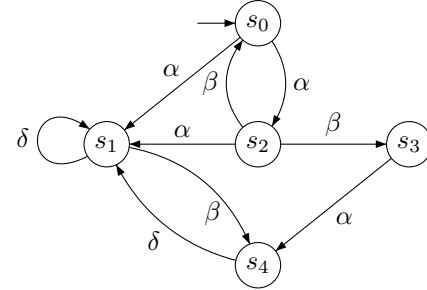


Exercise 1 (Realizability & Fairness):

(2 points)

Consider the transition system TS on the right (where atomic propositions are omitted). Decide which of the following fairness assumptions $\mathcal{F}_i$ are realizable for TS . Justify your answers!



1. $\mathcal{F}_1 = (\{\{\alpha\}\}, \{\{\delta\}\}, \{\{\alpha, \beta\}\})$
2. $\mathcal{F}_2 = (\{\{\alpha, \delta\}\}, \{\{\alpha, \beta\}\}, \{\{\delta\}\})$
3. $\mathcal{F}_3 = (\{\{\alpha, \delta\}, \{\beta\}\}, \{\{\alpha, \beta\}\}, \{\{\delta\}\})$

Solution:

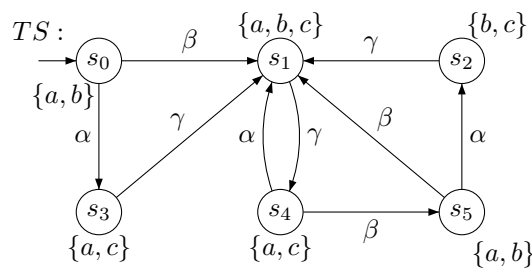
Note that only the unconditional fairness constraints are relevant to decide realizability.

1. $\mathcal{F}_1 = (\{\{\alpha\}\}, \{\{\delta\}\}, \{\{\alpha, \beta\}\})$ is not realizable fair. Consider the states s_1 and s_4 . There are no $\mathcal{F}_1$ fair path fragments starting from s_1 or s_4 , as on each such path fragment, α transitions never occur. This violates the unconditional fairness constraint $\{\{\alpha\}\}$.
2. $\mathcal{F}_2 = (\{\{\alpha, \delta\}\}, \{\{\alpha, \beta\}\}, \{\{\delta\}\})$ is realizable fair, as all SCCs contain the actions α or δ .
3. $\mathcal{F}_3 = (\{\{\alpha, \delta\}, \{\beta\}\}, \{\{\alpha, \beta\}\}, \{\{\delta\}\})$ is realizable fair. Again, all SCCs contain the actions α or δ and they all contain β .

Exercise 2 (Model Checking Regular Safety Properties):

(3 points)

Consider the following transition system TS



and the regular safety property

$$P_{\text{safe}} = \text{"always if } a \text{ is valid and } b \wedge \neg c \text{ was valid somewhere before, then neither } a \text{ nor } b \text{ holds thereafter at least until } c \text{ holds"}$$

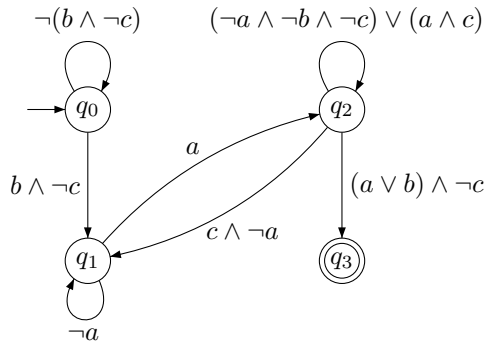
As an example, it holds:

$$\begin{aligned} \{b\}\emptyset\{a, b\}\{a, b, c\} &\in \text{pref}(P_{\text{safe}}) \\ \{a, b\}\{a, b\}\emptyset\{b, c\} &\in \text{pref}(P_{\text{safe}}) \\ \{b\}\{a, c\}\{a\}\{a, b, c\} &\in \text{BadPref}(P_{\text{safe}}) \\ \{b\}\{a, c\}\{a, c\}\{a\} &\in \text{BadPref}(P_{\text{safe}}) \end{aligned}$$

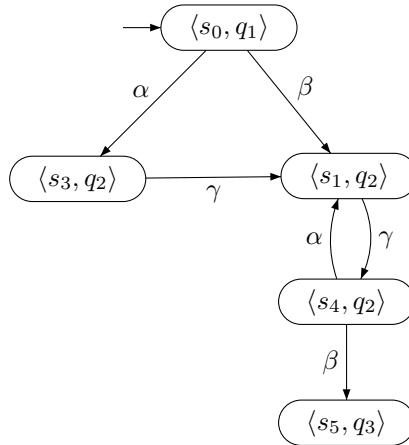
- a) Define an NFA $\mathcal{A}$ such that $\mathcal{L}(\mathcal{A}) = \text{MinBadPref}(P_{\text{safe}})$.
- b) Decide whether $TS \models P_{\text{safe}}$ using the $TS \otimes \mathcal{A}$ construction.
Provide a counterexample if $TS \not\models P_{\text{safe}}$.

Solution: _____

- a) The NFA that accepts the set of minimal bad prefixes:



- b) First we apply the $TS \otimes \mathcal{A}$ construction which yields:



A counterexample to $TS \models P_{\text{safe}}$ is given by the following initial path fragment in $TS \otimes \mathcal{A}$:

$$\pi_{\otimes} = \langle s_0, q_1 \rangle \langle s_3, q_2 \rangle \langle s_1, q_2 \rangle \langle s_4, q_2 \rangle \langle s_5, q_3 \rangle$$

By projection on the state component, we get a path in the underlying transition system:

$$\pi = s_0 s_3 s_1 s_4 s_5 \text{ with } \text{trace}(\pi) = \{a, b\}\{a, c\}\{a, b, c\}\{a, c\}\{a, b\}$$

Obviously, $\text{trace}(\pi) \in \text{BadPref}(P_{\text{safe}})$, so we have $\text{Traces}_{\text{fin}}(TS) \cap \text{BadPref}(P_{\text{safe}}) \neq \emptyset$. Therefore, $TS \not\models P_{\text{safe}}$.

Exercise 3 (Quantitative Fairness):

(3 points)

Let us introduce the notion of *quantitative fairness* $\exists_p X$, where X is a subset of some atomic propositions $AP \neq \emptyset$ and p is a real number. We are not only interested in something occurring (say event a , that is $X = \{a\}$) infinitely often, but also the ratio of the occurrence, say p .

For a finite word π , let $Freq_X$ be the number of times some Y with $X \subseteq Y$ occurs at some position $i < n$. For example, let $\pi = \{a\}\{b, c\}\{a, c\}\{c\}\{b, c\}\{c\}\{a\}\{c\}$, then $Freq_{\{a\}}(\pi) = 3$ and $Freq_{\{b, c\}}(\pi) = 2$.

For an infinite word π , let π_n be the finite prefix of length n , i.e., $\pi = \pi_n \cdot \pi'$, where $|\pi_n| = n$ and $\pi' \in \Sigma^\omega$. The semantics of quantitative fairness is as follows:

$$\pi \models \exists_p X \quad \text{iff} \quad \liminf_{n \rightarrow \infty} \left(\frac{1}{n} Freq_X(\pi_n) \right) = p$$

For example, the word $\pi = a^\omega$ satisfies $\exists_p \{a\}$ with $p = 1$.

- Give a formal definition for $Freq_X$.
- Show that for any word π and letter a , $\liminf_{n \rightarrow \infty} \frac{1}{n} Freq_a(\pi_n) \leq 1$.
- Show that $\exists_p \{a\}$ with $p = 0$ is not same as $\neg \exists^\infty a$. That is, find a word π such that $\pi \models \exists_p \{a\}$ and $\pi \models \exists^\infty a$.

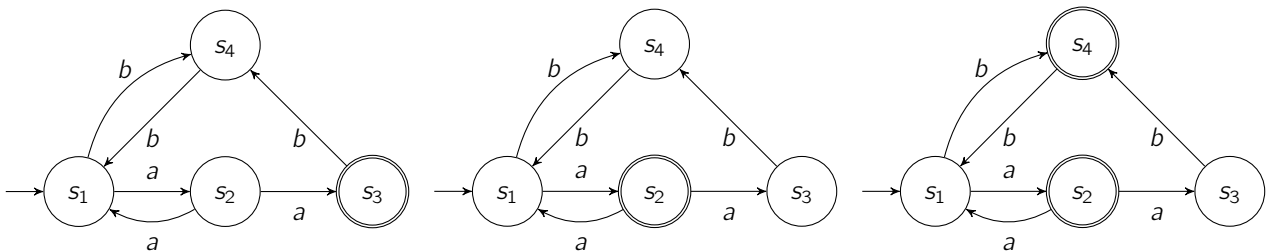
Solution:

- $Freq_X: (2^{AP})^* \rightarrow \mathbb{N}$ with $\pi \mapsto |\{i | i \leq |\pi| \wedge X \subseteq \pi[i]\}|$.
- By definition, $Freq_X(\pi) \leq n$ for $n = |\pi|$, thus $\frac{1}{n} Freq_X(\pi) \leq 1$. As the sequence of real numbers is bounded from above, the limit inferior exists.
- Words where the gap between successive a 's are growing should do. We consider the word $\{a\}\{a\}\emptyset\{a\}\emptyset\emptyset\emptyset\{a\}\emptyset\emptyset\emptyset\emptyset\emptyset\emptyset\{a\}$ where $\pi[i] = \{a\}$ iff $i = 2^k$ for some k . The ratio is then a sequence $1, 1, \frac{2}{3}, \frac{3}{4}, \frac{3}{5}, \frac{3}{6}, \frac{3}{7}, \frac{4}{8}, \dots$. The sequence only increases at $i = 2^k$. We consider this subsequence; if this goes to zero, then so does the complete sequence. For $m > 3$ the sequence is given by $b_m = \frac{m+1}{2^m}$. To show that the sequence goes to zero, we show that for all $m > M$ it is smaller than the harmonic sequence, that is, smaller than $\frac{1}{m}$. For $m > 6$, we have that $b_m < \frac{2m}{2^m} < \frac{m}{2^{m-1}} < \frac{1}{2^{\frac{m-1}{2}}} < \frac{1}{m}$.

Exercise 4 (NBA):

(2 points)

- Give the language for the following three NBA:



- Give an NBA for:
 - "initially a occurs, and at some point b occurs" with $\Sigma = \{a, b, c\}$.
 - "if a occurs somewhere, then afterwards (b occurs infinitely often iff c occurs infinitely often).

Solution: _____

a) For each of the three automata, any of the given languages are correct.

- a)
- $(aa + bb + aabb)^* \cdot aa(bb(aa + bb)^*)aa^\omega$
 - $(aa + bb)^* \cdot ((aa + bb)^* aabb)^\omega$
 - $((aa + bb)^* aabb)^\omega$
- b)
- $(aa + bb + aabb)^* \cdot a \cdot ((a + abb)(bb)^*)a^\omega$
 - $(aa + bb)^* \cdot a \cdot (a(bb)^*a)^\omega$
 - $((bb)^*aa)^\omega$
- c)
- $(aa + bb + aabb)^\omega$
 - $(aa + bb)^\omega$

