行为时序逻辑中公平性的研究与完善

唐郑熠, 李均涛, 李 祥
(贵州大学 计算机软件与理论研究所, 贵阳 550025)

摘 要: 基于行为时序逻辑(TLA)的并发系统描述,就是对系统的初始状态、系统行为和行为的公平性进行规约和描述,但 TLA 中的公平性具有局限性,无法准确地描述某些系统的行为,从而限制了 TLA 的描述能力。通过研究 TLA 中公平性的推导过程,分析公平性的概念与定义方法,并以实际例子说明它的局限性。在此基础上,提出以加入两级新的公平性方式对其进行完善。最后,证明了新公平性等级之间的蕴涵关系。完善后的公平性具有更强的描述能力,能够对系统进行更完整的描述与规约。

关键词: 行为时序逻辑; 公平性; 并发系统; 系统描述; 蕴涵关系
中图分类号: TP301.2 **文献标志码**: A **文章编号**: 1001-3695(2010)05-1788-03
doi:10.3969/j.issn.1001-3695.2010.05.052

Research and improvement of fairness in temporal logic of actions

TANG Zheng-yi, LI Jun-tao, LI Xiang
(*Institute of Computer Software & Theory, Guizhou University, Guiyang* 550025, *China*)

Abstract: The description of concurrent system based on TLA is specifying the initial state, actions and actions fairness of concurrent system. But the fairness in TLA can't describe some systems' actions accurately. This limitation restrict the description ability of TLA. This paper analyzed the definition and conception by studying on the derivation process of TLA's fairness and used practical example to show the limitation of TLA's fairness. On this basis, it put forward to improve the fairness system by adding tow new fairness levels. Finally, it proved the implication relation of new fairness levels. The improved fairness has stronger description ability, and can describe and specify systems more entirely.

Key words: TLA(temporal logic of action); fairness; concurrent system; system description; implication relation

0 引言

行为时序逻辑(TLA)[1]是由美国科学家 Lamport 提出的一种组合了时序逻辑与行为逻辑的程序逻辑,用于对并发系统进行描述和验证。它引入了行为和运转的概念,使得系统和系统属性能够用相同的逻辑来表示。目前,微软、欧盟等公司和组织都已成立了专门的项目组,将 TLA 应用于系统规约和验证。

TLA 用逻辑公式来描述系统的初始状态、系统行为和活性(liveness);TLA 用行为的公平性(fairness)的概念来描述活性,即行为发生的频率[2]。TLA 将行为的公平性分为强弱两级,但这两级公平性只能够描述行为无限次发生的情况,限制了 TLA 对系统的描述能力。本文将对 TLA 中公平性的概念和定义进行深入研究,并对其进行推导和展开;同时,以实际例子说明了其局限性,提出以加入两级新的公平性的方式对其进行完善;最后,证明了新公平性等级之间的蕴含关系了。

1 预备知识

本章首先简要介绍一些 TLA 中的定义。

定义 1 原本变量(primed variable)[1],变量的下一状态值。如果用 v 表示变量 v 的值,那么 v 的原本变量 v' 表示变量 v 在下一状态的值。

定义 2 行为(action)[1],由变量、原本变量及常量符号组成的布尔表达式。变量与当前状态相关,原本变量与下一状态相关。

定义 3 哑步(stuttering steps)[1],是一种特殊的行为,在该行为发生后,系统中所有变量的值都保持不变。

定义 4 状态函数(state function)[1],由变量和常量符号组成的非布尔表达式。

定义 5 标记转移系统[2],一个标记转移系统 $T=(Q,I,A,\delta)$。其中:系统中所有变量的一次有效赋值称为一个状态 q,所有的状态(即所有可能的赋值)构成状态集合,记为 Q;初始状态 $I\subseteq Q$;A 是所有行为构成的集合;$\delta\subseteq Q\times A\times Q$。

定义 6 运转(run)[2],它是由无限或有限多个状态组成的序列 $\sigma=q_0\overset{A_0}{\rightarrow}q_1\overset{A_1}{\rightarrow}q_2\cdots$。其中:$q_0\in I, A_i\in A, (q_i,A_i,q_{i+1})\in\delta$。$\sigma^{+i}=q_i\overset{A_i}{\rightarrow}q_{i+1}\overset{A_{i+1}}{\rightarrow}q_{i+2}\cdots$TLA 引入了哑步,有限长的运转可以通过哑步扩展为无限长的运转,因此 TLA 中的运转都无限长。

定义 7 使能(enabled)[1]。一个行为 $A\in A$ 在状态 $q_i\in Q$ 是使能的,当且仅当存在状态 $q_j\in Q$,使得 $(q_i,A_i,q_j)\in\delta$,记为 Enabled A。

定义 8 对于时序逻辑公式 F,运转 σ,有[3]:

$\sigma\models F$,当且仅当 $\sigma^{+0}\models F$。

收稿日期: 2009-09-09; **修回日期**: 2009-10-21

作者简介:唐郑熠(1984-),男,系统分析师,博士研究生,主要研究方向为模型检测、协议分析(willian_falcon@126.com);李均涛(1969-),男,工程师,博士研究生,主要研究方向为模型检测;李祥(1942-),男,教授,博导,主要研究方向为计算复杂性、密码学.

$\sigma \models \Box F$,当且仅当$\forall n \in \mathrm{Nat}, \sigma^{+n} \models F$。

$\sigma \models \Diamond F$,当且仅当$\exists n \in \mathrm{Nat}, \sigma^{+n} \models F$。

定义 9　对于行为 A 和状态函数 f,有$[A]_f \equiv A \vee (f' = f)$,$\langle A \rangle_f \equiv A \wedge (f' \neq f)$。

2　TLA 中的公平性

TLA 中行为的公平性是对于一次运转而言的,分为强弱两级。

定义 10　弱公平性(weak fairness)[1]。对于一次运转 σ,如果$\sigma \models \Box((\Diamond\langle A\rangle_f) \vee (\Diamond A \ \mathrm{Enabled}\langle A\rangle_f))$,则行为 A 在该运转 σ 上具有弱公平性,记为 $\sigma \models \mathrm{WF}_f(A)$。

下面将其展开:

$$\sigma \models \mathrm{WF}_f(A)$$
$$\equiv \sigma \models \Box((\Diamond\langle A\rangle_f) \vee (\Diamond A \ \mathrm{Enabled}\langle A\rangle_f))$$
$$\equiv \sigma \models \Box((\Diamond\langle A\rangle_f) \vee (A \ \Box\mathrm{Enabled}\langle A\rangle_f))$$
$$\equiv \sigma \models \Box(\Box\mathrm{Enabled}\langle A\rangle_f \Rightarrow \Diamond\langle A\rangle_f)$$
$$\equiv \forall n: (\sigma^{+n} \models \Box\mathrm{Enabled}\langle A\rangle_f \Rightarrow \Diamond\langle A\rangle_f)$$
$$\equiv \forall n: (\sigma^{+n} \models \Box\mathrm{Enabled}\langle A\rangle_f \Rightarrow \sigma^{+n} \models \Diamond\langle A\rangle_f)$$
$$\equiv \forall n: (\forall m: (\sigma^{+n+m} \models \mathrm{Enabled}\langle A\rangle_f) \Rightarrow \exists k: (\sigma^{+n+k} \models \langle A\rangle_f))$$
$$\equiv \forall n: ((\forall m: (q_{n+m}, \langle A\rangle_f, q_{n+m+1}) \in A) \Rightarrow (\exists k: A_{n+k} = \langle A\rangle_f))$$

弱公平性的含义是,如果一个行为在一次运转上的所有状态都是使能的,那么这个行为一定会发生无限多次。

定义 11　强公平性(strong fairness)[1]:对于一次运转 σ,如果$\sigma \models \Box((\Diamond\langle A\rangle_f) \vee (\Diamond\Box A \ \mathrm{Enabled}\langle A\rangle_f))$,则行为 A 在该运转 σ 上具有强公平性,记为 $\sigma \models \mathrm{SF}_f(A)$。

下面将其展开:

$$\sigma \models \mathrm{SF}_f(A)$$
$$\equiv \sigma \models \Box((\Diamond\langle A\rangle_f) \vee (\Diamond\Box A \ \mathrm{Enabled}\langle A\rangle_f))$$
$$\equiv \sigma \models (\Box\Diamond\langle A\rangle_f) \vee (\Diamond\Box A \ \mathrm{Enabled}\langle A\rangle_f)$$
$$\equiv \sigma \models (\Box\Diamond\langle A\rangle_f) \vee (A \ \Box\Diamond\mathrm{Enabled}\langle A\rangle_f)$$
$$\equiv \sigma \models (\Box\Diamond\mathrm{Enabled}\langle A\rangle_f \Rightarrow \Box\Diamond\langle A\rangle_f)$$
$$\equiv \sigma \models \Box(\Diamond\mathrm{Enabled}\langle A\rangle_f \Rightarrow \Diamond\langle A\rangle_f)$$
$$\equiv \forall n: (\sigma^{+n} \models \Diamond\mathrm{Enabled}\langle A\rangle_f \Rightarrow \Diamond\langle A\rangle_f)$$
$$\equiv \forall n: (\sigma^{+n} \models \Diamond\mathrm{Enabled}\langle A\rangle_f \Rightarrow \sigma^{+n} \models \Diamond\langle A\rangle_f)$$
$$\equiv \forall n: (\exists m: (\sigma^{+n+m} \models \mathrm{Enabled}\langle A\rangle_f) \Rightarrow \exists k: (\sigma^{+n+k} \models \langle A\rangle_f))$$
$$\equiv \forall n: ((\exists m: (q_{n+m}, \langle A\rangle_f, q_{n+m+1}) \in A) \Rightarrow (\exists k: A_{n+k} = \langle A\rangle_f))$$

强公平性的含义是,如果一个行为在一次运转上的无限多个状态是使能的,那么这个行为一定会发生无限多次。

强公平性蕴涵弱公平性$(\mathrm{SF}_f(A) \Rightarrow \mathrm{WF}_f(A))$,这是显而易见的,因为$(\Diamond\Box\text{-}\ \mathrm{Enabled}\langle A\rangle_f) \Rightarrow (\Diamond\text{-}\ \mathrm{Enabled}\langle A\rangle_f)$。也就是说,如果一个行为 A 在一次运转 σ 上具有强公平性,那么它也一定具有弱公平性。值得注意的是,能满足弱公平性的运转要比能满足强公平性的运转多。

3　TLA 中公平性的不足与完善

3.1　基于 TLA 的并发系统规约与描述

用 TLA 来对并发系统进行描述与规约,需要将系统的初始状态、行为以及活性规约成时序逻辑公式,然后将它们表示为一个合取式。其中,初始状态和行为的合取又被称为系统的安全性,即排除系统不应该出现的行为[4]。系统的活性是指最终会发生的行为,在 TLA 中是用行为的公平性来描述的[5]。

用伪代码书写的简单程序:

```
var natural x, y = 0;
do
    ⟨true→x: = x + 1⟩
    ⟨true→y: = y + 1⟩
od
```

Lamport 使用 TLA 对上述简单程序进行的规约与描述[1]如下:

$$\mathrm{Init}_\Phi \equiv (x = 0) \wedge (y = 0)$$
$$M_1 \equiv (x' = x + 1) \wedge (y' = y)$$
$$M_2 \equiv (y' = y + 1) \wedge (x' = x)$$
$$M \equiv M_1 \vee M_2$$
$$\Phi \equiv \mathrm{Init}_\Phi \wedge \Box[M]_{\langle x,y\rangle} \wedge \mathrm{WF}_{\langle x,y\rangle}(M_1) \wedge \mathrm{WF}_{\langle x,y\rangle}(M_2)$$

简单程序包含一个由 Dijkstra 定义的 do 语句[6]。这个程序所表示的系统从"$(x = 0) \wedge (y = 0)$"(Init_Φ)这个状态开始运行,不断地执行"$(x' = x + 1) \wedge (y' = y)$"($M_1$)、"$(y' = y + 1) \wedge (x' = x)$"($M_2$)和"$(x' = x) \wedge (y' = y)$"(哑步)这三个行为中的一个。同时,由于 M_1 和 M_2 这两个行为的执行没有任何先决条件,完全是随机选择的,这两个行为在系统中的任何状态都是使能的。可以用弱公平性来描述这两个行为执行的频率,即无限次执行。

基于 TLA 的规约与描述程序代码中 Φ 描述了符合以下条件的运转 σ:

a)起始状态都是 Init_Φ。

b)只出现行为 M_1、M_2 和哑步。

c)对于运转 σ 中的任意状态 q_i,$\exists (j \geqslant i)$,$A_j = M_1$ 或 M_1 在 q_j 上不使能。

d)对于运转 σ 中的任意状态 q_i,$\exists (j \geqslant i)$,$A_j = M_2$ 或 M_2 在 q_j 上不使能。

3.2　TLA 中公平性的不足

显而易见,Φ 所描述的运转 σ 中,行为 M_1 和 M_2 都是无限次地发生,但公式 Φ 无法描述图 1 所示的运转。

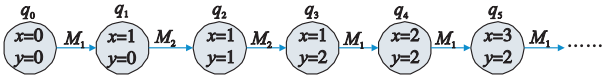

图1　一个公式Φ无法描述的运转

图 1 中的运转 σ,行为 M_2 只是在"$q_1 \rightarrow q_2$""$q_2 \rightarrow q_3$"的迁移中发生两次,其他时候发生的行为都是 M_1。在状态 q_3,显然不满足$((\Diamond\langle M_2\rangle_{\langle x,y\rangle}) \vee (\Diamond\text{-}\ \mathrm{Enabled}\langle A\rangle_{\langle x,y\rangle}))$,因此该运转不满足 $\mathrm{WF}_{\langle x,y\rangle}(M_2)$,也就不满足公式 Φ。

很明显,公式 Φ 无法描述那些 M_1 或 M_2 只发生有限次的运转,但是这样的运转却是简单程序执行时可能出现的情况。公式 Φ 无法描述这样的运转,显然也就无法完整地描述简单程序所表示的系统。

即使将弱公平性换成强公平性也无法解决这个问题,因为 TLA 中的强弱两级公平性都只能描述行为无限次发生或无限次不使能的情况,而无法描述系统行为有限次发生或有限次使能的情况。

3.3　TLA 中公平性的完善

为了解决这个问题,本文提出的方案是加入两级新的公平性来描述行为有限次发生或有限次使能的情况,从而构成四级公平性。

定义 12　一级公平性(one-level fairness):对于一次运转 σ,如果$\sigma \models \Diamond((\Diamond\langle A\rangle_f) \vee (\Diamond\text{-}\ \mathrm{Enabled}\langle A\rangle_f))$,则行为 A 在该运转 σ 上具有一级公平性,记为 $\sigma \models \mathrm{L1F}_f(A)$。

下面将其展开：

$\sigma \models L1F_f(A)$

$\equiv \sigma \models \Diamond((\Diamond\langle A\rangle_f) \vee (\Diamond \text{Enabled}\langle A\rangle_f))$

$\equiv \sigma \models \Diamond((\Diamond\langle A\rangle_f) \vee (-\Box \text{Enabled}\langle A\rangle_f))$

$\equiv \sigma \models \Diamond(\Box \text{Enabled}\langle A\rangle_f \Rightarrow \Diamond\langle A\rangle_f)$

$\equiv \exists n:(\sigma^{+n} \models \Box \text{Enabled}\langle A\rangle_f \Rightarrow \Diamond\langle A\rangle_f)$

$\equiv \exists n:(\sigma^{+n} \models \Box \text{Enabled}\langle A\rangle_f \Rightarrow \sigma^{+n} \models \Diamond\langle A\rangle_f)$

$\equiv \exists n:(\forall m:(\sigma^{+n+m} \models \text{Enabled}\langle A\rangle_f) \Rightarrow \exists k:(\sigma^{+n+k} \models \langle A\rangle_f))$

$\equiv \exists n:((\forall m:(q_{n+m}, \langle A\rangle_f, q_{n+m+1}) \in A) \Rightarrow (\exists k:A_{n+k} = \langle A\rangle_f))$

一级公平性的含意是，如果一个行为在一次运转上出现连续的无限多次使能，那么这个行为一定会发生有限多次。

定义 13 二级公平性(tow-level fairness)。对于一次运转 σ，如果 $\sigma \models \Diamond((\Diamond\langle A\rangle_f) \vee (\Diamond - \text{Enabled}\langle A\rangle_f))$，则行为 A 在该运转 σ 上具有二级公平性，记为 $\sigma \models L2F_f(A)$。

下面将其展开：

$\sigma \models L2F_f(A)$

$\equiv \sigma \models \Diamond((\Diamond\langle A\rangle_f) \vee (\Diamond\Box - \text{Enabled}\langle A\rangle_f))$

$\equiv \sigma \models (\Diamond\Diamond\langle A\rangle_f) \vee (\Diamond\Diamond\Box - \text{Enabled}\langle A\rangle_f)$

$\equiv \sigma \models (\Diamond\Diamond\langle A\rangle_f) \vee (\Diamond\Box A \text{ Enabled}\langle A\rangle_f)$

$\equiv \sigma \models \Diamond((\Diamond\langle A\rangle_f) \vee (\Box - \text{Enabled}\langle A\rangle_f))$

$\equiv \sigma \models \Diamond((\Diamond\langle A\rangle_f) \vee (- \Diamond \text{Enabled}\langle A\rangle_f))$

$\equiv \sigma \models \Diamond(\Diamond \text{Enabled}\langle A\rangle_f \Rightarrow \Diamond\langle A\rangle_f)$

$\equiv \exists n:(\sigma^{+n} \models \Diamond \text{Enabled}\langle A\rangle_f \Rightarrow \Diamond\langle A\rangle_f)$

$\equiv \exists n:(\sigma^{+n} \models \Diamond \text{Enabled}\langle A\rangle_f \Rightarrow \sigma^{+n} \models \Diamond\langle A\rangle_f)$

$\equiv \exists n:(\exists m:(\sigma^{+n+m} \models \text{Enabled}\langle A\rangle_f) \Rightarrow \exists k:(\sigma^{+n+k} \models \langle A\rangle_f))$

$\equiv \exists n:((\exists m:(q_{n+m}, \langle A\rangle_f, q_{n+m+1}) \in A) \Rightarrow (\exists k:A_{n+k} = \langle A\rangle_f))$

二级公平性的含义是，如果一个行为在一次运转上是有限多次使能的，那么这个行为一定会发生有限多次。

定义 14 三级公平性(three-level fairness)，即 TLA 中的弱公平性，记为 $\sigma \models L3F_f(A)$。

定义 15 四级公平性(four-level fairness)，即 TLA 中的强公平性，记为 $\sigma \models L4F_f(A)$。

用一级公平性($L1F_f(A)$)就可以描述那些行为 M_1 或 M_2 只发生有限次，或者行为 M_1 和 M_2 都只发生有限次的运转。

3.4 新公平性等级之间的蕴涵关系

定理 1 $L2F_f(A) \Rightarrow L1F_f(A)$

证明 $L1F_f(A) \equiv \Diamond((\Diamond\langle A\rangle_f) \vee (\Diamond - \text{Enabled}\langle A\rangle_f))$，$L2F_f(A) \equiv \Diamond((\Diamond\langle A\rangle_f) \vee (\Diamond\Box - \text{Enabled}\langle A\rangle_f))$

因为，$\Diamond\Box \Rightarrow \Diamond$，所以 $L2F_f(A) \Rightarrow L1F_f(A)$。

定理 2 $L4F_f(A) \Rightarrow L3F_f(A)$

证明 即 TLA 中的强公平性蕴涵弱公平性。

定理 3 $L3F_f(A) \Rightarrow L1F_f(A)$

证明 $L1F_f(A) \Rightarrow ((\Diamond\langle A\rangle_f) \vee (\Diamond - \text{Enabled}\langle A\rangle_f))$，$L3F_f(A) \equiv \Diamond((\Diamond\langle A\rangle_f) \vee (\Diamond - \text{Enabled}\langle A\rangle_f))$

因为，$\Box \Rightarrow \Diamond$，所以 $L3F_f(A) \Rightarrow L1F_f(A)$。

定理 4 $L4F_f(A) \Rightarrow L2F_f(A)$

证明 $L2F_f(A) \equiv \Diamond((\Diamond\langle A\rangle_f) \vee (\Diamond\Box - \text{Enabled}\langle A\rangle_f))$，$L4F_f(A) \equiv \Box((\Diamond\langle A\rangle_f) \vee (\Diamond\Box - \text{Enabled}\langle A\rangle_f))$

因为，$\Box \Rightarrow \Diamond$，所以 $L4F_f(A) \Rightarrow L2F_f(A)$。

4 结束语

行为时序逻辑通过规约系统的初始状态和系统行为来表示系统的安全性，通过规约系统行为的公平性来表示系统的活性，从而将整个系统用一个时序逻辑公式来表示。系统行为的公平性将直接影响到系统描述的正确性和完整性。对于公平性进行深入的研究和分析有助于对并发系统进行正确的描述，而对于公平性进行完善和扩展则有助于增强 TLA 的描述能力，更好地描述并发系统。

参考文献：

[1] LAMPORT L. The temporal logic of action[J]. ACM Trans on Programming Languages and Systems, 1994, 16(3): 872-923.

[2] MERZ S. Modeling and developing systems using TLA$^+$[J]. Escuela de Verano, 2005, 73(3): 207-244.

[3] 万良. 基于行为时序逻辑 TLA 的系统、规则与协议检测的研究[D]. 贵阳：贵州大学，2009.

[4] 张昭理，洪帆，肖海军. 基于 Petri 网的混合安全策略建模与验证[J]. 计算机应用研究，2008，25(2)：509-511.

[5] LAMPORT L. Specifying systems[M]. New York: Addison-Wesley, 2002.

[6] DIJKSTRA E. A discipline of programming[M]. New Jersey: Prentice-Hall, 1976.

(上接第 1772 页)

3 结束语

在设计试验中，最重要的是模型确定。选择 Microsoft 神经网络挖掘算法构建了中医舌诊知识库，验证了可对应的所有记录训练数据，其构建的中医舌诊人工神经网络能够对非样本测试值进行合理的预测。在中医专家试用后，效果令人满意；并证明采用神经网络技术构建中医诊断神经网络知识库，为中医学教学实践应用计算机技术提供了一个新方法，对中医舌象临床诊断规范化应用是一新拓展，也是对中医现代化标准化研究应用的有效探索。

参考文献：

[1] 朱文锋. 中医诊断学[M]. 北京：中国中医药出版社，2000.

[2] 周怡，叶明全，张艳，等. 医学信息决策与支持系统[M]. 北京：人民卫生出版社，2009.

[3] 朱德利. SQL Server 2005 数据挖掘与商业智能完全解决方案[M]. 北京：电子工业出版社，2007.

[4] 周越，杨杰，沈利. 中医舌象信息的数字化方法研究[J]. 生物医学工程学杂志，2004，21(6)：917-920.

[5] 吴芸，周昌乐，张志枫. 中医舌诊八纲辨证神经网络知识库构建[J]. 计算机应用研究，2008，23(6)：188-189.

[6] 王士同. 人工神经网络教程[M]. 北京：电子工业出版社，2006.

[7] MUNDY J. 数据仓库工具箱[M]. 闫雷鸣，译. 北京：清华大学出版社，2007.

[8] 崔雷. 医学数据挖掘[M]. 北京：高等教育出版社，2006.

[9] 白云静，申洪波，孟庆刚. 中医证候研究的人工神经网络方法探析[J]. 中医药学刊，2004，22(12)：21-22.