

基于时序的离散事件系统的可诊断性

李占山 陈 超 叶寒锋

(吉林大学符号计算与知识工程教育部重点实验室 长春 130012)

(吉林大学计算机科学与技术学院 长春 130012)

摘 要 提出一种基于事件之间的时序关系判定可诊断性的方法。首先通过添加通讯事件把全局模型分解成几个局部模型来缩减模型的规模,删除局部模型中的无用路径以降低状态空间;其次利用通讯事件和可观测事件之间的时序关系,对受限局部模型的可诊断性进行判定,得出几个判定性质,然后把这些性质运用到局部模型的可诊断性判定中,以避免同步操作的高复杂性;最后通过实例对可诊断性判定的过程进行分析。

关键词 模型分解,受限局部模型,可诊断性

中图法分类号 TP31 **文献标识码** A

Diagnosability of Discrete-event Systems Based on Temporal

LI Zhan-shan CHEN Chao YE Han-feng

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

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

Abstract This paper proposed a new diagnosis approach based on the temporal relationship between events. In order to reduce the scale of the model, we first added some communication events to divide the global model. Then we deleted some useless road in the local models to reduce the space of states. According to the temporal relationship between communication events and observable events, we could get the diagnosability of the limited model and some properties. We used the properties to get the diagnosability of the local models, which avoids the high complexity of the synchronization operation. Finally we gave some examples to analysis the steps of the diagnosed process.

Keywords Model decomposition, Limited local model, Diagnosability

离散事件系统可诊断性的任务是对一个已知的系统,在可观测事件及建模抽象一定的情况下,根据可观测事件序列,把一个故障与其他故障或者是正常行为区分开。如果可以区分,则这个系统就是可诊断的。

20 世纪 90 年代,文献[1-3]是最早提出用离散事件系统对动态系统进行故障诊断的几篇典型论文,其给出了通过创建诊断器来判定系统是否可诊断的方法,即判定诊断器中是否存在含有二义性状态的循环。这种基本方法的缺点在于需要构建系统的全局诊断器,而诊断器的计算与系统(确定的)全局模型的状态数目呈指数级增长,因而导致与系统的组件数目也呈双指数级增长。为解决该问题, Jiang 等人在文献[4], Yoo 与 Lafortune 在文献[5]分别独立提出了一种新算法——双模型(twin plant)方法,其可以在关于系统模型状态的多项式时间内完成。但是,该方法对于大规模系统来说,依然是难以适用的,这是因为系统的双模型依然与系统的状态数目呈四次方增长。上述方法都是对整个系统进行建模来得出可诊断性,它只能处理系统规模较小的情况,而且它的缺点是空间复杂性太大。当系统规模很大的时候,对全局模型直

接求其可诊断性相当困难,因此很多学者将离散事件系统按照一定的规则划分成多个子系统(或者称为组件),此时每一个组件对应的模型称为局部模型,然后分别对每个局部模型进行诊断。典型的方法有分散式诊断^[6]和分步式诊断^[7]。文献[6]中各个子系统之间不存在通信事件,分别对每一个子系统建模,并进行诊断推理得到各个局部模型的可诊断性。此外,通过添加一个协调器(coordinator)来协调各局部模型的诊断结果,到达优化并产生最终的全局诊断结果,然而这些局部诊断器依然是基于系统的全局模型。文献[7]中方法与分散式诊断不同,各个局部模型之间必须要用通信事件进行连接,不需要额外引进一个协调器,而是由各子系统之间通信的一致性来逐步优化各子诊断;对各个局部模型构建诊断器和检测器进行可诊断性的判定,若各个局部模型都是不可诊断的,则对每一个检测器进行剪枝操作,然后把剪枝后的各个局部模型的检测器进行同步,得出全局模型的诊断结果。但是,构造检测器是一个相当复杂的过程,同步后所得到的系统规模也相当庞大。我们提出的新思想是,把一个全局模型按照一定的规则划分成若干局部模型,局部模型可诊断性的判定

到稿日期:2012-01-10 返修日期:2012-03-20 本文家国家自然科学基金项目(60873148, 60973089, 61170314),吉林省自然科学基金项目(20071106, 20101501, 20100185),国家教育部博士点专项基金(20100061110031)和吉林大学跨学科项目(2009JC038)资助。

李占山 教授,主要研究方向为基于模型的诊断、智能规划与调度、产品配置和约束求解, E-mail: zslizsli@163. com; 陈 超 硕士,主要研究方向为基于模型的诊断、约束求解。

根据文献[8]得到,如果每一个局部模型都是不可诊断的,则对各局部模型进行剪枝操作,只保留那些对判定可诊断性有用的信息;然后对剪枝后的局部模型进行受限处理,得到受限局部模型;最后对受限模型进行可诊断性的判定。该方法其实是在同步中对判断可诊断性有用的关键信息单独提炼出来,避免对两个局部模型进行同步操作,以便得到与同步后一致的可诊断性,其能够节省时间,提高诊断效率。

本文第2节介绍把全局模型划分成局部模型的方法,然后进行必要的操作来缩减模型的规模;第3节提出一种新的模型,其称为受限局部模型,并给出对其进行可诊断性判定的方法,即先考虑在一条路径上仅出现一个通信事件的情况,然后处理一条路径上出现多个通信事件的情况;第4节利用受限局部模型可诊断性判定方法的特点,来判定局部模型的可诊断性。

1 背景知识

使用一些先进的编译技术,通过离线方式编译系统状态、观测与诊断的信息,从而提高在线诊断的效率,本文用有限状态自动机(FSMs)来描述系统的行为。

定义 1^[7] 一个局部模型 G_i 是一个自动机 $G_i = (Q_i, E_i, T_i, q_{0i})$, 其中:

Q_i 是有限状态的集合;

E_i 是 Γ_i 中发生的事件的集合;

T_i 表示转换的集合, $T_i \subseteq Q_i \times E_i \times Q_i$;

q_{0i} 表示初始状态。

集合 E_i 可以划分为 4 个互不相交的集合:

1) N_i : 正常事件集合。该事件发生后,部件可以改变其内部的状态。

2) F_i : 故障事件集合。该事件发生后,部件就处于故障状态。

3) O_i : 可观测事件集合。该事件发生后会被系统监测到。

4) C_i : 通信事件集合。该事件在一部件上发生后至少在另一个部件也发生。

路径: 从初始状态 q_0 ($q_0 \in I$) 开始,经过一系列连续的转换到达状态 q_1 ,我们称之为路径,表示为 $t_i = \langle q_0, e_i, q_1 \rangle$ 。

关键路径: 路径 p_1 中含有故障事件,路径 p_2 中无故障事件,且有 $Obs(p_1) = Obs(p_2)$,则称 (p_1, p_2) 是一对关键路径。

可区分路径: Γ 中有两条路径 p_1, p_2 ,若 $Obs(p_1) \neq Obs(p_2)$,则称路径 p_1 和 p_2 是可区分路径。

若模型中的所有路径都是互相可区分的,则这个模型是可区分的,否则是不可区分的。

定义 2^[7] 子系统的全局模型 G 是自动机 $G = (Q, E, T, q_0)$, 其中:

$Q \subseteq Q_{i_1} \times \dots \times Q_{i_k}$ 表示状态的集合;

$E = \bigcup_{j=1}^k E_j$ 表示事件的集合;

$q_0 = (q_{0i_1}, \dots, q_{0i_k})$ 表示初始状态;

$T \subseteq T_{i_1} \times \dots \times T_{i_k}$ 表示转换的集合。

定义 3^[7] 故障 f 是可诊断的,当且仅当故障 f 发生后存在有限数目的可观测事件 l ,使得 f 有效发生。

令 p_f 为 G 中一条从开始状态 q_0 到 f 发生后的故障状态 q_f 的路径,且 s_f 为 G 中以 q_f 状态开始的路径。 $Obs(p)$ 为任

意从 q_0 开始的路径 p 的可观测序列,令 $Obs^{-1}(p)$ 为 G 中从 q_0 开始的路径 p' 的集合,其中 $Obs(p') = Obs(p)$ 。

故障 f 是可诊断的,当且仅当:

$$\forall p_f, s_f, \exists l \in N: |Obs(s_f)| \geq l$$

$$\Rightarrow (\forall p \in Obs^{-1}(p_f s_f), f \text{ 在 } p \text{ 中发生})$$

定义 4^[7] 系统是可诊断的,当且仅当每个故障事件都是可诊断的。

定义 5^[7] 子系统中发生的故障 f 是局部可诊断的,当且仅当故障 f 发生后子系统中存在有限数目的观测 l ,使得 f 有效发生。

可诊断性的定义 5 和上面的定义 3 类似,区别在于只考虑子系统内的可观测事件。假设 γ 是子系统, $Obs_\gamma(p)$ 是 γ 的可观测事件在 $Obs(p)$ 上的映射所得的可观测序列, $Obs_\gamma^{-1}(p)$ 是 Γ 中一系列的路径 p' 且有 $Obs_\gamma(p') = Obs_\gamma(p)$,则 f 是局部可诊断的,当且仅当:

$$\forall p_f, s_f, \exists l \in N: |Obs_\gamma(s_f)| \geq l$$

$$\Rightarrow (\forall p \in Obs_\gamma^{-1}(p_f s_f), f \text{ 在 } p \text{ 中发生})$$

定义 6^[7] 子系统是局部可诊断的,当且仅当子系统中发生的每个故障事件都是局部可诊断的。

定义 7^[7] 语言 $L \subseteq E^*$,是 E 上有序事件的集合。

假设有一条路径 $q_0 \xrightarrow{obs_1} \dots \xrightarrow{obs_{n-1}} q_{n-1} \xrightarrow{obs_n} q_n$,其观测序列可简写成 $obs_1 obs_2 obs_3 \dots obs_n$,若 $L_1 = obs_2 obs_3 \dots obs_i$,则这条路径可表示为 $q_0 \xrightarrow{obs_1} q_1 \xrightarrow{L_1} q_i \xrightarrow{obs_{i+1}} \dots \xrightarrow{obs_n} q_n$,简写成 $obs_1 L_1 obs_{i+1} \dots obs_n$ 。

2 全局模型划分成局部模型

系统规模很大时,对全局模型直接求其可诊断性相当困难。因此很多学者将离散事件系统按照一定的规则划分成一个个的子系统(或者称为组件),此时每一个组件对应的模型称为局部模型。分布式诊断添加通信事件将全局系统分解为一些小的子系统,然后各子系统同样根据相应的子观测进行诊断推理,产生各自的子诊断。本文中添加通信事件的方法与文献[9]中的类似,文献[9]中是由行为出发的,而且模型中没出现故障状态,对其进行必要的后续改进,以缩减模型的规模。

域是一组具有相同数据类型的值的集合。

$S'_i(k)$ 表示由 G_i 向 G_j 发送信息 k ; $r'_i(k)$ 表示 G_i 从 G_j 接受信息 k 。

$Out(q_i)$ 是 q_i 的输出域。

当系统中存在故障事件时,假设一个全局模型中的事件分为两个域,即 $domain_1$ 和 $domain_2$ 。对于每一个转换 $[q_1, e_1, q_2]$,做如下操作。

(1) 由 $domain_1$ 事件生成的局部模型

1) 当 $e_1 \in domain_1$, $\exists e_2 \in Out(q_2)$ 时,若 $e_2 \in domain_1$,则不做任何操作;若 $e_2 \in domain_2$,则在 q_1 与 q_2 之间做如下操作: $[q_1, e_1, q_1 - q_2]$, $[q_1 - q_2, s_2^1(q_2), q_2]$ 。

2) 当 $e_1 \in domain_2$, $\exists e_2 \in Out(q_2)$ 时,若 $e_2 \in domain_1$,则做如下操作: $[q_1, r_1^1(q_2), q_2]$;若 $e_2 \in domain_2$,则 e_2 变成空事件,即合并 q_1, q_2 状态为 q_1 状态。

3) 当 e_1 是故障事件 f 时,做如下操作: $[q_1, f, q_1 - q_2]$, $[q_1 - q_2, s_2^1(q_2), q_2]$ 。

(2) 由 $domain_2$ 事件生成的局部模型和 $domain_1$ 生成的过程类似:

1) 当 $e_1 \in domain_2$, $\exists e_2 \in Out(q_2)$ 时, 若 $e_2 \in domain_2$, 则不做任何操作; 若 $e_2 \in domain_1$, 则在 q_1 与 q_2 之间做如下操作: $[q_1, e_1, q_1 - q_2], [q_1 - q_2, s_2^1(q_2), q_2]$ 。

2) 当 $e_1 \in domain_1$, $\exists e_2 \in Out(q_2)$ 时, 若 $e_2 \in domain_2$, 则做如下操作: $[q_1, r_2^1(q_2), q_2]$; 若 $e_2 \in domain_1$, 则 e_2 变成空事件, 即合并 q_1, q_2 状态为 q_1 状态。

3) 当 e_1 是故障事件 f 时, 做如下操作: $[q_1, r_2^1(q_2), q_2]$ 。

下面是一个具体的实例。

图 1(a) 是一个全局模型, f 是故障事件, o_1, o_2, o_3, o_4 是可观测量事件。

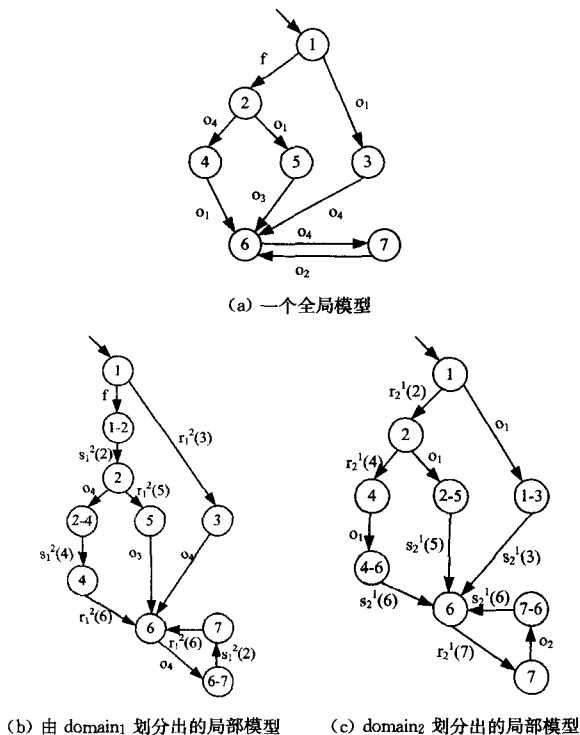


图 1

全局模型按以下两个域进行分解, $domain_1 = \{o_3, o_4\}$, $domain_2 = \{o_1, o_2\}$ 。

由 $domain_1$ 生成的模型 G_1 中, 状态 1 到状态 2 所经历的事件是 f 。根据(1)中的 3), 在 $domain_1$ 生成的局部模型中添加状态 1-2, 并由 G_1 向 G_2 发送一个消息, 状态 2 到状态 5 经历 $domain_2$ 的事件, 而状态 5 的输出事件是 $domain_1$ 的事件, 所以在状态 2 和状态 5 中添加从 G_2 接收到的一个消息。

在常见的模型中, 通信事件一般是由 c_i 来表示的。把上面得到的模型转化为一般形式, 即把 $r_2^1(2), s_1^1(2)$ 这对通信事件换成 $c_1; s_2^1(3), r_1^1(3)$ 换成 $c_2; r_2^1(4), s_1^1(4)$ 换成 $c_3; s_2^1(5), r_1^1(5)$ 换成 $c_4; s_2^1(6), r_1^1(6)$ 换成 $c_5; r_2^1(7), s_1^1(7)$ 换成 c_6 。由此得到图 2。

图 2 中的全局模型中, 由状态 6 开始的路径是所有的路径公共的部分。因为是公共的路径, 所以每次在判定可诊断性的时候, 都可以出现相同的观测序列, 因而对于可诊断性的判断无影响, 其实完全可以化简掉, 可以把它化简成另一种形式, 用 tra_i 去替代模型中出现的公共部分的观测序列。图 1(a) 全局模型中的 $o_2 o_4$ 循环可以用 tra_1 替代。

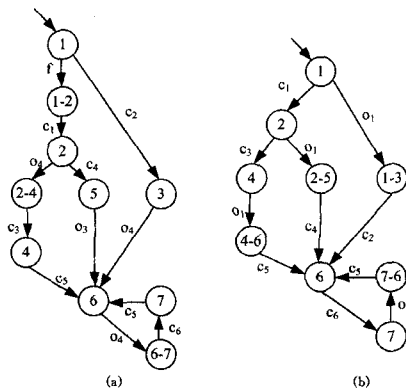


图 2 由图 1 转化得到的常见模型

全局模型的规模很大, 不合适直接找关键路径。当划分成局部模型后, 系统规模明显变小, 此时可以寻找关键路径。从域 $\{o_3, o_4\}$ 形成的子模型中可以看出, 关键路径是 $\{f c_1 o_4 c_3 c_5, c_2 o_4\}$, 由该域得到的模型可化简成图 3(a), 再根据域 $\{o_1, o_2\}$ 中被删掉的路径 $\{f c_1 c_4 o_3\}$ 知道, c_4 不在模型中出现, 则由域 $\{o_1, o_2\}$ 形成的模型中把 c_4 出现的那条路径删除, 然后只保留关键路径, 得到图 3(b)。

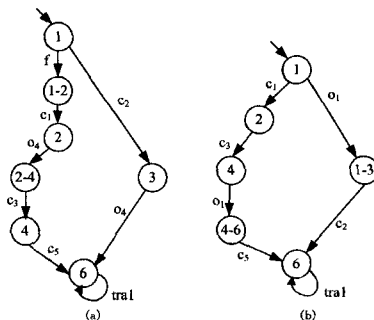


图 3 合并事件并保留关键路径

剩下的是只含有关键路径的局部模型。在第 4 节中, 对局部模型的可诊断性进行判定。

3 受限局部模型可诊断性的判定

在进行局部模型可诊断性的判定之前, 先定义一种特殊的局部模型, 其称为受限局部模型。该模型的特点是观测事件仅出现在通信事件的一侧, 然后根据观测事件和通信事件的时序进行可诊断性的判断。为了便于理解, 暂时先考虑在一条路径上仅出现一个通信事件的情况, 然后再处理一条路径上出现多个通信事件的情况。

定义 8(受限局部模型) 一个局部模型 G_i , 其观测事件只出现在通信事件的一侧, 即观测事件要么都在通信事件之前发生(左侧), 要么都在通信事件之后发生(右侧), 这样的局部模型称为受限局部模型。

若一个局部模型中通信事件一侧是观测事件, 另一侧是 tra_i , 则该模型称为受限局部模型。

文献[7]中用到的两个局部模型在状态 y_4 之后的路径都出现在公共路径中, 之后出现的观测序列用 tra_1 表示, 对可诊断性的判定无影响。 tra_1 对受限局部模型的判定无影响, 认为图 5(a) 仍是一个受限局部模型。

图 4 是在文献[7]中出现的两个受限局部模型。

图 4 中, f 是故障事件; o_3, o_4, o_5 是可观测量事件; c_1, c_2 是通信事件; 图 4(a) 中的故障 f 是局部不可诊断的, 这种情况

下只有和图 4(b)进行同步才能得出故障 f 的可诊断性。

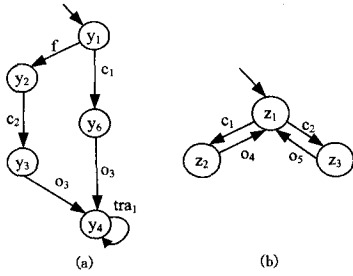


图 4 图(a)和图(b)分别是两个子系统的自动机

同步图 4 的两个子系统可知 f 是可诊断的,但是同步产生的模型规模明显变大。根据模型的结构信息和事件之间的时序信息可知,可以不经过同步即可判断其可诊断性。在图 4(b)中含有 c_1 事件的路径中必然会发生事件 o_4 ,而含有 c_2 事件的路径中必然会发生 o_5 。图 1、图 2 同步后的路径中必然会出现含 c_1 的路径中有事件 o_4 而无事件 o_5 ,含 c_2 的路径中有事件 o_5 而无事件 o_4 ,由此可得出下面的性质。

性质 1 Γ_1 和 Γ_2 是两个可以互相通信的受限局部模型, Γ_1 中有故障出现且是局部不可诊断的,若对应的 Γ_2 中含有相同通信事件的路径是可区分的,则该故障在全局模型中是可诊断的。

Γ_1 是局部不可诊断的,所以至少存在一条和故障 f 所在的路径有相同观测序列的路径。若含有故障的路径为 $L_1 c_1$,则另一条路径是 $L_1 c_2$ 或 $c_2 L_1$ 。通信事件 c_1, c_2 对应 Γ_2 中的路径是可区分的,为 $L_2 c_1$ 或 $c_1 L_2, L_3 c_2$ 或 $c_2 L_3$ 。可区分的情况分为 2 种,一种是存在着不同的观测事件域,如图 4 右图那样。假设 o_4 仅在 L_2 中出现,而 o_5 仅在 L_3 中出现;另一种是出现的事件域是一样的,但由于事件之间的时序关系,存在着可区分的观测序列。假设 L_2 中有观测序列 $o_6 \cdots o_7, L_3$ 中有观测序列 $o_7 \cdots o_6$,同步之后,第一种情况可以看出在有 c_1 的路径上会出现事件 o_4 ,而在 c_2 的路径上会出现 o_5 ,两条路径可以区分开,可知,同步之后是可诊断的。第二种情况同步之后,在有 c_1 的路径上 o_6 永远在 o_7 之前出现,而在有 c_2 的路径上 o_7 永远在 o_6 之前出现,其仍然是可诊断的。由此可见,性质 1 的结论是正确的。

定义 9(弱可区分路径) 令 p_{c_i} 为 Γ 中一条从初始状态 q_0 到 c_i 发生后的状态 q_{j+1} 的路径, s_{c_i} 为以 q_{j+1} 状态开始到达稳定状态的路径: $p_{c_i} = q_0 \xrightarrow{obs_1} \cdots \xrightarrow{obs_j} q_j \xrightarrow{c_i} q_{j+1}, s_{c_i} = q_{j+1} \xrightarrow{obs_{j+1}} \cdots \xrightarrow{obs_n} q_n$ 。若 Γ 中 $\exists p_1, p_2$ 两条路径,且满足 $Obs(p_1) = Obs(p_2)$,假设 c_1, c_2 分别是 p_1, p_2 路径上的通信事件,若 $Obs(p_{c_1}) \neq Obs(p_{c_2})$,则称 p_1, p_2 是弱可区分路径。

若模型中的路径都是弱不可区分的,则称这个模型是弱不可区分的,否则是弱可区分的。从上面的定义可以看出,在说弱可区分和弱不可区分时,这个模型首先是不可区分的。

若图 4(b)中的 o_5 换成 o_4 ,可诊断性判断就不能根据上面的性质得到。

性质 2 Γ_1 和 Γ_2 是两个可以互相通信的受限局部模型, Γ_1 中有故障出现且是局部不可诊断的, Γ_1 和 Γ_2 中若有一个是弱不可区分的,则该故障是不可诊断的。

若 Γ_1 和 Γ_2 都是弱不可区分的,假设 Γ_1 中的路径 $L_1 c_1, L_1 c_2, \Gamma_2$ 中的路径为 $L_2 c_1, L_2 c_2$,同步的时候可以看出, $(L_1 \parallel L_2) c_1$ 和 $(L_1 \parallel L_2) c_2$ 明显是不可诊断的。若仅有一个是弱不

可区分的,假设 Γ_1 中的路径是弱不可区分的,为 $L_1 c_1, L_1 c_2$;而 Γ_2 中的路径是弱可区分的,为 $L_2 c_1, c_2 L_2$ 。当同步的时候可以看出 $(L_1 \parallel L_2) c_1$ 和 $L_1 c_2 L_2$ 明显是不可诊断的($\parallel$ 表示同步)。

当受限局部模型 Γ_1 和 Γ_2 都有弱可区分路径时,诊断结果应该根据不同的情况加以分析。从例 1 可以看出,可诊断性是不明确的。

例 1 图 5(a)和图 5(b)都是弱可区分的,同步的结果是可诊断的。从图中可以看出,图 5(a)模型的两条路径是 $o_3 c_1, c_2 o_3$,图 5(b)模型的两条路径是 $c_1 o_4, o_4 c_2$,两个模型经过同步之后的结果是 $o_3 c_1 o_4, o_4 c_2 o_3$,可知含有 c_1 的路径上 o_3 出现在 o_4 之前,而含有 c_2 的路径上 o_4 出现在 o_3 之前,所以,同步的结果必然是可诊断的。图 5(a)和图 5(c)的两个模型同样是弱可区分的,但是同步的结果却是不可诊断的,图 5(a)模型的两条路径是 $o_3 c_1, c_2 o_3$,图 5(c)模型的两条路径是 $o_4 c_1, c_2 o_4$,同步的结果是 $(o_3 \parallel o_4) c_1$ 和 $c_2 (o_3 \parallel o_4)$,可知同步后的路径不可区分的,所以是不可诊断的。

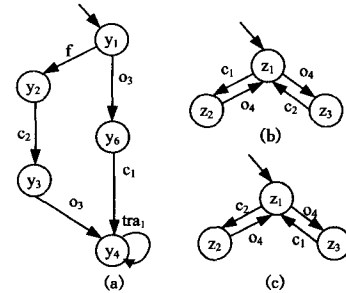


图 5 子系统都是含有弱可区分路径时的可诊断性

性质 3 Γ_1 和 Γ_2 是两个可以互相通信的受限局部模型, Γ_1 中有故障出现且是局部不可诊断的,若 Γ_1 和 Γ_2 都是弱可区分的,且 Γ_1 和 Γ_2 中,一个模型的观测事件全在 c_i 之前发生,另一个模型的观测事件全在 c_i 之后发生,则该故障是可诊断的,否则是不可诊断的。

假设 Γ_1 中的路径为 $L_1 c_1, c_2 L_1, \Gamma_2$ 中对应通信事件所在的路径为 $c_1 L_3 (L_3 c_1), L_3 c_2 (c_2 L_3)$,同步时可以看出 $L_1 c_1 L_3$ 和 $L_3 c_2 L_1$ 明显是可诊断的。而若 Γ_2 的路径为 $L_3 c_1, c_2 L_3$,同步之后 $(L_1 \parallel L_3) c_1$ 和 $c_2 (L_1 \parallel L_3)$,其结果是不可诊断的。

由性质 3 可知,观测事件和通信事件之间的时序关系对于可诊断性的判定有很大影响。

上述情况均基于一个假设:在不满足性质 1 的情况下,一个模型的一条路径上仅出现一个通信事件,而在一般的模型中该假设是不成立的。一条路径上可能出现多个通信事件的情况,受限局部模型路径上的通信事件都满足受限的条件,即其观测事件均在通信事件的一侧。此时,可选一模型的任一条路径,把这条路径上的通信事件 c_i 都提取出来,然后保持其它路径不变,再考虑使得这个系统可诊断所需的条件,另一条路径上的观测事件必须在通信事件的另一侧,找出符合条件的通信事件集。在另一个模型上先检查 c_i 是否满足判定 3,即对应于上一个模型 c_i 的观测事件是否在 c_i 另一侧,若不满足,则是不可诊断的;若满足,则和上个模型进行一样的处理,找出另一条路径上符合条件的通信事件集,检查两个模型得出的通信事件是否有交集,若交集不为空,则该系统就是可诊断的,否则在第一个模型的被选择路径上找下一个通信事件继续处理。具体步骤如下所示:

(1)任取一个模型上的一条路径,从这条路径的第一个通信事件 c_i 开始,在另一条路径上寻找对应满足弱可区分性的通信事件集。

(2)从另一个模型中找出 c_i ,若不满足性质 3,即不满足一个模型的观测事件全在 c_i 之前发生,另一个模型的观测事件全在 c_i 之后发生,则回到(1)中的路径中找 c_i 的下一个通信事件;若满足性质 3,则在该模型中找出另一条路径上对应与 c_i 可能满足弱可区分性的通信事件集。

(3)若(1)和(2)中得到的两个通信事件集交集不为空,即满足性质 3,则该系统可诊断;若交集为空,则回到(1)中的路径来找 c_i 的下一个通信事件。

图 3(a)中可观测事件在 c_2 的右侧,则另一条路径上可观测事件必定要在通信事件左侧才有可能满足弱可区分的条件,符合这些条件的通信事件有 $\{c_3, c_5\}$ 。图 3(b)中 c_2 的可观测事件在左侧,则另一条路径上可观测事件必定要在通信事件右侧才有可能满足弱可区分的条件,符合条件的通信事件有 $\{c_1, c_3\}$,两个模型中有通信事件 c_3 共同满足条件,所以系统是诊断的。

4 局部模型可诊断性的判断

在局部模型中,有些路径的有无对于可诊断性的判断无任何影响,对其进行剪枝,并不影响可诊断性的判定。所以在对局部模型的可诊断性进行判断之前,先进行必要的剪枝,即只保留那些关键路径,并对模型进行化简。

与受限局部模型的处理方法一样,先考虑一条路径上仅出现一个通信事件的情况。

性质 4 G_1 和 G_2 是两个可以互相通信的局部模型, G_1 中有故障出现且是局部不可诊断的,总能找到与之对应的受限局部模型 Γ_1 和 Γ_2 ,使得 G_1 和 G_2 同步的诊断结果与 Γ_1 和 Γ_2 根据时序进行可诊断性判定的结果是一致的。

G_1 和 G_2 是两个局部不可诊断模型,假设 G_1 中的关键路径为 $L_1 c_1 L_2, L_3 c_2 L_4 L_2$ (其中 $L_3 L_4 = L_1$)。通信事件 c_1, c_2 同一侧相同的观测事件(左侧 L_3 , 右侧 L_2)剪枝,化简成受限局部模型 Γ_1 含有的路径为 $L_4 c_1, c_2 L_4$ 。 G_2 中对应的不可区分路径假设为 $L_6 c_1 L_5, L_8 L_7 c_2 L_8$ (其中 $L_5 = L_7 L_8$)。同样对其进行剪枝操作,得到另一个受限局部模型 Γ_2 ,其包含路径 $c_1 L_7, L_7 c_2$ 。 G_1 和 G_2 同步的结果是可诊断的, Γ_1 和 Γ_2 根据时序进行可诊断性判定的结果也是可诊断的。当 G_2 中对应的不可区分路径为 $L_6 c_1 L_5, L_9 c_2 L_{10} L_5$ (其中 $L_6 = L_9 L_{10}$)时,同理可判断, G_1 和 G_2 同步的诊断结果与 Γ_1 和 Γ_2 根据时序进行可诊断性判定的结果都是不可诊断的。

可以把一些局部模型化简成与其可诊断性等价的受限局部模型,再根据受限局部模型的性质对其进行可诊断性的判定。

上面所处理都是在模型的一条路径上仅出现了一个通信事件的情况。而在正常的模型中,一条路径上可能出现多个通信事件,一种处理情况是从含有故障的局部模型的关键路径中逐对地考虑通信事件,根据性质 4,构造出它的受限局部模型,而不含故障的局部模型根据对应的通信事件构造自己的受限局部模型,如果受限局部模型是可诊断的,则整个系统是诊断的。这种方法需要构造的受限局部模型的数目是关键路径上两条路径通信事件数乘积的 2 倍。

可以不必构造受限局部模型,只根据它们的性质,就可进行可诊断性的判定。从含有故障模型的一条路径 L 出发,找

出第一个通信事件,令 p_{c_i} 为 G 中一条从初始状态 q_0 到 c_i 发生后的状态 q_k 的路径,其观测序列为 $obs_1 \cdots obs_j$, 状态 q_k 之后的路径上出现的第一个观测事件为 obs_{j+1} 。则另一条路径上的通信事件可分为 3 种情况,第一种是在 obs_1 到 obs_j 观测事件序列之间的通信事件集 C_1 ;第二种是在事件 obs_{j+1} 之后的路径上出现的通信事件集 C_2 ;第三种是 obs_j 与 obs_{j+1} 两者之间的出现的通信事件集 C_3 ,根据性质 2 可知这类通信事件是不可诊断的。根据性质 3,对应上面的 3 种情况,在另一个模型中做如下操作:一条路径中对应 c_i 的 p'_{c_i} ,其观测序列为 $obs'_1 \cdots obs'_m$,第一种情况下,得到另一条路径上 obs'_{m+1} 之后的出现的通信事件集 C'_1 ;第二种情况下,得到另一条路径上 obs'_1 到 obs'_m 之间的通信事件集 C'_2 ;若 C_1 与 C'_1 或 C_2 与 C'_2 两个事件集有交集,则这个系统就是可诊断的,否则,从 L 中找下一个通信事件,做同样的操作,直到能判定系统是诊断的或考虑完路径上的所有通信事件仍是不可诊断的。具体步骤如下:

(1)对含有故障模型取关键路径,另一个模型根据对应的通信事件取不可区分路径。

(2)任取含有故障模型的一条路径 L ,找出第一个通信事件 c_i 。

(3)该模型另一条路径上的通信事件可以分成 3 种情况:

1) obs_1 到 obs_j 观测事件序列之间的通信事件集。

2) 在事件 obs_{j+1} 之后的路径上出现的通信事件集。

3) obs_j 与 obs_{j+1} 两者之间的出现的通信事件集。根据性质 2,这部分的通信事件诊断不出故障,可以不考虑。

(4)先在另一个模型的一条路径上找出 c_i ,针对上述 3 种情况,在另一条路径上分别对应如下情况:

1) 对应(3)中的 1), obs'_{m+1} 观测事件之后出现的通信事件集。

2) 对应(3)中的 2), obs'_1 到 obs'_m 观测事件序列之间的通信事件集。

(5)若(3)、(4)对应的 1), 2)的通信事件集交集不为空,则系统就是可诊断的;若为空,则在最初的路径上找 c_i 之后的通信事件,进入步骤(3)。

结束语 在文献[7]的实例中,先要构造图 4 中两个局部模型的检测器,图 4(a)的检测器构造完后有 17 个状态和 34 个转换,图 4(b)的检测器有 9 个状态和 14 个转换。图 4(a)和图 4(b)的检测器同步后有 21 个状态和 38 个转换。对于一般模型而言,假设局部模型 a 的状态数是 m ,局部模型 b 的状态数是 n ,则构造检测器后 a 的空间复杂度是 $O(n^2)$, b 的空间复杂度是 $O(m^2)$,模型 a 和 b 同步后的系统空间复杂度是 $O(m^2 \times n^2)$,时间复杂度是 $O(m^2 \times n^2)$ 。本文中只需要考虑原有的模型中的状态和转换数,即图 4(a)的 5 个状态和 6 个转换,图 4(b)的 3 个状态和 4 个转换。在同步过程中影响可诊断性判定的关键因素是事件之间的时序关系,本文给出的方法是把这一关键因素从模型中提取出来单独考虑,这样很多对判定可诊断性无用的信息就可不考虑了。此时,模型规模进一步缩减,可以不必进行同步,只需检测本文中给出的 3 个性质即可判断可诊断性。对于一般模型而言,从本文给出的算法可知,从一个模型的一条路径开始,搜索另一模型上的所有路径,算法在时间上的复杂度是 $O(m \times n)$,空间复杂度是 $O(m+n)$ 。

(下转第 251 页)

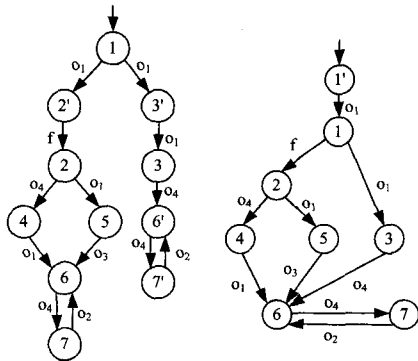
与传统免疫理论不同,近年兴起的受体编辑理论认为 T 淋巴细胞在一定条件下可以改变自身受体的特异性及其亲和力。受该理论启发,本文提出了一种基于受体编辑的实值阴性选择算法 RERNS,在 RERNS 算法中采用了两种受体编辑方法:DRE 和 DREINS。其中 DRE 改善了算法对边界区域的覆盖;DREINS 扩大了算法对非自体空间的覆盖。理论分析与实验验证表明,RERNS 算法的检测性能优于 RNS 和 V-detector 算法。

参考文献

- [1] Forrest S, Perelson A S, Allen L, et al. Self-nonspecific discrimination in a computer[C]//Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy. Los Alamitos: IEEE Computer Soc Press, 1994: 202-212
- [2] Forrest S, Beauchemin C. Computer immunology[J]. Immunol Rev, 2007, 216(1): 176-197
- [3] 李涛. 计算机免疫学[M]. 北京: 电子工业出版社, 2004: 147-159
- [4] Timmis J. Artificial immune systems—today and tomorrow[J]. Natural Computing, 2007, 6(1): 1-18
- [5] Balhrop J, Esponda F, Forrest S, et al. Coverage and generalization in an artificial immune system[C]//GECCO 2002. New York: Morgan Kaufmann Publishers Inc, 2002: 3-10

- [6] 张衡, 吴礼发, 张毓森, 等. 一种 r 可变阴性选择算法及其仿真分析[J]. 计算机学报, 2005, 28(010): 1614-1619
- [7] 何申, 罗文坚, 王煦法. 一种检测器长度可变的非选择算法[J]. 软件学报, 2007, 18(6): 1361-1368
- [8] Gonzalez F, Dasgupta D, Gomez J. The effect of binary matching rules in negative selection[C]//GECCO 2003. Chicago: Springer Berlin, 2003: 196-206
- [9] Ji Z, Dasgupta D. Real-valued negative selection algorithm with variable-sized detectors [C] // GECCO 2004. Washington: Springer Berlin, 2004: 287-298
- [10] Ji Z. A boundary-aware negative selection algorithm[C]//The Ninth IASTED, Benidorm: Acta Press, 2005: 29-42
- [11] Ji Z, Dasgupta D. Estimating the detector coverage in a negative selection algorithm [C] // GECCO 2005. Washington: ACM Press, 2005: 281-288
- [12] Ji Z, Dasgupta D. V-detector: An efficient negative selection algorithm with “probably adequate” detector coverage[J]. Information Sciences, 2009, 179(10): 1390-1406
- [13] Nemazee D. Receptor editing in lymphocyte development and central tolerance[J]. Nature Reviews Immunology, 2006, 6(10): 728-740
- [14] 罗微, 马骊, 王小宁. T 细胞受体编辑与修正[J]. 中华微生物学和免疫学杂志, 2008, 28(3): 278-281

(上接第 214 页)



(a) 未合并状态之前的图 (b) 合并状态之后的图
图 6

第 3 节中的 3 个性质包括了通信事件和可观测事件之间时序信息的所有情况,所以单独抽取时序信息对可诊断性的判定和全局模型可诊断性判定的结果是一致的。本文侧重的是快速地对可诊断性做出判定。提取时序信息由于简化了很多其他信息,因此其带来的后果是不能得出具体的关键路径。

在全局模型分解成局部模型时,可以对一些状态进行合并以达到缩减模型规模的效果。与文献[10]的方法类似,从开始状态到无故障状态出现的路径 p ,若有一不含故障的路径和 p 有相同的观测,则合并这两条路径,例如图 6(a)中的事件 o_1 ;出现故障状态的路径,若存在一条路径到达稳定状态的观测与其一致,则同样可以合并一致的观测;例如图 6(a)的 $o_2 o_4$ 循环,图 6(b)是图 6(a)经过状态合并后得到的图,图 6(b)中从状态 1 开始考虑模型的划分,即是第 2 节中用到的全局模型。如果全局模型是可诊断的,在划分成局部模型时,域的选择对可诊断性的判断有很大的影响,有可能在划分出的某一个局部模型中能直接判断出该系统是可诊断的。所以,域的有效选择对局部模型可诊断性的判定有很大影响。以后要做的工作是,如何选取合适的域,把一个全局模型划分

成 n 个局部模型;如何运用时序信息,以最少的局部模型判定全局模型的可诊断性。

参考文献

- [1] Lin F. Diagnosability of discrete-event systems and its applications[J]. J. Discrete Event Dyn. Syst.: Theory Appl., 1994, 4(2): 197-212
- [2] Bavishi S. Automated fault diagnosis using a discrete event systems framework[C]//Proceedings of the 1994 IEEE International Symposium on. 1994: 213-218
- [3] Sampath M, Sengupta R, Lafortune S, et al. Diagnosability of discrete-event systems in IEEE Trans[J]. Automat. Contr., 1995, 40: 1555-1575
- [4] Jiang S, Huang Z, Chandra V, et al. A polynomial algorithm for testing diagnosability of discrete event systems[J]. IEEE Transactions on Automatic Control, 2001, 46(8): 1318-1321
- [5] 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
- [6] Debouk R, Lafortune S, Teneketzis D. Coordinated Decentralized Protocols for Failure Diagnosis of Discrete Event Systems[J]. Discrete Event Dynamic Systems, 2000, 10(1/2): 33-86
- [7] Pencolé Y. Diagnosability analysis of distributed discrete event systems[C]//Proceedings of European Conference on Artificial Intelligence(ECAI'04). 2004: 43-47
- [8] Grastien A. Symbolic Testing of Diagnosability[C]//DX 09. 2009: 131-138
- [9] Khoumsi A. Coordination of Components in a Distributed Discrete-Event System[C]//Processing of the 4th International Symposium on Parallel and Distributed Computing(ISPDC'05). 2005: 299-306
- [10] Schumann A. Towards Efficiently Diagnosing Large Scale Discrete-Event Systems[D]. Australian National University, 2007