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

$$\begin{aligned} \text{safety} &= \texttt{initially a} \\ &= \{A_0A_1... \in (2^{AP})^\omega | a \in A_0\} \\ \text{liveness} &= \texttt{eventually a happens} \\ &= \{A_0A_1... \in (2^{AP})^\omega | \exists i \in \mathbb{N} \cdot a \in A_i\} \end{aligned}$$

b

$$\begin{aligned} \text{safety} &= \texttt{a never happens} \\ &= \{A_0A_1... \in (2^{AP})^\omega | \forall i \in \mathbb{N} \cdot a \notin A_i\} \\ \text{liveness} &= \texttt{eventually a happens infinitely often} \\ &= \{A_0A_1... \in (2^{AP})^\omega | \exists^\infty i \in \mathbb{N} \cdot a \in A_i\} \end{aligned}$$

c

$$\begin{aligned} \text{safety} &= \texttt{initially a} \\ &= \{A_0A_1... \in (2^{AP})^\omega | a \in A_0\} \\ \text{liveness} &= \textit{such liveness property doesn't exist} \\ &= \textit{because for every liveness property it holds } \text{pref(E)} = (2^{AP})^* \\ &= \textit{hence any finite prefix can be extended to satisfy property E} \\ &= \textit{one needs to check the trace as a whole to ensure it does not satisfy E} \end{aligned}$$

d

$$\begin{aligned} \text{safety} &= \textit{such safety property doesn't exist} \\ &= \textit{because safety properties have bad prefixes} \\ &= \textit{thus, it is sufficient to check prefixes of traces} \\ &= \textit{to ensure it does not satisfy E} \\ \text{liveness} &= \texttt{eventually a happens infinitely often} \\ &= \{A_0A_1... \in (2^{AP})^\omega | \exists^\infty i \in \mathbb{N} \cdot a \in A_i\} \end{aligned}$$

Exercise 2: Safety-Liveness Decomposition

a

$$P^{(1)}_{\text{safe}} = cl(P_1) = P_1 = \{A_0A_1... \in (2^{AP})^\omega | \forall i \in \mathbb{N} \cdot (a \in A_i \longrightarrow b \in A_{i+1})\}$$
$$P^{(1)}_{\text{live}} = P_1 \cup [(2^{AP})^\omega \setminus P_1] = (2^{AP})^\omega = \{A_0A_1... \in (2^{AP})^\omega | true\}$$

b

$$P^{(2)}_{\text{safe}} = cl(P_2) = (2^{AP})^\omega = \{A_0A_1... \in (2^{AP})^\omega | true\}$$
$$P^{(2)}_{\text{live}} = P_2 \cup [(2^{AP})^\omega \setminus P_2] = P_2 = \{A_0A_1... \in (2^{AP})^\omega | \forall i \in \mathbb{N} \cdot \exists j \in \mathbb{N} \cdot (j > i \wedge a \in A_j)\}$$

c

$$\begin{aligned}
P^{(3)}_{\text{safe}} &= cl(P_3) = \{A_0A_1... \in (2^{AP})^\omega | \quad |\{i \in \mathbb{N} | a \in A_i\}| \leq 3\} \\
P^{(3)}_{\text{live}} &= \{\mathrm{A}_0A_1... \in (2^{AP})^\omega | \quad |\{i \in \mathbb{N} | a \in A_i\}| = 3\} \bigcup \\
&\qquad \{\mathrm{A}_0A_1... \in (2^{AP})^\omega | \quad |\{i \in \mathbb{N} | a \in A_i\}| > 3\} \\
&= \{A_0A_1... \in (2^{AP})^\omega | \quad |\{i \in \mathbb{N} | a \in A_i\}| \geq 3\}
\end{aligned}$$

d

$$\begin{aligned}
P^{(4)}_{\text{safe}} &= cl(P4) = \{A_0A_1... \in (2^{AP})^\omega | a \in A_0\} \\
P^{(4)}_{\text{live}} &= \{\ \mathrm{A}_0A_1... \in (2^{AP})^\omega | a \in A_0 \wedge \forall i \in \mathbb{N} \cdot \exists j \in \mathbb{N} \cdot (j > i \wedge a \in A_j)\} \quad \bigcup \\
&\qquad\qquad\qquad\qquad \{\ \mathrm{A}_0A_1... \in (2^{AP})^\omega | a \notin A_0\} \\
&= \{A_0A_1... \in (2^{AP})^\omega | (a \in A_0 \wedge \forall i \in \mathbb{N} \cdot \exists j \in \mathbb{N} \cdot (j > i \wedge a \in A_j)) \vee (a \notin A_0)\}
\end{aligned}$$

e

$$P^{(5)}_{\text{safe}} = cl(P_5) = P_5 = \{A_0A_1... \in (2^{AP})^\omega | true\}$$
$$P^{(5)}_{\text{live}} = P_5 \cup [(2^{AP})^\omega \setminus P_5] = P_5 = \{A_0A_1... \in (2^{AP})^\omega | true\}$$

Exercise 3: Model Checking

a)

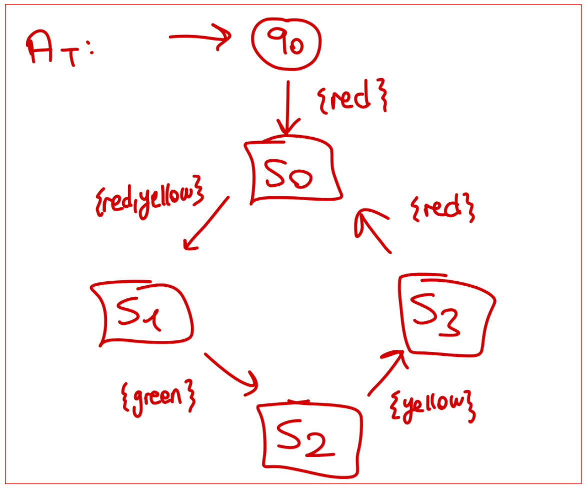

Figure 1: NFA A_T

b)

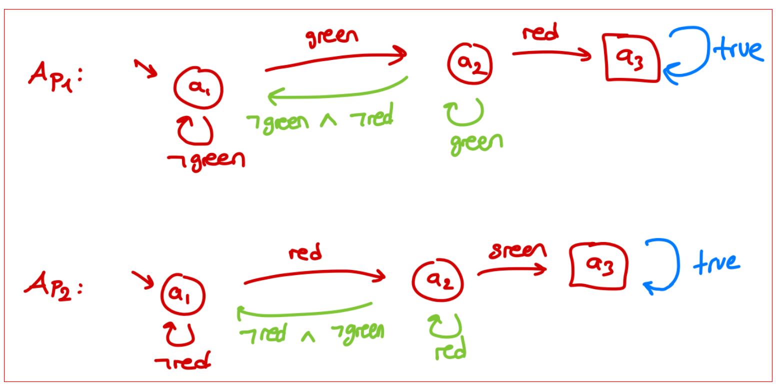

Figure 2: NFAs A_{P_1} and A_{P_2}

c)

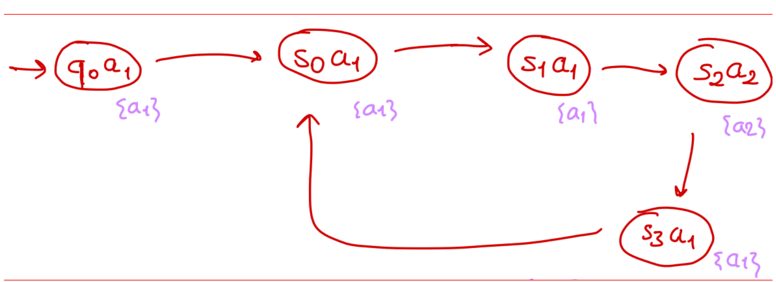

Figure 3: Accepting language $A_T \cap A_{P_1}$ is empty, no accepting state is reachable: $T \models P_1$

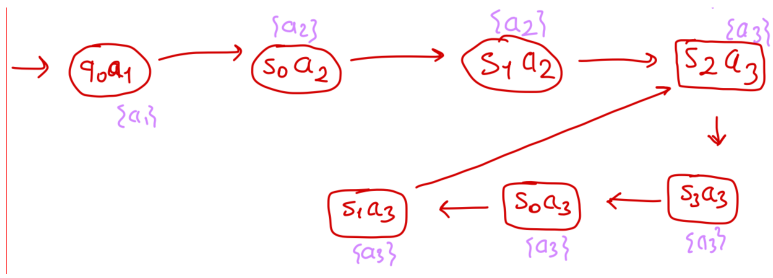

Figure 4: Accepting language $A_T \cap A_{P_2}$ is not empty, any accepting state is reachable: $T \nvDash P_2$