

# Cyber Physical Systems - Discrete Models

## Exercise Sheet 9 Solution

Alper Ari  
aa508@uni-freiburg.edu

Onur Sahin  
os141@uni-freiburg.de

December 20, 2023

### Exercise 1: Safety & Liveness

a

$$\begin{aligned}\text{safety} &= \text{initially } a \\ &= \{A_0 A_1 \dots \in (2^{AP})^\omega \mid a \in A_0\} \\ \text{liveness} &= \text{eventually } a \text{ happens} \\ &= \{A_0 A_1 \dots \in (2^{AP})^\omega \mid \exists i \in \mathbb{N} \cdot a \in A_i\}\end{aligned}$$

b

$$\begin{aligned}\text{safety} &= a \text{ never happens} \\ &= \{A_0 A_1 \dots \in (2^{AP})^\omega \mid \forall i \in \mathbb{N} \cdot a \notin A_i\} \\ \text{liveness} &= \text{eventually } a \text{ happens infinitely often} \\ &= \{A_0 A_1 \dots \in (2^{AP})^\omega \mid \exists^\infty i \in \mathbb{N} \cdot a \in A_i\}\end{aligned}$$

c

$$\begin{aligned}\text{safety} &= \text{initially } a \\ &= \{A_0 A_1 \dots \in (2^{AP})^\omega \mid a \in A_0\} \\ \text{liveness} &= \text{such liveness property doesn't exist} \\ &= \text{because for every liveness property it holds } \text{pref}(E) = (2^{AP})^* \\ &= \text{hence any finite prefix can be extended to satisfy property } E \\ &= \text{one needs to check the trace as a whole to ensure it does not satisfy } E\end{aligned}$$

d

$$\begin{aligned}\text{safety} &= \text{such safety property doesn't exist} \\ &= \text{because safety properties have bad prefixes} \\ &= \text{thus, it is sufficient to check prefixes of traces} \\ &= \text{to ensure it does not satisfy } E \\ \text{liveness} &= \text{eventually } a \text{ happens infinitely often} \\ &= \{A_0 A_1 \dots \in (2^{AP})^\omega \mid \exists^\infty i \in \mathbb{N} \cdot a \in A_i\}\end{aligned}$$

## Exercise 2: Safety-Liveness Decomposition

a

$$P_{\text{safe}}^{(1)} = cl(P_1) = P_1 = \{A_0A_1\ldots \in (2^{AP})^\omega \mid \forall i \in \mathbb{N} \cdot (a \in A_i \longrightarrow b \in A_{i+1})\}$$

$$P_{\text{live}}^{(1)} = P_1 \cup [(2^{AP})^\omega \setminus P_1] = (2^{AP})^\omega = \{A_0A_1\ldots \in (2^{AP})^\omega \mid \text{true}\}$$

b

$$P_{\text{safe}}^{(2)} = cl(P_2) = (2^{AP})^\omega = \{A_0A_1\ldots \in (2^{AP})^\omega \mid \text{true}\}$$

$$P_{\text{live}}^{(2)} = P_2 \cup [(2^{AP})^\omega \setminus P_2] = P_2 = \{A_0A_1\ldots \in (2^{AP})^\omega \mid \forall i \in \mathbb{N} \cdot \exists j \in \mathbb{N} \cdot (j > i \wedge a \in A_j)\}$$

c

$$P_{\text{safe}}^{(3)} = cl(P_3) = (2^{AP})^\omega = \{A_0A_1\ldots \in (2^{AP})^\omega \mid |\{i \in \mathbb{N} \mid a \in A_i\}| \leq 3\}$$

$$P_{\text{live}}^{(3)} = \{A_0A_1\ldots \in (2^{AP})^\omega \mid |\{i \in \mathbb{N} \mid a \in A_i\}| = 3\} \cup \{A_0A_1\ldots \in (2^{AP})^\omega \mid |\{i \in \mathbb{N} \mid a \in A_i\}| > 3\}$$

d

$$P_{\text{safe}}^{(4)} = cl(P_4) = \{A_0A_1\ldots \in (2^{AP})^\omega \mid a \in A_0\}$$

$$P_{\text{live}}^{(4)} = \{A_0A_1\ldots \in (2^{AP})^\omega \mid a \in A_0 \wedge \forall i \in \mathbb{N} \cdot \exists j \in \mathbb{N} \cdot (j > i \wedge a \in A_j)\} \cup \{A_0A_1\ldots \in (2^{AP})^\omega \mid a \notin A_0\}$$

e

$$P_{\text{safe}}^{(5)} = cl(P_5) = P_5 = \{A_0A_1\ldots \in (2^{AP})^\omega \mid \text{true}\}$$

$$P_{\text{live}}^{(5)} = P_5 \cup [(2^{AP})^\omega \setminus P_5] = P_5 = \{A_0A_1\ldots \in (2^{AP})^\omega \mid \text{true}\}$$

### Exercise 3: Model Checking

a)

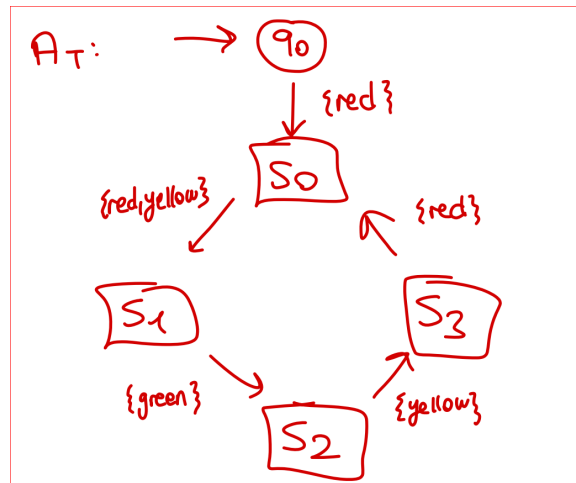


Figure 1: NFA  $A_T$

b)

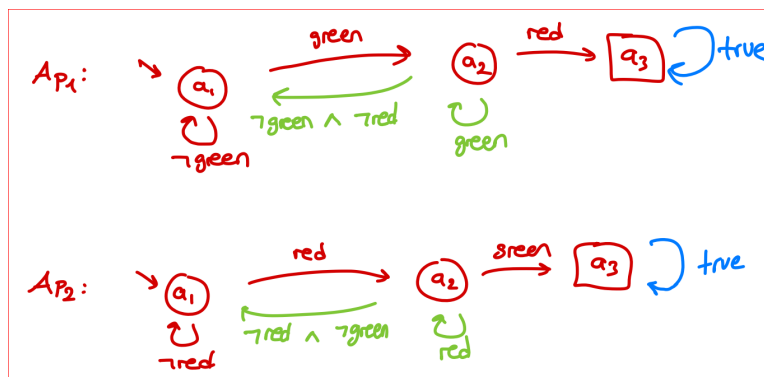


Figure 2: NFAs  $A_{P_1}$  and  $A_{P_2}$

c)

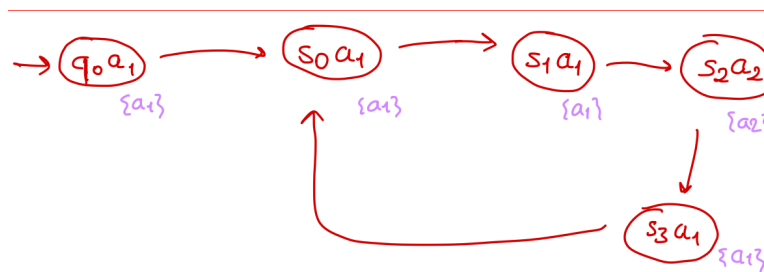


Figure 3: Accepting language  $A_T \cap A_{P_1}$  is empty, no accepting state is reachable:  $T \models P_1$

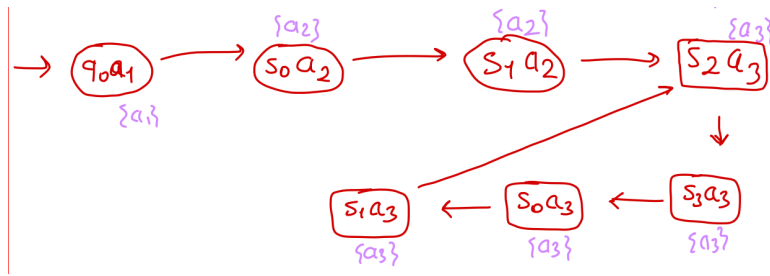


Figure 4: Accepting language  $A_T \cap A_{P_2}$  is not empty, any accepting state is reachable:  $T \not\equiv P_2$