1	2	3	Σ
7	4.5	5	16.5

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 $\boxed{7/8}$

a

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

b

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

c

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

Counter example: $(2^{AP})^\omega$
- is a liveness property: $\text{pref}((2^{AP})^\omega) = (2^{AP})^+$
- is also a safety property: $cl((2^{AP})^\omega) = (2^{AP})^\omega$
- is even an invariant: invariant condition $\phi = true$

(−1)

d

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

Exercise 2: Safety-Liveness Decomposition

4.5/5

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

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

d

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

set of traces where $a \in A_0$ and $a \notin A_0$ would be empty. -0.5
$a \in A_0$ from P_4 cancels out due to intersection with $(2^{AP})^\omega \setminus cl(P_4)$

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

5/10

a)

2/2

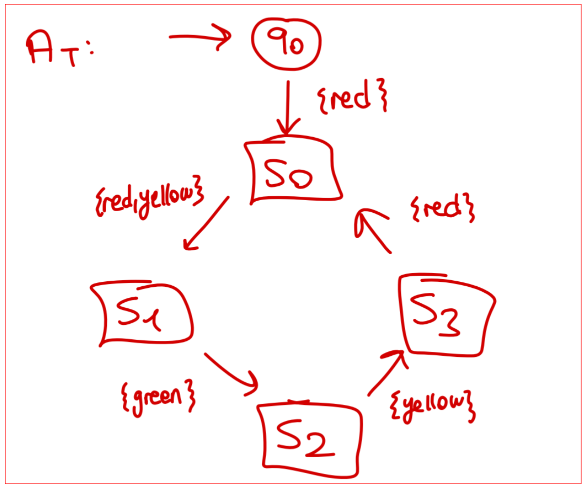

Figure 1: NFA A_T

b)

3/3

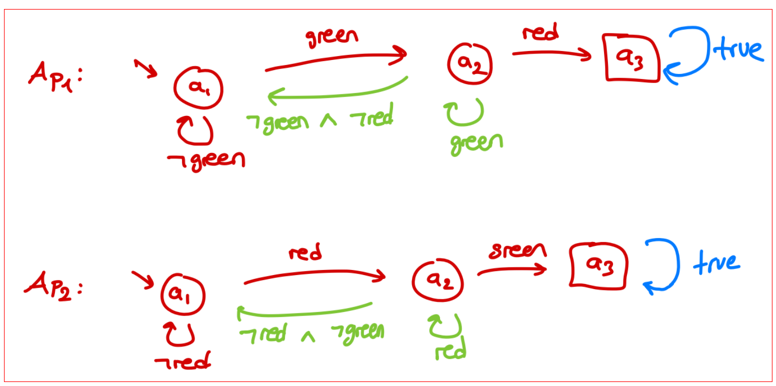

Figure 2: NFAs A_{P_1} and A_{P_2}

c)

1/5

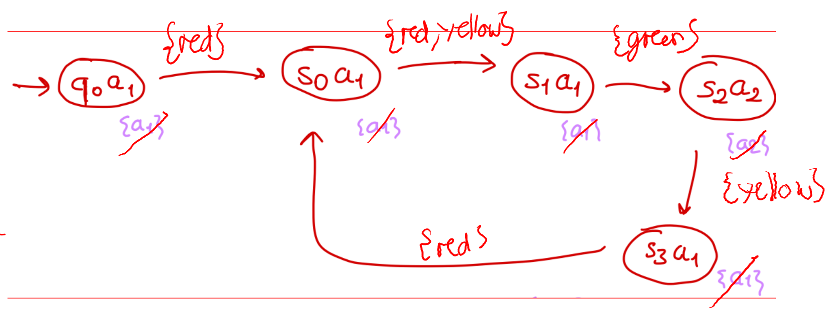

Figure 3: Accepting language $A_T \cap A_{P_1}$ is empty, no accepting state is reachable: $T \vDash P_1$ (✓)

The intersection automata should have labels on the transitions, not on the states (TS have labels on states)

The labels should be sets of atomic propositions {green, yellow, red}, not names of states.

−2 ×2

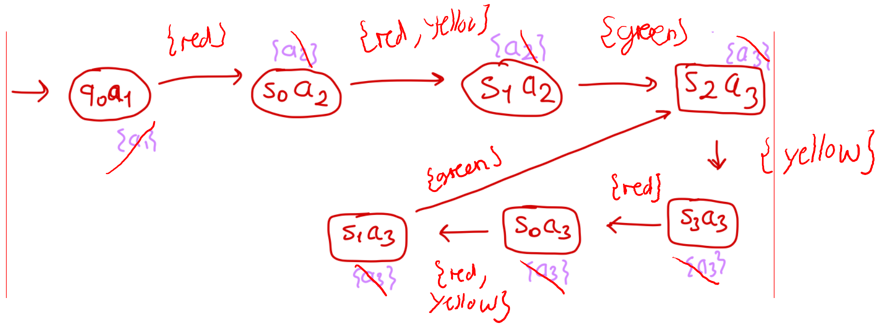

Figure 4: Accepting language $A_T \cap A_{P_2}$ is not empty, any accepting state is reachable: $T \not\models P_2$ (✓)