Decentralized Diagnosis for Nonfailures of Discrete Event Systems Using Inference-Based Ambiguity Management

Shigemasa Takai, Member, IEEE, and Ratnesh Kumar, Fellow, IEEE

Abstract—The task of decentralized decision-making involves interaction of a set of local decision-makers, each of which operates under limited sensing capabilities and is thus subjected to ambiguity during the process of decision-making. In a prior work [2] we made an observation that such ambiguities are of differing gradations and presented a framework for inferencing over various local control decisions of varying ambiguity levels to arrive at a global control decision. A similar inferencing-based framework for the management of ambiguities in the decentralized diagnosis of failures was reported in [1], [3]. For each event-trace executed by a system being monitored, each local diagnoser issues its own diagnosis decision (failure or nonfailure or unsure), tagged with a certain ambiguity level (zero being the minimum). A global diagnosis decision is taken to be a “winning” local diagnosis decision, i.e., one with a minimum ambiguity level. The computation of an ambiguity level for a local decision requires an assessment of the self-ambiguities as well as the ambiguities of the others, and an inference based up on such knowledge. The present work extends this to the decentralized diagnosis of nonfailures which requires that any ambiguity about the non-occurrence of a failure be resolved within a uniformly bounded delay. It is known that the decentralized diagnosability for failures does not imply that for nonfailures, and vice-versa. Further the following difference exists: Once the ambiguity about the occurrence of a failure is resolved, future observations do not cause the ambiguity to reoccur. The same is not true when one is concerned with the diagnosis for nonfailures, and so a different formulation is needed. In order to characterize the class of systems for which the ambiguity about the non-occurrence of a failure can be resolved within a uniformly bounded delay, we introduce the notion of N-inference diagnosability for NonFailures (also called N-inference NF-diagnosability), where the index N represents the maximum ambiguity level of any winning local decision. We present a method for verifying N-inference NF-diagnosability, and also establish various properties of it.

Index Terms—Discrete event systems, decentralized diagnosis, inferencing, knowledge, ambiguity, inference diagnosability for nonfailures.

I. INTRODUCTION

In any decentralized decision-making paradigm, such as decentralized control or diagnosis, multiple decision-makers, each with its limited sensing and/or control capabilities, interact to come up with the global decisions. Presence of limited sensing capabilities can lead to ambiguity in knowing the system state and thereby ambiguity in decision-making. In the context of decentralized control of discrete event systems (DESs), a knowledge-based mechanism for assessing the self-ambiguities was presented in [6], and later the same architecture was used for assessing the self-ambiguities as well as the ambiguities of the others in [7]. The process of utilizing the knowledge of the self-ambiguities together with the ambiguities of the others for the sake of decision-making was referred to as “inferencing” in [7] and “conditioning” in [10]. The ideas of conditioning were used in the context of diagnosis in [9]. These prior inferencing-based approaches were limited to a “single-level” of inferencing, and a comprehensive framework allowing multi-level inferencing over various local control decisions of varying levels of ambiguity was presented in [2].

In the context of decentralized diagnosis, the following simple technique for the management of ambiguity was suggested in [4]. When a local diagnoser is ambiguous about whether or not a failure has occurred it simply opts to issue no diagnosis decision, i.e., a diagnosis decision is issued by a local diagnoser only when it is unambiguous about it. This led to the introduction of the notion of codiagnosability in [4] that required that for each failure trace executable by the system being monitored, there be at least one local diagnoser that can unambiguously determine this within a bounded delay. In [4], the notion of strong codiagnosability for bounded-delay diagnosis of both failures and nonfailures was also introduced without involving any inferencing. An extension reported in [9] considered decentralized diagnosis based on the ideas of “conditioning” introduced in the setting of decentralized control and introduced the notion of conditional codiagnosability that is weaker than codiagnosability. As is the case with conditional coobservability [10], conditional codiagnosability involves a single level of inferencing over the knowledge about ambiguities.

A framework for the inference-based ambiguity management in the setting of decentralized diagnosis for failures was reported in [1], [3]. This framework supports (i) inferencing utilizing the knowledge of the self-ambiguities as well as the ambiguities of the other decision-makers, (ii) inferencing over an arbitrary number of levels of ambiguity. Each local diagnoser uses its observations of the system behavior to come up with its diagnosis decision together with a grade or level of ambiguity for that diagnosis decision. The computation of an ambiguity level of a local decision requires the assessment of the self-ambiguities together with the ambiguities of the others. In general a local diagnoser will issue a failure (resp., nonfailure) decision with an ambiguity level N following a certain observation if for each nonfailure (resp., failure) trace, producing the same observation as the one received, that local diagnoser knows there exists another local diagnoser that can issue a nonfailure (resp., failure) decision with an ambiguity level at most N − 1. It is also possible that a local diagnosis decision is neither “failure” nor “nonfailure”, but “unsure”.

Following the execution of each event all local diagnosers receiving a new observation issue a new diagnosis decision, tagged with a certain level of ambiguity. The global diagnosis decision is taken to be the same as a local diagnosis decision whose ambiguity level is the minimum. (Such a local decision can be considered to be a “winning” local decision.) In [1], [3], the notion of inference diagnosability for Failures (also called inference F-diagnosability) was formulated to characterize the class of diagnosable systems in the proposed framework. A system is said to be diagnosable for failures if the global diagnosis decisions are such that there are no missed detections, i.e., diagnosis decision is “failure” following the execution of any failure trace within a bounded delay. Also there are no false alarms, i.e., the global diagnosis decision following a nonfailure (resp., failure) trace is not “failure” (resp., “nonfailure”).

While knowing whether or not a failure occurred sometimes in a bounded past is important for taking corrective actions, knowing frequently (with bounded length gaps) whether or not the system is currently healthy can be useful for scheduling maintenance actions. The former is the property of diagnosability for failures, whereas the latter is the property of diagnosability for nonfailures. In this paper we establish that,

• The two properties (diagnosability for failures versus nonfailures) are independent of each other and study the diagnosis for nonfailures in the inference-based framework (diagnosis for failures in the inference-based framework was studied in our prior work [3]).
Also another difference exists between the two settings: In case of failure diagnosis, once the ambiguity about the occurrence of a failure is resolved, future observations do not cause the ambiguity to reoccur. The same is not true in case of diagnosis for nonfailures. Consequently, the definition of diagnosability for nonfailures requires that system’s nonfailure status be known repeatedly with bounded length gaps. To the best of our knowledge, this is a new concept introduced in this paper. (In contrast diagnosability for failures requires that the failure status be resolved within a bounded length delay.)

In order to characterize the class of systems for which the nonfailure status can be known frequently, with bounded length gaps, we introduce the notion of $N$-inference diagnosability for NonFailures (also called $N$-inference NF-diagnosability), where the index $N$ represents the maximum ambiguity level of any winning local decision. We present a method for verifying $N$-inference NF-diagnosability, and also establish various properties of it.

In particular we establish that the classes of systems that are $N$-inference NF-diagnosable form a monotonically increasing sequence as a function of $N$. We also show that there exist systems that are centrally diagnosable for nonfailures but not so decentrally (i.e., not $N$-inference NF-diagnosable for any index $N$). Then we show that the notion of strong codiagnosability studied in [4] is similar to the notion of 0-inference diagnosability for failures and nonfailures. Further the notions of NF-codiagnosability and conditional NF-codiagnosability introduced in [9] are similar to those of 0-inference NF-diagnosability and 1-inference NF-diagnosability, respectively. We also show an example that is 2-inference NF-diagnosable but not 1-inference NF-diagnosable.

The work presented above is based on the conference version [8]. A full version of this paper, which includes all omitted proofs, is available at the Web site:

http://is.ee.eng.osaka-u.ac.jp/takai/dia-inf2.pdf

II. NOTATION AND PRELIMINARIES

We consider a DES modeled by a finite nondeterministic automaton $G = (X, \Sigma, \alpha, X_0, X_m)$, where $X$ is the finite set of states, $\Sigma$ is the finite set of events, a partial function $\alpha : X \times (\Sigma \cup \{\varepsilon\}) \rightarrow 2^X$ is the transition function, $X_0 \subseteq X$ is the set of initial states, and $X_m \subseteq X$ is the set of marked or accepting states. $G$ is said to be deterministic if the transition function can be written as a partial function $\alpha : X \times \Sigma \rightarrow X$ and $|X_0| = 1$. Let $\Sigma^*$ be the set of all finite sequences of events including the empty sequence $\varepsilon$. Elements of $\Sigma^*$ are called traces, and subsets of $\Sigma^*$ are called languages. The transition function $\alpha$ can be generalized to $\alpha : 2^X \times \Sigma \rightarrow 2^X$ in a natural way. The generated and marked (or accepted) languages of $G$ are respectively defined as, $L(G) := \{s \in \Sigma^* | \alpha(X_0,s) \neq \emptyset\}$, and $L_m(G) := \{s \in \Sigma^* | \alpha(X_0,s) \cap X_m \neq \emptyset\}$.

For traces $s, t \in \Sigma^*$, the notation $t \leq s$ means that $t$ is a prefix of $s$. For a language $K$, the set of all prefixes of traces in $K$ is denoted by $pr(K), i.e., pr(K) = \{s \in \Sigma^* | \exists t \in K; st \in K\}$. K is said to be (prefix-)closed if $K = pr(K)$. A closed language $K$ is said to be deadlock-free if for any $s \in K$, there exists a trace $t \neq s$ such that $st \in K$; otherwise $s$ is called a deadlocking trace of $K$. For each trace $s \in \Sigma^*$, $|s|$ denotes its length. For any $m \in \mathbb{N}$, $N$ denotes the set of all nonnegative integers, let $\Sigma^{\geq m} := \{s \in \Sigma^* | |s| \geq m\}$ denote the set of all traces with $m$ or more events.

We review the inference-based decentralized diagnosis framework introduced in [1], [3]. Let $I = \{1, 2, \ldots, |I|\}$, where $|I|$ is the cardinality of $I$, denote the index set of local diagnosers that perform the task of diagnosis without sharing their observations. We assume that the limited sensing capabilities of the $i$th local diagnoser $D_i (i \in I)$ can be represented as the local observation mask, $M_i : \Sigma \cup \{\varepsilon\} \rightarrow \Delta_i \cup \{\varepsilon\}$, where $\Delta_i$ is the set of locally observed symbols, and $M_i(\varepsilon) = \varepsilon$. The map $M_i$ is generalized to $M_i : \Sigma^* \rightarrow \Delta_i^*$ and $M_i : 2^{\Sigma^*} \rightarrow 2^{\Delta_i^*}$ in a natural way.

Let $L := L(G) \neq \emptyset$ be the generated language of a plant $G$ (system to be diagnosed), and $K \subseteq L$ be a nonempty closed language representing a nonfailure specification language. Traces in $L \setminus K$ are considered failure traces and the task of diagnosis is to determine the execution of any trace in $L \setminus K$ within an additional bounded number of system executions. Without loss of generality, the plant language $L$ can be taken to be deadlock-free. Otherwise we can extend each deadlocking trace by an unbounded sequence of a newly added event that is unobservable to all diagnosers. This will make the language deadlock-free without altering any diagnosability property since the newly added event does not produce any observation to any of the diagnosers.

Let the set $C = \{0, 1, \phi\}$ be the set of diagnosis decisions, where “0” represents a nonfailure decision, “1” represents a failure decision, and “$\phi$” represents an unsure decision. Each inference-based local diagnoser $D_i$ is defined as a map $D_i : M_i(L) \rightarrow C \times N$, where for each $s \in L$, $D_i(M_i(s)) = (c_i(M_i(s)), n_i(M_i(s)))$. Here $c_i(M_i(s)) \in C$ denotes the diagnosis decision of $D_i$ following an observation $M_i(s) \in M_i(L)$, and $n_i(M_i(s)) \in N$ denotes the ambiguity level of the diagnosis decision of $D_i$. Let $n(s)$ be the minimum ambiguity level of local decisions, i.e., $n(s) := \min_{i \in I} n_i(M_i(s))$.

The decentralized diagnoser $\{D_i\}_{i \in I}$ that consists of local diagnosers $D_i (i \in I)$ issues global diagnosis decisions. Formally, $\{D_i\}_{i \in I}$ is defined as a map $\{D_i\}_{i \in I} : L \rightarrow C$. For each $s \in L$, the diagnosis decision $\{D_i\}_{i \in I}(s)$ is given as follows:

$$\{D_i\}_{i \in I}(s) = \begin{cases} 0, & \text{if } \forall i \in I \text{ s.t. } n_i(M_i(s)) = n(s); \\ c_i(M_i(s)) = 0, & \text{if } s = \varepsilon; \\ 1, & \text{if } \exists i \in I \text{ s.t. } n_i(M_i(s)) = n(s); \\ c_i(M_i(s)) = 1, & \text{if } s = \varepsilon; \\ \phi, & \text{otherwise.} \end{cases}$$

In other words, the global diagnosis decision is taken to be the same as a local diagnosis decision possessing the minimum level of ambiguity.

A useful notion of a decentralized diagnoser is the largest ambiguity level $N \in N$ of any sure decision, and the preservation of surety of a decision with a decrease in the ambiguity-level (if a certain ambiguity-level decision is “sure”, then all lower ambiguity-level decisions are also “sure”). We refer to such a diagnoser to be “$N$-infering”.

Definition 1: [3] A decentralized diagnoser $\{D_i\}_{i \in I} : L \rightarrow C$ is said to be $N$-infering if the following two conditions hold:

1. $\forall s \in L \{D_i\}_{i \in I}(s) \neq \phi \Rightarrow n(s) \leq N$, $\forall s', s'' \in L \{D_i\}_{i \in I}(s) \neq \phi \land n(s') \leq n(s) \Rightarrow D_i(s') = D_i(s') \neq \phi$.

III. INFERENCE-BASED DECENTRALIZED DIAGNOSIS FOR NONFAILURES

We presented a framework for inference-based diagnosis for failures in [1], [3]. The notion of diagnosability for failures guarantees that any failure can be detected within a uniformly bounded delay. However it does not guarantee that the non-occurrence of a failure is unambiguously known. The following example illustrates such a situation.

Example 1: We consider a plant modeled by the finite automaton $G$ shown in Fig. 1(a). Let $|I| = 2$.

$$M_1(\sigma) = \begin{cases} \sigma, & \text{if } \sigma \in \{a, c\}; \\ \varepsilon, & \text{otherwise} \end{cases}, \quad M_2(\sigma) = \begin{cases} \sigma, & \text{if } \sigma \in \{b, c\}; \\ \varepsilon, & \text{otherwise.} \end{cases}$$
diagnoser \( \{ D_i \}_{i \in I} \) should satisfy
\[
(\exists m \in \mathcal{N})(\forall s \in K) \quad (\forall s \in K \text{ s.t. } |t| \geq m)(\exists u \leq t \text{ s.t. } \{ D_i \}_{i \in I}(su) = 0). \quad (1)
\]

Further it is desired that there are no “false alarms”, i.e., the decentralized diagnoser never issues a failure (resp., nonfailure) decision following a nonfailure (resp., failure) trace. Thus, the following should hold:
\[
(\forall s \in K) \quad \{ D_i \}_{i \in I}(s) \neq 1, \quad (2)
\]
\[
(\forall s \in L - K) \quad \{ D_i \}_{i \in I}(s) \neq 0. \quad (3)
\]

IV. EXISTENCE/SYNTHESIS OF INFERENCE-BASED DECENTRALIZED DIAGNOSERS

Let \( N \in \mathcal{N} \) be a given nonnegative integer. \( (N \) represents a parameter for the inference diagnosability and is elaborated later.) Given a plant language \( L \) and a nonfailure specification language \( K \subseteq L \), we inductively define a monotonically decreasing sequence \( \{ (F_k, H_k) \}_{0 \leq k \leq N + 1} \) of language pairs as follows [1], [3]:
- Base step:
  \[
  F_0 := L - K, \quad H_0 := K.
  \]
- Induction step:
  \[
  F_{k+1} := F_k \cap \bigcap_{i \in I} M_i^{-1} M_i(H_k),
  \]
  \[
  H_{k+1} := H_k \cap \bigcap_{i \in I} M_i^{-1} M_i(F_k). \]

The computation of the sequence \( \{ (F_k, H_k) \}_{0 \leq k \leq N + 1} \) of language pairs starts with \( F_0 = L - K \), the set of Failure traces, and \( H_0 = K \), the set of nonfailure or “Healthy” traces. Note that \( F_{N+1} \) is a sublanguage of \( F_0 \). Once \( F_{N+1} \) consists of those traces for which for each \( i \in I \) there exists an \( M_i \) indistinguishable trace in \( H_k \). As a result when the plant executes a trace in \( F_{N+1} \) all the local diagnosers will be ambiguous as to whether the executed trace is in \( F_{N+1} \) or in \( H_k \). The sublanguage \( H_{N+1} \) of \( H_k \) can be understood in a similar fashion.

Using the finite sequence \( \{ (F_k, H_k) \}_{0 \leq k \leq N} \) of language pairs, a local diagnoser computes its diagnosis decision and associates a level of ambiguity with such a decision as follows. For each \( s \in L \), the \( i \)-th local diagnoser \( D_i \) computes
\[
n_i^l(M_i(s)) := \min \{ k | [M_i(s) \notin M_i(H_k)] \lor [k = N + 1] \},
\]
\[
n_i^b(M_i(s)) := \min \{ k | [M_i(s) \notin M_i(F_k)] \lor [k = N + 1] \}. \quad (5)
\]

Note that \( n_i^l(M_i(s)) \) and \( n_i^b(M_i(s)) \) are bounded above by \( N + 1 \). Here \( n_i^l(M_i(s)) \) represents the ambiguity level of a failure decision “contemplated” by the \( i \)-th diagnoser following the observation \( M_i(s) \).

When \( n_i^l(M_i(s)) < N + 1 \), it denotes the minimum index \( k \) such that the observation \( M_i(s) \) does not match with the observations of any of the traces in \( H_k \).

Similarly, the notation \( n_i^b(M_i(s)) \) represents the ambiguity level of a nonfailure decision “contemplated” by the \( i \)-th diagnoser following the observation \( M_i(s) \). Then, the diagnosis decision and ambiguity level following an observation \( M_i(s) \in M_i(L) \), i.e., \( D_i(M_i(s)) = (c_i(M_i(s)), n_i(M_i(s))) \), is determined as follows:
\[
c_i(M_i(s)) = \begin{cases} 0, & \text{if } n_i^l(M_i(s)) < n_i^b(M_i(s)) \\ 1, & \text{if } n_i^l(M_i(s)) < n_i^b(M_i(s)) \\ \phi, & \text{if } n_i^l(M_i(s)) = n_i^b(M_i(s)) \end{cases}
\]

and
\[
n_i(M_i(s)) = \min \{ n_i^l(M_i(s)), n_i^b(M_i(s)) \}. \quad (7)
\]
Example 3: We consider a plant modeled by the finite automaton $G$ shown in Fig. 3(a). Let $|I| = 2$,

$$
M_1(\sigma) = \begin{cases} 
\sigma, & \text{if } \sigma \in \{a, a', a'', c, d, d'\} \\
\varepsilon, & \text{otherwise.}
\end{cases}
$$

$$
M_2(\sigma) = \begin{cases} 
\sigma, & \text{if } \sigma \in \{b, b', b'', c, d, d'\} \\
\varepsilon, & \text{otherwise.}
\end{cases}
$$

Also, let $K \subseteq L$ be a language generated by the finite automaton $R$ shown in Fig. 3(b).

We synthesize the decentralized diagnoser using (4)-(7) for $N = 2$. We first need to compute the language pairs $\{(F_k, H_k)\}_{0 \leq k \leq 2}$. Initially, we have

$$
F_0 = dd'(fc^* + ab'fca + ba'fca'),
$$

$$
H_0 = \text{pr}(dd'(a(c^* + b'a'c^*) + b(c^* + b'b'c^*)�))
$$

Since

$$
M_1(F_0) = dd'(c^* + ac^* + a'c^*�),
$$

$$
M_2(F_0) = dd'(c^* + b'b'c^* + bc^*�),
$$

$$
M_1(H_0) = \text{pr}(dd'(a(c^* + a''c^*) + c^* + a'c^*)�),
$$

$$
M_2(H_0) = \text{pr}(dd'(c^* + b'b'c^* + b(c^* + b'b'c^*)�)),
$$

we have

$$
F_1 = F_0, \quad H_1 = dd'(\text{pr}(a(c^* + b') + b(c^* + a')))�.
$$

Also, since

$$
M_1(F_1) = dd'(c^* + ac^* + a'c^*�),
$$

$$
M_2(F_1) = dd'(c^* + b'b'c^* + bc^*�),
$$

$$
M_1(H_1) = dd'(\text{pr}(a(c^* + e) + c^* + a')�),
$$

$$
M_2(H_1) = dd'(\text{pr}(c^* + b' + b(c^* + e))�),
$$

we have

$$
F_2 = dd'(fc^* + ab'f + ba'f�), \quad H_2 = H_1. \quad (\exists m \in N) (\forall s \in H_{N+1})(\exists u \leq t \text{ s.t. } su \notin H_{N+1}).
$$

The local decisions of $D_1$ and $D_2$ are shown in Table I. For example, $D_2(\text{dd'ac})$ is computed as follows. By (4) and (5), we have $n_1(\text{dd'ac}) = 3$ and $n_2(\text{dd'ac}) = 2$. Since $2 = n_1(\text{dd'ac}) < n_2(\text{dd'ac}) = 3$, we have $c_1(\text{dd'ac}) = 0$ and $n_1(\text{dd'ac}) = 2$, which implies that $D_1$ makes a nonfailure decision following the observation $\text{dd'ac} \in M_1(L)$ with the ambiguity level $2$.

Then, the global diagnosis decisions of the decentralized diagnoser $\{D_i\}_{i \in I}$ are computed as shown in Table II. For example, $\{D_i\}_{i \in I}(\text{dd'ac})$ is computed as follows. Since $2 = n_1(\text{dd'ac}) < n_2(\text{dd'ac}) = 3$ and $c_1(\text{dd'ac}) = 0$, we have $n(\text{dd'ac}) = 2$ and $\{D_i\}_{i \in I}(\text{dd'ac}) = 0$.

We introduce the notion of $N$-inference diagnosability for NonFailures (also called $N$-inference NF-diagnosability). The decentralized diagnoser has no missed detections and false alarms under this condition. In fact this condition serves as a necessary and sufficient condition for the existence of an $N$-inferring decentralized diagnoser with no missed detections and false alarms.

Definition 2: The pair $(L, K)$ of languages is said to be $N$-inference NF-diagnosable if

$$(\exists m \in N) (\forall s \in H_{N+1})(\exists u \leq t \text{ s.t. } su \notin H_{N+1}).$$

The property of $N$-inference NF-diagnosability requires that the set of healthy traces whose ambiguity is not resolved by the $N$-level inferencing, i.e., traces in $H_{N+1}$, are such that their healthy
extensions beyond a certain bound are guaranteed to possess a prefix whose ambiguity is resolved by at most the N-level inferencing. We show that N-inference NF-diagnosability is a necessary and sufficient condition for the existence of an N-inferencing decentralized diagnoser \( \{ D_i \}_{i \in I} \) satisfying (1), (2), and (3).

**Theorem 1:** There exists an N-inferring decentralized diagnoser \( \{ D_i \}_{i \in I} : L \rightarrow C \) satisfying (1), (2), and (3) if and only if \( (L, K) \) is N-inference NF-diagnosable.

In the following we show that the system of Example 3 is 2-inference NF-diagnosable but it is not 1-inference NF-diagnosable.

**Example 4:** We revisit the setting of Example 3. We have

\[
F_1 = F_0, \quad H_1 = dd' \{ pr(a(c^2 + b') + b(c^2 + a')) \},
\]

\[
F_2 = dd' \{ f(c^2 + ab' f + ba' f), \quad H_2 = H_1.\]

For example, any nonfailure extension of a trace \( dd'ac \in H_1 \) is also in \( H_2 \), which implies that \( (L, K) \) is not 0-inference NF-diagnosable. Further, since \( H_2 = H_1 \), it is not 1-inference NF-diagnosable. Since

\[
M_1(F_2) = dd'(c^2 + a + a'),
\]

\[
M_2(F_2) = dd'(c^2 + b + b'),
\]

\[
M_1(H_2) = dd' \{ pr(a(c^2 + e) + c^2 + a') \},
\]

\[
M_2(H_2) = dd' \{ pr(c^2 + b + b(c^2 + e)) \},
\]

we have

\[
F_3 = F_2, \quad H_3 = dd' \{ pr(ab + ba') \}.
\]

For any \( s \in H_2 \), any nonfailure extension \( st \) with \( |t| \geq 3 \) is not in \( H_3 \), which implies that \( (L, K) \) is 2-inference NF-diagnosable. By Table II, we can verify that \( \{ D_i \}_{i \in I} \) is a 2-inferencing decentralized diagnoser satisfying (1), (2), and (3) for \( m \geq 3 \).

**Remark 1:** In [1], [3], we introduced the notion of N-inferring diagnosability for Failures (also called N-inference F-diagnosability). Given \( N \in \mathbb{N} \), N-inference NF-diagnosability does not imply N-inference F-diagnosability, and vice-versa. For example, we consider the case of \( N = 2 \). The system of Example 3 is 2-inference NF-diagnosable but not 2-inference F-diagnosable. Also, the system of Example 1 is 2-inference F-diagnosable but not 2-inference NF-diagnosable.

The computation of local decisions using (4)-(7) and the verification of N-inference NF-diagnosability require computing the sequence \( \{(F_k, H_k)\}_{0 \leq k \leq N+1} \) of language pairs. In [1], [3], we presented a recursive method for computing it and discussed the complexity. The complexity of this step is polynomial in the sizes of plant/specification models, whereas N-fold exponential in \(|I|\) (the total number of sites) [3].

Let \( R_{HN+1} \) be a finite *determinized* acceptor of \( H_{N+1} \), i.e., \( L_m(R_{HN+1}) = H_{N+1} \). The following theorem shows that N-inferring NF-diagnosability can be verified using \( R_{HN+1} \), and can be easily proved.

**Theorem 2:** The pair \( (L, K) \) of languages is not N-inference NF-diagnosable if and only if there exists a cycle of marked states in a finite determinized acceptor \( R_{HN+1} \) of \( H_{N+1} \).

V. PROPERTIES OF N-INFEERENCE NF-DIAGNOSABILITY

In this section, we establish various properties of N-inference NF-diagnosability. First we establish that the classes of N-inference NF-diagnosable systems form a monotonically increasing sequence as a function of \( N \). Since the sequence \( \{(F_k, H_k)\}_{k \in \mathbb{N}} \) of language pairs is monotonically decreasing as a function of \( k \in \mathbb{N} \), the following result is easily obtained.

**Theorem 3:** For any \( N \in \mathbb{N} \), if the pair \( (L, K) \) of languages is N-inference NF-diagnosable, then it is \( (N+1) \)-inference NF-diagnosable.

\[
(\exists m \in \mathbb{N})(\forall s \in K)(\forall t \in K \text{ s.t. } |t| \geq m)
\]

\[
(\exists u \leq t)(\forall v \in M^{-1} M(su) \cap L; v \in K).
\]

**Theorem 4:** If the pair \( (L, K) \) of languages is N-inference NF-diagnosable, then it is also N-diagnosable.

However, the converse relation of Theorem 4 need not hold. For example, the system of Example 3 is 2-inference NF-diagnosable, but not 1-inference NF-diagnosable.

The converse relation of Theorem 3 need not hold. For example, the system of Example 3 is 2-inference NF-diagnosable, but not 1-inference NF-diagnosable.

Next we show that there are systems that are centrally diagnosable but not diagnosable decentrally. We define a centralized version of diagnosability for nonfailures. The global observation mask \( M \) is defined as a map \( M : \Sigma \cup \{\varepsilon\} \rightarrow (\Delta_1 \cup \{\varepsilon\}) \times (\Delta_2 \cup \{\varepsilon\}) \times \cdots \times (\Delta_n \cup \{\varepsilon\}) \), where for each \( \sigma \in \Sigma \cup \{\varepsilon\} \), \( M(\sigma) = (M_1(\sigma), M_2(\sigma), \ldots, M_n(\sigma)) \).

**Definition 3:** The pair \( (L, K) \) of languages is said to be diagnosable for nonfailures (also called NF-diagnosable) if

\[
(\exists s \in L)(\forall t \in K) |L - |t| \geq m)
\]

\[
(\exists u \leq t)(\forall v \in M^{-1} M(su) \cap L; v \in K).
\]

The converse relation of Theorem 3 need not hold. For example, the system of Example 3 is 2-inference NF-diagnosable, but not 1-inference NF-diagnosable.

The converse relation of Theorem 3 need not hold. For example, the system of Example 3 is 2-inference NF-diagnosable, but not 1-inference NF-diagnosable.
Theorem 5: The pair \((L, K)\) of languages is 0-inference NF-diagnosable if and only if
\[
(\exists m \in \mathcal{N})(\forall s \in K)(\forall t \in K \text{ s.t. } |t| \geq m) (\exists i \in I)(\forall v \in E_i(su); \; u \in K),
\]
where \(E_i(su) := M_i^{-1} M_i(su) \cap L\).

The following remark compares 0-inference NF-diagnosability with the strong codiagnosability [4] defined as follows.

Definition 4: [4] The pair \((L, K)\) of languages is said to be strongly codiagnosable if it is codiagnosable, i.e.,
\[
(\exists m \in \mathcal{N})(\forall s \in L - K)(\forall t \in L - K \text{ s.t. } |t| \geq m) (\exists i \in I)(\forall u \in E_i(st); \; u \in L - K),
\]
and
\[
(\exists m \in \mathcal{N})(\forall s \in K)(\forall t \in K \text{ s.t. } |t| \geq m) (\exists i \in I)(\forall u \in E_i(st); \; u \in K).
\]

Remark 2: Since
\[
(\exists i \in I)(\forall u \in E_i(st); \; u \in K)
\]
implies
\[
(\exists u \leq t)(\exists i \in I)(\forall v \in E_i(su); \; v \in K),
\]
0-inference NF-diagnosability is weaker than the second condition of strong codiagnosability.

The following is an immediate corollary of Theorem 5, and the equivalence of codiagnosability and 0-inference F-diagnosability.

Corollary 1: If the pair \((L, K)\) of languages is strongly codiagnosable, then it is 0-inference F-diagnosable and 0-inference NF-diagnosable.

As shown in the following example, the converse relation of Corollary 1 need not hold.

Example 6: We consider a DES modeled by the automaton \(G\) shown in Fig. 5(a). Let \(|I| = 2\), and
\[
M_1(\sigma) = \begin{cases} \sigma, & \text{if } \sigma \in \{a, a', c\} \\ \epsilon, & \text{otherwise} \end{cases},
\]
\[
M_2(\sigma) = \begin{cases} \sigma, & \text{if } \sigma \in \{b, b', c\} \\ \epsilon, & \text{otherwise} \end{cases}.
\]

Also, we consider a language \(K \subseteq L\) which is generated by the automaton \(R\) shown in Fig. 5(b).

Since the occurrence of the failure can be detected by both \(D_1\) and \(D_2\) after observing \(c\), \((L, K)\) is codiagnosable, or equivalently, 0-inference F-diagnosable. But it is not strongly codiagnosable since for any nonfailure trace \(s \in (aa')^* + (bb')^*\), \(sf \in E_i(s) - K\) (\(i = 1, 2\)). On the other hand, any nonfailure trace whose last element is \(a\) (resp., \(b\)) is unambiguous for \(D_1\) (resp., \(D_2\)), which implies that \((L, K)\) is 0-inference NF-diagnosable.

The notion of NF-codiagnosability introduced in [9] is also similar to that of 0-inference NF-diagnosability.

Definition 5: [9] The pair \((L, K)\) of languages is said to be NF-codiagnosable if
\[
(\exists m \in \mathcal{N})(\forall s \in K)(\forall t \in K \text{ s.t. } |t| \geq m) (\exists i \in I)(\forall uu' \in E_i(st) \text{ s.t. } M_i(u) = M_i(s); \; u \in K).
\]

The following corollary follows from Theorem 5.

Corollary 2: If the pair \((L, K)\) of languages is 0-inference NF-diagnosable, then it is NF-codiagnosable.

Finally we show that the notion of conditional NF-codiagnosability introduced in [9] is similar to that of 1-inference NF-diagnosability. We first prove the following characterization of 1-inference NF-diagnosability.

Theorem 6: The pair \((L, K)\) of languages is 1-inference NF-diagnosable if and only if
\[
(\exists m \in \mathcal{N})(\forall s \in K)(\forall t \in K \text{ s.t. } |t| \geq m) (\exists u \leq t)(\exists i \in I)(\forall v \in E_i(su) \text{ s.t. } v \in L - K) (\exists j \in I)(\forall uu' \in E_j(v); \; w \in L - K).
\]

The following corollary follows from Theorem 6 and compares 1-inference NF-diagnosability with conditional NF-codiagnosability [9] as defined below.

Definition 6: [9] The pair \((L, K)\) of languages is said to be conditionally NF-codiagnosable if
\[
(\exists m \in \mathcal{N})(\forall s \in K)(\forall t \in K \text{ s.t. } |t| \geq m) (\exists i \in I)(\forall uu' \in E_i(st) \text{ s.t. } M_i(u) = M_i(s), \; u \in L - K) (\exists j \in I)(\forall uu' \in E_j(uu'); \; w \in L - K).
\]

Corollary 3: If the pair \((L, K)\) of languages is 1-inference NF-diagnosable, then it is conditionally NF-codiagnosable.

Remark 3: The notion of (conditional) NF-codiagnosability introduced in [9] is weaker than the one we consider since it asks for knowing frequently (with bounded length gaps) whether the system was healthy in a bounded past (as opposed to currently—knowing the nonfailure status currently, rather in bounded past, is more meaningful).

VI. CONCLUSION

The paper studies decentralized diagnosis for nonfailures in an inference-based framework for ambiguity management. Such a framework was first proposed for decentralized control [2] and later used for decentralized diagnosis for failures [1], [3]. As shown in this paper, decentralized diagnosability for failures does not imply that for nonfailures, and vice-versa. Further the following key difference exists: The ambiguity about the occurrence of a failure once resolved remains that way with any additional future observation. The situation is not the same for nonfailures, i.e., additional future observation can cause ambiguity about nonfailures to reoccur. This difference calls for a different formulation for nonfailure diagnosis (when compared to failure diagnosis). We introduce the notion of N-inference NF-diagnosability as a necessary and sufficient condition for the existence of an N-inferring decentralized diagnoser which has no missed detections or false alarms, and for which the ambiguity levels of sure decisions never exceed the bound \(N\) (i.e., at most \(N\) levels of inferencing suffices to arrive at a correct diagnosis decision). We show that higher the value of \(N\), the weaker is the corresponding notion of N-inference NF-diagnosability. Yet, the notion of centralized diagnosability for nonfailures is weaker than N-inference NF-diagnosability for any \(N\). We have provided a method for verifying N-inference NF-diagnosability and synthesized a corresponding decentralized diagnoser. The complexity of verification as well as synthesis is \(N\)-fold exponential in the number of sites.
and so there is a trade-off between the diagnosis capability versus the cost of computation. The parameter $N$ should be chosen so that the on-line computation of the diagnosis decision remains feasible. Extension to the setting of distributed diagnosis (i.e., one involving communication among the local diagnosers) [5] is a future research direction.

REFERENCES