

Advanced Model Checking Summer term 2014

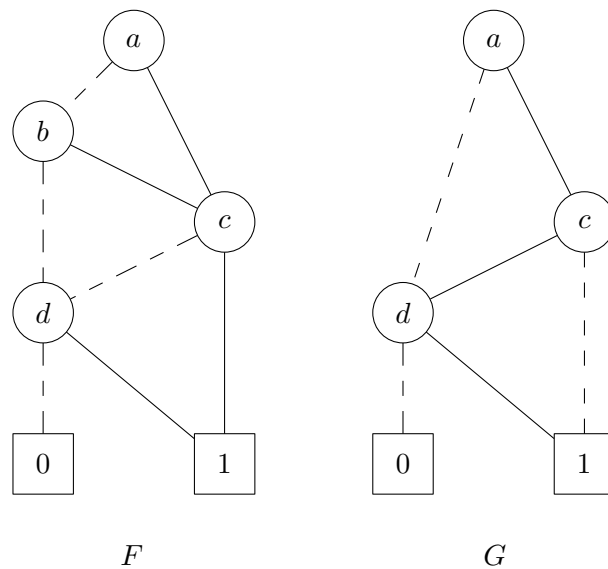
– Series 10 –

Hand in on **2 July** before the exercise class.

Exercise 1

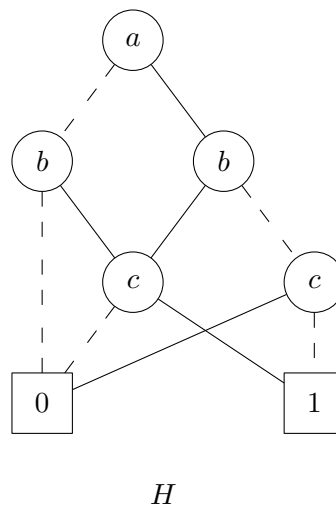
(4 points)

- a) Compute $F \vee G$ for the following ROBDDs F and G .



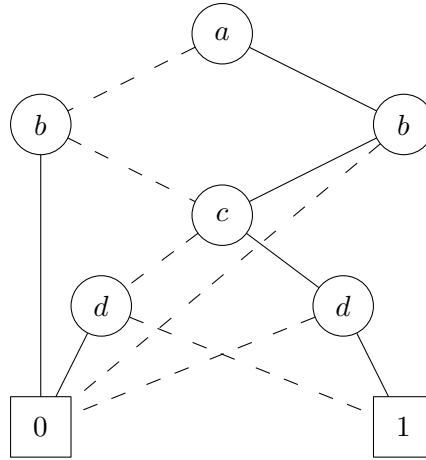
Provide the intermediate steps.

- b) Compute $H|_{b=1}$, given the ROBDD H below.



Provide the intermediate steps.

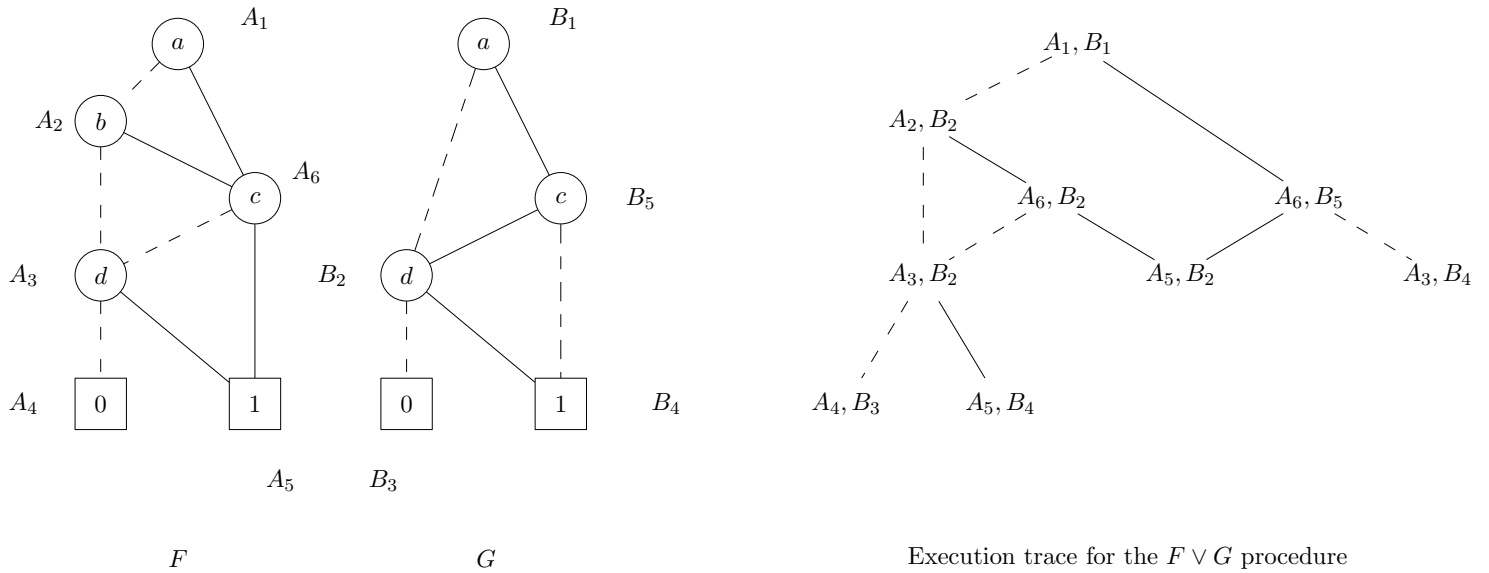
- c) Compute $\exists a.(\exists d.f(a,b,c,d))$ in the form of an ROBDD for the function f defined by the ROBDD below.



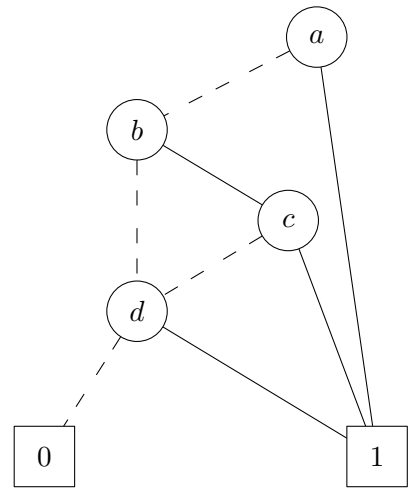
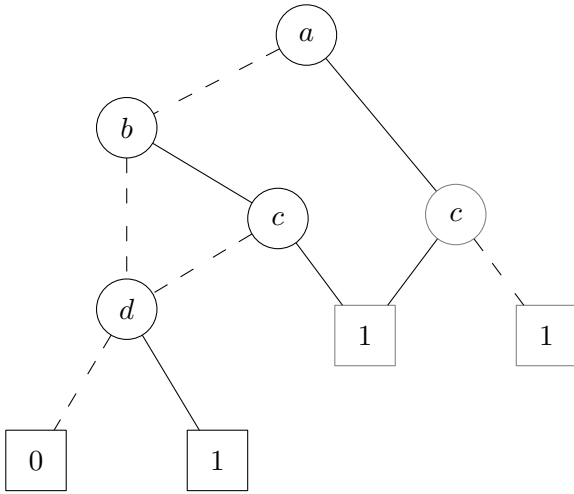
Provide intermediate steps.

Solution:

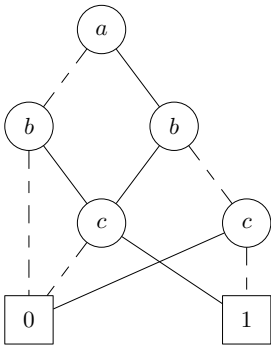
- a) First consider the execution trace of the $F \vee G$ procedure without the reduction step (on the left):



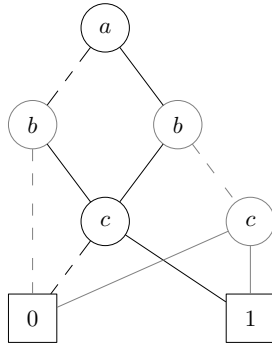
Now the resulting BDD is on the left, then after the reduction step is applied we eliminate the gray nodes and obtain the ROBDD which is on the right:



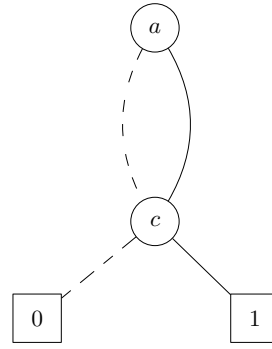
b) The solution steps are as follows, from left to right:



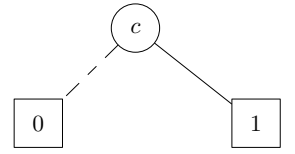
Step: Initial



Step: Second

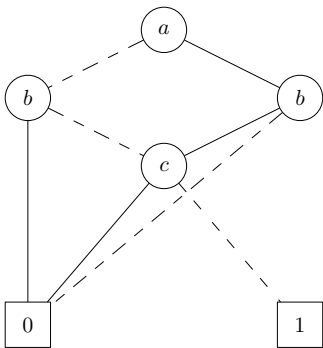


Step: Third

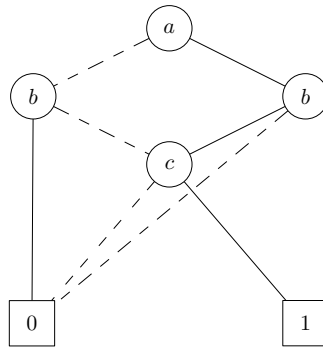


Step: Initial

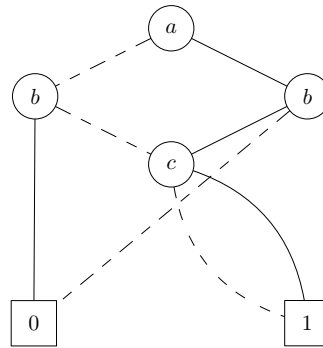
c) First consider computation of $\exists d.f(a,b,c,d)$ from left to right:



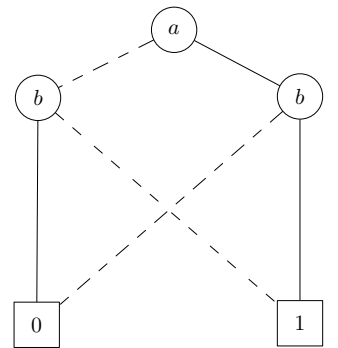
First (H_1): Restrict d to 0



Second (H_2): Restrict d to 1

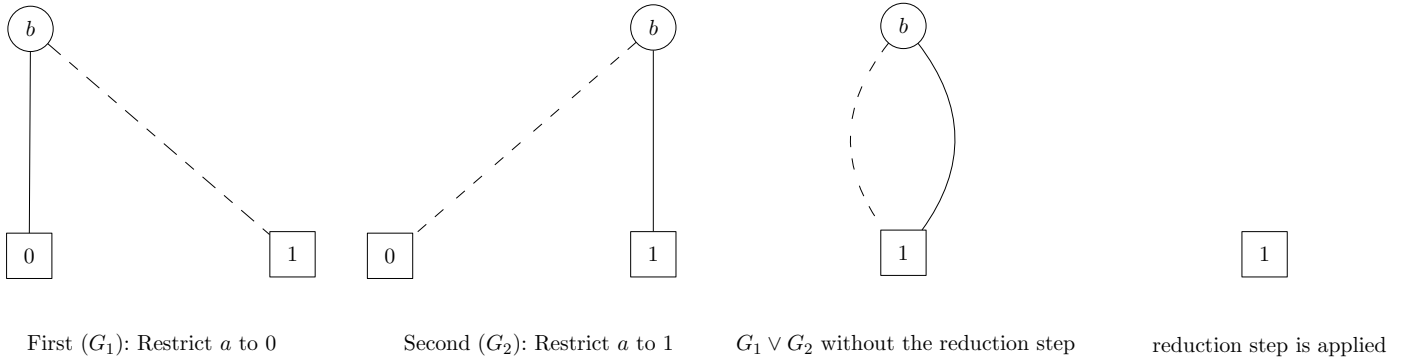


$H_1 \vee H_2$ without the reduction step



reduction step is applied

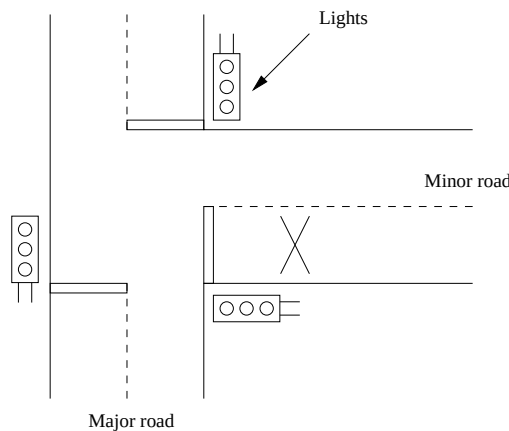
The next figure shows the computation for $\exists a.(\exists d.f(a,b,c,d))$:



Exercise 2

(4 points)

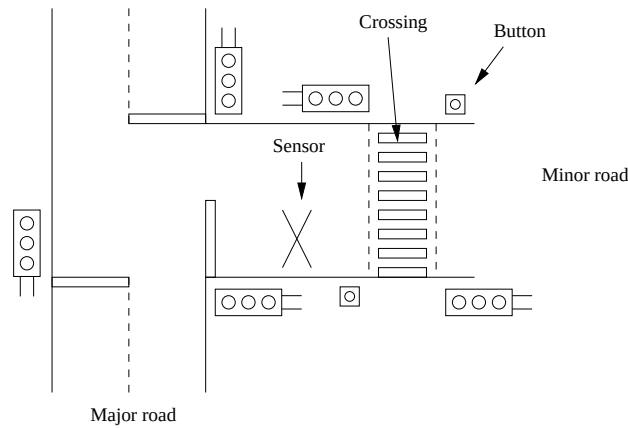
A control system must ensure the safe and correct functioning of a set of traffic lights at a T-junction between a major and a minor road. The lights will be set to green on the major road and red on the minor road unless a vehicle is detected by a sensor in the road just before the lights on the minor road. In this case the lights will be switchable in the standard manner and allow traffic to leave the minor road. After a suitable interval the lights will revert to their default position to allow traffic to flow on the major road again. Once a vehicle is detected the sensor will be disabled until the minor-road lights are set to red again. A sketch of the T-junction is provided below.



Questions:

- First we ignore all timing issues involved and concentrate on the qualitative aspects of the behavior of the traffic lights. Model the above system as a network of (timed) automata. For convenience, you may assume that the two major-road lights are fully synchronized and can be modeled as a single light. Complement your system model by adding a process that regulates the arrival of cars in the minor road.
- Adapt your model so as to incorporate the following timing constraints. Deal with each timing constraint separately so as to reduce the complexity. Indicate for each timing constraint the necessary adaptations to your un-timed model:
 - a minor-road light stays on green for 30 seconds
 - all interim lights stay on for 5 seconds
 - there is a one second delay between switching one light off and another on (e.g. switching from red to yellow)

- (d) the major-road lights must be on green for at least 30 seconds in each cycle
- (e) (More involved.) but must respond to the sensor immediately after that.
- c) We extend the T-junction in the following way. Suppose there is a pedestrian crossing a short distance down the minor road but beyond the sensor. There is a button on each side of the road for pedestrians to indicate they wish to cross. The crossing should only allow people to cross when the ‘minor lights’ are set to red in order to minimize waiting times for traffic on the minor road. The new situation is sketched below.



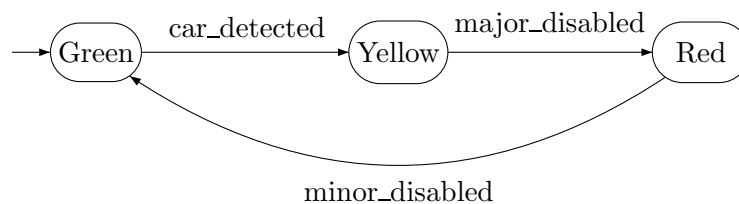
Extend your timed model of the previous question in order to cope with this new situation.

- d) Does the crossing indeed only allow pedestrians to cross when the ‘minor lights’ are set to red?

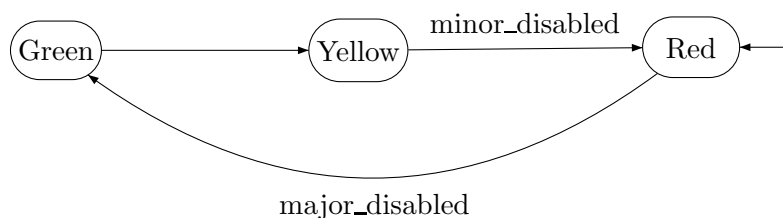
Solution:

- a) The Timed automata are:

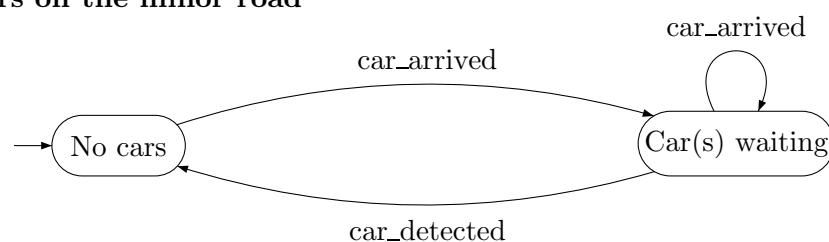
Major-road lights



Minor-road lights



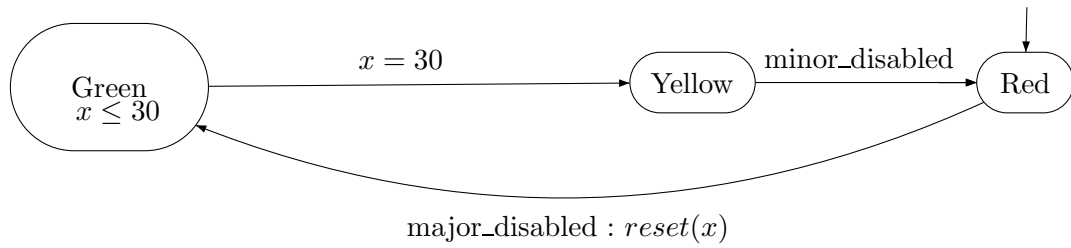
Cars on the minor road



b) Required adaptations:

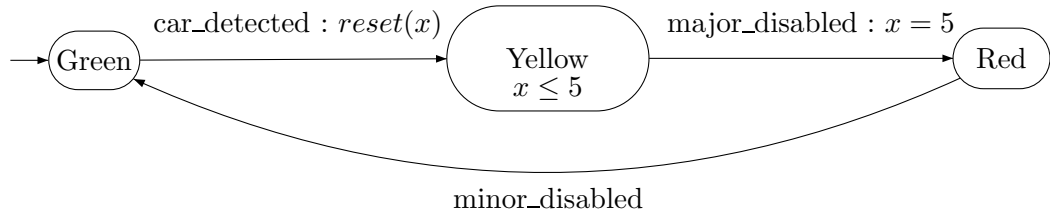
(a) A Minor light stays on green for 30 seconds:

Minor-road lights

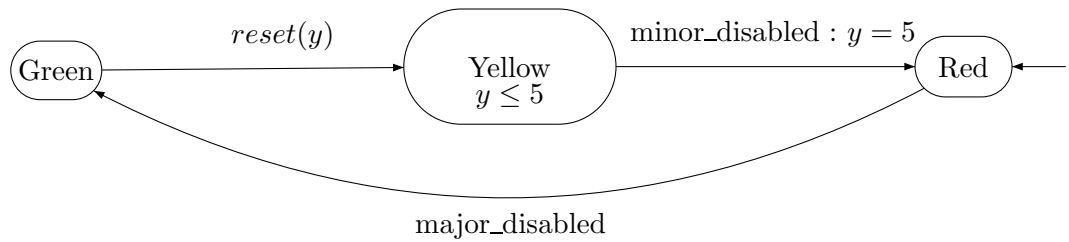


(b) All interim lights stay on for 5 seconds:

Major-road lights

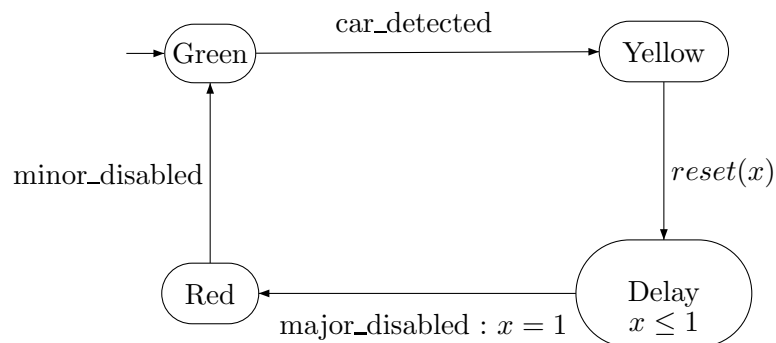


Minor-road lights



(c) The one second delay between switching the lights:

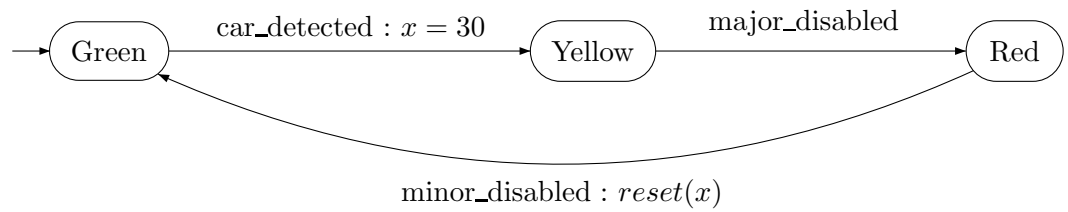
Major-road lights



Here for the Major-road light, for switching from red to green, the rest are similar.

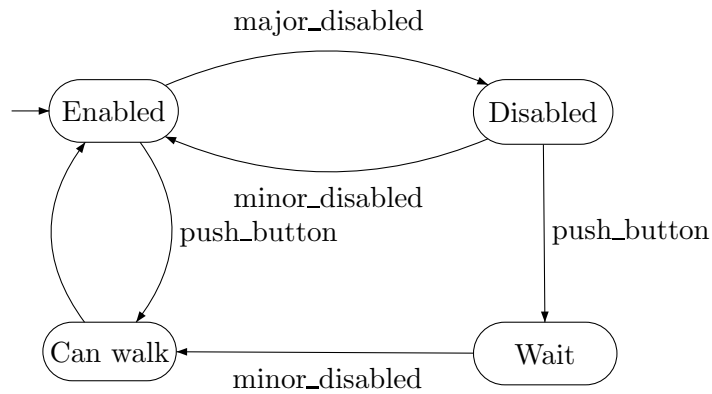
(d) The Major-road lights must be on green for at least 30 seconds:

Major-road lights



- (e) but must respond to the sensor immediately after that: The same as for the previous point. We can not enforce responding to the sensor immediately after the time has elapsed because the sensor is incorporated by the means of labels and synchronization over them.

c) Pedestrian:

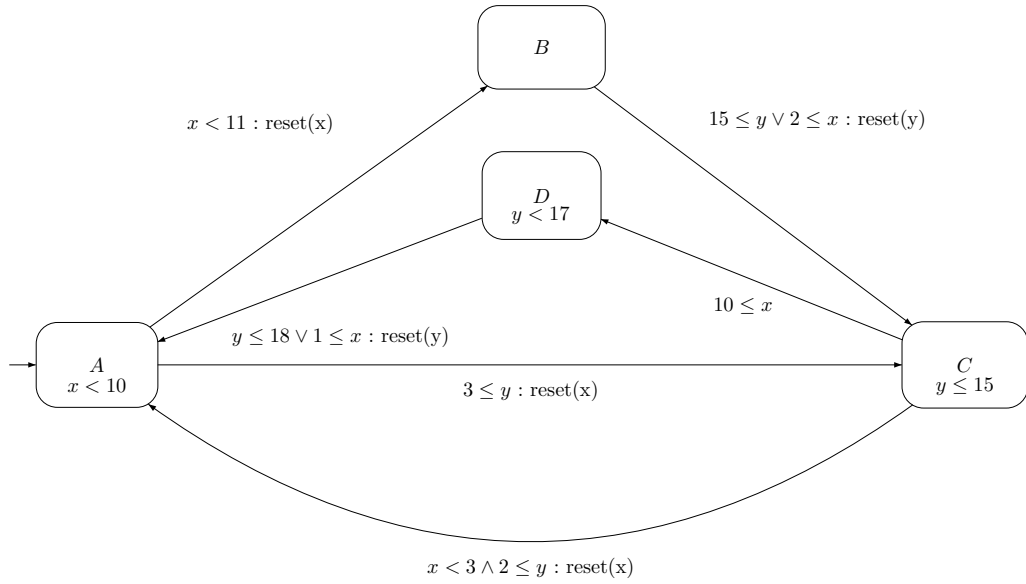


- d) Does the crossing indeed only allows pedestrians to cross when the ‘minor lights’ are set to red? **Yes**, since we allow walking only after the red light for the minor road is ON. Which is ensured by synchronization of automata by labels ‘major_disabled’ and ‘minor_disabled’.

Exercise 3

(2 points)

For the timed automaton below, check whether it is (a) non-zeno and (b) timelock-free.



Solution: The state of the underlying $TS(TA)$ is represented as $\langle l, x, y \rangle$ where l stands for a location name.

(a) The given TA exhibits Zeno behavior since the following infinite time-convergent path exists:

$$\langle A, 0, 0 \rangle \xrightarrow{4} \langle A, 4, 4 \rangle \longrightarrow \langle C, 0, 4 \rangle \longrightarrow \langle A, 0, 4 \rangle \longrightarrow \langle C, 0, 4 \rangle \longrightarrow \dots$$

(b) The given TA is not Timelock-free since $Paths_{div}(\langle D, 18, 16 \rangle) = \emptyset$. This state is reachable by the following path:

$$\begin{aligned} &\langle A, 0, 0 \rangle \xrightarrow{5} \langle A, 5, 5 \rangle \longrightarrow \langle B, 0, 5 \rangle \xrightarrow{2} \langle B, 2, 7 \rangle \longrightarrow \\ &\langle C, 2, 0 \rangle \xrightarrow{8} \langle C, 10, 8 \rangle \longrightarrow \langle D, 10, 8 \rangle \xrightarrow{8} \langle D, 18, 16 \rangle \end{aligned}$$