DOI: 10.7641/CTA.2017.60619

具有多项式时间复杂性的离散事件系统安全诊断

刘富春†, 罗 苹

(广东工业大学 计算机学院, 广东 广州 510006)

摘要: 离散事件系统的故障诊断能将已发生的不可观故障事件及时诊断出来, 但往往容易忽略故障诊断期间系统的安全性. 为解决这一问题, 提出了一种具有多项式时间复杂性的安全故障诊断方法. 先对离散事件系统的安全可诊断性进行了形式化, 再通过构造一个非法语言识别器对系统被禁止操作序列进行识别, 并在此基础上构建了一个对系统实施安全诊断的安全验证器, 得到了一个关于离散事件系统安全可诊断性的充分必要条件, 实现了对系统的安全故障诊断. 同时, 通过对安全验证器的构建与安全可诊断性的判定的复杂性分析, 得到了该安全故障诊断方法可在多项式时间内实现等结论.

关键词: 离散事件系统; 故障诊断; 安全诊断; 多项式时间复杂性

中图分类号: TP13 **文献标识码**: A

Polynomial-time verification of safe diagnosability of discrete-event systems

LIU Fu-chun†, LUO Ping

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

Abstract: Fault diagnosis of discrete event systems (DESs) is to detect the unobservable fault events occurring in systems within a finite delay, but the safety of the involved systems during the detection delay is always neglected. In order to solve this problem, this paper aims to propose an approach for safe diagnosability of DESs with a polynomial-time complexity. Firstly, the notion of safe diagnosability of DESs is formalized. Then the recognizer of illegal language is constructed to identify the sequences of the forbidden operations. Based on the recognizer, the safe verifier is constructed to perform the safe diagnosis for a given system. Furthermore, a necessary and sufficient condition of safe diagnosability of DESs is presented. It is worth noting that the safe diagnosability of DESs can be realized with a polynomial complexity by analyzing the complexity of constructing the verifier and the complexity of checking of the safe diagnosability of DESs.

Key words: discrete event systems; fault diagnosis; safe diagnosability; polynomial-time complexity

1 引言(Introduction)

近年来, 离散事件系统的故障诊断研究引起了国内外许多学者的广泛关注. 尽管目前关于系统故障检测的方法有很多, 包括基于数学模型的定量分析方法和专家系统等人工智能方法, 但由 Sampath 等人在文[1]中提出基于诊断器方法是离散事件系统故障诊断研究中最为广泛使用的方法[2]. 文[3]针对概率自动机系统模型, 在Sampath等人的基于诊断器方法基础上提出了一种随机离散事件系统的故障诊断方法. Qiu和Kumar将这种方法由集中式系统推广至分布式系统, 提出了一种分布式离散事件系统故障诊断方法[4]. 张仁远和甘永梅等人则对离散事件系统拟同余关系算法进行了改进[5]. 本文作者也对离散事件系统的故障诊断问题进行了研究, 分别对随机离散事件系统和模糊离散事件系统提出了一种分散诊断方法[6]和一种模糊诊断方法[7]. 同时, 对于离散事件系统的监控理论还提出了一种非确定型系统的双模拟控制实现方法[8].

尽管运用上述各种故障诊断方法, 能确保系统在故障发生之后的有限时延内将所发生的故障事件诊

收稿日期: 2016−08−16; 录用日期: 2017−02−21.

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

本文责任编委: 张化光.

国家自然科学基金项目(61673122, 61273118), 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资助(2016PY01).

Supported by National Natural Science Foundation of China (61673122, 61273118), Provincial Major Program of Guangdong (2014KZDXM033), Public Welfare Research and Capacity Building Project of Guangdong (2015A030402006) and Major Awards Incubation Project of School of Computers of Guangdong University of Technology (2016PY01).

断出来, 但是在故障被诊断出来之前的那段时延期间, 系统仍然可能会执行某些被禁止的非法操作, 这对于已处于故障运行模式的“病态”系统来说是极其危险的. 针对离散事件系统故障诊断的安全性, Paoli 和 Lafortune提出了一种安全故障诊断机制[9]. 本文作者也分别对随机离散事件系统和模糊离散事件系统提出了一种相应的安全故障诊断方法[10–11]. 特别是在文[11–12]中, 针对糊离散事件系统基于诊断器的故障诊断方法为指数时间复杂度的问题, 分别提出了一种具有多项式时间复杂性的模糊故障诊断方法和安全故障诊断方法, 将Yoo和Lafortune提出的双模型故障诊断算法[13]推广至模糊离散事件系统.

针对以有限状态自动机为模型的离散事件系统故障诊断的安全性问题, 本文提出一种具有多项式时间复杂性的安全故障诊断方法. 先对这种离散事件系统的安全可诊断性进行形式化, 再通过构造一个非法语言识别器对系统被禁止操作进行识别, 并在非法语言识别器的基础上构建一个安全验证器, 从而得到一个判定离散事件系统安全可诊断性的充分必要条件, 实现对系统的安全诊断. 这种安全故障诊断方法既能保证所有故障一旦发生之后能及时被诊断出来, 又能确保在故障诊断期间系统不会执行任何被禁止的危险操作. 通过分析安全验证器的构建的复杂性与安全可诊断性的判定的复杂性, 将得到该安全故障诊断方法可在多项式时间内实现等结论. 这不仅改进了文[9]中提出的具有指数时间复杂性的安全故障诊断方法, 而且也弥补了文[11–12]中提出的具有多项式时间复杂性的故障诊断方法仅限于模糊系统的局限性.

2 离散事件系统(Discrete event systems)

一个离散事件系统是指有限状态自动机[1]: $G=(X,\Sigma,\delta_{\rm G},x_0)$, 其中: X为有限状态集, Σ 为事件集, $x_0\in X$为初始状态, $\delta_{\rm G}$为状态转移函数$\delta_{\rm G}: X\times\Sigma\to X$.

事件集Σ可划分为可观事件集$\Sigma_{\rm o}$和不可观事件集$\Sigma_{\rm uo}$, 即$\Sigma=\Sigma_{\rm o}\cup\Sigma_{\rm uo}$. 记故障事件集为$\Sigma_{\rm f}$, 类似文[1]中假设$\Sigma_{\rm f}\subseteq\Sigma_{\rm uo}$, 表示故障事件均为不可观事件, 并根据故障事件对系统的不同影响, 将故障事件集划分为不同类型$\Sigma_{\rm f}=\Sigma_{\rm f1}\cup\Sigma_{\rm f2}\cup\cdots\cup\Sigma_{{\rm f}m}$, 其中: m为故障类型数, 事件$\sigma_{\rm f}\in\Sigma_{{\rm f}i}$表示$\sigma_{\rm f}$为第$i$种类型的故障事件.

为方便起见, 引入文[1]中的以下符号: Σ^*为Σ的克林闭包; $\bar{s}$表示事件串s的前缀闭包; L表示G的生成语言, 即$L=\{s\in\Sigma^*:(\exists x\in X)\delta_{\rm G}(x_0,s)=x\}$; $L/s=\{t\in\Sigma^*: st\in L\}$表示由发生在事件串$s$之后的所有事件串组成的$s$的后缀语言; $\Psi(\Sigma_{{\rm f}i})=\{s\in L: s_{\rm f}\in\Sigma_{{\rm f}i}\}$表示以$\Sigma_{{\rm f}i}$中某故障事件结尾的所有事件串集, 其中$s_{\rm f}$表示$s$的末尾事件.

定义 1[1] 投影P是指映射$P:\Sigma^*\to\Sigma_{\rm o}^*$, 它满足$P(\epsilon)=\epsilon$, 且对任意$\sigma\in\Sigma$, 当$\sigma\in\Sigma_{\rm o}$时$P(\sigma)=\sigma$, 当$\sigma\in\Sigma_{\rm uo}$时$P(\sigma)=\epsilon$; 对任意$s\in\Sigma^*$和$\sigma\in\Sigma$, $P(s\sigma)=P(s)P(\sigma)$. P^{-1}表示P的反投射映射: 对于$u\in\Sigma_{\rm o}^*$, $P^{-1}(u)=\{s|s\in L: P(s)=u\}$.

3 离散事件系统安全可诊断性的形式化(Formalization of safe diagnosability of DESs)

根据不同的故障类型, 将被禁止事件串分为相应的不同类型$\Omega=\Omega_1\cup\Omega_2\cup\cdots\cup\Omega_m$, 其中: m为被禁止事件串类型数, Ω_i表示第i种类型的被禁止事件串集.

定义 2 设Ω是离散事件系统G的被禁止事件串集, 将G的非法语言定义为$\zeta=\bigcup\limits_{i=1}^{m}\zeta_i$, 其中$\zeta_i$定义为

$$\zeta_i=\{t\in L/s: s\in\Psi(\Sigma_{{\rm f}i})\wedge(\exists u\in t)u\in\Omega_i\},$$

这里$u\in t$表示u是t中的某子串.

定义 3[9] 设$G=(X,\Sigma,\delta_{\rm G},x_0)$是一个离散事件系统, 如果$G$同时满足以下可诊断条件和安全性条件, 则称$G$为安全可诊断系统:

I) 可诊断条件.

对任意$\Sigma_{{\rm f}i}\in\Sigma_{\rm f}$, 存在$n\in\mathbb{N}^+$, 使得

$$(\forall s\in\Psi(\Sigma_{{\rm f}i}))(\forall t\in L/s)[\|t\|\geqslant n\Rightarrow D_1],$$

其中D_1为$\omega\in P^{-1}(P(st))\Rightarrow\Sigma_{{\rm f}i}\in\omega$.

II) 安全性条件.

对任意$\Sigma_{{\rm f}i}\in\Sigma_{\rm f}$, 都有

$$(\forall s\in\Psi(\Sigma_{{\rm f}i}))(\forall t\in L/s)\bar{t}_c\cap\zeta_i=\varnothing.$$

4 非法语言识别器与安全验证器的构造(Construction of the illegal language recognizer and the safe verifier)

为简单起见, 下面仅考虑一种类型的故障事件和一种类型的被禁止事件的情形(即$m=1$), 对于多种类型的情形可类似考虑.

首先给出非法语言识别器的状态标签集: $\nabla=\{N,F_i-NB,F_i-B_i\}$, 其中: N 表示无故障事件发生; F_i-NB表示发生了故障事件但故障发生后无执行被禁止操作; F_i-B_i表示发生了故障事件并且故障发生后又执行了被禁止操作.

定义 4 设$G=(X,\Sigma,\delta_{\rm G},x_0)$, 将$G$的非法语言识别器构造为如下有限状态自动机:

$$G_{\rm r}=(Q_{\rm r},\Sigma,\delta_{\rm r},(x_0,N)),$$

其中: i) $(x_0,N)\in Q_{\rm r}$为初始状态; ii) $Q_{\rm r}$为状态集, 这里$Q_{\rm r}\subseteq X\times\theta(s)$, 其中$\theta(s)$为定义如下的标识函数:

$$\theta(s)=\begin{cases}N, & \text{如果}\Sigma_{\mathrm{f}i}\notin s,\\ F_i-NB, & \text{如果}\Sigma_{\mathrm{f}i}\in s\text{且}s\notin\zeta_i,\\ F_i-B_i, & \text{如果}\Sigma_{\mathrm{f}i}\in s\text{且}s\in\zeta_i.\end{cases}\quad(1)$$

iii) δ_{r}为状态转移函数δ_{r}: $Q_{\mathrm{r}}\times\Sigma\to Q_{\mathrm{r}}$: 对于$s\in L$, 其转移规则为

1) 当$\Sigma_{\mathrm{f}i}\notin s$时,

$$\begin{cases}\delta_{\mathrm{r}}((x_0,N),s)=(x_0,N),\\ \delta_{\mathrm{r}}((x_0,\theta(s)),s)=(x_0,\theta(s)).\end{cases}$$

2) 当$\Sigma_{\mathrm{f}i}\in s$且$s\notin\zeta$时,

$$\begin{cases}\delta_{\mathrm{r}}((x_0,N),s)=(\delta_{\mathrm{G}}(x_0,s),F_i-NB),\\ \delta_{\mathrm{r}}((x,F_i-NB),s)=(x,F_i-NB).\end{cases}$$

3) 当$\Sigma_{\mathrm{f}i}\in s$且$s\in\zeta$时,

$$\begin{cases}\delta_{\mathrm{r}}((x_0,N),s)=(\delta_{\mathrm{G}}(x_0,s),F_i-B_i),\\ \delta_{\mathrm{r}}((x,F_i-NB),s)=(\delta_{\mathrm{G}}(x,s),F_i-B_i),\\ \delta_{\mathrm{r}}((x,F_i-B_i),s)=(x,F_i-B_i).\end{cases}$$

下面将G的安全验证器构造为有限自动状态机:

$$G_{\mathrm{v}}=(Q_{\mathrm{v}},\Sigma,\delta_{\mathrm{v}},q_0),$$

其中: 初始状态为$q_0=(x_0,N,x_0,N)$, 状态集为$Q_{\mathrm{v}}=X\times\nabla\times X\times\nabla$, 状态转移函数为$\delta_{\mathrm{v}}$: $Q_{\mathrm{v}}\times\Sigma\to Q_{\mathrm{v}}$, 其具体形式见定义5.

定义 5　设Θ_{f}为Ω_i中被禁止事件串的最后一个事件的集合, 即$\Theta_{\mathrm{f}}=\{\sigma\in\Sigma:(\exists t\in\Sigma^*)t\sigma\in\zeta_i\}$. 安全验证器$G_{\mathrm{v}}$的状态转移函数$\delta_{\mathrm{v}}: Q_{\mathrm{v}}\times\Sigma\to 2^{Q_{\mathrm{v}}}$定义如下: 对于$s=t\sigma\in\Sigma^*$且$\delta_{\mathrm{v}}((x_0,N,x_0,N),t)=(\delta_{\mathrm{G}}(x_0,t),l_1,\delta_{\mathrm{G}}(x_0,t),l_2)$,

1) 如果$\Sigma_{\mathrm{f}i}\notin t$, 则

① 当$\sigma\in\Sigma_{\mathrm{o}}$时,

$$\delta_{\mathrm{v}}((x_1,l_1,x_2,l_2),\sigma)=(\delta_{\mathrm{G}}(x_1,\sigma),l_1,\delta_{\mathrm{G}}(x_2,\sigma),l_2).$$

② 当$\sigma\in\Sigma_{\mathrm{uo}}-\Sigma_{\mathrm{f}i}$时,

$$\delta_{\mathrm{v}}((x_1,l_1,x_2,l_2),\sigma)=\begin{cases}(\delta_{\mathrm{G}}(x_1,\sigma),l_1,x_2,l_2),\\ (x_1,l_1,\delta_{\mathrm{G}}(x_2,\sigma),l_2),\\ (\delta_{\mathrm{G}}(x_1,\sigma),l_1,\delta_{\mathrm{G}}(x_2,\sigma),l_2).\end{cases}$$

③ 当$\sigma\in\Sigma_{\mathrm{f}i}$时,

$$\delta_{\mathrm{v}}((x_1,l_1,x_2,l_2),\sigma)=\begin{cases}(\delta_{\mathrm{G}}(x_1,\sigma),F_i-NB,x_2,l_2),\\ (x_1,l_1,\delta_{\mathrm{G}}(x_2,\sigma),F_i-NB),\\ (\delta_{\mathrm{G}}(x_1,\sigma),F_i-NB,\\ \delta_{\mathrm{G}}(x_2,\sigma),F_i-NB).\end{cases}$$

2) 如果$\Sigma_{\mathrm{f}i}\in t,\ s\in\zeta_i,\ \sigma\in\Theta_{\mathrm{f}}$, 则

① 当$\sigma\in\Sigma_{\mathrm{o}}$时,

$$\delta_{\mathrm{v}}((x_1,l_1,x_2,l_2),\sigma)=(\delta_{\mathrm{G}}(x_1,\sigma),F_i-B_i,\delta_{\mathrm{G}}(x_2,\sigma),F_i-B_i).$$

② 当$\sigma\in\Sigma_{\mathrm{uo}}$时,

$$\delta_{\mathrm{v}}((x_1,l_1,x_2,l_2),\sigma)=\begin{cases}(\delta_{\mathrm{G}}(x_1,\sigma),F_i-B_i,x_2,l_2),\\ (x_1,l_1,\delta_{\mathrm{G}}(x_2,\sigma),F_i-B_i),\\ (\delta_{\mathrm{G}}(x_1,\sigma),F_i-B_i,\\ \delta_{\mathrm{G}}(x_2,\sigma),F_i-B_i).\end{cases}$$

3) 如果$\Sigma_{\mathrm{f}i}\in t,\ s\in\zeta_i,\ \sigma\notin\Theta_{\mathrm{f}}$, 则

① 当$\sigma\in\Sigma_{\mathrm{o}}$时,

$$\delta_{\mathrm{v}}((x_1,l_1,x_2,l_2),\sigma)=(\delta_{\mathrm{G}}(x_1,\sigma),l_1,\delta_{\mathrm{G}}(x_2,\sigma),l_2).$$

② 当$\sigma\in\Sigma_{\mathrm{uo}}$时,

$$\delta_{\mathrm{v}}((x_1,l_1,x_2,l_2),\sigma)=\begin{cases}(\delta_{\mathrm{G}}(x_1,\sigma),l_1,x_2,l_2),\\ (x_1,l_1,\delta_{\mathrm{G}}(x_2,\sigma),l_2),\\ (\delta_{\mathrm{G}}(x_1,\sigma),l_1,\delta_{\mathrm{G}}(x_2,\sigma),l_2).\end{cases}$$

4) 如果$\Sigma_{\mathrm{f}i}\in t,\ s\notin\zeta_i$,则

① 当$\sigma\in\Sigma_{\mathrm{o}}$时,

$$\delta_{\mathrm{v}}((x_1,l_1,x_2,l_2),\sigma)=(\delta_{\mathrm{G}}(x_1,\sigma),l_1,\delta_{\mathrm{G}}(x_2,\sigma),l_2).$$

② 当$\sigma\in\Sigma_{\mathrm{uo}}$时,

$$\delta_{\mathrm{v}}((x_1,l_1,x_2,l_2),\sigma)=\begin{cases}(\delta_{\mathrm{G}}(x_1,\sigma),l_1,x_2,l_2),\\ (x_1,l_1,\delta_{\mathrm{G}}(x_2,\sigma),l_2),\\ (\delta_{\mathrm{G}}(x_1,\sigma),l_1,\delta_{\mathrm{G}}(x_2,\sigma),l_2).\end{cases}$$

5　安全可诊断性的充分必要条件 (Necessary and sufficient condition of safe diagnosability)

如果在安全验证器G_{v}中状态序列$q_1,q_2,\cdots,q_n$和事件序列$e_1,e_2,\cdots,e_n$满足

$$[(\forall k\leqslant n-1)(\delta_{\mathrm{v}}(q_k,e_k)=q_{k+1}]\wedge(\delta_{\mathrm{v}}(q_n,e_n)=q_1),$$

则称这个状态序列为G_{v}中的一个状态环, 记为$C=<q_1,q_2,\cdots,q_n>$.

如果状态序列$q_1,q_2,\cdots,q_n$和事件序列$e_1,e_2,\cdots,e_n$满足:

1) $(\forall k\leqslant n)[q_k=(x_1^k,N,x_2^k,F_i-NB)\vee q_k=(x_1^k,N,x_2^k,F_i-B_i)\vee q_k=(x_1^k,F_i-NB,x_2^k,N)\vee q_k=(x_1^k,F_i-B_i,x_2^k,N)]$.

2) $[(\forall k\leqslant n-1)(\delta_{\mathrm{v}}(q_k,e_k)=q_{k+1})]\wedge(\delta_{\mathrm{v}}(q_n,e_n)=q_1)$, 则称这个状态序列$q_1,q_2,\cdots,q_n$为$G_{\mathrm{v}}$中的一个故障冲突状态环, 记为$FC=<q_1,q_2,\cdots,q_n>$.

定理 1　设$G=(X,\Sigma,\delta_{\mathrm{G}},x_0)$是一个离散事件系统, $G_{\mathrm{v}}=(Q_{\mathrm{v}},\Sigma,\delta_{\mathrm{v}},q_0)$是$G$的安全验证器, 则$G$为安全可诊断的充分必要条件是: 1) G的安全验证器G_{v}中不存在故障冲突环, 且2) G_{v}中不存在形如$q_k=(x_1^k,F_i-B_i,x_2^k,N)$或$q_k=(x_1^k,N,x_2^k,F_i-B_i)$的不确定状态.

证 下面先用反证法证明必要性. 设G是一个安全可诊断系统.

1) 如果安全验证器$G_{\rm v}$中存在一个故障冲突环$FC =< q_1, q_2, \cdots, q_n >$, 其中$q_k = (x_1^k, N, x_2^k, F_i - NB)$, $k \in \{1, 2, \cdots, n\}$, 则根据$G_{\rm v}$的构造可知, G中一定存在两条轨迹$u, v \in L$, 使得$P(u) = P(v)$, $x_1^1 = \delta_{\rm G}(x_0, u)$, $x_2^1 = \delta_G(x_0, v)$, $\Sigma_{{\rm f}i} \notin u$, $\Sigma_{{\rm f}i} \in v$. 从而在G中必然存在两条投影相同的路径g_1和g_2使得$P(g_1) = P(g_2)$, 且$\Sigma_{{\rm f}i} \notin g_1$, $\Sigma_{{\rm f}i} \in g_2$, 这与已知$G$是安全可诊断系统相矛盾.

2) 如果$G_{\rm v}$中存在形如$q_i = (x_1^i, F_i - B_i, x_2^i, N)$或$q_i = (x_1^i, N, x_2^i, F_i - B_i)$的不确定状态. 不妨设$q_i = (x_1^i, F_i - B_i, x_2^i, N)$, 必然在$G_{\rm v}$中存在相应的$s \in \Sigma^*$使得$q_i = \delta_{\rm v}(q_0, s)$, 且在$G$中必然存在两条投影相同的路径$g_1$和$g_2$使得$P(g_1) = P(g_2) = P(s)$, 且$\Sigma_{{\rm f}i} \notin g_1, \Sigma_{{\rm f}i} \in g_2$, 这与已知$G$是安全可诊断系统相矛盾.

下面再用反证法证明充分性. 设安全验证器$G_{\rm v}$中不存在故障冲突环, 也不存在形如$q_k = (x_1^k, F_i - B_i, x_2^k, N)$或$q_k = (x_1^k, N, x_2^k, F_i - B_i)$的不确定状态. 假设系统$G$不是安全可诊断的, 则$(\exists u_1 \in \Psi(\Sigma_{{\rm f}i}))(\forall t \in L/u_1)[\|t_1\| > n \wedge (t_1 \cap \Omega_i \neq \varnothing)]$. 因此, 在$G$中存在$s = u_2 t_2 \in \Sigma^*$满足$\Sigma_{{\rm f}i} \notin u_2$, $P(u_1) = P(u_2)$, $P(t_1) = P(t_2)$. 从而在$G_{\rm v}$中存在相应的$d \in \Sigma^*$, 使得$P(d) = P(u_1 t_1) = P(u_2 t_2)$. 根据安全验证器的转移规则可知, 在$G_{\rm v}$中必然存在某个状态形如$q_i = (x_1^i, F_i - B_i, x_2^i, N)$或$q_i = (x_1^i, N, x_2^i, F_i - B_i)$, 这与已知条件$G_{\rm v}$中不存在这种形式的不确定状态相矛盾.

下面给出两个例子阐述上述安全诊断方法与结论.

例 1 考虑图1中的系统G, 其中: $\Omega_i = \{\sigma_s\}$, $\Sigma_{{\rm f}i} = \Sigma_{\rm f} = \{\sigma_{\rm f}\}$, $\Sigma_{\rm o} = \{\alpha, \gamma, \beta, \tau\}$. 下面通过构造安全验证器的方法证明$G$为安全可诊断系统.

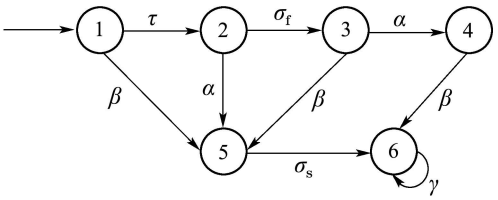

图 1 离散事件系统G

Fig. 1 Discrete event system G

根据定义4和定义5, 分别构造非法语言识别器$G_{\rm r}$和安全验证器$G_{\rm v}$, 如图2–3所示.

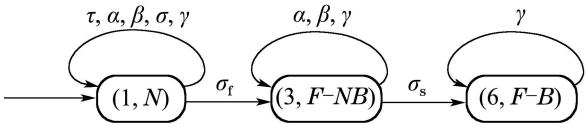

图 2 非法语言识别器$G_{\rm r}$

Fig. 2 Recognizer of illegal language $G_{\rm r}$

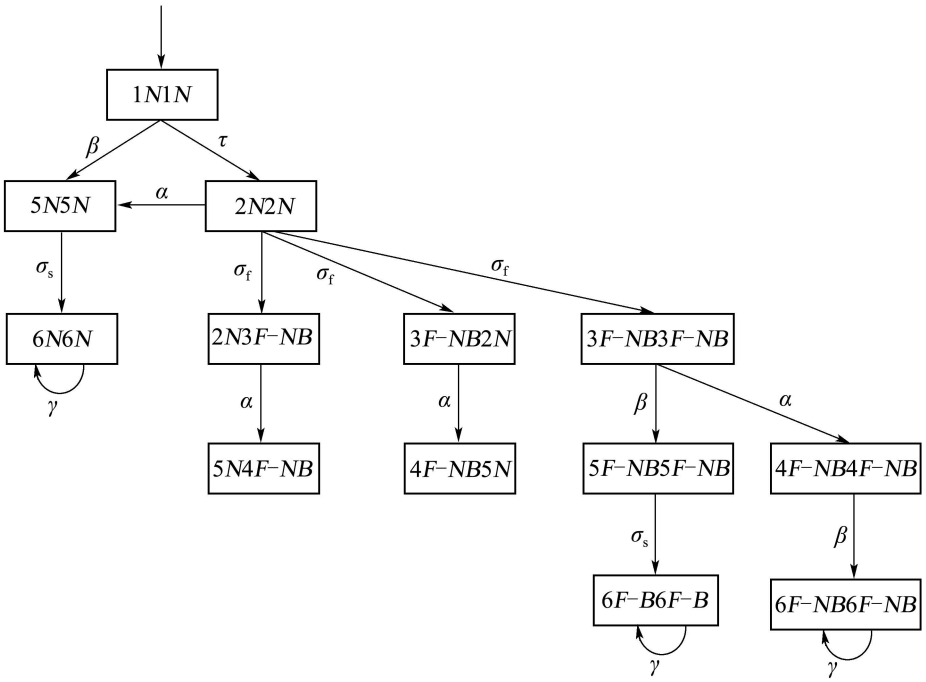

图 3 安全验证器$G_{\rm v}$

Fig. 3 Safe verifier $G_{\rm v}$

由于在$G_{\rm v}$中既不存在故障冲突环也不存在形如$q_k = (x_1^k, F - B, x_2^k, N)$或$q_k = (x_1^k, N, x_2^k, F - B)$的不确定状态, 根据定理1可知, 系统$G$为安全可诊断系统.

例 2 考虑图4中的系统G, 其中: $\Omega_i = \{\sigma_s\}$, $\Sigma_{{\rm f}i} = \Sigma_{\rm f} = \{\sigma_{\rm f}\}$, $\Sigma_{\rm o} = \{\alpha, \gamma, \beta, \tau\}$. 下面通过构造

安全验证器的方法证明G不是安全可诊断系统.

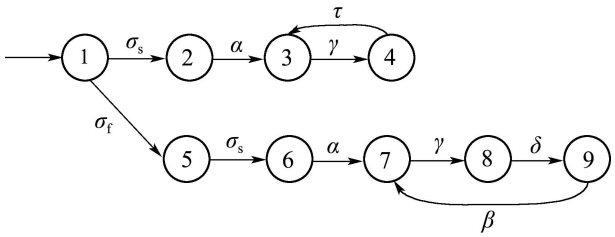

图 4　离散事件系统G

Fig. 4　Discrete event system G

根据定义4和定义5, 分别构造非法语言识别器G_r和安全验证器G_v, 如图5–6所示.

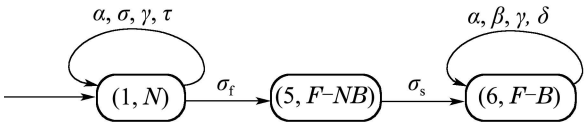

图 5　识别器G_r

Fig. 5　Verifier G_r

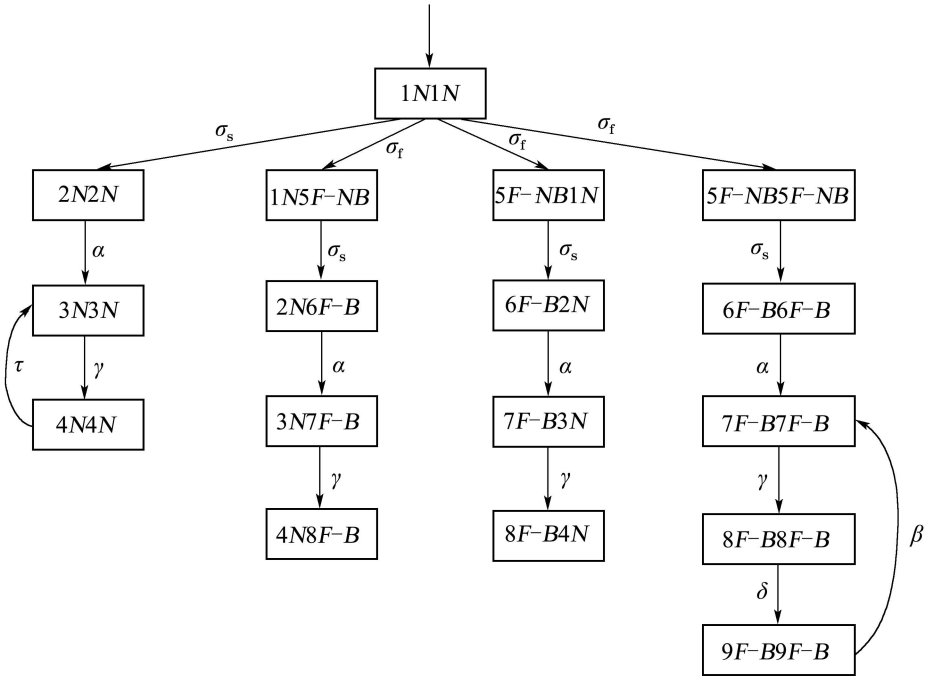

图 6　安全验证器G_v

Fig. 6　Verifier G_r

从图6可知, 尽管G_{v2}中不存在故障冲突环, 但是存在不确定状态, 如$(2, N, 6, F-B)$和$(7, F-B, 3, N)$. 根据定理1得, 系统G不是安全可诊断系统.

6　离散事件系统安全诊断的复杂性分析 (Complexity analysis of safe diagnosability of DESs)

根据定理1可知, 上述安全诊断方法的复杂性主要在于两个方面: 一是构造安全验证器G_v的复杂性, 二是根据G_v判断G是否为安全可诊断的复杂性.

定理 2　设$G=(X, \Sigma, \delta_G, x_0)$是一个离散事件系统, 其中: $\|X\|=n_1$, $\|\Sigma\|=n_2$. 对给定的故障事件集Σ_{fi}和相应的被禁止事件串集Ω_i, 构造G的安全验证器G_v的复杂度为$O(n_1^2 n_2)$.

证　根据定义5可知, 安全验证器G_v的每一个状态转移次数最多为$3n_2$, 而它的所有可达状态数最多为$9n_1^2$. 因此, 构造该安全验证器G_v所需次数最多为$27n_1^2 n_2$, 即构造G_v的复杂度为$O(n_1^2 n_2)$.

定义 6　安全验证器$G_v=(Q_v, \Sigma, \delta_v, q_0)$的定向图是指$DG_v=(V_{DG}, E_{DG})$, 其中顶点集$V_{DG}$和边集$E_{DG}$分别定义如下:

$$V_{DG}=\{(x_1, l_1, x_2, l_2)\in Q_v : l_1 \neq l_2\},$$

$$E_{DG}=\{(u, v) : u, v\in Q_v, (\exists \sigma\in\Sigma)\delta_v(u, \sigma)=v\}.$$

根据定理1, 可以用G_v的定向图DG_v描述G的安全可诊断性, 于是得到如下结论:

定理 3　给定一个离散事件系统G, 如果G_v的定向图DG_v不存在环且不包含F_i-B_i标签的顶点, 则G为安全可诊断系统.

证　根据定义6及定理1易得.

引理 1[14]　设$DG_v=(V_{DG}, E_{DG})$是一个定向图, 关于DG_v中是否存在环的判定复杂性为$O(\|V_{DG}\|+\|E_{DG}\|)$.

定理 4 设$G_{\rm v}=(Q_{\rm v},\Sigma,\delta_{\rm v},q_0)$是离散事件系统$G$的安全验证器, 判定$G_{\rm v}$中是否存在故障冲突环和不确定状态的复杂性为$\mathrm{O}(n_1^4n_2)$.

证 因为$G_{\rm v}$的状态集为$Q_{\rm v}=X\times\nabla\times X\times\nabla$, 所以$G_{\rm v}$的所有可达状态数最多为$9n_1^2$, 即$\|V_{\rm DG}\|\leqslant 9n_1^2$, 从而判定$G_{\rm v}$中是否存在不确定状态的复杂性为$\mathrm{O}(n_1^2)$. 根据定义6, 有$\|E_{\rm DG}\|\leqslant 81n_1^4n_2$. 因此, 根据引理1得, 判定$G_{\rm v}$中是否存在故障冲突环的复杂性为$\mathrm{O}(\|V_{\rm DG}\|+\|E_{\rm DG}\|)\leqslant\mathrm{O}(n_1^4n_2)$, 从而判定$G_{\rm v}$中是否存在故障冲突环和不确定状态的复杂性为$\mathrm{O}(n_1^4n_2)$.

定理 5 设$G=(X,\Sigma,\delta_{\rm G},x_0)$是一个离散事件系统, 其中: $\|X\|=n_1$, $\|\Sigma\|=n_2$. 判定G是否为安全可诊断的复杂性为$\mathrm{O}(n_1^4n_2)$.

证 根据定理1可知, 判定G是否为安全可诊断的复杂性主要在于构造安全验证器$G_{\rm v}$的复杂性和根据$G_{\rm v}$判断G是否为安全可诊断的复杂性. 定理2已经证明了构造$G_{\rm v}$的复杂度为$\mathrm{O}(n_1^2n_2)$, 而定理4已经证明了根据$G_{\rm v}$判定$G_{\rm v}$中是否存在故障冲突环和不确定状态的复杂性为$\mathrm{O}(n_1^4n_2)$. 因此, 判定G是否为安全可诊断的整体复杂性为$\mathrm{O}(n_1^4n_2)$.

7 小结(Conclusions)

本文提出了一种具有多项式时间复杂性的离散事件系统安全诊断方法, 不仅能将发生的所有故障及时诊断出来, 又能确保系统在故障诊断期间不执行任何不安全操作. 在此基础上，我们可进一步考虑以非确定离散事件系统[8]及以随机离散事件系统[10]为模型的安全诊断及其算法优化等问题, 这些问题将在后续研究中深入探讨.

参考文献(References):

[1] SAMPATH M, SENGUPTA R, LAFORTUNE S, et al. Diagnosability of discrete-event systems [J]. *IEEE Transactions on Automatic Control*, 1995, 40(9): 1555 – 1575.

[2] ZAYTOON J, LAFORTUNE S. Overview of fault diagnosis methods for discrete event systems [J]. *Annual Reviews in Control*, 2013, 37(2): 308 – 320.

[3] THORSLEY D, TENENKETZIS D. Diagnosability of stochastic discrete-event systems [J]. *IEEE Transactions on Automatic Control*, 2005, 50(4): 476 – 492.

[4] QIU W, R KUMAR. Decentralized failure diagnosis of discrete event systems [J]. *IEEE Transaction on Systems, Man, and Cybernetics-part A: Systems and Humans*, 2006, 36(2): 384 – 395.

[5] ZHANG Renyuan, GAN Yongmei, CHAO Wujie, et al. Improved algorithm of quasi-congruence in discrete-event system [J]. *Control Theory & Applications*, 2012, 29(2): 151 – 156.
(张仁远, 甘永梅, 晁武杰, 等. 离散事件系统拟同余关系的改进算法 [J]. 控制理论与应用, 2012, 29(2): 151 – 156.)

[6] LIU F C, QIU D W, XING H Y, et al. Decentralized diagnosis of stochastic discrete event systems [J]. *IEEE Transactions on Automatic Control*, 2008, 53(2): 535 – 546.

[7] LIU F C, QIU D W. Diagnosability of fuzzy discrete-event systems: a fuzzy approach [J]. *IEEE Transaction on Fuzzy Systems*, 2009, 17(2): 1063 – 6706.

[8] LIU Fuchun. Realization of bisimilarity control of nondeterministic discrete event systems [J]. *Control Theory & Applications*, 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 [J]. 控制理论与应用, 2015, 32(1): 75 – 79.)

[9] PAOLI A, LAFORTUNE S. Safe diagnosability for fault-tolerant supervision of discrete-event systems [J]. *IEEE Transactions on Automatic Control*, 2005, 41(8): 1335 – 1347.

[10] LIU F C, QIU D W. Safe diagnosability of stochastic discrete event systems [J]. *IEEE Transactions on Automatic Control*, 2008, 53(5): 1291 – 1296.

[11] LIU F C. Safe diagnosability of fuzzy discrete-event systems and a polynomial-time verification [J]. *IEEE Transactions on Fuzzy Systems*, 2015, 23(5): 1534 – 1544.

[12] LIU F C. Polynomial-time verification of diagnosability of fuzzy discrete event systems [J]. *Science China (Information Sciences)*, 2014, 57(6): 1 – 10.

[13] CORMEN T H, LEISERSON C E, RIVEST R L. *Introduction to Algorithms* [M]. Cambridge, MA: MIT Press, 1990.

[14] YOO T, LAFORTUNE S. Polynomial-time verification of diagnosability of partially observed discrete-event systems [J]. *IEEE Transactions on Automatic Control*, 2002, 47(9): 1491 – 1495.

作者简介:

刘富春 (1971–), 男, 教授, 博士生导师, 入选广东省高校“千百十人才工程”第二层次(省级), 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;

罗 苹 (1990–), 女, 硕士研究生, 目前研究方向为算法分析与设计、离散事件系统故障检测理论与应用, E-mail: 540548571@qq.com.