

DOI:10.19651/j.cnki.emt.2209378

一种离散事件系统边界可诊断性验证方法*

冉宁^{1,2} 李婷婷^{1,3} 张照彦¹ 郝晋渊⁴

(1. 河北大学电子信息工程学院 保定 071002; 2. 河北大学节能技术研发中心 保定 071002;
3. 河北大学物联网智能技术研究中心 保定 071002; 4. 河北大学中央兰开夏传媒与创意学院 保定 071002)

摘要: 针对有效验证离散事件系统故障后是否具有可诊断性问题,设计了一种基于 Petri 网的边界可诊断性的验证方法。首先,根据 Petri 网的结构特性,提出了显示可达图的概念及其构建算法;其次,提出了一种基于显示可达图的验证器及其构造算法,分析系统故障发生后是否具有可诊断性以及计算满足系统可诊断性的边界值;最后,通过实例对所设计的方法进行验证。实验结果表明,设计方法可以有效验证系统故障后是否具有可诊断性并计算系统满足可诊断性的边界值,计算过程较为简单,对实际工业应用中离散事件系统故障可诊断性问题具有借鉴意义。

关键词: 离散事件系统;Petri 网;故障诊断;边界可诊断性

中图分类号: TP11;TN0 **文献标识码:** A **国家标准学科分类代码:** 510.80

A method for boundary diagnosability analysis for discrete event systems

Ran Ning^{1,2} Li Tingting^{1,3} Zhang Zhaoyan¹ Hao Jinyuan⁴

(1. College of Electronic Information Engineering, Hebei University, Baoding 071002, China;

2. Laboratory of Energy-Saving Technology, Hebei University, Baoding 071002, China;

3. Laboratory of IoT Technology, Hebei University, Baoding 071002, China;

4. HBU-UCLAN School of Media, Communication and Creative Industries, Hebei University, Baoding 071002, China)

Abstract: In order effectively verify the diagnosability of discrete event system after failure, a method of boundary diagnosability verification based on Petri net was designed. Firstly, according to the structural characteristics of Petri net, the concept of visible reachable graph and its construction algorithm are proposed. Secondly, a verifier based on visible reachability graph and its construction algorithm are proposed to analyze whether the system is diagnosable after the occurrence of faults and calculate the boundary values that meet the requirement of system diagnosable. Finally, an example is given to verify the proposed method. The experimental results show that the design method can effectively verify whether the system has diagnosable ability after failure and give diagnosable boundary value. The calculation process is relatively simple, which can be used for reference to the problem of fault diagnosable ability of discrete event system in practical industrial applications.

Keywords: discrete event system; Petri net; fault diagnosis; boundary diagnosability

0 引言

离散事件系统(discrete event system, DES)是一种在离散时间点上由异步、突发的事件驱动而发生状态变化的动态系统,具有随机性、并发性以及系统状态强离散化等特点^[1]。大部分自动控制系统从系统状态逻辑演化层面可以抽象为 DES 进行研究,如柔性制造系统、轨道交通系统、通信系统等。DES 运行过程中存在设备老化、电器故障等问

题导致系统不可避免地发生故障,从而影响 DES 安全稳定地运行,因此对 DES 进行及时有效的故障诊断具有重要意义。

目前用于研究 DES 的建模工具主要有 Petri 网和自动机等^[2]。Petri 网具有严格的数学表达式和直观的图形,因此常用于解决 DES 故障诊断、资源配置优化、监控器综合等问题^[3-9]。在设计 DES 故障诊断算法时,需要满足系统具有可诊断性这一重要特性,因此验证系统是否具有可诊

收稿日期:2022-03-23

* 基金项目:国家自然科学基金(61903119)、河北省高等学校科学技术研究项目(BJ2021008)、河北省引进留学人员资助项目(C20190319)、河北省高等学校人文社会科学研究项目(SY202106)、河北省人力资源社会保障课题(JRS-2020-3025)、河北省社会发展研究课题(20210301141)、保定市文化艺术科学规划项目(BWGY044)、2021年度河北大学高校思想政治理论课研究专项资助

断性成为 DES 故障诊断研究领域的热点之一^[10-15]。

文献[14-15]提出了一种标签 Petri 网故障可诊断性验证方法,将边界可诊断性的概念拓展到 Petri 网。该方法使用范围广且计算次数优于基于状态自动机的方法,但其可达图的状态数随系统的复杂性呈指数增长。文献[16]在文献[14-15]基础上,提出一种基础可达性验证器的验证方法,通过引入基础标识和最小解释的概念构建基础可达图,避免了状态组合爆炸的问题。缺点在于约束条件限制,即无死锁状态以及不存在无限长的不可观变迁。文献[17]提出一种分布式 Petri 网边界可诊断的验证方法。该方法在 Petri 网数学表达式基础上将系统变迁序列发生转换为整数线性规划问题,进而判断系统是否满足边界可诊断性。优点在于只通过线性规划的求解即可验证可诊断性,计算复杂度较低,具有一定的前景性。文献[18-19]提出一种分布式 Petri 网协同可诊断性的验证方法,并给出协同可诊断的充要条件,即故障发生后不会出现任意长的模糊序列,同时构造一个验证器来分析系统边界协同可诊断性并给出求解满足可诊断的边界值的算法。进行可诊断性验证的同时,提出了诊断器的构造算法,并降低系统计算复杂度,但仍需要满足的约束条件限制。

本文通过与文献[20-21]的两种故障可诊断研究方法对比,表明本设计方法的实用性和有效性。文献[20]分析包含时序关系和可自行恢复故障的离散事件动态系统。该方法建立一种带有时序约束的自动机模型,并在此模型的基础上提出一种在线诊断算法。优点在于根据时序约束筛选,减少诊断路径的数量,节省诊断时间。缺点在于设计故障诊断问题是有前提假设条件,如观测序列与实际产生序列顺序保持一致等,对于实际系统还需进一步深入研究。文献[21]提出了输入输出可诊断的结构,构建包含四个诊断器模型的方法,以减少诊断器模型中的标记数量。设计一种在线故障检测与定位的简化模型诊断器。优点在于该方法避免状态组合爆炸的问题,计算复杂度较低。缺点在于将故障建模为库所形式这种建模方法在很多工业应用不易实现。

DES 的边界可诊断性是在可诊断性概念的基础上设定了一个边界值 K ,要求在故障发生后的 K 步之内根据可观测事件序列的发生检测到故障的发生。针对 DES 的可诊断性问题,本文提出一种基于有界 Petri 网的边界可诊断验证方法。首先,提出显示可达图的概念和算法;其次,基于显示可达图提出边界可诊断性验证算法,同时给出有界 Petri 网满足边界可诊断性的充要条件;最后,通过实例说明本文所提算法的实用性和有效性。

1 Petri 网的基础知识

Petri 网是一个四元组 $N = (P, T, F, W)$,其中, P 代表库所 (place) 集合, T 代表变迁 (transition) 集合, $F \subseteq (P \times T) \cup (T \times P)$ 称为 Petri 网的流关系,表示库所

与变迁之间有向弧的集合, $W: F \rightarrow N^+$ 是一个映射,其中 N^+ 表示正整数集合,该映射为每条弧分配一个权值。

$y \in P \cup T$ 是 Petri 网的结点, y 的前置集 $\cdot y$ 定义为:

$$\cdot y = \{z \in P \cup T \mid (z, y) \in F\} \quad (1)$$

y 的后置集 $y \cdot$ 定义为:

$$y \cdot = \{z \in P \cup T \mid (y, z) \in F\} \quad (2)$$

Petri 网的标识 $M: P \rightarrow N$ 是一个映射,其中 N 表示自然数集合,该映射为每一个库所分配若干个托肯 (token)。 $M(p)$ 代表库所 p 中的托肯数。 (N, \mathbf{M}_0) 表示一个初始标识为 \mathbf{M}_0 的 Petri 网系统。 $R(N, \mathbf{M}_0)$ 表示 Petri 网中由初始标识 \mathbf{M}_0 可达的所有标识集合。当 $\exists B \in N, \forall p \in P, \forall \mathbf{M} \subseteq R(N, \mathbf{M}_0)$, 使得 $M(p) \leq B$ 成立,则称为是有界 (bounded) 的 Petri 网。

Petri 网的关联矩阵 $[A]$ 用一个 $|P| \times |T|$ 的整数矩阵,其中 $[A](p, t) = W(t, p) - W(p, t)$ 。 $[A](p, \cdot)$ 表示库所对应关联矩阵中的行向量, $[A](\cdot, t)$ 表示变迁所对应关联矩阵中的列向量。

给定 Petri 网,一个变迁 $t \in T$ 在标识 \mathbf{M} 下是使能 (enabled) 的当且仅当: $\forall p \in \cdot t, M(p) \geq W(p, t)$, 记为 $\mathbf{M}[t]$ 。给定变迁序列 $\sigma = t_1 t_2 \dots t_n, \mathbf{M}[\sigma]$ 表示变迁序列 σ 在标识 \mathbf{M} 下是使能的。 $L(N, \mathbf{M}_0) = \{\sigma \mid \mathbf{M}_0[\sigma]\}$ 表示在初始标识 \mathbf{M}_0 下可使能的所有变迁序列集合。 $L(N, \mathbf{M}_0) / \sigma = \{\sigma' \mid \sigma \sigma' \in L(N, \mathbf{M}_0)\}$ 表示变迁序列 σ 发生后可使能的变迁序列集合。 $|\sigma|$ 为变迁序列 σ 的长度。

给定 Petri 网,变迁序列 $\sigma \in L(N, \mathbf{M}_0)$ 是死锁 (deadlock) 当且仅当 $\exists t \in T$, 使得 $\mathbf{M}_0[\sigma] \mathbf{M}, \mathbf{M}[t]$ 。Petri 网无死锁 (deadlock-free) 当且仅当 $\forall \mathbf{M} \in R(N, \mathbf{M}_0), \exists t \in T, \mathbf{M}[t]$ 。

一个有限状态自动机是一个四元组 $G = (Q, D, \Delta, q_0)$,其中 Q 代表有限状态集合, D 称为字母表, $\Delta \subseteq Q \times D_c \times Q$ ($D_c = D \cup \{\epsilon\}$, ϵ 是一个空符号) 代表状态与状态之间的变迁关系, $q_0 \in Q$ 是自动机的初始状态。

标签 Petri 网 (labeled Petri net) 表示为 (N, \mathbf{M}_0, I) , 其中 (N, \mathbf{M}_0) 为 Petri 网系统; $I: T \rightarrow D \cup \{\epsilon\}$ 为标签函数,赋予变迁集合相应的标签符号。若标签函数赋予变迁为 ϵ 时,则变迁 t 为故障变迁,故障变迁集合记为 T_ϵ ,在 Petri 网结构中用黑色小矩形表示。当标签函数赋予变迁为 D 中一个字母时,则变迁 t 是可观变迁,可观变迁集合记为 T_a ,令表示可观变迁序列集合 T_a^* 。

标签函数的定义为:

$$I(\epsilon) = \epsilon \quad (3)$$

$$\text{当 } t \in T_a \text{ 时, } I(t) = d, d \in D \quad (4)$$

$$\text{当 } t \in T_\epsilon \text{ 时, } I(t) = \epsilon \quad (5)$$

$$\text{当 } \sigma \in T_a^* \wedge t \in T \text{ 时, } I(\sigma t) = I(\sigma) I(t) \quad (6)$$

给定一个变迁序列 σ , 令 $\sigma \cap T_\epsilon \neq \emptyset$ 表示 σ 至少包含 T_ϵ 中的一个变迁, $\sigma \cap T_\epsilon = \emptyset$ 表示 σ 不包含 T_ϵ 中的变迁; 令 $I^{-1}(\omega)$ 代表观测值为 ω 的变迁序列集合, 即 $I^{-1}(\omega) =$

$\{\sigma \in L(N, \mathbf{M}_0) \mid I(\sigma) = \omega\}$ 。从初始标识出发,以故障变迁结束的变迁序列集合 $\Phi(T_c)$ 。

给定一个 Petri 网 $N = (P, T, F, W)$, 当故障变迁集合 $T_c \subseteq T$, 则其无故障子网为 $N' = (P, T', F', W)$, 即删除网 N 中的故障变迁和与之相连的有向弧, 其中 $T' = T \setminus T_c, F' = ((P \times T_c) \cap (T_c \times P)) \cup F$ 。

例 1 给定一个有界标签 Petri 网, 如图 1 所示。其中, 库所集合 $P = \{p_1, p_2, p_3, p_4\}$, 可观变迁集合 $T_o = \{t_2, t_3, t_4, t_5\}$, 故障变迁集合 $T_c = \{t_1\}$; 可观变迁的标签为 $I(t_2) = I(t_3) = a, I(t_4) = I(t_5) = b$ 。可达标识为 $\mathbf{M}_0 = [1, 0, 0, 0]^T, \mathbf{M}_1 = [0, 1, 0, 0]^T, \mathbf{M}_2 = [0, 0, 0, 1]^T, \mathbf{M}_3 = [0, 0, 1, 0]^T$, 其无故障子网如图 2 所示。

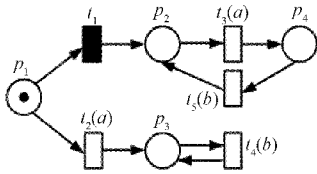


图 1 一个标签 Petri 网

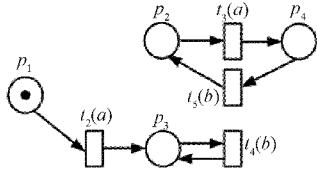


图 2 标签 Petri 网的无故障子网

2 显示可达图

可达图 (reachability graph, RG) 既能分析 Petri 网系统的状态变化, 还能描述到达系统状态的变迁序列, 因此常作为分析有界 Petri 网的工具。给定一个初始标识为 \mathbf{M}_0 的有界 Petri 网, $R(N, \mathbf{M}_0)$ 是标识集。根据有界 Petri 网的可达性, 以为 $R(N, \mathbf{M}_0)$ 节点集合构成一个有向图, 称为可达图。

本节在可达图的基础上提出显示可达图 (visible reachability graph, VRG) 的概念。显示可达图与可达图的结构一致, 唯一区别在于显示可达图能够识别不可观测的故障变迁。本节根据以下定义设计算法并构建有界标签 Petri 网的显示可达图, 如算法 1 所示。

定义 1 有界 Petri 网的显示可达图是一个有限状态自动机 $G = (Q, D, \Delta, q_0)$, 其中:

- 1) $Q = R(N, \mathbf{M}_0)$ 有限状态集合;
- 2) $\Delta \subseteq Q \times D_c \times Q$ 表示自动机两个状态之间变迁关系, 其中 $D_c = D \cup \{e\}$;
- 3) q_0 表示自动机的初始状态。

算法 1 显示可达图构建算法

输入: 有界标签 Petri 网;

输出: 显示可达图;

```

1 以  $\mathbf{M}_0$  为显示可达图的首个节点, 并标注为“新”;
2  while 存在标注为“新”的节点时 do
3  选择一个标注“新”的节点, 设定为  $\mathbf{M}$ ;
4   if 在节点  $\mathbf{M}$  下满足存在可使得的变迁  $t$  then
5  计算  $\mathbf{M}' = \mathbf{M} + [A](\cdot, t)$ ;
6  if 显示可达图中不存在节点  $\mathbf{M}'$  then
7  在显示可达图中加入状态  $\mathbf{M}'$ ;
8  从  $\mathbf{M}$  到  $\mathbf{M}'$  添加一条有向弧;
9   if  $t \in T_c$  then
10     在有向弧旁边标为  $t$ ;
11  end if
12  if  $t \in T_o$  then
13     在有向弧旁边标为  $t(b)$ , 其中  $b = I(t)$ ;
14  end if
15  end if
16  end if
17  删去节点的“新”标注;
18  给  $\mathbf{M}$  节点标注为“旧”, 给节点标注为“新”;
19  end while
20  删除所有状态标号。
    
```

例 2 考虑例 1 中有界标签 Petri 网模型及其无故障子网, 执行算法 1 可构建 Petri 网的显示可达图 $G = (Q, D, \Delta, q_0)$ 和无故障子网的显示可达图 $G^E = (Q^E, D^E, \Delta^E, q_0^E)$, 如图 3 和 4 所示; 其中 $q_0 = \mathbf{M}_0$ 为初始状态, 故障变迁为 t_1 。

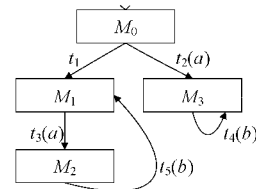


图 3 有界 Petri 的显示可达图

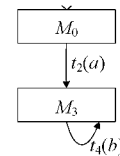


图 4 无故障子网的显示可达图

3 系统边界可诊断性的验证算法

本节假设在故障发生后无死锁状态, 首先给出有界标签 Petri 网满足边界可诊断性的定义; 再次, 提出 T 验证器和有界 Petri 网满足边界可诊断性的充要条件。

定义 2 一个有界标签 Petri 网 (N, \mathbf{M}_0, I) 和一个正整数 K 值, 如果满足:

$$[\forall \sigma' \in \Phi(T_c)], [\forall \sigma'' \in L(N, \mathbf{M}_0)/\sigma'],$$

$$[|\sigma''| \geq K] \Rightarrow \forall \sigma \in I^{-1}(I(\sigma' \sigma'')), [\exists T_c \cap \sigma \neq \emptyset]$$

(7)

则系统具有边界可诊断性。

根据定义 2, 一个有界 Petri 网满足边界可诊断性当且仅当系统中不存在两条变迁序列 $\sigma, \sigma' \in L(N, \mathbf{M}_0)$ 满足以下条件:

- 1) σ 包含故障变迁, σ 发生故障后的变迁序列长度为 K ;
- 2) σ' 不包含故障变迁;
- 3) σ 和 σ' 观测值相同, 即 $I(\sigma) = I(\sigma')$ 。

T 验证器是一个有限状态自动机 $Z = (Q^Z, D^Z, \Delta^Z, q_0^Z)$, 其构建算法如算法 2 所示。

命题 1 给定一个有界标签 Petri 网 N , 令 N' 表示无故障子网, 若 T 验证器由初始状态 q_0^Z 经过路径 $\sigma^Z = (\sigma_1, \sigma_2)$ 到达 $q^Z = (q, l; q^Z)$ 状态, 则:

- 1) $\sigma_1 \in L(N, \mathbf{M}_0), \sigma_2 \in L(N', \mathbf{M}_0)$;
- 2) $I(\sigma_1) = I(\sigma_2)$;
- 3) σ_1 包含故障变迁, $l = Y$ 表示系统正常运行;
- 4) σ_1 不包含故障变迁, $l = E$ 表示系统发生故障;
- 5) 令 X_E 表示所有含 $l = E$ 的状态集合, 即 $X_E \subseteq Q^Z$ 。

定义 3 给定一个验证器 $Z = (Q^Z, D^Z, \Delta^Z, q_0^Z)$, 在 E 状态集合中 $x, x' \in X_E, x = (q_1, E; q_1^E)$ 经过 i 个路径均可达到状态 $x' = (q_2, E; q_2^E)$, 其中 $i \in \mathbb{N}^+$ 为正整数, $\sigma_i^Z = (\sigma_1^i, \sigma_2^i)$ 且 $\sigma_i^Z \in (D^Z)^*$ 表示两个含 E 状态之间所经过第 i 个路径, 则两个含 E 状态之间在 Petri 网中所对应的变迁序列长度最大值的定义为:

$$J(x) = \max_i |\sigma_i^Z| \quad (8)$$

σ_i^Z 表示 $x, x' \in X_E$ 两个状态之间在 Petri 网中所对应的变迁序列; 若 x 状态经过路径 σ_i^Z 又达到该状态, 形成一条回路, 则称这条回路为 E 回路。

算法 2 执行步骤如下:

行 1 至行 14 运行结束后需要删除自动机状态集合 Q^Z 中不能由初始状态 q_0^Z 可达的状态。在执行过程中, 当 $t \in T_c$, Petri 网中 $(q_1, t, q_2) \in \Delta$ 状态变化, 则在验证器中有 $((q_1, l; q_1^E)(t, \epsilon)(q_2, E; q_2^E)) \in \Delta^Z$, 其中“E”表示系统中故障变迁已经发生。当 $t_1, t_2 \in T_a, I(t_1) = I(t_2)$, Petri 网中状态 $(q_1, t_1, q_2) \in \Delta$ 及其无故障子网状态 $(q_1^E, t_2, q_2^E) \in \Delta^E$ 均变化, 则在验证器有 $((q_1, l; q_1^E)(t_1, t_2)(q_2, l; q_2^E)) \in \Delta^Z$, 其中“ $l = Y$ ”表示系统正常运行。

行 15 至行 24 对有界标签 Petri 网的边界可诊断性进行判断: 若验证器中出现 E 回路, 此时输出即网系统为不可诊断。若验证器中无 E 回路, 对于所有的 E 状态执行: 计算两个含 E 状态所经过路径之间在 Petri 网所对应的变迁序

算法 2 T 验证器构建算法

输入: 有界标签 Petri 网;

输出: T 验证器 $Z = (Q^Z, D^Z, \Delta^Z, q_0^Z)$, 边界值 K ;

- 1 由算法 1 构建 Petri 网的显示可达图 $G = (Q, D, \Delta, q_0)$;
- 2 由算法 1 构建无故障子网的显示可达图 $G^E = (Q^E, D^E, \Delta^E, q_0^E)$;
- 3 令 $Q^Z = q \times \{Y, E\} \times q^E$;
- 4 令 $D^Z = (T_a \times T_c) \times (T_a \times \{\epsilon\})$;
- 5 令 $q_0^Z = (q_0, Y; q_0^E)$;
- 6 $\Delta^Z = q^Z \times D^Z \times q^Z$ 计算过程如下:
- 7 if $t \in T_c, (q_1, t, q_2) \in \Delta$ then
- 8 $((q_1, l; q_1^E)(t, \epsilon)(q_2, E; q_2^E)) \in \Delta^Z$;
- 9 end if
- 10 if $t_1, t_2 \in T_a, I(t_1) = I(t_2)$ 且 $(q_1^E, t_2, q_2^E) \in \Delta^E, (q_1, t_1, q_2) \in \Delta$ then
- 11 $((q_1, l; q_1^E)(t_1, t_2)(q_2, l; q_2^E)) \in \Delta^Z$;
- 12 end if
- 13 删除不能从初始状态到达的状态。
- 14 while $\forall x, x' \in X_E, x$ 状态经过路径 $\sigma_i^Z = (\sigma_1^i, \sigma_2^i)$ 达到状态 x' do:
- 15 求解两个状态之间在 Petri 网所对应的变迁序列长度 $|\sigma_i^Z|$;
- 16 if $x = x'$ 且 $|\sigma_i^Z| \neq 0$ then
- 17 $w = -1$;
- 18 break
- 19 if $x = x'$ 且 $|\sigma_i^Z| = 0$ 或 $x \neq x'$ then
- 20 $J(x) = \max_i |\sigma_i^Z|$;
- 21 end if
- 22 end while
- 23 $w = \max_{x \in X_E} J(x)$;
- 24 $K = 1 + w$ 。

列长度最大值为 $J(x)$ 。

综上所述, 选取所有 E 状态经过路径在 Petri 网所对应的变迁序列长度最大值 $w = \max_{x \in X_E} J(x)$, 即满足网系统可诊断性的边界值为 $K = 1 + \max_{x \in X_E} J(x)$ 。

命题 2 有界标签 Petri 网满足边界可诊断性当且仅当其验证器中任意两个 E 状态经过路径在 Petri 网中所对应的变迁序列长度最大值均小于正整数 K 。

证明: 根据定义 2, 一个有界 Petri 网满足边界可诊断性当且仅当系统中不存在两条变迁序列 $\sigma, \sigma' \in L(N, \mathbf{M}_0)$ 满足以下条件:

- 1) σ 含故障变迁, 且故障变迁发生后的变迁序列长度为 K ;

- 2) σ' 不含故障变迁;
- 3) σ 和 σ' 观测值相同, 即 $I(\sigma) = I(\sigma')$ 。

由定义 3 和命题 1 可得: 在验证器中任意两个 E 状态之间变迁序列长度值均小于 K 值。首先, 给定的标签 Petri 网是有界的, 则验证器中的状态是有限个。路径 σ_i^z 为任意长当且仅当序列构成一条 E 回路; 其次, 求解任意两个含 E 状态经过路径在 Petri 网中所对应的变迁序列长度最大值均满足小于 K 值, 则有界标签 Petri 网是边界可诊断的。综上所述, 有界标签 Petri 网满足边界可诊断性只需验证器中任意两个 E 状态经过路径在 Petri 网中所对应的变迁序列长度值均小于正整数 K 即可。证毕。

例 3 例 1 中 Petri 网执行算法 2 可得, 网系统的 T 验证器, 如图 5 所示。

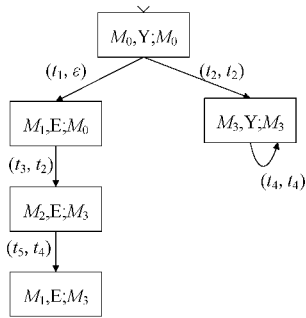


图 5 例 1 中 Petri 网构建的 T 验证器

初始标识 $q_0^z = (M_0, Y; M_0)$, 故障变迁发生后 $X_E = \{(M_1, E; M_0), (M_2, E; M_3), (M_1, E; M_3)\}$, 没有出现 E 回路。 X_E 中除下文所述 3 种情况外, 其余的任意两种状态均为不可达。

当状态 $(M_1, E; M_0)$ 经过路径 1 (t_3, t_2) 到达状态 $(M_2, E; M_3)$ 时, 两个状态经过路径 1 在 Petri 网中对应的变迁序列长度最大值为 1; 当状态 $(M_2, E; M_3)$ 经过路径 2 (t_5, t_4) 到达状态 $(M_1, E; M_3)$ 时, 两个状态经过路径 2 在 Petri 网中对应的变迁序列长度最大值为 1; 当状态 $(M_1, E; M_0)$ 经过路径 3 $(t_3, t_2) (t_5, t_4)$ 到达状态 $(M_1, E; M_3)$ 时, 两个状态经过路径 3 在 Petri 网中的对应变迁序列长度最大值为 2; 网系统的边界值为一个正整数 $K = 1 + \max_{x \in X_E} J(x) = 3$, 故例 1 的网系统具有 3-可诊断性。

4 实例分析

4.1 案例分析

如图 6 所示, 圆柱孔特征加工的加工单元可抽象为一个有界标签 Petri 网模型^[22]。

库所和变迁分别为 $P = (p_1, p_2, p_3, p_4, p_5, p_6), T = (t_1, t_2, t_3, t_4, t_5)$, 库所和变迁的物理意义如表 1 和表 2 所示。初始标识为 $M_0 = [2, 0, 0, 0, 1, 2]^T$, 库所 p_1 有两个托肯, 对应两个托盘; 库所 p_3 有一个托肯, 对应于钻床可工作; 库所 p_6 有两个托肯, 对应于缓冲区有两个空位。

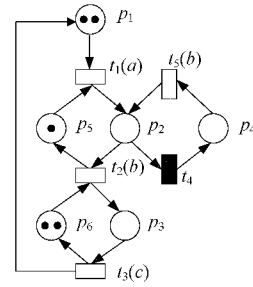


图 6 Petri 网模型

表 1 库所物理意义

库所	物理意义
p_1	托盘就绪
p_2	钻床加工
p_3	缓冲区工件就绪可用
p_4	钻床维修
p_5	钻床可用
p_6	缓冲区有空位

表 2 变迁物理意义

变迁	物理意义
t_1	运送平台 1 装载工件至钻床
t_2	钻床加工并由运送平台 1 卸载工件
t_3	运送平台 2 装载工件并在镗床加工
t_4	钻床发生故障
t_5	钻床维修

标签函数 $I(t_1) = a, I(t_2) = I(t_5) = b, I(t_3) = c$, 其中, 故障变迁集为 $T_e = \{t_4\}$ 表示钻床发生故障。网系统的可达标识集, 如表 3 所示。

表 3 可达标识集

状态	标识
M_0	$[2, 0, 0, 0, 1, 2]^T$
M_1	$[1, 1, 0, 0, 0, 2]^T$
M_2	$[1, 0, 1, 0, 1, 1]^T$
M_3	$[0, 1, 1, 0, 0, 1]^T$
M_4	$[0, 0, 2, 0, 1, 0]^T$
M_5	$[1, 0, 0, 1, 0, 2]^T$
M_6	$[0, 0, 1, 1, 0, 1]^T$

执行算法 1 可得, 有界标签 Petri 网的显示可达图 G 及其无故障子网的显示可达图 G^E , 分别如图 7 和 8 所示。

执行算法 2 可得, Petri 网模型的 T 验证器, 如图 9 所示, 其中初始标识为 $q_0^z = (M_0, Y; M_0)$ 。

由验证器可得: 故障变迁发生后, 出现含 E 状态为 $X_{E1} = \{(M_5, E; M_1), (M_1, E; M_2), (M_5, E; M_2)\}$ 和

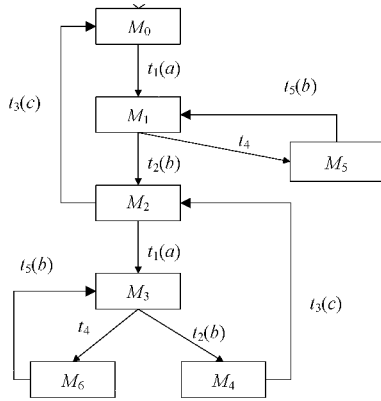


图 7 Petri 网的显示可达图

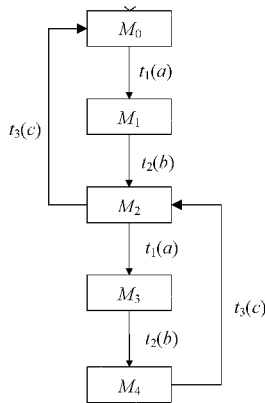


图 8 无故障子网的显示可达图

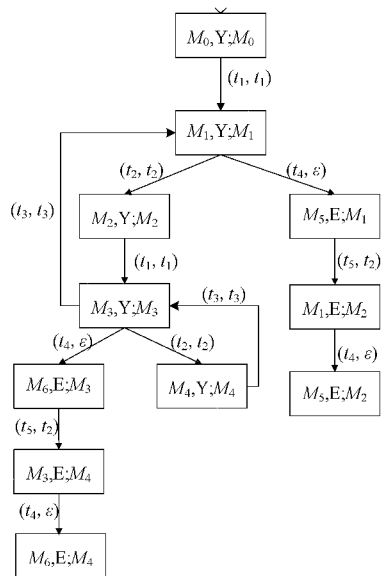


图 9 图 6 中 Petri 网构建的 T 验证器

$X_{E2} = \{(M_6, E; M_3), (M_3, E; M_4), (M_6, E; M_4)\}$, 其中没有出现 E 回路。在 X_{E1} 和 X_{E2} 中除下文所述 3 种情况外, 其余的任意两种状态均为不可达。

当状态 $(M_5, E; M_1)$ 经过路径 1 (t_5, t_2) 到达状态至

$(M_1, E; M_2)$ 时, 两个状态经过路径 1 在 Petri 网中对应变迁序列长度最大值为 1; 当状态 $(M_1, E; M_2)$ 经过路径 2 (t_4, ϵ) 到达状态 $(M_5, E; M_2)$ 时, 两个状态经过路径 2 在 Petri 网中对应变迁序列长度最大值为 1; 当状态 $(M_5, E; M_1)$ 经过路径 3 $(t_5, t_2) (t_4, \epsilon)$ 到达状态 $(M_5, E; M_2)$ 时, 两个状态经过路径 3 在 Petri 网中对应变迁序列长度最大值为 2。

当状态 $(M_6, E; M_3)$ 经过路径 4 (t_5, t_2) 到达状态 $(M_3, E; M_4)$ 时, 两个状态经过路径 4 在 Petri 网中对应变迁序列长度最大值为 1; 当状态 $(M_3, E; M_4)$ 经过路径 5 (t_4, ϵ) 至 $(M_6, E; M_4)$ 时, 两个状态经过路径 5 在 Petri 网中对应变迁序列长度最大值为 1; 当状态 $(M_6, E; M_3)$ 经过路径 6 $(t_5, t_2) (t_4, \epsilon)$ 至 $(M_6, E; M_4)$ 时, 两个状态经过路径 6 在 Petri 网中对应变迁序列长度最大值为 2。

因此, 网系统的边界值为一个正整数 $K = 1 + \max_{x \in X_E} J(x) = 3$, 故网系统具有 3-可诊断性。

4.2 仿真分析

实例首先利用 Petri 网对圆柱孔特征加工的加工系统进行建模, 并给出了 Petri 网模型中各库所和变迁的含义; 其次通过构建显示可达图的定义和算法, 即实例中所对应的 Petri 网及无故障子网的显示可达图, 根据算法 1 可分别如图 7 和 8 所示; 最后, 提出一种基于 Petri 网的边界可诊断性验证方法并构建如图 9 所示的验证器, 根据算法 2 求解出满足边界可诊断的边界值。

通过仿真分析可得实例所对应 Petri 网系统满足边界可诊断时, 任意两个可达 E 状态之间变迁序列长度最大值, 如图 10 所示。对于系统为边界可诊断所对应的边界值, 即所有任意两个可达 E 状态之间变迁序列长度最大值再加 1。

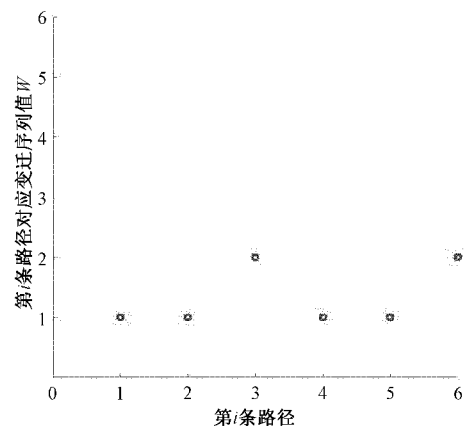


图 10 第 i 条路径对应长度值

图中横坐标是验证器中任意两个能够可达的 E 状态所经过第 i 条路径, 纵坐标是任意两个 E 状态经过第 i 条路径在 Petri 网中对应变迁序列长度值 $\omega = \{1, 1, 2, 1, 1, 2\}$, ω 值的详细描述如下文所述。

对于任意两个可达的 E 状态中,当状态 $(M_5, E; M_1)$ 到达状态 $(M_1, E; M_2)$ 时,经过路径 1 在 Petri 网中对应变迁序列长度最大值为 1,即 $w_1 = 1$;当状态 $(M_1, E; M_2)$ 到达状态 $(M_5, E; M_2)$ 时,经过路径 2 在 Petri 网中对应变迁序列长度最大值为 1,即 $w_2 = 1$;当状态 $(M_5, E; M_1)$ 到达状态 $(M_5, E; M_2)$ 时,经过路径 3 在 Petri 网中对应变迁序列长度最大值为 2,即 $w_3 = 2$;当状态 $(M_6, E; M_3)$ 到达状态 $(M_3, E; M_4)$ 时,经过路径 4 在 Petri 网中对应变迁序列长度最大值为 1,即 $w_4 = 1$;当状态 $(M_3, E; M_4)$ 至状态 $(M_6, E; M_4)$ 时,经过路径 5 在 Petri 网中对应变迁序列长度最大值为 1,即 $w_5 = 1$;当状态 $(M_6, E; M_3)$ 至状态 $(M_6, E; M_4)$ 时,经过路径 6 在 Petri 网中对应变迁序列长度最大值为 2,即 $w_6 = 2$ 。

由定义 2 和命题 2 可得,满足 Petri 网边界可诊断的边界值为一个正整数且大于所有 E 状态在 Petri 网所对应的长度值,故边界值为 3。

关于验证实例是否满足边界可诊断性这一问题,是根据本文所提的一种基于 Petri 网的边界可诊断性验证方法来实现。该方法具有有效性和实用性两个优点:首先,该方法与文献[20]中基于时序约束的自动机模型构建的诊断器相比较,计算过程更为简便。此外,该方法构建一个可诊断性的验证器并能求解该系统可诊断性的边界值,适用范围较为广泛。其次,该方法将实例中故障建模为 Petri 网中的变迁相比于文献[21]中以故障作为 Petri 网中的库所更加贴合实际工业应用。

5 结 论

本文提出一种基于有界 Petri 的离散事件系统边界可诊断性的验证方法。首先将系统抽象为 Petri 网,并构建有界 Petri 网及其无故障子网所对应的显示可达图,并将显示可达图转化为有限状态自动机;其次,构建一个验证器对有界 Petri 网及其无故障子网的显示可达图进行并行分析,验证有界 Petri 网故障发生后是否具有边界可诊断性,并求解所对应的边界值;最后,通过实例验证和仿真分析表明本文所提方法的实用性和有效性。

本文提出的边界可诊断性验证方法在系统故障无死锁的假设下有效,这一假设在一定程度上影响该方法的应用范围。下一步将研究含死锁状态的 DES 边界可诊断性验证方法。

参考文献

- [1] 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[J]. 控制理论与应用, 2017, 34(6): 717-722.
- [2] 阙蔡雄,刘富春,赵锐,等. 基于 Petri 网诊断器的离散事件系统模式故障的在线诊断[J]. 控制理论与应用, 2020, 37(7): 1621-1627.
- [3] 刘富春,曹越,赵锐,等. 离散事件系统最小故障诊断基的求解与应用[J]. 信息与控制, 2020, 49(5): 521-526, 535.
- [4] 叶丹丹,罗继亮. 部分可观 Petri 网结构信息在故障诊断中的应用[J]. 控制理论与应用, 2015, 32(3): 366-373.
- [5] 郝晋渊,孙丹丹,郝真鸣,等. 基于标签 Petri 网的自动制造系统初始资源配置优化[J]. 电子测量与仪器学报, 2020, 34(8): 30-36.
- [6] 曾倩,袁海文,张莉,等. 测试系统多智能体建模技术及应用[J]. 仪器仪表学报, 2012, 33(6): 1427-1434.
- [7] 欧阳丹彤,罗知雨,耿雪娜,等. 分布式离散事件系统的安全可诊断性算法[J]. 吉林大学学报(理学版), 2018, 56(3): 594-600.
- [8] 郝真鸣,李承旺,张超岩,等. 一种有界 Petri 网的可诊断性验证方法[J]. 河北大学学报(自然科学版), 2022, 42(1): 8-15.
- [9] 钱伟伟,王有远,张振华. 基于使用阈值和时间有色 Petri 网的任务与资源分配研究[J]. 组合机床与自动化加工技术, 2019, (2): 154-156, 160.
- [10] PAIVA P, CARVALHO L K, BASILIO J C. Diagnosability and online diagnosis of discrete-event systems modeled by acyclic labeled Petri nets[J]. Ifac Papersonline, 2017, 50(1): 13630-13635.
- [11] MA Z, ZHOU H, LI Z, et al. Design of Monitor-based Supervisors in Labeled Petri Nets-ScienceDirect[J]. IFAC-PapersOnLine, 2018, 51(7): 374-380.
- [12] CHEN Y F, BARKAOUI K. Maximally permissive petri net supervisors for flexible manufacturing systems with uncontrollable and unobservable transitions [J]. Asian Journal of Control, 2015, 16(6): 1646-1658.
- [13] SAYEDMOUCHAWEH M. Discrete event systems-diagnosis and diagnosability [J]. Springerbriefs in Electrical & Computer Engineering, 2014, 44(2): 475-491.
- [14] CABASINO M P, GIUA A, LAFORTUNE S, et al. A new approach for diagnosability analysis of petri nets using verifier nets [J]. Automatic Control, IEEE Transactions on, 2012, 57(12): p. 3104-3117.
- [15] CABASINO M P, GIUA A, POCCI M, et al. Discrete event diagnosis using labeled Petri nets. An application to manufacturing systems [J]. Control Engineering Practice, 2011, 19(9): 989-1001.
- [16] CABASINO M P, GIUA A, LAFORTUNE S, et al. A new approach for diagnosability analysis of petri nets using verifier nets [J]. IEEE Transactions on Automatic Control, 2012, 57(12): 3104-3117.
- [17] KODAMA A, NISHI T. Petri net representation and

- reachability analysis of 0-1 integer linear programming problems [J]. Information Sciences, 2017, 400: 157-172.
- [18] VIANA G, MOREIRA M V, BASILIO J C. Codiagnosability analysis of discrete-event systems modeled by weighted automata[J]. IEEE Transactions on Automatic Control, 2019, DOI: 10.1109/TAC.2019.2897268.
- [19] RAN N, SU H, GIUA A, et al. Codiagnosability analysis of bounded petri nets[C]. IEEE Transactions on Automatic Control, 2018, DOI: 10.1109/tac.2017.2742659.
- [20] 廖盟. 离散事件动态系统的若干故障诊断问题研究[D]. 武汉: 华中科技大学, 2017, DOI: 10.7666/d.D01311499.
- [21] RAMIREZ-TREVINO A, RUIZ-BELTRAN E, ARAMBURO-LIZARRAGA J, et al. Structural diagnosability of DES and design of reduced petri net diagnosers[J]. IEEE Transactions on Systems Man & Cybernetics Part A Systems & Humans, 2012, 42(2): 416-429.
- [22] 苏永胜. 基于 Petri 网的机械产品装配与工艺设计缺陷辨识模型与方法研究[D]. 成都: 电子科技大学, 2013, DOI: CNKI:CDMD:2.1013.330433.

作者简介

冉宁, 博士, 副教授, 主要研究方向为智能系统与控制、系统优化等。

E-mail: ranning87@hotmail.com

李婷婷, 硕士研究生, 主要研究方向为智能系统、系统优化等。

E-mail: 1099170213@qq.com

张照彦, 博士, 副教授, 主要研究方向为电网故障诊断。

E-mail: zhangzhaoyan@hbu.edu.cn

郝晋渊(通信作者), 硕士, 讲师, 主要从事人工智能、信息技术、新媒体传播等。

E-mail: hjy@hbu.edu.cn