15/15+2

Cyber Physical Systems - Discrete Models
Exercise Sheet 7 Solution

Alper Ari
aa508@uni-freiburg.edu

Onur Sahin
os141@uni-freiburg.de

December 5, 2023

5/7

Exercise 1: Linear-Time Properties

for (ii) and (iii), you were supposed to give any trace. Not only those in the set of traces of the TS.

1. Property P_1 :
   - i $\{A_0 A_1 A_2 ... | \forall i \in \mathbb{N} \cdot a \in A_i \lor b \in A_i\}$
   - ii $\{a\}(\{a\}\{a,b\})^\omega$
   - iii $\{a\}\emptyset(\{a\}\{a,b\})^\omega$
   - iv $T \nvDash P_1$ because not all of the traces satisfy P_1 (example above).
2. Property P_2 :
   - i $\{A_0 A_1 A_2 ... | \forall i \in \mathbb{N} \cdot a \in A_i \land b \in A_i\}$
   - ii – $\{a,b\}^\omega$ −0.25
   - iii $\{a\}\emptyset(\{a\}\{a,b\})^\omega$
   - iv $T \nvDash P_2$ because none of the traces satisfy P_2 (example above).
3. Property P_3 :

   only one dot per quantifier!
   - i $\{A_0 A_1 A_2 ... | \forall i \in \mathbb{N} \cdot (b \in A_i \longrightarrow \exists j \in \mathbb{N} \cdot j \leq i \land a \in A_j)\}$
   - ii $\{a\}(\{a\}\{a,b\})^\omega$
   - iii – $\{b\}\emptyset^\omega$ −0.25
   - iv $T \vDash P_3$ because all traces satisfy P_3.
4. Property P_4 :
   - i $\{A_0 A_1 A_2 ... | \forall i \in \mathbb{N} \cdot (a \in A_i \longrightarrow \exists j \in \mathbb{N} \cdot j \geq i \cdot b \in A_j)\}$
   - ii $\{a\}(\{a\}\{a,b\})^\omega$
   - iii – $\{a\}\emptyset^\omega$ −0.25
   - iv $T \vDash P_4$ because all traces satisfy P_4.
5. Property P_5 :

   $\land j \neq i \land i \neq k \land k \neq j$ −0.25
   - i $\{A_0 A_1 A_2 ... | \exists i,j,k \in \mathbb{N} \cdot (a \in A_i \land a \in A_j \land a \in A_k) \land (\forall z \in \mathbb{N}/\{i,j,k\}) \cancel{\land (i \neq j \neq k)} \cdot a \notin A_z\}$
   - ii – $\{a\}\{a\}\{a\}\emptyset^\omega$ −0.25
   - iii $\{a\}\emptyset(\{a\}\{a,b\})^\omega$
   - iv $T \nvDash P_5$ because no traces satisfy P_5.
6. Property P_6 :
   - i $\{A_0 A_1 A_2 ... | \exists^\infty i \in \mathbb{N} \cdot a \in A_i \Longrightarrow \exists^\infty j \in \mathbb{N} \cdot b \in A_j\}$
   - ii $\{a\}(\{a\}\{a,b\})^\omega$

iii – $\{a\}^\omega$ – 0.25

iv $T \vDash P_6$ because all traces satisfy P_6. ✓

7. Property P_7 :

i $\{A_0A_1A_2 ... | \exists i \in \mathbb{N} \cdot \forall j \in \mathbb{N} \cdot j \geq i \cdot a \notin A_j\}$ ✓

ii – $\emptyset^\omega$ – 0.25

iii $\{a\}\emptyset(\{a\}\{a,b\})^\omega$ ✓

iv $T \nvDash P_7$ because no traces satisfy P_7. ✓

4/4

Exercise 2: Complement of LT-Properties

(a) **If $\tau \models \neg E$ holds, it follows that $\tau \not\models E$ holds:**
True. Proof by contradiction. Assume $\tau \models \neg E \wedge \tau \models E$.
Then it follows that $\tau \in \neg E \wedge \tau \in E$.
Since the fact that $E \cap \neg E = \emptyset$, the assumption contradicts.
Therefore, if $\tau \models \neg E$ holds, it follows that $\tau \not\models E$ holds.

(b) **If $\tau \not\models \neg E$ holds, it follows that $\tau \models E$ holds:**
True. Proof by contradiction. Assume $\tau \not\models E \wedge \tau \not\models \neg E$.
Then $\tau \notin E \wedge \tau \notin \neg E$.
This leads to $\tau \notin (E \cup \neg E)$ which actually means $\tau \notin (2^{AP})^\omega$ which is a contradiction.
Therefore, if $\tau \not\models \neg E$ holds, it follows that $\tau \models E$ holds.

(c) **If $T \models \neg E$ holds, it follows that $T \not\models E$ holds:**
False. A counter example would be $T = \emptyset$ which is a transition system without any traces.
In this case the system has no trace which violates both E and $\neg E$.
So, the given statement is false.

(d) **If $T \not\models \neg E$ holds, it follows that $T \models E$ holds:**
False. A counter example would be T with traces $\{a^\omega, b^\omega\}$ and property E = "always b".
Here, $T \not\models \neg E$ is false because one of the traces already satisfies E.
And, $T \models E$ is also false because one of the traces already doesn't satisfy E.
So, the given statement is false.

4/4

Exercise 3: Invariant checking I

Start: $U = \{ \}$

$\pi = \{ \}$

call 1: $s = s_0$

$\pi = \{\} \longrightarrow \pi = \{s_0\}$

$U = \{\} \longrightarrow U = \{s_0\}$

$s \models \Phi$

call 2: $s' = s_3$

$\pi = \{s_0\} \longrightarrow \pi = \{s_0, s_3\}$

$U = \{s_0\} \longrightarrow U = \{s_0, s_3\}$

$s \models \Phi$

call 3: $s' = s_2$

$\pi = \{s_0, s_3\} \longrightarrow \pi = \{s_0, s_3, s_2\}$

$U = \{s_0, s_3\} \longrightarrow U = \{s_0, s_3, s_2\}$

$s' \models \Phi$

call 4 $s' = s_0$

$\pi = \{s_0, s_3, s_2\} \longrightarrow \pi = \{s_0, s_3, s_2, s_0\}$

$U = \{s_0, s_3, s_2\}$

pop

$\pi = \{s_0, s_3, s_2, s_0\} \longrightarrow \pi = \{s_0, s_3, s_2\}$

return false

pop

$\pi = \{s_0, s_3, s_2\} \longrightarrow \{s_0, s_3\}$

return false

call 5: $s' = s_3$

$\pi = \{s_0, s_3\} \longrightarrow \pi = \{s_0, s_3, s_3\}$

$U = \{s_0, s_3, s_2\}$

pop

$\pi = \{s_0, s_3, s_3\} \longrightarrow \pi = \{s_0, s_3\}$

return false

pop

$\pi = \{s_0, s_3\} \longrightarrow \pi = \{s_0\}$

return false

pop

$\pi = \{s_0\} \longrightarrow \pi = \{ \}$

return false

call 6: $s = s_1$

$\pi = \{\} \longrightarrow \pi = \{s_1\}$

$U = \{s_0, s_3, s_2\} \longrightarrow \{s_0, s_3, s_2, s_1\}$

$s \models \Phi$

call 7: $s' = s_3$

$\pi = \{s_1\} \longrightarrow \pi = \{s_1, s_3\}$

$U = \{s_0, s_3, s_2, s_1\}$

pop

$\pi = \{s_1, s_3\} \longrightarrow \pi = \{s_1\}$

return false

call 8: $s' = s_4$

$\pi = \{s_1\} \longrightarrow \pi = \{s_1, s_4\}$

$U = \{s_0, s_3, s_2, s_1\} \longrightarrow U = \{s_0, s_3, s_2, s_1, s_4\}$

$s \not\models \Phi$

return true

return true

return no, $\pi = \{s_1, s_4\}$

end

2/2

Exercise 4: Invariant checking II

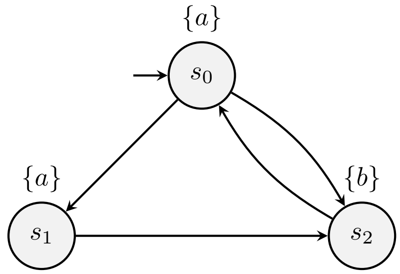

Figure 1: Transition system with 3 states

this is minimal too, if you take away state s_2, it would not be a counter example anymore.

$$\phi = a$$

~~no~~n-minimal $= \{s_0, s_1, s_2\}$

minimal $= \{s_0, s_2\}$

and of minimal length