A Taxonomy of LT properties

Invariant $\subset$ Safety "nothing bad ever happens" Liveness "something good eventually happens"

An LT property P_{inv} is an invariant if there is a propositional formula φ s.t. for all $\sigma \in P_{inv}$ and all $i \geq 0$, $\sigma[i] \models \varphi$

Given that

$$
\begin{aligned}
TS \models P_{inv} &\iff Traces(TS) \subseteq P_{inv} \\
&\iff trace(\pi) \in P_{inv} \quad \forall \pi \text{ path of } G(TS) \\
&\Rightarrow L(s) \models \phi \quad \forall s \text{ on a path of } G(TS) \\
&\Rightarrow \boxed{L(s) \models \phi \quad \forall s \in Reach(TS)}
\end{aligned}
$$

all reachable state of TS satisfy ϕ

we can conclude that an invariant is a "state-property"; in fact, invariant properties can be linearly checked on transition systems whose state graph is finite.

Exercise Show that P_{mutex} is an invariant

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

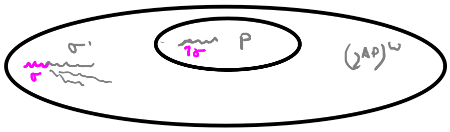
for $\sigma = \sigma_0 \ldots \sigma_n \sigma_{n+1} \ldots$ $\quad \sigma_{<n} = \sigma_0 \ldots \sigma_n$; $\sigma_{<0} = \varepsilon$

$pref(\sigma) = \bigcup_{n \in \omega} \sigma_{<n}$

"bad Prefix"

Safety P_{safe} $\quad \forall \sigma \in (2^{AP})^\omega \setminus P_{safe} \;\; \exists n \geq 0 : \sigma_{<n} (2^{AP})^\omega \cap P_{safe} = \emptyset$

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



set of finite path fragments on $G(TS)$

$Traces_{fin}(TS) := \bigcup_{s \in S} Traces_{fin}(s)$; $Traces_{fin}(s) := trace(Path_{fin}(s))$

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

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

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

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

$\Rightarrow TS \not\models P_{safe}$.

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

$\Rightarrow \exists n \geq 0 : \sigma_{<n} \in BadPref(P_{safe})$

$\Rightarrow \sigma_{<n} \in Traces_{fin}(TS) \cap BadPref(P_{safe})$ $\square$

weaker than full trace inclusion $\Rightarrow$ good to show that refinement is ok

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

$\forall$ 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 $TS' \models P$

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

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

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

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

Safety "constraints" finite behaviour while liveness imposes conditions on infinite behaviour

Liveness P_{live} $\forall w \in (2^{AP})^* \; \exists \sigma \in (2^{AP})^\omega : w\sigma \in P_{live}$

"something good happens"

$$\Updownarrow$$

$$pref(P_{live}) = (2^{AP})^*$$

Exercise Give the properties informally specified as

1. "each process eventually enters the critical section"
2. "each process enters the critical section infinitely often"
3. "each waiting process eventually enters the critical section"

there are LT prop that are neither safety nor liveness prop., but:

Decomposition theorem $\forall$ LT prop P $\exists P_s$ safety, P_ℓ liveness : $P = P_s \cap P_\ell$