Corrections to “Polynomial Test for Stochastic Diagnosability of Discrete-Event Systems”

Jun Chen, Student Member, IEEE, Christoforos Keroglou, Christoforos N. Hadjicostis, Senior Member, IEEE, and Ratnesh Kumar, Fellow, IEEE

Abstract—This paper provides corrections to the algorithms presented by Chen et al. in 2013 for testing diagnosability of stochastic discrete event systems.

Index Terms—Discrete event systems, failure diagnosis, complexity, PSPACE-hard

I. INTRODUCTION

Two notions of diagnosability for stochastic discrete event systems (DESs) were studied in [1]. It turns out that the nondeterminism resulting from partial observability was incorrectly handled, and the reported testing algorithms only test the sufficiency condition for non-diagnosability. (See Example 1 below.) Corrected algorithms are presented below. We first illustrate the drawback of the testing algorithms of [1].

Example 1: Consider the stochastic plant model $G$ and deterministic nonfault specification generator $R$ shown in Fig. 1, where $f$ is a fault event and unobservable, and $e$ is the only other unobservable event. The behaviors after the occurrence of $f$ as well as $e$ are identical, and so clearly the system is not S-Diagnosable as well as not SS-Diagnosable (see Definition 1 below). However, in the testing automaton obtained using Algorithm of [1], as shown in Fig. 1(d), there is no closed ambiguous strongly connected component (SCC) or bi-closed ambiguous SCC (whose existence is required by the algorithms of [1] for violation of S- and S-Diagnosability, respectively).

In this correction, we present necessary and sufficient conditions for SS-Diagnosability and S-Diagnosability that properly account for nondeterminism. Our testing algorithm for SS-Diagnosability is of exponential complexity. Separate polynomial tests for sufficiency, and also for necessity, are also provided. We also show that polynomial test for necessity and sufficiency is (likely) not possible by establishing the PSPACE-hardness of SS-Diagnosability. We briefly review the required notation and preliminaries; more details can be found in [1, Section 2].

Notations: A stochastic DES can be modeled as a stochastic automaton $G$ which is denoted by $G = (X, Σ, α, x₀)$, where $X$ is the set of states, $Σ$ is the finite set of events, $x₀ ∈ X$ is the initial state, and $α : X × Σ × X → [0, 1]$ is the transition probability function [2]. $G$ is said to be non-stochastic if $α : X × Σ × X → \{0, 1\}$, and a non-stochastic DES is said to be deterministic if $∀x ∈ X, σ ∈ Σ, \sum_{x′ ∈ X} α(x, σ, x′) ≤ 1$. The transition probability function $α$ can be extended from domain $X$ to $X × Σ × X$ in a natural way. Define the language generated by $G$ as $L(G) := \{s ∈ Σ^* : \exists x ∈ X, α(x₀, s, x) > 0\}$. The observations of events are filtered through an observation mask, $M : Σ → \overline{Σ}$, satisfying $M(ε) = ε$, where $Δ$ is the set of observable symbols. An event $σ$ is said to be unobservable if $M(σ) = ε$; the set of unobservable events is denoted by $Σ^uo$ and the set of observable events is then denoted by $Σ − Σ^uo$. The observation mask can be extended from domain $Σ$ to $Σ^*$ in a natural way.

For a stochastic DES $G = (X, Σ, α, x₀)$, its nonfaulty behaviors are specified in the form of a deterministic automaton $R = (Q, Σ, β, q₀)$ such that $L(R) = K$ is the set of nonfaulty traces. Then the remaining traces $L − K$ are called the faulty behaviors. The refinement of $G$ with respect to $R$, Fig. 1. A counter example, where $M(f) = M(e) = ε$, $M(α) = α$ and $M(b) = b$. 

The research was supported in part by the National Science Foundation under the grants, NSF-ECCS-0801763, NSF-ECCS-0926029, and NSF-CCF-1331390.

Jun Chen and Ratnesh Kumar are with the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011 USA (e-mail: {junchen,zkumar}@iastate.edu). Christoforos Keroglou and Christoforos Hadjicostis are with the Department of Electrical and Computer Engineering, University of Cyprus, Nicosia, Cyprus (email: {keroglou,christoforos,ladjic}@ucy.ac.cy)
denoted as $G^R$, can be used to capture the traces violating the given specification in the form of the reachability of a faulty state and is given by $G^R := (X \times \bar{Q}, \Sigma, \gamma, (x_0, q_0))$, where $\bar{Q} = Q \cup \{F\}$, and $\forall(x, \bar{q}, (x', \bar{q}')) \in X \times \bar{Q}, \sigma \in \Sigma, \gamma((x, \bar{q}, \sigma, (x', \bar{q}'))) = \alpha(x, \sigma, x')$ if the following holds: $(\bar{q}, \bar{q}' \in Q \land \beta(\bar{q}, \sigma, \bar{q}') > 0) \lor (\bar{q} = \bar{q}' = F) \lor (\bar{q}' = F \land \Sigma_{q' \in Q} \beta(\bar{q}, \sigma, q') = 0)$, and otherwise $\gamma((x, \bar{q}, \sigma, (x', \bar{q}'))) = 0$.

**Definition 1:** A state $(x, \bar{q}_1, (x', \bar{q}'_1))$ of $T$ is ambiguous if $\bar{q}_1 = F$. An SCC of $T$ is ambiguous if it contains an ambiguous state. A trace $s \in L$ is ambiguous if there exists $s' \in L$ such that either $(s, s')$ or $(s', s)$ transitions $T$ to an ambiguous state; it is recurrent if there exists a recurrent state $(x, \bar{q})$ in $G^R$ such that $\gamma((x_0, q_0), s, (x, \bar{q})) > 0$; it is persistently ambiguous if it is recurrent, ambiguous, and all its extensions in $L$ are ambiguous.

**Lemma 1:** $(G, R)$ is not SS-Diagnosable if and only if there exists a persistently ambiguous faulty trace.

**Proof:** We first show that there exists a persistently ambiguous faulty trace if and only if there exists a faulty trace whose extensions are all ambiguous. The necessity is obvious. To show the sufficiency, we argue that since $G^R$ has a finite state space, every faulty trace $s$ has an extension that is recurrent and faulty. Moreover, when all of the extensions of $s$ are ambiguous, then its extension that is recurrent is persistently ambiguous by Definition 2.

Next we show that $(G, R)$ is not SS-Diagnosable if and only if there exists a faulty trace whose extensions are all ambiguous. To show the sufficiency, suppose there exists a faulty trace $s_f \in L - K$ such that for any $t \in L \setminus s_f$, $s_f$ is ambiguous. Then $Pr(t : t \in L \setminus s_f, |t| \geq n, Pr_{amb}(s_f t) > 0) = 0$. So given any $0 < \tau < 1$, $\exists s \in L - K, \forall n \in \mathbb{N}$, $Pr(t : t \in L \setminus s, |t| \geq n, Pr_{amb}(s t) > 0) > \tau$. Therefore, $(G, R)$ is not SS-Diagnosable. On the other hand, if there does not exist a faulty trace whose extensions are all ambiguous, i.e., all faulty traces have at least one extension that is not ambiguous, then for any $s_f \in L - K$, there exists $t_1 \in L \setminus s_f$ such that $Pr_{amb}(s_f t_1) = 0$. Denote $n_1 := |t_1|$ and $p_1 = 1 - Pr(t_1) < 1$. For other extensions $t \in L \setminus s_f \cap T^{n_1}$ such that $s_f t$ is ambiguous, $s_f t$ has at least one extension that is not ambiguous and so there exists an extension $t_2 \in L/s_f t$ such that $Pr_{amb}(s_f t_2) = 0$. Let $n_2 := |t_2|$ and $p_2 = 1 - Pr(t_2) < 1$. In general, any ambiguous extensions of $s_f$ would have at least one unambiguous extension. Let $n_k$ be the length of the $k$th shortest unambiguous extension of $s_f$, and so

$$Pr(t : t \in L \setminus s_f, |t| \geq n_k, Pr_{amb}(s_f t) > 0)$$

$$\leq \prod_{i=1}^{k} Pr(t_i : t_i \in L \setminus s_f t_{i-1}, |t_i| = n_i - n_i-1$$

$$Pr_{amb}(s_f t_1 \ldots t_{i-1}) > 0) \times Pr(t \in L \setminus s_f t_{1} \ldots t_k, Pr_{amb}(s_f t_1 \ldots t_k) > 0)$$

$$\leq \prod_{i=1}^{k} (1 - p_i) \times Pr(t \in L \setminus s_f t_1 \ldots t_k$$

$$Pr_{amb}(s_f t_1 \ldots t_k) > 0)$$

$$\leq \prod_{i=1}^{k} (1 - p_i).$$

Since $\forall i, 1 - p_i < 1$, the above quantity approaches (if not equals) 0 as $k$ increases, equivalently as $n_k$ increases. Therefore, for any $\tau > 0$, there should exist $n_k > 0$, such that

$$Pr(t : t \in L \setminus s_f, |t| \geq n_k, Pr_{amb}(s_f t) > 0) < \tau.$$ 

Hence, $(G, R)$ is SS-Diagnosable when every faulty trace has at least one extension that is not ambiguous.

Therefore the proof for Lemma 1 is complete.

Next we introduce various notions related to the SCCs in the testing automaton $T$. 

**A. Conditions for SS-Diagnosability**

We first review the testing automaton $T$ constructed in [1, Algorithm 1]. For a given stochastic automaton $G = (X, \Sigma, \alpha, x_0)$ and a deterministic nonfault specification $R = (Q, \Sigma, \beta, q_0)$, $T$ is constructed as $T = G^R \times G^R$ such that in each step, the first copy of $G^R$ takes lead by executing a sequence of unobservable events followed by a single observable event, whereas the second copy responds by executing indistinguishable nonfaulty traces. This automaton is denoted as $T = (Z, \Sigma \times Z, \delta, z_0)$, where

- $Z = (X \times \bar{Q}) \times (X \times \bar{Q})$;
- $z_0 = ((x_0, q_0), (x_0, q_0))$ is the initial state;
- $\delta : Z \times \Sigma \times Z \to [0, 1]$ is defined as: $\forall ((x_1, \bar{q}_1), (x_2, \bar{q}_2)), ((x_1', \bar{q}_1'), (x_2', \bar{q}_2')) \in Z$ and $(\sigma_1, \sigma_2) \in \Sigma \times \Sigma$,

$$\delta((x_1, \bar{q}_1), (x_2, \bar{q}_2)), (\sigma_1, \sigma_2), ((x_1', \bar{q}_1'), (x_2', \bar{q}_2'))) = \alpha(L_{G^n}((x_1, \bar{q}_1), (x_1', \bar{q}_1')) \times \alpha(L_{G^n}((x_2, \bar{q}_2), (x_2', \bar{q}_2'))$$

if the following holds:

$$(\sigma_1 \in \Sigma - \Sigma_{amb}) \land (M(\sigma_1) = M(\sigma_2)) \land (\bar{q_2} \neq F) \land (L_{G^n}((x_2, \bar{q}_2), (x_2', \bar{q}_2'))) \neq 0$$

and 0 otherwise.

The following definition is based on the testing automaton $T$ constructed in [1, Algorithm 1].

**Definition 2:** A state $((x_1, \bar{q}_1), (x_2, \bar{q}_2))$ of $T$ is ambiguous if $\bar{q}_1 = F$. An SCC of $T$ is ambiguous if it contains an ambiguous state. A trace $s \in L$ is ambiguous if there exists $s' \in L$ such that either $(s, s')$ or $(s', s)$ transitions $T$ to an ambiguous state; it is recurrent if there exists a recurrent state $((x_1, \bar{q}), (x_2, \bar{q}))$ in $G^R$ such that $\gamma((x_0, q_0), s, (x_1, \bar{q})) > 0$; it is persistently ambiguous if it is recurrent, ambiguous, and all its extensions in $L$ are ambiguous.
Definition 3: For an SCC \( C_T \) of \( T \), a set of states \( I^1_T \subseteq (X \times \mathcal{Q})^2 \) is an initial set of states with respect to the 1st copy of \( C_T \) if it can be reached by a single 1st copy trace, i.e., there exists \( s_1 \in L \), such that \( \forall ((x_1,q_1),(x_2,q_2)) \in I^1_T, \exists s_2 \in L, \delta(((x_0,q_0),(x_0,q_0)),(s_1,s_2),((x_1,q_1),(x_2,q_2))) > 0 \).

The 1st copy generated language from \( I^1_T \) is denoted as \( L^1(T,I^1_T) := \{ s_2 \in \Sigma^* : \exists (x_1,q_1),(x_2,q_2) \in I^1_T, (x_1,q_1), (x_2,q_2) \in (X \times \mathcal{Q})^2, s_2 \in \Sigma^* \text{ s.t. } \delta(((x_1,q_1),(x_2,q_2)),(s_1,s_2),((x_1,q_1),(x_2,q_2))) > 0 \}. \)

An initial set of states \( I^2_T \) with respect to the 2nd copy of \( C_T \), and the corresponding 2nd copy generated language \( L^2(T,I^2_T) \) are dually defined.

Definition 4: For an SCC \( C_T \) of \( T \) containing a state \(((x_1,q_1),(x_2,q_2))\), its 1st copy projection in the plant model \( G^R \) is defined as \( C^1_G := (X^1_G,\gamma^1_C) \), where the state space is given by \( X^1_G := \{ (x,\eta) \in X \times \mathcal{Q} : \exists s \in \Sigma^*, \eta \in \Sigma - \Sigma_{u_0}, \gamma((x_1,q_1),s,(x,\eta)) > 0 \} \), and for any \(((x_1,q_1),(x_2,q_2)) \in X^1_G \), \( \eta \in \Sigma - \Sigma_{u_0}, \gamma^1_C((x_1,q_1),\eta,(x_2,q_2)) = \alpha((L_G))^C\alpha((x_1,q_i),\eta,(x_2,q_2))) \).

A set of states \( I^1_G \subseteq X^1_G \) is an initial set of states of \( C^1_G \) if there exists \( I^1_T \) of \( C_T \), such that \( I^1_G = \{ (x_1,q_1) \in X^1_G : \exists (x_2,q_2) \in X \times \mathcal{Q}, ((x_1,q_1),(x_2,q_2)) \in I^1_T \}. \)

The generated language of \( C^1_G \) from \( I^1_G \) is denoted as \( L(G^R,I^1_G) := \{ s \in \Sigma^*: \exists (x_1,q_1) \in I^1_G, (s,(x_1,q_1)) > 0 \} \).

Example 2: See the system in Fig. 2. The testing automaton in Fig. 2(d) has one SCC \( C_T \) consisting of states \(((4,F),(1,1))\), \(((4,F),(2,1))\) and the transitions among them (see Fig. 2(e) (left)). There is only one initial set of states with respect to the 1st copy, namely \( I^1_T = \{((4,F),(1,1)),((4,F),(2,1))\} \), and \( L(T,I^1_T) = \{b,c\}^* \).

Dually we have, \( I^2_T = \{((4,F),(1,1)),((4,F),(2,1))\} \), and \( L(T,I^2_T) = \{b,c\}^* \). The 1st copy projection of \( C_T \) is given by Fig. 2(e) (middle) with \( I^1_C = \{((4,F))\} \) and \( L(G^R,I^1_C) = \{b,c\}^* \), the 2nd copy projection of \( C_T \) is given by Fig. 2(e) (right) with \( I^2_C = \{(1,1),(2,1))\} \), \( L(G^R,I^2_C) = \{b,c\}^* \).

Next in order to provide necessary and sufficient condition, sufficient condition, and necessary condition, respectively, for non-SS-Dignosability, we introduced the notions of \( G^R \)-closed, weakly \( G^R \)-closed, and weakly \( G^R \)-closed, respectively, for the SCCs of \( T \).

Definition 5: Given an SCC \( C_T \) of \( T \) containing a state \(((x_1,q_1),(x_2,q_2))\) such that \((x_1,q_1)\) is a recurrent state in \( G^R \),

1) it is said to be \( G^R \)-closed if there exists an initial set of states \( I^1_T \) such that \( L(T,I^1_T) = L(G^R,I^1_C) \);

2) it is said to be weakly \( G^R \)-closed if for any state \(((x_1,q_1))\) of its 1st copy projection \( C^1_C \), \( \sigma_1 \in \Sigma - \Sigma_{u_0}, \) and \(((x_1,q_1),(x_2,q_2)) \in X \times \mathcal{Q} \) such that \( \gamma^1_C((x_1,q_1),\sigma_1,(x_2,q_2)) > 0 \), there exist \( \sigma_2 \in \Sigma \) such that \( \delta(((x_1,q_1),(x_2,q_2)),(\sigma_1,\sigma_2),(x_1,q_1),(x_2,q_2))) > 0 \) and \( ((x_1,q_1),(x_2,q_2)) \) are states of \( C_T \);

3) it is said to be strongly \( G^R \)-closed if for any state \(((x_1,q_1),(x_2,q_2))\) of \( C_T \), it holds that for all \( \sigma_1 \in \Sigma - \Sigma_{u_0}, \) and \(((x_1,q_1),(x_2,q_2)) \in X \times \mathcal{Q} \), such that \( \gamma^1_C((x_1,q_1),\sigma_1,(x_2,q_2)) > 0 \), there exist \( \sigma_2 \in \Sigma \) such that \( \delta(((x_1,q_1),(x_2,q_2)),(\sigma_1,\sigma_2),(x_1,q_1),(x_2,q_2))) > 0 \) and \( ((x_1,q_1),(x_2,q_2)) \) are states of \( C_T \).

Example 3: Consider again the SCC \( C_T \) in Fig. 2(e) (left). Since \( L(T,I^1_T) = \{b,c\}^* = L(G^R,I^1_C) \), it is \( G^R \)-closed, and is also weakly \( G^R \)-closed. However, for state \(((4,F),(1,1))\) of \( C_T \), it holds that \( \gamma^1_C((4,F),c,(4,F)) > 0 \) while for any \(((x_1,q_1),(x_2,q_2))\) and \( \sigma \), \( \delta(((4,F),(1,1)),(c,\sigma),(x_1,q_1),(x_2,q_2)) = 0 \) and \( ((x_1,q_1),(x_2,q_2)) \) is a state of \( C_T \).

Therefore \( C_T \) is not strongly \( G^R \)-closed.

Theorem 1: Given a pair of \((G,R)\):

1) it is not SS-Diagnosable if and only if there exists an ambiguous \( G^R \)-closed SCC in \( T \);

2) if it is not SS-Diagnosable, then there exists an ambiguous weakly \( G^R \)-closed SCC in \( T \);

3) it is not SS-Diagnosable if there exists an ambiguous strongly \( G^R \)-closed SCC in \( T \).

Proof: When there exists an ambiguous \( G^R \)-closed SCC \( C_T \), let \( s \in L - K \) be the faulty trace that reaches the initial set of states \( I^1_C \). Since \( L(T,I^1_T) = L(G^R,I^1_C) \), for
any $t \in L \setminus s$, there exists $s'^t \in K$ such that $(s_t, s'^t)$ reaches an ambiguous state of $C_T$. Therefore, all extensions of $s$ are ambiguous. Moreover, $s$ is recurrent, and so $s$ is persistently ambiguous. According to Lemma 1, $(G, R)$ is not SS-Diagnosable. The sufficiency of (1) follows. To show the necessity of (1), suppose every ambiguous SCC of $T$ is not $G^R$-closed. Then for any recurrent faulty trace $s \in L - K$, there exists $t \in L \setminus s$ such that $s_t$ is not ambiguous, i.e., there is no persistently ambiguous faulty trace. According to Lemma 1, $(G, R)$ is SS-Diagnosable.

By the definitions of $G^R$-closed and weakly $G^R$-closed SCC, if an SCC is $G^R$-closed, then it is weakly $G^R$-closed. When $(G, R)$ is not SS-Diagnosable, there exists an ambiguous $G^R$-closed SCC, according to (1), and hence there exists an ambiguous weakly $G^R$-closed SCC. Thus (2) is proven.

By the definitions of $G^R$-closed and strongly $G^R$-closed SCC, if an SCC is strongly $G^R$-closed, then it is $G^R$-closed. When there exists an strongly ambiguous $G^R$-closed SCC in $T$, there exists an ambiguous $G^R$-closed SCC, and hence $(G, R)$ is not SS-Diagnosable, according to (1). Thus (3) is proven.

**Algorithm 1:** To check the necessary and sufficient condition for SS-Diagnosability in condition (1) in Theorem 1, do the following:

- Identify the set of SCCs in $T$ which contains an ambiguous state $\{(x_1, F), (x_2, \overline{x}_1)\}$ such that $x_1, F$ is a recurrent faulty state in $G^R$.
- For each SCC $C_T$ identified above,
  - Identify the corresponding closed SCC $C^1_G$ in $G^R$, such that $C^2_G$ contains $(x_1, F)$, and obtain $C^1_G$ by collapsing the unobservable events in $C^1_G$. Note that $\gamma^1_G(x_2, F) = 0$ for all $x_2, F$.
  - Identify the sets of initial states $I^2_T$ such that each $I^1_T \subseteq I^2_T$ is an initial set of states with respect to the 1st copy of $C_T$.
  - For each set of initial states $I^1_T \in I^2_T$, obtain the initial states $I^1_G$, of $C^1_G$, by projecting out the second coordinate of states of $I^1_T$.
- Check whether there exists $C_T$ with initial set of states $I^1_T$ such that $L(T, I^1_T) = L(G^R, I^1_G)$. If yes, then the system is not SS-Diagnosable; else the system is SS-Diagnosable.

Note the above algorithm requires identifying initial states and checking language equivalence, both of which require determination, and hence has exponential complexity, $O(2^n |\Sigma|^2 \times |Q|^2 \times |\Sigma|)$.

**Remark 1:** The condition for necessity and sufficiency of SS-Diagnosability above is included merely for completion, fitting our same framework that also provides, separately, a polynomial complexity necessary condition and a polynomial complexity sufficient condition. Otherwise, a necessary and sufficient condition for SS-Diagnosability has already been presented in literature [3]; this test as well as ours are both of exponential complexity.

**Remark 2:** Condition (2) in Theorem 1 is a necessary condition for testing non-SS-Diagnosability (i.e., its negation provides a sufficient condition for testing SS-Diagnosability) that can be checked in polynomial time. To check this condition, we first identify all the SCCs in $T$ that are ambiguous. For each such SCC $C_T$ and its 1st copy projection $C^1_G$, check whether there exists a transition $\gamma^1_G((x_1, \overline{x}_1), a, (x'_1, \overline{x}'_1)) > 0$ in $C^1_G$ such that, $\delta(((x_1, \overline{x}_1), (x_2, \overline{x}_2), (x_1, \overline{x}_1), (x'_1, \overline{x}'_1), (x'_2, \overline{x}'_2))) = 0$ for all $(x_2, \overline{x}_2), (x'_2, \overline{x}'_2)$. $C_T$ is weakly $G^R$-closed if and only if such transition doesn’t exist. The complexity for testing condition (2) in Theorem 1 is $O(|\Sigma|^6 \times |Q|^3 \times |\Sigma|^2)$.

**Condition (3) in Theorem 1:** is a sufficient condition for testing non-SS-Diagnosability (i.e., its negation provides a necessary condition for testing SS-Diagnosability). To check this condition, we first identify all the SCCs in $T$ that are ambiguous. For each such SCC, iteratively remove all its states violating the definition of strongly $G^R$-closed SCC, until a strongly $G^R$-closed SCC is found or $C_T$ contains no states. Note the iteration terminates in polynomial time, namely, $O(|\Sigma|^6 \times |Q|^3 \times |\Sigma|^2)$.

**Example 4:** To show that condition (2) in Theorem 1 is only a necessary condition for non-SS-Diagnosability, consider the example in Fig. 3. It can be checked that there exists a weakly $G^R$-closed SCC in $T$, specifically the SCC consisting of states $\{(4, F), (1, 1)\}$ and $\{(4, F), (2, 2)\}$ and the transitions among them. Yet $(G, R)$ is SS-Diagnosable as can be checked by using condition (1) in Theorem 1. Hence (2) in Theorem 1 is only necessary for testing non-SS-Diagnosability.

![Fig. 3. A counter example, where $M(f) = \epsilon$, $M(a) = a$, $M(b) = b$, $M(c) = c$ and $M(d) = d$.](Image 341x120 to 534x426)
See Fig. 2, where \((G, R)\) is not SS-Diagnosable, since \(T\) has a \(G^R\)-closed ambiguous SCC as discussed in Example 3. However it does not have any strongly \(G^R\)-closed ambiguous SCC. Therefore, \((3)\) in Theorem 1 is only a sufficient condition for non-SS-Diagnosability.

B. Verification of SS-Diagnosability is PSPACE-hard

Having established a necessary and sufficient test for SS-Diagnosability with exponential complexity, we next show that most likely the verification of SS-Diagnosability cannot have a polynomial complexity algorithm by showing that indeed it is PSPACE-hard, by providing a polynomial-time reduction of the Universality problem to an instance of the SS-Diagnosability problem. Since the former is PSPACE-hard, this proves that the SS-Diagnosability problem is PSPACE-hard.

Given a nondeterministic finite automaton \(G_N\) over the alphabet \(\Sigma\), the Universality problem asks if the language \(L(G_N)\) contains all finite words over \(\Sigma\), i.e., if \(L(G_N) = \Sigma^*\). Next we give the formal definition of the Universality problem, reproduced from [4].

**Definition 6**: Given a nondeterministic finite automaton \(G_N = (X_N, \Sigma_o, \delta_N, X_N^0)\) such that the set of initial states \(X_N^0 = X_N\), do we have \(L(G_N) = \Sigma_o^*\)?

When \(|\Sigma| \geq 2\), the Universality problem with all states initial is known to be PSPACE-hard [4]. We now establish a polynomial reduction from the Universality problem with all states initial to an instance of the SS-Diagnosability problem. For any \(G_N = (X_N, \Sigma_o, \delta_N, X_N^0)\), let \(G = (X, \Sigma, \alpha, x_0)\) be such that \(X = \{x_0\} \cup X_N \cup \{x_f\}\) where \(x_0\) and \(x_f\) are new states (not in \(X_N\)) and \(\Sigma = \Sigma_o \cup \{\sigma_o, \sigma_f\}\) where \(\sigma_o, \sigma_f\) are new events (not in \(\Sigma_o\)) that are unobservable and \(\Sigma_o\) (events of \(G_N\)) is the set of observable events with \(|\Sigma_o| \geq 2\) and \(M(\sigma) = \sigma, \forall \sigma \in \Sigma_o\). We assign probabilities as follows:

1. \(\alpha(x_0, \sigma_f, x_f) = \frac{1}{|X_N| + 1}\), and \(\forall \sigma \in \Sigma_o, \alpha(x_f, \sigma, x_f) = \frac{1}{|\Sigma_o|}\);
2. \(\forall x \in X_N, \alpha(x_0, \sigma_o, x) = \frac{1}{|X_N| + 1};\)
3. \(\forall x, x' \in X_N \text{ and } \forall \sigma \in \Sigma_o, \text{ if } x' \in \delta_N(x, \sigma), \alpha(x, \sigma, x') = \frac{1}{\sum_{\sigma \in \Sigma_o} |\delta_N(x, \sigma)|};\)
4. \(\alpha(x, \sigma, x') = 0\) for all other cases.

**Remark 3**: Note that (if we ignore probabilities): i) \(G\) can be seen as the union of \(G_N = (X_N, \Sigma_o, \delta_N, X_N)\) and the singleton state automaton \(G_F = (\{x_f\}, \Sigma, \delta_f, x_f)\), whose language \(L(G_F) = \Sigma_o^*;\) ii) there exists a transition (with unobservable event) from \(x_0\) to each state in \(X_N\) and a transition (also with unobservable event) to \(x_f\).

To construct a diagnosability problem, we let \(R\) be such that \(K = L(R) = \sigma_o L(G_N) \subseteq \sigma_o \Sigma_o\). Then \(L - K = \sigma_f \Sigma_o^*\). Moreover, \(X_N\) can be seen as the set of states of \(G\) that are consistent with the nonfaulty behaviour of \(G\) and \(x_f\) can be seen as the singleton state that is consistent with faulty behaviour of \(G\), i.e., all nonfaulty traces in \(K\) will transition \(G\) to states in \(G_N\) while all faulty traces in \(L - K\) will transition \(G\) to the singleton state \(x_f\).

The following theorem shows that every instance of the language universality problem of \(G_N = (X_N, \Sigma_o, \delta_N, X_N)\) with all states initial, can be reduced to an instance of SS-Diagnosability problem (as it was described in previous paragraph). Thus, the SS-Diagnosability problem is PSPACE-hard.

**Theorem 2**: Verification of SS-Diagnosability is PSPACE-hard.

**Proof**: We argue that \(L(G_N) = \Sigma_o^*\) if and only if \(G\) (as in Fig. 4 and as described above) is not SS-Diagnosable.

\(<\) If \(L(G_N) = \Sigma_o^*\), then for all \(s \in L - K = \sigma_f \Sigma_o^*\), there exists \(s' \in \sigma_o \Sigma_o^*\) such that \(M(s) = M(s')\). Therefore all extensions of the faulty trace \(\sigma_f\) are ambiguous. Moreover, \(\sigma_f\) is recurrent, and so \(\sigma_f \in L - K\) is persistently ambiguous. According to Lemma 1, \(G\) is not SS-Diagnosable.

\(\rightarrow\) If \(L(G_N) \neq \Sigma_o^*\), i.e., \((G_N) \subset \Sigma_o\), then there exists \(s \in \Sigma_o^*\) such that \(s \notin L(G_N)\). Notice that \(\forall u \in \Sigma_o^*\), \(us \notin L(G_N)\) since \(\delta_N(X_N, us) = \delta_N(\delta_N(X_N, u), s) \subseteq \delta_N(X_N, s) = \emptyset\). Since for any faulty trace \(s_f \in L - K = \sigma_f \Sigma_o^*\), there exists an extension \(us\) such that \(us \in L \setminus s_f\) and \(s_f us\) is unambiguous. Thus every faulty trace has at least one unambiguous extension, i.e., there is no persistently ambiguous faulty trace. According to Lemma 1, \(G\) is SS-Diagnosable.

This establishes the reduction with complexity of \(O(|X_N|^2 \times |\Sigma_o|)\) and concludes that the verification of SS-Diagnosability is PSPACE-hard.

\(\blacksquare\)

III. CONDITIONS FOR S-DIAGNOSABILITY

Having studied SS-Diagnosability, we next study the S-Diagnosability property, which, as established in [5], is key to the existence of an online detector that can achieve desired levels of false-negatives/positives. We need a few definitions. Let us denote the set of traces that are persistently ambiguous as \(L_{PA}\). Given a recurrent trace \(s \in L\), let us denote \(C(s) \subseteq M^{-1}[M(s)]\) as the set of indistinguishable traces that reach the same closed SCC in \(G^R\) as \(s\).

**Definition 7**: A pair of persistently ambiguous traces \((s_f, s_n) \in (L - K) \times K\) is said to be a persistently ambiguous pair if

1. both \(s_f\) and \(s_n\) are persistently ambiguous, and
2. \(\forall t_n \in K \setminus s_n, \exists f \neq L_{PA} \cap C(s_f)\) s.t. \(M(t_f) = M(t_n)\).

Theorem 3: Given a pair of persistently ambiguous traces \((s_f, s_n) \in (L - K) \times K\), then \(s_f \cap s_n\) contains an indistinguishable trace \(s_m\) that is unambiguously observed.

**Proof**: Let \(s_m = s_f \cap s_n\) be an indistinguishable trace. Since \(s_f\) is persistently ambiguous, \(s_m\) is persistently ambiguous. \(s_m\) is unambiguous because it is a subpath of both \(s_f\) and \(s_n\) and has the same probability as \(s_m\).

\(\blacksquare\)
Definition 8: Two closed SCCs in $G^R$ are said to be $p$-equivalent with respect to a given pair of distributions, if the generated probabilities for each $o \in \Delta^*$ by the two SCCs starting from those distributions are the same.

Remark 4: As provided by [6], given two SCCs with $n_1$ and $n_2$ states and stationary distributions $\pi_1$ and $\pi_2$, respectively, one can construct a basis for the $(n_1 + n_2)$-dimensional vector space that includes $[\pi_1 \pi_2]$. Then the two SCCs are $p$-equivalent if and only if for every string corresponding to one of the basis, the generated probabilities by the two SCCs are the same. Note that the verification can be done in polynomial complexity, namely, $O(|X|^4 \times |Q|^4 \times |\Sigma|)$.

Lemma 2: $(G, R)$ is not S-Diagnosable if and only if there exists a persistently ambiguous pair $(s_f, s_n)$ that reach two closed SCCs in $G^R$ that are $p$-equivalent.

Proof: We first prove that when there is no persistently ambiguous pair $(s_f, s_n)$, $(G, R)$ is S-Diagnosable. Suppose for any $s_f \in L_{PA}$ and $s_n \in K \cap M^{-1}[M(s_f)]$ such that $s_n$ is recurrent, $(s_f, s_n)$ is not a persistently ambiguous pair. Let $s_f \in L_{PA}$ be any persistently ambiguous faulty trace, and $s_n \in K$ be arbitrary such that $M(s_f) = M(s_n)$. Since there is no persistently ambiguous pair, there exists $t_n^1 \in L\{s_n\}$ such that either $s_n t_n^1 \notin K$ or $\forall t_f' \in L\{L_{PA} \cap C(s_f)\}, M(t_f') \neq M(t_n^1)$. Denote $n_1 := |t_n^1|$ and $p_1 = 1 - Pr(t_n^1) < 1$. For other extensions $t_n \in K\{s_n \cap \Sigma^{n_1} \text{such that} \exists s_f' \in L_{PA} \cap C(s_f), t_f' \in L\{s_f'\}, M(s_f,t_f') = M(s_n,t_n)$, $s_f't_f'$ is persistently ambiguous and hence $(s_f',t_f')$ is not a persistently ambiguous pair. Therefore there exists $t_n^2 \in L\{s_n\}$ such that either $s_n t_n^2 \notin K$ or $\forall t_f' \in L\{L_{PA} \cap C(s_f)\}, M(t_f') \neq M(t_n^2)$. Let $n_2 := |t_n^2|$ and $p_2 = 1 - Pr(t_n^2)$. Let $n_k$ be the $k$th shortest extension $t_n$ of $s_n$ such that either $s_n t_n \notin K$ or $\forall t_f \in L\{L_{PA} \cap C(s_f)\}, M(t_f) \neq M(t_n)$. Then we have

$$Pr(t_n \in K\{s_n \} : |t_n| \geq n_k, \exists t_f \in L\{L_{PA} \cap C(s_f)\}, M(t_f) = M(t_n))$$

$$\leq \prod_{i=1}^{k}(1 - p_i).$$

Since $\forall i, 1 - p_i < 1$, the above quantity approaches (if not equals) 0 as $n_k$ increases. Therefore, for any $\rho, \tau > 0$, there should exist $n \in \mathbb{N}$, such that

$$Pr(t_n \in K\{s_n \} : |t_n| \geq n, \exists t_f \in L\{L_{PA} \cap C(s_f)\}, M(t_f) = M(t_n))$$

$$< \rho \tau.$$

Moreover

$$Pr(s_n t_n \in K : |t_n| \geq n, \exists t_f \in L\{L_{PA} \cap C(s_f)\}, M(t_f) = M(t_n))$$

$$\leq \sum_{s_n \in K : M(s_n) = M(s_f)} Pr(s_n) Pr(t_n \in K) \sum_{|t_n| \geq n, \exists t_f \in L\{L_{PA} \cap C(s_f)\}, M(t_f) = M(t_n))$$

$$< \sum_{s_n \in K : M(s_n) = M(s_f)} Pr(s_n) \rho \tau < \rho \tau.$$
1) it is said to be bi-$G^R$-closed if there exist $I_1^T$ and $I_2^T$ with $I_1^T \cap I_2^T \neq \emptyset$, such that $L(T, I_1^T) = L(G^o, I_{C^o})$ for $i \in \{1, 2\}$;

2) it is weakly bi-$G^R$-closed if it is weakly $G^R$-closed and for any state $(x_2, \overline{q}_2)$ of its 2nd projection $C_{o^2}$, $\sigma_2 \in \Sigma - \Sigma_{uo}$, and $(x_2, \overline{q}_2) \in X \times \overline{Q}$, such that $\gamma_{o^2}((x_2, \overline{q}_2), \sigma_2, (x_2, \overline{q}_2)) > 0$, there exist $\sigma_1 \in \Sigma$ such that $\delta(((x_1, \overline{q}_1), (x_2, \overline{q}_2)), (\sigma_1, \sigma_2), ((x_1, \overline{q}_1), (x_2, \overline{q}_2))) > 0$ and $((x_1, \overline{q}_1), (x_2, \overline{q}_2)), ((x_1, \overline{q}_1), (x_2, \overline{q}_2))$ are states of $C_T$;

3) it is strongly bi-$G^R$-closed if it is strongly $G^R$-closed and for any state of $(x_1, \overline{q}_1), (x_2, \overline{q}_2)$ in $C_T$, it holds that for all $\sigma_2 \in \Sigma - \Sigma_{uo}, (x_2, \overline{q}_2) \in X \times \overline{Q}$, such that $\gamma_{o^2}((x_2, \overline{q}_2), \sigma_2, (x_2, \overline{q}_2)) > 0$, there exist $\sigma_1 \in \Sigma, (x_1, \overline{q}_1) \in X \times \overline{Q}$ such that $\delta(((x_1, \overline{q}_1), (x_2, \overline{q}_2)), (\sigma_1, \sigma_2), ((x_1, \overline{q}_1), (x_2, \overline{q}_2))) > 0$ and $((x_1, \overline{q}_1), (x_2, \overline{q}_2))$ is a state of $C_T$.

**Definition 10:** For a SCC $C_T$ of $T$, and its projections $C_{o^1}$ and $C_{o^2}$, a pair of distributions $\pi_1$ over $C_{o^1}$ and $\pi_2$ over $C_{o^2}$ is said to be reachable, if there exist a state of $(x_1, \overline{q}_1), (x_2, \overline{q}_2)$ in $C_T$ and a trace pair $(s, t)$ such that $\delta(((x_0, \overline{q}_0), (x_0, \overline{q}_0)), (s, t), ((x_1, \overline{q}_1), (x_2, \overline{q}_2))) > 0$, and the distribution over $C_{o^1}$ given $M(s) = \pi_1$ and the distribution over $C_{o^2}$ given $M(t) = \pi_2$. A SCC $C_T$ of $T$ is p-equivalent if there exist reachable distribution $\pi_1$ over $C_{o^1}$ and $\pi_2$ over $C_{o^2}$, such that $C_{o^1}$ and $C_{o^2}$ are p-equivalent with respect to $\pi_1$ and $\pi_2$.

**Theorem 3:** Given a pair of $(G, R)$:

1) it is not S-Diagnosable if and only if there exists an ambiguous, bi-$G^R$-closed, p-equivalent SCC in $T$;

2) if it is not S-Diagnosable, then there exists an ambiguous, weakly bi-$G^R$-closed, p-equivalent SCC in $T$;

3) it is not S-Diagnosable if there exists an ambiguous, strongly bi-$G^R$-closed, p-equivalent SCC in $T$.

**Proof:** When there exists an ambiguous, bi-$G^R$-closed and p-equivalent SCC $C_T$, let $s_f \in L - K$ be the faulty trace that reaches the initial set (first copy) of states $I_2^T$ and $s_n \in K$ be the nonfaulty trace that reaches the initial set (second copy) of states $I_2^0$. Since $L(T, I_1^T) = L(G^o, I_{C^o})$, $s_f$ is persistently ambiguous. Since $L(T, I_2^T) = L(G^o, I_{C^o})$, then for any $t_o \in K \backslash s_n$, there exists $t_f \in L \backslash [L_{PA} \cap C(s_f)]$ such that $M(t_f) = M(t_o)$. Therefore $(s_f, s_n)$ is a persistently ambiguous pair. Moreover, since $C_{o^1}$ and $C_{o^2}$ are p-equivalent after the observation $M(s_f) = M(s_n)$, according to Lemma 2, $(G, R)$ is not S-Diagnosable. The sufficiency of (1) follows. To show the necessity of (1), suppose every ambiguous bi-$G^R$-closed SCC of $T$ is not p-equivalent. Then for any persistently ambiguous pair $(s_f, s_n) \in (L - K) \times K$, $s_f$ and $s_n$ reach two SCCs in $G^R$ that are not p-equivalent. According to Lemma 2, $(G, R)$ is S-Diagnosable.

By the definitions of bi-$G^R$-closed and strongly bi-$G^R$-closed SCC, if an SCC is bi-$G^R$-closed, then it is weakly bi-$G^R$-closed. When $(G, R)$ is not S-Diagnosable, then there exists an ambiguous, bi-$G^R$-closed, p-equivalent SCC, according to (1), and hence there exists an ambiguous, weakly bi-$G^R$-closed, p-equivalent SCC. Thus (2) is proven.

By the definitions of bi-$G^R$-closed and strongly bi-$G^R$-closed SCC, if an SCC is strongly bi-$G^R$-closed, then it is bi-$G^R$-closed. When there exists an ambiguous, strongly bi-$G^R$-closed, p-equivalent SCC in $T$, there exists an ambiguous, bi-$G^R$-closed, p-equivalent SCC, and hence, according to (1), $(G, R)$ is not S-Diagnosable. Thus (3) is proven.

**Algorithm 2:** To check the necessary and sufficient condition for S-Diagnosability in condition (1) in Theorem 3, do the following:

- Check the SS-Diagnosability of the system using Algorithm 1. If $(G, R)$ is SS-Diagnosable, then it is also S-Diagnosable, and stop; else proceed to next step.

- Identify the set of SCCs $C_T$ in $T$ that contain an ambiguous state $((x_1, F), (x_2, \overline{q}_2))$ such that both $(X_1, F)$ and $(x_2, \overline{q}_2)$ are recurrent states in $G^R$, and the sets of initial states of sets $\mathcal{I}_T$ such that for each $I_1^T \in \mathcal{I}_T^0$, $L(T, I_1^T) = L(G^o, I_{C^o})$.

- For each SCC $C_T$ with initial states $I_1^T \in \mathcal{I}_T^0$ identified above,
  - Identify the corresponding closed SCC $C_{o^2}$ in $G^R$ such that $C_{o^2}$ contains $(x_2, \overline{q}_2)$, and obtain $C_{o^2}$ by collapsing the unobservable events in $C_{o^2}$.
  - Identify the sets of initial states set $\mathcal{I}_T^2$ such that each set $I_2^T \in \mathcal{I}_T^2$ is an initial set of states with respect to the 2nd copy of $C_T$ and $I_1^T \cap I_2^T \neq \emptyset$.
  - For each set of initial states $I_2^T \in \mathcal{I}_T^2$, obtain the initial states $I_{C^o}^T$ of $C_{o^2}$ by projecting out the first coordinate of states of $I_2^T$.

- Check whether there exists $C_T$ identified above with initial set of states $I_1^T$ such that $L(T, I_1^T) = L(G^o, I_{C^o})$.

If no, the system is S-Diagnosable, otherwise identify the set of SCCs $C_T$ and $I_{C^o}^T, I_{C^o}^R$ that violate above condition.

- For each pair of $I_{C^o}^T$ and $I_{C^o}^R$ identified above, find all the reachable distributions $\pi_1$ over $C_{o^1}$ and $\pi_2$ over $C_{o^2}$.

- Check whether there exist $C_T$, $C_{o^1}$, $C_{o^2}$ and $\pi_1, \pi_2$ identified above, such that $C_{o^1}$ and $C_{o^2}$ are p-equivalent with respect to $\pi_1$ and $\pi_2$. If yes, then the system is not S-Diagnosable; else the system is S-Diagnosable.

Note that the last step of Algorithm 2 requires evaluating over all reachable initial distributions $\pi_{o^1}^T$ over $I_1^T$ and $\pi_{o^2}^T$ over $I_2^T$. Performing such evaluation in a decidable manner is an open problem at this point.

**Example 5:** For system in Fig. 2, according to Example 2, $I_1^T \cap I_2^T \neq \emptyset$ and $L(T, I_1^T) = L(G^o, I_{C^o}) = \{b, c\}^*$ for $i \in \{1, 2\}$. Therefore $C_T$ is bi-$G^R$-closed. Furthermore, the only reachable initial distribution over $I_{C^o}^T$ is [1] and the only reachable initial distribution over $I_{C^o}^R$ is [0.5, 0.5], from which $C_{o^1}$ and $C_{o^2}$ are p-equivalent, and so non-S-Diagnosability can be concluded for the system in Fig. 2.

**IV. Conclusion**

In this paper, we corrected the error of [1] by presenting revised necessary and sufficient conditions for SS/S-S-Diagnosability, the first of which has exponential complexity while the termination of the second remains an open problem. We also provide polynomial tests for sufficiency, and polynomial tests for necessity, for SS-Diagnosability. We further
show that the verification of SS-Diagnosability is actually PSPACE-hard.

REFERENCES


