Tutorial 7: Timed & Hybrid Automata

CS60030 Formal Systems

PALLAB DASGUPTA,
FNAE, FASc,
A K Singh Distinguished Professor in AI,
Dept of Computer Science & Engineering
Indian Institute of Technology Kharagpur
Email: pallab@cse.iitkgp.ac.in
Web: http://cse.iitkgp.ac.in/~pallab

INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

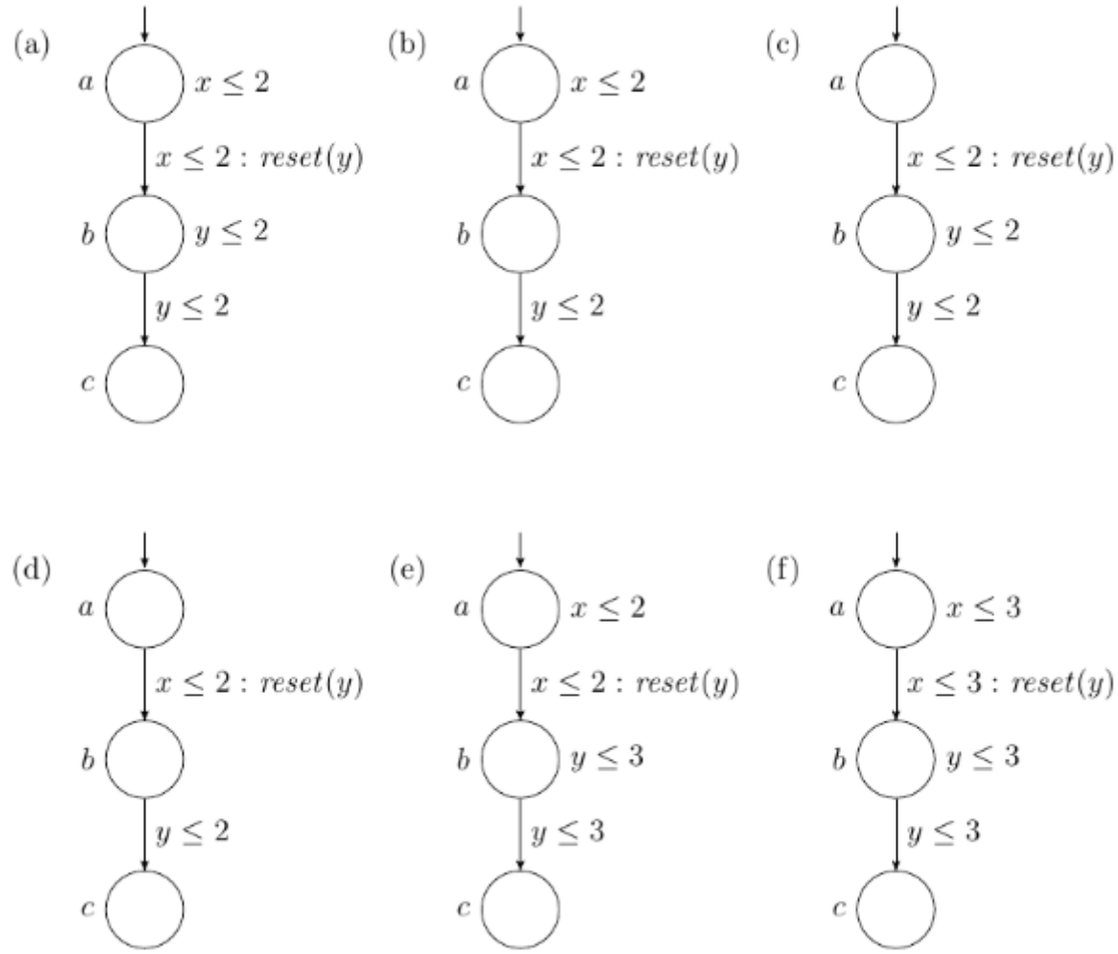
FMSAFE

FORMAL METHODS FOR SAFETY CRITICAL SYSTEMS

TCTL

Which formula is true in which automaton?

1. $AF_{\leq 4}\, c$
2. AFEG b
3. $(AF_{\leq 5}\, c) \wedge (EG_{\leq 5}\, \neg c)$
4. (EG a) ^ (EFEG b)
5. (EG a) ^ (¬ EFEG b)
6. $(AF_{\leq 6}\, c) \wedge (EG_{\leq 6}\, \neg c)$



Answer:

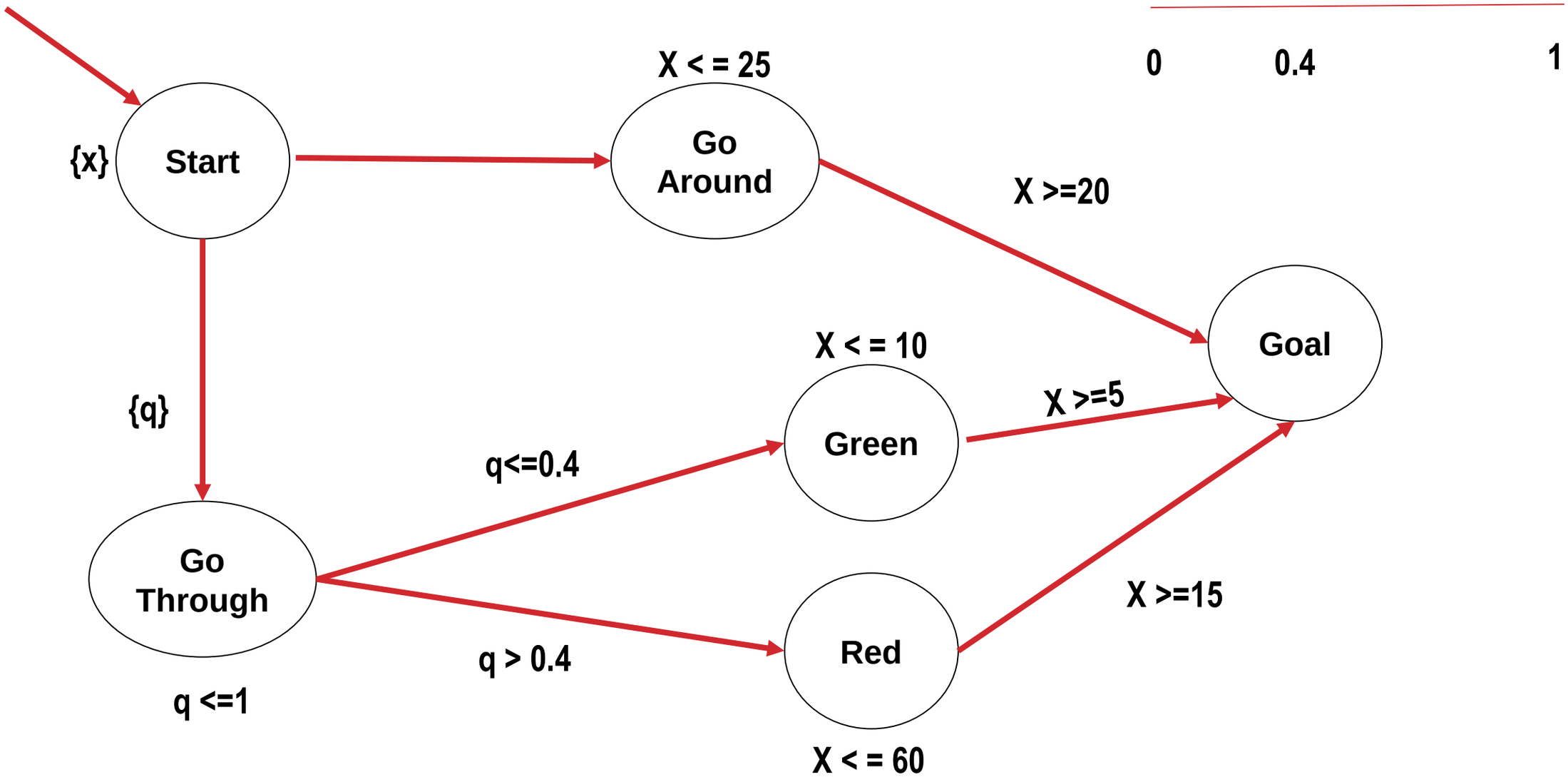
1-(a) 2-(b) 3-(e) 4-(d) 5-(c) 6-(f)

Modelling Timed Automata

1. Consider the following problem of modeling a car approaching a town, the driver can choose to go around the town or through it. In the town there is a signal controlled crossing. If the driver is lucky the light will be green, and if he is unlucky the light will be red.

   If he chooses to go around the town the time it will take will be chosen from a uniform distribution between 20 and 25. If the driver chooses to go through the town there is 0.4 probability that the lights are green and 0.6 probability that they will be red. The time to reach Goal are again chosen from uniform distributions; 5 to 10 for Green and 15 to 60 for Red. Model this problem using a timed automata.

Solution

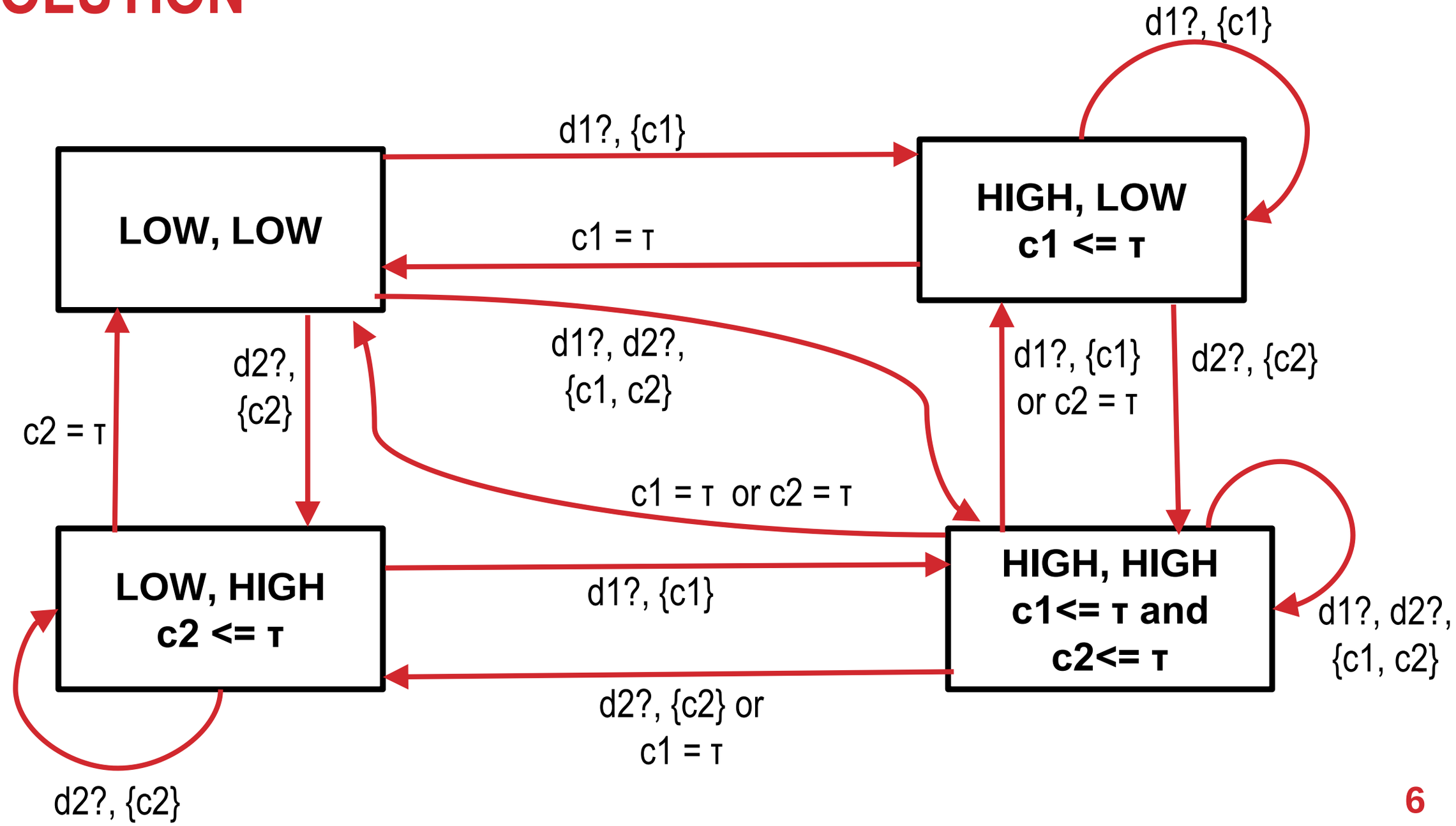

0
0.4
1
X < = 25
{x}
Start
Go
Around
X >=20
Goal
X < = 10
{q}
Green
X >=5
q<=0.4
Go
Through
q > 0.4
Red
X >=15
q <=1
X < = 60

Modelling Timed Automata

2. Consider two plants P1 and P2 each having two modes of operation HIGH and LOW depending on their sampling frequencies.

Consider that the controllers for both the plants are scheduled together in a processor and the events d1, d2 represent the scenario that high valued disturbances are being experienced by P1 and P2 respectively. It is recommended that whenever a plant is detected to face high disturbances, it switches to a HIGH mode. After τ ms from the time when the disturbance is found to be absent, the controller for the plant is switched to the LOW mode. Encode the entire uniprocessor scheduling scenario using a Timed Automata

SOLUTION


d1?, {c1}
LOW, LOW
d1?, {c1}
HIGH, LOW
c1 <= τ
c1 = τ
d1?, d2?,
{c1, c2}
d2?,
{c2}
c2 = τ
d1?, {c1}
or c2 = τ
d2?, {c2}
c1 = τ or c2 = τ
LOW, HIGH
c2 <= τ
d1?, {c1}
HIGH, HIGH
c1<= τ and
c2<= τ
d1?, d2?,
{c1, c2}
d2?, {c2} or
c1 = τ
d2?, {c2}

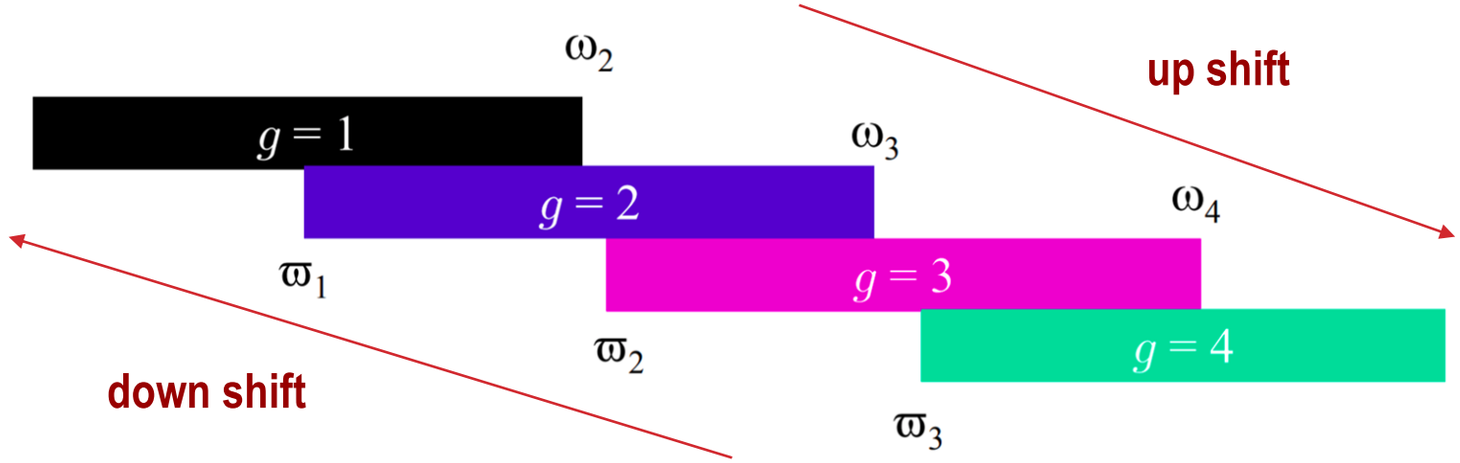
Modelling Hybrid Automata

Consider a semi-automatic transmission system in a car. The gear transmission can be done either manually (as per the drivers will) or automatically (as per the cars will). If the angular velocity crosses certain threshold the automatic transmission takes prominence. The diagram below shows the thresholds. The state dynamics of for i^{th} gear is as follows.

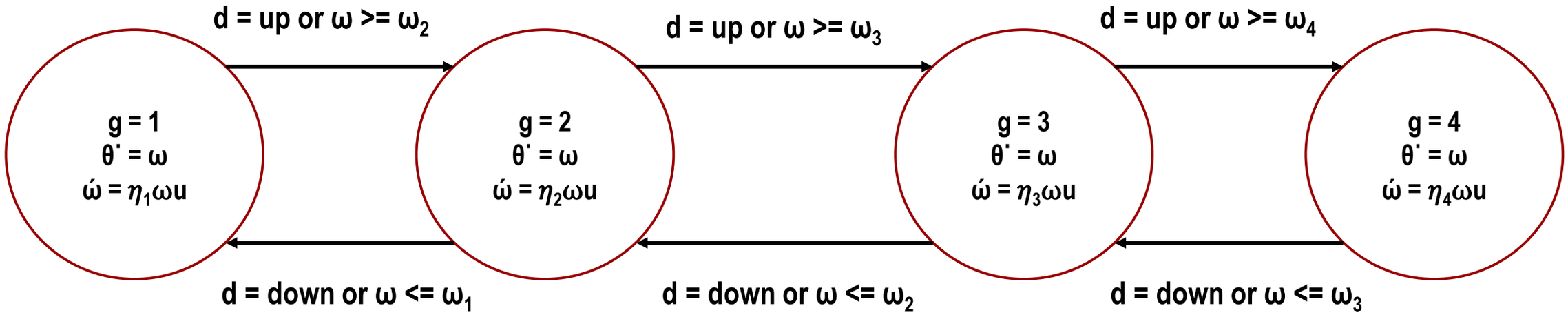
$\dot{\omega} = \eta_i \omega u$, where η_i is the gear ratio for i^{th} gear, $u \in [-1,1]$ is the throttle

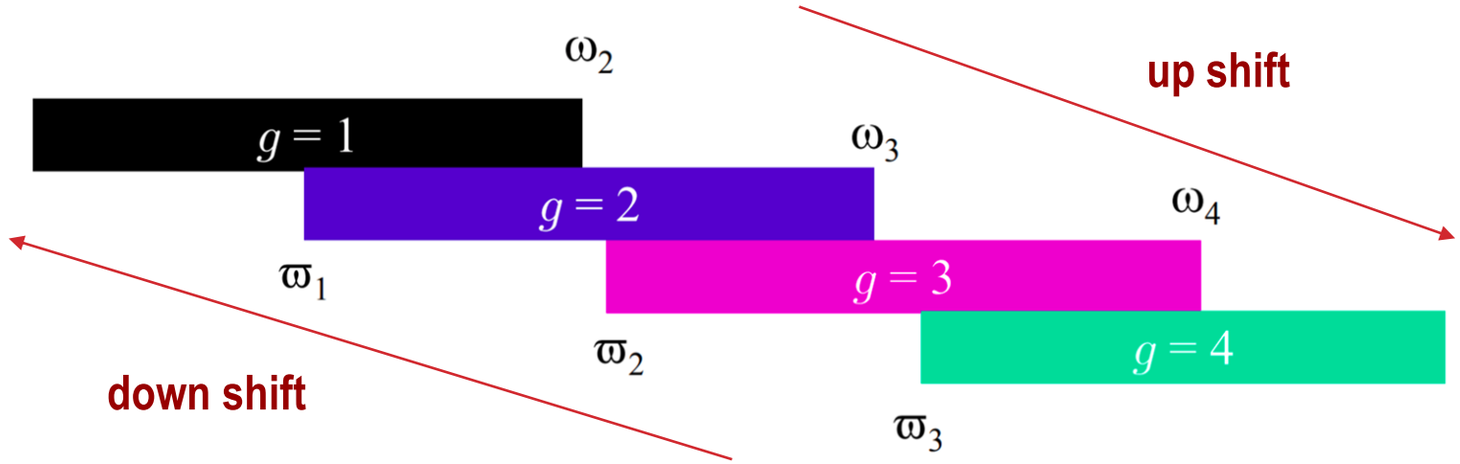
$d = \{up, down\}$ is the drivers input. Also the position is given by θ.

Design a hybrid automata to model the system.

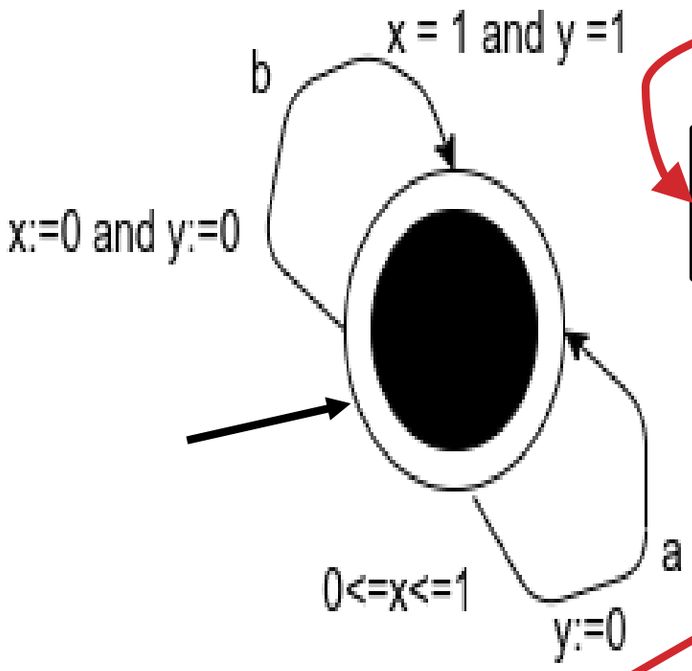


SOLUTION


d = up or ω >= ω2
d = up or ω >= ω3
d = up or ω >= ω4
g = 1
θ˙ = ω
ώ = η1ωu
g = 2
θ˙ = ω
ώ = η2ωu
g = 3
θ˙ = ω
ώ = η3ωu
g = 4
θ˙ = ω
ώ = η4ωu
d = down or ω <= ω1
d = down or ω <= ω2
d = down or ω <= ω3


ω2
up shift
g = 1
ω3
g = 2
ω4
ϖ1
g = 3
ϖ2
g = 4
down shift
ϖ3

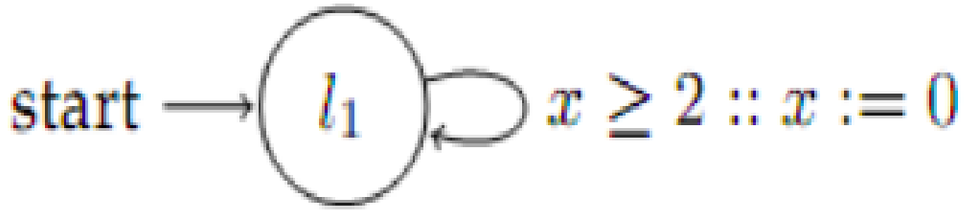
Region Graphs for Timed Automata



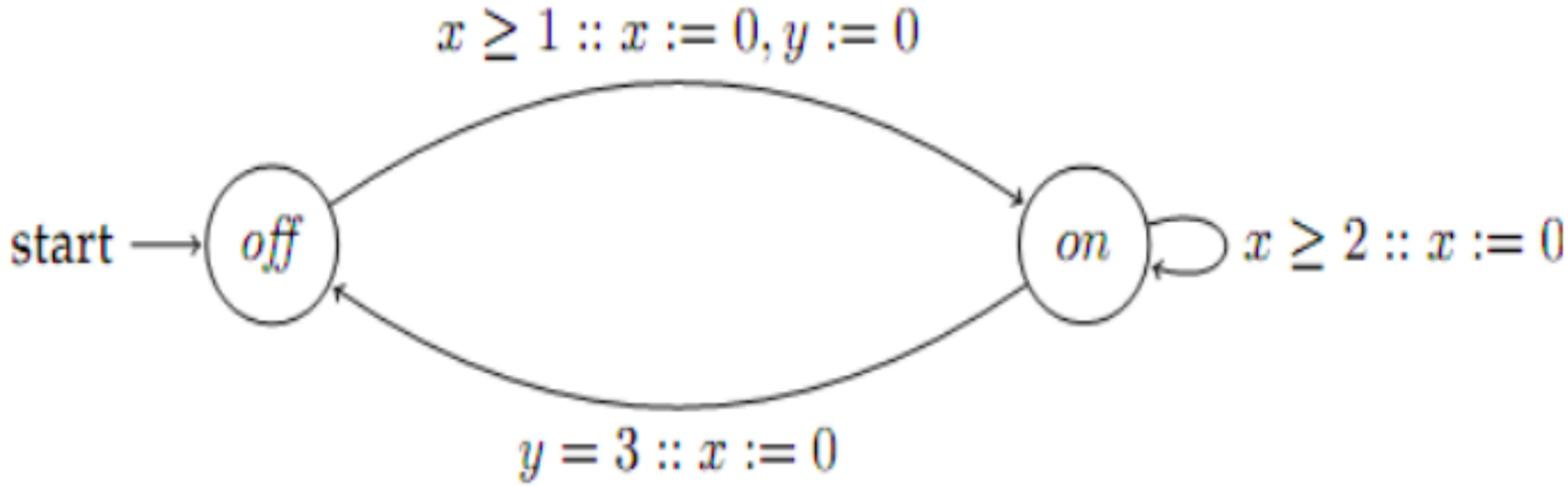
Region Graph For Timed Automata

Draw a region graph of the following timed automata.

1

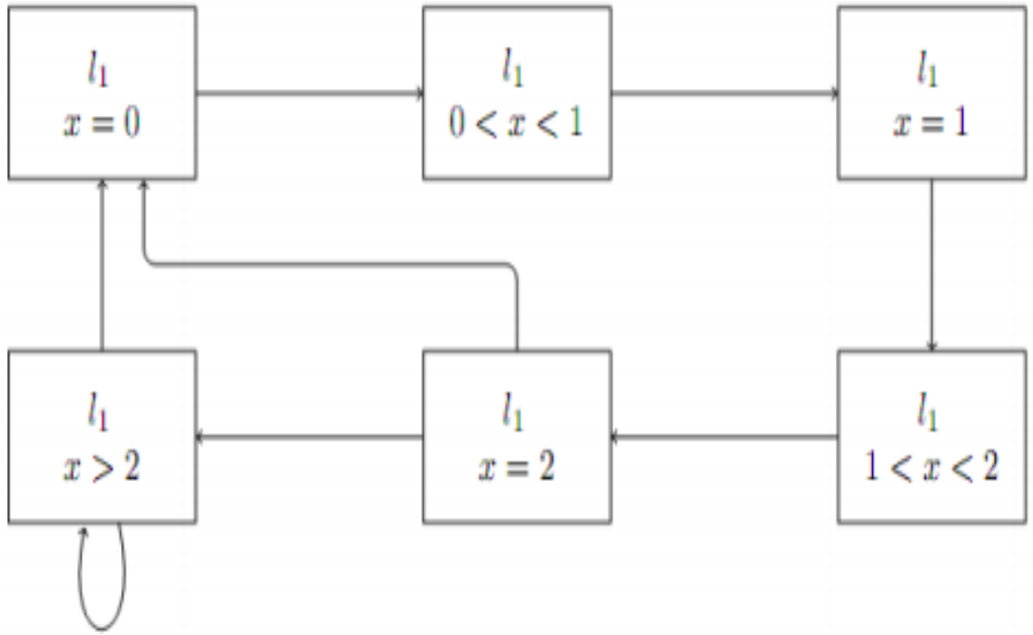


2



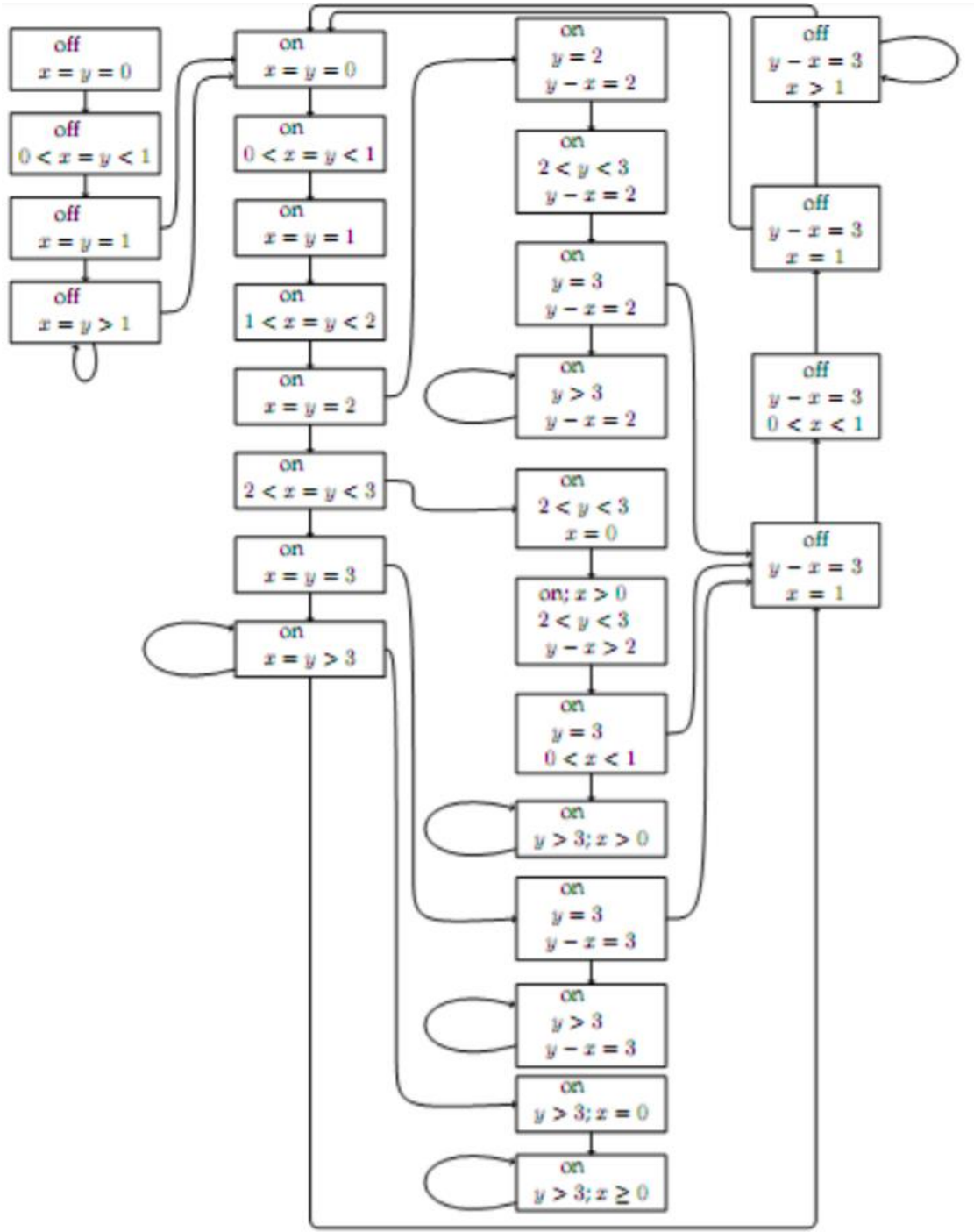
SOLUTIONS

1



SOLUTIONS

2

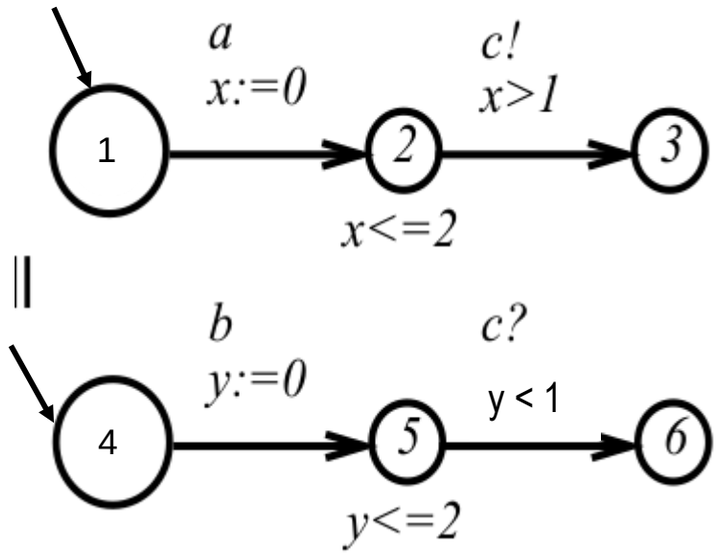

off
$x = y = 0$
off
$0 < x = y < 1$
off
$x = y = 1$
off
$x = y > 1$
on
$x = y = 0$
on
$0 < x = y < 1$
on
$x = y = 1$
on
$1 < x = y < 2$
on
$x = y = 2$
on
$2 < x = y < 3$
on
$x = y = 3$
on
$x = y > 3$
on
$y = 2$
$y - x = 2$
on
$2 < y < 3$
$y - x = 2$
on
$y = 3$
$y - x = 2$
on
$y > 3$
$y - x = 2$
on
$2 < y < 3$
$x = 0$
on; $x > 0$
$2 < y < 3$
$y - x > 2$
on
$y = 3$
$0 < x < 1$
on
$y > 3; x > 0$
on
$y = 3$
$y - x = 3$
on
$y > 3$
$y - x = 3$
on
$y > 3; x = 0$
on
$y > 3; x \geq 0$
off
$y - x = 3$
$x > 1$
off
$y - x = 3$
$x = 1$
off
$y - x = 3$
$0 < x < 1$
off
$y - x = 3$
$x = 1$

TIMELOCKS AND ZENO BEHAVIOUR

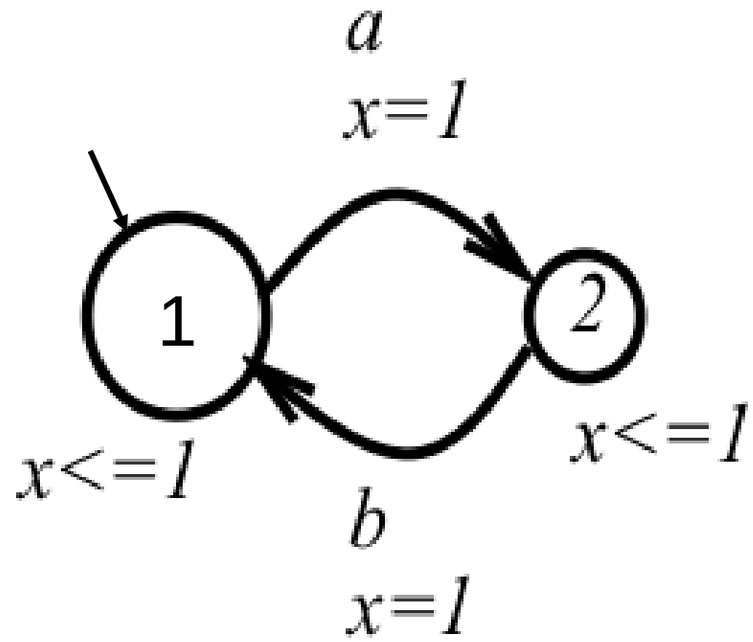
Study the given timed automata. Which one of them exhibit timelock?

Which one of them exhibits a zeno behaviour?

1

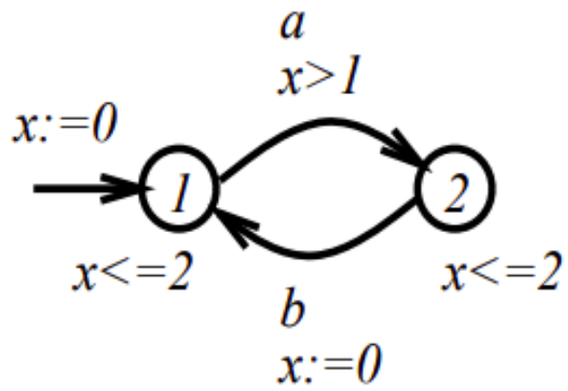


2

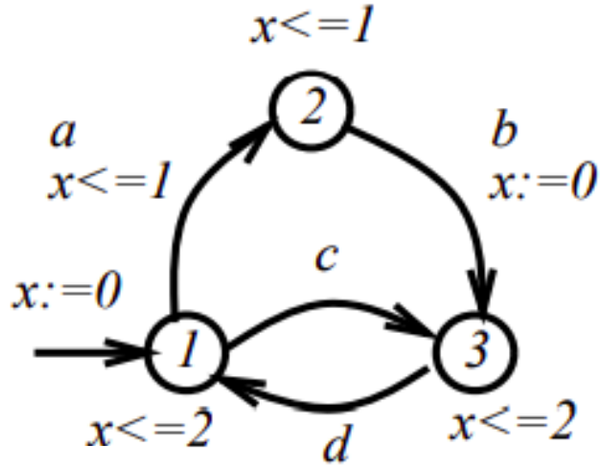


TIMELOCKS AND ZENO BEHAVIOUR

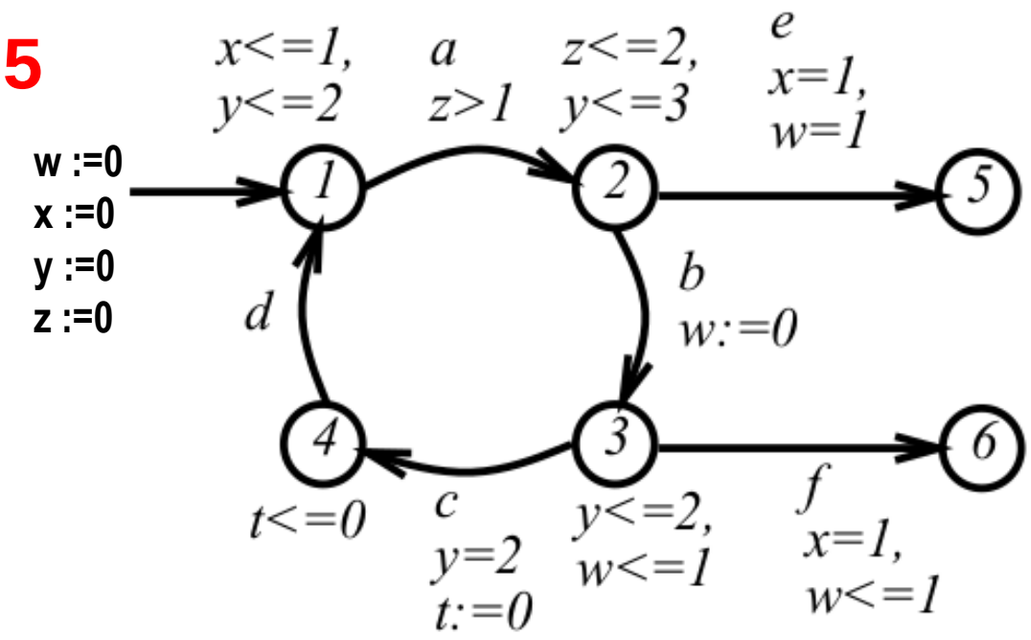
3



4



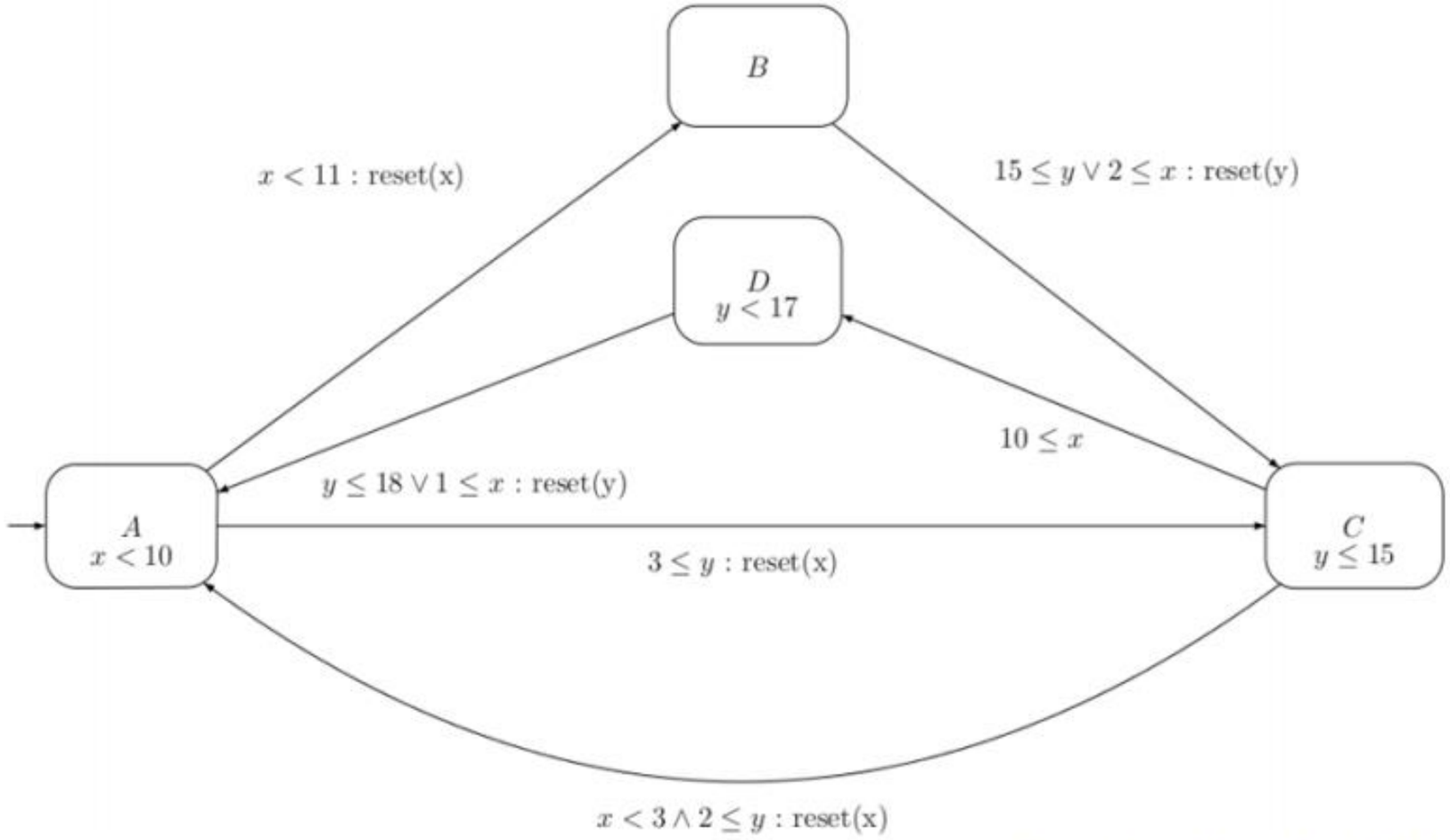
5



PRACTICE PROBLEMS

For the Timed-Automaton given below check whether it is:

1. Non-Zeno. 2. Timelock-Free.



PRACTICE PROBLEMS

Automobiles today have the features listed below. Implement each feature as a timed automaton.

1. The dome light is turned on as soon as any door is opened. It stays on for 30 seconds after all the doors are shut. What sensors are needed?

2. Once the engine is started, a beeper is sounded and a red warning light is indicated if there are passengers that have not buckled their seat belt. The beeper stops sounding after 30 seconds, or as soon as the seat belts are buckled, whichever is sooner. The warning light is on all the time the seat belt is unbuckled. Assume that the sensors provide a warn event when the ignition is turned on and there is a seat with passenger not buckled in, or if the ignition is already on and a passenger sits in a seat without buckling the seatbelt. Assume further that the sensors provide a noWarn event when a passenger departs from a seat, or when the buckle is buckled, or when the ignition is turned off.