§4 推理验证

§4.1 一阶迁移系统的推理

例子: 互斥协议

T	$a = s_0$	$\longrightarrow$	$(y, t, a) := (1, 1, s_1)$
	$a = s_1 \wedge (x = 0 \vee t = 0)$	$\longrightarrow$	$(a) := (s_2)$
	$a = s_2$	$\longrightarrow$	$(y, a) := (0, s_3)$
	$a = s_3$	$\longrightarrow$	$(y, t, a) := (1, 1, s_1)$
	$b = t_0$	$\longrightarrow$	$(x, t, b) := (1, 0, t_1)$
	$b = t_1 \wedge (y = 0 \vee t = 1)$	$\longrightarrow$	$(b) := (t_2)$
	$b = t_2$	$\longrightarrow$	$(x, b) := (0, t_3)$
	$b = t_3$	$\longrightarrow$	$(x, t, b) := (1, 0, t_1)$
Θ	$(a = s_0 \wedge b = t_0 \wedge x = 0 \wedge y = 0 \wedge t = 0)$		

安全性质: 互斥协议满足以下性质:

$$(T, \Theta) \models_I \Box(a = s_1 \wedge b \neq t_1 \wedge b \neq t_2 \rightarrow a = s_2 R b \neq t_2)$$

主要适用规则

主要适用规则如下

$$\frac{\begin{array}{l}\zeta \Rightarrow \varphi' \\ \{\varphi' \wedge \neg\psi\} T \{\varphi'\} \\ \varphi' \Rightarrow \varphi\end{array}}{\zeta \Rightarrow \psi R \varphi}$$

尝试 1

令

$$\begin{array}{lcl}\zeta & \equiv & (a = s_1 \wedge b \neq t_1 \wedge b \neq t_2) \\ \psi & \equiv & (a = s_2) \\ \varphi & \equiv & (b \neq t_2) \\ \varphi' & \equiv & \varphi\end{array}$$

需要 $\zeta \Rightarrow \varphi$ 和 $\forall t \in T, \{\varphi' \wedge \neg\psi\} t \{\varphi'\}$ 。

试证:
$\{\varphi' \wedge \neg\psi\} t_6 \{\varphi'\}$ 。
需要

$$(b \neq t_2) \wedge (a \neq s_2) \wedge b = t_1 \wedge (y = 0 \vee t = 1) \rightarrow (t_2 \neq t_2)$$

证明失败。

尝试 2

令

$$\begin{aligned}\zeta &\equiv (a = s_1 \wedge b \neq t_1 \wedge b \neq t_2)\\ \psi &\equiv (a = s_2)\\ \varphi &\equiv (b \neq t_2)\\ \varphi' &\equiv (a = s_1 \wedge (b = t_0 \vee b = t_3 \vee (b = t_1 \wedge x = 1 \wedge t = 0))) \vee (a = s_2 \wedge b \neq t_2)\end{aligned}$$

试证：

$\{\varphi' \wedge \neg\psi\}t_6\{\varphi'\}$ 。

需要

$$\begin{aligned}&((a = s_1 \wedge (b = t_0 \vee b = t_3 \vee (b = t_1 \wedge x = 1 \wedge t = 0))) \vee (a = s_2 \wedge b \neq t_2))\wedge\\ &(b \neq t_2) \wedge (a \neq s_2) \wedge b = t_1 \wedge (y = 0 \vee t = 1)\\ &\rightarrow (a = s_1 \wedge (t_2 = t_0 \vee t_2 = t_3 \vee (t_2 = t_1 \wedge x = 1 \wedge t = 0))) \vee (a = s_2 \wedge t_2 \neq t_2)\end{aligned}$$

$$\begin{aligned}&((a = s_1 \wedge (b = t_0 \vee b = t_3 \vee (b = t_1 \wedge x = 1 \wedge t = 0)))\wedge\\ &(b \neq t_2) \wedge (a \neq s_2) \wedge b = t_1 \wedge (y = 0 \vee t = 1)\\ &\rightarrow (a = s_1 \wedge (t_2 = t_0 \vee t_2 = t_3 \vee (t_2 = t_1 \wedge x = 1 \wedge t = 0))) \vee (a = s_2 \wedge t_2 \neq t_2)\end{aligned}$$

$$\begin{aligned}&((a = s_1 \wedge ((b = t_1 \wedge x = 1 \wedge t = 0))) \wedge (y = 0)\\ &\rightarrow (a = s_1 \wedge (t_2 = t_0 \vee t_2 = t_3 \vee (t_2 = t_1 \wedge x = 1 \wedge t = 0))) \vee (a = s_2 \wedge t_2 \neq t_2)\end{aligned}$$

证明失败。

尝试 3

令

$$\begin{aligned}\zeta &\equiv (a = s_1 \wedge b \neq t_1 \wedge b \neq t_2)\\ \psi &\equiv (a = s_2)\\ \varphi &\equiv (b \neq t_2)\\ \varphi' &\equiv (a = s_1 \wedge (b = t_0 \vee b = t_3 \vee (b = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1))) \vee (a = s_2 \wedge b \neq t_2)\end{aligned}$$

试证：

$\{\varphi' \wedge \neg\psi\}t_6\{\varphi'\}$ 。

需要

$$\begin{aligned}&((a = s_1 \wedge (b = t_0 \vee b = t_3 \vee (b = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1))) \vee (a = s_2 \wedge b \neq t_2))\wedge\\ &(b \neq t_2) \wedge (a \neq s_2) \wedge b = t_1 \wedge (y = 0 \vee t = 1)\\ &\rightarrow (a = s_1 \wedge (t_2 = t_0 \vee t_2 = t_3 \vee (t_2 = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1))) \vee (a = s_2 \wedge t_2 \neq t_2)\end{aligned}$$

$$\begin{aligned}&((a = s_1 \wedge (b = t_0 \vee b = t_3 \vee (b = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1)))\wedge\\ &(b \neq t_2) \wedge (a \neq s_2) \wedge b = t_1 \wedge (y = 0 \vee t = 1)\\ &\rightarrow (a = s_1 \wedge (t_2 = t_0 \vee t_2 = t_3 \vee (t_2 = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1))) \vee (a = s_2 \wedge t_2 \neq t_2)\end{aligned}$$

因此 $a = s_1 \wedge b \neq t_1 \wedge b \neq t_2 \Rightarrow a = s_2 Rb \neq t_2$ ，

即 $\Box(a = s_1 \wedge b \neq t_1 \wedge b \neq t_2 \rightarrow a = s_2 Rb \neq t_2)$ 。

分两种情况来证明，分析的时候可能方便些。

我们有 $\zeta \rightarrow \zeta_1 \vee \zeta_2$ ，

其中 $\zeta_1 = (a = s_1 \wedge b = t_0)$, $\zeta_2 = (a = s_1 \wedge b = t_3)$,

令

$$\varphi_1 \equiv (a = s_1 \wedge (b = t_0 \vee (b = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1))) \vee (a = s_2 \wedge b \neq t_2)$$

则 $\zeta_1 \Rightarrow \psi R \varphi_1$ 。
因此 $\zeta_1 \Rightarrow a = s_2 R b \neq t_2$ 。

同理 $\zeta_2 \Rightarrow a = s_2 R b \neq t_2$ 。
因此 $\zeta \Rightarrow a = s_2 R b \neq t_2$ 。

$\cdots$

活性性质: 互斥协议满足以下性质:

$$(T, \Theta) \models_I \Box(a = s_1 \rightarrow \Diamond a = s_2)$$

主要适用规则

主要适用规则如下

$$\frac{\begin{array}{l}\varphi \Rightarrow (\psi \vee \zeta) \\ \zeta \Rightarrow (w_x^e \wedge (\psi \vee COND_T)) \\ \{\zeta \wedge e = v\} T \{\psi \vee (\zeta \wedge e \sqsubset v)\}\end{array}}{\varphi \Rightarrow \Diamond \psi}$$

尝试 1

选择 f 满足

$$\begin{array}{llll} I(f(t_0,0)) = 1 & I(f(t_1,0)) = 0 & I(f(t_2,0)) = 2 & I(f(t_3,0)) = 1 \\ I(f(t_0,1)) = 1 & I(f(t_1,1)) = 3 & I(f(t_2,1)) = 2 & I(f(t_3,1)) = 1 \end{array}$$

令

$$\begin{array}{rcl} W & = & (\{0,1,2,3\}, \leq) \\ w & = & (0 \leq x \leq 3) \\ e & = & f(b,t) \\ \varphi & = & (a = s_1) \\ \psi & = & (a = s_2) \\ \zeta & = & (a = s_1) \end{array}$$

需要

$$\begin{array}{l} \varphi \Rightarrow (\psi \vee \zeta) \\ \zeta \Rightarrow w_x^e \wedge (\psi \vee V_{t \in T} COND_t) \\ \forall t \in T, \{\zeta \wedge e = v\} t \{\psi \vee (\zeta \wedge e < v)\} \end{array}$$

试证:
$\{\zeta \wedge e = v\} t_6 \{\psi \vee (\zeta \wedge e < v)\}$ 。
需要

$$\begin{array}{l} ((a = s_1 \wedge f(b,t) = v) \wedge b = t_1 \wedge (y = 0 \vee t = 1)) \\ \rightarrow (a = s_2 \vee (a = s_1 \wedge f(t_2,t) < v)) \end{array}$$

$$\begin{array}{l} ((a = s_1 \wedge f(t_1,t) = v) \wedge b = t_1 \wedge (y = 0 \vee t = 1)) \\ \rightarrow (a = s_2 \vee (a = s_1 \wedge f(t_2,t) < v)) \end{array}$$

令

$$\begin{array}{rcl} W & = & (\{0,1,2,3\}, \leq) \\ w & = & (0 \leq x \leq 3) \\ e & = & f(b,t) \\ \varphi & = & (a = s_1) \\ \psi & = & (a = s_2) \\ \zeta & = & (a = s_1 \wedge y = 1) \end{array}$$

因此 $\varphi \Rightarrow \Diamond \psi$ 。