Synthesis of Over-Approximating Inference-Based Decentralized Supervisors for Discrete Event Systems

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

Abstract—In our past work, we presented a framework for the decentralized control of discrete event systems involving inferencing over ambiguities about the system state of various local decision-makers, and introduced the notion of N-inference-observability as an existence condition of a certain decentralized supervisor. When a given specification fails to satisfy the N-inference-observability property, a supervisor achieving the given specification does not exist, and a technique for synthesizing a decentralized supervisor that achieves an N-inference-observable superlanguage is presented here (a dual problem of computing an N-inference-observable sublanguage was studied in our past work).

Index Terms—Discrete event systems, decentralized control, inferencing, knowledge, ambiguity, inference-observability.

I. INTRODUCTION

In any decentralized decision-making paradigm, such as decentralized control, 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 as well as the ambiguities of the others was presented in [3]. 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 [3] and “conditioning” in [9]. These prior inferencing-based approaches were limited to a “single-level” of inferencing, and a comprehensive framework allowing multi-level of inferencing was presented in [1]. The notion of N-inference-observability was formulated in [1] to characterize the class of languages achievable using N levels of inferencing.

When a given specification fails to satisfy the N-inference-observability property, an N-infering decentralized supervisor achieving the given specification does not exist, and a technique for synthesizing a decentralized supervisor that achieves an N-inference-observable superlanguage is presented here (a dual problem of computing an N-inference-observable sublanguage was studied in [5]). Computation of a superlanguage that “over-approximates” or “relaxes” a given specification language is useful in certain applications. For example, in databases, concurrency management is used for avoiding loss of serializability. This can be relaxed by scheduling certain transaction-operations for which it may not be known a-priori whether they can cause a loss in serializability, since it is always possible to “rollback” to a previous consistent state and reschedule those rolled-back operations. This allows for a trade-off between the operational-concurrency and time-cost of rollback and recovery. The computation of synthesizable suplanguages is also quite useful in the context of a fault-tolerant control. See for example [7] where a notion of fault-tolerant control for DESs is introduced: Given a plant, possessing both faulty and nonfaulty behaviors, a goal of fault-tolerant control is to ensure that the plant recovers from any fault, either fully or partially, within a bounded delay. In this setting, the computation of a fault-tolerant control requires the synthesis of a superlanguage (of the specification language) consisting of a certain amount of post-fault behaviors that must be tolerated during the time the recovery actions are being executed. See [6] for more details.

We present a control strategy that synthesizes an N-inference-observable superlanguage of a given specification language. We provide a closed form formula for the synthesized language, and also show that it equals the specification language when the latter is strongly N-inference-observable, a property introduced in this paper. Regardless of the choice of the inferencing level N, the synthesized superlanguage is smaller than the infimal closed, controllable, and C&P-coobservable superlanguage (see Theorem 6); this justifies our superlanguage computation method presented in this paper. The synthesized language also possesses the desired property that as the level of inferencing N is increased, the synthesized language becomes smaller meaning a tighter over-approximation to the specification language is obtained.

II. NOTATION AND PRELIMINARIES

We consider a DES modeled by an automaton \( G = (Q, \Sigma, \delta, q_0, Q_m) \), where \( Q \) is the set of states, \( \Sigma \) is the finite set of events, a partial function \( \delta : Q \times \Sigma \to Q \) is the transition function, \( q_0 \in Q \) is the initial state, and \( Q_m \subseteq Q \) is the set of marked states. Let \( \Sigma^* \) be the set of all finite traces of elements of \( \Sigma \), including the empty trace \( \varepsilon \). The function \( \delta \) can be generalized to \( \delta : Q \times \Sigma^* \to Q \) in the natural way. The generated and marked languages of \( G \), denoted by \( L(G) \) and \( L_m(G) \), respectively, are defined as \( L(G) = \{ s \in \Sigma^* | \delta(q_0, s) \text{ is defined} \} \) and \( L_m(G) = \{ s \in \Sigma^* | \delta(q_0, s) \in Q_m \} \). Let \( K \subseteq \Sigma^* \) be a language. We denote the set of all prefixes of traces in \( K \) by \( \mathcal{P}(K) \). For supervisory control purposes [2], the event set \( \Sigma \) is partitioned into two disjoint subsets \( \Sigma_0 \) and \( \Sigma_{nc} \) of controllable and uncontrollable events, respectively. \( K \) is said to be (prefix-)closed if \( K = \mathcal{P}(K) \). For supervisory control purposes [2], the event set \( \Sigma \) is partitioned into two disjoint subsets \( \Sigma_0 \) and \( \Sigma_{nc} \) of controllable and uncontrollable events, respectively. \( K \) is said to be (prefix-)closed if \( K = \mathcal{P}(K) \).

Let the set \( C = \{0, 1, \phi \} \) be the set of control decisions, where “0” represents a disablement decision, “1” represents an enablement decision, and “\( \phi \)” represents an unsure (or pass) decision. Formally, a supervisor is defined as a map \( S : L(G) \times \Sigma \to C \) such that \( S(s, \sigma) = 1 \) for each \( s \in L(G) \) and \( \sigma \in \Sigma_{nc} \). We define the generated language \( L(S/G) \) under the control action of \( S \). For this, we inductively define a sequence \( \{L^k\} \) of languages as follows:

- \( L^0 := \{\varepsilon\} \);
- \( L^{k+1} := \begin{cases} \{s\sigma \in L(G) \cap L^k\Sigma | S(s, \sigma) = 1\}, & \text{if } L^k \text{ is defined and } \\ \{s\sigma \in L(G) \cap L^k\Sigma | S(s, \sigma) \neq \phi \} & \text{undefined, otherwise.} \end{cases} \)

Then,

\[ L(S/G) := \bigcup_{k \in \mathbb{N}} L^k, \text{ if } \forall k \in \mathbb{N} \text{ } L^k \text{ is defined } \]
\[ \text{undefined, otherwise,} \]

where \( \mathbb{N} \) denotes the set of nonnegative integers.

\( S \) is said to be valid when \( L(S/G) \) is defined, i.e., none of the control decisions for feasible events are unsure. When it is clear from context that \( L(S/G) \) is defined, the validity of \( S \) is understood and not explicitly mentioned. For a valid supervisor \( S \), the definition of \( L(S/G) \) can be presented in the following simplified manner:

- \( \varepsilon \in L(S/G); \)
- \( \forall s \in L(S/G), \forall \sigma \in \Sigma, s\sigma \in L(S/G) \iff [s\sigma \in L(G) \wedge S(s, \sigma) = 1]. \)
We review the inference-based decentralized control framework introduced in [1] and the procedure for synthesizing an N-inference-observable sublanguage introduced in [5]. In the decentralized control setting, there exist \( n \) local supervisors, whose decisions are fused to obtain a global control decision so that the controlled behavior satisfies a (global) specification. Let \( \Sigma_c \) be the set of all controllable events for the \( i \)th local supervisor \( S_i \), \( i \in \{1, 2, \cdots, n\} \), in which case, \( \Sigma_c = \bigcup_{i \in I} \Sigma_{c_i} \). For each controllable event \( \sigma \in \Sigma_c \), the index set of local supervisors for which \( \sigma \) is controllable is denoted by \( I_n(\sigma) = \{i \in I: \sigma \in \Sigma_{c_i}\} \). The limited sensing capability of the \( i \)th local supervisor \( S_i \) (\( i \) is represented as a local observation mask, \( M_i : \Sigma \cup \{e\} \rightarrow \Delta_i \cup \{e\} \), where \( \Delta_i \) is the set of locally observed symbols, and \( M_i(e) = e \). Traces \( s, s' \in \Sigma^* \) are said to be \( M_i \)-indistinguishable if \( M_i(s) = M_i(s') \).

In our inference-based decentralized control framework, each local supervisor uses its observations of the system behavior to come up with its control decision together with an ambiguity level for that control decision. A local supervisor will issue a disablement (resp., enablement) decision with an ambiguity level \( N \) for a locally controllable event following a certain observation if for each “ambiguous” trace, producing the same observation as the one received, and possessing a feasible and legal (resp., illegal) controllable event extension, that local supervisor knows there exists another local supervisor that can issue an enablement (resp., disablement) decision with an ambiguity level at most \( N - 1 \). The global control decision for a controllable event is taken to be the same as a local control decision whose ambiguity level is the minimum.

Each inference-based local supervisor \( S_i \) is a map \( M_i : L(G) \times \Sigma \rightarrow C \times N \), where for each \( s \in L(G) \) and \( \sigma \in \Sigma_{c_i} \), \( S_i(M_i(s), \sigma) = (c_i(M_i(s), \sigma), n_i(M_i(s), \sigma)) \). Here \( c_i(M_i(s), \sigma) \in C \) denotes the control decision of \( S_i \) for a locally controllable event \( \sigma \in \Sigma_{c_i} \) following an observation \( M_i(s) \in M_i(L(G)) \), and \( n_i(M_i(s), \sigma) \in N \) denotes the ambiguity level of the control decision of \( S_i \). Let \( n(s, \sigma) \) be the minimal ambiguity level of local decisions, i.e., \( n(s, \sigma) := \min_{i \in I_n(\sigma)} n_i(M_i(s), \sigma) \).

Given local supervisors \( S_i \) (\( i \in I \)), the corresponding decentralized supervisor, denoted by \( \{S_i\}_{i \in I} : L(G) \times \Sigma \rightarrow C \), issues a global control decision that is the same as the minimum ambiguity level local control decision:

\[
\{S_i\}_{i \in I}(s, \sigma) := \begin{cases} 
1, & \text{if } \forall i \in I_n(\sigma) \text{ s.t. } n_i(M_i(s), \sigma) = n(s, \sigma) ; \\
0, & \text{if } \forall i \in I_n(\sigma) \text{ s.t. } n_i(M_i(s), \sigma) = n(s, \sigma) ; \\
\phi, & \text{otherwise}.
\end{cases}
\]

On the other hand, \( \{S_i\}_{i \in I}(s, \sigma) := 1 \) for any \( s \in L(G) \) and \( \sigma \in \Sigma_{c_i} \). \( \{S_i\}_{i \in I} \) is said to be \( N \)-infering if for each controllable event, all winning enablement or all winning disablement decisions have ambiguity levels below \( N \).

**Definition 1:** [1] A decentralized supervisor \( \{S_i\}_{i \in I} : L(G) \times \Sigma \rightarrow C \) is said to be \( N \)-infering if for each \( s \in \Sigma_c \), either

\[
\forall s \in L(\{S_i\}_{i \in I}/G) \text{ s.t. } \sigma \in L(G), \quad \{S_i\}_{i \in I}(s, \sigma) = 0 \Rightarrow n(s, \sigma) \leq N.
\]

or

\[
\forall s \in L(\{S_i\}_{i \in I}/G) \text{ s.t. } \sigma \in L(G), \quad \{S_i\}_{i \in I}(s, \sigma) = 1 \Rightarrow n(s, \sigma) \leq N.
\]

Given a specification \( K \subseteq L(G) \) of the plant language, we divide \( K \) into a set of language pairs, one pair for each controllable event \( \sigma \in \Sigma_c \). The set \( D_0(\sigma) \subseteq K \) is the set of traces in \( K \) where \( \sigma \) must be disabled, whereas the set \( E_0(\sigma) \subseteq K \) is the set of traces where \( \sigma \) must be enabled. Using these as the base step, we inductively define a monotonically decreasing sequence of language pairs \( (D_k(\sigma), E_k(\sigma)) \) as follows:

- \( D_0(\sigma) := \{s \in K | s \in L(G) - K\} \)
- \( E_0(\sigma) := \{s \in K | s \in K \} \)
- \( D_{k+1}(\sigma) := D_k(\sigma) \cap \left( \bigcap_{i \in I_n(\sigma)} M_i^{-1} M_i(E_k(\sigma)) \right) \)
- \( E_{k+1}(\sigma) := E_k(\sigma) \cap \left( \bigcap_{i \in I_n(\sigma)} M_i^{-1} M_i(D_k(\sigma)) \right) \)

Note that \( D_{k+1}(\sigma) \) is a sublanguage of \( D_k(\sigma) \) consisting of traces for which there exists an \( M_i \)-indistinguishable trace in \( E_k(\sigma) \) for each \( i \in I_n(\sigma) \). As a result all the local supervisors that have control over \( \sigma \) will be ambiguous about their control decision for \( \sigma \) following the execution of a trace in \( D_{k+1}(\sigma) \). The sublanguage \( E_{k+1}(\sigma) \) of \( E_k(\sigma) \) can be understood in a similar fashion.

Then we have the following definition of \( N \)-inference-observability.

**Definition 2:** [1] A language \( K \subseteq L(G) \) is said to be \( N \)-inference-observable if for any \( \sigma \in \Sigma_c \), \( D_{N+1}(\sigma) = \emptyset \) or \( E_{N+1}(\sigma) = \emptyset \).

The following theorem shows the necessity and sufficiency of \( N \)-inference-observability for the existence of an \( N \)-infering decentralized supervisor enforcing the given specification.

**Theorem 1:** [1] For a nonempty language \( K \subseteq L(G) \), there exists an \( N \)-inference decentralized supervisor \( \{S_i\}_{i \in I} : L(G) \times \Sigma \rightarrow C \) such that \( L(\{S_i\}_{i \in I}) = K \) if and only if \( K \) is controllable and \( N \)-inference-observable.

When a given specification fails to satisfy the \( N \)-inference-observability property, an \( N \)-inference supervisor achieving the entire specification does not exist, and a technique for synthesizing a decentralized supervisor that achieves an \( N \)-inference-observable sublanguage of the specification was presented in [5]. The main idea was to issue a disablement decision tagged with ambiguity level \( N + 1 \) for traces for which a control decision remains ambiguous even after \( N \) levels of inferencing. The sublanguage synthesis procedure is summarized next. For each \( s \in L(G) \) and \( \sigma \in \Sigma_{c_i} \), the ith local supervisor \( S_i^N \) computes

\[
n_{i}^{N-N}(M_i(s), \sigma) := \begin{cases} 
\min\{k \in N \cap M_i(s) \notin M_i(E_k(\sigma))\}, & \text{if } D_{N+1}(\sigma) = \emptyset \lor E_{N+1}(\sigma) \neq \emptyset, \\
\min\{k \in N \cap [M_i(s) \notin M_i(E_k(\sigma)) \lor [k = N + 1\} & \text{if } D_{N+1}(\sigma) \neq \emptyset \land E_{N+1}(\sigma) \neq \emptyset,
\end{cases}
\]

\[
n_{i}^{N-N}(M_i(s), \sigma) := \begin{cases} 
\min\{k \in N \cap M_i(s) \notin M_i(D_k(\sigma))\}, & \text{if } D_{N+1}(\sigma) = \emptyset \lor E_{N+1}(\sigma) \neq \emptyset, \\
\min\{k \in N \cap [M_i(s) \notin M_i(D_k(\sigma)) \lor [k = N + 1\} & \text{if } D_{N+1}(\sigma) \neq \emptyset \land E_{N+1}(\sigma) \neq \emptyset,
\end{cases}
\]

The notation \( n_{i}^{N-N}(M_i(s), \sigma) \) represents the ambiguity level of a disablement decision “contemplated” by the ith supervisor for the event \( \sigma \) following the observation \( M_i(s) \). Similarly, \( n_{i}^{N-N}(M_i(s), \sigma) \) represents the ambiguity level of an enablement decision “contemplated” by the ith supervisor for the event \( \sigma \) following the observation \( M_i(s) \). Then the control decision and its ambiguity level, i.e., \( S_i^N(M_i(s), \sigma) = (c_i^N(M_i(s), \sigma), n_i^N(M_i(s), \sigma)) \), is determined as
follows:

\[
c_i^N(M_i(s), σ) = \begin{cases} 
1, & \text{if } n_{i,N}^d(M_i(s), σ) < n_{i,N}^d(M_i(s), σ) \\
0, & \text{if } [D_{N+1}^e(σ) \neq Φ \land E_{N+1}^e(σ) \neq Φ] \\
& \land n_{i,N}^d(M_i(s), σ) = n_{i,N}^e(M_i(s), σ) = N + 1 \}
\end{cases}
\]

and

\[
n_i^N(M_i(s), σ) = \min\{n_i^d(M_i(s), σ), n_i^e(M_i(s), σ)\}. \quad (4)
\]

It was shown in [5] that the decentralized supervisor \( \{S_i^N\}_{i ∈ I} : L(G) × Σ → C \) consists of local supervisors \( S_i^N : M_i(L(G)) × Σ_i → C \times N \) (\( i ∈ I \)) given by (1)–(4) is N-inferencing and satisfies \( L(\{S_i^N\}_{i ∈ I} / G) \subseteq K \) whenever \( K \) is controllable. Further, if \( K \) is controllable and N-inference-observable, then \( L(\{S_i^N\}_{i ∈ I} / G) = K \) holds.

IV. SYNTHESIS FOR ENFORCING N-INFERENCE-OBSERVABLE SUPERLANGUAGE

The decentralized supervisor for which the local supervisors are given by (1)–(4) issues a disablement decision tagged with ambiguity level \( N + 1 \) in those situations when a control decision remains ambiguous even after \( N \) levels of inferencing. It turns out that just doing the “dual”, namely, issuing an enablement decision tagged with the ambiguity level \( N + 1 \) in the aforementioned situations is not enough to achieve an N-inference-observable superlanguage.

For the sake of argument, let us modify the decentralized supervisor \( \{S_i^N\}_{i ∈ I} \) by replacing the disablement decision in (3) with the enablement decision as follows:

\[
c_i^N(M_i(s), σ) = \begin{cases} 
1, & \text{if } [n_{i,N}^d(M_i(s), σ) < n_{i,N}^d(M_i(s), σ) \\
& \land [D_{N+1}^e(σ) \neq Φ \land E_{N+1}^e(σ) \neq Φ] \\
0, & \text{otherwise}
\end{cases}
\]

We show through the following example that the above modified supervisor need not be valid, i.e., there may exist traces in \( L(G) − K \) following which the control decision may be “unsafe”.

**Example 1:** We consider a plant \( G \) with \( L(G) = \{abc, bacd\} \), and a specification language \( K = \{abc, bac\} \). Let \( n = 2, Σ = Σ_1c = Σ_2c = \{c\}, M_1(σ) = \{σ, ε\}, \text{and } M_2(σ) = \{σ, ε\}. \)

Since \( a \) and \( b \) are uncontrollable, \( ab \) is enabled. Also, we have \( E_k(ε) = \{ab\} \) and \( D_k(c) = \{ba\} \) for any \( k ∈ N \). Since \( M_1(1a) = a \in M_1(E_{N+1}(c)) \cap M_1(D_{N+1}(c)), \) we have \( n_{i,N}^d(M_1(1a), c) = n_{i,N}^e(M_2(ba), c) = N + 1 \). In the same way, we can obtain \( n_{1,N}^d(M_2(ba), c) = n_{2,N}^e(M_2(ba), c) = N + 1 \). By (5) and (4), the controllable event \( c \) is enabled following \( ba \) with the ambiguity level \( N + 1 \). Further, since \( d \) is uncontrollable, it is enabled following \( bacd \). Since \( M_1(bacd) = ad \notin M_1(E_0(ε)) \) and \( M_1(bacd) \notin M_1(D_0(ε)) \), the ambiguity levels of both the local enabling and disabling decisions of \( S_i^N \) are zero. So the local control decision of \( S_i^N \) on \( c \) following \( bacd \) is unsure. The local control decision of \( S_2 \) on \( c \) following \( bacd \) is unsure, too. Therefore, the global decision on \( c \) following \( bacd \) is unsure, which implies that the modified supervisor \( \{S_i^N\}_{i ∈ I} \) using (5) instead of (3) is not valid.

The reason why the modified supervisor \( \{S_i^N\}_{i ∈ I} \) is not valid is that traces in \( L(G) − K \) are not taken into account in computing the control decisions, while such traces do get included in the synthesized language because of the enablement decisions following the traces for which a control decision remains ambiguous even after \( N \) levels of inferencing. In order to also take the traces in \( L(G) − K \) into account, we define a new monotonically decreasing sequence of language pairs \( (D_k(σ), E_k(σ)) \). To enforce a superlanguage of \( K \), an enablement decision is required for \( σ ∈ Σ \), following traces in \( E_0(σ) := \{s ∈ L(G) \mid σ ∈ K\} \) and \( D_0(σ) := \{σ ∈ K\} \). Then the traces that can cause ambiguity are the traces in \( D_k(σ) = \{s ∈ L(G) \mid σ ∈ K\} \), following which a disablement decision for \( σ \) is desired (so as to maintain closeness with \( K \)). This motivates us to consider the following monotonically decreasing sequence of language pairs for each \( σ ∈ Σ \) (which are then used to synthesize a decentralized supervisor for achieving an N-inference-observable superlanguage):

\[
\tilde{D}_k(σ) := \{s ∈ L(G) \mid σ ∈ K\}, \quad \tilde{E}_k(σ) := \{s ∈ L(G) \mid σ ∈ K\}.
\]

For each \( s ∈ L(G) \) and \( σ ∈ Σ_c \), let

\[
\tilde{n}_{i,N}^d(M_i(s), σ) := \min\{k ∈ N \mid M_i(s) \notin M_i(\tilde{E}_k(σ))\},
\]

\[
\tilde{n}_{i,N}^e(M_i(s), σ) := \min\{k ∈ N \mid M_i(s) \notin M_i(\tilde{D}_k(σ))\},
\]

\[
\tilde{n}_{i,N}^d(M_i(s), σ) := \min\{k ∈ N \mid M_i(s) \notin M_i(\tilde{D}_k(σ))\},
\]

\[
\tilde{n}_{i,N}^e(M_i(s), σ) := \min\{k ∈ N \mid M_i(s) \notin M_i(\tilde{D}_k(σ))\}.
\]

We define a local supervisor \( \tilde{S}_i^N : M_i(L(G)) × Σ_i → C × N \). The pair \( \tilde{S}_i^N(M_i(s), σ) = (\tilde{c}_i^N(M_i(s), σ), \tilde{n}_{i,N}^d(M_i(s), σ)) \) of its control decision and ambiguity level for a locally controllable event \( σ ∈ Σ_i \) following an observation \( M_i(s) ∈ M_i(L(G)) \) is determined as follows:

\[
\tilde{c}_i^N(M_i(s), σ) = \begin{cases} 
1, & \text{if } n_{i,N}^d(M_i(s), σ) < n_{i,N}^d(M_i(s), σ) \\
& \land [\tilde{D}_{N+1}(σ) \neq Φ \land \tilde{E}_{N+1}(σ) \neq Φ] \\
0, & \text{otherwise}
\end{cases}
\]

and

\[
\tilde{n}_{i,N}^N(M_i(s), σ) = \min\{n_{i,N}^d(M_i(s), σ), \tilde{n}_{i,N}^e(M_i(s), σ)\}. \quad (9)
\]

We denote the minimal ambiguity level of local decisions by \( \tilde{n}_{i,N}(σ), \text{ i.e., } \tilde{n}_{i,N}(σ) := \min_{σ∈Iσ(σ)} \tilde{n}_{i,N}(M_i(s), σ) \).

We first show that the decentralized supervisor defined by the local supervisors (6)–(9) is valid and achieves a superlanguage of \( K \). This requires the following lemma, whose proof is analogous to that of [5, Lemma 2].

**Lemma 1:** For any \( N ∈ N \), consider the decentralized supervisor \( \{S_i^N\}_{i ∈ I} : L(G) × Σ → C \) for which the local supervisors are given by (6)–(9). Then for any \( s ∈ L(G) \) and any \( σ ∈ Σ_c \),

\[
σ ∈ L(G) \Rightarrow \{S_i^N\}_{i ∈ I}(s, σ) ∈ \{0, 1\},
\]

\[
σ ∈ K \Rightarrow \{S_i^N\}_{i ∈ I}(s, σ) = 1.
\]
Using the above lemma, the following lemma shows that the decentralized supervisor defined by the local supervisors (6)–(9) is valid and achieves a superlanguage of $\overline{K}$.

**Lemma 2:** For any $N \in \mathbb{N}$, consider the decentralized supervisor $\{\overline{S}^N_i\}_{i \in I} : L(G) \times \Sigma \to C$ for which the local supervisors are given by (6)–(9). Then $L(\{\overline{S}^N_i\}_{i \in I}/G)$ is defined and $\overline{K} \subseteq L(\{\overline{S}^N_i\}_{i \in I}/G)$.

The next lemma, whose proof is analogous to that of [5, Lemma 4], establishes the $N$-inferingness of the decentralized supervisor defined by the local supervisors (6)–(9).

**Lemma 3:** For any $N \in \mathbb{N}$, the decentralized supervisor $\{\overline{S}^N_i\}_{i \in I} : L(G) \times \Sigma \to C$ for which the local supervisors are given by (6)–(9) is $N$-inerring.

Using the lemmas of the section, the main result of the section is established in the following theorem.

**Theorem 2:** For any $N \in \mathbb{N}$, consider the decentralized supervisor $\{\overline{S}^N_i\}_{i \in I} : L(G) \times \Sigma \to C$ for which the local supervisors are given by (6)–(9). Then $L(\{\overline{S}^N_i\}_{i \in I}/G)$ is a closed, controllable, and $N$-inference-observable superlanguage of $\overline{K}$. Further, $\{\overline{S}^N_i\}_{i \in I}$ is $N$-inerring.

**Remark 1:** From the definition of local supervisors given by (6)–(9), their synthesis complexity is determined by the complexity of computing the languages $\{D_k(\sigma), E_k(\sigma)\}$ for which the local supervisors are given by (6)–(9). Thus, $L(\{\overline{S}^N_i\}_{i \in I}/G)$ is a closed, controllable, and $N$-inference-observable superlanguage of $\overline{K}$. Further, $\{\overline{S}^N_i\}_{i \in I}$ is $N$-inerring.

**Example 2:** We consider a plant modeled by the automaton $G$ shown in Fig. 1(a). Let $n = 2$, $\Sigma_c = \Sigma_{ic} = \Sigma_{2c} = \{c\}$.

$$\begin{align*}
M_1(\sigma) &= \begin{cases} 
\sigma, & \text{if } \sigma \in \{a, a', a'', d\} \\
\epsilon, & \text{otherwise}
\end{cases} \\
M_2(\sigma) &= \begin{cases} 
\sigma, & \text{if } \sigma \in \{b, b', b'', d\} \\
\epsilon, & \text{otherwise}
\end{cases}
\end{align*}$$

Also, let $K \subseteq L(G)$ be a closed language generated by the automaton $G_K$ shown in Fig. 1(b). $K$ is controllable, but it is not 2-inference-observable [5].

We synthesize the decentralized supervisor $\{\overline{S}^N_i\}_{i \in I}$ for the controllable language $K$. We need to compute the languages $\{\overline{D}_k(c), \overline{E}_k(c)\}$ for $k \leq 3$ in order to synthesize the local supervisors $S^N_1$ and $S^N_2$ given by (6)–(9).

We have $\overline{D}_0(c) = \{a, b, ab'a'', ba'bb', d, dab', dba'\}$,

We have $\overline{E}_0(c) = \{a, b, ba'c, da, db, dab'a'', dab'b'\}$.

The local decisions of $S^N_1$ and $S^N_2$ computed using (6)–(9) are shown in Table I. Then, the global control decisions of the decentralized supervisor $\{\overline{S}^N_i\}_{i \in I}$ on $c$ are computed as shown in Table II. It follows from Table II that $L(\{\overline{S}^N_i\}_{i \in I}/G)$ is defined and $K \subseteq L(\{\overline{S}^N_i\}_{i \in I}/G)$. The equality does not hold since $dc$ is illegal but $c$ is enabled following $d$. The automaton shown in Fig. 2 generates $L(\{\overline{S}^N_i\}_{i \in I}/G)$. By Theorem 2, $L(\{\overline{S}^N_i\}_{i \in I}/G)$ is 2-inference-observable, and $\{\overline{S}^N_i\}_{i \in I}$ is 2-inerring.
In this section, we establish several properties attesting to the quality of the supervisor defined. The first property establishes a necessary and sufficient condition of strong $N$-inference-observability under which the language synthesized by the decentralized supervisor is the same as the specification language. We also obtain a formula of the achieved superlanguage. Using this formula, we next show that as the inferencing level $N$ is increased, the achieved superlanguage becomes smaller, i.e., a tighter over-approximation results. Finally, regardless of the level of inferencing explored, the proposed supervisor achieves the language smaller than the infimal closed, controllable, and C&P-coobservable superlanguage.

The notion of strong $N$-inference-observability is defined as follows.

Definition 3: A language $K \subseteq L(G)$ is said to be strongly $N$-inference-observable if, for any $\sigma \in \Sigma_c$, $D_{N+1}(\sigma) \cap D_0(\sigma) = \emptyset$ or $E_{N+1}(\sigma) = E_0(\sigma) = \emptyset$.

Remark 2: It is easy to see using an inductive argument that, for each $k \in N$ and $\sigma \in \Sigma_c$, $E_k(\sigma) \subseteq E_k(\sigma)$ and $D_k(\sigma) \subseteq D_k(\sigma)$. It follows then that the strong $N$-inference-observability is indeed stronger than the $N$-inference-observability. Strong $N$-inference-observability can be understood in a similar way as $N$-inference-observability introduced in [1], where an intuitive interpretation of the latter concept can also be found.

We show that controllability and strong $N$-inference-observability of $K$ are necessary and sufficient conditions for the decentralized supervisor $\{\hat{S}_i^N\} \subseteq L(G)$ to achieve exactly $\overline{K}$. We need the following lemma which clarifies the condition when an illegal controllable event gets enabled by the decentralized supervisor $\{\hat{S}_i^N\} \subseteq L(G)$. The proof of this lemma is analogous to that of [5, Lemma 5].

Lemma 4: For any $N \in N$, consider the decentralized supervisor $\{\hat{S}_i^N\} : L(G) \times \Sigma \rightarrow C$ for which the local supervisors are given by (6)--(9). Then for any $s \in L(G)$ and any $\sigma \in \Sigma_c$ such that $s \in L(G) - \overline{K}$,

$$\{\hat{S}_i^N\} \subseteq L(G) \quad \text{if and only if} \quad \{\hat{S}_i^N\} \subseteq L(G) \quad \text{and} \quad \{\hat{S}_i^N\} \subseteq L(G) - \overline{K}.$$  

The following theorem follows from Lemmas 1 and 4.

Theorem 3: For any $N \in N$, consider the decentralized supervisor $\{\hat{S}_i^N\} : L(G) \times \Sigma \rightarrow C$ for which the local supervisors are given by (6)--(9). Then, $L(\{\hat{S}_i^N\} \subseteq L(G))$ is $\overline{K}$ if and only if $K$ is nonempty, controllable, and strongly $N$-inference-observable.

Proof: We first prove the sufficiency part. By Lemma 1, it suffices to show that $\{\hat{S}_i^N\} \subseteq L(G) - \overline{K}$ for any $s \in \overline{K}$ and $\sigma \in \Sigma_c$ such that $s \in L(G) - \overline{K}$. Since $K$ is strongly $N$-inference-observable, $D_{N+1}(\sigma) \cap D_0(\sigma) = \emptyset$ or $E_{N+1}(\sigma) = \emptyset$. By Lemma 4, if $E_{N+1}(\sigma) = \emptyset$, then $\{\hat{S}_i^N\} \subseteq L(G)$ is $\overline{K}$. We consider the case that $D_{N+1}(\sigma) \cap D_0(\sigma) = \emptyset$. Since $s \in D_0(\sigma)$, we have $s \notin D_{N+1}(\sigma)$. It follows from Lemma 4 that $\{\hat{S}_i^N\} \subseteq L(G) - \overline{K}$.

We next prove the necessity part. Since $L(\{\hat{S}_i^N\} \subseteq L(G)) = \overline{K}$, $K$ is nonempty and controllable. It remains to show that $K$ is strongly $N$-inference-observable. Suppose for contradiction that there exists $\sigma \in \Sigma_c$ such that $D_{N+1}(\sigma) \cap D_0(\sigma) = \emptyset$ and $E_{N+1}(\sigma) = \emptyset$. Consider any $s \in D_{N+1}(\sigma) \cap D_0(\sigma)$. We have $s \notin \overline{K}$ and $s \in L(G) - \overline{K}$. Further, we have by Lemma 4 that $\{\hat{S}_i^N\} \subseteq L(G) - \overline{K}$. Since $s \in \overline{K}$, $L(\{\hat{S}_i^N\} \subseteq L(G))$, we have $s \in L(G) - \overline{K}$. This is a contradiction.

The following example shows that the necessary and sufficient condition of Theorem 3 is strictly stronger than the condition of $N$-inference-observability and controllability.

**Example 3:** We consider a plant modeled by the automaton $G$ shown in Fig. 3(a). Let $n = 2$, $\Sigma_c = \Sigma_1c = \Sigma_2c = \{a, c\}$,

$$M_1(\sigma) = \begin{cases} \sigma, & \text{if } \sigma \in \{a, a', d\} \\ \varepsilon, & \text{otherwise} \end{cases} \quad \text{and} \quad M_2(\sigma) = \begin{cases} \sigma, & \text{if } \sigma \in \{b, b', d\} \\ \varepsilon, & \text{otherwise} \end{cases}$$

Also, let $K \subseteq L(G)$ be a closed language generated by the automaton $G_K$ shown in Fig. 3(b). Clearly, $K$ is controllable. Also, by [1, Example 1], $K$ is 2-inference-observable.

We synthesize the decentralized supervisor $\hat{S}^2_i$ for both $K$ and $\hat{S}^2_i \subseteq L(G)$. Then $L(\hat{S}^2_i \subseteq L(G))$ is defined and $K \subseteq L(\hat{S}^2_i \subseteq L(G))$. The equality does not hold since $bc$ is illegal but $c$ is enabled following $b$. The automaton shown in Fig. 4 generates $L(\hat{S}^2_i \subseteq L(G))$.
The paper complements our prior work on an inference-based framework for decentralized control [1] by proposing a scheme to synthesize a decentralized supervisor when the given specification language is not necessarily achievable, and instead an over-approximation (i.e., a superlanguage) to the specification language is achieved (a dual problem of computing a sublanguage was studied in [5]). The proposed scheme is parameterized by $N$ representing the level of inferencing, and we establish the desired property that as $N$ is increased, a tighter over-approximation to the specification language results. A user can thus choose $N$ based on the desired degree of closeness to the specification language versus the degree of computational complexity.

**REFERENCES**


