软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(3):465−475 [doi: 10.3724/SP.J.1001.2012.04028]

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

不完备模型下的离散事件系统诊断方法*

王晓宇[1,2], 欧阳丹彤[1,2+], 赵 剑[1,2]

[1](吉林大学 计算机科学与技术学院,吉林 长春 130012)

[2](吉林大学 符号计算与知识工程教育部重点实验室,吉林 长春 130012)

Discrete-Event System Diagnosis upon Incomplete Model

WANG Xiao-Yu[1,2], OUYANG Dan-Tong[1,2+], ZHAO Jian[1,2]

[1](College of Computer Science and Technology, Jilin University, Changchun 130012, China)

[2](Key Laboratory of Symbolic Computation and Knowledge Engineering of Ministry of Education, Jilin University, Changchun 130012, China)

+ Corresponding author: E-mail: ouyangdantong@163.com

Wang XY, Ouyang DT, Zhao J. Discrete-Event system diagnosis upon incomplete model. *Journal of Software*, 2012,23(3):465−475. http://www.jos.org.cn/1000-9825/4028.htm

Abstract: There are two properties of incomplete: the incomplete of model definition and causality. With the condition of incomplete model definition, the method of constraint between online observation and the off-line model are proposed to process disordered and undefined events to obtain practical trajectory. Contrast to no being diagnosed by a complete model, this method expands the applicative scope and breaks the model limitation. On condition of causality incomplete, the usage of causal diagram to connect components is proposed. This method solves the halfway diagnostic problem caused by setting models separately, meanwhile enhancing accuracy. It has been tested that the diagnostic way under those two conditions brings out expected results according to certain incomplete models. It also reformulates model partially and improves the model maturity.

Key words: dynamic diagnosis; incomplete model

摘 要: 提出不完备模型的两种不完备性:模型定义不完备和因果关系不完备.在模型定义不完备条件下,用在线观测与模型共同约束的方法处理观测乱序及未定义事件,得到可行的诊断轨迹.相对于基于完备模型假设下不能诊断的结论,该方法扩展了诊断方法的适用范围,放松了对模型的约束要求.在因果不完备条件下,提出用因果图联系部件,解决分布式诊断中由于部件独立建模而导致的不彻底诊断,提高了诊断的精确性.通过实验验证,两种条件下的诊断方法均能在相应的不完备模型中得到预期诊断结果,并对模型进行局部修订,提高模型的完备性.

关键词: 动态诊断;不完备模型

中图法分类号: TP181 **文献标识码**: A

* 基金项目: 国家自然科学基金(60973089, 60873148, 60773097, 61003101); 吉林省科技发展计划项目基金(20101501, 20100185, 20090108, 20080107);教育部博士点专项基金(20100061110031); 浙江省自然科学基金(Y1100191); 欧盟合作项目(155776-EM-1-2009-1-IT-ERAMUNDUS-ECW-L12); 吉林大学符号计算与知识工程教育部重点实验室开放项目(93K-17-2009-K05)

收稿时间: 2010-12-24; 修改时间: 2011-01-31; 定稿时间: 2011-04-02

1 离散事件系统诊断背景

离散事件系统诊断是一种基于模型诊断的动态方法[1−3],通过离线模型的建立和在线观测,共同得出观测到达之前的系统运行过程.该方法对于已经成熟的静态诊断方法进行了一定的扩展,不仅可以指出部件级别的故障,还能够指出这些故障的原因[4].同时,在运行动态诊断方法时,系统不必完全停机,使得诊断方法能够更好地应用于实时系统监测[5].

离散事件系统的基于模型诊断方法将系统映射成为某种模型(Petri网[6]、自动机[1,7]等),部件行为在动态诊断模型中映射为事件或状态.而系统从初始状态开始到最后停机期间所能进行的全部工作根据系统特性被映射成为全局模型或局部模型组.对于小型系统,全局模型有很好的执行效果[8];对于有明显边界标志的分布式系统,分布式的模型能够在短时间内并行执行并得到诊断结果[9,10].而在时序定义完全的系统上,自动机链模型的增量方法能够依据已有结果专注于当前模型段,通过在线诊断和诊断结果重用来加速[11,12].

上述方法基于一个共同的假设:模型完备.即当观测序列到达时,必能在待诊断空间内找到相容的轨迹.但随着系统规模的扩张,建立起一个能够涵盖所有系统行为细节模型的难度也随之迅速增加.

为了满足精确的故障诊断及隔离(FDI),或者用更多的领域知识对系统模型进行加细,或者对诊断系统的框架进行重定义,使其能够对模型不完备做出合理的处理.前者在模型的普适性和可扩展性上成本较高;而后者能够根据观测动态调整模型,更适应复杂且不断扩张的系统.

不完备模型的基于模型诊断最早由文献[13]提出,处理静态系统上由于局部观测的不完备而导致的多候选诊断.文献[14]将这种方法扩展到离散事件系统上,提出了在模型自动机的事件缺失的情况下,如何根据观测自动机进行同步,得到候选诊断路径的方法.同时定义了不完备度的概念,指出当不完备度在[0,1]上变化时,对诊断路径规模的影响.

模型的另一种不完备性在于因果关系不完备.文献[15]指出:在静态诊断系统中,若模型因果不完备,会导致极小碰集丢失解,从而得到不彻底诊断.并提出了用因果图解决这种不彻底诊断的方法.

总体上,不完备模型是指由于建模时某些行为描述的缺失,导致对运行中出现的事件或者状态出现不能解释的情况.这些事件和状态相对于系统来说是突发的,不完备模型上的诊断方法能够处理该类系统突发事件,给出一个相对合理的解释.这相对于仅能处理定义事件的完备假设下的诊断方法是一种突破.

本文通过对不完备模型的研究,扩展了完备模型下的诊断方法,得到不同程度不完备模型下的诊断方法:

(1) 在事件时序定义不完备的条件下,提出用无序集合的方法解决与传感器无关的观测序列混乱的问题.根据观测序列的时序和模型的逻辑关系,确定观测序列对应的诊断结果.一方面放松了对转移函数定义的要求,缩减了模型空间;另一方面对传感器发回序列的顺序要求有所降低.

(2) 对未定义事件的处理是不完备模型下诊断的核心问题,本质是对突发情况的处理,这种突发情况往往是建模过程中未曾考虑但会影响诊断结果的关键问题.已有的完备假设条件下的诊断对这种突发状况无能为力,现有的经典诊断方法和系统也都是建立在模型完备的假设上.为了取消这种限制模型规模和应用的假设,提出用观测序列中未定义事件的闭包计算来解决不完备模型上的诊断,得到可能的模型轨迹,并将未定义事件根据时序推理加入模型中.

(3) 因果不完备出现在分布式诊断中,分布式诊断是在部件层次上进行的诊断.由于诊断空间小,并行计算诊断效率很高,但是部件之间的交互被忽略.因此,出现了由于故障传播影响的故障误判和不彻底诊断问题.我们提出用因果图来描述部件隐含的因果关系,考虑部件之间交互,从而除去冗余的诊断结果,得到故障根源.

不完备模型上的诊断方法能够在现有模型不能诊断的空间上得到诊断结果,使诊断方法有更好的模型适应性和更精确的诊断结果.

本文第 2 节给出基本定义,简述在完备模型下,诊断的基本方法和模型框架.第 3 节提出事件定义不完备模型的诊断方法.第 4 节提出因果定义不完备模型的诊断方法.第 5 节给出实验结果、适用范围、相应分析及工作展望.

2 完备诊断模型框架

在离散事件系统诊断中,常用自动机对实际系统进行建模.自动机的每个状态表示一段持续稳定的局部或系统情况,每个事件则描述的是系统中发生的一些改变.在离散事件系统中,模型框架通常可以定义如下:

定义 1(自动机)[9]. 自动机定义为一个五元组$A=(S,E,T,I,F)$,其中,S是状态集合,包含空状态$\varnothing$;E是事件集合,包含空事件ε;T是转移集合,$T\subseteq S\times E\times S$,表示系统从一个状态经某事件触发转移到另外一个状态;I是初始状态集合,$I\subseteq S$;F是终止状态集合,$F\subseteq S$.

为了将转移的状态和事件加以区分并且保持原有的状态与事件之间的关系信息,给出定义 2~定义 4:

定义 2(转移条件). 若有状态、事件和转移等集合符合定义 1,定义转移条件Φ_{pre}为如下函数:

$$\Phi_{pre}(t)=(\exists t\in T)((t=s_1\times e\times s_2)\rightarrow s_1)\wedge(s_1\in S)\wedge(e\in E).$$

定义 3(转移结果). 若有状态、事件和转移等集合符合定义 1,定义转移结果Φ_{res}为如下函数:

$$\Phi_{res}(t)=(\exists t\in T)((t=s_1\times e\times s_2)\rightarrow s_2)\wedge(s_1\in S)\wedge(e\in E).$$

定义 4(触发). 若有状态、事件和转移等集合符合定义 1,定义触发Φ_e为如下函数:

$$\Phi_e(t)=(\exists t\in T)((t=s_1\times e\times s_2)\rightarrow e\wedge(s_1\in S)\wedge(s_2\in S)\wedge(e\in E)).$$

转移条件经过触发到达转移结果,而转移结果又可以作为下一个转移的转移条件,则在自动机中可以表示成为一个状态事件交替出现的动作序列,描述了系统的变化过程,称作一条轨迹.

定义 5(轨迹)[16]. 在自动机中,定义$traj=\langle s_0e_0s_1e_1\ldots s_ie_i\ldots e_ns_{n+1}\rangle, s_i\in S, e_i\in E$.

轨迹是一条状态与事件间隔出现的序列,表示状态由事件触发转移到另外一个状态,事件不断到来,驱动状态改变的一个过程.从初始状态到终止状态,可以接受的轨迹称为一条路径.

定义 6(路径)[16]. 路径$path$定义为如下的轨迹:$traj=\langle s_0e_0s_1e_1\ldots e_{n-1}s_n\rangle, s_0\in I, s_n\in F$.

路径的定义与轨迹的定义类似,区别在于定义了初始状态和终止状态.路径能够表示系统的一次完整运行过程.

定义 7(事件相关). 若$e_1,e_2\in traj$,e_1,e_2事件相关.

事件相关的定义是为了与观测序列相联系,实际观测到的只有事件而非状态.

定义 8(观测). $o\in E$,若 o 是可以被传感器探测到并返回诊断器的事件,则定义谓词 $OBS(o)$为真;否则,$OBS(o)$为假.

观测事件是系统中的特定事件集合,包含于事件集合.这些事件是在线计算中不可或缺的.在一段在线时间内观测到的事件序列被称为一个观测窗口.模型中所有与观测窗口事件序列相容的轨迹(路径),都被当作诊断结果.

定义 9(观测序列)[7]. 在一条轨迹$traj=\langle s_0e_0s_1e_1\ldots s_ie_i\ldots e_{n-1}s_n\rangle$,对$traj$中的全部状态和事件向观测事件上进行投影,得到一条可观测事件的序列,称为观测序列,记为Obs.映射P定义如下:

$$P(x)=\begin{cases}\lambda, \text{ if } OBS(s_i\in S)\\ \varepsilon, \text{ if } (OBS(e_i)=\text{false})\wedge(e_i\in E).\\ e_i, \text{ if } (OBS(e_i)=\text{true})\wedge(e_i\in E)\end{cases}$$

映射 P 的意义在于将实际传感器观测不到的状态和事件在轨迹中除掉,模型中全部轨迹在映射下得到的是在线观测所能得到的全部事件序列集合.

定义 10(观测相容序列)[7]. 观测相容序列是观测序列的逆映射,若有观测序列$Obs=\langle o_1o_2\ldots o_i\ldots o_n\rangle$定义$P^{-1}$为一个映射:$P^{-1}(Obs)=\forall traj, P(traj)=Obs$. $traj$称为观测相容序列.

定义 9 和定义 10 是一个互逆的过程,但不是一一映射.给定一条轨迹,在映射P下,有且只有一条与之相应的观测序列,但是若给定观测序列,在逆映射P^{-1}下将变得较为复杂.

在完备模型的诊断器中,逆映射的结果是一条或者多条候选轨迹.若模型出现不完备,逆映射结果是完全不确定的,能否得到诊断轨迹是不确定的,得到多少条轨迹也是不确定的.为了在不完备模型条件下给出候选结果,下文将提出一种诊断框架.

3 事件不完备下的诊断方法

在基于完备模型假设的离散事件系统诊断中,诊断根据在线观测事件序列,在离线的模型中寻找相容路径或者轨迹.模型完备的假设保证了根据观测事件必能找到一条解释观测事件并与模型行为相容的路径,取消假设则不能保证路径的得出.在复杂系统中,预定完备模型仅存于有一定抽象的假设之中,需要有更多的专家知识和细节知识作为模型背景才能够建立良好的系统模型.不完备模型方法放松了这种假设的约束,根据有限的观测与模型的重构进行诊断,并可以对模型加以修正.

3.1 不确定事件顺序

首先放松最简单的约束:模型顺序相对观测事件不完备.这里不包括由于传感器的不稳定性导致诊断器收到的观测序列与实际序列不符[17].本文中的事件顺序不完备是指:存在观测事件序列,其到达顺序与发出顺序相同,在模型中不存在一条与观测相容的模型轨迹.当观测到与模型不相容的轨迹时,考虑存在非严格定义的事件顺序.

以动态诊断中经典的三容水箱为例,向水箱 $C3$ 中注入中水位水,定义规程事件为关闭 $R4$,打开 $R3$,打开 $Sf1$;而在当前的初始状态下,按照打开 $Sf1$,打开 $R3$,关闭 $R4$ 的动作序列也是可行的.

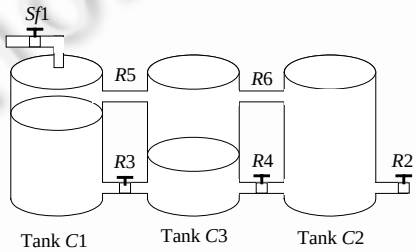

Fig.1 Triple container

图 1 三容水箱

在打开 $Sf1$ 之后的一段时间内,打开 $R3$ 是可行的,而当时间过长,$C1$ 中的水将从管道 $R5$ 流向 $C3$,$C1$ 溢出.或者在打开阀门 $Sf1$,$R3$ 之后,未关闭 $R4$ 阀门,导致的结果是 $C3$ 始终未满.因此可以得到下述结论:事件序列顺序的不完备是可行的;顺序不完备的事件序列需要有时间的约束.为了在时间上对事件序列顺序混乱有所约束,给出如下的定义:

定义 11(相对时间). $\exists e_1,e_2\in E$ 且 e_1 与 e_2 相关.设 e_1 发生的时间为 x_1,e_2 发生的时间为 x_2,则 $\max|x_2-x_1|$ 定义为 e_1 与 e_2 之间的相对时间,记作 $RT(e_1,e_2)$.

相对时间的值域定义在 $[1,\infty)$ 上,且为整数.当相对时间为 1 时,二者连续发生.在相对时间的基础上,向自动机中加入时间上的约束.

定义 12(时序自动机). 定义时序自动机 $TA=(S,E,T,R,I,F)$,其中,R 是相对时间集合.$\forall RT(e_1,e_2)\in R,e_1,e_2\in E$.

基于时间自动机,可以建立一个解决观测序列与模型不相容的模型框架.对于调度序列不唯一的事件划分无序集合,在出现不相容的观测序列时,放松对模型事件顺序的约束.

定义 13(相关事件闭包). $\exists e_i\in E,i=0,1,2,\ldots,n,e\in E$,若存在最小的事件集合 $E_{\min}$,使得 $\forall e_i\in E_{\min}$,都与 $E_{\min}\backslash e$ 中所有的事件相关,而 $\forall e_i\notin E_{\min}$ 不能与 $E_{\min}$ 中全部事件相关,则称 $E_{\min}$ 是一个相关事件闭包.

定义 14(无序集合). $\exists e,e_0,e_1,\ldots,e_n\in E_{\min}$ 为相关事件闭包,且 e 与 $e_0,e_1,\ldots,e_n$ 的相对时间为 $RT(e,e_0),RT(e,e_1),\ldots,RT(e,e_n)$.若存在多于一个无时序冲突的事件序列,则 $e_0,e_1,\ldots,e_n$ 构成了一个关于 e 的无序集合,记作 $\Psi(e)$.

无序集合划分对于离散事件系统的基于模型诊断来说是懒惰的,仅在完备假设下不存在相容轨迹时才考虑观测乱序,并开始计算无序集合.

在三容水箱的例子中,定义 $RT(OpenSf1,OpenR3)=2$,$RT(OpenSf1,CloseR4)=2$,设每个事件执行到下一个事件

执行的间隔为 1.那么,*OpenSf*1,*OpenR*3,*CloseR*4 这 3 个事件可以按照⟨*OpenSf*1,*OpenR*3,*CloseR*4⟩或⟨*OpenSf*1,*CloseR*4, *OpenR*3⟩排列.因此有关于 *OpenSf*1 的无序集合 Ψ(*OpenSf*1)={*OpenSf*1,*CloseR*4,*OpenR*3}.

这些与预定事件序列不一致的观测序列可以用时序的方法加以解决.当观测事件序列出现与模型定义不一致的时候(此时诊断过程已经执行过诊断,但是找不到一致的轨迹),在一致的事件序列与不一致的事件序列的边界上计算无序集合,根据时序关系得出可行的一致性轨迹.下面给出算法 1.

算法 1. 时序不完备的诊断方法 Incomplete EventTime Model Diagnosis(IETMD).

输入:时间自动机模型$A=(S,E,T,R,I,F)$,观测序列$Obs=\langle o_1,o_2,\ldots,o_n\rangle$;

输出:轨迹 *traj*.

1. Initial: $\Gamma\leftarrow s_i,s_i\in I$
2. until $\Gamma\subseteq F$ do
3. if $t\in T,t=s\times e\times s',e\in E\cap Obs$
4. for all t
5. *Union*(*traj*,*t*),*Update*(*s*,*s*′,Γ)
6. else
7. $\exists t\in T,t=s\times e\times s',e\in E,e\notin Obs$
8. *Union*(*path*,*t*),*Update*(*s*,*s*′,Γ)
9. *loop*
10. if $\neg(\exists traj)$ consist with *Obs*
11. $o\leftarrow o_1,\Pi\leftarrow Obs$
12. compute $\Psi(o)$
13. for all $o_i\in\Psi(o)$
14. search $t\in T,t=s\times e\times s',e\in E\cap\Pi$
15. *Sequence*(*t*),*Union*(*traj*,*t*),*Update*(*s*,*s*′,Γ)
16. if $\Psi(o)\in Obs$
17. $\Pi=Obs\setminus\Psi(o),o=first(\Pi)$
18. goto step 12
19. else
20. Return *traj*.

Uinon 函数的作用是将转移连接到相应的轨迹中去.在诊断过程中,可以出现多个相同观测事件,产生多条相容轨迹,故保留多条候选相应的诊断结果.*Update* 函数的作用是将当前状态更新,将一个转移的条件状态映射到结果状态上去,自动机向终止状态运行一步.*Sequence* 函数的作用是将当前找到的转移按照时间自动机中预定的时间进行调度,按照观测到的实际顺序整理出一条合理且相容的轨迹.first 函数是将现有观测序列中首个观测事件取出.

本节提出的方法仅放松了事件序列的完备性,即:得到正确顺序且已知的观测序列,但可能不存在一条轨迹与该观测序列一致.常规诊断在这种情况下,会陷入全局的盲目搜索中;而增加时序信息则限定了诊断空间,在常规诊断效率的线性时间内,得到了常规诊断不能得到的诊断结果.

3.2 在未定义事件观测上的诊断方法

继续放松对事件的约束,在排除观测到的未定义事件是由正常事件变形所导致之后,考虑一类未定义事件的出现:即不完备的事件集合,记作E_{in}.不完备的事件集合是对模型进行的重新定义.

对于不完备事件集合的出现,首先需要判断的是该事件是否为故障事件,以决定为系统的模型中添加故障行为还是正常行为.根据对该事件的所在轨迹系统行为进行推导,通常有如下 4 种情况:

(1) 若该事件所在的轨迹的前期轨迹和后续轨迹均为正常行为,该事件应该是一个正常事件;

(2) 前期轨迹是正常行为轨迹,后续轨迹出现了故障,则该事件应予考虑为故障事件;

(3) 前期轨迹是故障行为,而后续轨迹为正常行为,则该事件为前期故障的互补事件,彼此作为故障掩盖;

(4) 前期轨迹为故障轨迹,后续轨迹依然为故障轨迹,则该事件为故障事件.

在 4 种情况下,对未定义事件的集合作进一步的划分:不确定正常事件集合 E_{in}^{N},不确定故障事件集合 E_{in}^{F},不确定掩盖事件集合 E_{in}^{R}.

本节工作主要集中在不确定的模型下,根据观测得到未定义部分的信息,对未定义信息进行穷因、推理、抽象,并得到一个重构的模型.该工作需要在原有模型的事件集合基础上,根据观测得到的未定义事件集合,对模型的行为进行时序推理、事件调整、轨迹重定义等一系列工作.首先定义不完备的事件集合:

定义 15(不完备事件集合). $\forall e\in E_{in}(OBS(e)=\text{true})\wedge(e\notin E)$,其中,$E_{in}$是不完备事件集合,$E$是自动机中的事件集合,$OBS(e)$是判断事件能否观测的谓词.

不完备事件集合中的事件均是被观测到的,但是未被离线建立的模型所定义的事件.对该事件的出现,轨迹中应当能够将其分离出来,而剩余的轨迹不受这种分离的影响.因此,对于某事件,存在着一个最小的不受影响的轨迹集合.

定义 16(前缀闭包). 若存在事件集合$Q=\{e_i\}$,$\forall e\in Q(\exists \Psi(e_i)\vee(e_i\in(\Psi(e_j),e_j\in Q)))$,$\Psi(e_i)$有唯一的时间上限,且$\forall e'\notin Q,\bigcup_{e_i}\in Q\bigcup\Psi(e')\Rightarrow\perp$,则称$Q$为前缀闭包,记作$\Psi^{+}(Q)$.

定义 17(后缀闭包). 若存在事件集合$R=\{e_i\}$,$\forall e\in R(\exists \Psi(e_i)\vee(e_i\in(\Psi(e_j),e_j\in R)))$,$\Psi(e_i)$有唯一的时间下限,且$\forall e'\notin R,\bigcup_{e_i}\in R\bigcup\Psi(e')\Rightarrow\perp$,则称$R$为后缀闭包,记作$\Psi^{-}(Q)$.

上述两个定义从时间上限制了未定义事件的时序,未定义事件的出现在后缀闭包之后以及前缀闭包之前.观测事件序列由未定义事件进行划分.未定义事件之前的观测事件在后缀闭包中进行诊断,而之后的观测事件在前缀闭包中进行诊断,未定义事件的定义由两段诊断结果共同决定.在算法 1 的基础上,添加对未定义事件的处理.事件乱序和事件未定义合成事件不完备.

算法 2. 事件不完备下的诊断方法.

输入:自动机 A 时序自动机 TA,观测集合 Obs;

输出:诊断结果,不完备事件集合 $E_{in}=E_{in}^{N}\cup E_{in}^{F}\cup E_{in}^{R}$.

1. 初始化:
2. do
3. $CompleteModelDiagnsosis(A,Obs)$.
4. until consist
5. If method IETMD return complete result
6. return $diagnosis(TA,Obs)$
7. else
8. $\exists e_i\in Obs,e\notin E$
9. $obs_1=\langle e_1,\ldots,e_{i-1}\rangle,obs_2=\langle e_{i+1},\ldots,e_n\rangle$
10. compute $\Psi^{+}(obs_1),\Psi^{-}(obs_2)$
11. $dia_1=diagnosis(\Psi^{+}(obs_1),obs_1)$
12. $dia_2=diagnosis(\Psi^{-}(obs_2),obs_2)$
13. if $\exists AB(e_m)\in dia_1\&\&\neg\exists AB(e_n)\in dia_2$
14. $E_{in}^{F}=E_{in}^{F}\cup\{e_i\}$
15. $Add(T,e_i)$
16. $dia=dia_1\oplus e_i\oplus dia_2$
17. if $\exists AB(e_m)\in dia_1\&\&\neg\exists AB(e_n)\in dia_2$

18. $E_{in}^{R}=E_{in}^{R}\cup\{e_i\}$
19. $Add(T,e_i)$
20. $dia=dia_1\oplus e_i\oplus dia_2$
21. if $\neg\exists AB(e_m)\in dia_1\&\&\neg\exists AB(e_n)\in dia_2$
22. $E_{in}^{F}=E_{in}^{F}\cup\{e_i\}$
23. $Add(T,e_i)$
24. $dia=dia_1\oplus e_i\oplus dia_2$
25. if $\neg\exists AB(e_m)\in dia_1\&\&\neg\exists AB(e_n)\in dia_2$
26. $E_{in}^{N}=E_{in}^{N}\cup\{e_i\}$
27. $Add(T,e_i)$
28. $dia=dia_1\oplus e_i\oplus dia_2$
29. return dia.

4 因果不完备

因果不完备是不完备模型的另一种表现:在分布式系统中,诊断器建立在部件层上,每个诊断结果的诊断空间仅为单独的部件行为轨迹.当出现故障传播或超越部件级别的故障时,分布式诊断将无法得出完整的诊断结果.因果不完备的出现是由于部件之间的因果联系部分没有显式表达,诊断系统对此不予以考虑而造成的.分布式系统中,各部件之间由于协作任务或顺序执行,存在着协作上或时间上的隐含约束,对这种隐含约束的忽略造成了分布式诊断中不完备的结果.这种结果可以导致故障的反复发生,且该故障不是根源性的故障.

本文提出用故障传播与部件因果图结合的方法来解决因果不完备的诊断.故障传播是指在系统运行过程中,已经发生的故障不会消失,是随着系统运行而传播,从而对接下来发生的正常事件有所影响的情况.在模型中,已经发生的故障事件可以表示为自动机可接受的事件序列的前缀.即若$\exists traj=\langle s_0e_1s_1e_2\ldots e_is_i\ldots e_ns_n\rangle$且$e_j$是故障事件,则$e_{j+1}\ldots e_n$是受故障传播影响的事件.

定义 18(部件因果图). 定义部件因果图是一个二元组$CTG=(N,R)$,其中:N是一个有序对的集合,$N=(A_i,t_i)$,$t_i\in A_i$,A_i是自动机链中的一个自动机,t_i是A_i中的一个转移,且t_i的触发事件是一个通信事件c_i;R是一个二元关系集合,$R\subseteq N\times N$.

图2给出的一组自动机包含3个相关的部件.其中:通信事件是相同事件,对于相连部件是可见的;而除通信事件之外的事件对相连部件不可见.

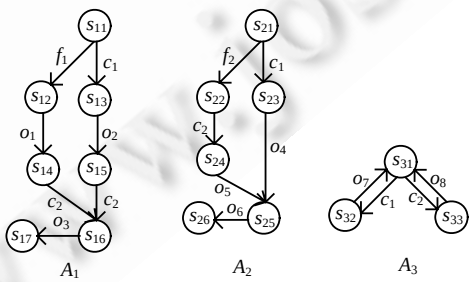

Fig.2 Example for automaton team

图2 自动机组例

从全局角度看部件自动机以及部件因果图,可以得到一个联系了所有相关部件的因果图,如图3所示.

根据部件因果图,可以在部件级诊断器的基础上建立一个面向全局的诊断,该诊断考虑了部件之间相互影响的因果关系,同时在时间和空间上是局部诊断量级,无需扩展到全局诊断上.

引入两个函数计算通信事件的映射和逆映射:

定义 19(通信事件映射). 设有自动机$A_i=(S_i,E_i,T_i,I_i,F_i)$,通信事件$c_i\in E$,$Proj(A_i)=c_i$是自动机$A_i$到通信事件上的一个映射.

定义 20(通信事件逆映射). 若$Proj(A_i)=c_i$,则定义$\Sigma=Proj^{-1}(c_i)$是一个自动机的集合,满足$Proj(A_j)=c_i$.

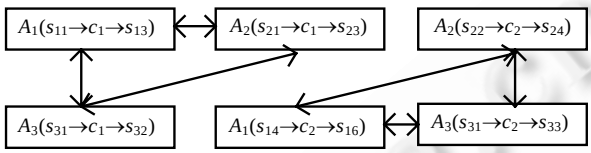

Fig.3 Component causal relation

图 3 部件因果图

在离散事件系统诊断中,求解一条最短或包括故障最少的相容轨迹未必是完全正确的,至少未必是完备的诊断结果.根据部件因果图向诊断结果中追加轨迹的方法可以进一步解释故障原因,虽然这种方法增加了轨迹的长度,却能够给出更合理而完备的诊断结果.具体的方法见算法 3.

算法 3. 因果不完备诊断方法.

输入:自动机链$\Omega=(A_1,A_2,\ldots,A_n)$,观测窗口组$W=(Obs_1,Obs_2,\ldots,Obs_n)$;

输出:因果不完备结果轨迹 *traj*.

1. $\Delta=Diagnosis(A_i,Obs_i)$
2. for all $c_i\in\Delta$
3. compute $\Sigma=Proj^{-1}(c_i)$
4. for all $A_j\in\Sigma$
5. if $Diagnosis(A_j,Obs_j)$ exist fault
6. $traj=Diagnosis(A_i,Obs_i)\oplus Diagnosis(A_j,Obs_j)$
7. else
8. $traj=Diagnosis(A_i,Obs_i)$
9. return *traj*

算法在当前的部件自动机A_i上进行局部诊断,根据在诊断结果中的通信事件计算与A_i的当前诊断轨迹有关联的部件集合.在每个共享通信事件的逆映射集合上,得出故障传播的路径.如果有故障,则将两个故障联系起来并同步得到高层结果;否则,不考虑故障.图 4 是在图 2 中所列的自动机组上的一个简单例子.

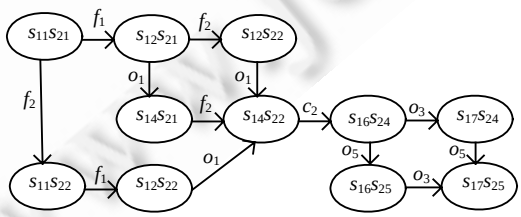

Fig.4 Diagnosis by synchronization

图 4 同步诊断结果

给定自动机A_1,A_2,A_3,观测分别是$\langle o_1o_3\rangle$,$\langle o_5o_6\rangle$,$\langle o_8\rangle$.在自动机A_2中得到的诊断结果是$\langle s_{21}f_2s_{22}c_2s_{24}o_5s_{25}o_6s_{26}\rangle$,且包含故障事件$f_2$,则该诊断结果是一条故障轨迹.该轨迹包含通信事件$c_2$.在通信事件$c_2$上,有$\sum c_2=\{A_1,A_3\}$;$A_1$的诊断结果是$\langle s_{11}f_1s_{12}o_1s_{14}c_2s_{16}o_3s_{17}\rangle$,包含故障事件;$A_3$的诊断结果为$\langle s_{31}c_2s_{33}o_8s_{31}\rangle$,没有包含故障事件.全局诊断器认为,$A_1$与$A_2$相互影响,并将诊断结果同步为一个同步机,如图 4 所示,而A_3不受A_2的故障影响,独立得到本

地的诊断结果.

由得出的结果可以看出,同步的诊断结果可以包含A_1和A_2的局部诊断,并且能够得到多故障的相互影响结果.更进一步,如果部件独立窗口的时间顺序能够联合有序,则可以在当前诊断结果上化简到线性的空间,且计算诊断的时间也是线性的.这种同步的诊断结果包含了更完备的信息,可以得到接近于全局完备性的诊断结果,而基本保留局部诊断的时间.

5 实验结果

5.1 事件不完备实验结果

在离散事件系统的基于模型故障诊断中,标准测试集均约束于模型完备的条件.本文实验建立在标准测试集合的基础上[18],在标准测试集的状态与事件上添加时钟,并且将模型中的某些事件删除或作乱序处理,得到诊断时间和找出原模型中的常序事件的正确率,见表 1.

Table 1 Results of time and correct ratio under different disorder miss order level

表 1 不同乱序率下花费时间和正确率结果

乱序率组1: 模型规模20	乱序率组2: 模型规模100	乱序率组3: 模型规模400	乱序率组4: 模型规模1 000	乱序率组5: 模型规模2 000	
5%	0.47s/100%	0.93s/100%	1.88s/100%	4.01s/100%	9.83s/100%
10%	0.53s/100%	1.09s/100%	2.1s/100%	4.92s/100%	12.09s/99%
20%	0.7s/100%	1.35s/100%	2.43s/100%	5.89s/100%	16.45s/97%
40%	0.98s/100%	1.87s/100%	2.92s/98%	7.34s/98%	21.6s/95%
80%	1.39s/100%	2.04s/99%	3.87s/96%	9.7s/95%	30.87s/92%
100%	1.86s/100%	3.5s/97%	5.2s/93%	15.2s/92%	45.6s/90%

未定义事件的诊断测试选择了一个较小规模的测试集合(状态数 400),当缺失事件占观测比例不同时,得到诊断结果的时间和候选结果的规模也有所不同,见表 2.值得注意的是,当未定义事件占观测事件的比例不断增加时,候选诊断结果将以指数级增加.当未定义事件达到较高的比例时,候选诊断空间过于庞大,失去了诊断的意义.

Table 2 Results of time and number of candidate trajectorises under different ratio undefined events

表 2 不同未定义事件比例下的诊断时间和候选轨迹数

未定义事件比例 (%)	时间 (s)	得到候选轨迹
5	0.53	3
10	0.68	8
20	1.15	42
40	1.61	201

由表 2 可见,当模型中存在较少未定义事件时,事件不完备的诊断方法能够在较合理时间内得到相应的诊断结果.当未定义事件在模型定义中占据比例更多时,可行的轨迹候选数量将急剧增加,因此计算和存储这些轨迹所耗用的时间和空间也随之相应增加.这不仅影响了诊断的速度,也影响了诊断结果的精确度,在诊断提取过程中,因为过多的冗余轨迹出现而导致失败.因此,事件不完备模型上的诊断方法所能够处理的未定义事件是有限的.

5.2 因果不完备实验结果

根据标准测试集[18],在 30 个有至少一个通信事件联系的部件上,每个部件有 6 个状态.待诊断的空间为 6^{30}.对因果不完备的情况进行诊断,仅针对因果不完备得到的诊断时间为 305ms,相比于在该标准测试集合上,2009 年得到的最好结果(7s~10s),诊断因果不完备并不占用较多时间,但是给出了更完备的结果.

不完备因果的诊断结果时间效果远低于诊断结果的原因在于:

(1) 该方法仅在某故障反复出现时对诊断结果的完备性提出质疑,在全部诊断过程中连续发生的特定故障比例较少,故因果诊断执行的次数较少;

(2) 因果诊断方法根据已经得出的常规诊断结果,在几个相关部件上运行.局部诊断结果已经存在,并且因果诊断的空间仅限定于几条轨迹,因此诊断时间较短.

5.3 适用范围和展望

无论是否存在着完备模型假设,诊断的基础空间均定义在离散事件系统上.表 3 从模型特点、时序要求、观测序列要求及其他特点等方面来讨论两种不完备性质与完备模型诊断空间的异同.

(1) 事件定义不完备的模型要求是有时序的离散事件系统,但是该要求并不是必要的.时序不存在时,退化为相对时间为 1,此时候选添加的轨迹会增加,但是依然能够得出;

(2) 因果不完备的模型是分布式,因仅在分布式诊断中才会产生因果不完备的情况.

Table 3 Different model and corresponding characters

表 3 模型与相应特点

类型	模型特点	时序要求	观测序列特点	其他特点要求
事件乱序	全局模型或分布式模型	模型要求基本有序观	测有序	无
事件不完备	全局模型或分布式模型	模型要求基本有序	观测事件可以不在模型中存在,且有序	无
因果不完备	分布式模型	无	无	有通信事件联合各部件
完备模型	全局模型或分布式模型	无	顺序、要求严格事件定义	无

上述各种方法适用于离散事件系统的诊断,凡是具有离散事件系统[19]特性的实际系统如通信网络[9]、航天器[20]等,均可以在运行过程中用上述系列方法进行监控和诊断.

在不完备模型上的诊断方法,可以通过对模型的基本行为和结构的研究扩展为自动建模方法,通过观测序列的添加完善行为细节.因果不完备方法可以对分布式系统诊断的模型进行重构,根据部件之间因果关系和部件自身行为框架,得到高层模型或分解模型,使之符合所要求的模型粒度.

References:

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

[2] Zad SH, Kwong RH, Wonham WM. Fault diagnosis in discrete-event systems: Framework and model reduction. IEEE Trans. on Automatic Control, 2003,48(7):1199−1212. [doi: 10.1109/TAC.2003.814099]

[3] Jiang SB, Kumar R. Failure diagnosis of discrete-event systems with linear-time temporal logic specifications. IEEE Trans. on Automatic Control, 2004,49(6):934−945. [doi: 10.1109/TAC.2004.829616]

[4] Sampath M, Lafortune S, Teneketzis D. Active diagnosis of discrete-event systems. IEEE Trans. on Automatic Control, 1998,43(7): 908−929. [doi: 10.1109/9.701089]

[5] Zhao XF, Ouyang DT. On-Line diagnosis of discrete event systems with two successive temporal windows. AI Communications, 2008,21(4):249−262. [doi: 10.3233/AIC-2008-0439]

[6] Ouali MS, Ait-Kadi D, Rrzg N. Fault diagnosis model based on Petri net with fuzzy colors. Computers & Industrial Engineering, 1999,37(1-2):173−176. [doi: 10.1016/S0360-8352(99)00048-0]

[7] 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]

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

[9] Pencolé Y, Cordier MO. A formal framework for the decentralised diagnosis of large scale discrete event systems and its application to telecommunication networks. Artificial Intelligence, 2005,164(1-2):121−170. [doi: 10.1016/j.artint.2005.01.002]

[10] Pencolé Y. Diagnosability analysis of distributed discrete event systems. In: Saitta L, Mantaras RL, eds. Proc. of the 16th European Conf. on Artificial Intelligence (ECAI 2004). Valencia: IOS Press, 2004. 43−47.

[11] Cordier MO, Grastien A. Exploiting independence in a decentralised and incremental approach of diagnosis. In: Veloso M, ed. Proc. of the 20th Int'l Joint Conf. on Artificial Intelligence (IJCAI 2007). Hyderabad: AAAI Press, 2007. 292−297.

[12] Grastien A, Cordier MO, Largouët C. Automata slicing for diagnosing discrete-event systems with partially ordered observations. Advances in Artificial Intelligence. 2005. 270−281. [doi: 10.1007/11558590_27]

[13] Console L, Dupré DT, Torasso P. A theory of diagnosis for incomplete causal models. In: Sriharan NS, ed. Proc. of the 11th Int'l Joint Conf. on Artificial Intelligence (IJCAI'89). Detroit: AAAI Press, 1989. 1311−1317.

[14] Zhao XF. Research on some problems about model-based diagnosis of discrete event systems [Ph.D. Thesis]. Changchun: Jilin University, 2009 (in Chinese with English abstract).

[15] Wolfgang M, Stumptner M. Modeling context-dependent faults for diagnosis. In: Frisk E, Nyberg M, Krysander M, Aslund J, eds. Proc. of the 20th Int'l Workshop on Principles of Diagnosis. Stockholm: Linkoping University, 2009. 211−218.

[16] Grastien A, Cordier MO, Largouet C. Incremental diagnosis of discrete-event systems. In: Giunchiglia F, ed. Proc. of the 19th Int'l Joint Conf. on Artificial Intelligence (IJCAI 2005). San Francisco: Morgan Kaufmann Publishers, 2005. 1564−1565.

[17] 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]

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

[19] Cassandras CG, Lafortune S. Introduction to Discrete Event Systems. 2nd ed., Springer-Verlag, 2008. 48−96.

[20] Kurien J, R-Moreno MD. Intrinsic hurdles in applying automated diagnosis and recovery to spacecraft. IEEE Trans. on Systems, Man, and Cybernetics—Part A: Systems and Humans, 2010,40(5):945−958. [doi: 10.1109/TSMCA.2010.2052035]

附中文参考文献:

[14] 赵相福.离散事件系统基于模型诊断的若干问题研究[博士学位论文].长春:吉林大学,2009.

王晓宇(1984－),女,吉林长春人,博士生,主要研究领域为基于模型诊断.

欧阳丹彤(1968－),女,博士,教授,博士生导师,CCF 高级会员,主要研究领域为自动推理,基于模型诊断.

赵剑(1980－),男,博士生,讲师,主要研究领域为基于模型诊断.