

## Advanced Model Checking Summer term 2014

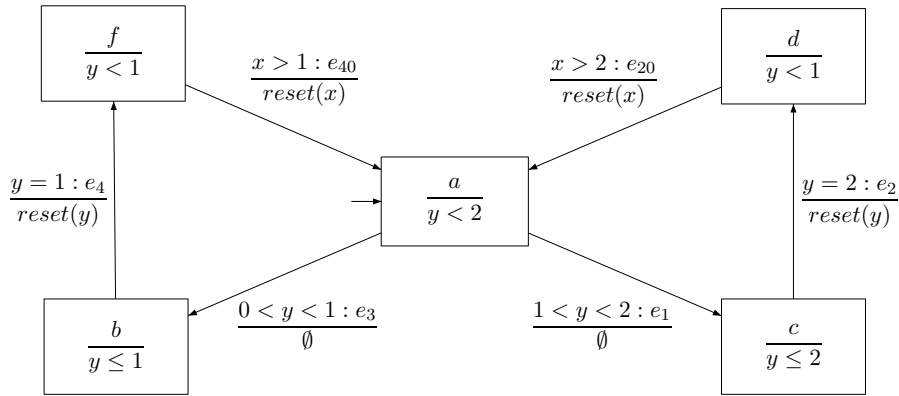
### – Series 11 –

Hand in on **9 July** before the exercise class.

#### Exercise 1

(4 points)

Give the formal semantics of the following timed automaton  $TA$  by means of a transition system. That is, formally define the components of the (infinite) transition system.



#### Solution:

The semantic of  $TA$  is given by the transition system  $TS(TA) = (S, Act, \rightarrow, I, AP, L)$  where:

- $AP = \{a, b, c, d, f\}$  and  $Act = \{e_1, e_2, e_3, e_4, e_{40}, e_{20}\}$ .
- $S = \{\langle a, t_x, t_y \rangle \mid a \in AP \wedge t_x, t_y \in \mathbb{R}_{\geq 0}\}$ , where  $t_x$  and  $t_y$  are shorthands for the clock evaluation  $\eta$  with  $\eta(x) = t_x$  and  $\eta(y) = t_y$ , respectively.
- $I = \{\langle a, 0, 0 \rangle\}$ .
- $\rightarrow$  is defined as ( $d'$  represents the amount of delay):

|                               |                        |                                         |                                                                   |
|-------------------------------|------------------------|-----------------------------------------|-------------------------------------------------------------------|
| $\langle a, t_x, t_y \rangle$ | $\xrightarrow{d'}$     | $\langle a, t_x + d', t_y + d' \rangle$ | for all $t_x \geq 0, 0 \leq t_y + d' < 2$ and $d' > 0$            |
| $\langle a, t_x, t_y \rangle$ | $\xrightarrow{e_3}$    | $\langle b, t_x, t_y \rangle$           | for all $t_x \geq 0$ and $0 < t_y < 1$                            |
| $\langle a, t_x, t_y \rangle$ | $\xrightarrow{e_1}$    | $\langle c, t_x, t_y \rangle$           | for all $t_x \geq 0$ and $1 < t_y < 2$                            |
| $\langle b, t_x, t_y \rangle$ | $\xrightarrow{d'}$     | $\langle b, t_x + d', t_y + d' \rangle$ | for all $t_x \geq 0$ and $0 \leq t_y + d' \leq 1$ , with $d' > 0$ |
| $\langle b, t_x, t_y \rangle$ | $\xrightarrow{e_4}$    | $\langle f, t_x, 0 \rangle$             | for all $t_x \geq 0$ and $t_y = 1$                                |
| $\langle f, t_x, t_y \rangle$ | $\xrightarrow{d'}$     | $\langle f, t_x + d', t_y + d' \rangle$ | for all $t_x \geq 0$ and $0 \leq t_y + d' < 1$ , with $d' > 0$    |
| $\langle f, t_x, t_y \rangle$ | $\xrightarrow{e_{40}}$ | $\langle a, 0, t_y \rangle$             | for all $t_x > 1$ and $0 \leq t_y < 2$                            |
| $\langle c, t_x, t_y \rangle$ | $\xrightarrow{d'}$     | $\langle c, t_x + d', t_y + d' \rangle$ | for all $t_x \geq 0$ and $0 \leq t_y + d' \leq 2$ , with $d' > 0$ |
| $\langle c, t_x, t_y \rangle$ | $\xrightarrow{e_2}$    | $\langle d, t_x, 0 \rangle$             | for all $t_x \geq 0$ and $t_y = 2$                                |
| $\langle d, t_x, t_y \rangle$ | $\xrightarrow{d'}$     | $\langle d, t_x + d', t_y + d' \rangle$ | for all $t_x \geq 0$ and $0 \leq t_y + d' < 1$ , with $d' > 0$    |
| $\langle d, t_x, t_y \rangle$ | $\xrightarrow{e_{20}}$ | $\langle a, 0, t_y \rangle$             | for all $t_x > 2$ and $0 \leq t_y < 2$                            |

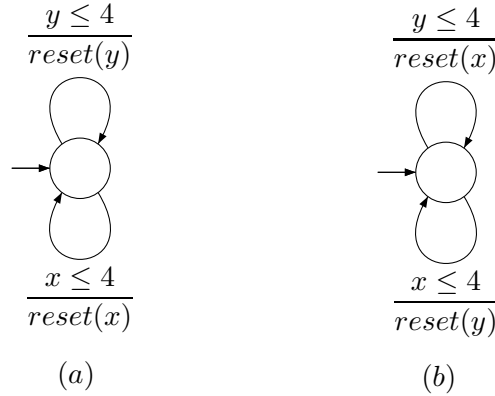
The set of reachable states in  $TS(TA)$  is:

$$\begin{aligned} & \{\langle a, 0, 0 \rangle\} \cup \{\langle b, t_x, t_y \rangle \mid t_x, t_y \in \mathbb{R}_{\geq 0}, 0 < t_x = t_y < 1\} \cup \\ & \{\langle f, t_x, 0 \rangle \mid t_x \in \mathbb{R}_{\geq 0}, 0 < t_x < 1\} \cup \{\langle f, t_x, t_y \rangle \mid t_x, t_y \in \mathbb{R}_{\geq 0}, 0 < t_x < t_y < 1\} \cup \\ & \{\langle a, 0, t_y \rangle \mid t_y \in \mathbb{R}_{\geq 0}, 0 < t_y < 1\} \cup \{\langle c, t_x, t_y \rangle \mid t_x, t_y \in \mathbb{R}_{\geq 0}, 1 < t_x < t_y < 2\} \cup \\ & \{\langle d, t_x, 0 \rangle \mid t_x \in \mathbb{R}_{\geq 0}, 1 < t_x < 2\} \cup \{\langle c, t_x, t_y \rangle \mid t_x, t_y \in \mathbb{R}_{\geq 0}, 1 < t_x = t_y < 2\} \end{aligned}$$

## Exercise 2

(2 points)

Consider the following two timed automata  $TA_1$  and  $TA_2$ .



As these automata only have a single location, their *states* can be thought of as a point in the real plane. A point  $(d, e) \in \mathbb{R}_{\geq 0}^2$  then represents that clock  $x$  has value  $d$  and clock  $y$  has value  $e$ . Determine the reachable state space of both timed automata. Justify your answers.

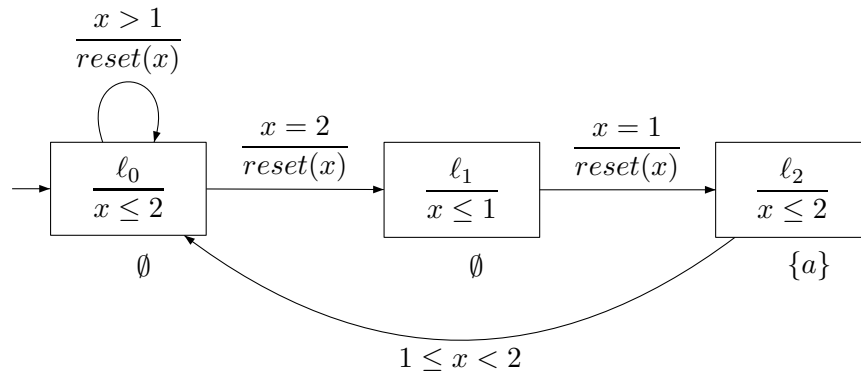
**Solution:**

- (a) The state space is  $\{(x, y) \mid x \geq 0 \wedge y \geq 0\}$ , i.e.,  $\mathbb{R}_{\geq 0}^2$ . The important point is that e.g., any point  $y > x + 4$  can be reached by resetting clock  $x$ . E.g., at point  $(4, 4)$ , resetting  $x$  yields  $(0, 4)$ , from there time may advance to  $(1, 5)$ , say, and we can reset  $x$  again, yielding  $(0, 5)$ . Thus, the surface  $\{(x, y) \mid x \leq 4 \wedge y \geq 0\}$  is reachable. By just advancing  $x$  (i.e., no reset), also values  $(x, y)$  with  $x, y \geq 4$  can be reached. By symmetry, the same holds for resetting of  $y$ .
- (b) The state space is  $\{(x, y) \mid 0 \leq y \leq x + 4 \wedge 0 \leq x \leq y + 4\}$ . The crucial point is that clock  $x$  cannot be reset once  $y > 4$ , which is possible in part (a) of this exercise.

## Exercise 3

(3 points)

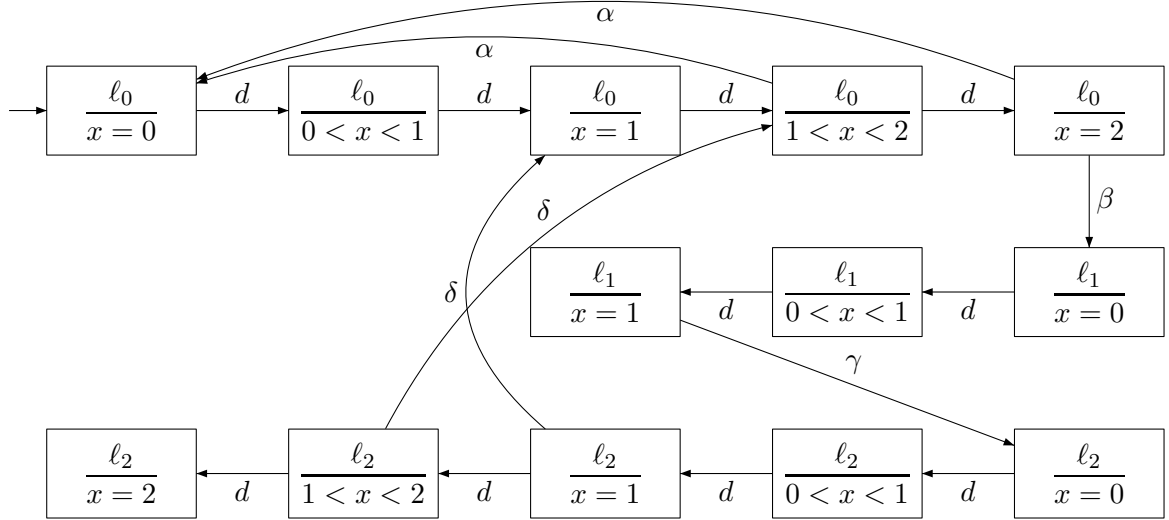
Consider the following timed automaton  $TA$ .



- (a) Determine the set of states  $Sat(\exists \Diamond^{\leq 4} a)$ .
- (b) Determine the region transition system  $RTS(TA, true)$ .
- (c) Is the TA timelock-free? Justify your answer.

**Solution:**

- (a)  $Sat(\exists \Diamond^{\leq 4} a) = \{\langle \ell_0, t_x \rangle \mid 0 \leq t_x \leq 2\} \cup \{\langle \ell_1, t_x \rangle \mid 0 \leq t_x \leq 1\} \cup \{\langle \ell_2, t_x \rangle \mid 0 \leq t_x < 2\}$ . Note that  $\langle \ell_2, 2 \rangle$  is not contained in this set, because there is no time-divergent path starting in this state and hence there is also no time-divergent path that satisfies  $\Diamond^{\leq 4} a$ .
- (b) The region transition system  $RTS(TA, true)$  is given by the following picture.



- (c) The region transition system contains a state,  $\langle \ell_2, x = 2 \rangle$ , which has no outgoing transitions. There is no time-divergent path starting from this state, and thus the timed automaton  $TA$  contains a timelock.

#### Exercise 4

(1 points)

- (a) Find a counterexample showing that

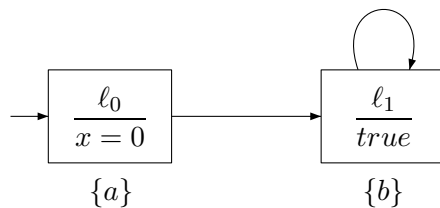
$$\forall \Diamond^{\leq d} \Phi \wedge \forall \Diamond^{\leq d} \Psi \not\equiv \forall \Diamond^{\leq d} (\Phi \wedge \Psi),$$

where  $\Diamond^{\leq d} = \Diamond^{[d, d]}$  for  $d \in \mathbb{R}_{\geq 0}$ .

- (b) Does this also hold for  $J = [0, \infty)$ ? Justify your answer.

**Solution:**

- (a) This equivalence does not hold. A transition takes no time and as a result, the automaton can be in more than one location at a given time point. To give a counterexample, consider the following timed automaton  $TA$  with all the guard and location invariants as  $true$  and the TCTL formula  $\Phi = \forall \Diamond^{\leq 0} a \wedge \forall \Diamond^{\leq 0} b$  and  $\Phi' = \forall \Diamond^{\leq 0} (a \wedge b)$ . Then  $TA \models \Phi$  but  $TA \not\models \Phi'$ .



(b) Consider the same timed automaton. Then  $TA \models \forall \Diamond a \wedge \forall \Diamond b$ , but  $TA \not\models \forall \Diamond (a \wedge b)$ .