Symbolic Fault Diagnosis of Discrete-Event Systems Based on State-Tree Structures

Deguang Wang, Xi Wang, *Member, IEEE*, Jing Yang, Qiwei Tang, and Zhiwu Li, *Fellow, IEEE*

APPENDIX

We need the following definitions and lemmas for the proofs later.

Definition 1. [*Observation-Adjacency*] *For any two basic state-trees $b, b' \in \mathcal{B}(\mathbf{ST})$, b' is said to be observation-adjacent to b (write as $b \overset{\sigma}{\rightarrowtail} b'$) if there exists a string $s\sigma t$ in which $s, t \in \Sigma_{uo}^*$ and $\sigma \in \Sigma_o$ such that $b' = \Delta(b, s\sigma t)$.* $\Diamond$

Assume in the diagnoser $\mathbf{G}_d = (\mathcal{A}_d, \Sigma_o, \Delta_d, A_{d0}, \hat{\kappa})$ $cl = (A_1, -1) \xrightarrow{\sigma_1} \cdots \xrightarrow{\sigma_{n-2}} (A_{n-1}, -1) \xrightarrow{\sigma_{n-1}} (A_n, -1) \xrightarrow{\sigma_n} (A_1, -1)$ with $n \geq 1$ is an F-indeterminate cycle. A cycle $cl' = b_1 \overset{\sigma_1}{\rightarrowtail} \cdots \overset{\sigma_{n-2}}{\rightarrowtail} b_{n-1} \overset{\sigma_{n-1}}{\rightarrowtail} b_n \overset{\sigma_n}{\rightarrowtail} b_1$ is called an *underlying faulty cycle* of cl if $b_i \in A_i$ and $b_i \in B_F$. Intuitively, if there is an F-indeterminate cycle, then the system has a cycle in the faulty mode F such that when it evolves on the cycle, it will generate the event sequence periodically. The cycle in the mode F and the corresponding event sequence keeps the diagnoser in the F-uncertain cycle indefinitely, and in this case, the system is not diagnosable.

Lemma 1. *Let $p = (A_1, -1) \xrightarrow{\sigma_1} \cdots \xrightarrow{\sigma_{n-2}} (A_{n-1}, -1) \xrightarrow{\sigma_{n-1}} (A_n, -1)$ $(n \geq 2)$ be a path in the diagnoser $\mathbf{G}_d$. For any $b_n \in A_n$, there exist $b_i \in A_i$ $(1 \leq i \leq n-1)$ such that $b_i \overset{\sigma_i}{\rightarrowtail} b_{i+1}$.*

A. Proof of Theorem 2 in Section III

Proof: (only if): Suppose that $\mathbf{G}$ is diagnosable, but there exists an F-indeterminate cycle cl in the diagnoser $\mathbf{G}_d = (\mathcal{A}_d, \Sigma_o, \Delta_d, A_{d0}, \hat{\kappa})$. Since $\mathbf{G}_d$ is reachable, there exists an event sequence that can take the diagnoser into a BSTA A_k belonging to cl. Let $b_n \in A_n$ belong to an underlying faulty cycle of cl. By Lemma 1, there exist basic state-trees $b_1, \cdots, b_{n-1}$ such that $b_i \overset{\sigma_i}{\rightarrowtail} b_{i+1}$ $(1 \leq i \leq n-1)$. After reaching b_n, the system may remain on the underlying faulty cycle causing the diagnoser to stay on the F-indeterminate cycle indefinitely. Therefore, there exists a trajectory for the system leading to basic state-trees in B_F such that the corresponding event sequence throws the diagnoser into a cycle of F-uncertain BSTA and keeps it there indefinitely. Hence, the system is not diagnosable, which leads to a contradiction. So the necessity holds.

(if): Assume that no F-indeterminate cycle exists in the diagnoser $\mathbf{G}_d$. After the occurrence of F and the generation of a new observable event, the diagnoser reaches either F-certain or F-uncertain BSTA. If it is an F-certain BSTA, then it will remain F-certain (because fault is permanent) and the system is diagnosable. If it is an F-uncertain BSTA, then the number of F-uncertain BSTA is bounded. After the generation of a bounded number of observable events, the diagnoser will reach an F-certain BSTA (the diagnoser gets trapped indefinitely in a cycle of F-uncertain states only if the cycle is F-indeterminate).

Let n denote the number of events that it takes the diagnoser to detect and isolate. After the occurrence of F, the diagnoser can visit an F-uncertain BSTA $(A, -1)$ at most $|A \cap B_F|$ times. Then we have $n \leq c \times m + m$, where $c = \sum_{(A,-1) \in \mathcal{A}_d} |A \cap B_F|$ and m is the length of the longest path of faulty basic state-trees. Since $m \leq |B_F|$ and $c \leq |B_F| \cdot |\mathcal{A}_d|$, $n \leq c \times m + m \leq |B_F| \cdot |\mathcal{A}_d| \cdot |B_F| + |B_F| = |B_F|(|B_F| \cdot |\mathcal{A}_d| + 1)$. Consequently, the system is diagnosable with a finite delay $n = |B_F|(|B_F| \cdot |\mathcal{A}_d| + 1)$. So the sufficiency holds.

B. Proof of Proposition 1 in Section IV.B

Proof: Suppose no fault-free cycle exists in $\mathbf{G}$. Since faults are permanent, a cycle in $\mathbf{G}$ composed of several faulty basic state-trees and normal basic state-trees can not exist. Hence, at least one faulty cycle exists in $\mathbf{G}$, which leads to the F-uncertain cycle cl. In this case, event σ_n is not eligible at normal basic state-trees satisfying M_n. Hence, after the occurrence of σ_n the successor predicate of M_n must be faulty, which leads to a contradiction.

C. Proof of Proposition 2 in Section IV.B

Proof: From Proposition 1, there exists at least one fault-free cycle formed by basic state-trees in $\mathbf{G}$ that has the same observation $(\sigma_1\sigma_2\cdots\sigma_n)^*$. Then, we only need to show that a corresponding faulty cycle formed by basic state-trees in $\mathbf{G}$ also shares the same observation as cl. Suppose $(\forall i \in [1, n], \forall \sigma_f \in \Sigma_f)$ $\Delta(M_i \wedge P_N, \sigma_f) \equiv \mathit{false}$. Then, we have $M_{(i+1)mod_n} \wedge P_F = \langle \Delta(M_i \wedge P_F, \sigma_i) \rangle$. Based on Lemma 1, for any $b_{n+1} \models M_1 \wedge P_F$, there exist $b_i \models M_i \wedge P_F$ $(1 \leq i \leq n)$ such that $b_i \overset{\sigma_i}{\rightarrowtail} b_{i+1}$. Let $b_{n+1} = b_1$. Then $b_1, \cdots, b_n$ forms an underlying faulty cycle, we can infer that a corresponding faulty cycle formed by basic state-trees in $\mathbf{G}$ with the same observation as cl exists. Hence, the cycle cl is an F-indeterminate one as well.

D. Wang is with the School of Electrical Engineering, Guizhou University, Guiyang 550025, China (e-mail: dgwang@gzu.edu.cn, wdeguang1991@163.com).

X. Wang is with the School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China and also with the Lehrstuhl für Regelungstechnik, Friedrich-Alexander-Universität Erlangen-Nürnberg, Cauerstr. 7, 91058 Erlangen, Germany. (e-mail: wangxi@xidian.edu.cn, xi.wang@fau.de).

J. Yang is with the School of Electrical Engineering, Guizhou University, Guiyang 550025, China (e-mail: jyang7@gzu.edu.cn).

Q. Tang is with the Hitachi Building Technology (Guangzhou) Co., Ltd, Guangzhou 510700, China (e-mail: tangqiwei@hitachi-helc.com).

Z. Li is with the Institute of Systems Engineering, Macau University of Science and Technology, Taipa, Macau and also with the School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China (e-mail: zhwli@xidian.edu.cn).

D. Proof of Proposition 3 in Section IV.B

Proof: It can be proved using mathematical induction.
BASIS STEP: For $k = 1$, $S^{cl}_{n+1} \preceq S^{cl}_1$ is true because $S^{cl}_1 = M_1 \wedge P_F$ and $S^{cl}_2 = \langle \Delta(S^{cl}_1, \sigma_1)\rangle \preceq M_2 \wedge P_F = \langle \Delta(M_2 \wedge P_N, \Sigma_f) \cup \Delta(M_1 \wedge P_F, \sigma_1)\rangle$, with the same reasoning along the event sequence $\sigma_1, \ldots, \sigma_n$, we have $S^{cl}_n = \langle \Delta(S^{cl}_{n-1}, \sigma_{n-1})\rangle \preceq M_n \wedge P_F = \langle \Delta(M_n \wedge P_N, \Sigma_f) \cup \Delta(M_{n-1} \wedge P_F, \sigma_{n-1})\rangle$. Hence, $S^{cl}_{n+1} = \langle \Delta(S^{cl}_n, \sigma_n)\rangle \preceq M_1 \wedge P_F = \langle \Delta(M_1 \wedge P_N, \Sigma_f) \cup \Delta(M_n \wedge P_F, \sigma_n)\rangle = S^{cl}_1$.
INDUCTIVE STEP: Suppose $S^{cl}_{1+kn} \preceq S^{cl}_{1+(k-1)n}$. We need to show $S^{cl}_{1+(k+1)n} \preceq S^{cl}_{1+kn}$. Since $S^{cl}_{1+kn} = \langle \Delta(S^{cl}_{kn}, \sigma_n)\rangle$ and $S^{cl}_{(k+1)n} \preceq S^{cl}_{kn}$, $S^{cl}_{(k+1)n} = \langle \Delta(S^{cl}_{(k+1)n})\rangle \preceq \langle \Delta(S^{cl}_{kn}, \sigma_n)\rangle = S^{cl}_{1+kn}$.

E. Proof of Theorem 4 in Section IV.B

Proof: (only if): Suppose that cl is an F-indeterminate cycle. Then we need to show that the fixed point reached by sequence S'^{cl} associated with cl is no-empty.

Since cl is an F-indeterminate cycle, at least one faulty cycle formed by basic state-trees in $\mathbf{G}$ exists. Assume there exist exactly m faulty cycles ($m \geq 1$). There exist a string s^j_i in Σ^*_{uo} and a basic state-tree b^j_i satisfying $M_i \wedge P_F$ such that $b^j_{(i+1)_{mod_n}} = \Delta(b^j_i, s^j_i \sigma_i)$ and $b^j_1 = \Delta(b^j_n, s^j_n \sigma_n)$ ($1 \leq i \leq n$, $1 \leq j \leq m$). Thus, $(\forall k \in \mathbb{N}^*)$ $b^j_i \models S^{cl}_{i+nk}$, indicating that all the terms of S'^{cl} are non-empty. Clearly, the reached fixed point is also non-empty.

(if): Suppose that sequence S'^{cl} associated with cl has a non-empty fixed point. Now, we need to show that cl is an F-indeterminate cycle. From Proposition 1, the existence of a faulty cycle sharing the same observation with cl is sufficient.

We know that there exists an integer $k \in \mathbb{N}^*$ such that $S^{cl}_{1+kn} = S^{cl}_{1+(k-1)n}$. Due to $S^{cl}_{1+kn} \not\equiv false$, we assume that the predicate S^{cl}_{1+kn} holds exactly on the basic state-tree subset $B_{S^{cl}_{1+kn}} = \{b_1, \ldots, b_m\}$. According to the definition of sequence S^{cl}, there exist $b_i, b_j \in B_{S^{cl}_{1+kn}}$, and $t = s_1\sigma_1 s_2\sigma_2 \ldots s_{n-1}\sigma_{n-1} s_n\sigma_n$ with $s_l \in \Sigma^*_{uo}$ such that $b_i = \Delta(b_j, t)$ ($1 \leq l \leq n, 1 \leq i, j \leq m$). By repeating this procedure to b_i at least m times, we can infer that b_i is certainly visited twice, which indicates the existence of at least one faulty cycle. Therefore, the cycle cl is F-indeterminate.