

不完备离散事件系统的当前状态不透明性

刘富春[†], 张旭, 赵锐

(广东工业大学 计算机学院, 广东 广州 510006)

摘要: 本文针对不完备系统模型, 研究不完备离散事件系统的当前状态不透明性. 根据系统的实际输出与预测输出之间的差异, 构建了一个具有学习功能的学习诊断器. 这种学习诊断器不仅能够模拟系统的状态转移, 而且还可以将系统缺失的状态信息通过学习得到恢复. 通过引入集合覆盖理论处理由学习诊断器得出的结果, 提出了一种基于学习诊断器的不完备离散事件系统当前状态不透明性的验证算法.

关键词: 离散事件系统; 不完备模型; 不透明性; 学习诊断器

引用格式: 刘富春, 张旭, 赵锐. 不完备离散事件系统的当前状态不透明性. 控制理论与应用, 2019, 36(7): 1067 – 1071

DOI: 10.7641/CTA.2018.80060

Current-state opacity of incomplete discrete-event systems

LIU Fu-chun[†], ZHANG Xu, ZHAO Rui

(School of Computers, Guangdong University of Technology, Guangzhou Guangdong 510006, China)

Abstract: This paper aims to propose an approach of the current-state opacity for incomplete discrete-event systems (DES) in which some information may be unavailable or even missing. According to the difference between the actual output and the predicted output of the incomplete system, a learning diagnoser is constructed. Note that the learning diagnoser not only can simulate the state transition of the system, but also can restore the absent state information from the system through learning. After the set coverage theory is introduced to deal with the results obtained by the learning diagnoser, a method to verify the current state opacity of an incomplete system is proposed based on the learning diagnoser.

Key words: Discrete-event system; incomplete model; opacity; learning diagnoser

Citation: LIU Fuchun, ZHANG Xu, ZHAO Rui. Current-state opacity of incomplete discrete-event systems. *Control Theory & Applications*, 2019, 36(7): 1067 – 1071

1 引言

近年来, 离散事件系统的状态不透明性在数字签名、信息认证、入侵检测、数据加密等领域取得了重要应用. 具有状态不透明性的系统要求对于任意一条到达系统秘密状态的路径, 至少存在另一条从相同状态出发到达非秘密状态的路径, 使得这两条路径因具有相同观测结果而使入侵者无法区分, 从而达到有效抵御入侵者攻击的目的.

在文献[1]中, Bryans将状态不透明性应用到离散事件系统中, 研究了Petri网的不透明性. 文献[2]针对离散事件系统提出了基于状态的不透明性方法. Wu和Lafortune根据系统中状态分类, 提出了一个验证状态不透明性的状态转换算法^[3]. 在文献[4]中, Lin研究

了离散事件系统基于事件的不透明性, 提出了强不透明性和弱不透明性概念, 并通过引入一种两个自动机的合成规则, 得到了离散事件系统事件不透明性的验证方法. 我们也对不透明性开展了研究, 将不透明性概念应用于故障诊断和故障预测, 分别提出了一种基于不透明性的相对故障诊断方法和相对故障预测方法^[5-6].

然而, 在实际应用中, 往往可能出现因某些原因造成系统部分信息缺失的现象. 为此, 欧阳丹彤等人研究了不完备系统模型的故障诊断问题, 通过引入 P 同步性概念, 提出了一种不完备离散事件系统的故障诊断方法^[7-8]. Kwong和Yonge-Mallo也针对一类不完备离散事件系统, 提出了一种不完备系统建模和故障

收稿日期: 2018-01-20; 录用日期: 2018-09-04.

[†]通信作者. E-mail: fliu2011@163.com; Tel.: +86 13725145446.

本文责任编辑: 赵千川.

国家自然科学基金项目(61673122), 广东省教育厅省级重大项目(2014KZDXM033), 广东省公益研究与能力建设专项资金项目(2015A030402006), 广东工业大学计算机学院重大奖项培育项目(2016PY01)资助.

Supported by the National Natural Science Foundation of China (61673122), the Provincial Major Program of Guangdong (2014KZDXM033), the Public Welfare Research and Capacity Building Project of Guangdong (2015A030402006) and the Major Awards Incubation Project of School of Computers of Guangdong University of Technology (2016PY01).

诊断方法^[9].

本文继续文献[9]的工作,针对这类不完备离散事件系统模型进一步研究其当前状态不透明性.先通过对比实际输出与预测输出之间的差异,构建了一个具有学习功能的学习诊断器.它不仅能够模拟系统的状态转移,而且还可以将系统缺失的状态信息通过学习得到恢复.然后运用集合覆盖理论,对不完备系统模型进行分割、残差、增加残差等运算,提出了一种基于学习诊断器的不完备离散事件系统的当前状态不透明性的验证方法,最后通过一个实例,阐述了学习诊断器的构造过程和当前状态不透明性验证方法的具体运用.

2 离散事件系统及其不透明性

离散事件系统是指一个有限状态自动机 $G = (X, \Sigma, \delta, x_0, Y, \lambda)$,其中: X 为有限状态集, Σ 为有限事件集, δ 为转移函数, x_0 为初始状态, Y 为输出集, λ 为输出映射函数 $\lambda: X \rightarrow Y$.对于状态 $x, x' \in X$,如果 $\lambda(x) = \lambda(x')$,且存在状态 x_1, x_2, \dots, x_{l-1} 和事件 $\sigma_1, \sigma_2, \dots, \sigma_{l-1}$,满足 $x_{i+1} = \delta(x_i, \sigma_{i+1}), 0 \leq i \leq l-1, x_0 = x, x_l = x', \lambda(x_i) = \lambda(x)$,则称状态 x' 为状态 x 的毗邻输出^[11],记为 $x \Rightarrow x'$.

事件集 Σ 分为可观事件集 Σ_o 和不可观事件集 Σ_{uo} ,即 $\Sigma = \Sigma_o \cup \Sigma_{uo}$.记故障事件集为 Σ_f ,它满足 $\Sigma_f \subseteq \Sigma_{uo}$.根据故障对系统的不同影响,往往将故障分为不同类型 F_1, F_2, \dots, F_m .本文用 K 表示系统的条件集,即 $K = \{N, F_1, F_2, \dots, F_m\}$,其中 N 表示正常条件.同时,根据系统的条件集对状态集 X 进行相应分类 $X = X_N \dot{\cup} X_{F_1} \dot{\cup} X_{F_2} \dot{\cup} \dots \dot{\cup} X_{F_m}$,其中符号 $\dot{\cup}$ 为互不相交的并集运算.

定义1 条件映射是指一个映射 $k: X \rightarrow K$,它满足对任意 $x \in X$,如果 $x \in X_N$,则 $k(x) = N$;如果 $x \in X_{F_i}$,则 $k(x) = F_i$,其中 $i \in \{1, 2, \dots, m\}$.并且定义 $\forall z \subseteq X, k(z) = \bigcup_{x \in z} k(x)$.

为方便起见,引入文献[10]中的符号: Σ^* 为 Σ 的克林闭包, L 为系统 G 的生成语言, $L(G, x_i)$ 为 G 中从状态 x_i 出发的所有运动轨迹的集合.

定义2 投影 P 是指映射 $P: \Sigma^* \rightarrow \Sigma_o^*$,它满足当 $\sigma \in \Sigma_o$ 时, $P(\sigma) = \sigma$;当 $\sigma \in \Sigma_{uo}$ 时, $P(\sigma) = \varepsilon$;并且对任意 $\sigma \in \Sigma$ 和 $t \in \Sigma^*$, $P(t\sigma) = P(t)P(\sigma)$. P 的反投影定义为 $P^{-1}(\mu) = \{t | t \in L, P(t) = \mu\}$,其中 $\mu \in \Sigma_o^*$.

定义3 给定系统 G 的秘密状态集 $X_s \subseteq X$ 和非秘密状态集 $X_{ns} \subseteq X$,如果 G 满足如下条件:

$$(\forall x_i \in X)(\forall t \in L(G, x_i))(\delta(x_i, t) \in X_s \Rightarrow$$

$$(\exists t' \in L(G, x_i))(\delta(x_i, t') \in X_{ns} \wedge P(t) = P(t')),$$

则称 G 具有当前状态的不透明性.

直观上,系统 G 具有当前状态的不透明性表示:对于到达秘密状态的每条路径 t ,都存在另一条到达非秘密状态的路径 t' ,使得这2条路径具有相同的投影.显然,具有当前状态不透明性的系统能够使入侵者无法确定系统的当前状态是否处于秘密状态.

3 不完备离散事件系统

对于离散事件系统 $G = (X, \Sigma, \delta, x_0, Y, \lambda)$,诊断器可以构造为一个有限状态自动机^[11]

$$D = (Z \cup \{z_0\}, Y, \zeta, z_0, \hat{K}, k), \quad (1)$$

其中: $Z \cup \{z_0\}$ 为状态集; $z_0 = (z_0, 0)$ 为初始状态, $z_0 \in 2^X - \emptyset$;转移函数为 $\zeta: Z \cup \{z_0\} \times Y \rightarrow Z$; \hat{K} 为输出集;输出映射为 $k: Z \cup \{z_0\} \rightarrow \hat{K}$;其中状态转移 $z_{k+1} = \zeta(z_k, y_{k+1})$ 可通过如下的条件得出:

$$\begin{cases} z_1 = \zeta(z_0, y_1) = z_0 \cap \lambda^{-1}(\{y_1\}), \\ z_{k+1} = \Psi(z_k) \cap \lambda^{-1}(\{y_{k+1}\}), k \geq 1, \end{cases} \quad (2)$$

这里 $\Psi(z) = \{x | \exists x' \in z: x' \Rightarrow x\}$.

但是,上述诊断器 D 的构造是以在完备离散事件系统的基础上构造出来的,一旦系统中出现了状态缺失(即系统 G 为不完备模型)时该诊断器的构造方法就不再适用.为此,针对不完备系统模型,作者引用类似文献[9]中的方法,引入2个辅助模型:真实模型(true model) $G_t = (X, \Sigma_t, \delta_t, x_0, Y, \lambda)$ 和名义模型(nominal model) $G_n = (X, \Sigma_n, \delta_n, x_0, Y, \lambda)$,其中 $\Sigma_n \subseteq \Sigma_t, \delta_n \subseteq \delta_t$.

本文把根据名义模型 G_n 构造的诊断器称为名义诊断器,记为 D_n .给定一个输出序列 y_1, y_2, \dots, y_k ,如果对所有 $k \geq 1$,状态转移都满足 $\Psi(z_k) \cap \lambda^{-1}(\{y_{k+1}\}) \neq \emptyset$,其中 z_k 为 D_n 中的状态估计,则称 G_n 与 G_t 的输出序列是一致的.

为弥补 G_n 与 G_t 之间差异,可引入假设转移 H 对 G_n 进行修正.用有序状态对 $d = (x_{src}, x_{dst})$ 表示假设转移 H 中从状态 x_{src} 到状态 x_{dst} 的转移,简记为 d_{dst}^{src} ,其中 $x_{src}, x_{dst} \in X$.为了描述名义模型中的缺失转换,用 $\phi(z, x)$ 表示从起始状态到目标状态的所有假设转移,即

$$\phi(z, x) = \{d_x^{x'} | x' \in z, (\exists \sigma)\delta(x', \sigma) = x\}.$$

对于 $H = \phi(z, x)$,用 $dst(H)$ 表示 H 中目标状态 x ,即 $dst(H) = x$,并定义

$$\Phi(z, y) = \{\phi(z, x) | x \in \lambda^{-1}(\{y\})\}. \quad (3)$$

为了得到假设转移中状态之间的关系,本文运用文献[12]中提出的集合覆盖理论处理关于假设的集合覆盖问题.

定义4 一个集合覆盖是指一个四元组 $P = (D^*, M, R, M^+)$,其中 $D^* = \{d_1, \dots, d_n\}$ 为假设转移 d_i 的集合, $M = \{m_1, \dots, m_j\}$ 为表现形式 m_i 的集

合, $R \subseteq D^* \times M$ 为 D^* 和 M 之间的联系, 称为因果关系, M^+ 为 M 的一个子集.

集合覆盖描述了各个假设转移 D^* 与各表现形式 M 之间的因果关系. 由 d_i 引起的表现形式集记为 $\text{effect}(d_i) = \{m_j | (d_i, m_j) \in \mathbb{R}\}$, 发生 m_j 的假设转移集记为 $\text{cause}(m_j) = \{d_i | (d_i, m_j) \in \mathbb{R}\}$, 这里 $d_i \in D^*, m_j \in M$.

下面引入文献[9]中分割、残差、增加残差等运算及文献[12]中生成器概念以描述不完备模型的在名义模型中的假设转移.

定义 5 设 $\mathcal{G}_I = (g_1, \dots, g_n)$ 为一个(假设转移)生成器, $H \subseteq D^*$ 且 $H \neq \emptyset$, 如果对于任意的 $1 \leq k \leq n$ 且 $\mathcal{Q}_k = (q_{k1}, q_{k2}, \dots, q_{kn})$, 其中

$$q_{kj} = \begin{cases} g_j - H, & j < k, \\ g_j \cap H, & j = k, \\ g_j, & j > k, \end{cases} \quad (4)$$

则 $Q = \{\mathcal{Q}_k | \mathcal{Q}_k \text{ 为一个生成器}\}$ 称为 \mathcal{G}_I 与 H 的分割操作, 记为 $\text{div}(\mathcal{G}_I, H)$.

定义 6 设 $\mathcal{G}_I = (g_1, \dots, g_n)$ 为一个生成器, $H \subseteq D^*$ 且 $H \neq \emptyset, A \neq \emptyset$. 如果对任意 $i, g_i - H \neq \emptyset$, 则定义 \mathcal{G}_I 与 H 残差分割为

$$\text{res}(\mathcal{G}_I, H) = \{(g_1 - H), \dots, (g_n - H)\};$$

否则, 定义为 $\text{res}(\mathcal{G}_I, H) = \emptyset$. 如果对任意 $i, g_i - H \neq \emptyset$, 则定义 \mathcal{G}_I 与 H 的增加残差分割为

$$\text{augres}(\mathcal{G}_I, H) = \{(g_1 - H), \dots, ((g_n - H), A)\};$$

否则, 定义为 $\text{augres}(\mathcal{G}_I, H) = \emptyset$.

对于集合覆盖 $P = (D^*, M, R, M^+)$, \mathcal{G} 的类别中包括对 M 的所有解释, 若存在表现形式 $m_j \notin M$, 则需要对生成器集进行修正. 修正后的生成器集定义为

$$\text{revise}(\mathcal{G}_I, H) = F \cup \text{res}(Q, F), \quad (5)$$

这里 $F = \text{div}(\mathcal{G}_I, H)$, $Q = \text{augres}(\mathcal{G}_I, H)$, 其中 $H = \text{cause}(m_j)$.

假设 $\mathcal{G}_I = \{g_1, \dots, g_n\}$ 和 $\mathcal{Q}_J = \{q_1, \dots, q_m\}$ 是两个生成器, 记它们的并集为 $M(\mathcal{G}_I, \mathcal{Q}_J)$, 它表示生成器 \mathcal{G}_I 和 \mathcal{Q}_J 之间所包含的最小数量的生成器.

4 不完备离散事件系统的学习诊断

为研究不完备系统的不透明性, 引入一种具有学习功能的学习诊断器以尝试学习真实模型, 它以系统的输出序列作为输入, 得到在名义模型中缺少的信息, 并依据各假设预测系统缺失信息.

为了清晰描述学习诊断器中的状态和假设转移, 定义候选(candidate)为 $c = (\mathcal{G}, z)$, 其中 z 为系统的状态估计, \mathcal{G} 为生成器集, 表示所有的假设集.

假设 Z_n 为名义诊断器 D_n 中的状态集, ζ_n 为 D_n 的

转移函数, y 为输出序列中的一个输出事件. 通过 D_n 的状态转换 $z' = \zeta(z, y)$ 得到 $z' = \{x | \lambda(x) = y \wedge (\exists x' \in z : x' \Rightarrow x)\} = \Psi(z) \cap \lambda^{-1}(\{y\})$. 针对候选 c , 得到其更新:

$$\text{update}(c, y) = \begin{cases} \{(\mathcal{G}, z')\}, & \text{若 } z' \neq \emptyset, \\ \{(\mathcal{G}', \text{dst}(H)) | H \in \Phi(z, y), \\ \mathcal{G}' = \text{revise}(\mathcal{G}, H)\}, & \text{其他.} \end{cases}$$

将学习诊断器 LD 构造为一个有限状态自动机

$$LD = (W \cup \{\underline{w}_0\}, Y, t, \underline{w}_0, \hat{k}, k),$$

其中: $W \cup \{\underline{w}_0\}$ 为状态集, Y 为事件集, t 为转移函数 $t: W \cup \{\underline{w}_0\} \times Y \rightarrow W$, $\underline{w}_0 = (w_0, 0)$ 为初始状态, $\hat{k} \subseteq 2^k - \{\emptyset\}$ 为输出集, k 为输出映射.

对于 $w^1 = \{c_1^1, \dots, c_k^1\}$, $w^2 = \{c_1^2, \dots, c_l^2\}$, 其中 c_s^r 表示候选 (\mathcal{G}_s^r, z_s^r) , 如果 w^1 与 w^2 之间存在相同状态估计, 则定义 $\mu(w^1, w^2)$ 为将 w^2 中的重复状态合并到 w^1 , 即

$$\mu(w^1, w^2) = \begin{cases} w^1, & \text{若 } w^2 = \emptyset, \\ \mu(\{c_1^1, \dots, (M(\mathcal{G}_i^1, \mathcal{G}_1^2), z_i^1), \dots, c_k^1\}, \\ \{c_2^2, \dots, c_l^2\}), & \text{若 } z_i^1 = z_i^2, \\ \mu(\{c_1^1, \dots, c_k^1, c_2^2\}, \{c_2^2, \dots, c_l^2\}), & \text{其他.} \end{cases}$$

LD 中的状态转移函数 $w_{k+1} = t(w_k, y_{k+1})$ 通过如下公式得到:

$$\begin{cases} t(w_0, y_1) = \{(\emptyset, z_0 \cap \lambda^{-1}(\{y_1\}))\}, \\ t(w_k, y_{k+1}) = \text{update}(w_k, y_{k+1}), \forall k \geq 1. \end{cases} \quad (6)$$

直观上, 对于不完备离散事件系统 G , 上述学习诊断器 LD 将在不透明性条件下通过有限步学习使得系统的缺失状态信息得到恢复. 下面具体给出验证不完备系统是否具有当前状态不透明性算法.

算法 1 关于不完备离散事件系统 G 是否具有当前状态不透明性的验证方法

第1步 根据真实模型 G_t , 得出状态缺失的不完备模型 G_n 在具备当前状态不透明性的假设转移.

第2步 对于得到的假设转移使用分割、残差及增加残差运算进行处理, 得到生成器集 \mathcal{G} .

第3步 对于不完备模型 G_n , 通过引入候选 c 和学习诊断器 LD , 得到每步的生成器集 \mathcal{G}_i , 并用分割等方法修正 \mathcal{G}_i , 从而得到生成器集 \mathcal{G}^* .

第4步 对比第2步和第3步得到的生成器集 \mathcal{G} 和 \mathcal{G}^* , 如果 $\mathcal{G} = \mathcal{G}^*$, 则不完备系统 G 具有当前状态不透明性; 否则, G 不具有当前状态不透明性.

注 1 算法1的前2步得到一个具有当前状态不透明性的完备系统生成器集 \mathcal{G} , 而在第3步中不完备系统中的 G_n 通过学习诊断器 LD 得到另一个完备系统的生成器集 \mathcal{G}^* . 如

果 $G = G^*$, 则说明这2个完备系统是一致的, 从而不完备系统 G 具有当前状态不透明性. 反之, 则说明 G 不具有当前状态不透明性.

下面分析算法1的复杂性. 假设系统有 n 类表现形式 $M = \{m_1, \dots, m_n\}$, 令 $n_1 = \max|\lambda^{-1}(\{y\})|$. 由于每类表现形式的生成器的转移方式有 $2^n - 1$ 种, 所以生成器集 \mathcal{G} 包含的转移方式有 $(2^n - 1)n$ 种. 对于假设 H , 修正操作中每类的状态数为 n_1 , 故假设的最大数量为 nn_1 , 修正函数 $\text{revise}(\mathcal{G}, H)$ 最多有 $(2^n - 1) \cdot n^2 n_1$ 个假设. 由此, 如果候选状态为单一类型时, 则算法1的复杂度为 $O(2^n n^2 n_1)$. 如果候选状态包含 n_1 种类型时, 则算法1的复杂度为 $O(2^n n^2 n_1^2)$.

5 实例分析

下面通过一个具体实例阐述上述关于不完备系统是否具有当前状态不透明性的判定方法.

例 1 考虑图1中的离散事件系统 G , 其中不可观事件集 $\Sigma_{uo} = \{a, b\}$, 秘密状态集 $X_s = \{11\}$. 假设状态4和状态8在真实模型 G_t 中的转换 d_{11}^4 和 d_{11}^8 在名义模型 G_n 中的信息是缺失的. 下面选定 $\lambda\alpha\mu\varphi\lambda\eta\varphi\lambda\beta\theta$ 作为 G 的输出序列, 判断不完备系统 G 是否具有当前状态不透明性.

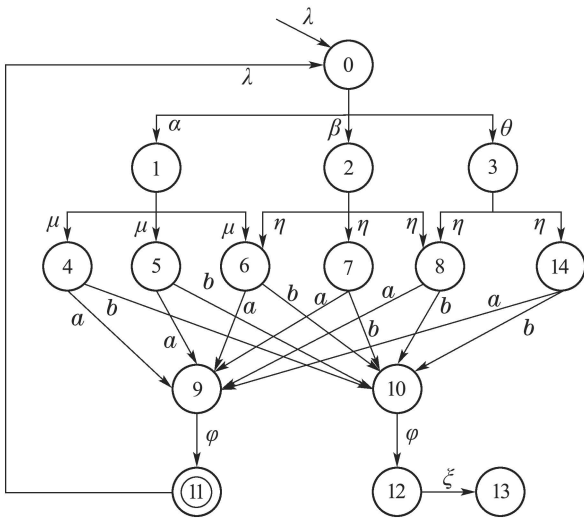


图1 离散事件系统 G
Fig. 1 Discrete-event system G

当输出序列 $\lambda\alpha\mu$ 发生后, 真实模型 G_t 的状态为 $z = \{4, 5, 6\}$. 在下一个输出 φ 发生后, 状态间接到达 $\{11, 12\}$, 此时可能发生的转换为 $\{d_{11}^4, d_{11}^5, d_{11}^6, d_{11}^7, d_{11}^8, d_{11}^9, d_{11}^{10}\}$. 在当前状态, 系统表现出了当前状态的不透明性, 因为存在着具有相同的投影的路径 $\lambda\alpha\mu\varphi$, 使外界无法确认系统的当前状态. 当输出 λ 发生后, 到达状态1. 由此可推断出上一步到达的是状态11, 假设转换为 $\{d_{11}^4, d_{11}^5, d_{11}^6\}$. 同理, 考虑剩余序列 $\lambda\eta\varphi\lambda\beta\theta\eta\varphi\lambda$, 得到当前状态不透明的假设为 $\{d_{11}^6, d_{11}^7, d_{11}^8\}$ 和 $\{d_{11}^8, d_{11}^{14}\}$. 因此, G_n 中丢失的转换来自 $\{d_{11}^4, d_{11}^5, d_{11}^6\}$, $\{d_{11}^6, d_{11}^7, d_{11}^8\}$ 或者 $\{d_{11}^8, d_{11}^{14}\}$ 中某个路径. 此时如果将假设 $H = \{d_1, d_2, d_3\}$ 添加到 G_n 时, $d_1 \in \{d_{11}^4, d_{11}^5, d_{11}^6\}$, $d_2 \in \{d_{11}^6, d_{11}^7, d_{11}^8\}$, $d_3 \in \{d_{11}^8, d_{11}^{14}\}$ 所得到的模型与真实模型 G_t 输出序列一致, 其诊断器的转移分析图如图2所示.

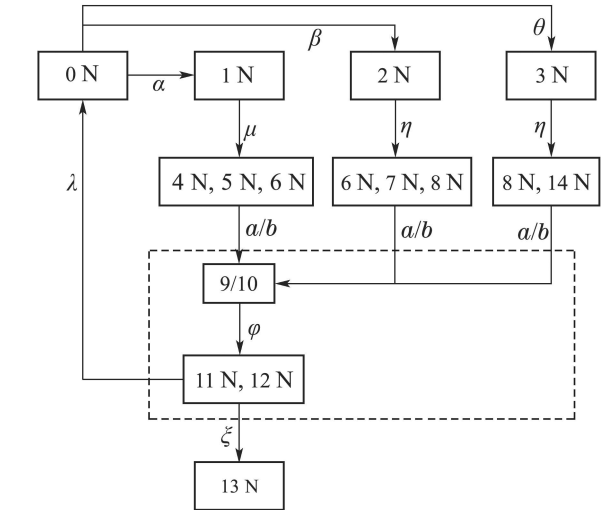


图2 诊断器状态转移
Fig. 2 State transitions of diagnoser

另一方面, 不完备模型在起始条件下的表现形式为 $M_0 = \emptyset, \mathcal{G}_0 = \emptyset$. 在发生输出序列 $\lambda\alpha\mu\varphi$ 后, 可得假设转移 $H_1 = \{d_{11}^4, d_{11}^5, d_{11}^6\}$, 此时 $\mathcal{G}_1 = \{(\{d_{11}^4, d_{11}^5, d_{11}^6\})\}$, $M_1 = \{m_1\}$. 当发生输出序列 $\lambda\beta\mu\varphi$ 后, $H_2 = \{d_{11}^6, d_{11}^7, d_{11}^8\}$, 由图2可知, 事件 μ 和事件 η 的发生都将到达状态6, 此时 $\mathcal{G}_2 = \{(\{d_{11}^4, d_{11}^5, d_{11}^6\}), (\{d_{11}^6, d_{11}^7, d_{11}^8\})\}$. 在发生输出序列 $\lambda\theta\eta\varphi\lambda$ 后, $H_3 = \{d_{11}^8, d_{11}^{14}\}$, 假设转移中出现了重复的转换, 所以

$$\mathcal{G}_3 = \{(\{d_{11}^4, d_{11}^5, d_{11}^6\}) (\{d_{11}^8\}) (\{d_{11}^6, d_{11}^7\}) (\{d_{11}^{14}\})\},$$

$$M_3 = \{m_1, m_2, m_3\}.$$

因此, 在发生输出序列 $\lambda\alpha\mu\varphi\lambda\eta\varphi\lambda\beta\theta\eta\varphi\lambda$ 时, 在系统具有当前状态不透明性条件下得到的生成器集为 $\mathcal{G} = \{(\{d_{11}^4, d_{11}^5, d_{11}^6\}) (\{d_{11}^8\}) (\{d_{11}^6, d_{11}^7\}) (\{d_{11}^{14}\})\}$.

然后, 引入学习诊断器, 初始候选 $c_0 = (\mathcal{G}_0, X)$, 其中 $\mathcal{G}_0 = \emptyset$. 在发生 $\lambda\alpha\mu$ 后, 出现的状态估计 $z_3 = \{4, 5, 6\}$. 此时 $\mathcal{G}_3 = \emptyset, c_3 = (\mathcal{G}_3, z_3)$. 在事件 φ 发生后, $z_4 = \{11, 12\}$. 由于 $X_s = \{11\}$ 并且事件 a 与 b 为不可观事件, 所以有 $c_{4a} = (\mathcal{G}_{4a}, \{11\}), c_{4b} = (\mathcal{G}_{4b}, \{12\}), \mathcal{G}'_{4a} = \{(\{d_{11}^4, d_{11}^5, d_{11}^6\})\}, \mathcal{G}'_{4b} = \{(\{d_{11}^6, d_{11}^7, d_{11}^8\})\}$. 当输出 λ 和 $\beta\eta$ 相继发生后, 可以进行类似分析. 直到当 φ 再次发生时, 由于 $X_s = \{11\}$ 且 $\Sigma_{uo} = \{a, b\}$, 出现了2个状态, 使外界无法判知系统当前到达的状态, 此时名义模型缺失的转换变为 $\{d_{11}^6, d_{11}^7, d_{11}^8\}$ 和 $\{d_{11}^6, d_{11}^7, d_{11}^8\}$. 由此得出候选

$$\mathcal{G}'_{8a} = \{(\{d_{11}^4, d_{11}^5, d_{11}^6\}) (\{d_{11}^6, d_{11}^7, d_{11}^8\})\},$$

$$\mathcal{G}'_{8b} = \{(\{d_{11}^4, d_{11}^5, d_{11}^6\}) (\{d_{11}^6, d_{11}^7, d_{11}^8\})\}.$$

当事件 λ 发生后, 得到如图3所示的最终生成器集为

$$\mathcal{G}^* = \{(\{d_{11}^4, d_{11}^5, d_{11}^6\}\{d_{11}^8\})(\{d_{11}^6, d_{11}^7\}\{d_{11}^{14}\})\}.$$

由 $\mathcal{G} = \mathcal{G}^*$ 得, 不完备系统具有当前状态不透明性.

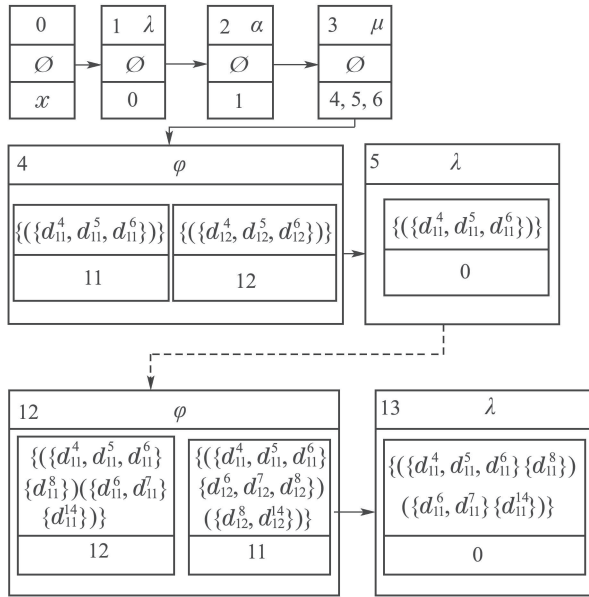


图 3 学习诊断器

Fig. 3 Learning diagnoser

6 总结

本文通过构建学习诊断器分析不完备模型的不透明性. 这种学习诊断器不仅能够模拟系统的状态转移, 而且可以将系统缺失的状态信息通过学习得到恢复, 进而实现对不完备系统当前状态不透明性的验证. 这种方法将完备离散事件系统的当前状态不透明性方法拓展至不完备系统模型. 在此基础上, 作者将在后续研究中进一步考虑不完备模型条件下初始状态不透明性以及具有双模拟关系的非确定离散事件系统^[13]的不透明性等相关问题.

参考文献:

[1] BRYANS J W, KOUTNY M, RYAN P Y A. Modelling opacity using petri nets. *Electronic Notes in Theoretical Computer Science*, 2005, 121: 101 – 115.
 [2] SABOORI A, HADJICOSTIS C N. Notions of security and opacity in discrete event systems. *IEEE Conference on Decision and Control*. Wuxi: IEEE, 2007: 5056 – 5061.

[3] WU Y C. Comparative analysis of related notions of opacity in centralized and coordinated architectures. *Discrete Event Dynamic Systems*, 2013, 23(3): 307 – 339.
 [4] LIN F. Opacity of discrete event systems and its applications. *Automatica*, 2011, 47(3): 496 – 503.
 [5] ZHAO R, LIU F, LIU Z. Relative diagnosability of discrete-event systems and its opacity-based test algorithm. *International Journal of Control Automation & Systems*, 2017, 15(4): 1693 – 1700.
 [6] ZHAO R, LIU F, TAN J. Relative predictability of failure event occurrences and its opacity-based test algorithm. *International Journal of Control*, 2017, 90(6): 1 – 9.
 [7] ZHAO X, OUYANG D. Model-based diagnosis of discrete event systems with an incomplete system model. *European Conference on Artificial Intelligence*. Greece: IOS Press, 2008: 189 – 193.
 [8] WANG Xiaoyu, OUYANG Dantong, ZHAO Jian. Discrete-event system diagnosis upon incomplete model. *Journal of Software*, 2012, 23(3): 465 – 475.
 (王晓宇, 欧阳丹彤, 赵剑. 不完备模型下的离散事件系统诊断方法. *软件学报*, 2012, 23(3): 465 – 475.)
 [9] YEUNG D L, KWONG R H. Fault diagnosis in discrete-event systems: incomplete models and learning. *Proceedings of American Control Conference*. Oregon: AAC, 2005: 3327 – 3332.
 [10] SAMPATH M, SENGUPTA R, LAFORTUNE S, et al. Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, 1995, 40(9): 1555 – 1575.
 [11] ZAD H, KWONG R H, WONHAM W M, et al. Fault diagnosis in discrete-event systems: framework and model reduction. *IEEE Transactions on Automatic Control*, 1998, 48(7): 1199 – 1212.
 [12] GUAN Q, JIANG Y. The parsimonious covering theory applied for communication equipment malfunction. *International Conference on Fuzzy Systems and Knowledge Discovery*. Xiamen: FSKD, 2014: 637 – 641.
 [13] LIU Fuchun. Realization of bisimilarity control of nondeterministic discrete event systems. *Control Theory and Technology*, 2015, 32(1): 75 – 79.
 (刘富春. 非确定离散事件系统双模拟控制的实现. *控制理论与应用*, 2015, 32(1): 75 – 79.)

作者简介:

刘富春 教授, 博士生导师, 目前研究方向为算法分析与设计、离散事件系统监控与故障检测理论与应用, E-mail: fliu2011@163.com;
 张旭 硕士研究生, 目前研究方向为算法分析与设计、离散事件系统监控与故障检测理论与应用, E-mail: 623870814@qq.com;
 赵锐 讲师, 目前研究方向为算法分析与设计、离散事件系统监控与故障检测理论与应用, E-mail: zhaorui118204@163.com.