

Cyber Physical Systems - Discrete Models

Exercise Sheet 7 Solution

Alper Ari
aa508@uni-freiburg.edu

Onur Sahin
os141@uni-freiburg.de

December 5, 2023

Exercise 1: Linear-Time Properties

1. Property P_1 :

- i $\{A_0A_1A_2...\mid \forall i \in \mathbb{N} \cdot a \in A_i \vee b \in A_i\}$
- ii $\{a\}(\{a\}\{a,b\})^\omega$
- iii $\{a\}\emptyset(\{a\}\{a,b\})^\omega$
- iv $T \not\models P_1$ because not all of the traces satisfy P_1 (example above).

2. Property P_2 :

- i $\{A_0A_1A_2...\mid \forall i \in \mathbb{N} \cdot a \in A_i \wedge b \in A_i\}$
- ii —
- iii $\{a\}\emptyset(\{a\}\{a,b\})^\omega$
- iv $T \not\models P_2$ because none of the traces satisfy P_2 (example above).

3. Property P_3 :

- i $\{A_0A_1A_2...\mid \forall i \in \mathbb{N} \cdot b \in A_i \longrightarrow \exists j \in \mathbb{N} \cdot j < i \cdot a \in A_j\}$
- ii $\{a\}(\{a\}\{a,b\})^\omega$
- iii —
- iv $T \models P_3$ because all traces satisfy P_3 .

4. Property P_4 :

- i $\{A_0A_1A_2...\mid \forall i \in \mathbb{N} \cdot (a \in A_i \longrightarrow \exists j \in \mathbb{N} \cdot j \geq i \cdot b \in A_j)\}$
- ii $\{a\}(\{a\}\{a,b\})^\omega$
- iii —
- iv $T \models P_4$ because all traces satisfy P_4 .

5. Property P_5 :

- i $\{A_0A_1A_2...\mid \exists i, j, k \in \mathbb{N} \cdot (a \in A_i \wedge a \in A_j \wedge a \in A_k) \wedge \forall z \in \mathbb{N} / \{i, j, k\} \cdot a \notin A_z\}$
- ii —
- iii $\{a\}\emptyset(\{a\}\{a,b\})^\omega$
- iv $T \not\models P_5$ because no traces satisfy P_5 .

6. Property P_6 :

- i $\{A_0A_1A_2...\mid \exists^\infty i \in \mathbb{N} \cdot a \in A_i \implies \exists^\infty j \in \mathbb{N} \cdot b \in A_j\}$
- ii $\{a\}(\{a\}\{a,b\})^\omega$

iii —

iv $T \models P_6$ because all traces satisfy P_6 .

7. Property P_7 :

i $\{A_0A_1A_2\ldots \mid \exists i \in \mathbb{N} \cdot \forall j \in \mathbb{N} \cdot j \geq i \cdot a \notin A_j\}$

ii —

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

iv $T \not\models P_7$ because no traces satisfy P_7 .

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 $E = \text{"always b"}$.

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.

Exercise 3: Invariant checking I

```

Start:  $U = \{\}$ 
 $\pi = \{\}$ 

call 1:  $S = S_0$ 
 $\pi = \{\} \rightarrow \pi = \{S_0\}$ 
 $U = \{\} \rightarrow U = \{S_0\}$ 
 $S \neq \emptyset$ 

call 2:  $S' = S_3$ 
 $\pi = \{S_0\} \rightarrow \pi = \{S_0, S_3\}$ 
 $U = \{S_0\} \rightarrow U = \{S_0, S_3\}$ 
 $S \neq \emptyset$ 

call 3:  $S' = S_2$ 
 $\pi = \{S_0, S_3\} \rightarrow \pi = \{S_0, S_3, S_2\}$ 
 $U = \{S_0, S_3\} \rightarrow U = \{S_0, S_3, S_2\}$ 
 $S \neq \emptyset$ 

call 4:  $S' = S_0$ 
 $\pi = \{S_0, S_3, S_2\} \rightarrow \pi = \{S_0, S_3, S_2, S_0\}$ 
 $U = \{S_0, S_3, S_2\}$ 
 $\text{pop}$ 
 $\pi = \{S_0, S_3, S_2, S_0\} \rightarrow \pi = \{S_0, S_3, S_2\}$ 
return false

 $\text{pop}$ 
 $\pi = \{S_0, S_3, S_2\} \rightarrow \{S_0, S_3\}$ 
return false

call 5:  $S' = S_3$ 
 $\pi = \{S_0, S_3\} \rightarrow \pi = \{S_0, S_3, S_3\}$ 
 $U = \{S_0, S_3, S_2\}$ 
 $\text{pop}$ 
 $\pi = \{S_0, S_3, S_3\} \rightarrow \pi = \{S_0, S_3\}$ 
return false

 $\text{pop}$ 
 $\pi = \{S_0, S_3\} \rightarrow \{S_0\}$ 
return false

call 6:  $S = S_1$ 
 $\pi = \{S_0\} \rightarrow \pi = \{S_0, S_1\}$ 
 $U = \{S_0, S_3, S_2\} \rightarrow \{S_0, S_3, S_2, S_1\}$ 
 $S \neq \emptyset$ 

call 7:  $S' = S_3$ 
 $\pi = \{S_0, S_1\} \rightarrow \pi = \{S_0, S_1, S_3\}$ 
 $U = \{S_0, S_3, S_2, S_1\}$ 
 $\text{pop}$ 
 $\pi = \{S_0, S_1, S_3\} \rightarrow \pi = \{S_0, S_1\}$ 
return false

call 8:  $S' = S_4$ 
 $\pi = \{S_0, S_1\} \rightarrow \pi = \{S_0, S_1, S_4\}$ 
 $U = \{S_0, S_3, S_2, S_1\} \rightarrow U = \{S_0, S_3, S_2, S_1, S_4\}$ 
 $S \neq \emptyset$ 
return true

return true

return NO,  $\pi = \{S_0, S_1, S_4\}$ 

end

```

Exercise 4: Invariant checking II

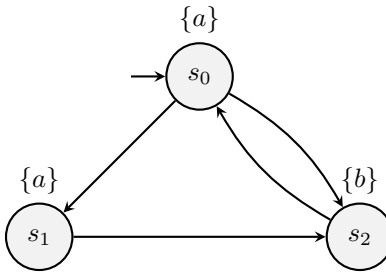


Figure 1: Transition system with 3 states

$$\phi = a$$

$$\text{non-minimal} = \{s_0, s_1, s_2\}$$

$$\text{minimal} = \{s_0, s_2\}$$