Advanced Topics in Computer Science
Exercises with (Some) Solutions

Teacher: Luca Tesei

Master of Science in Computer Science - University of Camerino

Contents

1 Timed Automata Modelling **1**

2 Timed Bisimulation and other Equivalences **9**

3 Region Graph and Zone Graph **11**

1 Timed Automata Modelling

Exercise 1.1 *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.*

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.*

Exercise 1.2 *Draw a Network of Timed Automata with three components: Train, Gate and Controller. The network must model the following scenario. When a Train is approaching a junction with normal road, an* $\mathrm{approach}$ *signal must be sent to the Controller of the system. This must happen between 3 and 6 minutes before the Train actually enters the junction. Upon receiving the signal, the controller must send a* close *signal to the Gate. The Gate, upon receiving this message, starts closing. This process can take between 1 and 2 minutes. Between 1 and 2 minutes after the Train completely crossed the junction, it must send to the Controller an* exit *signal, which is immediately forwarded to the Gate. After receiving this message, the Gate will open between 2 and 3 minutes.*

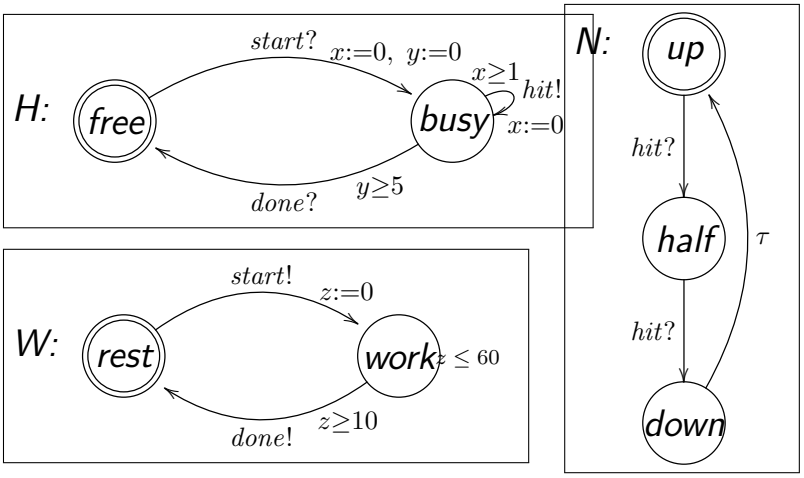
Exercise 1.3 *Michael Fischer's mutual exclusion algorithm uses timing. The algorithm uses just one global variable 'id', whose initial value is 0. In order to ensure mutual exclusion, each process P_i, $i \in \{1, \ldots, n\}$, executes the following pseudocode where 'delay' stands for a positive integer constant.*

```
while (true) do
begin
  'noncritical section';
  L: if (id != 0) then goto L;
  1: id := i;
  2: pause(delay);
  3:if (id != i) then goto L;
  'critical section';
  id := 0;
end
```

In the above pseudocode algorithm the statement pause(delay) makes the process wait for the amount of time specified by the constant 'delay'.

Draw a timed automaton using the syntax and the features of UPPAAL representing the execution of the algorithm by the generic process i.

Exercise 1.4 *Consider the following network of timed automata from the lecture.*



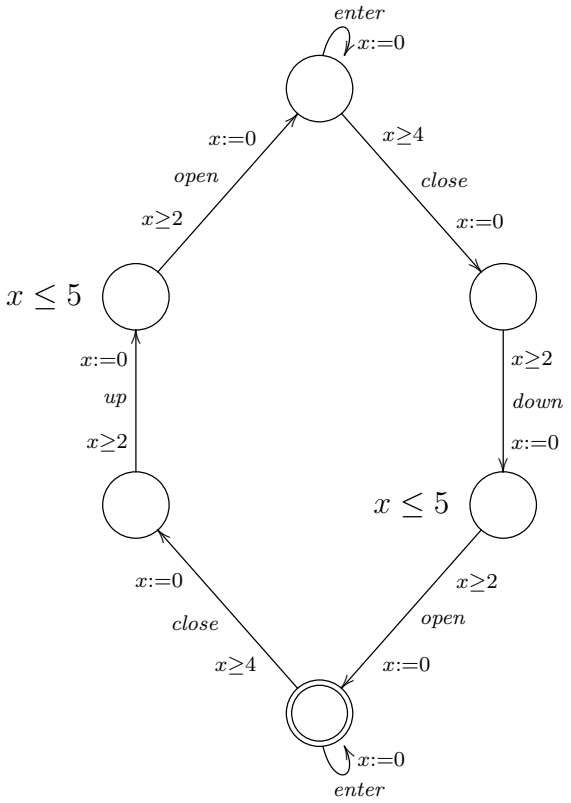
- *Give an example of a timed trace in the network above.*
- *Which of the following properties are true?*
  - *A[] (W.rest $\vee$ $z \leq 100$)*
  - *E⟨⟩ (W.rest $\wedge$ H.busy)*
  - *A⟨⟩ W.rest*
  - *E[] H.busy*
  - *W.work −− > W.rest*

Exercise 1.5 *Draw a Timed Automaton modeling the following scenario. A small elevator connects two floors: floor 0 and floor 1. The elevator can transport a maximum of 2 people and it always starts at floor 0. Then:*

- *Whenever the elevator is waiting at a floor and no passenger has entered yet, it can be called from the other floor. In this case, within 10 seconds, the elevator travels to the other floor, taking exactly 60 seconds.*
- *Whenever the elevator is waiting at a floor and it has not been called from the other floor, the first passenger can enter. Then:*
  - *If for 30 seconds no other passenger enters, then the elevator travels to the other floor, taking exactly 60 seconds.*
  - *If within 30 seconds a second passenger enters, then the elevator does not accept further passengers and, within 10 seconds, it travels to the other floor, taking between 60 seconds and 80 seconds.*

Solutions

Solution of Exercise 1.1

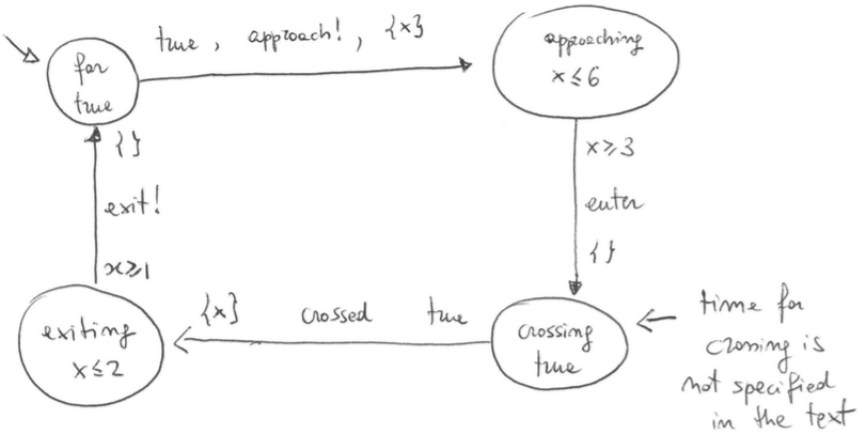


Provide two different timed traces of the system starting at the ground floor with the door open.

$$(1, enter)(5, close)(7, up)(9.5, open)\cdots$$
$$(0.1, enter)(2, enter)(6.7, close)\cdots$$

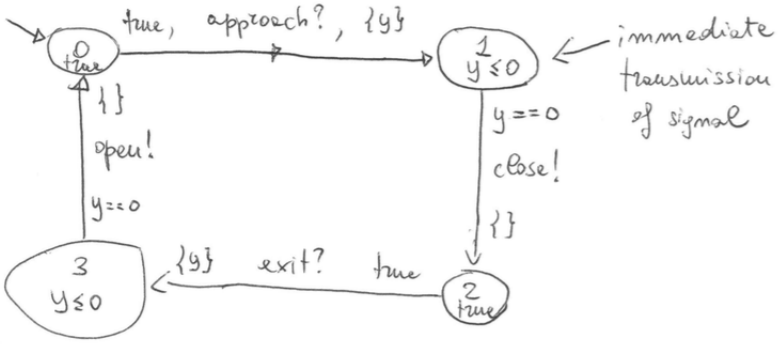
Solution of Exercise 1.2

Train EX-1



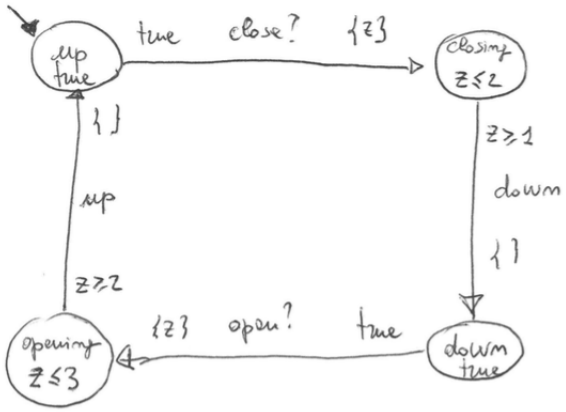
communication channels are exit and approach
the other actions are internal

Controller



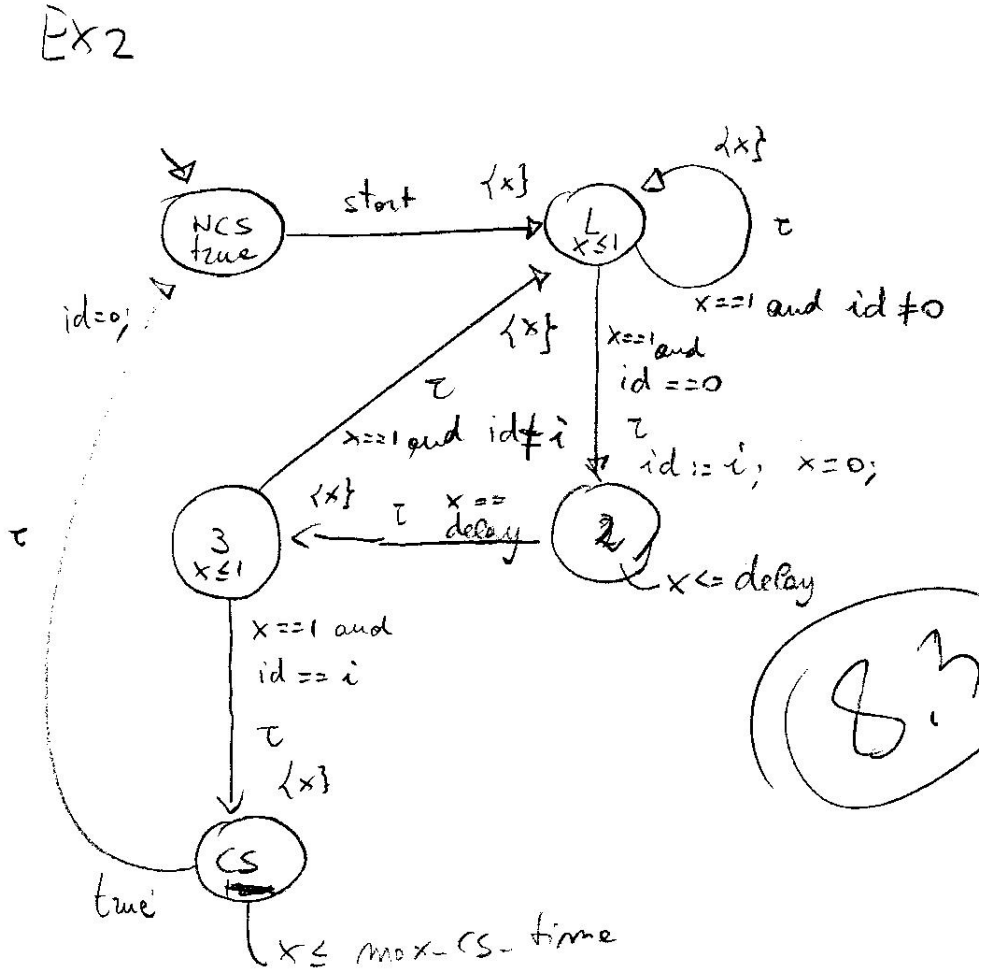
idem
all actions are communication channels

Gate



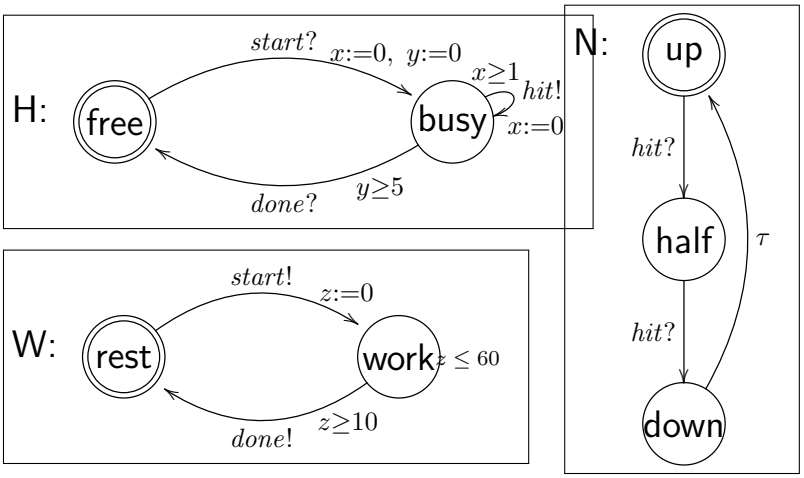
close and open are communication channels,
up and down are internal actions.

Solution of Exercise 1.3



Solution of Exercise 1.4

Consider the following network of timed automata from the lecture.



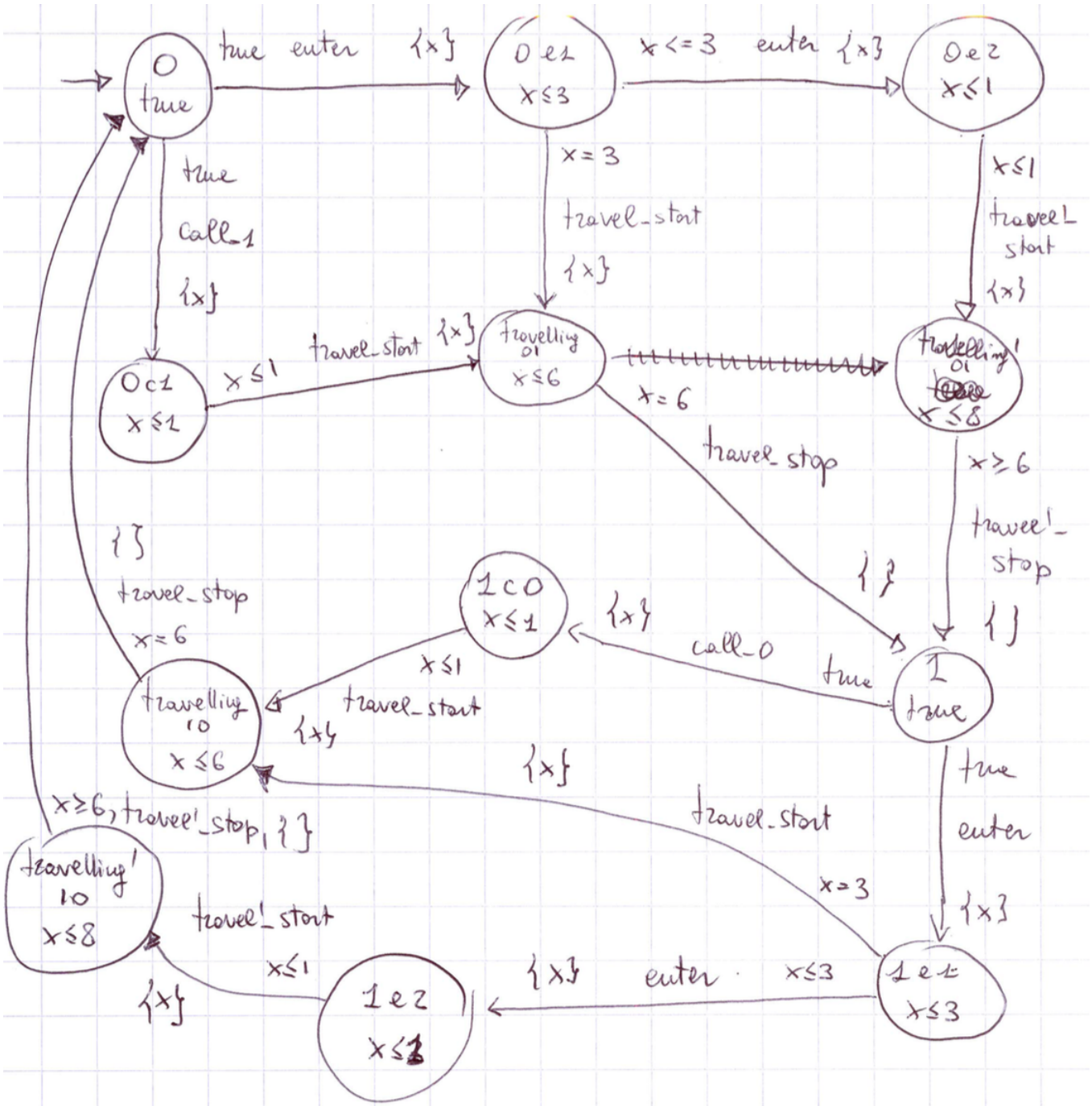
- Give an example of a timed trace in the network above.
  - A timed trace could be as follows:

$$(20, \tau)(40, \tau)(60, \tau)(60, \tau) \cdots$$

An example of a sequence of states could be:
$\big((free, rest, up), [x = 0, y = 0, z = 0]\big) \xrightarrow{\tau} \big((busy, work, up), [x = 0, y = 0, z = 0]\big) \xrightarrow{20} \big((busy, work, up), [x = 20, y = 20, z = 20]\big) \xrightarrow{\tau} \big((busy, work, half), [x = 0, y = 20, z = 20]\big) \xrightarrow{40} \big((busy, work, half), [x = 40, y = 60, z = 60]\big) \xrightarrow{\tau} \big((busy, work, down), [x = 0, y = 60, z = 60]\big) \xrightarrow{\tau} \big((free, rest, down), [x = 0, y = 60, z = 60]\big) \xrightarrow{\tau} \big((free, rest, up), [x = 0, y = 60, z = 60]\big) \cdots$

- Which of the following properties are true?
  - A[] (W.rest $\vee$ $z \leq 100$) : **True**
  - E$\langle\rangle$ (W.rest $\wedge$ H.busy) : **False**
  - A$\langle\rangle$ W.rest : **True**
  - E[] H.busy : **False**
  - W.work $--> $ W.rest : **True**

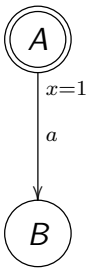
Solution of Exercise 1.5

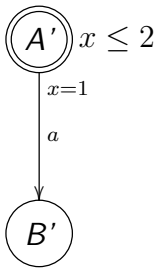


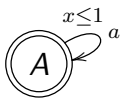
Ex 4, we let 1 time unit = 10 seconds

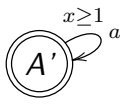
2 Timed Bisimulation and other Equivalences

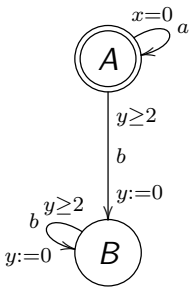
Exercise 2.1 *Consider the following timed automata and for each pair decide whether their initial states are (i) timed bisimilar (ii) untimed bisimilar.*

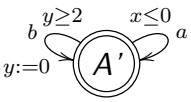












Solutions

Solution of Exercise 2.1

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

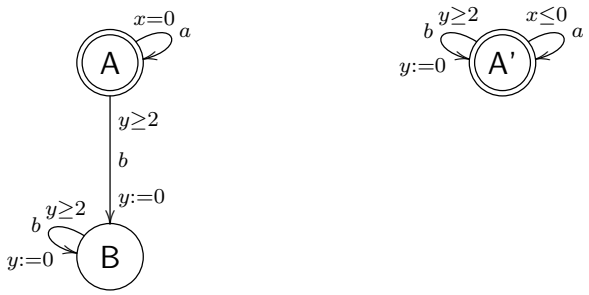
(i) The initial states are not timed bisimilar. A winning strategy for the attacker is to play $(A, [x = 0]) \xrightarrow{2.5} (A, [x = 2.5])$ which clearly can not be matched from $(A', [x = 0])$ due to the invariant.

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

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

(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.



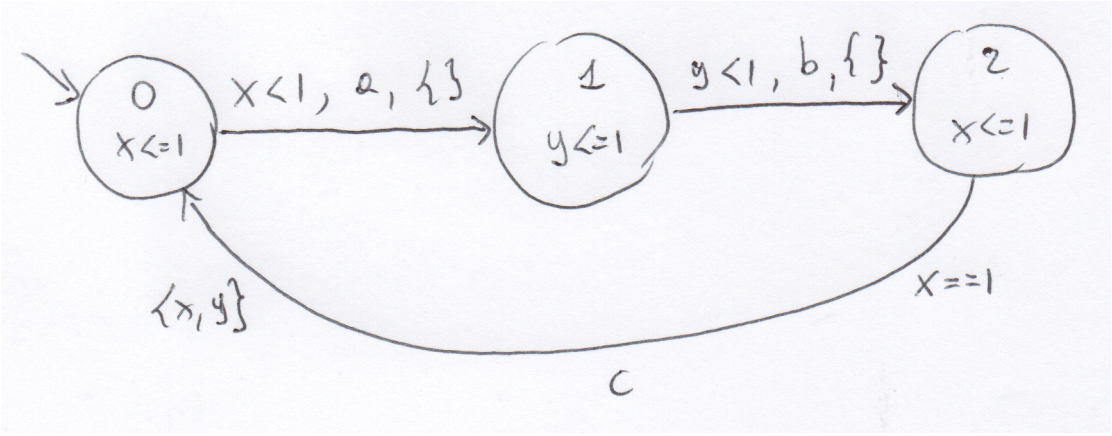
(i) The initial states are timed bisimilar. A bisimulation relating them is:

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

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

3 Region Graph and Zone Graph

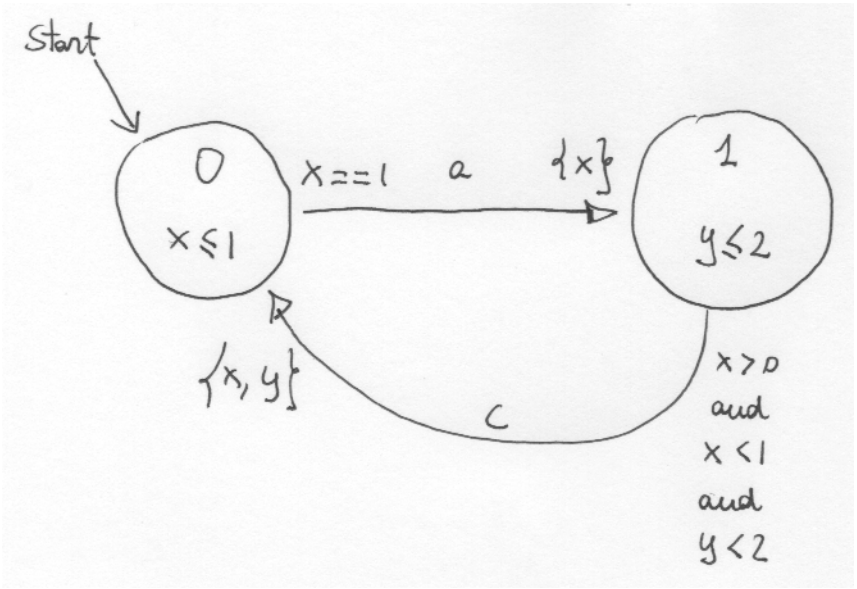
Exercise 3.1 *Consider the following timed automaton:*



1. *Draw the entire region graph of the automaton.*
2. *Determine if state* $(1, [x = 0.75, y = 0.75])$ *is reachable from the initial state.*

You can omit to draw transitions $\stackrel{\varepsilon}{\Longrightarrow}$ *that can be entailed by considering the reflexive and transitive closure of the drawn relation* $\stackrel{\varepsilon}{\Longrightarrow}$.

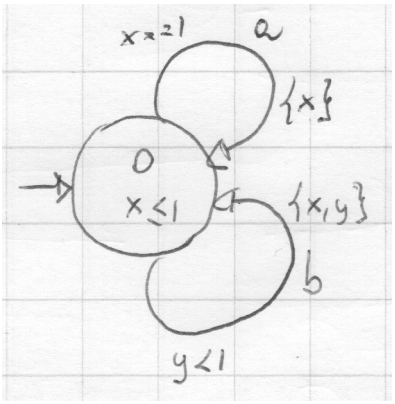
Exercise 3.2 *Consider the following timed automaton:*



1. *Draw the entire region graph of the automaton.*
2. *Determine if state* $(1, [x = 0.3, y = 0.7])$ *is reachable from the initial state.*

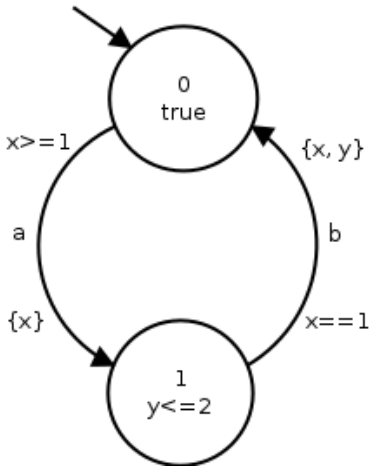
You can omit to draw transitions $\stackrel{\varepsilon}{\Longrightarrow}$ *that can be entailed by considering the reflexive and transitive closure of the drawn relation* $\stackrel{\varepsilon}{\Longrightarrow}$.

Exercise 3.3 *Draw the entire region graph of the following timed automaton:*



You can omit to draw transitions $\stackrel{\varepsilon}{\Longrightarrow}$ *that can be entailed by considering the reflexive and transitive closure of the drawn relation* $\stackrel{\varepsilon}{\Longrightarrow}$.

Exercise 3.4 *Consider the following timed automaton:*

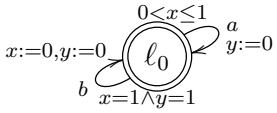


Draw the entire region graph of the automaton. You can omit to draw transitions $\stackrel{\varepsilon}{\Longrightarrow}$ *that can be entailed by considering the reflexive and transitive closure of the drawn relation* $\stackrel{\varepsilon}{\Longrightarrow}$.

Exercise 3.5 *Let* $C = \{x, y\}$ *be a set of clocks such that* $c_x = 2$ *and* $c_y = 2$.

- *Draw a picture with all regions for the clocks* x *and* y.
- *How many different regions there are on the picture?*
- *Select four different regions (corner point, line, two areas) and describe them via clock constraints.*
- *Try to find a general formula which describes a number of regions for two clocks and arbitrary maximal constants* c_x *and* c_y. *Solution:* $(c_x + 1)(c_y + 1) + 5c_xc_y + 3(c_x + c_y) + 3$

Exercise 3.6 *Draw a region graph of the following timed automaton.*

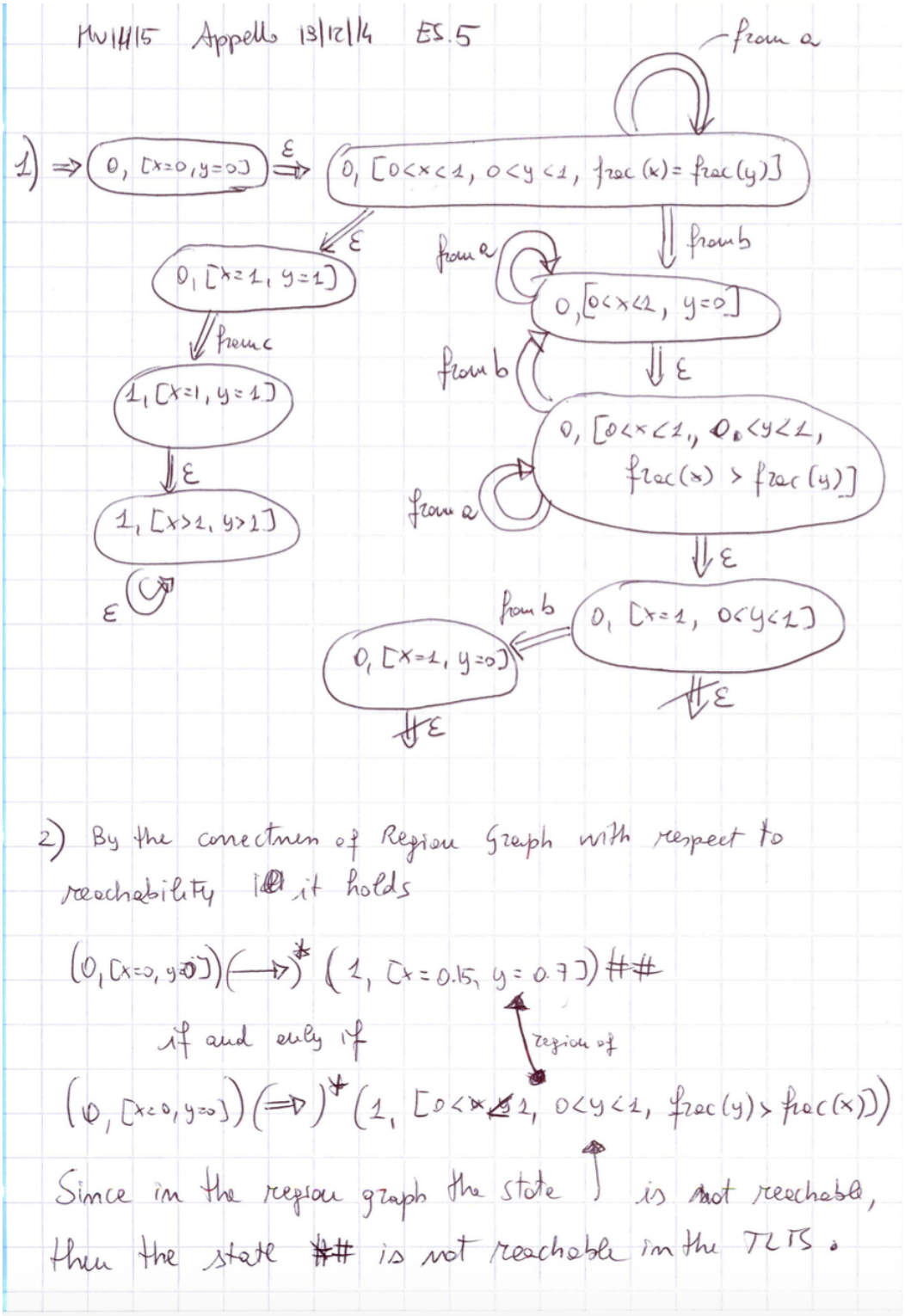


Using the region graph decide whether the following configurations

- (ℓ_0, v) *where* $v(x) = 0.7$ *and* $v(y) = 0.61$
- (ℓ_0, v) *where* $v(x) = 0.2$ *and* $v(y) = 0.41$

are reachable from the initial configuration.

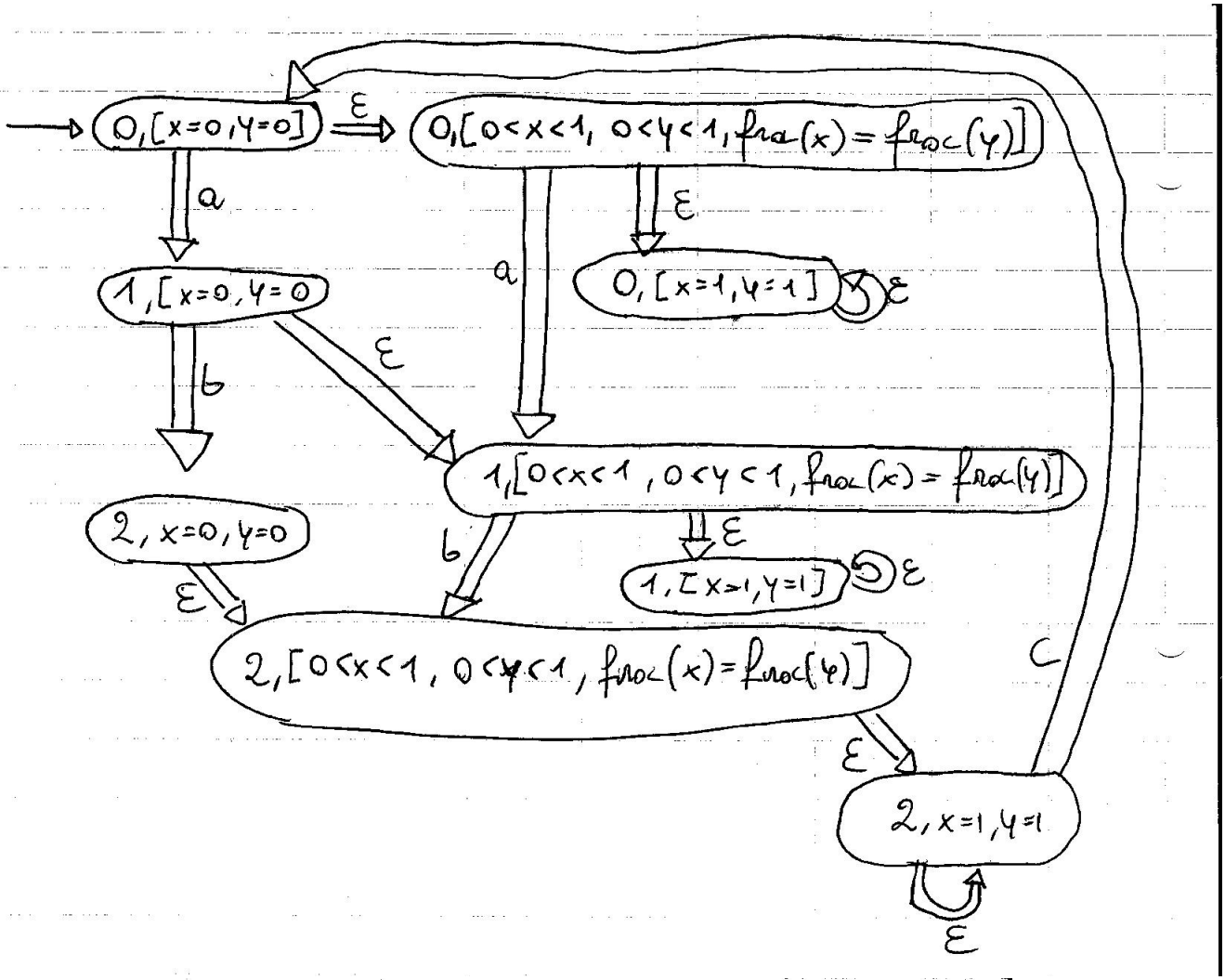
Exercise 3.7 *Consider the following timed automaton:*



1. **(5 points)** *Draw the entire region graph of the automaton.*
2. **(2 points)** *Determine if state* $(1, [x = 0.15, y = 0.7])$ *is reachable from the initial state.*

Solutions

Solution of Exercise 3.1



2) By the properties of the Region Graph

the state $(1, [x=0.75, y=0.75])$ is reachable if and only if the state $(1, [x=0.75, y=0.75]_{\equiv V})$ =

$= (1, [0<x<1, \quad 0<y<1, \quad frac(x) = frac(y)])$

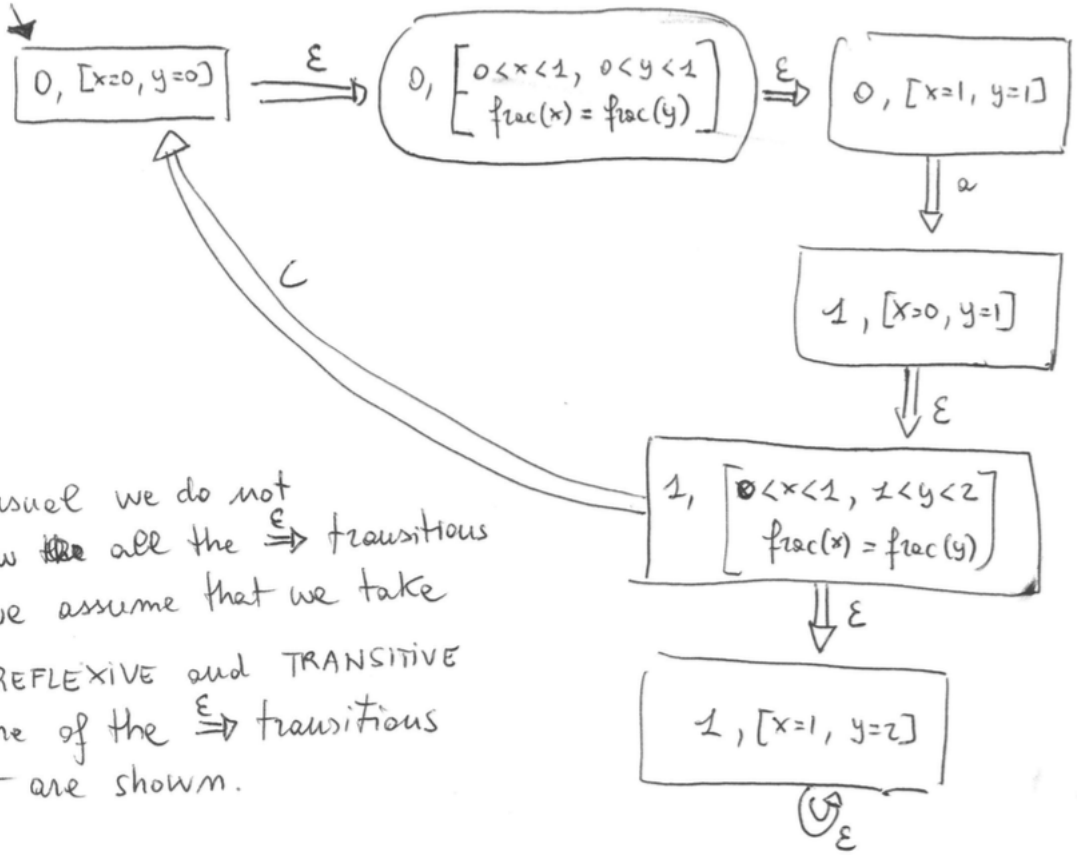
is reachable in the region graph.

Indeed this state can be reached in the region graph, so the answer is yes.

Solution of Exercise 3.2

The region graph of the given timed automaton is the following:

EX-1



As usual we do not draw all the $\stackrel{\varepsilon}{\Rightarrow}$ transitions as we assume that we take the REFLEXIVE and TRANSITIVE closure of the $\stackrel{\varepsilon}{\Rightarrow}$ transitions that are shown.

2. We know that (ℓ, v) is reachable in a TLTS derived from a timed automaton IF AND ONLY IF $(\ell, [v]_{\equiv_v})$ is reachable in the REGION GRAPH of the timed automaton.

Now, the region of the $v = [x = 0.3,\ y = 0.7]$ is

$[0<x<1,\ 0<y<1,\ \text{frac}(x) < \text{frac}(y)] = [v]_{\equiv}$

the state $[1, [v]_{\equiv}]$ is NOT REACHABLE in the Region Graph, therefore the state $[\ell, [x=0.3, y=0.7]]$ is NOT REACHABLE in the TLTS.

Solution of Exercise 3.5

Let $C = \{x, y\}$ be a set of clocks such that $c_x = 2$ and $c_y = 2$.

- All regions for the clocks x and y are depicted in Figure 1.
  - Graphical representation of the regions for clocks x and y.

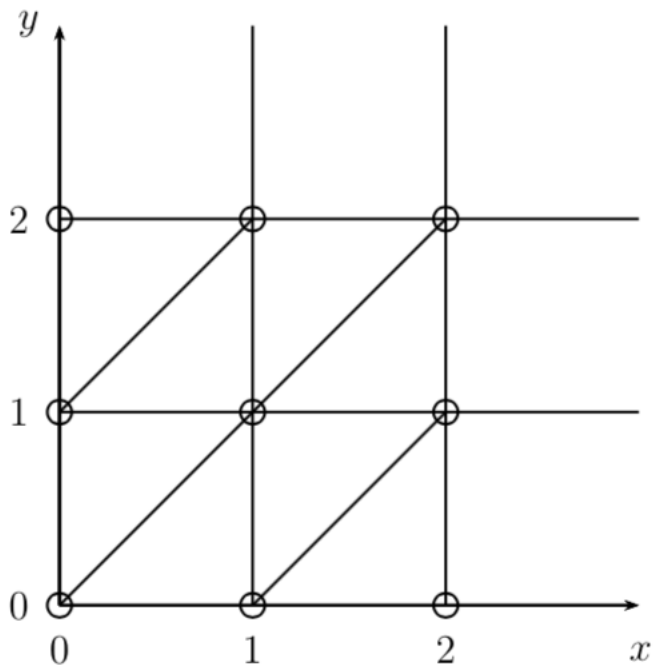
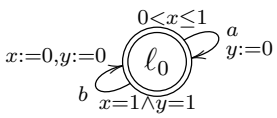


Figure 1: **Solution of Exercise 3.5**

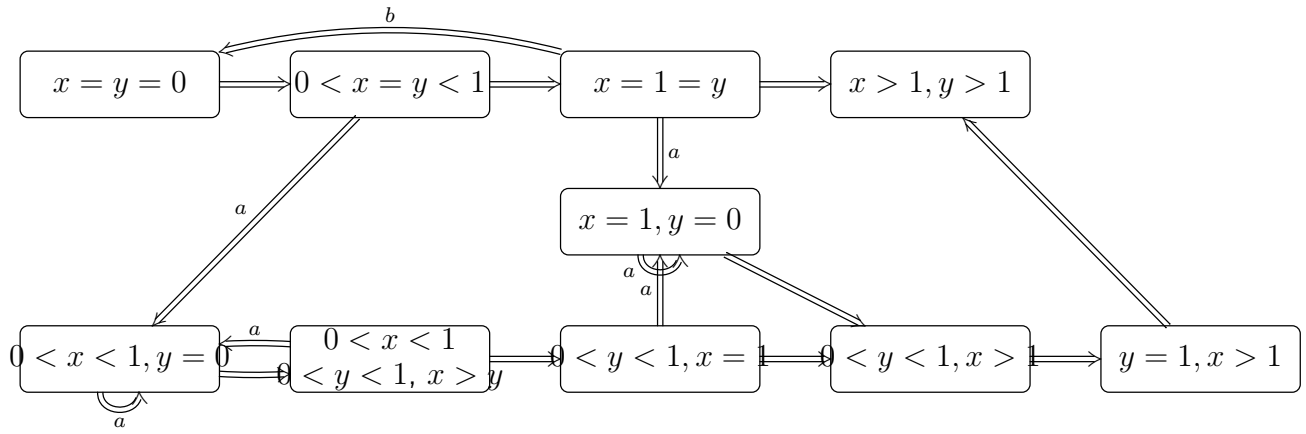
- How many different regions there are on the picture?
  - There are 9 corner points, 22 line segments, and 13 area regions.
- Select four different regions (corner point, line, two areas) and describe them via clock constraints.
  - Solution (for example): $[x = 0 \wedge y = 0], [0 < x < 1 \wedge 1 < y < 2 \wedge x + 1 = y], [0 < x < 1 \wedge 0 < y < 1 \wedge x < y]$, and $[1 < x < 2 \wedge 0 < y < 1 \wedge x > y + 1]$.
- Try to find a general formula which describes a number of regions for two clocks and arbitrary maximal constants c_x and c_y.
  - Solution: $(c_x + 1)(c_y + 1) + 5c_xc_y + 3(c_x + c_y) + 3$

Solution of Exercise 3.6

Draw a region graph of the following timed automaton.



Since there is only one location ℓ_0, it is omitted in symbolic states of the region graph.



Using the region graph decide whether the following configurations are reachable from the initial configuration.

- (ℓ_0, v) where $v(x) = 0.7$ and $v(y) = 0.61$
  - Solution: Yes, since the symbolic state

$$(\ell_0, [v]) = (\ell_0, 0 < x < 1 \wedge 0 < y < 1 \wedge x > y)$$

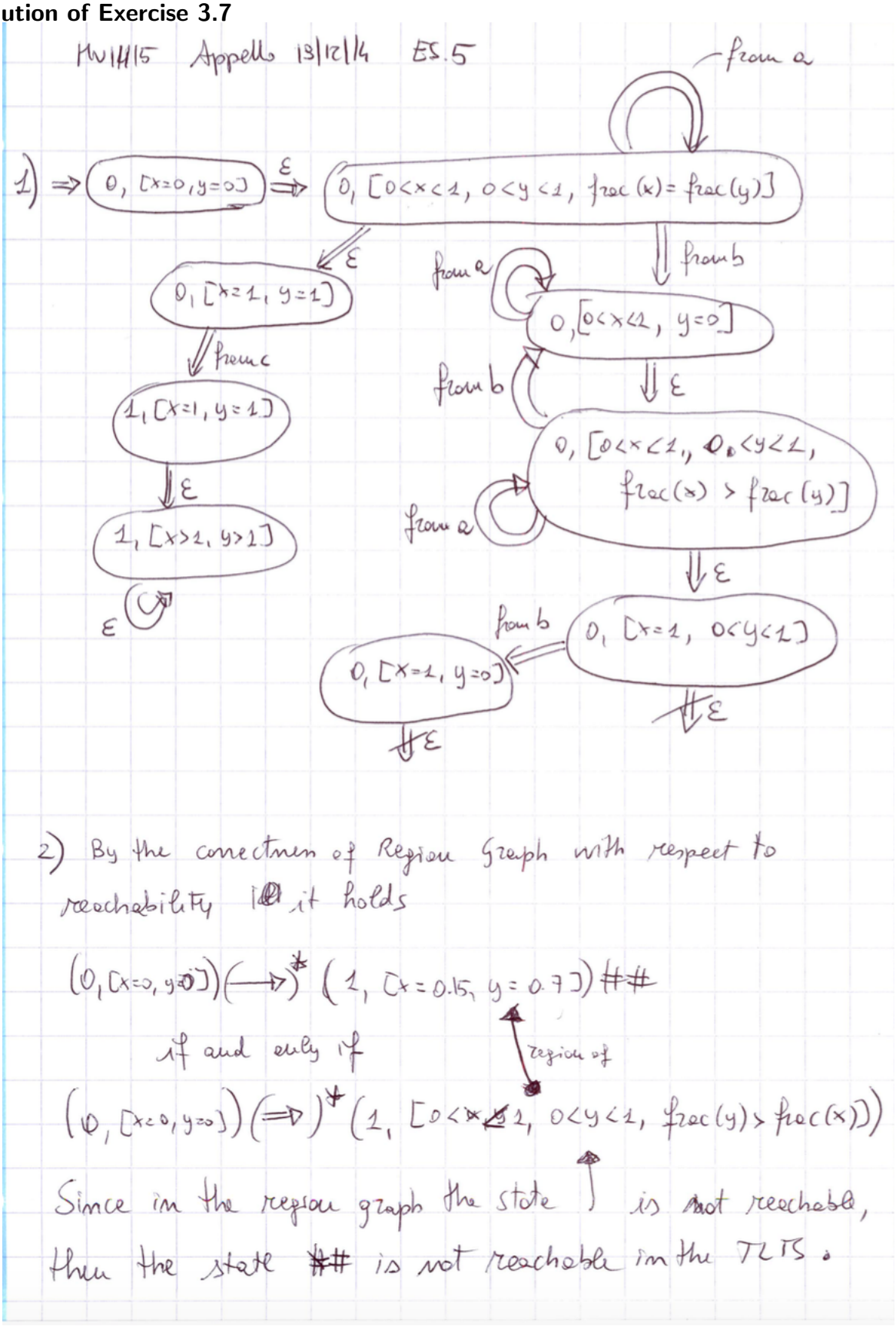
    is reachable from the initial symbolic state $(\ell_0, x = y = 0)$ of the region graph.

- (ℓ_0, v) where $v(x) = 0.2$ and $v(y) = 0.41$
  - Solution: No, since the symbolic state

$$(\ell_0, [v]) = (\ell_0, 0 < x < 1 \wedge 0 < y < 1 \wedge x < y)$$

    is *not* reachable from the initial symbolic state $(\ell_0, x = y = 0)$ of the region graph.

Solution of Exercise 3.7



2) By the correctness of Region Graph with respect to reachability it holds

$(0, [x=0, y=0]) (\longrightarrow)^* (1, [x=0.15, y=0.7])$ ##

if and only if

region of

$(0, [x=0, y=0]) (\Longrightarrow)^* (1, [0<x<1, 0<y<1, frac(y) > frac(x)])$

Since in the region graph the state ↑ is not reachable, then the state ## is not reachable in the TLTS.