LINEAR TIME BEH & PROPERTIES

A **PATH FRAGMENT of TS** is a path of its state graph:

$\pi \in S^* \cup S^\omega$ s.t. $\forall\, 0 \le i < |\pi| : \pi[i+1] \in Post(\pi[i])$

π maximal if $\pi \in S^*$ & $Post(last(\pi)) = \emptyset$ or $\pi \in S^\omega$

π initial if $\pi[0] \in I$

π path if initial & maximal

$\bigcup \{ trace(\pi) \mid \pi \text{ path}(TS) : \pi(s) \in I \}$

TRACE of π $\{L(\pi[i])\}_{0 \le i < |\pi|}$

$$Traces(TS) := \bigcup_{s \in I} traces(s)$$

An **LT property** (on AP) is an element P of $2^{(2^{AP})^\omega}$ i.e. $P \subseteq (2^{AP})^\omega$

Examples

P_{light}: "the traffic light is infinitely often red"

$\ni \{red\}\{red, yellow\}\{green\}\{red\}\{red, yellow\}\{green\}\ldots$

$\not\ni \{red\}\{\}\{green\}\{\}\{\}\{\}\ldots$

$\ni \{red\}^\omega$

$\ni X^\omega$ if $red \in X \subseteq AP$

$P_{mutex}(n) = \{ \{A_i\}_{i \ge 0} \in (2^{AP})^\omega \mid \forall i \ge 0\ \forall 1 \le h \le k \le n : \{c_h, c_k\} \subseteq A_i \Rightarrow h = k \}$

$= \forall i \ge 0 \bigwedge_{1 \le h \ne k \le n} \{c_h, c_k\} \not\subseteq A_i$

(thread h is in the critical section)

Exercise: What $P'(n) = \{ \{A_i\}_{i \ge 0} \in (2^{AP})^\omega \mid \forall i \ge 0\ \exists 1 \le h \le n.\ A_i = \{h\} \}$ states? Give two different traces satisfying $P'(n)$

Exercise: Let P_{slot}: "always price $= 0 \rightarrow$ eventually $\bigvee_{i=1}^{10}$ price $= i$". Give an example of an element of P_{slot} and one of $(2^{AP})^\omega \setminus P_{slot}$

$$\begin{array}{ccccccccccc} TS & & \omega & & I & & s_i \xrightarrow{\alpha_i} s_{i+1} & & & & \\ \pi & = & s_0 & \alpha_1 & s_2 & \cdots & \alpha_n & s_n & \alpha_{n+1} & \cdots & \\ & & \downarrow & & \downarrow & & & \downarrow & & & \\ & & L(s_0) & & L(s_2) & \cdots & & L(s_n) & \cdots & \in & P \text{ LT property} \end{array}$$

$$TS \models P$$

The importance of Traces

WLOG: no terminal states in TS (hence all maximal paths are infinite)

the trace of a maximal path of TS is $trace(\pi) = L(\pi[i])_{i \geq 0}$

Notice that $trace(\pi) \in (2^{AP})^\omega$

$$TS \models P \iff Traces(TS) \subseteq P$$

$s \in S$, $s \models P$ $\Leftrightarrow$ $traces(s) \subseteq P$

Read $Traces(TS) \subseteq Traces(TS')$ as "TS correctly implements TS'"

refinement — abstract model

Thm TS & TS' t.s. on the same atomic propositions then

$Traces(TS) \subseteq Traces(TS') \iff \forall$ LT prop. P $TS' \models P \Rightarrow TS \models P$

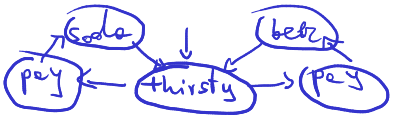
Proof ($\Rightarrow$) $TS' \models P \overset{def}{\iff} Traces(TS') \subseteq P$

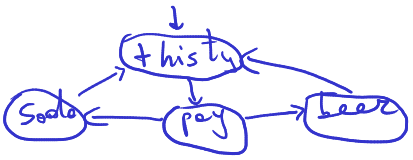
$\overset{hyp}{\Longrightarrow} Traces(TS) \subseteq P \overset{def}{\iff} TS \models P$

($\Leftarrow$) $TS' \models Traces(TS')$ since $Traces(TS') \subseteq Traces(TS')$

$\overset{hyp}{\Longrightarrow} TS \models Traces(TS') \overset{def}{\iff} Traces(TS) \subseteq Traces(TS')$ □

Cor $Traces(TS) = Traces(TS') \iff \forall P$ LT f.b : $TS \models P \iff TS' \models P$

Exercise: is 

equivalent to 

?

A Taxonomy of LT properties:

Invariant ⊂ Safety ⊂ Liveness

"nothing bad ever happens"

"something good eventually happens"

an LT property P_{inv} s.t. $\exists$ ϕ prop. f.b : $\forall i \geq 0 \; P_{inv}[i] \models \phi$

Note

$TS \models P_{inv} \iff Traces(TS) \subseteq P_{inv}$

$\iff trace(\pi) \in P_{inv} \; \forall \pi$ path of $G(TS)$

$\Rightarrow L(s) \models \phi \; \forall s$ on a path of $G(TS)$

$\Rightarrow \boxed{L(s) \models \phi \; \forall s \in Reach(TS)}$

all reachable state of TS satisfy ϕ

Exercise Show that P_{mutex} is an invariant $\phi = \neg crit_1 \vee \neg crit_2$

Safety

In general safety properties impose conditions on finite path fragments of executions e.g.

"before withdrawing money, a correct PIN is entered" (*)

Intuition: an infinite execution violating (*) has a finite prefix violating it

"bad Prefix"

Safety P_{safe} $\forall \sigma \in (2^{AP})^\omega \setminus P_{safe}$ $\exists n \geq 0 : \sigma[0,n]\,(2^{AP})^\omega \cap P_{safe} = \emptyset$

$BadPref(P) = \{\sigma \in (2^{AP})^* \mid \exists \sigma' \in (2^{AP})^\omega \setminus P : \sigma \in pref(\sigma') \wedge \sigma(2^{AP})^\omega \cap P = \emptyset\}$

Lemma $TS \models P_{safe} \iff Traces_{fin}(TS) \cap BadPref(P_{safe}) = \emptyset$

Proof ($\Rightarrow$) If $\hat{\sigma} \in Traces_{fin}(TS) \cap BadPref(P_{safe})$

$\Rightarrow \exists \sigma \in Traces(TS), n \geq 0 : \hat{\sigma} = \sigma[0,n]$

$\Rightarrow \sigma \notin P_{safe}$

$\Rightarrow TS \models P_{safe} \Rightarrow \bot$

($\Leftarrow$) If $TS \not\models P_{safe} \overset{def}{\iff} \exists \sigma \in Traces(TS) : \sigma \notin P_{safe}$

$\Rightarrow \exists n \geq 0 : \sigma[0,n] \in BadPref(P_{safe})$

$\Rightarrow \sigma[0,n] \in Traces_{fin}(TS) \cap BadPref(P_{safe}) \Rightarrow \bot$

□

weaker than full trace ⊆ ⇒ good to show that refinement on

thm $Traces_{fin}(TS) \subseteq Traces_{fin}(TS') \iff$

$\forall$ safety properties P $\quad TS' \models P \Rightarrow TS \models P$

Proof ($\Rightarrow$) P is a safety prop $\overset{L}{\Rightarrow} Traces_{fin}(TS') \cap BadPref(P) = \emptyset$

$\overset{hyp}{\Rightarrow} Traces_{fin}(TS) \cap BadPref(P) = \emptyset \overset{L}{\iff}$ ✓

($\Leftarrow$) Take $P = closure(Traces(TS'))$

P is a safety property and $TS' \models P$

$\overset{hyp}{\Rightarrow} Traces(TS) \subseteq P$

$\Rightarrow Traces_{fin}(TS) = pref(Traces(TS))$

$\subseteq pref(P) = pref(Traces(TS')) = Traces_{fin}(TS')$

Exercise: show that $P_{safety} \iff P = closure(P)$ where $closure(P) = \{\sigma \in (2^{AP})^\omega \mid pref(\sigma) \subseteq pref(P)\}$

□