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, $b' \in \mathcal{B}(\mathbf{ST})$ and two condition labels $\ell, \ell' \in \mathcal{L}$, $(b', \ell'$ is said to be observation-adjacent to (b, ℓ) (write as $(b, \ell) \overset{\sigma}{\rightarrowtail} (b', \ell')$) if there exists a string $s\sigma t$ in which $s, t \in \Sigma_{uo}^*$ and $\sigma \in \Sigma_o$ such that $b' = \Delta(b, s\sigma t)$ and $\ell' = \nabla(\ell, s\sigma t)$.* $\diamondsuit$

Assume in the diagnoser $\mathbf{G}_d = (\mathcal{A}_d, \Sigma_o, \Delta_d, A_{d0})$ $cl = A_{d1} \xrightarrow{\sigma_1} \cdots \xrightarrow{\sigma_{n-2}} A_{d(n-1)} \xrightarrow{\sigma_{n-1}} A_{dn} \xrightarrow{\sigma_n} A_{d1}$ with $n \geq 1$ is an F_i-indeterminate cycle ($1 \leq i \leq m$). A cycle $cl' = (b_1, \ell_1) \overset{\sigma_1}{\rightarrowtail} \cdots \overset{\sigma_{n-2}}{\rightarrowtail} (b_{n-1}, \ell_{n-1}) \overset{\sigma_{n-1}}{\rightarrowtail} (b_n, \ell_n) \overset{\sigma_n}{\rightarrowtail} (b_1, \ell_1)$ is called an *underlying faulty cycle* of cl if $(b_j, \ell_j) \in A_{dj}$ and $F_i \in \ell_j$ ($1 \leq j \leq n$). Intuitively, if there is an F_i-indeterminate cycle, then the system has a cycle in the faulty condition F_i such that when it evolves on the cycle, it will generate the event sequence periodically. The cycle in the F_i and the corresponding event sequence keeps the diagnoser in the F_i-uncertain cycle indefinitely, and in this case, the system is not diagnosable.

Lemma 1. *Let $p = A_{d1} \xrightarrow{\sigma_1} \cdots \xrightarrow{\sigma_{n-2}} A_{d(n-1)} \xrightarrow{\sigma_{n-1}} A_{dn}$ ($n \geq 2$) be a path in the diagnoser $\mathbf{G}_d$ and each A_{dj} be F_i-uncertain ($1 \leq j \leq n$). For any $(b_n, \ell_n) \in A_{dn}$, there exist $(b_k, \ell_k) \in A_{dk}$ ($1 \leq k \leq n-1$) such that $(b_k, \ell_k) \overset{\sigma_k}{\rightarrowtail} (b_{k+1}, \ell_{k+1})$.*

A. Proof of Theorem 2 in Section III

Proof: (only if): Suppose that $\mathbf{G}$ is diagnosable, but there exists an F_i-indeterminate cycle cl in the diagnoser $\mathbf{G}_d = (\mathcal{A}_d, \Sigma_o, \Delta_d, A_{d0})$. Since $\mathbf{G}_d$ is reachable, there exists an event sequence that can take the diagnoser into A_{dk} belonging to cl. Let $(b_n, \ell_n) \in A_{dn}$ belong to an underlying faulty cycle of cl. By Lemma 1, there exist pairs $(b_1, \ell_1), \cdots, (b_{n-1}, \ell_{n-1})$ such that $(b_j, \ell_j) \overset{\sigma_i}{\rightarrowtail} (b_{j+1}, \ell_{j+1})$ ($1 \leq j \leq n-1$). After reaching b_n with condition label ℓ_n, the system may remain on the underlying faulty cycle causing the diagnoser to stay on the F_i-indeterminate cycle indefinitely. Therefore, there exists a trajectory for the system leading to basic state-trees with fault label F_i such that the corresponding event sequence throws the diagnoser into a cycle of F_i-uncertain BSTAs 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_i-indeterminate cycle exists in the diagnoser $\mathbf{G}_d$. After the occurrence of F_i and the generation of a new observable event, the diagnoser reaches either F_i-certain or F_i-uncertain BSTA. If it is an F_i-certain BSTA, then it will remain F-certain (because fault is permanent) and the system is diagnosable. If it is an F_i-uncertain BSTA, then the number of F_i-uncertain BSTAs is bounded. After the generation of a bounded number of observable events, the diagnoser will reach an F_i-certain BSTA (the diagnoser gets trapped indefinitely in a cycle of F_i-uncertain BSTAs only if the cycle is F_i-indeterminate).

Let n denote the number of events that it takes the diagnoser to detect and isolate. After the occurrence of fault events in Σ_{f_i}, the diagnoser can visit an F_i-uncertain BSTA A_d at most $|N_{A_d}|$ times, where $|N_{A_d}|$ is the number of basic state-trees with fault labels F_i. Then we have $n \leq c \times M + M$, where $c = \sum_{A_d \in \mathcal{A}_d} |N_{A_d}|$ and M is the length of the longest path of faulty basic state-trees. Since $M \leq |\mathcal{A}_d|$ and $c \leq |\mathcal{A}_d| \cdot |\mathcal{A}_d|$, $n \leq c \times M + M \leq |\mathcal{A}_d| \cdot |\mathcal{A}_d| \cdot |\mathcal{A}_d| + |\mathcal{A}_d| = |\mathcal{A}_d|(|\mathcal{A}_d|^2 + 1)$. Consequently, the system is diagnosable with a finite delay $n = |\mathcal{A}_d|(|\mathcal{A}_d|^2 + 1)$. 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_i-uncertain cycle cl. In this case, event σ_n is not eligible at normal basic state-trees satisfying P_{nN}. Hence, after the occurrence of σ_n the successor predicate of P_{nN} 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 $(\forall k \in [1, n], \forall \sigma_f \in \Sigma_{fi})$ $\Delta(P_{kN}, \sigma_f) \equiv$ *false*. Let P_k be the predicate satisfied by the state estimation after occurring event σ_k. Then, we have $P_{(k+1) mod_n F_i} = \langle \Delta(P_{kF_i}, \sigma_k) \rangle \vee \langle \Delta(P_k, \sigma_k) \rangle_{F_i}$. Based

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).

on Lemma 1, for any $b_{n+1} \models P_{1F_i}$, there exist $b_k \models P_{kF_i}$ $(1 \leq k \leq n)$ such that $(b_k, \ell_k) \stackrel{\sigma_i}{\rightarrowtail} (b_{k+1}, \ell_{k+1})$. 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_i-indeterminate one as well.

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 $S^{cl}_1 = P_{1F_i}$ and $S^{cl}_2 = \langle\Delta(S^{cl}_1, \sigma_1)\rangle \preceq P_{2F_i} = \langle\Delta(P_{1F_i}, \sigma_1)\rangle \vee \langle\Delta(P_1, \sigma_1)\rangle_{F_i}$, with the same reasoning along the event sequence $\sigma_1, \ldots, \sigma_n$, we have $S^{cl}_n = \langle\Delta(S^{cl}_{n-1}, \sigma_{n-1})\rangle \preceq P_{nF_i} = \langle\Delta(P_{(n-1)F_i}, \sigma_{n-1})\rangle \vee \langle\Delta(P_{n-1}, \sigma_{n-1})\rangle_{F_i}$. Hence, $S^{cl}_{n+1} = \langle\Delta(S^{cl}_n, \sigma_n)\rangle \preceq P_{1F_i} = S^{cl}_1$.
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_i-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_i-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_l in Σ^*_{uo} and a basic state-tree b^j_l satisfying P_{lF_i} such that $b^j_{(l+1)_{mod_n}} = \Delta(b^j_l, s^j_l\sigma_l)$ and $b^j_1 = \Delta(b^j_n, s^j_n\sigma_n)$ $(1 \leq l \leq n, 1 \leq j \leq M)$. Thus, $(\forall k \in \mathbb{N}^*)$ $b^j_l \models S^{cl}_{l+nk}$, 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_i-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 $B_{S^{cl}_{1+kn}} = \{b_1, \ldots, b_N\}$. According to the definition of sequence S^{cl}, there exist $b_r, b_j \in B_{S^{cl}_{1+kn}}$, 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 $b_r = \Delta(b_j, t)$ $(1 \leq l \leq n, 1 \leq r, j \leq N)$. By repeating this procedure to b_r at least N times, we can infer that b_r is certainly visited twice, which indicates the existence of at least one faulty cycle. Therefore, the cycle cl is F_i-indeterminate.