软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2017,28(5):1091−1106 [doi: 10.13328/j.cnki.jos.005212]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

不确定观测下离散事件系统的可诊断性*

文习明[1,2], 余 泉[3,2], 常 亮[2], 王 驹[2]

[1](广东省委党校 信息技术教研部,广东 广州 510053)

[2](广西可信软件重点实验室(桂林电子科技大学),广西 桂林 541004)

[3](贵州省黔南师范学院 数学与统计学院,贵州 都匀 558000)

通讯作者: 文习明, E-mail: wenxim@mail2.sysu.edu.cn

摘 要: 从系统诊断的角度来看,可诊断性是离散事件系统的一个重要性质.其要求系统发生故障后经过有限步的观测可以检测并隔离故障.为简单起见,对离散事件系统可诊断性的研究大都假定观测是确定的,即观测到的事件序列与系统实际发生的可观测事件序列一致.而在实际应用中,由于感知器的精度、信息传输通道的噪声等原因,所获取的观测往往是不确定的.重点研究观测不确定条件下离散事件系统的可诊断性问题.首先扩展了传统可诊断性的定义,定义了观测不确定条件下的可诊断性;然后,分别给出各类观测不确定条件下的可诊断性判定方法;在更一般的情况下,各类观测不确定可能共同存在,因此,最后给出一般情况下的可诊断性判定方法.

关键词: 不确定观测;离散事件系统;可诊断性

中图法分类号: TP311

中文引用格式: 文习明,余泉,常亮,王驹.不确定观测下离散事件系统的可诊断性.软件学报,2017,28(5):1091−1106. http://www.jos.org.cn/1000-9825/5212.htm

英文引用格式: Wen XM, Yu Q, Chang L, Wang J. Diagnosability of discrete-event systems with uncertain observations. Ruan Jian Xue Bao/Journal of Software, 2017,28(5):1091−1106 (in Chinese). http://www.jos.org.cn/1000-9825/5212.htm

Diagnosability of Discrete-Event Systems with Uncertain Observations

WEN Xi-Ming[1,2], YU Quan[3,2], CHANG Liang[2], WANG Ju[2]

[1](Department of Information Technology, Guangdong Institute of Public Administration, Guangzhou 510053, China)

[2](Guangxi Key Laboratory of Trusted Software (Guilin University of Electronic Technology), Guilin 541004, China)

[3](School of Mathematics and Statistics, Qiannan Normal College for Nationalities, Duyun 558000, China)

Abstract: Diagnosability is an important property of discrete-event system (DES) from the perspective of diagnosis. It requires that every fault can be detected and isolated within a finite number of observations after its occurrence. In numerous literatures, diagnosability is studied under the assumption that an observation is certain, i.e., the observation corresponds to the sequence of observable events exactly taking place in the DES. But in practical applications, the assumption may become inappropriate. Due to various reasons such as the precision of sensors and noises in transmission channels, the available observation may be uncertain. This paper focuses on the diagnosability of DESs with uncertain observations. It extends the definition of diagnosability to cope with uncertain observations. Methods are given to check the diagnosability with three types of uncertain observations accordingly. In a more general scenario where

* 基金项目: 国家自然科学基金(61603152, 61463044, 61363030); 广西可信软件重点实验室研究课题(KX201604, KX201606, KX201419, KX201330); 贵州省科技厅项目(LH[2014]7421); 广西自然科学基金(2015GXNSFAA139285)

Foundation item: National Natural Science Foundation of China (61603152, 61463044, 61363030); Research Program of Guangxi Key Laboratory of Trusted Software (KX201604, KX201606, KX201419, KX201330); Scientific Research Fund of Guizhou Provincial Science and Technology Department (LH[2014]7421); Guangxi Natural Science Foundation (2015GXNSFAA139285)

收稿时间: 2016-07-15; 修改时间: 2016-09-25; 采用时间: 2016-12-07; jos 在线出版时间: 2017-01-20

CNKI 网络优先出版: 2017-01-20 16:06:35, http://www.cnki.net/kcms/detail/11.2560.TP.20170120.1606.008.html

multiple uncertainties exist in the observation, a method is also provided to check the diagnosability with all the uncertainties of the observation together.

Key words: uncertain observation; discrete-event system; diagnosability

离散事件系统诊断是一种基于模型诊断(model-based diagnosis,简称 MBD)的动态方法[1,2].通常采用有限状态自动机(finite state machine,简称 FSM)对离散事件系统(discrete-event system,简称 DES)[3]进行建模,结合实际观测,推理得到系统的诊断结果.通过诊断,可以判断实际系统运行是否正常;若有故障发生,则定位故障和确定故障类型,从而有助于及时排除故障,保障系统的正常运行.文献[4,5]分别对 MBD 和离散事件系统诊断的研究现状和进展进行了系统阐述.

离散事件系统诊断通常基于两个假定前提:系统模型的完备性和可诊断性,保证系统得到诊断结果的唯一性和正确性[6].系统模型的完备性前提是指:系统全部可能的行为均被包含在系统模型中.对于一些复杂的实际系统,建立完备的模型往往非常困难,因此,一些学者对系统不完备情况下的诊断展开了研究[6−9].

离散事件系统的可诊断性前提是指:在获得足够多的观测后,任意故障的发生均能够被唯一地判定.文献[1,10]分别从不同角度给出了离散事件系统可诊断性的定义.文献[10]从状态识别(state identification)的角度来讨论可诊断性,分别定义了离线(off-line)可诊断性和在线(on-line)可诊断性,并给出了判定方法.文献[1]从事件发觉(event detection)的角度来讨论可诊断性,分别定义了可诊断性和 I-可诊断性,并给出了判定方法.在文献[1]中,依据系统模型构建诊断器(diagnoser),该诊断器一方面完成诊断的任务,另一方面也用于判定可诊断性.其判定算法的时间复杂度是系统状态数的指数倍和故障类型数的双重指数倍.文献[11]对文献[1]中方法进行了改进,通过构造预诊断器,然后利用预诊断器的同步来判断可诊断性,该方法通常被称为双树(twin-plant)方法,其将可诊断性判定的效率由指数级降为多项式级,即系统状态数的四次方.

对于离散事件系统诊断和可诊断性的研究,出于简单性考虑,大都假定系统观测是确定的.即系统发生一系列行为后,在线观测系统能够准确获取可观测事件的信息,包括什么事件发生了以及这些事件发生的先后次序.但在实际应用中,由于信息传输以及感知器的精度等原因,往往很难获取到确定的观测信息,这给系统诊断和可诊断性判定带来了困难.因此,一些学者展开了不确定观测条件下离散事件系统诊断和可诊断性的研究.在文献[12]中,Lamperti 等人将观测不确定分为 4 类:时序不确定、丢失不确定、逻辑不确定和来源不确定,并提出各类观测不确定条件下的诊断方法,但并未对其可诊断性展开研究.Grastien 等人在文献[13,14]中分别考虑了观测部分有序(即时序不确定)离散事件系统的可诊断性和诊断问题.Su 等人在文献[15]中给出了时序不确定和逻辑不确定条件下离散事件系统可诊断性的判定方法.

本文重点对观测不确定条件下离散事件系统的可诊断性问题展开研究.可诊断性是诊断系统一个非常重要的性质,其保障诊断结果的正确性和唯一性.离散事件系统的诊断依赖于对实际系统的建模和实际观测,而实际观测的不确定会严重影响系统的可诊断性.通过采用更精密的感知器或更可靠的信息传输通道,在一定程度上可以消除一部分观测不确定,但这样花费的成本往往非常高.因此,对观测不确定条件下的可诊断性研究具有现实意义.

本文第 1 节给出离散事件系统诊断和可诊断性的相关概念和定义以及可诊断性的判定方法.第 2 节介绍各类观测不确定,并创新形式化其对实际观测的影响.第 3 节扩展传统可诊断性的定义,给出观测不确定条件下的可诊断性定义,并分别给出各类观测不确定条件下的可诊断性判定方法,证明其正确性.第 4 节提出各类观测不确定同时存在的情况下,可诊断性的判定方法.第 5 节对观测不确定条件下可诊断性判定的时间复杂度进行分析.第 6 节给出相关工作的比较分析.第 7 节总结本文的工作,并对未来进一步可能的研究进行展望.

1 离散事件系统的可诊断性

1.1 离散事件系统诊断

离散事件系统是由异步、突发的事件驱动状态演化的动态系统,其状态只取有限个离散值[3].通常采用有限

状态自动机对离散事件系统进行建模.

定义 1(离散事件系统模型)[1]. 离散事件系统模型通常用有限状态自动机 $G=(X,\Sigma,\delta,x_0)$来表示,其中,X 是有限状态集合,Σ是可能发生的有限事件集合,$\delta\subseteq X\times\Sigma\times X$ 是有限状态转移集合,x_0 是初始状态.

自动机状态在事件触发下的转移序列称为路径,记为 $p=(x_1,e_1,x_2,\ldots,e_{n-1},x_n)$,任意 $i\in\{1,\ldots,n-1\}$,有$(x_i,e_i,x_{i+1})\in\delta$.若 $x_1=x_n$,则称为环路.事件序列称为轨迹,记为$\sigma=e_1e_2\ldots e_{n-1}$.$|\sigma|$表示轨迹的长度,即轨迹中事件的个数.$\varepsilon$表示空轨迹,$\Sigma^*$表示$\Sigma$中所有有限事件序列(包含$\varepsilon$)的集合.从初始状态开始所有轨迹的集合称为自动机语言,记为 $L(G)$.显然,$L(G)\subseteq\Sigma^*$且前缀封闭.$L(G,x)\subseteq L(G)$表示终止于状态 x 的语言.

根据事件性质,将事件集合Σ划分为 3 个独立子集:Σ_o 是可观测事件集,Σ_u 是正常(不可观测)事件集,Σ_f 是故障(不可观测)事件集.观测函数 $P_o:\Sigma^*\to\Sigma_o^*$,记录系统轨迹中可观测事件序列,具体定义如下:

$$P_o(\sigma)=\sigma,\sigma\in\Sigma_o,\quad P_o(\sigma)=\varepsilon,\sigma\in\Sigma-\Sigma_o,$$
$$P_o(\varepsilon)=\varepsilon,\qquad P_o(\sigma e)=P_o(\sigma)P_o(e),\sigma\in\Sigma^*,e\in\Sigma.$$

类似地,故障函数 $P_f:\Sigma^*\to 2^{\Sigma_f}$,记录系统轨迹中故障事件的集合,具体定义如下:

$$P_f(\sigma)=\{\sigma\},\sigma\in\Sigma_f,\quad P_f(\sigma)=\varnothing,\sigma\in\Sigma-\Sigma_f,$$
$$P_f(\varepsilon)=\varnothing,\qquad P_f(\sigma e)=P_o(\sigma)\cup P_o(e),\sigma\in\Sigma^*,e\in\Sigma.$$

定义 2(离散事件系统诊断问题)[15]. 离散事件系统的诊断问题可表示为一个二元组(G,O),其中,G 是 DES 的模型;O 是观测,即系统运行时实际观测到的事件序列.

定义 3(候选诊断)[15]. 离散事件系统诊断问题(G,O)的候选诊断是一个二元组 $(x,F)\in X\times 2^{\Sigma_f}$,$x$ 是系统状态;F 是故障(事件)集,其满足条件:$\exists\sigma\in L(G,x),P_o(\sigma)=O\wedge P_f(\sigma)=F$.

DES 的诊断,其实质是根据在线观测事件序列,在离线模型中寻找相容轨迹,从而推测系统所处的状态以及是否有故障发生.在一般情况下,一个诊断问题可能存在多个候选诊断.因此,其诊断结果是一个候选诊断集.如果两个候选诊断的故障集不一致,则称存在冲突.冲突候选诊断的存在,将导致无法正确检测和孤立故障.一方面,我们会采取进一步的观测,以期待排除候选诊断之间的冲突;另一方面也会问:进一步观测是否一定可以排除候选诊断之间的冲突?离散事件系统可诊断性可以回答这个问题.

1.2 离散事件系统可诊断性

文献[1]首次从事件发觉的角度来定义离散事件系统的可诊断性,其具体定义如下.

定义 4(可诊断性)[1]. 离散事件系统 $G=(X,\Sigma,\delta,x_0)$是可诊断的,当其满足如下条件:

$$(\forall f\in\Sigma_f)(\exists n\in N)(\forall\sigma\in\bar{L}_G(f))(\forall\sigma'\in L(G)/\sigma,|P_o(\sigma')|\geqslant n),$$
$$(\forall l\in L(G)),P_o(l)=P_o(\sigma\sigma')\Rightarrow l\in L_G(f).$$

其中,$L(G)/\sigma=\{\sigma'\in\Sigma^*|\sigma\sigma'\in L(G)\}$表示轨迹$\sigma$的后继语言,$L_G(f)=(\Sigma^*f\Sigma^*)\cap L(G)$表示自动机语言中包含故障 f 的轨迹集合,$\bar{L}_G(f)=(\Sigma^*f)\cap L(G)$ 表示自动机语言中所有以故障f结尾的轨迹集合.

其直观含义是:如果系统可诊断,那么任意故障发生后,只要后继经过足够长的观测(n 步的延时观测),一定能探测到该故障的发生.换句话说,任意故障发生之后,总能产生不一样的观测,使得可以诊断出其类型.

上述定义基于两个假设:(1) 系统是活的(live),即,系统的运行是不会终止的;(2) 不存在不可观测事件环路,即不存在一条环路,其所有事件均为不可观测事件[1].假设(1)是为了简化问题,经过适当调整可以放弃这一假设;假设(2)是为了保障观测的顺利进行,如果存在不可观测事件环路,系统的状态转换可能会陷入一个无穷的不可观测事件环路,进而无法正常获取观测.它们被大多数文献普遍采用[1,11,14],本文也继续沿用这两个假设.

文献[11]提出了一种可诊断性判断的多项式时间复杂度算法——双树算法.该方法的具体过程如下:(1) 构造预诊断器;(2) 将预诊断器进行自同步,得到同步自动机;(3) 在同步自动机上检测是否具有故障冲突的环路,若不存在这样的环路,则系统可诊断,否则不可诊断.接下来形式化上述过程.

定义 5(预诊断器)[11]. 离散事件系统 $G=(X,\Sigma,\delta,x_0)$的预诊断器是在 G 的基础上构造的一个非确定性有限状态自动机 $G_o=(X_o,\Sigma_o,\delta_o,x_0^o)$,其中,

- G_o的有限状态集合$X_o=\{(x,F)|x\in X_1,F\subseteq\Sigma_f\}\cup\{(x_0,\varnothing)\}$,其中,$X_1=\{x\in X|\exists(x',e,x)\in\delta,e\in\Sigma_o\}$,$G$中通过某个可观测事件发生转移所达状态的集合,$F=P_f(\sigma),\exists\sigma\in L(G,x)$,即存在从$x_0$到$x$的轨迹,$F$为该轨迹上的故障集合.
- G_o的有限事件集合为Σ_o,即G的可观测事件集合.
- G_o的有限状态转移集合$\delta_o\subseteq X_o\times\Sigma_o\times X_o,((x,F),e,(x',F'))\in\delta_o$当且仅当$G$中存在一条路径$(x,e_1,x_1,\ldots,e_n,x_n,e,x'),n\geqslant 0,P_o(e_i)=\varepsilon$,对任意$i\in\{1,2,\ldots,n\},P_o(e)=e$,而且$F'=\bigcup_{i=1}^{n}P_f(e_i)\cup F$,即状态$x$经过若干不可观测事件最后加上一个可观测事件的发生之后转移到状态x',其故障标签是在x故障标签的基础上再合并这些不可观测事件可能导致的故障.
- $x_0^o=(x_0,\varnothing)\in X_o$是$G_o$的初始状态.

从预诊断器的构造可知,其实质上是抽取出原始自动机中的可观测事件所能到达的状态,为其加上故障标签,并重建其状态转换过程而形成的新自动机.由于事件全部为可观测事件,因此通常也被称为可观测自动机.

定义 6(自同步自动机)[11]. 预诊断器$G_o=(X_o,\Sigma_o,\delta_o,x_0^o)$的自同步自动机$G_d=G_o\otimes G_o=(X_d,\Sigma_o,\delta_d,x_0^d)$,其中,

- $X_d=\{(x_1^o,x_2^o)\,|\,x_1^o,x_2^o\in X_o\}$是$G_d$的有限状态集合;
- Σ_o是可观测事件集合,其作为G_d的有限事件集合;
- $\delta_d\subseteq X_d\times\Sigma_o\times X_d$是$G_d$的有限状态转移集合,$((x_1^o,x_2^o),e,(y_1^o,y_2^o))\in\delta_d$当且仅当$(x_1^o,e,y_1^o)\in\delta_o$且$(x_2^o,e,y_2^o)\in\delta_o$;
- $x_0^d=(x_0^o,x_0^o)\in X_d$是$G_d$的初始状态.

例 1:图 1(a)为一个简单的离散事件系统模型,图中的节点表示系统状态,节点之间的有向边表示状态的转移,其中,状态集合$X=\{0,1,2,3,4,5\}$,初始状态$x_0=0$,可观测事件集合$\Sigma_o=\{a,b,c\}$,正常事件集合$\Sigma_u=\{u\}$,故障事件集合$\Sigma_f=\{f\}$.其预诊断器如图 1(b)所示,由于系统只有一个故障事件f,为简单起见,我们用$N=\varnothing$表示没有故障发生,用$F=\{f\}$表示故障f发生,后续例子中将继续采用这种方式.其自同步自动机如图 1(c)所示.根据双树算法,离散事件系统是可诊断的,因为自同步自动机的环路中都没有出现故障冲突.如果观测到事件序列abc,即可判断发生了故障;如果观测到事件序列bac,即可判断系统运行正常.

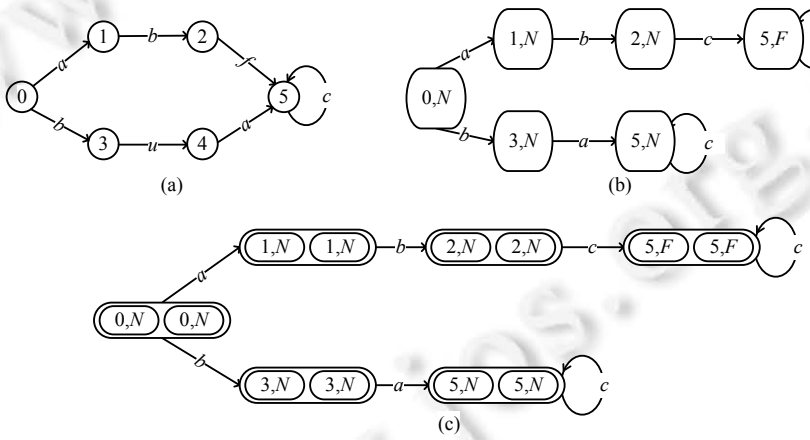


Fig.1 System model, pre-diagnoser and self-synchronized automaton

图 1 系统模型、预诊断器和自同步自动机

2 不确定观测

DES 的在线诊断,通过感知器在线观测可观测事件的发生,然后将信息传递给诊断器,诊断器在离线模型中寻找与观测相容轨迹,从而给出诊断结果.通常假定观测是确定的,即任意行为轨迹发生后,其可观测事件序列与实际观测到的事件序列一致.而在实际应用中,要获取确定观测却很困难,这极大地限制了诊断方法的适用范

围.Lamperti 和 Zanella 根据导致观测不确定的原因,将观测不确定分为 4 类:时序不确定、丢失不确定、逻辑不确定和来源不确定[12].

2.1 时序不确定

离散事件系统的事件发生是异步的,即事件的发生有严格的时间先后顺序.但在实际观测时,由于信息传输方面的原因,可能会导致事件时序的丢失,从而无法确定事件发生的先后顺序,在文献[12]中称其为时序不确定.

在文献[12]中,通过(有向无环)观测图来表示时序不确定观测.在离线判断可诊断性时,可能并无实际的观测,无法给出观测图.因此,我们假定时序不确定仅存在发生时间点临近的若干可观测事件之间.这一假定基于如下考虑:两个事件如果彼此发生的时间间隔太长,即使在传输过程中会有延时,也不足以导致时序变化.

我们用 $e\in\sigma$ 表示轨迹 σ 中包含事件 e,用 $\sigma'\subseteq\sigma$ 表示轨迹 σ' 是 σ 的子轨迹.

定义 7(相对时间). 给定离散事件系统 G 中的一条轨迹 σ,事件 $e_1,e_2\in\sigma$,它们沿轨迹 σ 发生的时间点分别为 x_1 和 x_2,则定义 $|x_1-x_2|$ 为 e_1 和 e_2 在轨迹 σ 中的相对时间,记为 $RT_\sigma(e_1,e_2)$.

相对时间的值域为[1,∞),且为整数.当相对时间为 1 时,二者连续发生.在此基础上定义时序不确定度.

定义 8(时序不确定度). 令可能丢失时序的可观测事件之间的最大相对时间为 d,时序不确定度为(d+1).

定义 9(疑似片段集). 给定离散事件系统 G 和时序不确定度 n,所有可能会丢失时序的可观测事件序列称为疑似片段集,记为

$$\Sigma_n^{//}(G)=\{\sigma'\mid(\forall e\in\sigma'.e\in\Sigma_o)\wedge(\exists e_1,e_2\in\sigma'.e_1\neq e_2)\wedge(\exists\sigma.\sigma'=P_o(\sigma)\wedge\forall e_1,e_2\in\sigma'.RT_\sigma(e_1,e_2)<n)\}.$$

由定义 9 可知,$\Sigma_1^{//}(G)=\varnothing$,对应着时序确定的情况.且 $\Sigma_{n-1}^{//}(G)\subseteq\Sigma_n^{//}(G)$,即随着时序不确定度的增长,可能丢失时序的事件片段也会增多.因此,可以通过控制时序不确定度来控制出现时序不确定的程度.在例 1 所示的离散事件系统中,$\Sigma_2^{//}(G)=\{ab,ac\},\Sigma_3^{//}(G)=\{ab,ac,ba,bc\}$.

定义 10(时序扩展). 疑似片段发生后,实际可能观测到的事件序列是其中所有原子事件的一个排列.疑似片段中所有原子事件的全排列,称为其时序扩展,记为 $E^{//}(\sigma),\sigma\in\Sigma_n^{//}(G)$.

将其扩展到任意可观测事件序列 $\sigma\in\Sigma_o^*$,可得时序扩展观测,记为 $E_o^{//}(\sigma,\Sigma_n^{//}(G))\in2^{\Sigma_o^*}$.其物理含义为:任意可观测事件序列发生后,因时序不确定(度为 n)可能观测到的事件序列集合.具体定义如下:

$$E_o^{//}(\sigma,\Sigma_n^{//}(G))=\begin{cases}\{\sigma\}, & \neg\exists\sigma'.(\sigma'\subseteq\sigma\wedge\sigma'\in\Sigma_n^{//}(G))\\ \bigcup\limits_{\sigma=\sigma_1\sigma'\sigma_2}E_o^{//}(\sigma_1,\Sigma_n^{//}(G))\times E^{//}(\sigma')\times E_o^{//}(\sigma_2,\Sigma_n^{//}(G)), & \sigma'\in\Sigma_n^{//}(G)\end{cases}.$$

其中,“×”为笛卡尔积.

易证,$E_o^{//}(\sigma,\Sigma_{n-1}^{//}(G))\subseteq E_o^{//}(\sigma,\Sigma_n^{//}(G))$.若 $E_o^{//}(\sigma,\Sigma_n^{//}(G))\cap E_o^{//}(\sigma',\Sigma_n^{//}(G))\neq\varnothing$,则表示事件序列 σ 和 σ' 可能产生相同的观测,即二者通过时序不确定观测不可区分.

2.2 丢失不确定

感知器探测到可观测事件的发生之后,将信息传输给诊断器的过程中,由于信息传输方面的原因,可能(但不一定)会导致信息丢失,从而无法确定该事件是否发生了.在文献[12]中将这种情况称为丢失不确定.

在文献[12]中,处理这类不确定观测条件下的诊断时,事先就给定了可能会丢失的可观测事件,即在允许某些事件丢失的情况下进行诊断.我们将可能会丢失的可观测事件集称为疑似丢失事件集,记为 Σ^ε.

定义 11(丢失扩展). 对任意 $e\in\Sigma^\varepsilon$,其发生之后观测到的信息可能是 e 或者 ε.令 $E^\varepsilon(e)=\{e,\varepsilon\}$,称为事件 e 的丢失扩展.

给定 Σ^ε,定义任意可观测事件序列 $\sigma\in\Sigma_o^*$ 的丢失扩展观测,记为 $E_o^\varepsilon(\sigma,\Sigma^\varepsilon)\in2^{\Sigma_o^*}$.其物理含义为:可观测事件序列发生后,因丢失不确定可能观测到的事件序列集合.具体定义如下:

$$E_o^\varepsilon(\sigma,\Sigma^\varepsilon)=\begin{cases}\{\sigma\}, & \neg\exists e.(e\in\sigma\wedge e\in\Sigma^\varepsilon)\\ \bigcup\limits_{\sigma=\sigma_1e\sigma_2}E_o^\varepsilon(\sigma_1,\Sigma^\varepsilon)\times E^\varepsilon(e)\times E_o^\varepsilon(\sigma_2,\Sigma^\varepsilon), & e\in\Sigma^\varepsilon\end{cases}.$$

2.3 逻辑不确定

某一事件发生之后,通过感知器感知到其发生,然后通过传输通道传输给诊断器.在这个过程中,由于感知器的精度或者传输过程中的信息失真,可能会导致诊断器接受到的并不是该事件发生的信息,而可能是另一事件发生的信息.文献[12]中将这种情况称为逻辑不确定.文献[12]中,用逻辑复合事件来表示.

定义 12(逻辑复合事件)[15]. 可观测事件 $a,b\in\Sigma_o$,若在观测过程中无法确切区分,则用 $a\|b$ 来表示,称为逻辑复合事件.

这里定义了两个事件的逻辑复合事件,其可推广为任意有限个事件的情形.甚至是可观测事件与空事件之间的逻辑不确定,例如 $a\|\varepsilon$,表示事件 a 发生与否无法确定.注意 $a\|\varepsilon$ 与 $a\in\Sigma^{\varepsilon}$之间的区别,虽然都表示事件 a 与ε之间的不确定:前者表示 a 发生与否无法确定,既有可能事件 a 发生了,但观测系统没有观测到,也有可能事件 a 根本没有发生,由于感知器的噪声导致观测系统误认为它发生了;后者表示事件 a 确实发生了,但可能由于信息丢失导致观测系统没有观测到其发生.

在文献[12]中,处理逻辑不确定观测条件下的诊断时,事先给定了逻辑复合事件.即假定根据事件信息之间的相似度或感知器精确度可以预判哪些事件可能存在逻辑不确定.逻辑复合事件的集合,记为$\Sigma^{\|}$.

定义 13(逻辑扩展). 逻辑复合事件中某个原子事件发生后,可能观测到其中的任一事件.我们将逻辑复合事件中所有原子事件的集合称为其逻辑扩展,记为 $E^{\|}(E),E\in\Sigma^{\|}$.

给定$\Sigma^{\|}$,可定义任意可观测事件序列 $\sigma\in\Sigma_o^*$ 的逻辑扩展观测,其物理含义为:任意可观测事件序列发生后,因逻辑不确定可能观测到的不超过其长度的事件序列集合,记为 $E_o^{\|}(\sigma,\Sigma^{\|})\in 2^{\Sigma_o^*}$.具体定义如下:

$$E_o^{\|}(\sigma,\Sigma^{\|})=\begin{cases}\{\sigma\}, & \neg\exists e.[e\in\sigma\wedge e\neq\varepsilon\wedge\exists E.E\in\Sigma^{\|}\wedge e\in E^{\|}(E)]\\ \bigcup\limits_{\sigma=\sigma_1 e\sigma_2} E_o^{\|}(\sigma_1,\Sigma^{\|})\times E^{\|}(E)\times E_o^{\|}(\sigma_2,\Sigma^{\|}), & \exists E.E\in\Sigma^{\|}\wedge e\in E^{\|}(E)\wedge e\neq\varepsilon\end{cases}.$$

注意:由于存在可观测事件与空事件之间的逻辑不确定,经过逻辑扩展,可能观测到超过原有长度的事件序列,这使得逻辑扩展观测的计算非常复杂.例如,$a\|\varepsilon\in\Sigma^{\|}$,则空事件序列$\varepsilon$经过扩展之后的观测集为$\{\varepsilon,a,aa,\ldots\}$.为简单起见,只计算长度不超过原有长度的事件序列.这样, $E_o^{\|}(\varepsilon,\Sigma^{\|})=\{\varepsilon\},E_o^{\|}(a,\Sigma^{\|})=\{\varepsilon,a\}$,依然有 $E_o^{\|}(\varepsilon,\Sigma^{\|})\cap E_o^{\|}(a,\Sigma^{\|})\neq\varnothing$.这种非对称的处理方式既简化了计算,又保留了事件序列之间的不可区分性.

2.4 来源不确定

当系统由多个不同的组件构成时,不同的组件中可能会发生相同的事件,观测系统观测到某个事件后,可能无法确定该事件来源于哪个组件.文献[12]中,把这种情况称为来源不确定.通过采用不同的感知器监测不同的组件,在诊断器中记录信息来源(感知器 ID),即可消除这种观测不确定.因此,在本文中不考虑来源不确定.

3 不确定观测下的可诊断性

各类观测不确定,会给离散系统的诊断造成影响.传统的可诊断性定义已不适用于不确定观测条件下系统的可诊断性刻画.我们将扩展可诊断性的定义,并分别给出各类不确定观测条件下判定可诊断性的方法.

3.1 不确定观测下的可诊断性

定义 14(不确定观测下的可诊断性). 离散事件系统 $G=(X,\Sigma,\delta,x_0)$,在存在不确定观测集 Σ_o^u 的条件下是可诊断的,当其满足如下条件:

$$(\forall f\in\Sigma_f)(\exists n\in N)(\forall\sigma\in\overline{L}_G(f))(\forall\sigma'\in L(G)/\sigma,|P_o(\sigma')|\geqslant n),$$

$$(\forall l\in L(G)),E_o^u(P_o(l),\Sigma_o^u)\cap E_o^u(P_o(\sigma\sigma'),\Sigma_o^u)\neq\varnothing\Rightarrow l\in L_G(f).$$

不确定观测集 Σ_o^u 既可以是 3 类不确定观测中某一类不确定观测集(疑似片段集、疑似丢失事件集或逻辑复合事件集),也可以是混合了多类不确定观测的复合不确定观测集. $E_o^u(P_o(l),\Sigma_o^u)$ 是对 $P_o(l)$的不确定性扩展.如果只包含 1 类观测不确定,则分别用 $E_o^{//}(P_o(l),\Sigma_n^{//}(G)),E_o^{\varepsilon}(P_o(l),\Sigma^{\varepsilon})$ 或 $E_o^{\|}(P_o(l),\Sigma^{\|})$ 替换即可.为简单起见,当包含

多类不确定观测时,$E_o^u(P_o(l),\Sigma_o^u)$ 的计算将在第 4 节介绍.

$E_o^u(P_o(l),\Sigma_o^u)\cap E_o^u(P_o(l'),\Sigma_o^u)\neq\varnothing$,即 l 和 l'发生后,由于观测不确定,观测到的均可能是事件序列 $l''\in E_o^u(P_o(l),\Sigma_o^u)\cap E_o^u(P_o(l'),\Sigma_o^u)$,因此无法区分.传统的可诊断性是定义 14 的特例,当观测确定时,不确定观测集为空,$E_o^u(P_o(l),\Sigma_o^u)=\{P_o(l)\}$,$E_o^u(P_o(l),\Sigma_o^u)\cap E_o^u(P_o(l'),\Sigma_o^u)\neq\varnothing$ 等价于 $P_o(l)=P_o(l')$.

我们将分别给出各类不确定观测下的可诊断性判定方法,它们都通过扩展传统的双树方法来实现.具体而言,就是针对各类不确定观测,分别构造不同的预诊断器,然后通过预诊断器的自同步来实现可诊断性的判定.

3.2 时序不确定观测下的可诊断性判定

定义 15(预诊断器 I). 通过扩展离散事件系统 G 的预诊断器 $G_o=(X_o,\Sigma_o,\delta_o,x_0^o)$ 可得在疑似片段集 $\Sigma_n^{//}(G)$ 条件下的预诊断器 $G_o^{//}=(X_o^{//},\Sigma_o^{//},\delta_o^{//},x_0^{//})$,其中,

- $X_o^{//}=X_o\cup X_o'$,是 $G_o^{//}$ 的有限状态集合,其中添加了 X_o' 中的状态点;
- $\Sigma_o^{//}=\Sigma_o$,为 $G_o^{//}$ 的有限事件集合;
- $\delta_o^{//}=\delta_o\cup\delta_o'\subseteq X_o^{//}\times\Sigma_o^{//}\times X_o^{//}$,是 $G_o^{//}$ 的有限状态转移集合,其中添加了 δ_o' 的状态转换;
- $x_0^{//}=(x_0,\varnothing)\in X_o^{//}$,是 $G_o^{//}$ 的初始状态.

其中,X_o' 和 δ_o' 是为了显式表示 $\Sigma_n^{//}(G)$ 中各疑似片段的时序扩展而添加的状态点和边的集合,通过不断调用算法 1 来实现.

算法 1. 疑似片段的显式时序扩展.

输入:疑似片段路径$(x_1,e_1,x_2,e_2,\ldots,e_{n-1},x_n)$.

输出:有向图 $G=(V,E)$.

1. Initial: $G=(V,E)$, $V=\{(x_i,1)|=1,2,\ldots,n\}$, $E=\{[(x_i,1),e_i,(x_{i+1},1)]|=1,2,\ldots,n-1\}$,
   $\Sigma=\{e_1,e_2,\ldots,e_n\}$ //(x_i,m)表示状态点 x_i 的第 m 个副本;Σ是疑似片段中事件的多重集
2. for i=1 to $n-1$ //依次确定第 i 层节点的后续节点
3. compute m //m 是第 i 层节点的个数,即 x_i 的副本数
4. for j=1 to m //依次确定(x_i,j)的后续节点
5. compute Σ' of (x_i,j) //计算(x_i,j)的前驱事件多重集
6. for each $e\in\Sigma-\Sigma'$ //确定(x_i,j)通过事件 e 转换之后的后续节点
7. compute k //k 是第$(i+1)$层当前节点的个数
8. if $\neg\exists j'.[(x_i,j),e,(x_{i+1},j')]\in E$
   //如果(x_i,j)找不到通过事件 e 转换之后的后续节点(简称 e 后续)
9. if $\exists r[(x_i,q),e',(x_{i+1},r)]\in E\wedge[(x_{i-1},p),e,(x_{i+1},r)]\in E\wedge[(x_{i-1},p),e',(x_i,j)]\in E$
   //如果在第$(i+1)$层的当前节点中可以找到节点直接添加 e 边成为(x_i,j)的 e 后续
10. $E=E\cup\{[(x_i,j),e,(x_{i+1},r)]\}$ //添加边
11. else
12. $V=V\cup\{(x_{i+1},k+1)\}$ //添加 x_{i+1} 的新副本$(x_{i+1},k+1)$
13. $E=E\cup\{[(x_i,j),e,(x_{i+1},k+1)]\}$ //添加边
14. Return G

由算法 1 可知,疑似片段的路径$(x_1,e_1,x_2,e_2,\ldots,e_{n-1},x_n)$扩展之后变成有向图 $G=(V,E)$.G 满足如下性质.

- 任意两点之间的任意两条不同路径都满足:路径上的事件多重集是相同的,但是顺序不同;
- $\{e_1,e_2,\ldots,e_n\}$的每一种排列都有一条从 x_1 到 x_n 路径上的事件序列与其一致.

可能会添加若干状态点,它们是疑似片段路径上状态点的复制.为区分不同副本,用(x_i,m)来标记,即 x_i 的第 m 个副本.之所以复制而不引进新的状态点,是因为时序不确定并没有改变系统的状态转换过程,仅仅是改变了

观测所得事件序列的顺序.

令 N 为疑似片段路径上状态点的个数,若疑似片段中没有相同的事件,则扩展之后各状态点的副本数正好与杨辉三角第 N 行的数一致.根据杨辉三角的性质可知,G 的节点数为 2^{N-1},即相对于原有状态数成指数级别的膨胀.又由于 $N\leqslant n$,其中,n 为时序不确定度,故有 G 的节点数不超过 2^n.

G_o 中的所有疑似片段路径都通过算法 1 进行扩展,即得到预诊断器 $G_o^{//}$.在 $G_o^{//}$ 中,所有疑似片段的时序扩展都显式表示,为自同步过程中将因时序不确定而导致无法区分的事件序列同步做准备.通过构造 $G_o^{//}$ 的自同步,得到自动机 $G_d^{//}=G_o^{//}\otimes G_o^{//}$,在 $G_d^{//}$ 上测试是否存在故障冲突的环路:若不存在,则系统可诊断;否则,不可诊断.

例 2:在图 1(a)所示的自动机 G 中,令时序不确定度为 2,则 $\Sigma_2^{//}(G)=\{ab,ac\}$,其预诊断器 $G_o^{//}$ 如图 2 所示.与图 1(b)相比,添加了状态点(1′,N),(5′,N)和对应的边.自同步自动机 $G_d^{//}$ 如图 3 所示,存在故障冲突环路,所以在时序不确定度为 2 的条件下 G 不可诊断.导致不可诊断的主要原因是 ab 成为疑似片段,事件序列 $abfc^*$和 $buac^*$发生之后,均可能观测到事件序列 bac^*或 abc^*,无法诊断系统是否运行正常.

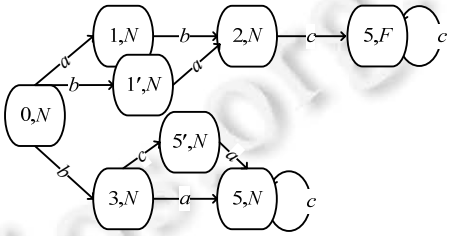


Fig.2 Pre-Diagnoser $G_o^{//}$ with the temporal uncertainty (n=2)

图 2 时序不确定条件下(n=2)的预诊断器 $G_o^{//}$

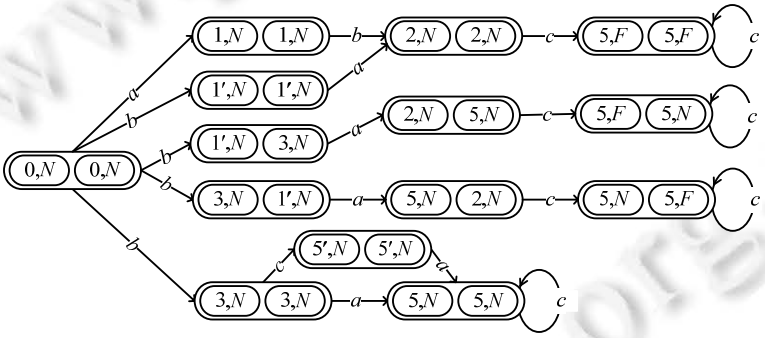


Fig.3 Self-Synchronized automaton $G_d^{//}$ of pre-diagnoser $G_o^{//}$

图 3 预诊断器 $G_o^{//}$ 的同步自动机 $G_d^{//}$

为了证明上述判定方法的正确性,我们先给出下面的两个引理.

引理 1. 在自动机 $G_o^{//}(X_o^{//},\Sigma_o^{//},\delta_o^{//},x_0^{//})$ 中具有如下性质:对于 $G_o^{//}$ 中任意以环路结束的路径:

$$p=((x_0,\varnothing),e_0,(x_1,F_1),\ldots,(x_k,F_k),e_k,\ldots,(x_n,F_n),e_n,(x_k,F_k)),$$

都有:

(1) $F_i=F_j$ 对任意的 $i,j\in\{k,k+1,\ldots,n\}$;

(2) $\exists uv^*\in L(G)$,满足 $e_0\ldots e_{k-1}\in E_o^{//}(P_o(u),\Sigma_m^{//}(G)),e_k\ldots e_n\in E_o^{//}(P_o(v),\Sigma_m^{//}(G)),P_f(u)=P_f(uv)=F_k$.

证明:由 $G_o^{//}$ 的构造过程可以直接证明,具体证明如下:

(1) 由 $G_o^{//}$ 的构造可知:任意 $((x,F),e,(x',F'))\in\delta_o^{//}$,都有 $F\subseteq F'$,因此在路径 p 中,有 $F_k\subseteq F_{k+1}\subseteq\ldots F_n\subseteq F_k$,所以,

$$F_k=F_{k+1}=\ldots=F_n.$$

(2) 当路径 p 中的所有状态点都来自 X_o 时,有$\exists uv^*\in L(G)$,满足 $P_o(u)=e_0\ldots e_{k-1}$,$P_o(v)=e_k\ldots e_n$,$P_f(u)=P_f(uv)=F_k$,这个结论在文献[11]中已给出.

当路径 p 中的部分状态点来自 X'_o 时,由 G''_o 的构造可知,p 中的任意形如

$$((x_i,F_i),e_i,(x'_{i+1},F'_{i+1}),e_{i+1},\ldots,(x'_{i+j},F'_{i+j}),e_{i+j},(x_{i+j+1},F_{i+j+1}))$$

的子序列(其中,$(x'_{i+i'},F'_{i+i'})\in X'_o,i'\in\{1,2,\ldots,j\}$)都对应一个子序列:

$$((x_i,F_i),e'_i,(x_{i+1},F_{i+1}),e'_{i+1},\ldots,(x_{i+j},F_{i+j}),e'_{i+j},(x_{i+j+1},F_{i+j+1}))\ .$$

其中,$(x_{i+i'},F_{i+i'})\in X_o,x_{i+i'}=x'_{i+i'},F_{i+i'}=F'_{i+i'}$ 且 $e_i\ldots e_{i+j}\in E''_o(e'_i\ldots e'_{i+j},\Sigma''_m(G))$.

因为 X'_o 中的状态点都是 X_o 中状态点的复制副本,$e_i\ldots e_{i+j}$ 属于 $e'_i\ldots e'_{i+j}$ 的时序扩展.

因此,对于任意 p 有如下结论:$\exists uv^*\in L(G)$,满足 $e_0\ldots e_{k-1}\in E''_o(P_o(u),\Sigma''_m(G)),e_k\ldots e_n\in E''_o(P_o(v),\Sigma''_m(G))$,$P_f(u)=P_f(uv)=F_k$. □

引理中的(1)说明 G''_o 中任意以环结束的路径,其环路部分的节点都具有相同的故障标签;(2)说明 G''_o 中任意以环路结束的路径在 G 都存在一条与其观测一致的(在时序不确定条件下无法区分)以环路结束的路径.

引理 2. 在自同步自动机 $G''_d=G''_o\otimes G''_o$ 中有如下性质:对于 G''_d 中任意以环路结束的路径:

$$p=(x_0^d,e_0,x_1^d,\ldots,x_k^d,e_k,\ldots,x_n^d,e_n,x_k^d),\text{其中},x_i^d=((x_i^1,F_i^1),(x_i^2,F_i^2)),i=1,2,\ldots,n\ ,$$

都有:

(1) 在 G''_o 中存在两条以环路结束的路径:

$$p_1=((x_0,\varnothing),e_0,(x_1^1,F_1^1),\ldots,(x_k^1,F_k^1),e_k,\ldots,(x_n^1,F_n^1),e_n,(x_k^1,F_k^1)),$$
$$p_2=((x_0,\varnothing),e_0,(x_1^2,F_1^2),\ldots,(x_k^2,F_k^2),e_k,\ldots,(x_n^2,F_n^2),e_n,(x_k^2,F_k^2)).$$

(2) $F_i^1=F_j^1,F_i^2=F_j^2$,对任意 $i,j\in\{k,k+1,\ldots,n\}$.

证明:由自同步自动机的定义和引理 1 可以证明. □

引理 2 说明,G''_d 中任意一条以环路结束的路径对应着 G''_o 中两条可能不同的以环路结束的路径.

定理 1. 给定 $\Sigma''_n(G)$ 的条件下,G 可诊断,当且仅当 G''_d 中不存在故障冲突的环路.即任意环路 $cl=(x_1^d,e_1,x_2^d,e_2,\ldots,x_n^d,e_n,x_1^d),n\geqslant 1,x_i^d=((x_i^1,F^1),(x_i^2,F^2)),i=1,2,\ldots,n$,都有 $F^1=F^2$.

证明:下面将分别证明其必要性和充分性.

(1) 先证:如果 G 可诊断,则 G''_d 中不存在故障冲突的环路.

假设 G''_d 中存在故障冲突的环路 $cl=(x_k^d,e_k,x_{k+1}^d,e_{k+1},\ldots,x_n^d,e_n,x_k^d),n\geqslant k,x_i^d=((x_i^1,F^1),(x_i^2,F^2))$,$i=k,k+1,\ldots,n$,$F^1\neq F^2$.由于 G''_d 中的状态点都是从初始状态可达的,因此存在一条从出初始状态开始以环路结束的路径 $p=(x_0^d,e_0,x_1^d,\ldots,x_k^d,e_k,\ldots,x_n^d,e_n,x_k^d)$.由引理 2 可知,$G''_o$ 中存在两条以环路结束的路径,分别为:

$$p_1=((x_0,\varnothing),e_0,(x_1^1,F_1^1),\ldots,(x_k^1,F^1),e_k,\ldots,(x_n^1,F^1),e_n,(x_k^1,F^1)),$$
$$p_2=((x_0,\varnothing),e_0,(x_1^2,F_1^2),\ldots,(x_k^2,F^2),e_k,\ldots,(x_n^2,F^2),e_n,(x_k^2,F^2)).$$

由引理 1 可知,存在 $l_1=u_1v_1^*\in L(G),l_2=u_2v_2^*\in L(G)$,满足:

$$e_0\ldots e_{k-1}\in E''_o(P_o(u_1),\Sigma''_n(G)),e_k\ldots e_n\in E''_o(P_o(v_1),\Sigma''_n(G)),P_f(u_1)=P_f(u_1v_1)=F^1,$$
$$e_0\ldots e_{k-1}\in E''_o(P_o(u_2),\Sigma''_n(G)),e_k\ldots e_n\in E''_o(P_o(v_2),\Sigma''_n(G)),P_f(u_2)=P_f(u_2v_2)=F^2.$$

故有 $e_0\ldots e_{k-1}(e_k\ldots e_n)^*\in E''_o(P_o(l_1),\Sigma''_n(G))\cap E''_o(P_o(l_2),\Sigma''_n(G))\neq\varnothing$.因为 $F^1\neq F^2$,不失一般性,我们假定 $f_k\in F^1-F^2\neq\varnothing$,则存在 $\sigma\in\overline{L}_G(f_k)$ 满足 $u_1=\sigma t,t\in L(G)/\sigma$.对任意 $n\in N$,存在 $m\in N$,使得 $|P_o(tv_1^m)|\geqslant n$.显然,

$$E''_o(P_o(u_2v_2^m),\Sigma''_n(G))\cap E''_o(P_o(\sigma tv_1^m),\Sigma''_n(G))\neq\varnothing\ .$$

但 $P_f(u_2v_2^m)=F^2$,即 $u_2v_2^m\notin L_G(f_k)$.根据可诊断性的定义(定义 14)可知,G 不可诊断,推出矛盾,必要性得证.

(2) 再证:如果 G_d'' 中不存在故障冲突的环路,则 G 可诊断.

由不存在故障冲突的环路可知, G_d'' 的任意状态点 $x=((x^1,F^1),(x^2,F^2))$,如果 $F^1\neq F^2$,则 x 一定不属于任何环路.因此, G_d'' 中的任意状态序列$(x_1,x_2,\ldots,x_k)$,其中, $x_i=((x_i^1,F_i^1),(x_i^2,F_i^2))$.如果任意 $i\in\{1,2,\ldots,k\}$都有 $F_i^1\neq F_i^2$,则该状态序列的长度一定小于 G_d'' 总状态数,即 $k\lhd|X_d''|$.换句话说, G_d'' 中任意存在故障冲突的状态点 x,最多经过 $(|X_d''|-1)$次状态转换后,一定会到达一个不存在故障冲突的状态点 y.由 G_d'' 中路径与 G_o'' 和 G 中路径之间的关系可知:

$$(\forall f\in\Sigma_f)(\forall\sigma\in\overline{L}_G(f))(\forall\sigma'\in L(G)/\sigma,|P_o(\sigma')|\geqslant(|X_d''|-1)),$$

$$(\forall l\in L(G)),E_o''(P_o(l),\Sigma_n''(G))\cap E_o''(P_o(\sigma\sigma'),\Sigma_n''(G))\neq\varnothing\Rightarrow l\in L_G(f).$$

根据可诊断性的定义(定义 14)可知,G 是可诊断的,充分性得证. □

3.3 丢失不确定观测下的可诊断性分析

定义 16(预诊断器 II). 通过扩展离散事件系统 G 的预诊断器 $G_o=(X_o,\Sigma_o,\delta_o,x_0^o)$ 可得在疑似丢失事件集Σ^ε条件下的预诊断器 $G_o^\varepsilon=(X_o^\varepsilon,\Sigma_o^\varepsilon,\delta_o^\varepsilon,x_0^\varepsilon)$,其中,

- $X_o^\varepsilon=X_o$ 是 G_o^ε 的有限状态集合,与 G_o 的状态集相同;
- $\Sigma_o^\varepsilon=\Sigma_o\cup\{\varepsilon\}$ 为 G_o^ε 的有限事件集合;
- $\delta_o^\varepsilon\subseteq X_o^\varepsilon\times\Sigma_o^\varepsilon\times X_o^\varepsilon$ 是 G_o^ε 的有限状态转移集合,其定义如下:

$$\delta_o^\varepsilon=\delta_o\cup\{(x,\varepsilon,x')\mid\exists e\in\Sigma_o,(x,e,x')\in\delta_o\wedge e\in\Sigma^\varepsilon\};$$

- $x_0^\varepsilon=(x_0,\varnothing)\in X_o^\varepsilon$ 是 G_o^ε 的初始状态.

从上述构造过程可知, G_o^ε 通过在 G_o 中加入空事件ε标识的边扩展而成.通过加入ε边,将因丢失不确定观测而导致无法区分的事件片段统一起来.

同样地,通过预诊断器 G_o^ε,可以构造其自同步自动机,然后在自同步自动机上测试是否具有故障冲突的环路:若不存在,则系统可诊断;否则,不可诊断.因为ε事件的特殊性,我们要相应地调整自同步自动机的构造过程.

定义 17(自同步自动机 II). 可观测自动机 G_o^ε 的自同步自动机 $G_d^\varepsilon=G_o^\varepsilon\otimes G_o^\varepsilon=(X_d,\Sigma_o^\varepsilon,\delta_d,x_0^d)$,其中,

- $X_d=\{(x_1^o,x_2^o)\mid x_1^o,x_2^o\in X_o\}$ 是 G_d^ε 的有限状态集合.
- $\Sigma_o^\varepsilon=\Sigma_o\cup\{\varepsilon\}$ 是 G_d^ε 的有限事件集合.
- $\delta_d\subseteq X_d\times\Sigma_o\times X_d$ 是 G_d^ε 的有限状态转移集合, $((x_1^o,x_2^o),e,(y_1^o,y_2^o))\in\delta_d$ 当且仅当满足如下条件之一:
  ① $(x_1^o,e,y_1^o)\in\delta_o^\varepsilon$,且$(x_2^o,e,y_2^o)\in\delta_o^\varepsilon$;
  ② $(x_i^o,e,y_i^o)\in\delta_o^\varepsilon$ 且 $e=\varepsilon, x_j^o=y_j^o, i,j\in\{1,2\}$且 $i\neq j$.
- $x_0^d=(x_0^o,x_0^o)\in X_d$ 是 G_d^ε 的初始状态.

通过修改同步自动机中的同步策略(在δ_d 中引入针对ε事件的同步策略),实现丢失事件发生之后的状态与该事件未发生前的状态之间的同步.定理 2 证明了在丢失不确定条件下可诊断性判定方法的正确性.

定理 2. 在给定疑似丢失集Σ^ε的条件下,G 可诊断,当且仅当 G_d^ε 中不存在故障冲突的环路.即任意环路 $cl=(x_1,e_1,x_2,e_2,\ldots,x_n,e_n,x_1), n\geqslant 1, x_i=((x_i^1,F_i^1),(x_i^2,F_i^2)), i=1,2,\ldots,n$,都有 $F_i^1=F_i^2$.

证明:这里有一点要特别说明.由于空事件ε的引入, G_d^ε 中的环路可以分为两类:一类是非空事件环,即环路中包含非空事件,其具有引理 2 所描述的性质,即对应着 G_o^ε 中的两条环路;另一类是空事件环,即环路中的所有事件都是空事件ε,其打破了“不存在不可观测事件环路”的假定,并不满足引理 2 所描述的性质.因此对非空事件环,其证明与定理 1 的证明类似,对空事件环,其证明要稍作修改.

G_d^ε 的任一空事件环 $cl=(x_k^d,e_k,x_{k+1}^d,\ldots,e_{n-1},x_n^d,e_n,x_k^d)$,$n>k, e_i=\varepsilon, i=k,\ldots,n$,分别对应 G_o^ε 的一个状态点 (x_k^1,F_k^1)和一个环路 $cl'=((x_k^2,F_k^2),e_k,(x_{k+1}^2,F_{k+1}^2),\ldots,(x_n^2,F_n^2),e_n,(x_k^2,F_k^2))$.

在 G_o^ε 中一定存在非空事件环: $cl''=((x_k^2,F_k^2),e_k'',(x_{k+1}^2,F_{k+1}^2),...,(x_n^2,F_n^2),e_n'',(x_k^2,F_k^2)),\exists i\in[k,n],e_i''\neq\varepsilon,e_i''\in\Sigma^\varepsilon$,即空事件环 cl' 是由于非空事件环中的丢失不确定事件确实发生丢失之后形成的.

在空事件环情况下,定理 2 的必要性证明思路如下:如果存在故障冲突的空事件环,那么在 G_o^ε 中就存在一条无环路的路径 $p_1=((x_0,\varnothing),e_0,(x_1^1,F_1^1),...,e_{k-1},(x_k^1,F_k^1))$ 和一条以环路结尾的路径 $p_2=((x_0,\varnothing),e_0,(x_1^2,F_1^2),...,e_{k-1},(x_k^2,F^2),e_k'',...,(x_n^2,F^2),e_n'',(x_k^2,F^2)),F_1^k\neq F^2$.两者获得的扩展观测交集非空,由可诊断性定义可知其不可诊断.定理 2 的充分性证明与定理 1 的充分性证明类似. □

例 3:在图 1(a)所示的自动机 G 中,考虑疑似丢失事件集$\{a\}$,则其预诊断器 G_o^ε 如图 4 所示.为简单起见,节点之间的多条边在图中用 1 条边表示,不同标识事件之间用“+”号连接.与图 1(b)相比,添加了两条标记为ε的边.自同步自动机 $G_d^\varepsilon=G_o^\varepsilon\otimes G_o^\varepsilon$ 如图 5 所示,由于存在具有故障冲突的环路,所以是不可诊断的.由于事件 a 的丢失不确定,使得事件序列 $abfc^*$和 $buac^*$发生之后,都可能观测到事件序列 bc^*,从而无法诊断系统是否运行正常.

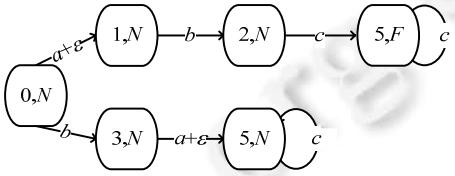


Fig.4 Pre-Diagnoser G_o^ε with the loss uncertainty of $\{a\}$

图 4 带丢失不确定观测$\{a\}$的预诊断器 G_o^ε

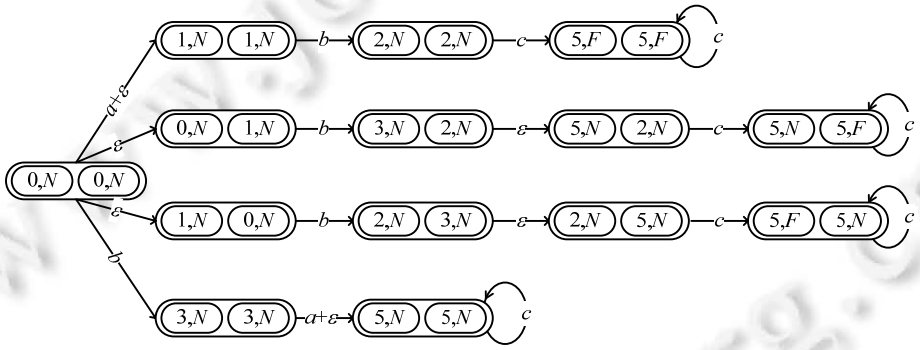


Fig.5 Self-Synchronized automaton G_d^ε of pre-diagnoser G_o^ε

图 5 带丢失不确定观测$\{a\}$的同步自动机 G_d^ε

3.4 逻辑不确定观测下的可诊断性分析

定义 18(预诊断器 III). 通过扩展离散事件系统 G 的预诊断器 $G_o=(X_o,\Sigma_o,\delta_o,x_0^o)$ 可得在逻辑复合事件集 $\Sigma^{\|}$条件下的预诊断器 $G_o^{\|}=(X_o^{\|},\Sigma_o^{\|},\delta_o^{\|},x_0^{\|})$,其中,

- $X_o^{\|}=X_o$ 是 $G_o^{\|}$ 的有限状态集合,与 G_o 的状态集相同;
- $\Sigma_o^{\|}=\Sigma_o\cup\{\varepsilon\}$ 为 $G_o^{\|}$ 的有限事件集合;
- $\delta_o^{\|}\subseteq X_o^{\|}\times\Sigma_o^{\|}\times X_o^{\|},\delta_o^{\|}=\{(x,e,x')\mid\exists e'\in\Sigma_o,(x,e',x')\in\delta_o,e\in E_o^{\|}(e',\Sigma^{\|})\}$;
- $x_0^{\|}=(x_0,\varnothing)\in X_o^{\|}$ 是 $G_o^{\|}$ 的初始状态.

从构造过程可知, $G_o^{\|}$ 通过对 G_o 增补一些边构造而成.G_o 中用原子事件标识的边,添加与其存在逻辑不确定关系的原子事件标识的边.通过加入这些边,将因逻辑不确定观测而导致无法区分的观测片段统一起来.

类似地,通过构造自同步自动机 $G_d^{\|}=G_o^{\|}\otimes G_o^{\|}$,然后在 $G_d^{\|}$ 中测试是否具有故障冲突的环路:若不存在这样的

环路,则系统可诊断;否则,不可诊断.由于存在原子事件与空事件ε的逻辑不确定,应采取自同步自动机 II(定义17)的同步策略.定理 3 证明了在逻辑不确定条件下可诊断性判定方法的正确性.

定理 3. 在给定逻辑不确定观测集$\Sigma^{\|}$的条件下,G 可诊断,当且仅当 $G_d^{\|}$ 中不存在故障冲突的环路.即任意环路 $cl=(x_1,e_1,x_2,e_2,...,x_n,e_n,x_1), n\geqslant 1, x_i=((x_i^1,F_i^1),(x_i^2,F_i^2)), i=1,2,...,n$,都有 $F_i^1=F_i^2$.

证明:其证明与定理 2 的证明类似. □

例 4:在图 1(a)所示的自动机 G 中,考虑逻辑复合事件集$\{a\|b\}$,则其预诊断器 $G_o^{\|}$ 如图 6 所示.与图 1(b)相比,分别添加了两条 a 边和两条 b 边.同步自动机 $G_d^{\|}=G_o^{\|}\otimes G_o^{\|}$ 如图 7 所示,由于存在故障冲突的环路,所以不可诊断.因为存在事件 a 和 b 之间的逻辑不确定观测,使得事件序列 $abfc^*$和 $buac^*$发生之后,均可能观测到事件序列 abc^*, bac^*,aac^*或 bbc^*,从而无法诊断系统是否运行正常.

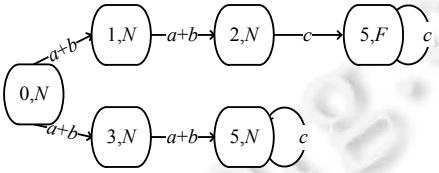


Fig.6 Pre-Diagnoser $G_o^{\|}$ with the logical uncertainty of $\{a\|b\}$

图 6 带逻辑不确定观测$\{a\|b\}$的预诊断器 $G_o^{\|}$

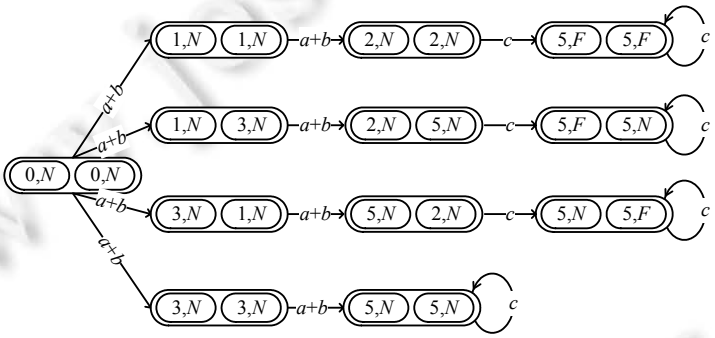


Fig.7 Self-Synchronized automaton $G_d^{\|}$ of pre-diagnoser $G_o^{\|}$

图 7 带逻辑不确定观测$\{a\|b\}$的同步自动机 $G_o^{\|}$

4 复合不确定观测下的可诊断性

上一节我们分别讨论了在时序不确定、丢失不确定和逻辑不确定观测条件下的离散事件系统可诊断性问题.但在实际应用中,这几类不确定性问题可能同时存在.下面我们将探讨同时存在这些观测不确定性的情况下,可诊断性的判定方法.从上一节的分析可知,虽然导致观测丢失不确定和逻辑不确定的原因不同,但对逻辑不确定中的空事件ε采用非对称的处理后,丢失不确定可以看做逻辑不确定的特例,因此,我们只讨论时序不确定和逻辑不确定混合的情况.

当观测中同时存在时序不确定和逻辑不确定时,情况会变得非常复杂.因为这些不确定性会发生相互正交作用[12],导致更复杂的观测不确定性.例如,如果 $ab\in\Sigma_2^{//}(G)$ 且 $b\|c\in\Sigma^{\|}$,即事件 a 和 b 连续发生时,存在时序不确定观测,同时,事件 b 和 c 存在逻辑不确定性;那么事件序列 ab 发生后,在复合不确定观测下,诊断器可能接收到的事件序列可能是 ab,ba,ac 或 ca.因此,我们首先要定义复合不确定观测下的观测扩展.

定义 19(复合扩展观测). 给定 $\Sigma_o^u=\Sigma_n^{//}(G)\cup\Sigma^{\|}$,可定义任意可观测事件序列 $\sigma\in\Sigma_o^*$ 的复合扩展观测:

$$E_o^u(\sigma,\Sigma_o^u)=\bigcup_{\sigma'\in E_o^{\|}(\sigma,\Sigma^{\|})}E_o^{//}(\sigma',\Sigma_n^{//}(G)\times\Sigma^{\|}).$$

其中,$\Sigma_n^{//}(G)\times\Sigma^{\|}=\bigcup_{\sigma\in\Sigma_n^{//}(G)}E_o^{\|}(\sigma,\Sigma^{\|})$ 是疑似片段集的逻辑扩展,其物理含义为:任意可观测事件序列发生后,因复合不确定可能观测到的不超过其长度的事件序列集合.

由定义可知,复合扩展观测是先考虑逻辑扩展,然后再考虑时序扩展.例如,令 $\Sigma_2^{//}(G)=\{ab\}$,$\Sigma^{\|}=\{b\|c\}$,则

$$\Sigma_2^{//}(G)\times\Sigma^{\|}=\{ab,ac\},E_o^u(ab,\Sigma_o^u)=\{ab,ba,ac,ca\}.$$

因为逻辑不确定扩展可能在σ'中引入空事件ε,为了保障构造出的预诊断器的正确性,在计算疑似片段的逻辑扩展时做了一定的技术处理.例如,$abc\in\Sigma_3^{//}(G)$,$\Sigma^{\|}=\{b\|\varepsilon\}$,则 $E_o^{\|}(abc,\Sigma^{\|})=\{abc,a\varepsilon c\}$.注意:这里$\varepsilon$必须保留,便于疑似片段 $a\varepsilon c$ 的显式扩展;否则只会各自扩展疑似片段 abc 和 ac,两者之间的联系会丢失.

在此基础之上,我们提出复合不确定观测下的可诊断性判断方法,其主要过程如下:

(1) 按照预诊断器 III 的定义构造 G 在逻辑复合事件集$\Sigma^{\|}$下的预诊断器 G_o' (考虑逻辑不确定).

(2) 根据时序不确定度 n,计算 G 的疑似片段集 $\Sigma_n^{//}(G)$,进而计算 G_o' 的疑似片段集 $\Sigma_n^{//}(G)\times\Sigma^{\|}$.

(3) 按照预诊断器 I 的定义构造 G_o' 在疑似片段集 $\Sigma_n^{//}(G)\times\Sigma^{\|}$ 下的预诊断器 G_o'' (考虑时序不确定).

(4) 由于空事件ε的引人,按照自同步自动机 II 的定义进行自同步,得到同步自动机 $G_o''\otimes G_o''$.

(5) 在同步自动机上测试是否具有故障冲突的环路:若不存在这样的环路,则系统可诊断;否则,不可诊断.

5 复杂性分析

与经典的双树方法类似,在各类观测不确定条件下,可诊断性判定的时间复杂度主要由如下 3 个过程构成:

(1) 预诊断器的构造;

(2) 同步自动机的构造;

(3) 同步自动机中是否具有故障冲突环路的判断.

在经典双树方法中,预诊断器的状态数最大为 $|X|\times2^{|\Sigma_f|}$,状态转移数最大为 $|X|^2\times2^{2|\Sigma_f|}\times|\Sigma_o|$,其中,

- $|X|$为离散事件系统的状态数,$|\Sigma_o|$和$|\Sigma_f|$分别为系统的可观测事件数和故障事件数;
- 同步自动机的状态数最大为 $|X|^2\times2^{2|\Sigma_f|}$,状态转移数最大为 $|X|^4\times2^{4|\Sigma_f|}\times|\Sigma_o|$.

因此,第(1)步的时间复杂度为 $O(|X|^2\times2^{2|\Sigma_f|}\times|\Sigma_o|)$;第(2)步的事件复杂度为 $O(|X|^4\times2^{4|\Sigma_f|}\times|\Sigma_o|)$;第(3)步的时间复杂度为 $O(|X|^4\times2^{4|\Sigma_f|})$.因此,总的时间复杂度为 $O(|X|^4\times2^{4|\Sigma_f|}\times|\Sigma_o|)$.但是在实际判定时,我们可以针对每个故障类型分别进行判断,这样,总体复杂度可以优化为 $O(|X|^4\times|\Sigma_o|\times|\Sigma_f|)$[12].

在处理时序不确定时,由于在构造预诊断器的过程中添加了若干状态点,因此其时间复杂度变为

$$O(|X'|^4\times|\Sigma_o|\times|\Sigma_f|),$$

其中,$|X'|$是疑似片段显式扩展所得预诊断器的状态数.由疑似片段的显式扩展算法 1 可知,$|X'|$是 $O(|X|\cdot2^n)$级别的,其中,n 为时序不确定度.因此,总体的时间复杂度为 $O(2^{4n}\times|X|^4\times|\Sigma_o|\times|\Sigma_f|)$.显然,时序不确定度越高,疑似片段就越多,要添加的状态点也就越多,可诊断性判定方法的效率就越低.但在时序不确定度较低时,可以认为其效率与经典双树效率相当.在实际应用中,可以通过先采取较低的时序不确定度,然后再逐渐增加的方式来控制时间复杂度的增长.

在处理丢失不确定和逻辑不确定性时构造的预诊断器,与经典双树方法相比,状态数均是 $O(|X|)$级别的;虽然添加了一些状态转换边,但是由于可选边仅限于$\Sigma_o\cup\{\varepsilon\}$中的边,其状态转移最大数依然是 $O(|X|^2\times|\Sigma_o|)$级别的.因此,总体时间复杂度依然为 $O(|X|^4\times|\Sigma_o|\times|\Sigma_f|)$.

综上所述,仅考虑单类观测不确定条件下可诊断性的判定,从时间复杂度的角度来看,时序不确定要比丢失不确定和逻辑不确定复杂.在多类观测不确定正交复合的情况下,虽然丢失不确定或逻辑不确定会导致出现时序不确定的疑似片段增加,但都是在时序不确定度允许的范围内,因此,其时间复杂度与仅考虑时序不确定时可

诊断性的判断属于同一复杂度级别的.

6 相关工作

下面我们介绍与本文研究内容密切相关的主要相关工作,并从系统模型、不确定性表示和解决问题的思路等方面进行比较分析.

Lamperti 等人在主动系统(active system)中讨论了在各类观测不确定条件下,系统的诊断问题[12,16].主动系统是一类特殊的离散事件系统,一个主动系统由一个在输入输出终端之间由链相互连接的组件集构成.正因为存在多个组件,所以他们讨论了来源不确定对系统诊断的影响,这是本文没有考虑的.他们通过有向无环图(观测图)来表示各种观测不确定:观测图中的节点是事件的集合,集合中的多个事件之间存在丢失不确定或逻辑不确定;节点之间的有向边表示时序先后关系,不存在路径连接的节点之间时序是不确定的.通过观测图,可以获得不确定观测的扩展观测,从而将不确定观测的条件下的诊断问题转换成若干与之对应的确定观测下的诊断问题,最终实现系统的诊断.他们只讨论了观测不确定条件下的诊断问题,并未讨论可诊断性问题.其诊断是在线进行的,可以根据实际观测得到观测图.但本文的可诊断性判定是离线进行的,无法事先获取观测图,因此我们采用在一定时序不确定度条件下猜测疑似失序片段的方式来处理时序不确定性.其通过不确定观测扩展,将不确定观测下的诊断问题转换为若干确定观测下的诊断问题的思路,对本文产生了重要影响.

吉林大学欧阳丹彤教授的研究团队在离散事件系统的诊断方法和可诊断性判定方面做了大量的研究工作[5,6,9],其中,文献[6]研究了不完备离散事件系统的可诊断性,文献[9]研究了不完备离散事件系统的诊断方法.他们主要考虑了两类不完备性:时序不完备和行为不完备.虽然模型不完备性和观测不确定性都致力于扩展离散事件系统诊断方法的适用性和实用性,但两者的着眼点不同.模型不完备性考虑的是由于系统建模不完善,导致即使观测确定也无法在系统模型中找到相容的事件轨迹,其研究着眼于降低系统建模的难度.而我们的研究假定系统模型是完备的,而允许系统观测是不确定的,着眼于减低观测系统的构建难度.系统模型的不完备,通过在线观测与离线模型的对比才能发现,因此,不完备离散事件系统的可诊断性判定是在线进行的,而本文讨论的观测不确定条件下的可诊断性是离线进行的.

Grastien 等人在文献[13,14]中分别将离散事件系统的可诊断性判断和诊断转换成可满足性问题(satisfiability problem,简称 SAT),然后通过调用 SAT 求解器来实现可诊断性的判定和系统诊断.他们采用简洁表示系统(succinct system representation)[13,14]对离散事件系统建模.与我们采用的有限状态自动机(定义 1)相比,简洁表示系统在表达上更简洁:它通过状态变量集而不是状态集来描述系统状态,通过对 n 个逻辑状态变量的不同赋值,可以表示 2^n 个不同的状态;它通过定义事件的转换函数来描述系统状态的转换,而不是显示地列举出所有状态之间的转换过程.事件 e 的转换函数 $\delta(e)$ 是若干 $\langle\varphi,c\rangle$ 对的集合,说明事件 e 在条件 φ 满足的条件下可执行,产生效果为 c.采用简洁表示系统一方面便于将离散事件系统的诊断问题转换为 SAT 问题,另一方面也能表示事件的并行.在某个状态不同事件的执行条件相互不矛盾,执行效果也相互不冲突,就可以并发执行.事件的并发执行,实质上对应时序不确定的情况.文献[13]将双树算法[11]判定可诊断性的思路编码成一个逻辑公式,从而将系统的可诊断性问题转化为该公式的可满足性问题.由于其允许事件的并行,所以其处理了时序不确定条件下的可诊断性判断问题.但其不能处理逻辑不确定或丢失不确定条件下的可诊断性判断问题.

Su 等人在文献[15]中也对观测不确定条件下的可诊断性展开了研究.和我们一样,他们也采用有限状态自动机构造系统模型.但他们只分别研究了时序不确定和逻辑不确定,而本文对时序不确定、丢失不确定和逻辑不确定都分别做了研究,而且对复合观测不确定的情况也做了研究.在处理时序不确定和逻辑不确定时,两者在技术路线上有很大的差异,尽管大家都是通过扩展双树算法来实现的.在处理时序不确定时,两者在时序不确定度和时序扩展的定义上都不相同,进而预诊断器的构造也各不同,最终导致可诊断性判断的时间复杂度也不同.我们定义的时序不确定度以事件发生的相对时间为依据,更加合理.他们方法的时间复杂度为 $O(|X|^4\times|\Sigma_o|^l\times|\Sigma_f|)$,其中,$l$ 是时序不确定水平[15];而我们的时间复杂度为 $O(2^{4n}\times|X|^4\times|\Sigma_o|\times|\Sigma_f|)$,其中,$n$ 是时序不确定度.我们的算法在时序不确定度较低和可观测动作数量较大时性能要更好一些.在处理逻辑不确定时,两者在预诊断器的构造

和同步策略上也都不同.导致这些不同的主要原因在于对如何排除干扰环路的技术处理上.为了避免干扰环路的出现,Su 等人在预诊断器的构造上做了相当复杂的技术处理[15];而本文则着眼于同步策略的修改.虽然大家的时间复杂度均为 $O(|X|^4\times|\Sigma_o|\times|\Sigma_f|)$,但是在构造的预诊断器中,他们的方法无论是节点数还是边数均大于我们的方法,因此,我们方法的实际效率要高一些.而且本文对各类观测不确定的处理方式更有利于处理复合观测不确定,这一点在本文第 4 节已有所体现.

7 结论与展望

离散事件系统可诊断性的研究出于简单性考虑,大都假定系统观测是确定的.但在实际应用中,由于信息传输以及感知器的精度等原因,往往很难获取到确定的观测信息.这给系统的可诊断性判定带来了困难.本文扩展了传统可诊断性的定义,给出观测不确定条件下的可诊断性定义,并给出其判定方法.

与观测确定条件下的可诊断性相比,在观测不确定条件下的可诊断性判断的效率会有所下降,特别是包含时序不确定时.但是,这里的可诊断性判断都是在离线情况下进行的,因此我们认为,从降低观测系统的建设成本以及提高诊断系统的鲁棒性来看,这种效率上的牺牲是值得的.

基于双树方法的可诊断性判定,其时间复杂度虽然只有系统状态数的多项式级别,但在系统规模很大时,其效率依然显得不高.因此,下一步将研究在分布式 MBD 中观测不确定条件下的可诊断性判定方法,以适应大规模系统可诊断性判定的需求.

References:

[1] Sampath M, Sengupta R, Lafortune S, Sinnamohideen K, Teneketzis D. Diagnosability of discrete-event systems. IEEE Trans. on Automatic Control, 1995,40(9):1555−1575. [doi: 10.1109/9.412626]

[2] Sampath M, Sengupta R, Lafortune S, Sinnamohideen K, Teneketzis D. Failure diagnosis using discrete-event models. IEEE Trans. on Control Systems Technology, 1996,4(2):105−124. [doi: 10.1109/87.486338]

[3] Cassandras CG, Lafortune S. Introduction to Discrete Event Systems. Springer-Verlag, 2006.

[4] Han X, Shi ZZ, Lin F. Research advances in model-based diagnosis. Chinese High Technology Letters, 2009,19(5):543−550 (in Chinese with English abstract). [doi: 10.3772/j.issn.1002-0470.2009.05.018]

[5] Zhao XF, Ouyang DT. Progress on model-based diagnosis of discrete-event systems. Journal of Frontiers of Computer Science and Technology, 2011,5(2):114−127 (in Chinese with English abstract).

[6] Wang XY, Ouyang DT, Zhao XF. Diagnosability of discrete event systems with an incomplete model. Ruan Jian Xue Bao/Journal of Software, 2015,26(6):1373−1385 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4585.htm [doi: 10.13328/j.cnki.jos.004585]

[7] Zhao XF, Ouyang DT. Model-Based diagnosis of discrete event systems with an incomplete system model. In: Proc. of the 18th European Conf. on Artificial Intelligence (ECAI 2008). Patras, 2008. 189−193.

[8] Kwong RH, Yeung DL. Fault diagnosis in discrete-event systems: Incomplete models and learning. IEEE Trans. on Systems, Man, and Cybernetics—Part B: Cybernetics, 2011,41(1):118−130. [doi: 10.1109/TSMCB.2010.2047257]

[9] Wang XY, Ouyang DT, Zhao J. Discrete-Event system diagnosis upon incomplete model. Ruan Jian Xue Bao/Journal of Software, 2012,23(3):465−475 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4028.htm [doi: 10.3724/SP.J.1001.2012.04028]

[10] Lin F. Diagnosability of discrete event systems and its applications. Discrete Event Dynamic Systems, 1994,4(2):197−212. [doi: 10.1007/BF01441211]

[11] Jiang SB, Huang ZD, Chandra V, Kumar R. A polynomial algorithm for testing diagnosability of discrete-event systems. IEEE Trans. on Automatic Control, 2001,46(8):1318−1321. [doi: 10.1109/9.940942]

[12] Lamperti G, Zanella M. Diagnosis of discrete-event systems from uncertain temporal observations. Artificial Intelligence, 2002, 137(1-2):91−163. [doi: 10.1016/S0004-3702(02)00123-6]

[13] Rintanen J, Grastien A. Diagnosability testing with satisfiability algorithms. In: Proc. of the 20th Int'l Joint Conf. on Artificial Intelligence (IJCAI 2007). Hyderabad, 2007. 532−537.

[14] Grastien A, Anbulagan A, Rintanen J, Kelareva E. Diagnosis of discrete-event systems using satisfiability algorithms. In: Proc. of the 22nd National Conf. on Artificial Intelligence (AAAI 2007). Vancouver, 2007. 305−310.

[15] Su XY, Zanella M, Grastien A. Diagnosability of discrete-event systems with uncertain observations. In: Proc. of the 25th Int'l Joint Conf. on Artificial Intelligence (IJCAI 2016). New York, 2016. 1265−1271.

[16] Lamperti G, Zanella M. Monitoring of active systems with stratified uncertain observations. IEEE Trans. on Systems, Man, and Cybernetics—Part A: Systems and Humans, 2011,41(2):356−369. [doi: 10.1109/TSMCA.2010.2069096]

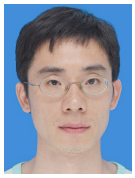
附中文参考文献:

[4] 韩旭,史忠植,林芬.基于模型诊断的研究进展.高技术通讯,2009,19(5):543−550.

[5] 赵相福,欧阳丹彤.离散事件系统基于模型诊断的研究进展.计算机科学与探索,2011,5(2):114−127.

[6] 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. http://www.jos.org.cn/1000-9825/4585.htm [doi: 10.13328/j.cnki.jos.004585]

[9] 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. http://www.jos.org.cn/1000-9825/4028.htm [doi: 10.3724/SP.J.1001.2012.04028]



文习明(1979－),男,湖北洪湖人,博士,讲师,主要研究领域为人工智能,知识表示与推理.

常亮(1980－),男,博士,教授,CCF 高级会员,主要研究领域为知识表示与推理,形式化方法,数据与知识工程.

余泉(1979－),男,博士,教授,主要研究领域为模态逻辑,描述逻辑和多智能主体认知规划.

王驹(1950－),男,博士,研究员,博士生导师,CCF 专业会员,主要研究领域为数理逻辑,人工智能,计算机理论.