Tutorial 7 - Solutions

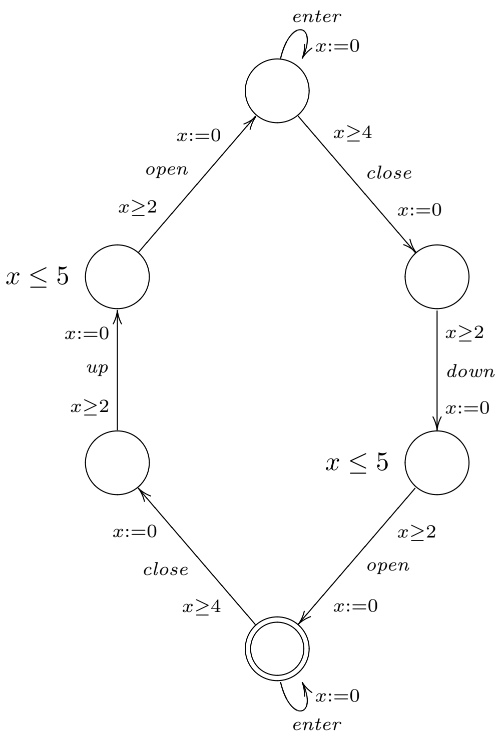
Exercise 1

Consider an autonomous elevator which operates between two floors. The requested behaviour of the elevator is as follows:

- The elevator can stop either at the ground floor or the first floor.
- When the elevator arrives at a certain floor, its door automatically opens. It takes at least 2 seconds from its arrival before the door opens but the door must definitely open within 5 seconds.
- Whenever the elevator's door is open, passengers can enter. They enter one by one and we (optimistically) assume that the elevator has a sufficient capacity to accommodate any number of passengers waiting outside.
- The door can close only 4 seconds after the last passenger entered.
- After the door closes, the elevator waits at least 2 seconds and then travels up or down to the other floor.

Your tasks are:

- Suggest a timed automaton model of the elevator. Use the actions *up* and *down* to model the movement of the elevator, *open* and *close* to describe the door operation and the action *enter* which means that a passenger is entering the elevator.
  - Timed automaton



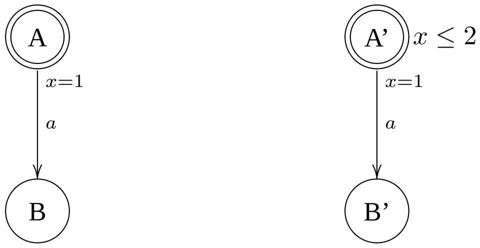
- Provide two different timed traces of the system starting at the ground floor with the door open.

$$(1, enter)(5, close)(7, up)(9.5, open)\cdots$$

$$(0.1, enter)(2, enter)(6.7, close)\cdots$$

Exercise 2

Consider the following timed automata and for each pair decide whether their initial states are (i) timed bisimilar (ii) untimed bisimilar.



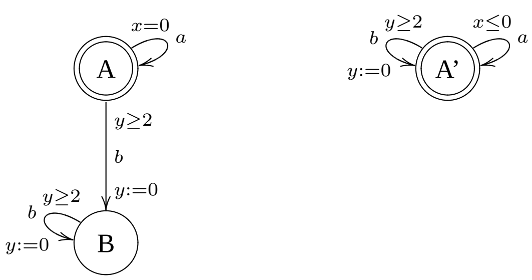
(i) The initial states are not timed bisimilar. A winning strategy for the attacker is to play $(A, [x = 0]) \xrightarrow{2.5} (A, [x = 2.5])$ which clearly can not be matched from $(A', [x = 0])$ due to the invariant.

(ii) The initial states are untimed bisimilar. A bisimulation relating them is for example

$$
\begin{aligned}
\mathcal{R} = &\big\{\big((A, [x = d]), (A', [x = d])\big) \mid d \leq 1\big\} && (1)\\
&\cup \big\{\big((A, [x = d]), (A', [x = d'])\big) \mid d > 1 \text{ and } 1 < d' \leq 2\big\} && (2)\\
&\cup \big\{\big((B, [x = d]), (B', [x = d])\big) \mid d \geq 1\big\} && (3)
\end{aligned}
$$

(i) The initial states are not timed bisimilar. Since timed bisimilarity implies untimed bisimilarity, this can be seen by arguing that they are not untimed bisimilar. See (ii).

(ii) A winning strategy for the attacker is simply to do an $(A, [x = 0]) \xrightarrow{a} (A, [x = 0])$ which can not be answered from the initial state $(A', [x = 0])$ because of the guard on the a transition.



(i) The initial states are timed bisimilar. A bisimulation relating them is:

$$
\begin{aligned}
\mathcal{R} = &\big\{\big((A, [x = d, y = d]), (A', [x = d, y = d])\big) \mid d \geq 0\big\}\\
&\cup \big\{\big((B, [x = d, y = d']), (A', [x = d, y = d'])\big) \mid d \geq 2, d' \geq 0\big\}
\end{aligned}
$$

(ii) Since timed bisimilarity implies untimed bisimilarity, by (i) the initial states are also untimed bisimilar.

Exercise 3

Let T be a timed transition system. Let us consider a labelled transition system T' where every time-delay action $d \in \mathbb{R}^{\geq 0}$ is replaced with the silent action τ. We now define that two states p and q from the timed transition system T are *time abstracted bisimilar* if and only if p and q are weakly bisimilar in T'.

- Is the notion of time abstracted bisimilarity equivalent to untimed bisimilarity?
  - No, see next bullet.
- If yes, prove your claim. If no, give a counter example.
  - A counter example is the following timed transition system

$$
\begin{tikzcd}
A \arrow[d, "a"] & B \arrow[d, "3"] \\
A' & B' \arrow[d, "a"] \\
& B''
\end{tikzcd}
$$

Now the initial states are time abstracted bisimilar since they are weakly bisimilar in the following labelled transition system:

$$
\begin{tikzcd}
A \arrow[d, "a"] & B \arrow[d, "\tau"] \\
A' & B' \arrow[d, "a"] \\
& B''
\end{tikzcd}
$$

On the other hand they can not be untimed bisimilar since $A \xrightarrow{a} A'$, but $B \stackrel{a}{\not\longrightarrow}$.