number of transitions in $G^k$ is $O((|\Sigma| + m(m-1)) \times |X| \times |\Sigma|^{m(m-1)(k+2)})$.

- $R_i^k$: Since there are $(m-1)$ $k$-delaying&masking models $\{C_{ij}^k\}$ involved in constructing $R_i^k = \bigcap_{j \in I, i \neq j} C_{ij}^k$, the number of states and transitions in $R_i^k$ are $O(|Y| \times |\Sigma|^{m+1})$ and $O((|\Sigma| + (m-1)) \times |Y| \times |\Sigma|^{m+1})$, respectively.

- $T_i^k$: Since there are $m$ local specification models $R_i^k$ ($i \in I$) involved in constructing the testing automaton $T_i^k = \bigcap_{i \in I} R_i^k$, the number of states and transitions are $O(|X| \times |Y|^m \times |\Sigma|^{2m(m-1)(k+2)})$, and $O((|\Sigma| + m(m-1)) \times |X| \times |Y|^m \times |\Sigma|^{2m(m-1)(k+2)})$, respectively.

- $\tilde{D}_i^k$: For the local diagnoser $\tilde{D}_i^k = \mathcal{M}_i(G \mid R_i^k)$, the number of states and transitions are $O(|X| \times |Y| \times |\Sigma|^{(m^2-1)(k+2)})$, and $O((|\Sigma| + m(m-1)) \times |X| \times |Y| \times |\Sigma|^{(m^2-1)(k+2)})$, respectively.
| \( |\Sigma|^2 \eta (k+2) \), respectively.

| Table 1: Summary of complexity analysis in Remark 1 |
|---|---|
| number of states | number of transitions |
| \( C_{ij}^k \) | \( \mathcal{O}(|\Sigma|^{k+2}) \) |
| \( G^k \) | \( \mathcal{O}(|X| \times |\Sigma|^{m(m-1)(k+2)}) \) |
| \( R^k_i \) | \( \mathcal{O}(|Y| \times |\Sigma|^{(m-1)(k+2)}) \) |
| \( T^k \) | \( \mathcal{O}(|X| \times |Y|^{m \times |\Sigma|^{2(m-1)(k+2)}}) \) |
| \( D^k_i \) | \( \mathcal{O}(|X| \times |Y| \times |\Sigma|^{(m^2-1)(k+2)}) \) |

From the above analysis, it can be concluded that the complexity of Algorithm 1 for verifying joint \( \text{ goup } \) \( k \)-diagnosability is \( \mathcal{O}(|\Sigma| + m(m-1)) \times |\Sigma| \times |\Sigma|^{m \times m \times |\Sigma|^{2(m-1)(k+2)}} \), and the complexity of synthesizing local diagnosers is \( \mathcal{O}(|\Sigma| + m(m-1)) \times |\Sigma| \times |\Sigma|^{(m(m-1)(k+2))} \). It is clear that complexity is polynomial in the number of plant and specification states, but grows exponentially in delay bound and the number of local diagnosers.

8 Hierarchy of Various Diagnosabilities

In this section, we compare various notions of distributed/decentralized diagnosabilities. In particular, we establish the following hierarchy:

\[
\text{Codignosable} \Leftrightarrow \text{Joint} \_\infty \text{-diagnosable} \\
\Rightarrow \text{Joint} \_k \text{-diagnosable} \\
\neq \text{Joint} \_k \text{-diagnosable} \\
\Rightarrow \text{Joint} \_0 \text{-diagnosable} \\
\Leftrightarrow \text{Diagnosable},
\]

where joint \( \text{goup } \) \( 0 \)-diagnosability (resp., joint \( \text{goup } \) \( 0 \)-diagnosability) denotes the \( P_{\text{goup } \text{-diagnosability}} \) under unbounded-delay (resp., zero-delay) communication.

In [18] we have shown that “codignosability \( \Leftrightarrow \text{joint} \_\infty \text{-diagnosability}” holds for a general protocol \( P_{\text{goup } \text{-diagnosability}} \in P_{\text{goup } \text{-diagnosability}} \). It follows that this relationship also holds for protocol \( P_{\text{goup } \text{-diagnosability}} \). The following proposition formally establishes the equivalence between joint \( \text{goup } \) \( 0 \)-diagnosability and diagnosability. For a collection of local masks \( \{M_i\} \ (i \in I = \{1, \ldots, m\}) \), we define a global mask \( \overline{M} = (M_1, \ldots, M_m) \) as follows:

- \( \forall \sigma \in \Sigma: \overline{M}(\sigma) = (M_1(\sigma), \ldots, M_m(\sigma)) \), and
• \( \forall s \in \Sigma^*, \sigma \in \Sigma : \overline{M}(s\sigma) = \overline{M}(s)\overline{M}(\sigma) \).

**Proposition 5** Given a plant \( G \) and a specification model \( R \) with \( L(R) \subseteq L(G) \), let \( \{M_i|i \in I\} \) be local masks, and \( \overline{M} = (M_1, \ldots, M_m) \) be a global mask. Then,

\[(L(G), L(R)) \text{ is joint}_{0}^{\text{iop}}\text{-diagnosable} \iff (L(G), L(R)) \text{ is diagnosable with respect to } \overline{M}.\]

**Proof:** It follows from definitions of joint_{0}^{\text{iop}}\text{-diagnosability} and diagnosability that we only need to show the following claim to prove the above proposition:

\[\forall s, t \in L(G), i \in I : \Upsilon_i^{\text{iop}, 0}(s, t) = 1 \iff \overline{M}(s) = \overline{M}(t).\]

According to Definition 3, \( \Upsilon_i^{\text{iop}, 0}(s, t) = 1 \) if and only if \( O_i^{\text{iop}, 0}(s) \cap O_i^{\text{iop}, 0}(t) \neq \emptyset \), where \( O_i^{\text{iop}, 0}(s) = \mathcal{M}_i(\Pi_{\Sigma}^{-1}(s) \cap L(G^0)) \), and \( G^0 = G|_{i \neq j} C_{ij}^0 \). The structure of \( C_{ij}^0 \) is shown in Figure 10, where \( a, b, c, \ldots \in \Sigma \), and their observations under \( M_i \) are \( a_1^i, b_1^i, c_1^i, \ldots \in \overline{X}_i \), respectively. Since events in \( \Sigma \) are executed synchronously and events in \( \bigcup_{i \in I} \Lambda_i \) are executed asynchronously in \( G^0 \), for \( s = a_1a_2 \cdots a_l \in L(G) \), it follows that

\[\Pi_{\Sigma}^{-1}(s) \cap L(G^0) = a_1(a_1^1 \parallel \cdots \parallel a_l^1) \cdots a_l(a_1^m \parallel \cdots \parallel a_l^m).\]

Applying observation mask \( M_i \) upon the above formula, we get

\[O_i^{\text{iop}, 0}(s) = \mathcal{M}_i(\Pi_{\Sigma}^{-1}(s) \cap L(G^0)) = a_1^i(a_1^1 \parallel \cdots \parallel a_l^1) \cdots a_l^i(a_1^m \parallel \cdots \parallel a_l^m).\]

Thus, for \( s = a_1 \cdots a_l \in L(G) \) and \( t = b_1 \cdots b_v \in L(G) \), \( \Upsilon_1^{\text{iop}, 0}(s, t) = 1 \) if and only if

\[\{a_1^i(a_1^1 \parallel \cdots \parallel a_l^1) \cdots a_l^i(a_1^m \parallel \cdots \parallel a_l^m)\} \cap \{b_1^j(b_1^1 \parallel \cdots \parallel b_v^1) \cdots b_v^j(b_1^m \parallel \cdots \parallel b_v^m)\} \neq \emptyset. \tag{14}\]

Since it is assumed that \( \Lambda_i \cap \Lambda_j = \emptyset \), i.e., \( a_i^i \neq b_j^j \) for \( i \neq j \), it follows from (14) that

\[a_1^1(a_1^2 \cdots a_l^m) \cdots a_l^i(a_1^m \cdots a_l^m) = b_1^1(b_1^2 \cdots b_v^m) \cdots b_v^j(b_1^m \cdots b_v^m),\]

which implies \( \overline{M}(s) = \overline{M}(t) \). On the other hand, if \( \overline{M}(s) = \overline{M}(t) \), we can similarly prove that \( \Upsilon_i^{\text{iop}, 0}(s, t) = 1 \) for all \( i \in I \). This completes the proof.

Figure 10: \( C_{ij}^0 \)

Next, we present the relationship between joint_{k}^{\text{iop}}\text{-diagnosability} and joint_{k+1}^{\text{iop}}\text{-diagnosability.}
Proposition 6 Given a plant $G$ and a specification model $R$ with $L(R) \subseteq L(G)$,

$$(L(G), L(R)) \text{ is joint}^\text{top}_{k+1}\text{-diagnosable} \iff (L(G), L(R)) \text{ is joint}^\text{top}_k\text{-diagnosable}.$$ 

Proof: ($\Rightarrow$) We prove this property by showing that if $(L(G), L(R))$ is not joint$^\text{top}_k$-diagnosable, then it is not joint$^\text{top}_{k+1}$-diagnosable as well. If $(L(G), L(R))$ is not joint$^\text{top}_k$-diagnosable, then $(L(G^k), L(R^k))$ is not codiagnosable with respect to $\{M_i\}$, i.e.,

$$\forall n \in N, \forall i \in I : \exists s \in L(G^k) - L(R^k) \text{ with } |s| \geq n, \exists u \in L(R^k) \text{ s.t. } M_i(s) = M_i(u_i).$$ 

By Proposition 2, $L(G^k) - L(R^k) \subseteq L(G^{k+1}) - L(R^{k+1})$ and $L(R^k) \subseteq L(R^{k+1})$. Since the extended observation masks $\{M_i\}$ do not depend on the delay bound, we have that

$$\forall n \in N, \forall i \in I : \exists s \in L(G^{k+1}) - L(R^{k+1}) \text{ with } |s| \geq n, \exists u \in L(R^{k+1}) \text{ s.t. } M_i(s) = M_i(u_i).$$ 

I.e., $(L(G^{k+1}), L(R^{k+1}))$ is not codiagnosable with respect to $\{M_i\}$. Thus, $(L(G), L(R))$ is not joint$^\text{top}_{k+1}$-diagnosable.

($\not\Rightarrow$) Example 2 shows a system which is joint$^\text{top}_1$-diagnosable, but not joint$^\text{top}_2$-diagnosable. Thus, in general, joint$^\text{top}_k$-diagnosability does not imply joint$^\text{top}_{k+1}$-diagnosability.

9 Conclusions and Future Work

This paper has studied the distributed failure diagnosis problem under the $k$-bounded communication delay. A similar setting has been used for distributed control in the work of Tripakis [25]. A notion of joint$^\text{top}_k$-diagnosability is introduced so that any failure can be diagnosed within a bounded delay of its occurrence by one of the local sites using its own observations and the $k$-bounded delayed observations received from other local sites, which communicate among each other using the immediate observation passing protocol. We have shown that such problem of distributed diagnosis can be reduced to an instance of decentralized diagnosis. Results from [17] for decentralized diagnosis are applied for verifying joint$^\text{top}_k$-diagnosability, and synthesizing local diagnosers. Further simplifications are presented to improve computational complexity. Finally, the notions of diagnosability, codiagnosability, and joint$^\text{top}_k$-diagnosability are compared. A future direction can be an approach for more general distributed diagnosis where communicated information is not necessarily limited to local observations, but local sites may compute local state estimates and exchange them to further refine the estimations to come up with their diagnosis decisions.

References


