

Classifying Fairness Levels Based on Temporal Logic Action

Li Jun-Tao, Li Xiang

Institute of Computer Software and Theory

jtxq@21cn.com

Abstract: TLA(Temporal Logic of Actions) and it's specifying language TLA+ have become an efficient and convenient approach for system specifying and verifying, and fairness is a vital property in TLA. We try to analyze fairness based on TLA, subdivide the fairness into levels of detail, and discuss the relationship between them.

Keywords: Transition System; TLA; Fairness; System specifying

基于行为时序逻辑 TLA 的公平性等级细分

李均涛, 李祥

贵州大学计算机软件与理论研究所, 贵阳, 中国, 550025

jtxq@21cn.com

【摘要】 基于行为时序逻辑 TLA(Temporal Logic of Actions)描述的并发系统强调系统的并发行为(Action); 建立在系统并发行为上的公平性是其中一个重要的性质。本文分析基于 TLA 的并发系统的公平性, 对公平性等级进行进一步细分, 并讨论它们之间的关系。

【关键词】 并发系统; 行为时序逻辑; 公平性; 系统描述与验证

1 引言

行为时序逻辑 (TLA^[1]: Temporal Logic of Actions) 是 Leslie Lamport 提出的一种程序逻辑, 其描述语言 TLA+能够同时表达模型程序与系统属性。它基于时序逻辑, 通过对行为及各种操作符的扩展定义, 可实现对并发系统及其性质的描述与验证。

基于行为时序逻辑 TLA(Temporal Logic of Actions) 描述的并发系统强调系统的并发行为(Action); 建立在系统并发行为上的公平性是其中一个重要的性质。本文分析基于 TLA 的并发系统的公平性, 对公平性等级进行细分, 讨论不同等级公平性之间的关系。

2 行为时序逻辑 TLA 简述

2.1 基本概念

定义1 系统状态: 并发系统程序中的所有变量的一次有效赋值。所有这种可能的赋值构成系统状态集, 记为 St 。

定义2 原本变量^[1]: 变量的下一状态值。在 TLA

公式或表达式中, 如果用 v 表示变量 v 的值, 那么 v 的原本变量表示变量 v 在下一状态的值, 记为 v' 。

定义3 行为(action)^[1]: 包含常量、变量、原本变量的布尔值表达式。系统的所有行为构成系统行为集, 记为 $\mathcal{A}$ 。

定义4 状态谓词(state predicate)^[1]: 不含原本变量的行为。

定义5 映射 $\llbracket \cdot \rrbracket: X \rightarrow X$ 的值^[1,2], 即 $\llbracket X \rrbracket \triangleq X$ 的值。如果 X 是变量, $\llbracket X \rrbracket$ 就是 X 的值; 如果 X 是谓词 (包括普通谓词和行为), 则 $\llbracket X \rrbracket$ 就是 X 的布尔值。

定义6 A 步^[1]: $s, t \in St$, $\langle s, t \rangle$ 是一个 A 步, 当且仅当 $\llbracket A \rrbracket = A(\forall v: s[v]/v, t[v]/v')$ 为真。其中 v 为状态变量。如果 $\langle s, t \rangle$ 是一个 A 步, 则可记为 $s \llbracket A \rrbracket t$ 。在 TLA 中, A 步记为 $\langle A \rangle_v$ 。

定义7 运转 (behavior)^[1]: 运转是由无限个状态组成的序列, 记为 σ 。其中第 i 个状态记为 σ_i :

$$\sigma \triangleq \sigma_0 \rightarrow \sigma_1 \rightarrow \sigma_2 \rightarrow \dots$$

$$\sigma^{+n} \triangleq \sigma_n \rightarrow \sigma_{n+1} \rightarrow \sigma_{n+2} \rightarrow \dots$$

定义8 使能(enabled)^{[1][2]}: 一个行为 $A \in \mathcal{A}$ 在状态 $s \in St$ 使能, 当且仅当 St 中存在状态 t , 使得

$s \llbracket A \rrbracket t$ 。A在s使能记为 $s \llbracket Enabled A \rrbracket$ 。其中 $Enabled A$ 称为使能谓词，使能谓词在TLA中记为 $ENABLED \langle A \rangle_v$ 。

2.2 TLA 公式的基本语法及语义

定义9 TLA公式：一个TLA公式 F 是对运转 σ 的一个判定；如果对 σ 来说， F 为真，则称 σ 满足 F ，记为 $\sigma \models F$ 。即： $\sigma \models F \triangleq \llbracket F \rrbracket(\sigma)$ 。

定义10 $\sigma \models (F \wedge G) \triangleq (\sigma \models F) \wedge (\sigma \models G)$
 $\sigma \models \neg F \triangleq \neg(\sigma \models F)$
 $\sigma \models (\exists s \in Q: F) \triangleq \exists s \in Q: (\sigma \models F)$
 $\sigma \models (\forall s \in Q: F) \triangleq \forall s \in Q: (\sigma \models F)$

所有不含量词的TLA公式都可以写成三种最简单公式的合取形式，他们是 P 、 $\Box P$ 和 $\Box A$ ；其中 P 是一个状态谓词， A 是一个行为。他们的含义如下：

定义11 如果对一次运转

$\sigma = \sigma_0 \rightarrow \sigma_1 \rightarrow \sigma_2 \rightarrow \dots$ 的第一个状态 σ_0 有 P 为真，则 $\sigma \models P$ 。即： $\sigma \models P \triangleq \llbracket P \rrbracket(\sigma_0)$ 。

定义12 如果对一次运转

$\sigma = \sigma_0 \rightarrow \sigma_1 \rightarrow \sigma_2 \rightarrow \dots$ 的每一个状态 $\sigma_i, (i \in N)$ 有 P 为真，则 $\sigma \models \Box P$ ^[1]。即： $\sigma \models \Box P \triangleq \forall i \in N: \llbracket P \rrbracket(\sigma_i)$ ^[6]

定义13 如果一次运转

$\sigma = \sigma_0 \rightarrow \sigma_1 \rightarrow \sigma_2 \rightarrow \dots$ 的第一步 $\sigma_0 \rightarrow \sigma_1$ 是一个 A 步，则 $\sigma \models A$ ；如果对 $\forall n: \sigma^{+n} \models A$ ，则 $\sigma \models \Box A$ 。即：

$$\begin{aligned}\sigma \models A &\triangleq \sigma_0 \llbracket A \rrbracket \sigma_1 \\ \sigma^{+n} \models A &\triangleq \sigma_n \llbracket A \rrbracket \sigma_{n+1} \\ \sigma \models \Box A &\triangleq \forall n \in Nat: \sigma^{+n} \models A\end{aligned}$$

由定义8、9、10、11不难推广到对一个任意的TLA公式 F ：

定义14 $\sigma \models \Box F \triangleq \forall n \in Nat: \sigma^{+n} \models F$ 。

由定义14容易得出：

$\sigma \models \Diamond F \triangleq \exists n \in Nat: \sigma^{+n} \models F$ ，这是因为：

$$\begin{aligned}\sigma \models \Diamond F &\triangleq \sigma \models \neg \Box \neg F \\ &\triangleq \neg(\sigma \models \Box \neg F) \\ &\triangleq \neg(\forall n \in N: \sigma^{+n} \models \neg F) \\ &\triangleq \neg(\forall n \in N: \neg(\sigma^{+n} \models F)) \\ &\triangleq \exists n \in Nat: \sigma^{+n} \models F\end{aligned}$$

2.3 一些时序逻辑重言式^[1]

我们用 F 和 G 表示时序逻辑公式，下面是本文将

要用到的一些时序逻辑重言式：

- 1) $\Box F \Rightarrow F$
- 2) $F \Rightarrow \Diamond F$
- 3) $\neg \Box F \Rightarrow \Diamond \neg F$
- 4) $\Box(F \wedge G) \equiv (\Box F) \wedge (\Box G)$
- 5) $\Diamond(F \vee G) \equiv (\Diamond F) \vee (\Diamond G)$
- 6) $(\Box F) \vee (\Box G) \Rightarrow \Box(F \vee G)$
- 7) $\Diamond(F \wedge G) \Rightarrow (\Diamond F) \wedge (\Diamond G)$
- 8) $\Box \Diamond(F \vee G) \equiv (\Box \Diamond F) \vee (\Box \Diamond G)$
- 9) $\Diamond \Box(F \wedge G) \equiv (\Diamond \Box F) \wedge (\Diamond \Box G)$
- 10) $\Box(F \Rightarrow G) \equiv (\Box F) \Rightarrow (\Box G)$
- 11) $\Diamond \Box F \Rightarrow \Box \Diamond F$

3 系统行为的公平性

一般地，行为的公平性可分为弱公平和强公平，下面是它们的语义和语法定义：

3.1 公平性的语义定义

定义15 弱公平性 (justice)^[3]：一次运转 $\sigma = \sigma_0 \xrightarrow{A_0} \sigma_1 \xrightarrow{A_1} \dots$ 对一个行为 A 来说是弱公平的，当且仅当满足以下条件：

如果对任意的 m ，在 σ_m 之后 A 总是使能的，则存在一些 $n \geq m$ ，使得 $A_n = A$ 。

定义16 强公平性 (compassion)^[3]：一次运转 $\sigma = \sigma_0 \xrightarrow{A_0} \sigma_1 \xrightarrow{A_1} \dots$ 对一个行为 A 来说是强公平的，当且仅当满足以下条件：

如果对任意的 m ， σ_m 之后 A 有无限多次使能，则存在一些 $n \geq m$ ，使得 $A_n = A$ 。

3.2 基于 TLA 的公平性语法定义

用 TLA 的语法公式来定义公平性即为：

定义17 弱公平性 $WF_v(A)$ ^[1]：

$$WF_v(A) \triangleq \Box \Diamond \neg ENABLED \langle A \rangle_v \vee \Box \Diamond \langle A \rangle_v$$

定义18 强公平性 $SF_v(A)$ ^[1]：

$$SF_v(A) \triangleq \Diamond \Box \neg ENABLED \langle A \rangle_v \vee \Box \Diamond \langle A \rangle_v$$

4 公平性等级的进一步细分

实际上，除了弱公平和强公平之外，公平性的等级还可以进行细分，本节我们将提出一种进一步细分的方法，并讨论各等级公平性之间的关系。

定义19 $F1$ 公平：一次运转 $\sigma = \sigma_0 \xrightarrow{A_0} \sigma_1 \xrightarrow{A_1} \dots$ 对一个行为 A 来说是 $F1$ 公平的，当且仅当满足以下条件：

在 σ 上 A 总是使能的，则必存在一些 n ，使得 $A_n = A$ 。

即： $F1(A) \triangleq \forall m \in N: \sigma^{+m} \models (Enabled A)$

$$\Rightarrow \exists n \in N: \sigma^{+n} \llbracket A \rrbracket \sigma^{+n+1}$$

改写成 TLA 的语法公式即为:

$$F1_v(A) \triangleq \Diamond \neg \text{ENABLED} \langle A \rangle_v \vee \Diamond \langle A \rangle_v$$

定义20 $F2$ 公平: 一次运转 $\sigma = \sigma_0 \xrightarrow{A_0} \sigma_1 \xrightarrow{A_1} \dots$ 对一个行为 A 来说是 $F2$ 公平的, 当且仅当满足以下条件:

在 σ 上 A 总是使能的, 则对任意 $m \in N$, 必有一些 $n \geq m$, 使得 $A_n = A$.

$$\text{即: } F2(A) \triangleq \forall k \in N: \sigma^{+k} (\text{Enabled } A)$$

$$\Rightarrow \forall m \in N: (\exists n \in N: \sigma^{+m+n} \llbracket A \rrbracket \sigma^{+m+n+1})$$

改写成 TLA 的语法公式即为:

$$F2_v(A) \triangleq \Diamond \neg \text{ENABLED} \langle A \rangle_v \vee \Box \Diamond \langle A \rangle_v$$

定义21 $F3$ 公平: 一次运转 $\sigma = \sigma_0 \xrightarrow{A_0} \sigma_1 \xrightarrow{A_1} \dots$ 对一个行为 A 来说是 $F3$ 公平的, 当且仅当满足以下条件:

在 σ 上存在状态 σ_m 使得 A 在其后总是使能的, 则必有一些 $n \in N$, 使得 $A_n = A$.

$$\text{即: } F3(A) \triangleq \exists m \in N: (\forall k \in N: \sigma^{+m+k} (\text{Enabled } A))$$

$$\Rightarrow \exists n \in N: \sigma^{+m} \llbracket A \rrbracket \sigma^{+m+1}$$

改写成 TLA 的语法公式即为:

$$F3_v(A) \triangleq \Box \Diamond \neg \text{ENABLED} \langle A \rangle_v \vee \Diamond \langle A \rangle_v$$

定义22 $F4$ 公平: 一次运转 $\sigma = \sigma_0 \xrightarrow{A_0} \sigma_1 \xrightarrow{A_1} \dots$ 对一个行为 A 来说是 $F4$ 公平的, 当且仅当满足以下条件:

在 σ 上存在状态 σ_m 使得 A 在其后总是使能的, 则对任意的 $l \in N$, 都有一些 $n \geq l$, 使得 $A_n = A$.

$$\text{即: } F4(A) \triangleq \exists m \in N: (\forall k \in N: \sigma^{+m+k} (\text{Enabled } A))$$

$$\Rightarrow \forall l \in N: (\exists n \in N: \sigma^{+l+n} \llbracket A \rrbracket \sigma^{+l+n+1})$$

改写成 TLA 的语法公式即为:

$$F4_v(A) \triangleq \Box \Diamond \neg \text{ENABLED} \langle A \rangle_v \vee \Box \Diamond \langle A \rangle_v$$

定义23 $F5$ 公平: 一次运转 $\sigma = \sigma_0 \xrightarrow{A_0} \sigma_1 \xrightarrow{A_1} \dots$ 对一个行为 A 来说是 $F5$ 公平的, 当且仅当满足以下条件:

在 σ 上任意的状态 σ_m 之后, 总有一个状态使得 A 使能, 则必有一些 $n \in N$, 使得 $A_n = A$.

$$\text{即: } F5(A) \triangleq \forall m \in N: (\exists k \in N: \sigma^{+m+k} (\text{Enabled } A))$$

$$\Rightarrow \exists n \in N: \sigma^{+n} \llbracket A \rrbracket \sigma^{+n+1}$$

改写成 TLA 的语法公式即为:

$$F5_v(A) \triangleq \Diamond \Box \neg \text{ENABLED} \langle A \rangle_v \vee \Diamond \langle A \rangle_v$$

定义24 $F6$ 公平: 一次运转 $\sigma = \sigma_0 \xrightarrow{A_0} \sigma_1 \xrightarrow{A_1} \dots$ 对一个行为 A 来说是 $F6$ 公平的, 当且仅当满足以下条件:

在 σ 上任意的状态 σ_m 或之后, 总有一个状态使

得 A 使能, 则必有一些 $n \geq m$, 使得 $A_n = A$.

$$\text{即: } F6(A) \triangleq \forall m \in N: (\exists k \in N: \sigma^{+m+k} (\text{Enabled } A))$$

$$\Rightarrow \exists n \in N: \sigma^{+n} \llbracket A \rrbracket \sigma^{+n+1}$$

改写成 TLA 的语法公式即为:

$$F6_v(A) \triangleq \Diamond \Box \neg \text{ENABLED} \langle A \rangle_v \vee \Box \Diamond \langle A \rangle_v$$

定义25 $F7$ 公平: 一次运转 $\sigma = \sigma_0 \xrightarrow{A_0} \sigma_1 \xrightarrow{A_1} \dots$ 对一个行为 A 来说是 $F7$ 公平的, 当且仅当满足以下条件:

在 σ 上存在一个状态 σ_m 使得 A 使能, 则必有一些 $n \in N$, 使得 $A_n = A$.

$$\text{即: } F7(A) \triangleq \exists m \in N: \sigma^{+m} (\text{Enabled } A)$$

$$\Rightarrow \exists n \in N: \sigma^{+n} \llbracket A \rrbracket \sigma^{+n+1}$$

改写成 TLA 的语法公式即为:

$$F7_v(A) \triangleq \Box \neg \text{ENABLED} \langle A \rangle_v \vee \Diamond \langle A \rangle_v$$

定义26 $F8$ 公平: 一次运转 $\sigma = \sigma_0 \xrightarrow{A_0} \sigma_1 \xrightarrow{A_1} \dots$ 对一个行为 A 来说是 $F8$ 公平的, 当且仅当满足以下条件:

在 σ 上存在一状态 σ_m 使得 A 使能, 则任意状态 σ_k 之后必有一些 n , 使得 $A_n = A$.

$$\text{即: } F8(A) \triangleq \exists m \in N: \sigma^{+m} (\text{Enabled } A)$$

$$\Rightarrow \forall k \in N: (\exists n \in N: \sigma^{+k+n} \llbracket A \rrbracket \sigma^{+k+n+1})$$

改写成 TLA 的语法公式即为:

$$F8_v(A) \triangleq \Box \neg \text{ENABLED} \langle A \rangle_v \vee \Box \Diamond \langle A \rangle_v$$

5 细分公平性之间的关系

显然, $F4$ 和 $F6$ 就是前文提到的弱公平和强公平, 且强公平蕴含弱公平^[1], 即 $F6 \Rightarrow F4$ 。进一步考察各公平性之间的关系, 我们有以下命题:

命题1 $F8(A) \Rightarrow F6(A) \Rightarrow F4(A) \Rightarrow F2(A)$ 。

证明: 选证 $F4(A) \Rightarrow F2(A)$

$$F4(A) \triangleq \exists m \in N: (\forall k \in N: \sigma^{+m+k} (\text{Enabled } A))$$

$$\Rightarrow \forall l \in N: (\exists n \in N: \sigma^{+l+n} \llbracket A \rrbracket \sigma^{+l+n+1})$$

$$\equiv \exists m \in N: (\sigma^{+m} \models \Box \neg \text{ENABLED} \langle A \rangle_v)$$

$$\Rightarrow \forall l \in N: (\sigma^{+l} \models \Diamond \langle A \rangle_v)$$

$$\equiv (\forall m \in N: \sigma^{+m} \models \Box \neg \text{ENABLED} \langle A \rangle_v)$$

$$\Rightarrow (\forall l \in N: \sigma^{+l} \models \Diamond \langle A \rangle_v)$$

$$\equiv \Diamond \Box \neg \text{ENABLED} \langle A \rangle_v \Rightarrow \Box \Diamond \langle A \rangle_v$$

$$\equiv \Box \Diamond \neg \text{ENABLED} \langle A \rangle_v \vee \Box \Diamond \langle A \rangle_v$$

$$\Rightarrow \Diamond \neg \text{ENABLED} \langle A \rangle_v \vee \Box \Diamond \langle A \rangle_v$$

$$\equiv \forall k \in N: \sigma^{+k} (\text{Enabled } A)$$

$$\Rightarrow \forall m \in N: (\exists n \in N: \sigma^{+m+n} \llbracket A \rrbracket \sigma^{+m+n+1})$$

$$\equiv F2(A)$$

命题 2 $F7(A) \Rightarrow F5(A) \Rightarrow F3(A) \Rightarrow F1(A)$ 。

证明：选证 $F7(A) \Rightarrow F5(A)$ ：

$$\begin{aligned}
 & F7(A) \\
 & \equiv \exists m \in N : \sigma^{+m} (Enabled\ A) \\
 & \Rightarrow \exists n \in N : \sigma^{+n} \llbracket A \rrbracket \sigma^{+n+1} \\
 & \equiv \Diamond ENABLED \langle A \rangle_v \Rightarrow \Diamond \langle A \rangle_v \\
 & \equiv \Box \neg ENABLED \langle A \rangle_v \vee \Diamond \langle A \rangle_v \\
 & \Rightarrow \Box \Diamond \neg ENABLED \langle A \rangle_v \vee \Diamond \langle A \rangle_v \\
 & \equiv \forall m \in N : (\exists k \in N : \sigma^{+m+k} (Enabled\ A)) \\
 & \Rightarrow \exists n \in N : \sigma^{+n} \llbracket A \rrbracket \sigma^{+n+1} \\
 & \equiv F5(A)
 \end{aligned}$$

命题 3 $F8(A) \Rightarrow F7(A), F6(A) \Rightarrow F5(A),$

$F4(A) \Rightarrow F3(A), F2(A) \Rightarrow F1(A)$

证明：选证 $F6(A) \Rightarrow F5(A)$ ：

$$\begin{aligned}
 & F6(A) \\
 & \equiv \forall m \in N : (\exists k \in N : \sigma^{+m+k} (Enabled\ A)) \\
 & \Rightarrow \exists n \in N : \sigma^{+n} \llbracket A \rrbracket \sigma^{+n+1} \\
 & \equiv \forall m \in N : \sigma^{+m} \models \Diamond ENABLED \langle A \rangle_v \Rightarrow \Diamond \langle A \rangle_v \\
 & \equiv \Box \Diamond ENABLED \langle A \rangle_v \Rightarrow \Diamond \langle A \rangle_v \\
 & \equiv \Diamond \Box ENABLED \langle A \rangle_v \Rightarrow \Diamond \langle A \rangle_v \\
 & \Rightarrow \Box \Diamond \neg ENABLED \langle A \rangle_v \vee \Diamond \langle A \rangle_v \\
 & \equiv \forall m \in N : (\exists k \in N : \sigma^{+m+k} (Enabled\ A)) \\
 & \Rightarrow \exists n \in N : \sigma^{+n} \llbracket A \rrbracket \sigma^{+n+1} \\
 & \equiv F5(A)
 \end{aligned}$$

另外，命题 1-3 的逆命题是不成立的，即三个命题中的蕴含关系都是真蕴含，不可能是等价关系。我们选取 $F4 \not\Rightarrow F6$ ，即弱公平不蕴含强公平来进行证明。其它逆命题不成立的证明是类似的。

命题 4 $F4 \not\Rightarrow F6$

证明：我们只需找到是弱公平但不是强公平的例子即可。

【例 1】一个变迁系统的状态转移图如图 1 所示：

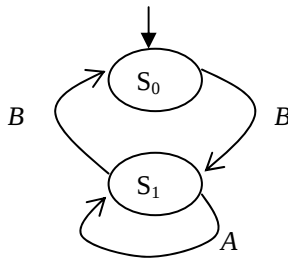


图 1

如果对一次运转 $\sigma = \sigma_0 \xrightarrow{A_0} \sigma_1 \xrightarrow{A_1} \dots$ ，取 $\sigma_0 = S_0, \sigma_1 = S_1, \sigma_2 = S_0, \sigma_3 = S_0, \dots$; $A_i = B$ ，即： $\sigma = S_0 \xrightarrow{B} S_1 \xrightarrow{B} S_0 \xrightarrow{B} S_1 \xrightarrow{B} S_0 \xrightarrow{B} \dots$ (S_0 和 S_1 是交替出现)。

由图 1 可知：行为 A 在运转 σ 上的状态 S_1 处是使能的，但在 S_0 处是不使能的，即 A 不是在 σ 上所有状态都使能。根据 $F4$ 的定义，尽管 A 在 σ 上没有发生，由于不存在一个 m 使得 A 在 σ_m 之后总是使能的，所以 σ 对 A 仍是弱公平的。然而，在 σ 上 S_0 和 S_1 是交替出现的，即 A 在 σ 上是无限多次使能的，但 A 没有发生，由 $F6$ 的定义， σ 对 A 不是强公平的。证毕■

6 结束语

行为的公平性通常以公平条件的形式出现在变迁系统中，并且几乎所有的公平条件都可以表示为行为的公平性^[2]。行为公平性的主要目的就是要保证行为在足够多次使能的情况下能够足够多次发生。公平性是对系统活性的表示方法，因此行为公平性的正确描述和表达至关重要，它直接影响基于 TLA 的描述与验证的效率，对公平性的深入分析和进一步细分将有助于我们对公平性的理解和应用。

致谢

感谢美国 GeneChiu 基金会的资金支持；感谢唐郑熠、吴勇、汪贻望以及所有支持帮助过本文工作的人们。

References (参考文献)

- [1] Leslie Lamport. *Specifying Systems* [M]. Addison-Wesley Longman Publishing Co., Inc. 2002.
- [2] Wolfgang Schreiner. *The TLA Logic of Action I*. <http://www.risc.uni-linz.ac.at/people/sch-reine>.
- [3] Leslie Lamport. *The Temporal Logic of Actions* [M]. ACM Transactions on Programming Languages and Systems. 1994.5, 16(3):872-923.
- [4] Nissim Francez. *Fairness* [M]. Texts and Monographs in Computer Science. Springer-Verlag, New York, Berlin, Heidelberg, Tokyo, 1986.
- [5] Stephan Eerz. *Modeling and Developing Systems Using TLA+* [M]. Escuela de Verano, 2005. Vol.73, Iss.3 (June 1987), pp207-244.