计算机科学
COMPUTER SCIENCE

离散事件系统弱可预测性的验证算法

曹卫华, 刘富春

引用本文

曹卫华, 刘富春. 离散事件系统弱可预测性的验证算法[J]. 计算机科学, 2023, 50(11A): 220800224-6.

CAO Weihua, LIU Fuchun. Verification Algorithm for Weak Prognosability of Discrete Event Systems [J]. Computer Science, 2023, 50(11A): 220800224-6.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220800224

离散事件系统弱可预测性的验证算法

曹卫华　刘富春
广东工业大学计算机学院　广州 510006

摘　要　对故障检测来说,预测比诊断更能降低故障对系统造成的损失,但即使大多数的故障事件串是可预测的,只要有一个故障事件串是不可预测只能诊断的,整个系统就是不可预测的,只能用诊断的方法处理,这对大多数的故障事件串是不利的。为此,提出了弱可预测性的概念。弱可预测性是对系统未来是否一定会处于故障状态这一情况的预测。相比可预测性,弱可预测性不要求所有故障事件串都是可预测的。对可预测的故障事件串,弱可预测性能够在故障发生之前发出警报,而对不可预测只能诊断的故障事件串,其也能在故障发生之后发出警报。文中构造了证明器来测试系统的弱可预测性,并基于这个证明器给出了测试系统弱可预测性的多项式复杂度的算法,给出了弱可预测性的充分必要条件。

关键词:离散事件系统;故障预测;弱可预测性;多项式复杂度;自动机
中图法分类号　TP206

Verification Algorithm for Weak Prognosability of Discrete Event Systems

CAO Weihua and LIU Fuchun
School of Computers,Guangdong University of Technology,Guangzhou 510006,China

Abstract　This paper proposes the concept of weak prognosability. For fault detection,prognosis can reduce the loss caused by faults to the system more than diagnosis. However,even if most fault strings are prognosable,as long as one fault string is unprognosable and can only be diagnosed,the whole system is unprognosable and can only be handled by diagnosis,which is unfavorable to most fault strings. The concept of weak prognosability can avoid this situation. Weak prognosability is the prediction of whether the system will be in a fault state in the future. Compared with prognosability,weak prognosability does not require all fault event strings to be prognosable. Weak prognosability can alarm the prognosable fault strings before the fault occurs,and it can also alarm the unprognosable but diagnosable fault strings after the fault occurs. A verifier is constructed to test the weak prognosability of the system,a polynomial algorithm of weak prognosability of the system is given based on the verifier,and the sufficient and necessary conditions of weak prognosability are also given.

Keywords　Discrete event system,Fault prognosis,Weak prognosability,Polynomial complexity,Automata

1　引言

本文研究离散事件系统的故障弱预测。离散事件系统是由异步突发事件驱动的具有离散状态空间的动态系统[1],在故障诊断[2-10]、故障预测[11-18]、可测性[19]、监督控制[20]、不透明性[21]等领域得到了广泛的研究和应用。

自从 Genc 等[11]提出离散事件系统的可预测性的概念后,离散事件系统的可预测性得到了广泛的研究[12-18]。文献[12]研究了离散事件系统的鲁棒故障预测,以处理观测损失的情况。文献[13-16]研究了离散事件系统的分布式故障预测,其中文献[13]给出了分布式故障预测的一个多项式算法,文献[14]的方法基于状态估计,文献[15]的方法基于推理,而文献[16]考虑具有有界延迟通信的离散事件系统的分布式故障预测。文献[17]研究了随机模型上的故障预测问题。文献[18]考虑了在观测永久丢失的情况下随机离散事件系统的故障预测问题。

上述文献对离散事件系统可预测性的研究都要求系统中所有故障事件串都是可预测的,如果系统中只有部分故障事件串是可预测的,其他故障事件串是不可预测只能诊断的,那么上述故障预测的方法是无法处理的,只能用故障诊断的方法处理。故障诊断和故障预测都是对系统故障的监督检测,但是诊断是在故障发生之后才发出警报而预测是在故障发生之前发出警报,因此预测比诊断更能避免故障对系统造成的损失。可预测性比可诊断性更强[11],一个系统是可预测的那它一定是可诊断的,但反过来未必成立,也就是说一个系统是可诊断的但它不一定是可预测的。在一个系统中即使大多数的故障事件串是可预测的,只要有一个故障事件串是不可预测只能诊断的,整个系统就是不可预测的[11],只能用诊断的方法来处理,所有的故障事件串都要在故障发生之后才能被发现和处理,这可能增加故障对系统造成的损失。这种只有部分故障事件串可预测的情况无法用文献[11]中可预测性的方法处理,而用文献[2]中可诊断性的方法处理也要在故障

基金项目:国家自然科学基金(61673122);广东省自然科学基金(2019A1515010548,2020A1515010941)
This work was supported by the National Natural Science Foundation of China(61673122) and Natural Science Foundation of Guangdong Province,China(2019A1515010548,2020A1515010941).
通信作者:曹卫华(hqu_cweihua@163.com)

发生后才能被发现和处理，这种情况下怎样才能让那些可预测的故障事件串中的故障在发生之前就被预测出来呢？文献[22]提出的DP-安全可控性可以解决这个问题，但它是将诊断和预测的方法结合在一起，相当于给系统同时做诊断和预测，和本文提出的弱可预测性的方法不同。弱可预测性去除了预测必须在故障发生之前完成的限制，所以比可预测性弱，它允许在故障发生之后才做出预测（是一种迟来的预测），从而对可预测的故障事件串能够在故障发生之前发出警报，而对不可预测只能诊断的故障事件串也能在故障发生之后发出警报。相比故障诊断对所有故障事件串都必须在故障发生之后才发出警报的处理方法，这种处理方法可以降低故障对系统造成的损失。

故障预测是对故障的预测，而故障弱预测本质上是对系统未来是否一定会处于故障状态的预测，也就是对系统未来的估计状态全都是故障状态这一情况的预测。因此它可能在故障发生之后才发出警报，但它并非要等系统的估计状态全都变成故障状态才发出警报，而是在估计状态为故障状态或预警状态时就发出警报，预警状态就是从该状态出发一定步数后必然发生故障的状态，因此它可能会比故障诊断更早发出警报。

相比故障预测要求所有故障事件串都是可预测的[11]，故障弱预测不要求所有的故障事件串都是可预测的，对系统的要求更低，所以它是一种弱预测，能够应用于更多的系统，扩充了预测的应用范围，适用于预测那些只有部分故障事件串可预测的系统。

本文提出了弱可预测性的概念，构造了证明器来测试系统的弱可预测性，给出了测试系统弱可预测性的多项式复杂度的算法，以及弱可预测性的充分必要条件。

2 离散事件系统

离散事件系统可以建模为确定自动机。

定义1[1] 一个确定自动机可以定义为 $G=(X,\Sigma,\delta,x_0)$，其中 X 是状态集合，Σ 是事件集合，$\delta:X\times\Sigma\to X$ 是状态转移函数，x_0 是初始状态。

对一个确定自动机 $G=(X,\Sigma,\delta,x_0)$，我们用 $L(G)$ 或者 L 表示 G 生成的语言，即 $L=L(G)=\{s\in\Sigma^*:(\exists x\in X)\delta(x_0,s)=x\}$，其中 Σ^* 表示在 Σ 上所有有限长度事件系列的集合，包括表示没有事件的 ϵ。为了方便起见，状态转移函数通常以下面的递归方式扩展为 $\delta:X\times\Sigma^*\to X$：对任意的 $s\in\Sigma^*$ 和 $\sigma\in\Sigma$，有：

$$\delta(x,\epsilon)=x$$

$$\delta(x,s\sigma)=\delta(\delta(x,s),\sigma)$$

事件集合 Σ 由可观事件集合 Σ_o 和不可观事件集合 Σ_{uo} 组成，即 $\Sigma=\Sigma_o\cup\Sigma_{uo}$。$\Sigma_f$ 表示故障事件的集合。对一个集合 X，$|X|$ 表示 X 中元素个数。$\Psi(\Sigma_f)$ 表示以 Σ_f 中的某个故障事件结尾的语言，即 $\Psi(\Sigma_f)=\{s\in L:(\exists\sigma\in\Sigma_f)s_f=\sigma\}$，其中 s_f 表示 s 的最后一个事件。包含故障事件的事件串被称为故障事件串。$\delta(x,\sigma)!$ 表示 $\delta(x,\sigma)$ 有定义。对任意 $s\in L$，$pr(s)$ 表示 s 的前缀集合，$|s|$ 表示 s 的长度，也就是 s 中的事件个数，L/s 表示 L 中 s 的后续语言，即 $L/s=\{t\in\Sigma^*:st\in L\}$，对任意 $n\in\mathbb{Z}$，s 的 n 步差距事件串 t 是只有在 $n\geqslant-|s|$ 时才存在并满足 $|t|-|s|=n$ 的事件串，s 的 n 步差距事件串集合定义为：

$$s\odot\Sigma^n=\begin{cases}s\Sigma^n, & \text{如果 } n\geqslant 0\\ \{t\in pr(s):|t|-|s|=n\}, & \text{如果 } -|s|\leqslant n<0\\ \varnothing, & \text{否则}\end{cases}$$

显然当 $-|s|\leqslant n<0$ 时，s 的 n 步差距事件串集合只包含一个元素，即 $|s\odot\Sigma^n|=1$，而当 $n<-|s|$ 时，s 的 n 步差距事件串集合不包含任何元素，即 $|s\odot\Sigma^n|=0$。

定义2[11] 映射 $P:\Sigma^*\to\Sigma_o^*$ 可以归纳定义为：$P(\epsilon)=\epsilon$，并且对 $s\in\Sigma^*$ 和 $\sigma\in\Sigma$ 有：

$$P(s\sigma)=\begin{cases}P(s)\sigma, & \text{如果 } \sigma\in\Sigma_o\\ P(s), & \text{否则}\end{cases}$$

P 的逆映射用 P^{-1} 表示。

对任意自动机 $G=(X,\Sigma,\delta,x_0)$ 和 $x\in X$，我们用 $L(G,x)$ 表示 G 中从 x 出发的语言，即 $L(G,x)=\{t\in\Sigma^*:(\exists s\in L)[\delta(x_0,s)=x\wedge t\in L/s]\}$，用 $L_\sigma(G,x)$ 表示 G 中从 x 出发并且以唯一的可观事件 σ 结尾的语言，即 $L_\sigma(G,x)=\{t\in L(G,x):(\exists u\in\Sigma_{uo}^*)t=u\sigma\}$。

3 弱可预测性

定义3 令 L 为离散事件系统 G 生成的语言，$\Sigma_f=\{\sigma_f\}$ 为故障集合，则 L 关于 Σ_f 和 P 是弱可预测的当且仅当 $(\forall s\in\Psi(\Sigma_f))(\exists n\in\mathbb{Z})[(s\odot\Sigma^n\cap L\neq\varnothing)\wedge(\forall t\in s\odot\Sigma^n\cap L)\mathbb{P}]$，其中，$\mathbb{P}:(\exists m\in\mathbb{N})(\forall u\in P^{-1}P(t)\cap L)(\forall v\in L/u)[|v|\geqslant m\wedge\sigma_f\notin u\Rightarrow\sigma_f\in v]$。

直观地说，一个离散事件系统 G 生成的语言 L 关于 Σ_f 和 P 是弱可预测的当且仅当对任意以故障结尾的事件串 $s\in\Psi(\Sigma_f)$，存在 $n\in\mathbb{Z}$，使得 $s\odot\Sigma^n\cap L\neq\varnothing$ 并且对任意 n 步差距事件串 $t\in s\odot\Sigma^n\cap L$，存在 $m\in\mathbb{N}$，使得对 L 中任意和 t 映射相同的事件串 u 及其任意后续 v，如果 v 的长度大于或等于 m（即 $|v|\geqslant m$）并且 u 中不存在故障（即 $\sigma_f\notin u$），则 v 中必然存在故障（即 $\sigma_f\in v$）。

例1 考虑图1中的系统 G，其中 $\Sigma=\{\alpha,\beta,u,f\}$，$\Sigma_o=\{\alpha,\beta\}$，$\Sigma_{uo}=\{u,f\}$ 和 $\Sigma_f=\{f\}$。根据图1可得 $\Psi(\Sigma_f)=\{\beta f,f\}$，当 $s=\beta f$，令 $n=-1$，则 $s\odot\Sigma^n\cap L=\{\beta\}$；令 $t=\beta$，则 $P^{-1}P(t)\cap L=\{\beta\}$；令 $u=\beta$，则 $L/u=\{f\alpha^*\}$。当 $m=1$，令 $v=f$，则 $|v|\geqslant m$，$f\notin u$ 和 $f\in v$。当 $s=f$，令 $n=2$，则 $s\odot\Sigma^n\cap L=\{f\alpha\beta\}$，令 $t=f\alpha\beta$，则 $P^{-1}P(t)\cap L=\{f\alpha\beta\}$，令 $u=f\alpha\beta$，则 $f\in u$。根据定义3可得系统 G 生成的语言 L 关于 Σ_f 和 P 是弱可预测的。这个例子中故障事件串 βf 是可预测的，当观察到可观事件串 β 时就可以发出警报，而故障事件串 f 是不可预测的，但它是可诊断的，在故障发生两步之后，当观察到可观事件串 $\alpha\beta$ 时就可以发出警报。所以根据文献[11]提出的可预测性的概念判断整个系统是不可预测的，无法用预测的方法处理，而根据文献[2]提出的可诊断性的概念判断整个系统是可诊断的，可以构造诊断器对系统进行在线诊断，但是对故障事件串 βf 的诊断只有在故障发生之后才能发出警报，也就是在故障发生一步之后，当观察到可观事件串 $\beta\alpha$ 才能发出警报，而这时故障可能已经对系统造成了一定损失，但弱可预测性可以避免这个损失，它对故障事件串 βf 可以在故障发生之前发出警报，而对故障事件串 f 这样不可预测只能诊断的串也能在故障发生之后发出警报，相比故障诊断对所有故障事件串都必须在故障发生之后才发出警报，故障弱预测对能预测的

故障事件串在故障发生之前发出警报而对不能预测只能诊断的故障事件串在故障发生之后发出警报的做法更能避免故障对系统造成的损失。

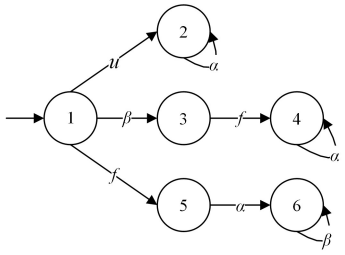

图 1　例 1 中的 G

Fig. 1　G in Example 1

弱可预测性和可诊断性是等价的。我们考虑了文献[2]中用形式化语言定义的可诊断性。大体说来,L 是可诊断的如果任意故障都能在一定时延后被诊断出来。下文简单回顾一下可诊断性的定义,如定义 4 所示。

定义 4　一个离散事件系统 G 生成的语言 L 关于 Σ_f 和 P 是可诊断的如果 $(\exists n\in\mathbb{N})(\forall s\in\Psi(\Sigma_f))(\forall t\in L/s)[|t|\geqslant n\Rightarrow\mathbb{D}]$,其中 $\mathbb{D}:w\in P^{-1}P(st)\cap L\Rightarrow\sigma_f\in w$。

命题 1(弱可预测性 VS 可诊断性)　令 L 为离散事件系统 G 生成的语言,则 L 关于 Σ_f 和 P 是弱可预测的当且仅当 L 关于 Σ_f 和 P 是可诊断的。

证明:用反证法证明充分性。假设 L 关于 Σ_f 和 P 是可诊断的但不是弱可预测的,则存在 $s\in\Psi(\Sigma_f)$,对任意 $n\in\mathbb{Z}$,有 $s\odot\Sigma^n\cap L=\emptyset$ 或者存在 $t\in s\odot\Sigma^n\cap L$,对任意 $m\in\mathbb{N}$,存在 $u\in P^{-1}P(t)\cap L$ 和 $v\in L/u$,使得 $|v|\geqslant m$,$\sigma_f\notin u$ 和 $\sigma_f\notin v$,当 $n\geqslant 0$,可得 $t\in s\Sigma^n\cap L\neq\emptyset$,令 $t=st'$,$w=uv$,则 $P(w)=P(st')$,$|t'|\geqslant n$ 和 $\sigma_f\notin w$,从而可知对任意 $n'\in\mathbb{N}$,存在 $t''\in L/s$ 和 $w'\in L$,使得 $|t''|\geqslant n'$,$w'\in P^{-1}P(st'')$ 和 $\sigma_f\notin w'$,根据定义 4 可知 L 关于 Σ_f 和 P 是不可诊断的,与假设矛盾。

用反证法证明必要性。假设 L 关于 Σ_f 和 P 是弱可预测的但不是可诊断的,则对任意 $n\in\mathbb{N}$,存在 $s\in\Psi(\Sigma_f)$,$t\in L/s$ 和 $w\in P^{-1}P(st)\cap L$,使得 $|t|\geqslant n$ 和 $\sigma_f\notin w$,则对任意的 $n'\in\mathbb{Z}$,当 $n'<-|s|$ 时,$s\odot\Sigma^n\cap L=\emptyset$。当 $-|s|\leqslant n'<0$ 时,令 $t'\in pr(s)$并满足 $|t'|-|s|=n'$,$u\in pr(w)$并且满足 $P(u)=P(t')$,$v\in L/u$ 并且满足 $w=uv$,则 $t'\in s\odot\Sigma^{n'}\cap L$,$u\in L$,$\sigma_f\notin u$ 和 $\sigma_f\notin v$,令 $m<|w|-|u|$,则 $|v|\geqslant m$。当 $n'\geqslant 0$ 时,令 $t'\in pr(st)$并且满足 $|t'|-|s|=n'$,$u\in pr(w)$并且满足 $P(u)=P(t')$,$v\in L/u$ 并且满足 $w=uv$,则 $t'\in s\odot\Sigma^{n'}\cap L$,$u\in L$,$\sigma_f\notin u$ 和 $\sigma_f\notin v$,令 $m<|w|-|u|$,则 $|v|\geqslant m$。综上可得,对任意 $n''\in\mathbb{Z}$,$s\odot\Sigma^n\cap L=\emptyset$或者存在 $t''\in s\odot\Sigma^{n''}\cap L$,对任意 $m'\in\mathbb{N}$存在 $u'\in P^{-1}P(t'')\cap L$ 和 $v'\in L/u'$,使得 $|v'|\geqslant m'$,$\sigma_f\notin u'$ 和 $\sigma_f\notin v'$,则 L 关于 Σ_f 和 P 不是弱可预测的,与假设矛盾。

备注 1　根据命题 1 可知弱可预测性和可诊断性是等价的,而根据文献[11]可知可诊断性弱于可预测性,所以弱可预测性弱于可预测性。

4　弱可预测性的测试算法

定义 5　给定确定自动机 $G=(X,\Sigma,\delta,x_0)$,可以构造故障识别器 $G_l=(X_l,\Sigma,\delta_l,x_{0,l})$,其中 $x_{0,l}=(x_0,N)$是初始状态;$X_l\subseteq X\times Y$ 是状态集合,包含所有从初始状态出发可以到达的状态;$Y=\{N,F\}$,标签 N 表示没有发生故障,标签 F 表示发生了故障。状态转移函数 $\delta_l:X_l\times\Sigma\to X_l$ 定义为:对任意 $x_l=(x,y)\in X_l$ 和 $\sigma\in\Sigma$ 有:

$$\delta_l((x,y),\sigma)=\begin{cases}(\delta(x,\sigma),y), & \text{如果 } \delta(x,\sigma)!\wedge\sigma\notin\Sigma_f\\(\delta(x,\sigma),F), & \text{如果 } \delta(x,\sigma)!\wedge\sigma\in\Sigma_f\\\text{未定义}, & \text{否则}\end{cases}$$

定义 6　给定故障识别器 $G_l=(X_l,\Sigma,\delta_l,x_{0,l})$,对任意 $x_l=(x,N)\in X_l$,如果存在 $n\in\mathbb{N}$,使得对任意 $s\in L(G_l,x_l)$ 有 $|s|\geqslant n\Rightarrow\sigma_f\in s$,则称 x_l 为预警状态,否则 x_l 为非预警状态。预警状态集合标记为 Q_W。

定义 7　给定自动机 $G=(X,\Sigma,\delta,x_0)$,G 中的一个环可以用 $C=(x_0,\sigma_1,x_1,\cdots,x_{m-1},\sigma_m,x_m)$表示,其中 $m\in\mathbb{N}$,x_0,$x_1,\cdots,x_m\in X$,$\sigma_1,\sigma_2,\cdots,\sigma_m\in\Sigma$,$x_0=x_m$,并且对任意 $i\in\{1,2,\cdots,m\}$有 $\delta(x_{i-1},\sigma_i)=x_i$。

定义 8　给定故障识别器 $G_l=(X_l,\Sigma,\delta_l,x_{0,l})$中的一个环 $C=(x_0,\sigma_1,x_1,\cdots,x_{m-1},\sigma_m,x_m)$,如果对环中任意一个状态 $x_i=(x,y)\in C$ 有 $y=N$,则称环 C 为 N 环。

定义 9　给定故障识别器 $G_l=(X_l,\Sigma,\delta_l,x_{0,l})$,可以构造规范自动机 $G_N=(X_N,\Sigma,\delta_N,x_{0,N})$,它是故障识别器 G_l 的子自动机,只包含 G_l 中标签为 N 的状态及其相关转移。如果 $x_{0,l}$的标签为 N 则 G_l 的初始状态为 $x_{0,N}=x_{0,l}$,否则不存在,$X_N=\{(x,y)\in X_l:y=N\}$是状态集合,状态转移函数 $\delta_N:X_N\times\Sigma\to X_N$ 定义为:对任意 $x_{1,N},x_{2,N}\in X_N$ 和 $\sigma\in\Sigma$,$\delta_N(x_{1,N},\sigma)=x_{2,N}$当且仅当 $\delta_l(x_{1,N},\sigma)=x_{2,N}$。

定义 10　给定故障识别器 $G_l=(X_l,\Sigma,\delta_l,x_{0,l})$和规范自动机 $G_N=(X_N,\Sigma,\delta_N,x_{0,N})$,可以构造证明器 $G_V=(X_V,\Sigma,\delta_V,x_{0,V})$,它是通过同步 G_l 和 G_N 构造出来的。其中 $x_{0,V}=(x_{0,l},x_{0,N})$是初始状态;$X_V\subseteq X_l\times X_N$ 是状态集合,它包含了所有从初始状态 $x_{0,V}$出发可以到达的状态。状态转移函数 $\delta_V:X_V\times\Sigma\to 2^{X_V}$ 的定义为:对任意 $x_V=(x_l,x_N)\in X_V$ 和 $\sigma\in\Sigma$,如果 $\sigma\in\Sigma_{uo}$,则

$$\delta_V((x_l,x_N),\sigma)=\begin{cases}\{(\delta_l(x_l,\sigma),x_N)\}, & \text{如果 } \delta_l(x_l,\sigma)!\\\text{未定义}, & \text{否则}\end{cases}$$

如果 $\sigma\in\Sigma_o$,则

$$\delta_V((x_l,x_N),\sigma)=$$
$$\begin{cases}\{(\delta_l(x_l,\sigma),x_N'):(\exists w\in L_\sigma(G_N,x_N))\delta_N(x_N,w)=x_N'\},\\\qquad\text{如果 } \delta_l(x_l,\sigma)!\wedge L_\sigma(G_N,x_N)\neq\emptyset\\\text{未定义}, \quad \text{否则}\end{cases}$$

定义 11　给定证明器 $G_V=(X_V,\Sigma,\delta_V,x_{0,V})$中的一个环 $C=(x_0,\sigma_1,x_1,\cdots,x_{m-1},\sigma_m,x_m)$,如果对环中任意一个状态 $x_i=((x_{i,1},y_{i,1}),(x_{i,2},y_{i,2}))\in C$ 有 $y_{i,1}=F$ 并且$(x_{i,2},y_{i,2})$是非预警状态,则称环 C 为 FN 不可预测环。

弱可预测性测试算法的伪代码如算法 1 所示。

算法 1　弱可预测性测试算法

输入:G,Σ_f,P

输出:YES——系统 G 生成的语言 L 关于 Σ_f 和 P 是弱可预测的

NO——系统 G 生成的语言 L 关于 Σ_f 和 P 不是弱可预测的

1. 根据定义 5 构造故障识别器 G_l。
2. 根据定义 9 构造规范自动机 G_N。
3. 根据定义 10 构造证明器 G_V。
4. 如果 G_V 存在 FN 不可预测环,返回 NO,否则返回 YES。

5　弱可预测性的充分必要条件

为了证明算法 1 的正确性,我们基于证明器 G_V 给出弱

可预测性的充分必要条件。

引理 1 给定故障识别器 $G_l=(X_l,\Sigma,\delta_l,x_{0,l})$，对任意 $x_l=(x,N)\in X_l$，x_l 是一个预警状态当且仅当 x_l 无法到达任何 N 环。

证明：用反证法证明充分性。假设 x_l 无法到达任何 N 环但 x_l 不是一个预警状态，则对任意 $n\in\mathbb{N}$，存在 $s\in L(G_l,x_l)$，使得 $|s|\geqslant n$ 和 $\sigma_f\notin s$。因为 G_l 中状态是有限的，当 n 足够大时，s 中必然包含一个环，因为 $\sigma_f\notin s$，所以这个环是一个 N 环，则 x_l 可以到达 N 环，与假设矛盾。

用反证法证明必要性。假设 x_l 是一个预警状态但是 x_l 可以到达一个 N 环，假设 x_l 经过事件串 s 可以到达这个 N 环的一个状态 x_l'，令这个 N 环对应的以 x_l' 为起点的循环子串为 t，则对任意 $n\in\mathbb{N}$，存在 $m\in\mathbb{N}$，使得 $|st^m|\geqslant n$ 并且 $\sigma_f\notin st^m$，则 x_l 不是预警状态，与假设矛盾。

引理 2 给定证明器 $G_V=(X_V,\Sigma,\delta_V,x_{0,V})$ 中的一个环 $C=(x_0,\sigma_1,x_1,\cdots,x_{m-1},\sigma_m,x_m)$，如果环中有一个状态 $x_i=((x_{i,1},y_{i,1}),(x_{i,2},y_{i,2}))\in C$ 满足 $y_{i,1}=F$ 和 $y_{i,2}=N$，则环 C 是 FN 不可预测环。

证明：用反证法证明。假设环 C 中有一个状态 $x_i=((x_{i,1},y_{i,1}),(x_{i,2},y_{i,2}))\in C$ 满足 $y_{i,1}=F$ 和 $y_{i,2}=N$ 但它不是 FN 不可预测环，则环 C 中存在一个状态 $x_i'=((x_{i,1}',y_{i,1}'),(x_{i,2}',y_{i,2}'))\in C$，使得 $y_{i,1}'\neq F$ 或者 $(x_{i,2}',y_{i,2}')$ 不是非预警状态。如果 $y_{i,1}'\neq F$，则 $y_{i,1}'=N$，因为 $y_{i,1}$ 可以到达 $y_{i,1}'$ 所以 $y_{i,1}=N$，与假设矛盾。如果 $(x_{i,2}',y_{i,2}')$ 不是非预警状态，那么 $(x_{i,2}',y_{i,2}')$ 是预警状态或者故障状态；如果 $(x_{i,2}',y_{i,2}')$ 是预警状态，根据引理 1，它无法到达任何 N 环，那么存在 $n\in\mathbb{N}$，对任意 $s\in L(G_l,(x_{i,2}',y_{i,2}'))$ 有 $|s|\geqslant n\Rightarrow\sigma_f\in s$，假设环 C 对应的以 $(x_{i,2}',y_{i,2}')$ 为起点的循环子串为 t，令 $s=t^m$，$m\in\mathbb{N}$，则当 $|s|\geqslant n$ 时有 $\sigma_f\in s$，则 $y_{i,2}'=F$，因为 $y_{i,2}'$ 可以到达 $y_{i,2}$，所以 $y_{i,2}=F$，与假设矛盾。如果 $(x_{i,2}',y_{i,2}')$ 是故障状态，则 $y_{i,2}'=F$，因为 $y_{i,2}'$ 可以到达 $y_{i,2}$，所以 $y_{i,2}=F$，与假设矛盾。

定理 1 令 $G=(X,\Sigma,\delta,x_0)$ 为一离散事件系统，L 为 G 生成的语言，$G_V=(X_V,\Sigma,\delta_V,x_{0,V})$ 为证明器，则 L 关于 Σ_f 和 P 是弱可预测的当且仅当 G_V 中不存在 FN 不可预测环。

证明：用反证法证明充分性。假设 G_V 中不存在 FN 不可预测环但 L 关于 Σ_f 和 P 不是弱可预测的，则存在 $s\in\Psi(\Sigma_f)$，对任意 $n\in\mathbb{Z}$，$s\odot\Sigma^n\cap L=\emptyset$ 或者存在 $t\in s\odot\Sigma^n\cap L$，对任意 $m\in\mathbb{N}$ 存在 $u\in P^{-1}P(t)\cap L$ 和 $v\in L/u$，使得 $|v|\geqslant m$，$\sigma_f\notin u$ 和 $\sigma_f\notin v$，因为 G_V 中状态有限，当 n 足够大时，t 和 u 在 G_V 中的同步必然出现环，又因为 t 中有故障而 u 中无故障，可知该环存在一个状态 $x_i=((x_{i,1},y_{i,1}),(x_{i,2},y_{i,2}))$ 满足 $y_{i,1}=F$ 和 $y_{i,2}=N$，根据引理 2 可知这个环是 FN 不可预测环，与假设矛盾。

用反证法证明必要性。假设 L 关于 Σ_f 和 P 是弱可预测的但是 G_V 中存在 FN 不可预测环，则存在 $s\in\Psi(\Sigma_f)$ 和 s'，$s''\in L$，使得 $s\in pr(s')$ 并且 s' 和 s'' 同步在 G_V 中到达这个 FN 不可预测环，令 $l\in L/s'$ 和 $l'\in L/s''$ 为这个 FN 不可预测环中同步的循环子串，则对任意 $n\in\mathbb{Z}$，如果 $n<-|s|$，则 $s\odot\Sigma^n\cap L=\emptyset$。如果 $-|s|\leqslant n<0$，令 $t\in pr(s)$ 并且满足 $|t|-|s|=n$，$u\in pr(s'')$ 并且满足 $P(u)=P(t)$，则 $\sigma_f\notin u$，又令 $v\in L/u$ 并且满足 $uv=s''l'^{m'}$，则对任意 $m\in\mathbb{N}$，存在 $m'\in\mathbb{N}$，使得 $|v|\geqslant m$ 并且 $\sigma_f\notin v$。如果 $n\geqslant 0$，令 $t\in pr(s'l'^{m'})$ 并且满足 $|t|-|s|=n$，$u\in pr(s'')$ 并且满足 $P(u)=P(t)$，则 $\sigma_f\notin u$，又令 $v\in L/u$ 并且满足 $uv=s''l'^{m'}$，则对任意 $m\in\mathbb{N}$，存在 $m'\in\mathbb{N}$，使得 $|v|\geqslant m$ 并且 $\sigma_f\notin v$。综上可得，对任意 $n\in\mathbb{Z}$，存在 $t\in s\odot\Sigma^n\cap L$，使得 $s\odot\Sigma^n\cap L=\emptyset$，或者存在 $u\in P^{-1}P(t)\cap L$ 和 $v\in L/u$，使得 $|v|\geqslant m$，$\sigma_f\notin u$ 和 $\sigma_f\notin v$。根据定义 3 可得 L 关于 Σ_f 和 P 不是弱可预测的，与假设矛盾。

备注 2 对一个离散事件系统 G，设 G 的状态数和事件数分别为 $|X|$ 和 $|\Sigma|$，表 1 列出了算法 1 中涉及的各个自动机的状态数和转移数。算法 1 的总体复杂度为 $O(|X|^3|\Sigma|)$，是 G 的状态数和事件数的多项式。

表 1 弱可预测性复杂度

Table 1 Complexity of weak prognosability

自动机	状态数	转移数
G	$\|X\|$	$\|X\|\|\Sigma\|$
G_l	$2\|X\|$	$2\|X\|\|\Sigma\|$
G_N	$2\|X\|$	$2\|X\|\|\Sigma\|$
G_V	$4\|X\|^2$	$8\|X\|^3\|\Sigma\|$
复杂度		$O(\|X\|^3\|\Sigma\|)$

6 在线故障弱预测

在线故障弱预测可以通过构造文献[2]中的诊断器 G_d 来实现。诊断器可以用函数 $D:\Sigma_o^*\rightarrow\{0,1\}$ 表示，当诊断器观察到一个可观事件串 s_o，对故障诊断来说，如果诊断器中 s_o 到达的状态（即估计状态）中包含的所有系统状态都是故障状态则返回 1。否则返回 0；而对故障弱预测来说，如果诊断器中 s_o 到达的状态中包含的系统状态为故障状态或预警状态则返回 1。否则返回 0。相比故障诊断，故障弱预测不用等估计状态中的系统状态都变成故障状态才返回 1。由此可知，从发出警报的及时性来说，故障弱预测的及时性优于故障诊断的及时性。

7 例子

例 2 我们考虑一个无人机参与搜索任务以寻找特定目标的例子[4]，它的整个搜寻过程建模成如图 2 所示的系统 G，其中 $\Sigma=\{\alpha,\beta,\gamma,\tau,f_1,f_2\}$，$\Sigma_o=\{\alpha,\beta,\gamma,\tau\}$，$\Sigma_{uo}=\{f_1,f_2\}$，$\Sigma_f=\{f_1,f_2\}$。在这个模型中，事件 β 表示“无人机寻找目标”，事件 α 表示“无人机返回机库”，事件 γ 表示“刮大风”，事件 τ 表示“无人机矫正航线继续寻找目标”，故障事件 f_1 表示“无人机偏离航线”，故障事件 f_2 表示“无人机燃油泄漏或者油位低”。如果无人机因为刮大风而偏离航线，它会矫正航线然后继续搜索，如果出现燃油泄漏或燃油油位低，无人机会迅速返回机库。

根据算法 1 构造故障识别器 G_l，规范自动机 G_N 以及证明器 G_V，分别如图 3－图 5 所示。因为 G_V 中不存在 FN 不可预测环，根据定理 1 可得系统 G 所生成的语言 L 关于 Σ_f 和 P 是弱可预测的。在这个例子中，以故障结尾的语言 $\Psi(\Sigma_f)=\{\beta\{\alpha\beta+\gamma f_1\tau\alpha\beta\}^*\gamma f_1,\beta\{\alpha\beta+\gamma f_1\tau\alpha\beta\}^* f_2,\beta\{\alpha\beta+\gamma f_1\tau\alpha\beta\}^*\gamma f_1\tau f_2\}$，预警状态集合 $Q_W=\{3N\}$。根据文献[2]的方法构造诊断器 G_d，如图 6 所示，对系统进行在线故障弱预测，对故障事件串 $\beta\{\alpha\beta+\gamma f_1\tau\alpha\beta\}^*\gamma f_1$ 来说，它是可预测的，当系统运行它的前缀 $\beta\{\alpha\beta\}^*\gamma$ 时，诊断器观察到可观事件串 $\beta\{\alpha\beta\}^*\gamma$，到达状态 $\{3N\}$，因为 $3N$ 是预警状态，所以返回 1，如果使用在线诊断的方法，诊断器必须再观察到事件 τ，到达

状态{5F}，才会返回1。对故障事件串$\beta\{\alpha\beta+\gamma f_1\tau\alpha\beta\}^* f_2$来说，可以分两种情况，第一种情况它是$\beta\{\alpha\beta\}^* f_2$，是不可预测只能诊断的，当系统运行$\beta\{\alpha\beta\}^* f_2\alpha\alpha$，诊断器观察到可观事件串$\beta\{\alpha\beta\}^*\alpha\alpha$，到达状态{6F}，才会返回1，第二种情况它是$\beta\{\alpha\beta+\gamma f_1\tau\alpha\beta\}^*\gamma f_1\tau\alpha\beta f_2$，是可预测的，当系统运行它的前缀$\beta\{\alpha\beta\}^*\gamma$，诊断器观察到可观事件串$\beta\{\alpha\beta\}^*\gamma$，到达状态{3N}，因为3N是预警状态，所以返回1。对故障事件串$\beta\{\alpha\beta+\gamma f_1\tau\alpha\beta\}^*\gamma f_1\tau f_2$来说，它也是可预测的，当系统运行$\beta\{\alpha\beta\}^*\gamma$，诊断器观察到可观事件串$\beta\{\alpha\beta\}^*\gamma$，到达状态{3N}，因为3N是预警状态，所以返回1。

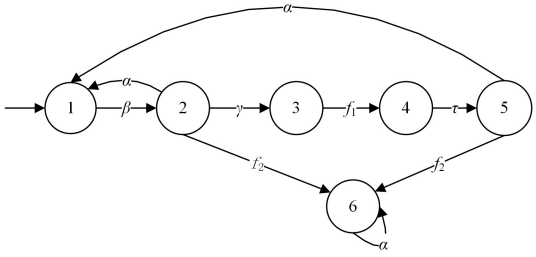

图2　例2中的G

Fig. 2　G in example 2

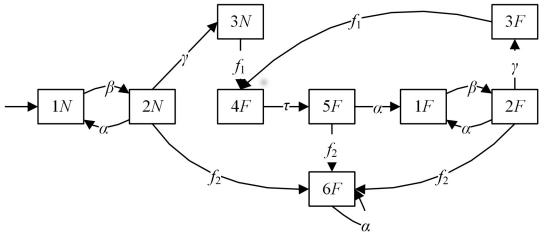

图3　例2中的G_l

Fig. 3　G_l in example 2

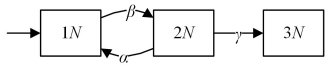

图4　例2中的G_N

Fig. 4　G_N in example 2

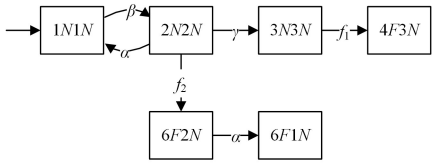

图5　例2中的G_V

Fig. 5　G_V in example 2

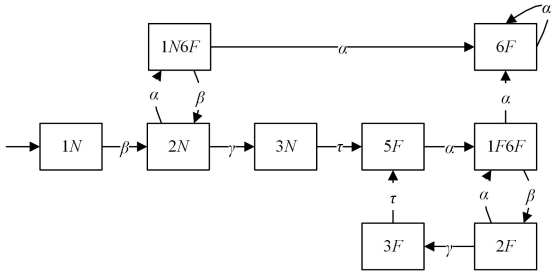

图6　例2中的G_d

Fig. 6　G_d in example 2

结束语　很多离散事件系统只有部分故障事件串是可预测的，这种情况下整个系统是不可预测的，无法用文献[11]中提出的预测的方法处理。为了让这些可预测的故障事件串在故障发生之前被检测出来，本文提出了离散事件系统的故障弱可预测性的概念，构造了证明器来测试系统的弱可预测性，并且基于证明器提出了测试系统弱可预测性的多项式算法，算法的复杂度是$O(|X|^3|\Sigma|)$，其中$|X|$和$|\Sigma|$分别是系统的状态数和事件数。特别地，给出了系统弱可预测的充分必要条件。此外，证明了弱可预测性和可诊断性等价，所以凡是可诊断的系统都可以用弱可预测性的方法来处理，而且发出警报比诊断更及时。因为弱可预测性允许故障发生后才发出警报，与可预测性必须在故障发生之前发出警报不同，所以发出警报后故障可能已经发生了也可能还没发生，这可能对收到警报后的处理工作造成影响，也许可以进一步改进。后续还可以研究分布式模式下的弱可预测性、随机模型下的弱可预测性和模糊模型下的弱可预测性等。

参 考 文 献

[1] CASSANDRAS C G, LAFORTUNE S. Introduction to discrete event systems[M]. New York: Springer, 2010.

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

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

[4] WHITE A, KARIMODDINI A, SU R. Fault diagnosis of discrete event systems under unknown Initial conditions[J]. IEEE Transactions on Automatic Control, 2019, 64(12): 5246-5252.

[5] CABRAL F G, MOREIRA M V. Synchronous Diagnosis of Discrete-Event Systems[J]. IEEE Transactions on Automation Science and Engineering, 2020, 17(2): 921-932.

[6] REN K, ZHANG Z, XIA C. Event-based fault diagnosis of networked discrete event systems[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2022, 69(3): 1787-1791.

[7] CAO L, SHU S, LIN F, et al. Weak Diagnosability of Discrete-Event Systems[J]. IEEE Transactions on Control of Network Systems, 2022, 9(1): 184-196.

[8] LU W, ZHANG L M, ZHU Y A. Partial Diagnosability Analysis of Discrete-event Systems[J]. Computer Science, 2015, 42(2): 177-181.

[9] FANG H, FANG X W, LI D Q. Review on Fault Diagnosis Theory and Application Based on Petri Nets[J]. Computer Science, 2014, 41(3): 17-22.

[10] WANG X Y, OUYANG D T, ZHAO X F, et al. Algorithm of Dynamic Event System's Synchronization Diagnosis[J]. Computer Science, 2010, 37(2): 180-182.

[11] GENC S, LAFORTUNE S. Predictability of event occurrences in partially-observed discrete-event systems[J]. Automatica, 2009, 45(2): 301-311.

[12] XIAO C, LIU F. Robust Fault Prognosis of Discrete-Event Systems Against Loss of Observations[J]. IEEE Transactions on Automation Science and Engineering, 2022, 19(2): 1083-1094.

[13] LIU F. Predictability of failure event occurrences in decentralized discrete-event systems and polynomial-time verification

[J]. IEEE Transactions on Automation Science and Engineering, 2019, 16(1): 498-504.

[14] YIN X, LI Z. Decentralized Fault Prognosis of Discrete-Event Systems Using State-Estimate-Based Protocols[J]. IEEE Transactions on Cybernetics, 2019, 49(4): 1302-1313.

[15] TAKAI S, KUMAR R. Inference-Based Decentralized Prognosis in Discrete Event Systems[J]. IEEE Transactions on Automatic Control, 2011, 56(1): 165-171.

[16] TAKAI S, KUMAR R. Distributed Failure Prognosis of Discrete Event Systems With Bounded-Delay Communications[J]. IEEE Transactions on Automatic Control, 2012, 57(5): 1259-1265.

[17] CHEN J, KUMAR R. Stochastic failure prognosability of discrete event systems[J]. IEEE Transactions on Automatic Control, 2015, 60(6): 1570-1581.

[18] LIAO H, LIU F C. Verification algorithm of fault prediction of random discrete event system under permanent loss of observation[J]. Application Research of Computers, 2022, 39(1): 106-112.

[19] SHU S, LIN F, HAO Y. Detectability of Discrete Event Systems [J]. IEEE Transactions on Automatic Control, 2007, 52(12): 2356-2359.

[20] WONHAM W M, RAMADGE P J. Modular supervisory control of discrete-event systems[J]. Mathematics of Control Signals and Systems, 1988, 1(1): 13-30.

[21] LIN F. Opacity of discrete event systems and its applications [J]. Automatica, 2011, 47(3): 496-503.

[22] YOKOMIZOWATANABE A T, BITTENCOURTLEAL A, CURY J E R, et al. Combining online diagnosis and prognosis for safe controllability[J]. IEEE Transactions on Automatic Control, 2022, 67(10): 5563-5569.

CAO Weihua, born in 1983, postgraduate. His main research interests include control theory and control engineering, algorithm analysis and design.