离散事件系统基于模式的安全故障诊断

刘富春[1†], 唐顺桥[1], 赵 锐[1], 邓秀勤[2], 崔洪刚[1,3]

(1. 广东工业大学 计算机学院, 广东 广州 510006; 2. 广东工业大学 应用数学学院, 广东 广州 510006;
3. 广东省东源县科技创新中心, 广东 河源 517500)

摘要: 基于模式的故障诊断方法能将触发系统故障的事件串诊断出来, 但在诊断期间系统仍然可能执行被禁止的不安全操作. 为此, 提出了一种离散事件系统基于S型和T型模式的安全诊断方法. 先对离散事件系统基于模式的安全可诊断性进行形式化, 再通过构造非法语言识别器和安全诊断器对系统发生的故障模式实施安全诊断, 最后分别得到了一个关于S型和T型模式的系统安全可诊断性的充分必要条件, 实现了离散事件系统基于模式的安全故障诊断.

关键词: 离散事件系统; 故障诊断; 故障模式; 安全诊断

引用格式: 刘富春, 唐顺桥, 赵锐, 等. 离散事件系统基于模式的安全故障诊断. 控制理论与应用, 2020, 37(1): 162 – 168

DOI: 10.7641/CTA.2019.80644

Safe pattern-based diagnosability of discrete-event systems

LIU Fu-chun[1†], TANG Shun-qiao[1], ZHAO Rui[1], DENG Xiu-qin[2], CUI Hong-gang[1,3]

(1. School of Computers, Guangdong University of Technology, Guangzhou Guangdong 510006, China;
2. School of Applied Mathematics, Guangdong University of Technology, Guangzhou Guangdong 510006, China;
3. Science and Technology Innovation Center of Dongyuan, Heyuan Guangdong 517500, China)

Abstract: The pattern-based diagnosis can detect the fault patterns that cause system failure, but the system may still perform the prohibited unsafe operations during diagnosis. In this paper, an approach for safe diagnosability of discrete-event systems (DESs) based on S–type and T–type of fault patterns is proposed. The notion of safe pattern-based diagnosability of DESs is formalized, then the recognizer of illegal language and the safe diagnoser are constructed to implement safe diagnosis for fault patterns of systems. Finally, the necessary and sufficient conditions of safe pattern-based diagnosability are proposed for S–type and T–type patterns, respectively, which results to the achievement of safe pattern-based diagnosis of systems.

Key words: discrete-event systems; fault diagnosis; fault patterns; safe diagnosability

Citation: LIU Fuchun, TANG Shunqiao, ZHAO Rui, et al. Safe pattern-based diagnosability of discrete-event systems. *Control Theory & Applications*, 2020, 37(1): 162 – 168

1 引言

近年来，离散事件系统的故障诊断研究引起了国内外众多学者的高度关注. 自Sampath等人在文献[1]中提出基于诊断器的故障诊断方法以来, 这种方法就被广泛使用. Zad等人[2]提出了一种基于状态的故障诊断机制. Moreira等人[3]将文献[1]的诊断算法进行优化, 提出了一种具有多项式时间复杂度的故障诊断方法. 文献[4]针对随机系统提出了一种随机离散事件系统的故障诊断方法. 笔者在文献[5]中提出了一种适用于处理不精确和不确定特性的模糊离散事件系统的模糊故障诊断方法. 吉林大学欧阳丹彤教授等人在文献[6]中深入研究了不完备离散事件系统的故障诊断等问题.

然而, 上述文献中的故障诊断方法都是将引起故障的操作视为一个事件(即故障事件). 近年来, 针对由多个事件组成的故障(称为故障模式), 也引起了许多学者的关注. 例如, Sahika等人在文献[7]中提出了基于模式的故障诊断方法, 将Sampath等人提出基于诊

收稿日期: 2018−08−28; 录用日期: 2019−04−02.
†通信作者. E-mail: fliu2011@163.com; Tel.: +86 13725145446.
本文责任编委: 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) and the Major Awards Incubation Project of School of Computers of Guangdong University of Technology (2016PY01).

断器的故障诊断方法[1]推广至对故障模式的诊断; 文献[8]对离散事件系统基于模式的故障诊断方法提出了一种语义分析方法, 对文献[7]中的模式诊断方法进行了改进; 文献[9]对离散事件系统中的模式语句进行了预测.

虽然运用上述不同的故障诊断方法都可以在故障发生后的一定时延内将所发生的故障诊断出来, 但在故障在发生后系统仍然可能会执行一些被禁止的非法操作, 为此, Paoli等人[10]在文献[1]的基础上对故障诊断提出了安全性要求, 得到了一种安全故障诊断方法; 随后, Deng等人[11]也提出了基于状态诊断的离散事件系统的安全诊断方法. 文献[12]对文献[10]中的方法进行了改进, 提出了一种具有多项式时间复杂度的安全诊断方法.

本文继续文献[7, 10]的工作, 针对离散事件系统基于模式的故障诊断的安全性问题, 提出一种基于模式的安全故障诊断方法. 先根据目前最常用的S型和T型两种模式, 引入S型和T型模式的可诊断条件和安全性条件, 对离散事件系统基于模式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非法操作进行识别. 然后在非法语言识别器的基础上, 构建相应的安全诊断器, 对系统发生的故障模式实施安全诊断. 最后, 分别得到一个关于S型和T型模式的系统安全可诊断性的充分必要条件. 该方法不仅能将触发系统的故障模式诊断出来, 还保证了系统在诊断期间不会执行任何被禁止的不安全操作.

2　离散事件系统

一个离散事件系统是指有限状态自动机[7]

$$G=(X,\Sigma,\delta,x_0,F),$$

其中: X为有限状态集合; Σ为事件集; $x_0\in X$为系统初始状态; δ为状态转移函数, $\delta: X\times\Sigma\to 2^X$; $F\subseteq X$为标记状态集; 事件集Σ可分为可观察事件集$\Sigma_{\rm o}$和不可观察事件集$\Sigma_{\rm uo}$, 即$\Sigma=\Sigma_{\rm o}\cup\Sigma_{\rm uo}$.

为方便起见, 引入以下符号: $\bar{s}$表示事件串s的前缀闭包; L为G所生成的语言, $L=\{s\in\Sigma^*|(\exists x\in X)\delta(x_0,s)=x\}$; 对于集合$A$, B, 用符号$A\backslash x$表示将元素x从集合A中除去, $A\backslash B$表示集合A中除去集合B中的元素. 投影$P:\Sigma^*\to\Sigma_{\rm o}^*$为一个满足如下规则的映射: 对任意的$\sigma\in\Sigma$, 如果$\sigma\in\Sigma_{\rm o}$, 则$P(\sigma)=\sigma$; 如果$\sigma\in\Sigma_{\rm uo}$, 则$P(\sigma)=\varepsilon$; 且$P(\varepsilon)=\varepsilon$, $P(s\sigma)=P(s)P(\sigma)$.

定义 1　给定两个事件串t和u, 如果$u=stv$, 则称t为u的子串, 记为$t\Xi u$; 如果删除事件串u中零个或多个事件(可连续也可不连续)后得到事件串t, 则称t为u的子序列, 记为$t\Upsilon u$. 给定一个事件串集K, 定义集合S为将K中事件串作为子序列的事件串集合, 即$S=\{s\in L|(\exists u\in K)(u\Upsilon s)\}$; 定义集合$T$为将$K$中的事件串作为子串的事件串集合, 即$T=\{s\in L|(\exists u\in K)(u\Xi s)\}$.

记

$$\Psi_{\rm S}(K)=\{s\sigma\in S|(\exists u\sigma\in K)(u\sigma\Upsilon s\sigma)\},$$

它表示S中所有以K中元素结尾的事件串集; 记集合$\Psi_{\rm T}(K)$为T中所有以K中元素结尾的事件串集, 即

$$\Psi_{\rm T}(K)=\{s\sigma\in T|(\exists u\sigma\in K)(u\sigma\Xi s\sigma)\}.$$

3　安全可诊断的形式化

基于模式的安全可诊断的目的是将系统中引发故障的故障模式及时诊断出来, 并要求在诊断期间不能执行被禁止操作.

定义 2　设Ω为离散事件系统G的被禁止事件串集, G的S型非法语言定义为

$$\zeta_{\rm fS}=\{u\in L/s|[s\in\Psi_{\rm S}(K)](\exists v\in\Omega)(v\in u)\};$$

G的T型非法语言定义为

$$\zeta_{\rm fT}=\{u\in L/s|[s\in\Psi_{\rm T}(K)](\exists v\in\Omega)(v\in u)\}.$$

定义 3　如果离散事件系统G同时满足以下条件, 则称G为基于S型模式的安全可诊断系统:

i) S型模式可诊断条件:

$$(\exists n\in\mathbb{N})(\forall s\in\Psi_{\rm S}(K))(\forall t\in L/s)(\|t\|\geqslant n\Rightarrow D_{\rm S}),$$

其中条件$D_{\rm S}$为$P^{-1}P(st)\cap L\subseteq S$.

ii) S型模式安全性条件:

$$(\forall s\in\Psi_{\rm S}(K))(\forall t\in L/s)(\exists t_{\rm c}\in\Sigma^*)(\bar{t}_{\rm c}\cap\zeta_{\rm fS}=\varnothing),$$

其中$t_{\rm c}$为满足i)中条件$D_{\rm S}$中t的最短事件串.

定义 4　如果离散事件系统G同时满足以下条件, 则称G为基于T型模式的安全可诊断系统:

i) T型模式可诊断条件:

$$(\exists n\in\mathbb{N})(\forall s\in\Psi_{\rm T}(K))(\forall t\in L/s)(\|t\|\geqslant n\Rightarrow D_{\rm T}),$$

其中条件$D_{\rm T}$为$P^{-1}P(st)\cap L\subseteq T$.

ii) T型模式安全性条件:

$$(\forall s\in\Psi_{\rm T}(K))(\forall t\in L/s)(\exists t_{\rm c}\in\Sigma^*)(\bar{t}_{\rm c}\cap\zeta_{\rm fT}=\varnothing),$$

其中$t_{\rm c}$为满足i)中条件$D_{\rm T}$中t的最短事件串.

4　基于S型模式的安全故障诊断

先引入一种标记自动机及其并行器.

定义 5　设G为一个基于S型模式诊断的离散事件系统, $s=\sigma_1\sigma_2\sigma_3\cdots\sigma_m$为一个触发S型模式故障的子序列, 则$G$的标记自动机构造为有限状态自动机$H_{\rm S}(s)=(Q_{\rm S},\Sigma,\delta_{\rm S},q_0^{\rm S},F_{\rm S})$, 其中$Q_{\rm S}=\{0,1,2,\cdots,||s||\}$为状态集, $\delta_{\rm S}$为转移函数$\delta_{\rm S}:Q_{\rm S}\times\Sigma\to Q_{\rm S}$, 对于$q_{\rm S}\in Q_{\rm S}\backslash\{||s||\}$, $\sigma\in\Sigma$, 若$\sigma=\sigma_{q_{\rm S}+1}$, 则$\delta_{\rm S}(q_{\rm S},\sigma)=q_{\rm S}+1$; 若$\sigma\neq\sigma_{q_{\rm S}+1}$, 则$\delta_{\rm S}(q_{\rm S},\sigma)=q_{\rm S}$; 且$\delta_{\rm S}(||s||,\sigma)=||s||$.

定义 6 设G为一个基于S型模式诊断的离散事件系统, 设所有触发S型模式故障的子序列为$K=\{s_1,s_2,\cdots,s_i\}$, 则G的并行器$G_{\rm lS}$构造为有限状态自动机$G_{\rm lS}=(Q_{\rm lS},\Sigma,\delta_{\rm lS},q_0^{\rm lS},F_{\rm lS})$, 其中状态集为$Q_{\rm lS}=X\times\prod_{j=1}^{i}l_j$, 初始状态为$q_0^{\rm lS}=(x_0,0,\cdots,0)$, 转移函数$\delta_{\rm lS}:Q_{\rm lS}\times\Sigma\to Q_{\rm lS}$定义为$\delta_{\rm lS}(q_{\rm lS},\sigma)=(\delta(x,\sigma),\delta_{\rm S1}(q_{\rm S1},\sigma),\cdots,\delta_{{\rm S}i}(q_{{\rm S}i},\sigma))$, 这里$q_{\rm lS}=(x,l_1,l_2,\cdots,l_i)\in Q_{\rm lS}$, $\sigma\in\Sigma$.

再构造非法语言识别器以对非法语言进行识别. 先引入一个标识符$\Phi_{\rm S}=\{S^1,S^2,B\}$, 其中: 标识$S^1$表示系统没有发生S型模式故障; 标识$S^2$表示系统发生了S型模式故障, 但此后没有发生被禁止事件串; 标识B表示系统发生了S型模式故障, 并且其发生之后又执行被禁止操作.

定义 7 设G为基于S型模式诊断的离散事件系统, 所有触发S型模式故障的子序列为$K=\{s_1,s_2,\cdots,s_i\}$, 则非法语言识别器$G_{\rm rS}$构造为有限状态自动机$G_{\rm rS}=\{Q_{\rm rS},\Sigma,\delta_{\rm rS},q_0^{\rm rS},F_{\rm rS}\}$, 其中: $Q_{\rm rS}\subseteq Q_{\rm lS}\times\Phi_{\rm S}$为状态集合; $q_0^{\rm rS}$为初始状态; $\delta_{\rm rS}:Q_{\rm rS}\times\Sigma\to Q_{\rm rS}$为转移函数, 对任意$\sigma\in\Sigma$, $s\in\Sigma^*$和$s'\in K$, $\delta_{\rm rS}$的转移规则如下:

1) 当$\sigma\notin K$时, $\delta_{\rm rS}(q_0^{\rm rS},\sigma)=(\delta_{\rm lS}(q_0^{\rm lS},\sigma),S^1)$;

2) 当$\sigma\in K$时, $\delta_{\rm rS}(q_0^{\rm rS},\sigma)=(\delta_{\rm lS}(q_0^{\rm lS},\sigma),S^2)$;

3) 当$q_{\rm rS}=\delta_{\rm rS}(q_0^{\rm rS},s)=(q_{\rm lS},S^1)$时, 如果$s'$不是$s\sigma$的子序列, 则$\delta_{\rm rS}(q_{\rm rS},\sigma)=(\delta_{\rm lS}(q_{\rm lS},\sigma),S^1)$; 如果$s'$是$s\sigma$的子序列, 则$\delta_{\rm rS}(q_{\rm rS},\sigma)=(\delta_{\rm lS}(q_{\rm lS},\sigma),S^2)$;

4) 当$q_{\rm rS}=\delta_{\rm rS}(q_0^{\rm rS},s)=(q_{\rm lS},S^2)$时, 如果$\zeta_{\rm fS}$不是$s\sigma$的子串, 则$\delta_{\rm rS}(q_{\rm rS},\sigma)=(\delta_{\rm lS}(q_{\rm lS},\sigma),S^2)$; 如果$\zeta_{\rm fS}$是$s\sigma$的子串, 则$\delta_{\rm rS}(q_{\rm rS},\sigma)=(\delta_{\rm lS}(q_{\rm lS},\sigma),B)$;

5) 当$q_{\rm rS}=\delta_{\rm rS}(q_0^{\rm rS},s)=(q_{\rm lS},B)$时, $\delta_{\rm rS}(q_{\rm rS},\sigma)=(\delta_{\rm lS}(q_{\rm lS},\sigma),B)$.

定义 8 设G为基于S型模式诊断离散事件系统, 其S型模式安全诊断器$G_{\rm vS}$构造为有限状态自动机$G_{\rm vS}=(Q_{\rm vS},\Sigma_{\rm o},\delta_{\rm vS},q_0^{\rm vS},F_{\rm vS})$, 其中$Q_{\rm vS}$为状态集合; $q_0^{\rm vS}=(x_0,0,0,\cdots,0,S^1)$为初始状态; $\delta_{\rm vS}$: $Q_{\rm vS}\times\Sigma_{\rm o}\to Q_{\rm vS}$为转移函数, 它满足

$$\delta_{\rm vS}(q_{\rm vS},\sigma)=\bigcup_{q_{\rm rS}\in q_{\rm vS}}\ \bigcup_{s\in L_\sigma(G_{\rm rS},q_{\rm rS})}\{(\delta_{\rm rS}(q_{\rm rS},s))\}.$$

定义 9 设$G_{\rm vS}$是离散事件系统G的S型模式安全诊断器, $q_{\rm vS}\in Q_{\rm vS}$. 如果对任意$q_{\rm rS}=(q_{\rm lS},\Phi_{\rm S})\in q_{\rm vS}$, 都有$F\in q_{\rm lS}$, 则称$q_{\rm vS}$为$F$–确定状态. 如果存在$q_{\rm rS}=(q_{\rm lS},\Phi_{\rm S})$, $q'_{\rm rS}=(q'_{\rm lS},\Phi'_{\rm S})\in q_{\rm vS}$使得$F\in q_{\rm lS}$, $F\notin q'_{\rm lS}$, 则称$q_{\rm vS}$为F–不确定状态.

下面给出S型模式安全可诊断的充分必要条件.

定理 1 给定基于S型模式诊断的离散事件系统$G=(X,\Sigma,\delta,x_0,F)$, 其S型模式安全诊断器为$G_{\rm vS}=(Q_{\rm vS},\Sigma_{\rm o},\delta_{\rm vS},q_0^{\rm vS},F_{\rm vS})$. G为S型模式安全可诊断的充分必要条件是S型模式安全诊断器$G_{\rm vS}$同时满足以下条件:

1) 不存在F–不确定状态$q_{\rm vS}\in Q_{\rm vS}$, 使得$(q_{\rm lS},\Phi_{\rm S})\in q_{\rm vS}$, 其中: $F\in q_{\rm lS}$, $B\in\Phi_{\rm S}$.

2) 不存在状态$q_{\rm vS},q'_{\rm vS}\in Q_{\rm vS}$, 其中$q_{\rm vS}$为$F$–不确定状态, $q'_{\rm vS}$为F–确定状态, 并且存在$e\in\Sigma_{\rm o}$和$(q'_{\rm lS},\Phi'_{\rm S})\in q'_{\rm vS}$, 使得$q'_{\rm vS}=\delta_{\rm vS}(q_{\rm vS},e)$, 其中: $F\in q'_{\rm lS}$, $B\in\Phi'_{\rm S}$.

证 下面先用反证法证明定理1的充分性.

假设G满足定理1中的条件1)和2), 但G不是S型模式安全可诊断的.

i) 若G不满足S型模式可诊断性条件,则存在事件串u,v, 使$P(u)=P(v)$, $u\in\Psi_{\rm S}(K)$, $v\notin\Psi_{\rm S}(K)$. 并且在$G_{\rm vS}$中, 一定存在状态$q_{\rm vS}\in Q_{\rm vS}$, 其中$q_{\rm rS},q'_{\rm rS}\in q_{\rm vS}$, 且$q_{\rm rS}=\delta_{\rm rS}(q_0^{\rm rS},P(u))=(q_{\rm lS},\Phi_{\rm S})$, $q'_{\rm rS}=\delta_{\rm rS}(q_0^{\rm vS},P(v))=(q'_{\rm lS},\Phi'_{\rm S})$, $F\in q_{\rm lS}$, $F\notin q'_{\rm lS}$, 那么$q_{\rm vS}$是F–不确定状态; 并且$B\in\Phi_{\rm S}$, $B\notin\Phi'_{\rm S}$, 这与满足定理1中的条件1)的这一假设相矛盾.

ii) 若G不满足安全性条件但满足诊断条件, 不妨设$u=u_1u_2\sigma$满足诊断条件, 其中: $u_1\in\Psi_{\rm S}(K)$, $u_2\in\zeta_{\rm fS}$, $\sigma\in\Sigma_{\rm o}$, 因为G不满足安全性条件, 所以对任意$t_{\rm c}$, 都有$\bar{t}_{\rm c}\cap\zeta_{\rm fS}=\varnothing$, $t_{\rm c}$为u中满足诊断条件中$D_{\rm S}$的最短事件串. 令$t_{\rm c}=u_2\sigma$, 即经过$u_1u_2\sigma$时故障刚好能够被诊断出来; 在$G_{\rm vS}$中存在状态$q_{\rm vS},q'_{\rm vS}\in Q_{\rm vS}$, 其中: $q_{\rm vS}=\delta_{\rm vS}(q_0^{\rm vS},P(u_1u_2))$, $q'_{\rm vS}=\delta_{\rm vS}(q_0^{\rm vS},P(u_1u_2\sigma))$, 并且$q_{\rm vS}$是$F$–不确定状态, $q'_{\rm vS}$是F–确定状态, 又因为$u_2\in\zeta_{\rm fS}$, 所以在$q'_{\rm vS}$中存在$q_{\rm rS}=(q_{\rm lS},\Phi_{\rm S})$, $B\in\Phi_{\rm S}$, 即不满足定理1中的条件2), 这与假设相矛盾.

再用反证法证明定理1的必要性.

假设系统G是S型模式安全可诊断的, 但其安全诊断器$G_{\rm vS}$不满足定理1中的条件1)或2).

i) 若G不满足条件1), 则存在F–不确定状态$q_{\rm vS}\in Q_{\rm vS}$, 使得$(q_{\rm lS},\Phi_{\rm S})\in q_{\rm vS}$, 其中$F\in q_{\rm lS}$, $B\in\Phi_{\rm S}$. 由于$q_{\rm vS}$为F–不确定状态, 则一定存在$q_{\rm rS},q'_{\rm rS}\in q_{\rm vS}$使$q_{\rm rS}=(q_{\rm lS},\Phi_{\rm S})$, $F\in\Phi_{\rm S}$, $q'_{\rm rS}=(q'_{\rm lS},\Phi'_{\rm S})$, $F\notin\Phi'_{\rm S}$, 由此可知, 在G中存在事件串u,v使得$P(u)=P(v)$, 其中$u\in\Psi_{\rm S}(K)$, $v\notin\Psi_{\rm S}(K)$, 即不满足S型模式可诊断条件.

ii) 若G不满足条件2), 即存在$q_{\rm vS},q'_{\rm vS}\in Q_{\rm vS}$, 其中$q_{\rm vS}$和$q'_{\rm vS}$为分别$F$–不确定状态和$F$–确定状态, 且存在$e\in\Sigma_o$, $(q'_{\rm lS},\Phi'_{\rm S})\in q'_{\rm vS}$, 使得$q'_{\rm vS}=\delta_{\rm vS}(q_{\rm vS},e)$, 其中$F\in q'_{\rm lS}$, $B\in\Phi'_{\rm S}$. 取$s=ue$, 令$q_{\rm vS}=\delta_{\rm vS}(q_0^{\rm vS},u)$, $q'_{\rm vS}=\delta_{\rm vS}(q_0^{\rm vS},s)$, 则存在$u'$, v使得$u'v\in P^{-1}(u)$, $u'\in\Psi_{\rm S}(K)$, $v\notin\Psi_{\rm S}(K)$, 再令$u=u_1u_2$, $u_1\notin\Psi_{\rm S}(K)$. 因为G是S 型模式安全可诊断的, 所以存在$t\in L/u_1$, 且

t满足条件$D_{\rm S}$, 此时满足条件$D_{\rm S}$的最短事件串为$t_{\rm c}=u_2e$. 又因为$(q'_{\rm lS},\Phi'_{\rm S})\in q'_{\rm vS}$, 其中$B\in\Phi'_{\rm S}$, 即$u_2e\cap\zeta_{\rm f}\neq\varnothing$, 即$G$不是S型模式安全可诊断的, 这与假设相矛盾.　　证毕.

注 1　设基于S型模式诊断的离散事件系统G, 其系统状态数为$\|X|=n_1$, 事件数$\|\Sigma\|=n_2$, 在安全诊断器$G_{\rm vS}$中, 其状态数与事件数最多分别为2^{n_1}和n_2, 则构造$G_{\rm vS}$的复杂度为O$(2^{n_1}\cdot n_2)$. 当判断定理1中的条件1)时, 需要遍历安全诊断器$G_{\rm vS}$中的所有状态, 所以复杂度为O(2^{n_1}), 当判断定理1中的条件2)时, 需要遍历所有的状态及事件, 即复杂度为O$(2^{n_1}\times n_2)$. 根据定理1, 验证G的S型模式安全可诊断性的复杂度为O$(n_2\cdot 2^{n_1})$.

例 1　考虑图1中系统G_1, 其中: $\Sigma_{\rm o}=\{b,d,\sigma_{\rm s}\}$, $\Omega=\{\sigma_{\rm s}\}$, 故障模式集$K_1=\{d,c\}$.

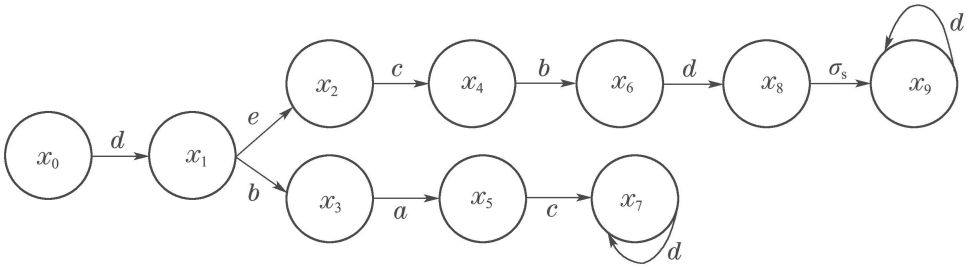

图 1　离散事件系统G_1

Fig. 1　Discrete-event system G_1

分别构造状态标记器和并行器如图2和图3所示.

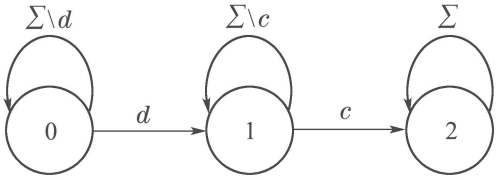

图 2　标记器$H_{\rm S}(s)$

Fig. 2　The label automaton $H_{\rm S}(s)$

分别构造S型模式非法语言识别器和安全诊断器如图4和图5所示.

由图5可知, 状态$\{(x_3,1,S^1),(x_6,F,S^2)\}$为$F$–不确定状态, 并且在$(x_3,1,S^1)$与$(x_6,F,S^2)$中都没有标识符$B$; 且由$F$–不确定状态$\{(x_3,1,S^1),(x_6,F,S^2)\}$经过可观事件$d$到达$F$–确定状态$\{(x_8,F,S^2),(x_7,F,S^2)\}$, 即$G_{\rm vS}$满足定理1条件, 所以系统$G_1$是S型模式安全可诊断的.

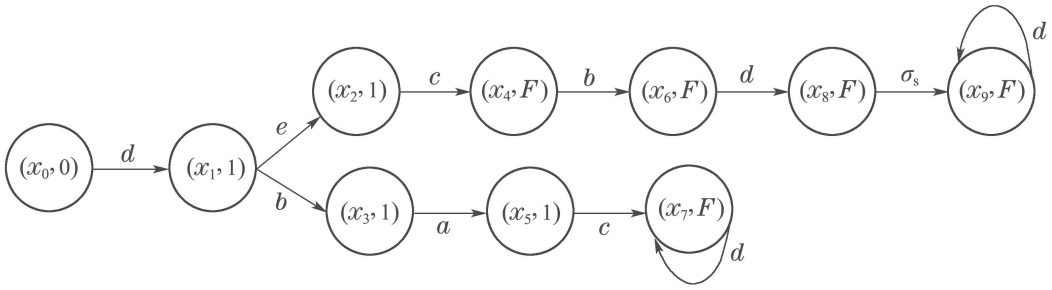

图 3　并行器$G_{\rm lS}$

Fig. 3　Parallel automaton $G_{\rm lS}$

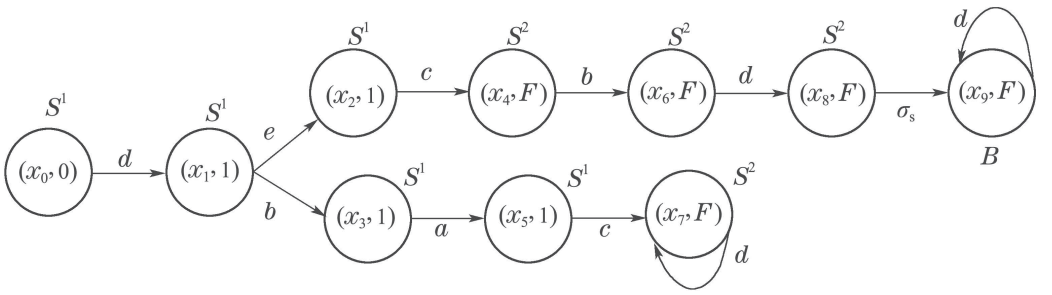

图 4　S 型模式非法语言识别器$G_{\rm rS}$

Fig. 4　S-type recognizer of illegal language $G_{\rm rS}$

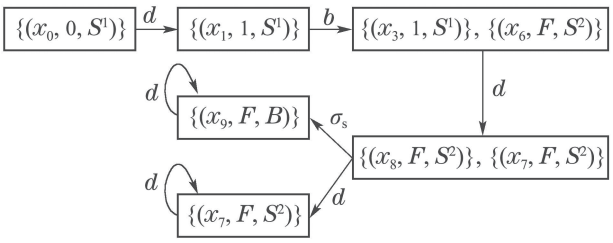

图 5 S 型安全诊断器$G_{\rm vS}$

Fig. 5 S-type safe diagnoser $G_{\rm vS}$

5 基于T型模式的安全故障诊断

定义 10 设G为一个基于T型模式诊断的离散事件系统, $s=\sigma_1\sigma_2\sigma_3\cdots\sigma_m$为触发T型模式故障的子串, 则$G$的标记自动机构造为有限状态自动机

$$H_{\rm T}(s)=(Q_{\rm T},\Sigma,\delta_{\rm T},q_0^{\rm T},F_{\rm T}),$$

其中: $Q_{\rm T}=\{0,1,\cdots,\|s\|\}$为状态集合, $\delta_{\rm T}$为转移函数, $\delta_{\rm T}:Q_{\rm T}\times\Sigma\to Q_{\rm T}$, 对于$q_{\rm T}\in Q_{\rm T}\backslash\{\|s\|\}$, $\sigma\in\Sigma$, 如果$\sigma=\sigma_{q_{\rm T}+1}$, 则$\delta_{\rm T}(q_{\rm T},\sigma)=q_{\rm T}+1$; 如果$\sigma\neq\sigma_{q_{\rm T}+1}$, 则$\delta_{\rm T}(q_{\rm T},\sigma)=0$; 且$\delta_{\rm T}(\|s\|,\sigma)=\|s\|$.

定义 11 设G为一个基于T型模式诊断的离散事件系统, 所有触发T型模式故障子串为$K=\{s_1,s_2,\cdots,s_i\}$, G的并行自动机$G_{\rm lT}$构造为有限状态自动机

$$G_{\rm lT}=(Q_{\rm lT},\Sigma,\delta_{\rm lT},q_0^{\rm lT},F_{\rm lT}),$$

其中: $Q_{\rm lT}=X\times\prod_{j=1}^{i}l_j,l_j\in Q_{{\rm T}i}$; $q_0^{\rm lT}=(x_0,0,\cdots,0)$; 转移函数$\delta_{\rm lT}:Q_{\rm lT}\times\Sigma\to Q_{\rm lT}$定义为$\delta_{\rm lT}(q_{\rm lT},\sigma)=(\delta(x,\sigma),\delta_{\rm T1}(q_{\rm T1},\sigma),\cdots,\delta_{{\rm T}i}(q_{{\rm T}i},\sigma))$, 这里$q_{\rm lT}=(x,l_1,l_2,\cdots,l_i)$, $\sigma\in\Sigma$.

下面构造非法语言识别器$G_{\rm rT}$以对非法操作进行识别. 引入禁止标识符$\Phi_{\rm T}=\{S^1,S^2,B\}$, 其中标识$S^1$表示系统没有发生T型模式故障; 标识$S^2$表示系统发生了T型模式故障, 但其发生之后没有发生被禁止事件串; 标识B表示系统即发生了T型模式故障又执行了被禁止事件串.

定义 12 设$G=(X,\Sigma,\delta,x_0,F)$为一个基于T型模式诊断的离散事件系统, 所有触发T型模式故障的子串为$K=\{s_1,s_2,\cdots,s_i\}$, G的T型模式非法语言识别器$G_{\rm rT}$构造为有限状态自动机

$$G_{\rm rT}=\{Q_{\rm rT},\Sigma,\delta_{\rm rT},q_0^{\rm rT},F_{\rm rT}\},$$

其中: $Q_{\rm rT}$为状态集合; 初始状态$q_0^{\rm rT}$; $\delta_{\rm rT}$为转移函数, 对于$\sigma\in\Sigma$, $s\in\Sigma^*$, $s'\in K$:

1) 当$\sigma\notin K$时, $\delta_{\rm rT}(q_0^{\rm rT},\sigma)=(\delta_{\rm lT}(q_0^{\rm lT},\sigma),S^1)$;

2) 当$\sigma\in K$时, $\delta_{\rm rT}(q_0^{\rm rT},\sigma)=(\delta_{\rm lT}(q_0^{\rm lT},\sigma),S^2)$;

3) 当$q_{\rm rT}=\delta_{\rm rT}(q_0^{\rm rT},s)=(q_{\rm lT},S^1)$时, 若$s'$不是$s\sigma$的子串, 则$\delta_{\rm rT}(q_{\rm rT},\sigma)=(\delta_{\rm lT}(q_{\rm lT},\sigma),S^1)$, 若$s'$是$s\sigma$的子串, 则$\delta_{\rm rT}(q_{\rm rT},\sigma)=(\delta_{\rm lT}(q_{\rm lT},\sigma),S^2)$;

4) 当$q_{\rm rT}=\delta_{\rm rT}(q_0^{\rm rT},s)=(q_{\rm lT},S^2)$时, 若$\zeta_{\rm fT}$不是$s\sigma$的子串, 则$\delta_{\rm rT}(q_{\rm rT},\sigma)=(\delta_{\rm lT}(q_{\rm lT},\sigma),S^2)$, 若$\zeta_{\rm fT}$是$s\sigma$的子串, 则$\delta_{\rm rT}(q_{\rm rT},\sigma)=(\delta_{\rm lT}(q_{\rm lT},\sigma),B)$;

5) 当$\delta_{\rm rT}(q_0^{\rm rT},s)=(q_{\rm lT},B)$时, $\delta_{\rm rT}(q_{\rm rT},\sigma)=(\delta_{\rm lT}(q_{\rm lT},\sigma),B)$.

定义 13 设基于T型模式诊断的离散事件系统$G=(X,\Sigma,\delta,x_0,F)$, 其T型模式安全诊断器$G_{\rm vT}$构造为有限状态自动机$G_{\rm vT}=(Q_{\rm vT},\Sigma_o,\delta_{\rm vT},q_0^{\rm vT},F_{\rm vT})$, 其中: $Q_{\rm vT}\subseteq 2^{Q_{\rm rT}}$为状态集; $\delta_{\rm vT}$为转移函数, 对于$q_{\rm vT}\in Q_{\rm vT}$, $\sigma\in\Sigma_{\rm o}$, 其转移规则如下:

$$\delta_{\rm vT}(q_{\rm vT},\sigma)=\bigcup_{q_{\rm rT}\in q_{\rm vT}}\ \bigcup_{s\in L_\sigma(G_{\rm rT},q_{\rm rT})}\{(\delta_{\rm rT}(q_{\rm rT},s))\}.$$

定义 14 设$G_{\rm vT}$为T型模式安全诊断器, 如果对任意$q_{\rm rT}=(q_{\rm lT},\Phi_{\rm T})\in q_{\rm vT}$, 都有$F\in q_{\rm lT}$, 则称$q_{\rm vT}$为$F$–确定状态. 如果存在$q_{\rm rT}=(q_{\rm lT},\Phi_{\rm T})$, $q'_{\rm rT}=(q'_{\rm lT},\Phi'_{\rm T})\in q_{\rm vT}$使得$F\in q_{\rm lT}$, $F\notin q'_{\rm lT}$, 则称$q_{\rm vT}$为F–不确定状态.

下面给出T型模式安全可诊断的充分必要条件.

定理 2 设基于T型模式诊断的离散事件系统$G=(X,\Sigma,\delta,x_0,F)$, 其T型模式安全诊断器为$G_{\rm vT}=(Q_{\rm vT},\Sigma_{\rm o},\delta_{\rm vT},q_0^{\rm vT},F_{\rm vT})$, 则$G$为T型模式安全模式诊断的充分必要条件是$G_{\rm vT}$同时满足以下条件:

1) 不存在F–不确定状态$q_{\rm vT}$, 使得$(q_{\rm lT},\Phi_{\rm T})\in q_{\rm vT}$, 其中: $F\in q_{\rm lT}$, $B\in\Phi_{\rm T}$.

2) 不存在状态$q_{\rm vT},q'_{\rm vT}\in Q_{\rm vT}$, 其中$q_{\rm vT}$为$F$–不确定状态, $q'_{\rm vT}$为F–确定状态, 并且存在$e\in\Sigma_o$和$(q'_{\rm lT},\Phi'_{\rm T})\in q'_{\rm vT}$, 使得$q'_{\rm vT}=\delta_{\rm vT}(q_{\rm vT},e)$, 其中: $F\in q'_{\rm lT}$, $B\in\Phi'_{\rm T}$.

证 利用反证法证明定理2的充分性.

假设系统G满足定理2中的条件1)和2), 但是G不是T型模式安全模式诊断.

i) 若G不满足可诊断性条件,则存在事件串u,v且$P(u)=P(v)$, $u\in\Psi_{\rm T}(K)$, $v\notin\Psi_{\rm T}(K)$. 在T型模式安全诊断器中$G_{\rm vT}$中存在状态$q_{\rm vT}\in Q_{\rm vT}$, 其中$q_{\rm rT},q'_{\rm rT}\in q_{\rm vT}$, 且$q_{\rm rT}=(q_{\rm lT},\Phi_{\rm T})$, $q'_{\rm rT}=(q'_{\rm lT},\Phi'_{\rm T})$, $F\in q_{\rm lT}$, $F\notin q'_{\rm lT}$, 则$q_{\rm vT}$为F–不确定状态; 由于$B\in\Phi_{\rm T}$, $B\notin\Phi'_{\rm T}$, 这与假设相矛盾.

ii) 若G不满足安全性条件但满足诊断条件, 设事件串$u=u_1u_2\sigma$满足诊断条件, 其中: $u_1\in\Psi_{\rm T}(K)$, $u_2\in\zeta_{\rm fT}$, $\sigma\in\Sigma_{\rm o}$. 因G不满足安全性条件, 所以对任意$\bar{t}_{\rm c}$, 有$\bar{t}_{\rm c}\cap\zeta_{\rm fT}=\varnothing$, $\bar{t}_{\rm c}$为u中满足诊断条件中$D_{\rm T}$的最短事件串, 令$t_{\rm c}=u_2\sigma$, 即经过事件串$u_1u_2\sigma$时故障刚好能够被诊断出来, 在$G_{\rm vT}$中存在$q_{\rm vT},q'_{\rm vT}\in Q_{\rm vT}$, 使得$q'_{\rm vT}=\delta_{\rm vT}(q_{\rm vT},\sigma)$, 且$q_{\rm vT}$为$F$–不确定状态, $q'_{\rm vT}$为F–确定状态, 又因为$u_2\in\zeta_{\rm fT}$, 所以在$q'_{\rm vT}$中存在$q_{\rm rT}=(q_{\rm lT},\Phi_{\rm T})$, 且$B\in\Phi_{\rm T}$, 即不满足定理2中的条

件2), 与假设相矛盾.

再利用反证法证明定理2的必要性.

i) 假设G是T型模式安全可诊断的系统, 但是$G_{\rm vT}$不满足定理2中的条件1), 则在$G_{\rm vT}$中存在一个F–不确定状态$q_{\rm vT}$, 且$(q_{\rm lT}, \Phi_{\rm T})$, $(q'_{\rm lT}, \Phi') \in q_{\rm vT}$, 其中$F \in q_{\rm lT}$, $F \notin q'_{\rm lT}$, $B \in \Phi_{\rm T}$. 设事件串$s \in \Sigma_{\rm o}^*$, 且$q_{\rm vT} = \delta_{\rm vT}(q_0^{\rm vT}, s)$, 则在并行器$G_{\rm lT}$中必然存在事件串$u$, $v \in P^{-1}(s)$, 使得$q_{\rm lT} = \delta_{\rm lT}(q_0^{\rm lT}, u)$, $q'_{\rm lT} = \delta_{\rm lT}(q_0^{\rm lT}, v)$; 又因为$F \in q_{\rm lT}$, 所以设$u = u_1u_2$, 且$u_1 \in \Psi_{\rm T}(K)$. 存在$t \in L/u_1$, 满足可诊断条件, 令$t' = u_1t (t = u_2t_{\rm c})$, 又因为$B \in \Phi_{\rm T}$, 所以$u_2 \in \zeta_{\rm fT}$, $u_2t_{\rm c} \cap \zeta_{\rm fT} \neq \varnothing$, 这与假设相矛盾.

ii) 假设G是T型模式安全可诊断的系统, 但是$G_{\rm vT}$不满足定理2中的条件2), 即存在$q_{\rm vT}$, $q'_{\rm vT} \in Q_{\rm vT}$, 其中$q_{\rm vT}$是$F$–不确定状态; $q'_{\rm vT}$是F–确定状态, 并存在$e \in \Sigma_{\rm o}$, 使$q'_{\rm vT} = \delta_{\rm vT}(q_{\rm vT}, e)$; 存在$(q'_{\rm lT}, \Phi'_{\rm T}) \in q'_{\rm vT}$, 其中$F \in q'_{\rm lT}$, $B \in \Phi'_{\rm T}$; 设事件串$s \in \Sigma_{\rm o}^*$, 且$q_{\rm vT} = \delta_{\rm vT}(q_0^{\rm vT}, s)$, 则在并行器$G_{\rm lT}$中存在事件串$u$, $v \in P^{-1}(s)$, 使得$q_{\rm lT1} = \delta_{\rm lT}(q_0^{\rm lT}, u)$, $q_{lT2} = \delta_{\rm lT}(q_0^{\rm lT}, v)$, $F \in q_{\rm lT1}$, $F \notin q_{\rm lT2}$; 再令$u = u_1u_2$, 并且使$u_1 \in \Psi_{\rm T}(K)$, G是T型模式安全可诊断的, 存在$t \in L/u_1$, 满足诊断条件$D_{\rm T}$, 因为$q'_{\rm vT}$是F–确定状态, 所以$t_{\rm c} = u_2e$, 即诊断器经过事件串se时故障恰好能够被诊断出来, 则存在$q'_{\rm lT} = \delta_{\rm lT}(q_0^{\rm lT}, u_1u_2e)$, 因为$B \in \Phi'$, 所以$u_2e \in \zeta_{\rm fT}$, 即$\bar{t} \cap \zeta_{\rm fT} \neq \varnothing$, 这同样与假设相矛盾.　　证毕.

注 2　与S型模式安全可诊断复杂性类似, 构造$G_{\rm vT}$的复杂度为O$(2^{n_1} \times n_2)$, 判断定理2中的条件1)2)的复杂度分别为O(2^{n_1})和O$(2^{n_1} \cdot n_2)$. 因此, 根据定理2, 验证G的T型模式安全可诊断性的复杂度为O$(n_2 \cdot 2^{n_1})$, 其中n_1, n_2为G的状态数和事件数.

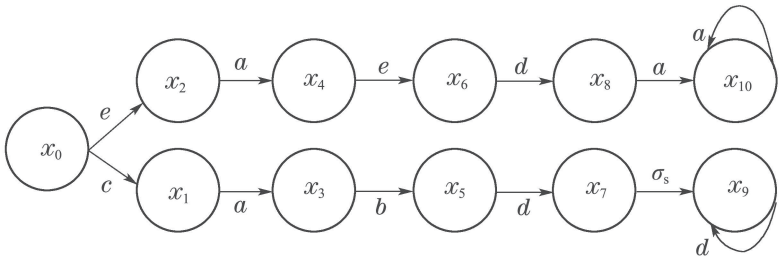

图 6 离散事件系统G_2

Fig. 6 Discrete-event system G_2

例 1　考虑图6中系统G_2, 其中: $\Sigma_{\rm o} = \{a, d, \sigma_{\rm s}\}$, $\Omega = \{\sigma_{\rm s}\}$, 故障模式集$K_2 = \{ab\}$.

构造T型模式标记器和安全诊断器如图7和图8所示.

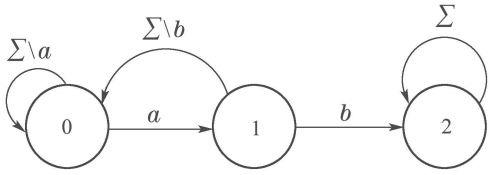

图 7 标记器$H_{\rm T}(s)$

Fig. 7 The label automaton $H_{\rm T}(s)$

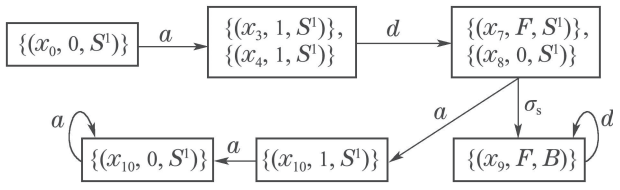

图 8 T型模式安全诊断器$G_{\rm vT}$

Fig. 8 T–type safe diagnoser $G_{\rm vT}$

由图8中可知, $G_{\rm vT}$中仅有状态$\{(x_7, F, S^1), (x_8, 0, S^1)\}$为$F$–不确定状态, 且在$(x_7, F, S^1)$与$(x_8, 0, S^1)$中没有标识符$B$, 即$G_{\rm vT}$满足定理2中条件1); 而$F$–确定状态$\{(x_9, F, B)\}$由$F$–不确定状态$\{(x_7, F, S^1), (x_8, 0, S^1)\}$经过可观事件$\sigma_s$到达, 并且在$(x_9, F, B)$中有标识符$B$, 即$G_{\rm vT}$不满足定理2中条件2), 所以$G_2$不是T型模式安全可诊断的.

6　总结

本文讨论了离散事件系统基于模式故障诊断的安全性问题, 提出了一种对故障模式进行安全诊断的方法, 它不仅能将S型模式和T型模式的故障在其发生之后诊断出来, 又能确保系统在模式诊断期间不执行任何被禁止的不安全操作. 该方法通过构造非法语言识别器和安全诊断器, 得到了一个关于离散事件系统可安全模式诊断的充分必要条件.

参考文献:

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

[2] ZAD H, KWONG R H, et al. Fault diagnosis in discrete-event systems: framework and model reduction. *IEEE Transactions on Automatic Control*, 1998, 48(7): 1199 – 1212.

[3] MOREIRA M V, JESUS T C, BASILIO J C. Polynomial time verification of decentralized diagnosability of discrete event systems. *IEEE Transactions on Automatic Control*, 2011, 56(7): 1679 – 1684.

[4] THORSLEY D, TENEKETZIS D. Diagnosability of stochastic discrete-event systems. *IEEE Transactions on Automatic Control*,

2005, 50(4): 476 – 492.

[5] LIU F, QIU D. Diagnosability of fuzzy discrete-event systems: a fuzzy approach. *IEEE Transactions on Fuzzy Systems*, 2006, 17(2): 372 – 384.

[6] WANG Xiaoyu, OUYANG Dantong, ZHAO Xiangfu. Diagnosability of discrete event systems with an incomplete model. *Journal of Software*, 2015, 26(6): 1373 – 1385.
(王晓宇, 欧阳丹彤, 赵相福. 不完备离散事件系统的可诊断性. 软件学报, 2015, 26(6): 1373 – 1385.)

[7] GENC S, LAFORTUNE S. Diagnosis of patterns in partially-observed discrete-event systems. *IEEE Conference on Decision and Control*. New Orleans: IEEE, 2007: 422 – 427.

[8] LAMPERTI G, ZHAO X. Diagnosis of active systems by semantic patterns. *IEEE Transactions on Systems Man & Cybernetics Systems*, 2017, 44(8): 1028 – 1043.

[9] JéRON T, MARCHAND H, GENC S, et al. Predictability of sequence patterns in discrete event systems. *IFAC Proceedings Volumes*, 2008, 41(2): 537 – 543.

[10] PAOLI A, LAFORTUNE S. Safe diagnosability for fault-tolerant supervision of discrete-event systems. *Automatica*, 2005, 41(8): 1335 – 1347.

[11] DENG W, QIU D. State-based safe-codiagnosability of discrete-event systems and a polynomial verification algorithm. *Chinese Control Conference*. Dalian: IEEE, 2017: 2397 – 2402.

[12] LIU Fuchun, LUO Ping. Polynomial-time verification of safe diagnosability of discrete-event systems. *Control Theory & Applications*, 2017, 34(6): 717 – 722.
(刘富春, 罗苹. 具有多项式时间复杂性的离散事件系统安全诊断. 控制理论与应用, 2017, 34(6): 717 – 722.)

作者简介:

刘富春 教授, 博士生导师, 从事控制理论、算法设计等研究, E-mail: fliu2011@163.com;

唐顺桥 硕士研究生, 从事控制理论、算法设计等研究, E-mail: 2215907230@qq.com;

赵 锐 讲师, 博士, 从事离散事件系统、智能计算等研究, E-mail: zhaorui118204@163.com;

邓秀勤 教授, 硕士, 从事智能计算、机器学习等研究, E-mail: dxq706@gdut.edu.cn;

崔洪刚 讲师, 博士, 从事大数据与智能计算等研究, E-mail: cuihg@163.com.