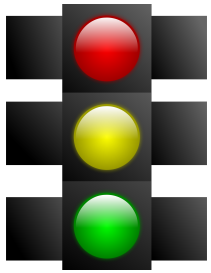
Unit-12: Modeling timing constraints

B. Srivathsan

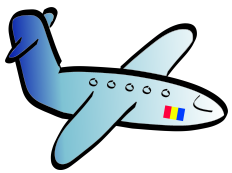
Chennai Mathematical Institute

NPTEL-course

July - November 2015



Traffic lights controller



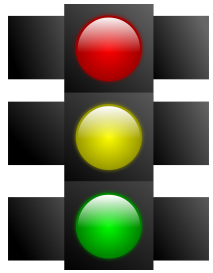
Flight control

Automatic gear control

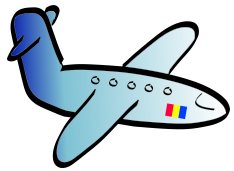
ATM

Pacemaker

Controllers need to adhere to **strict timing constraints**



Traffic lights controller



Flight control

Automatic gear control

ATM

Pacemaker

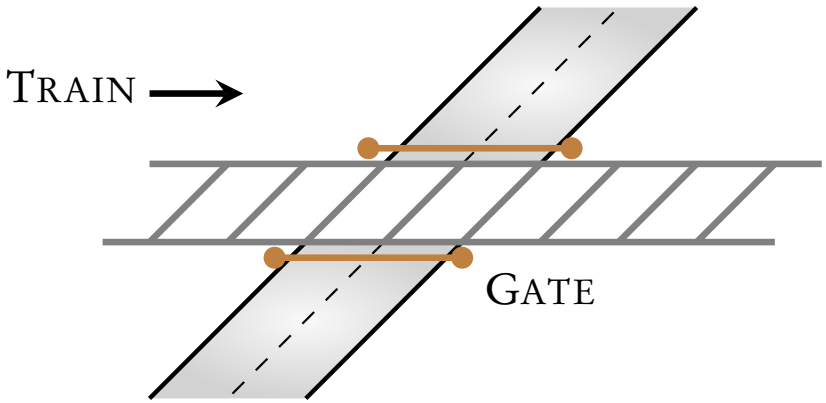
eg. when request for gear change is made, response should be within 1s

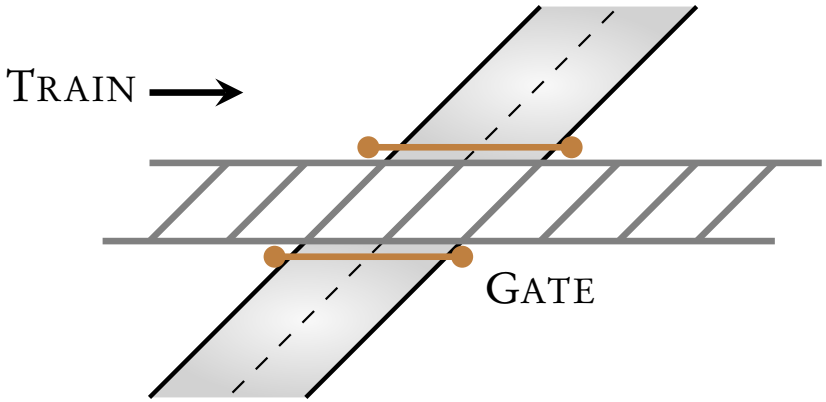
Controllers need to adhere to **strict timing constraints**

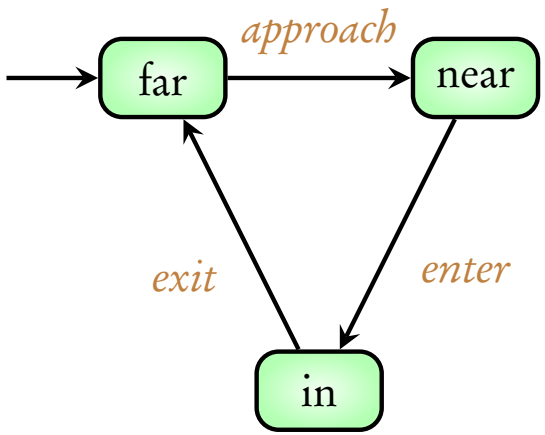
How do we model-check **systems with timing** constraints?

Adding time to transition systems

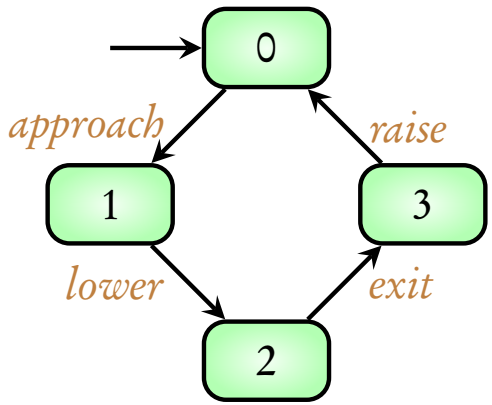
Example 1


TRAIN
GATE

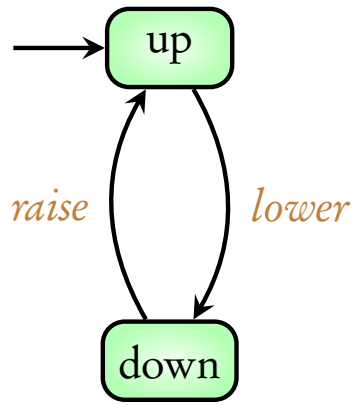




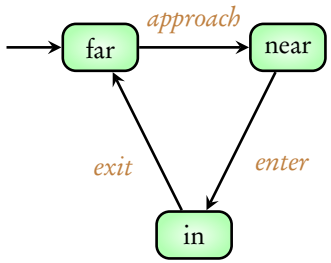
Train



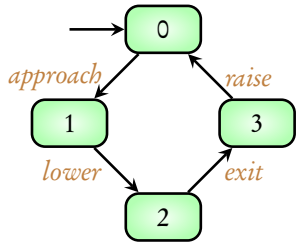
Controller



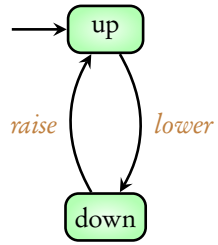
Gate



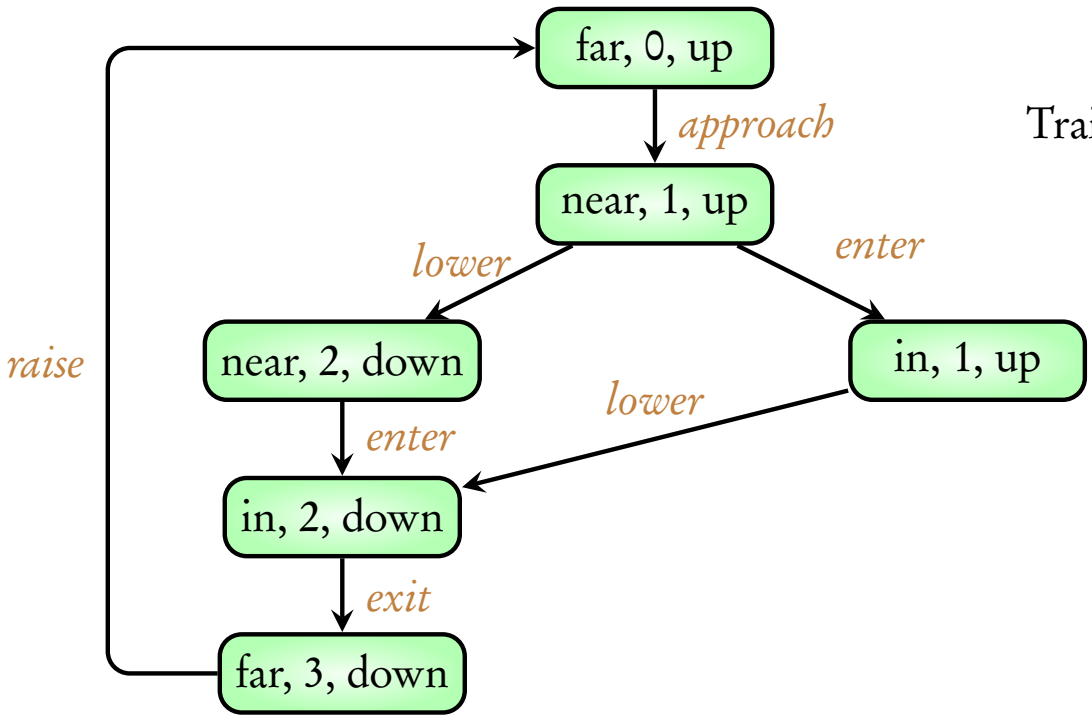
Train



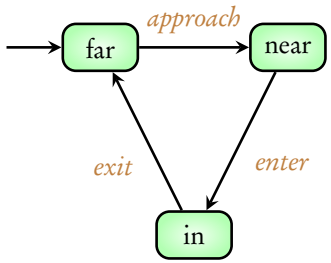
Controller



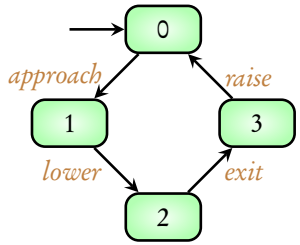
Gate



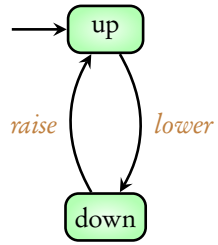
Train || Controller || Gate



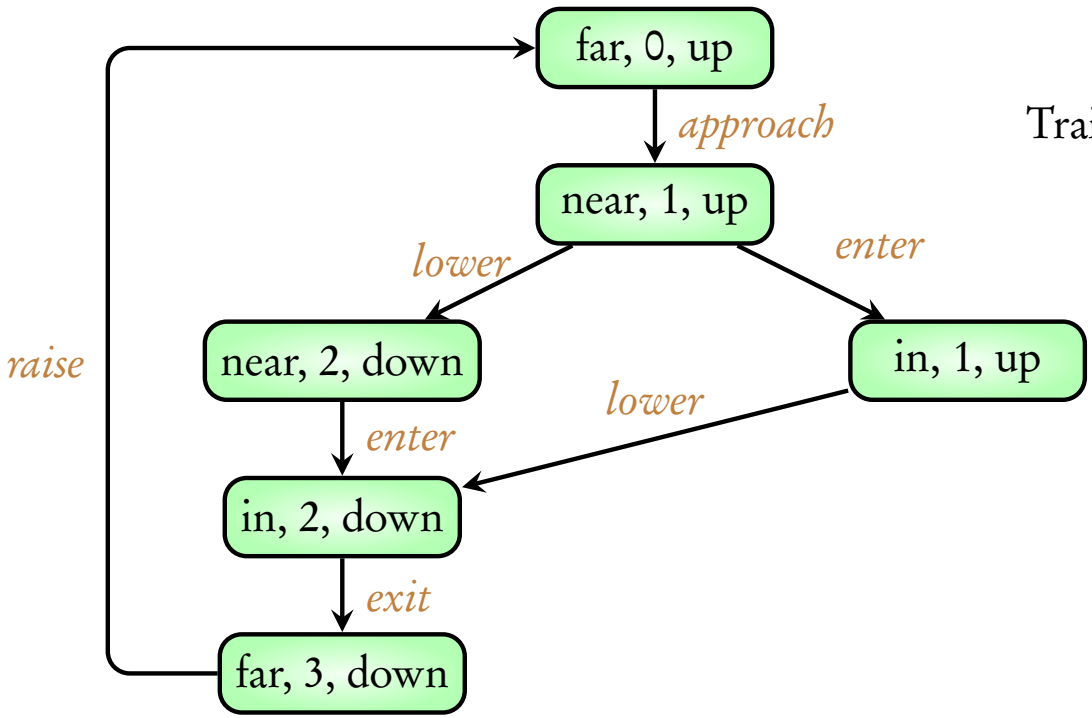
Train



Controller

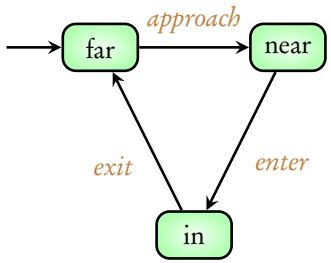


Gate

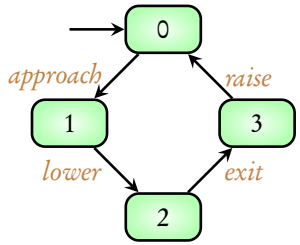


Train || Controller || Gate

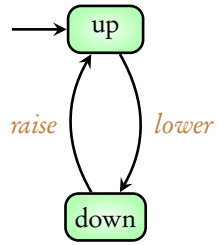
Unsafe state: Train is **in** when gate is still **up**



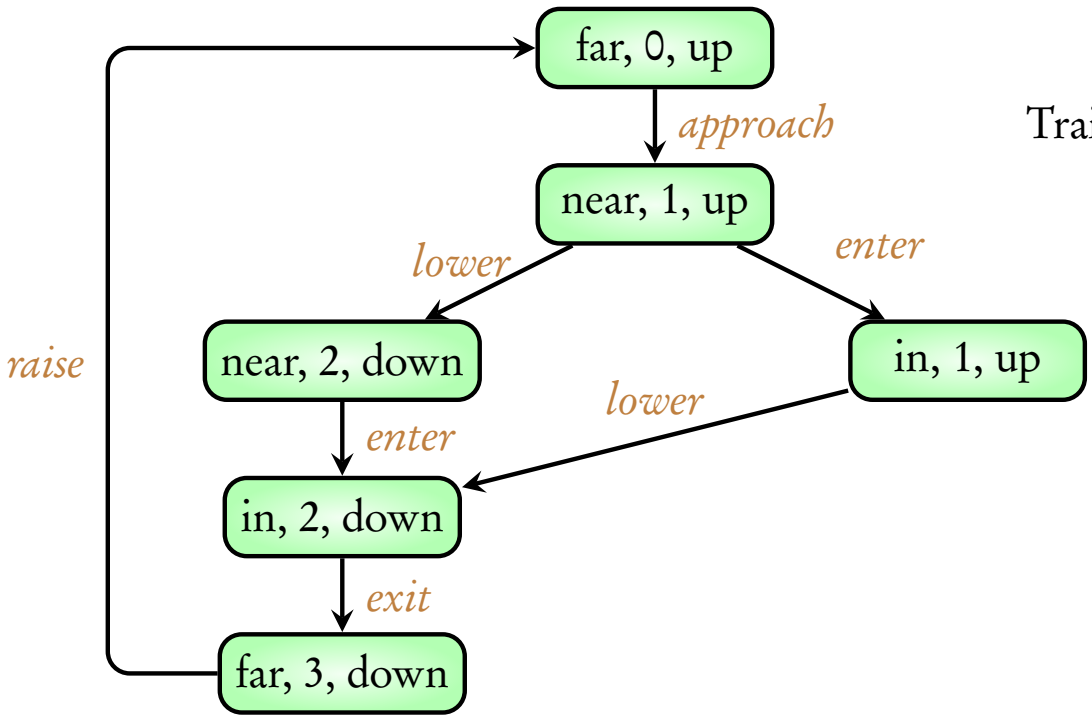
Train



Controller

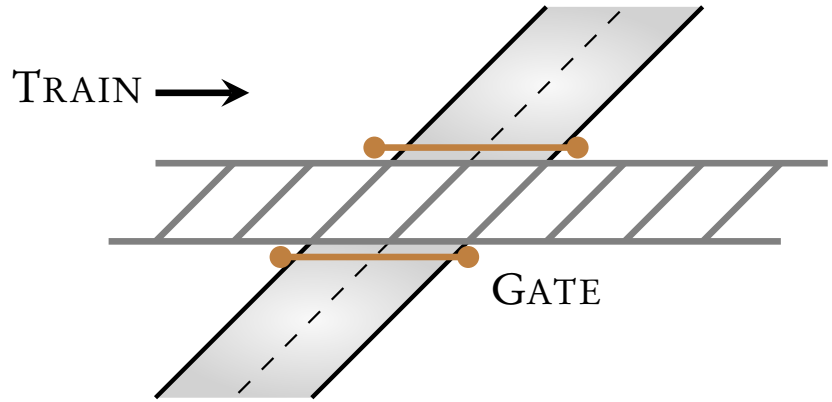


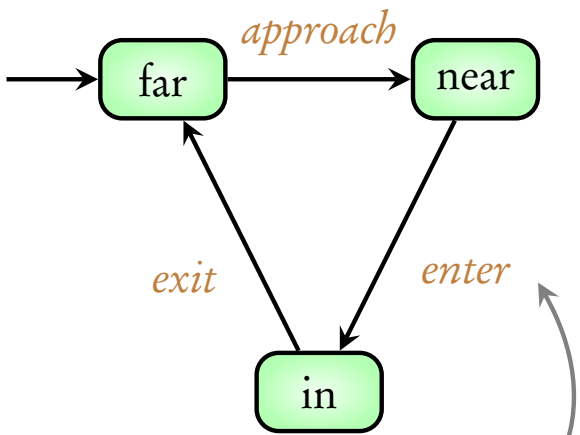
Gate



Train || Controller || Gate

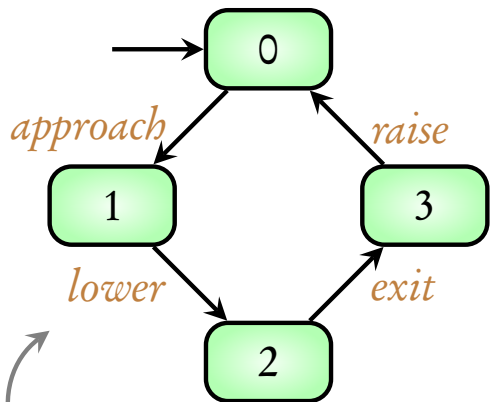
Unsafe state: Train is **in** when gate is still **up** - need to add **timing information** in the model





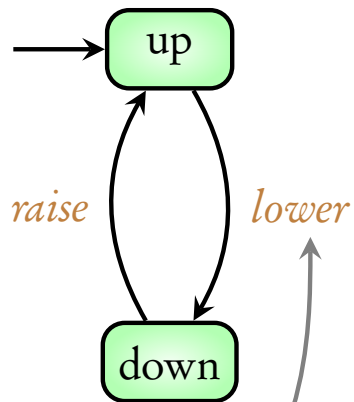
Train

after > 2 minutes



Controller

after $= 1$ minute

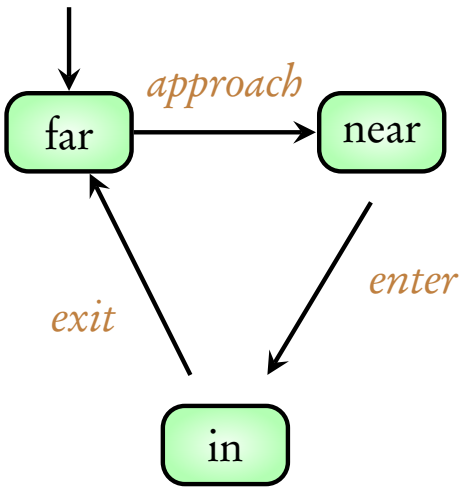


Gate

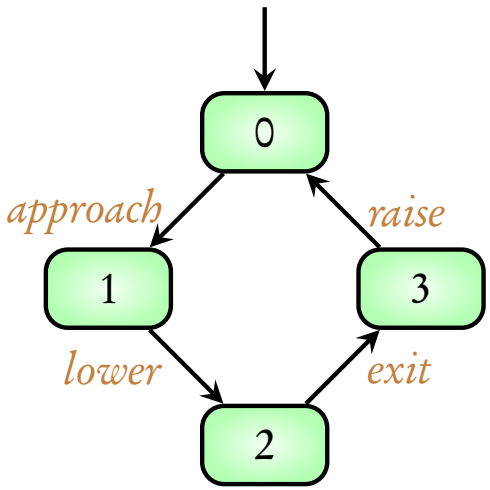
$<= 1$ minute

execution time

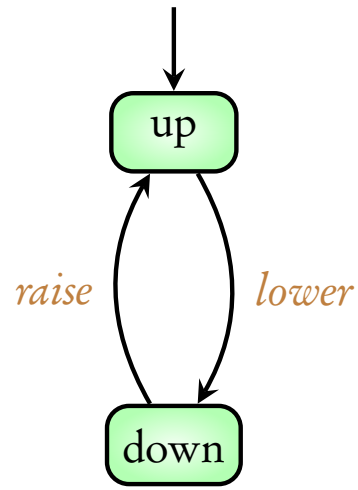
Coming next: Timed transition systems



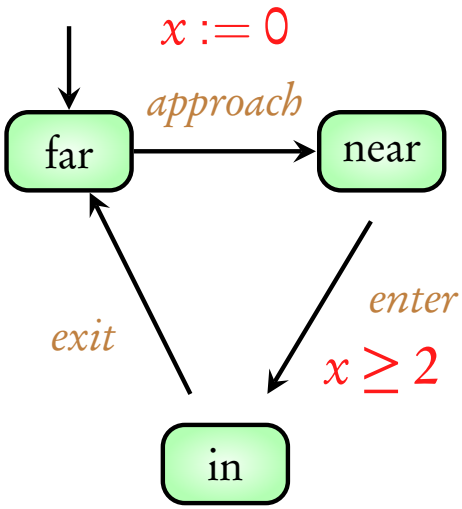
Train



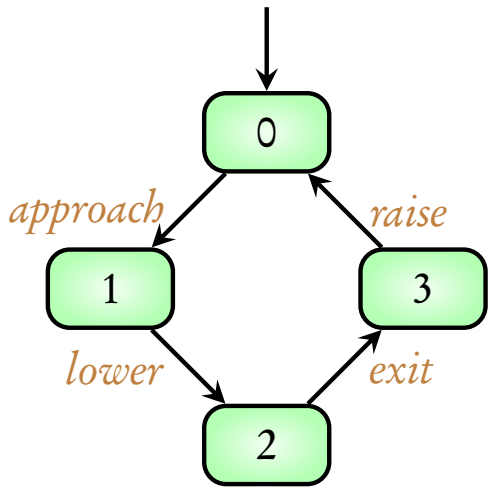
Controller



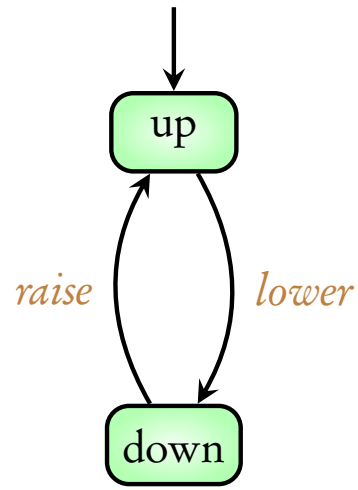
Gate



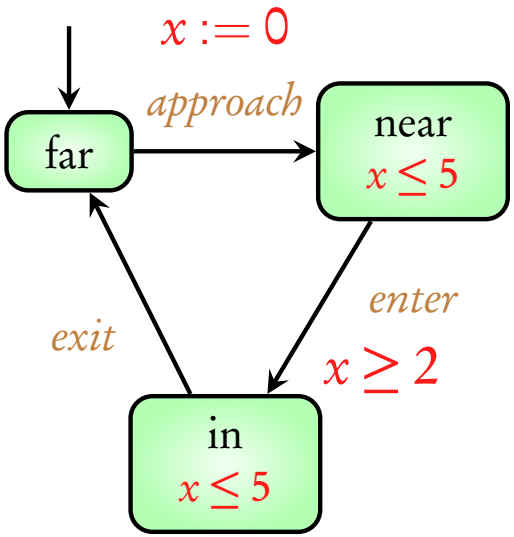
Train



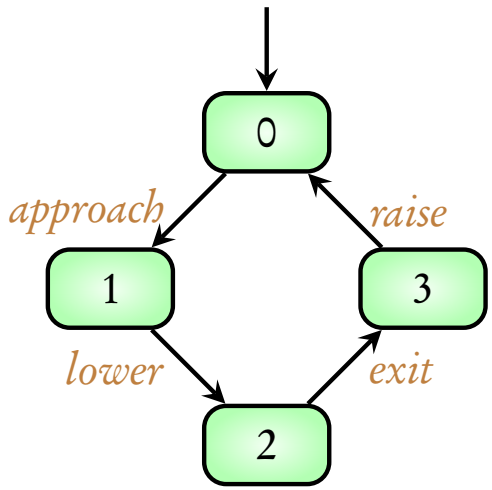
Controller



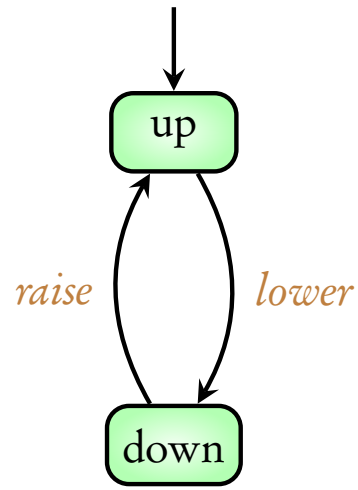
Gate



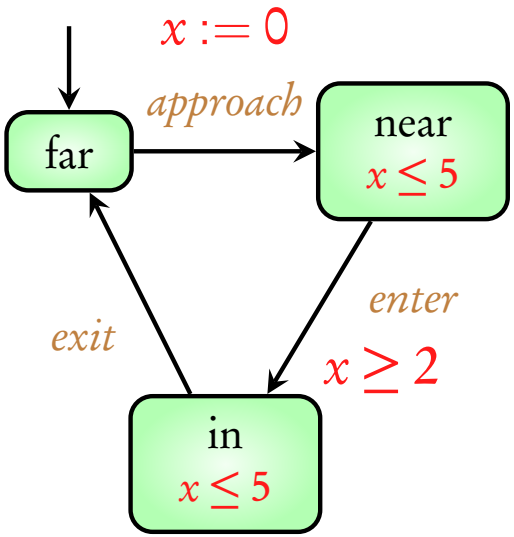
Train



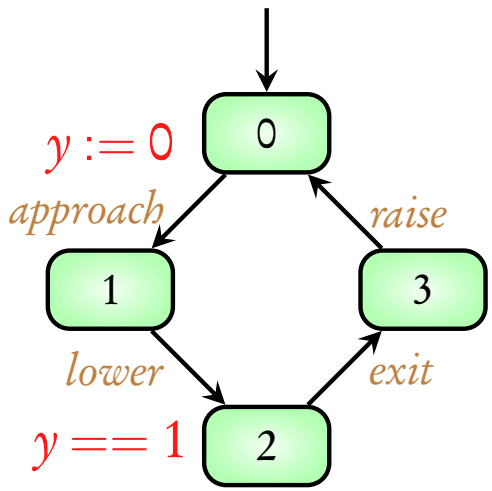
Controller



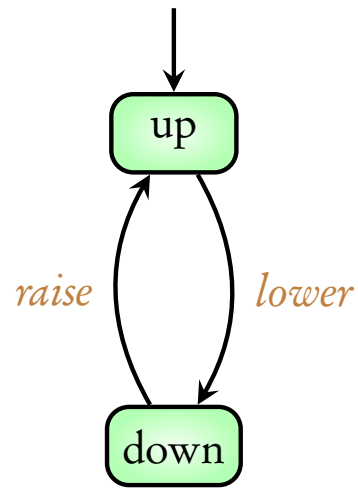
Gate



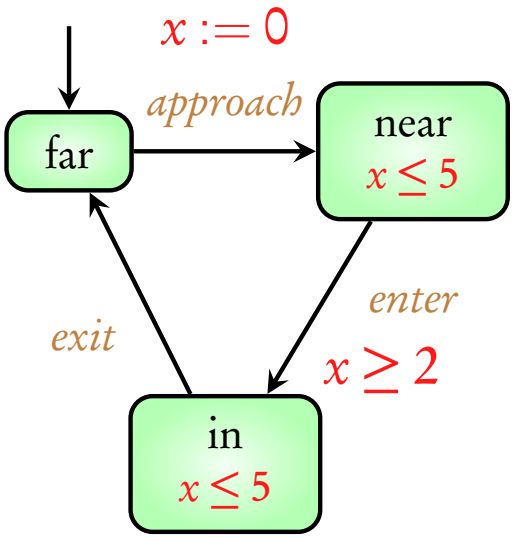
Train



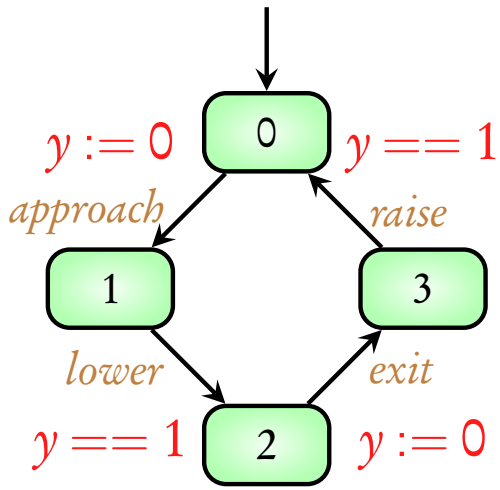
Controller



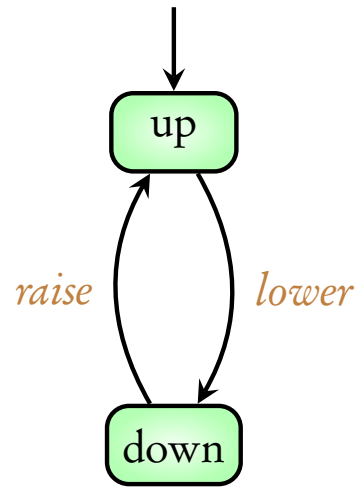
Gate



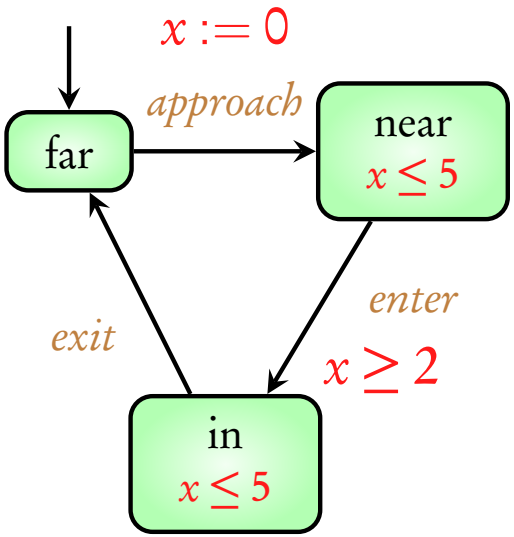
Train



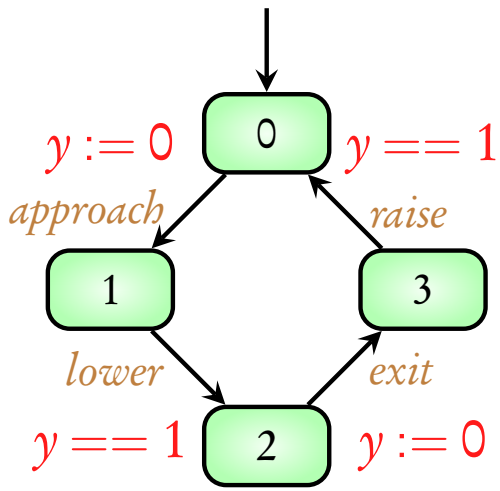
Controller



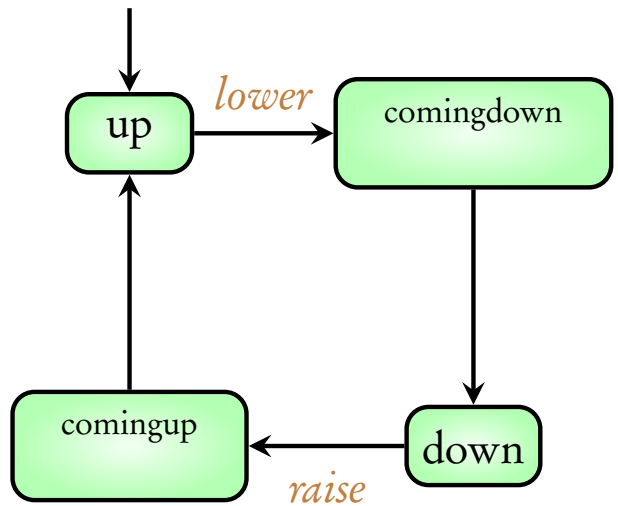
Gate



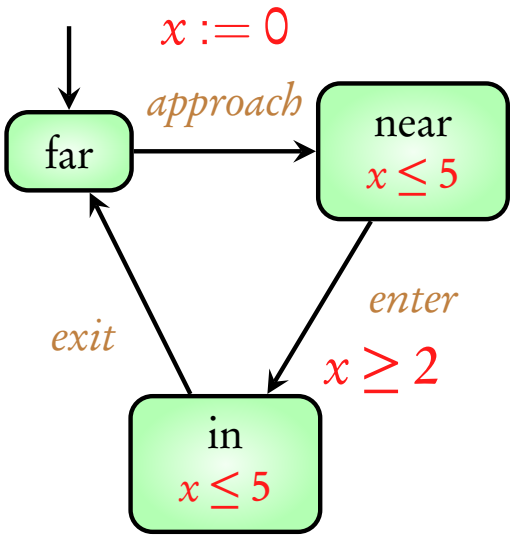
Train



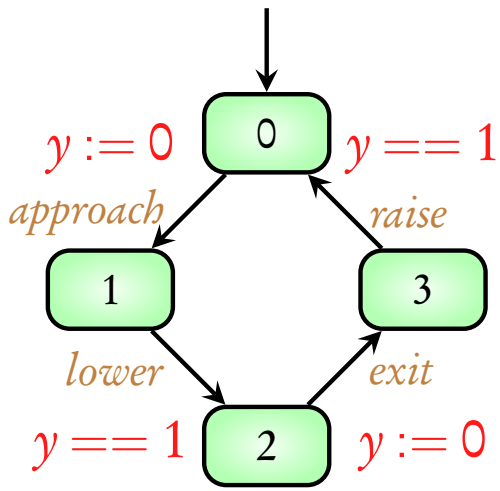
Controller



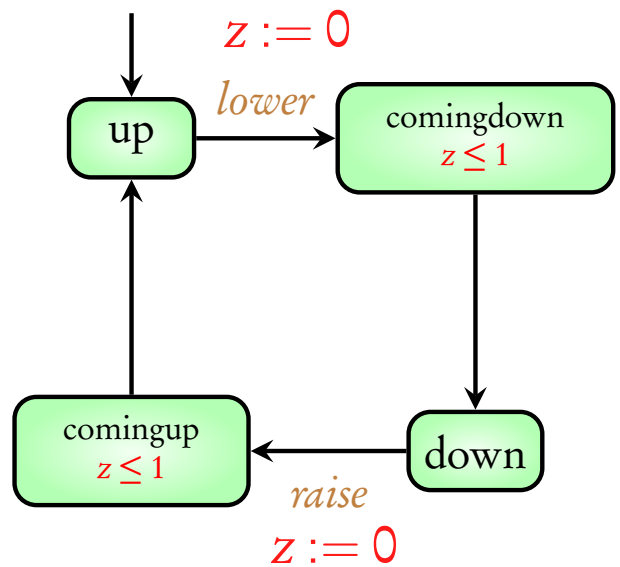
Gate



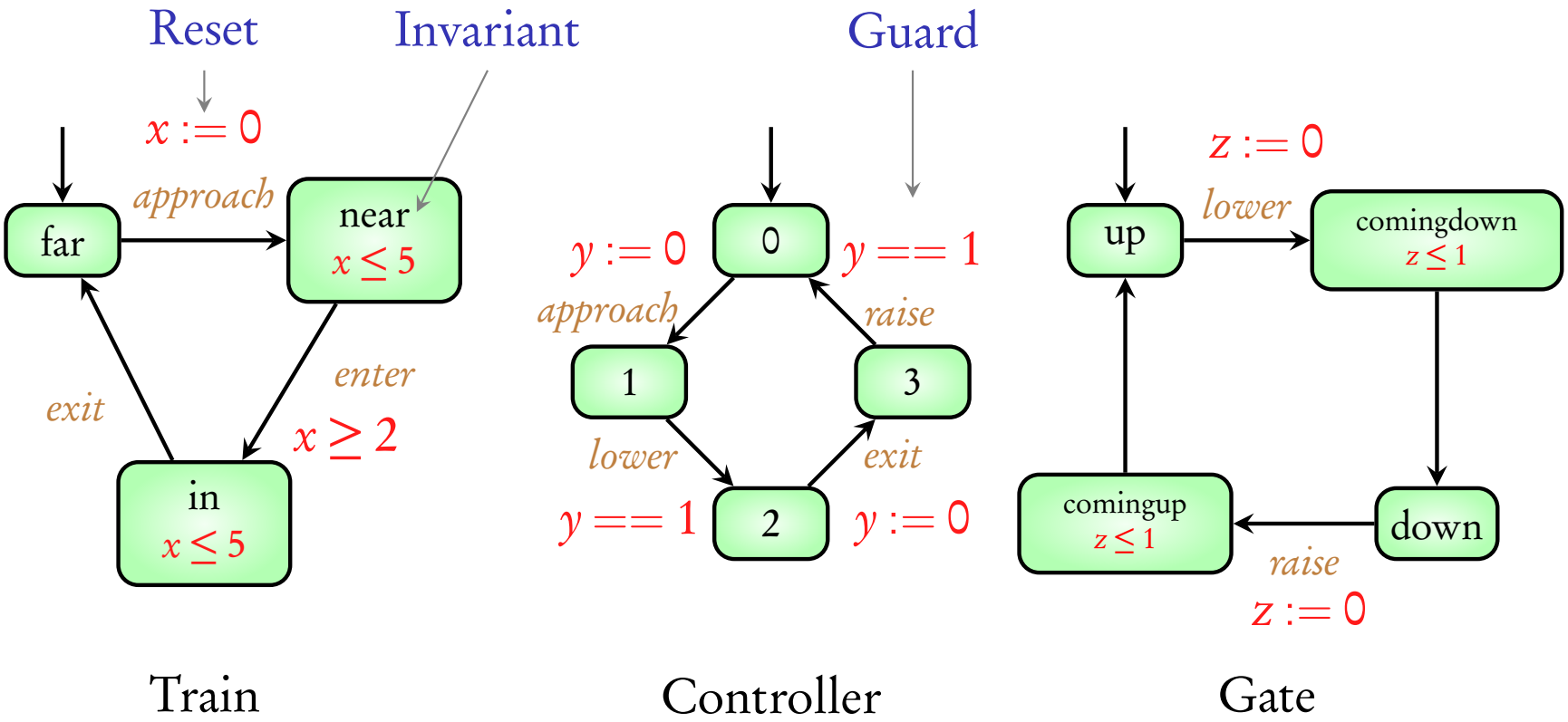
Train

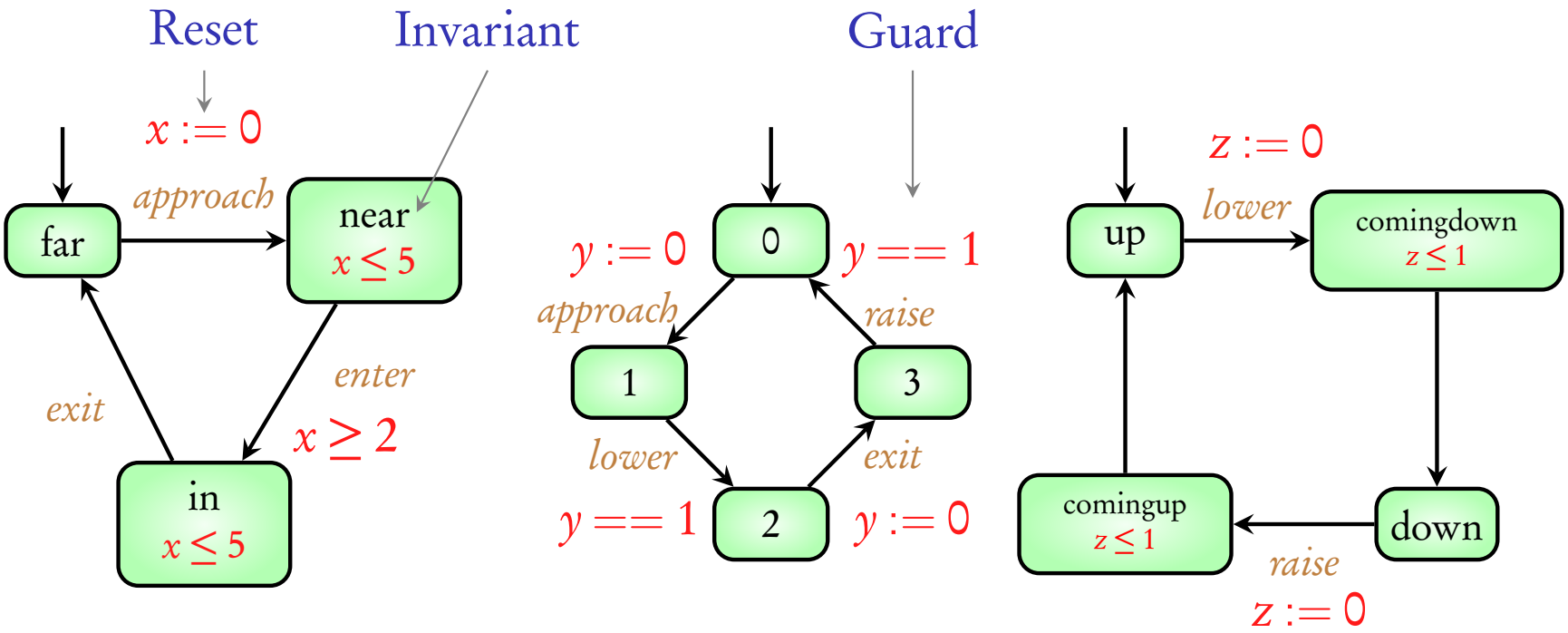


Controller



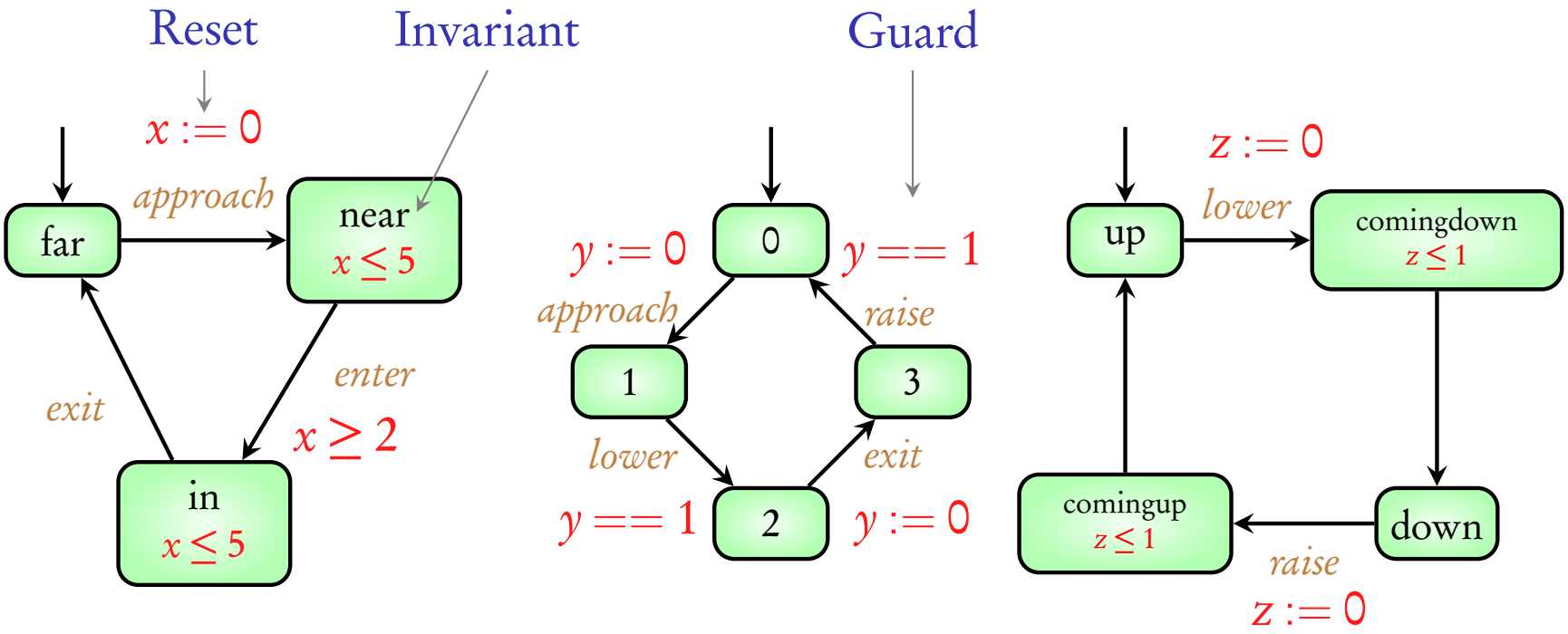
Gate


Reset
Invariant
Guard
$x := 0$
approach
far
near
$x \leq 5$
exit
enter
$x \geq 2$
in
$x \leq 5$
Train
$y := 0$
0
$y == 1$
approach
raise
1
3
lower
exit
$y == 1$
2
$y := 0$
Controller
$z := 0$
lower
up
comingdown
$z \leq 1$
comingup
$z \leq 1$
down
raise
$z := 0$
Gate



Train Controller Gate

Train || Gate || Controller



Train || Gate || Controller

Synchronous product gives timed transition system for the joint behaviour

Timed transition system

Transition system + **Clocks**

- Resets: to **start** measuring time
- Guards: to **impose** time constraint on action
- Invariants: to **limit** time spent in a state

UPPAAL - Model-checker for timed transition systems

Kim Larsen, Paul Pettersson, Wang Yi - **Computer-Aided Verification** Award in 2013 for UPPAAL

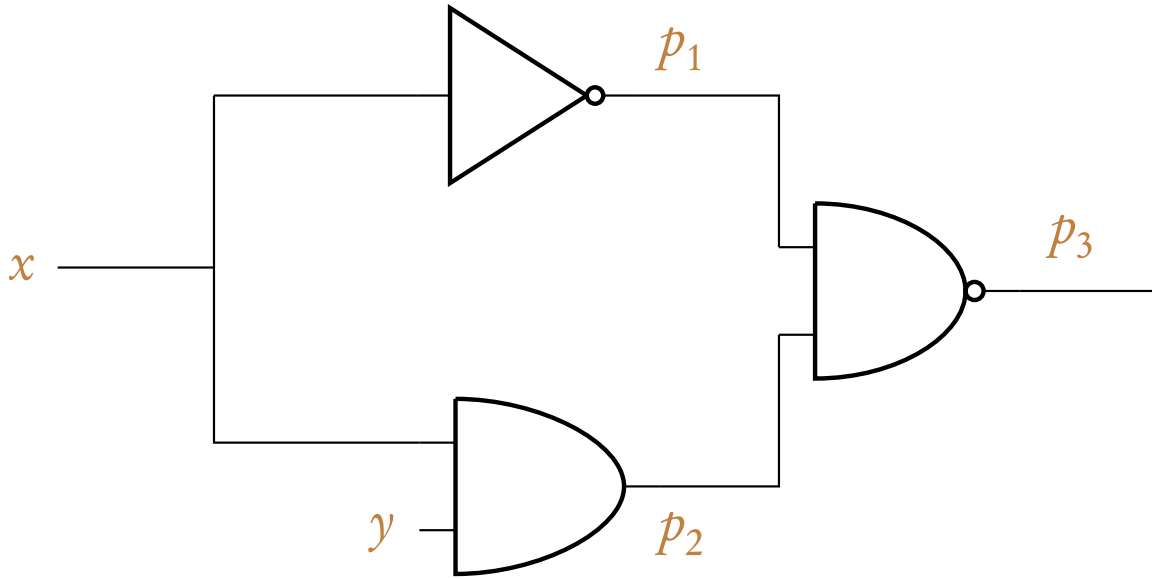
`www.uppaal.com`

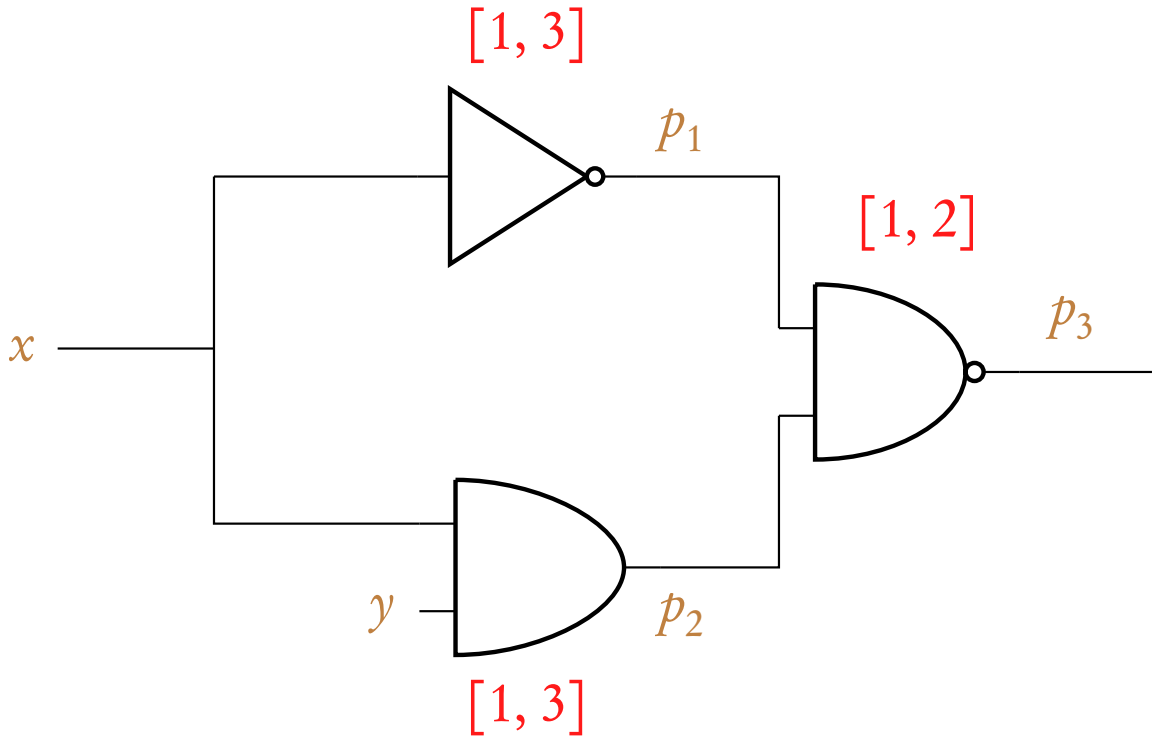
UPPAAL demo

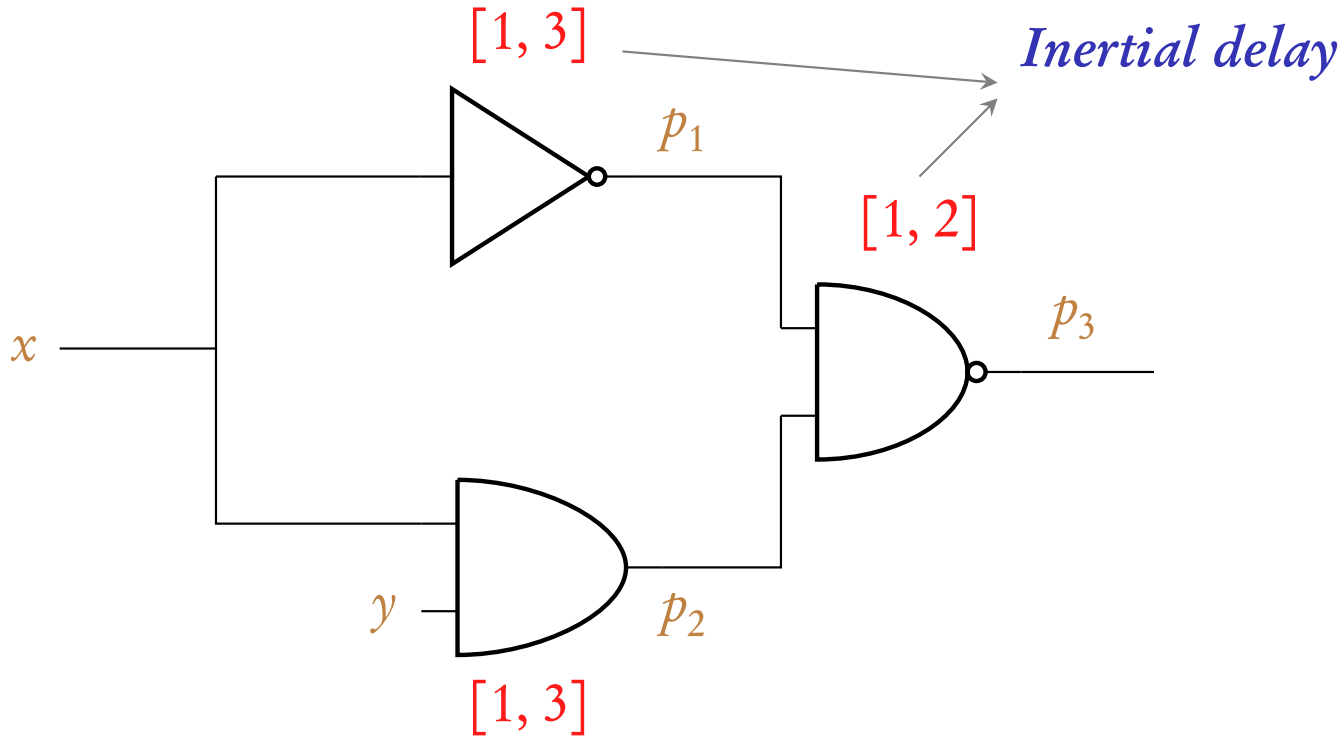
UPPAAL demo

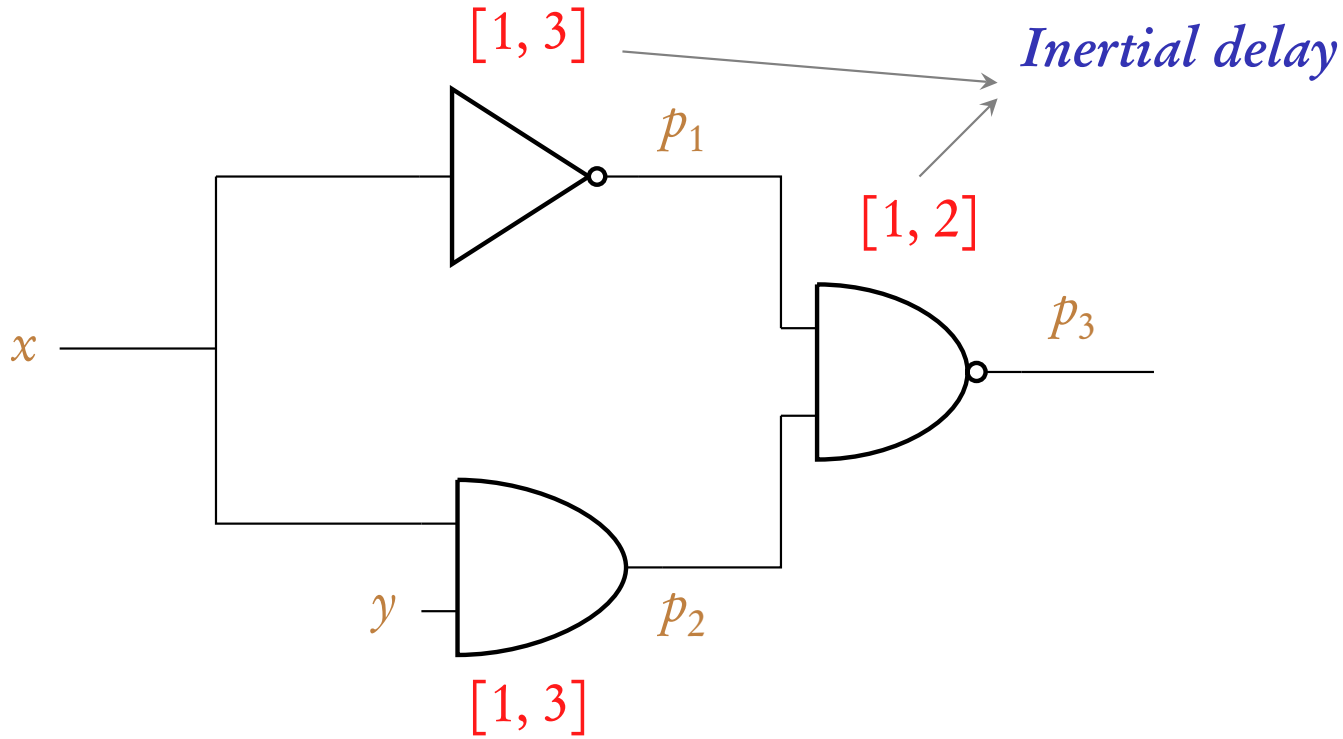
- Adding states, transitions and clocks
- Simulation environment
- (Subset of) CTL property verification

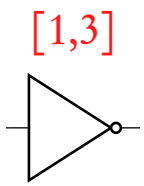
Example 2


p_1
x
p_3
y
p_2


[1, 3]
p_1
[1, 2]
p_3
x
y
p_2
[1, 3]

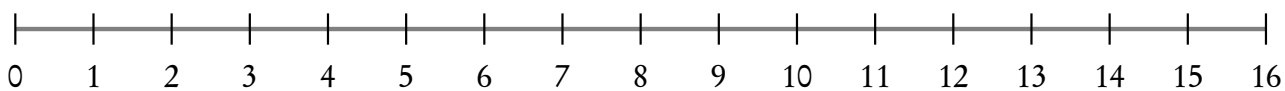

[1, 3]
Inertial delay
p_1
[1, 2]
x
p_3
y
p_2
[1, 3]

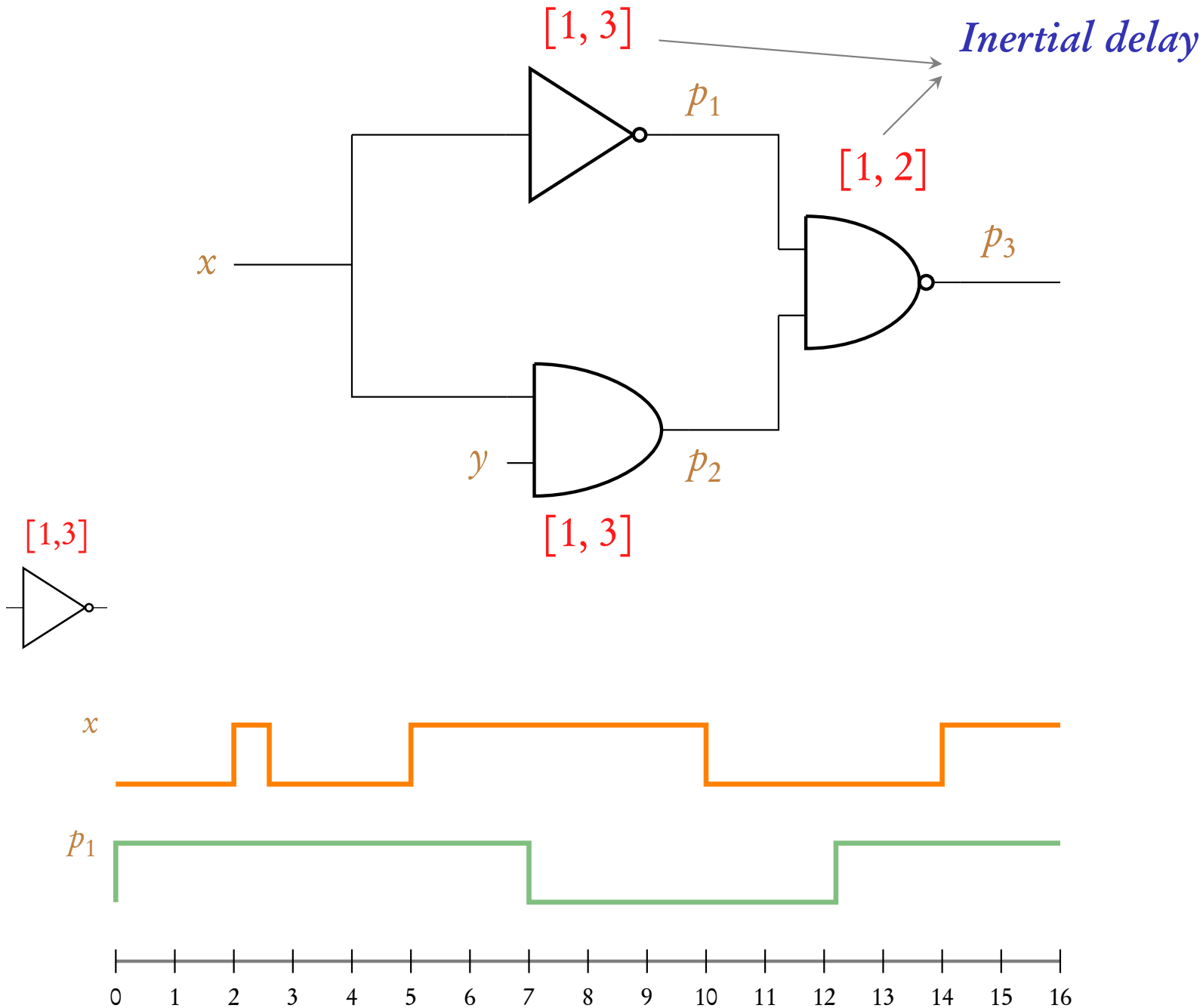

[1, 3]
Inertial delay
p_1
[1, 2]
p_3
x
y
p_2
[1, 3]

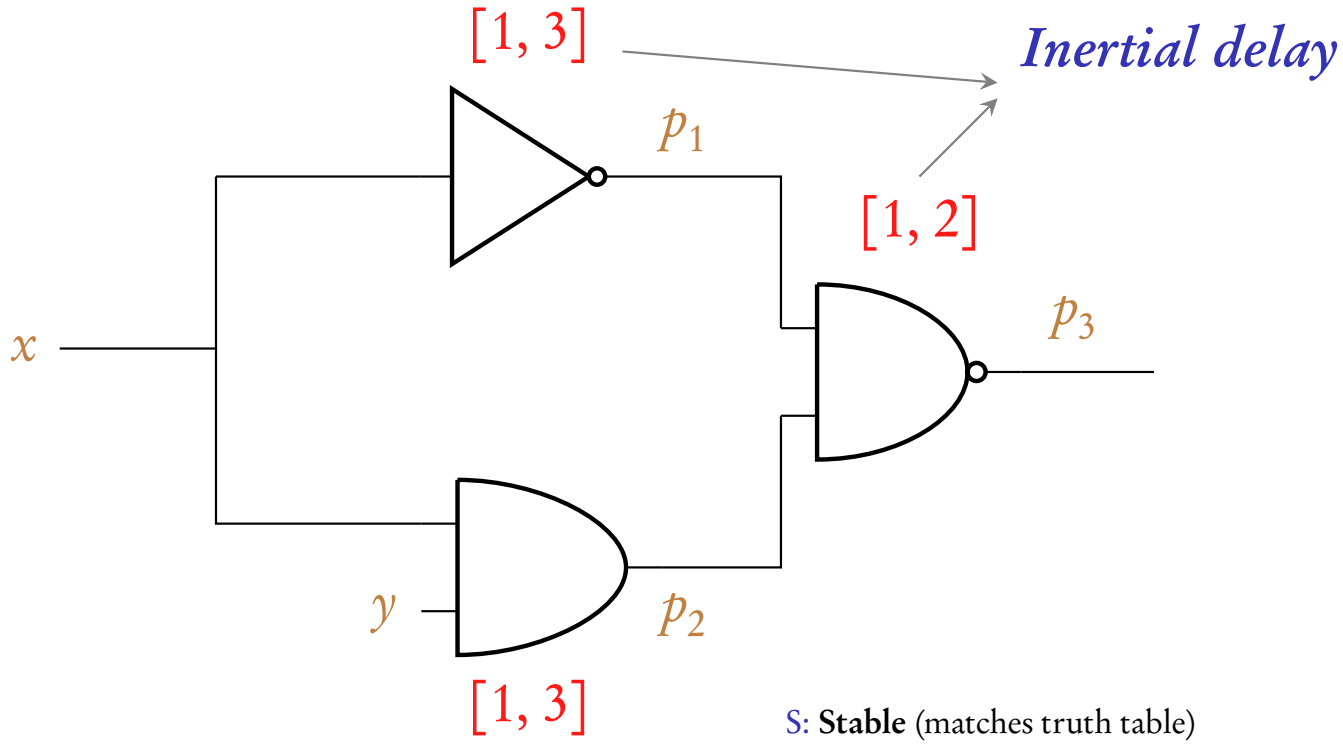

[1,3]

x

p_1


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

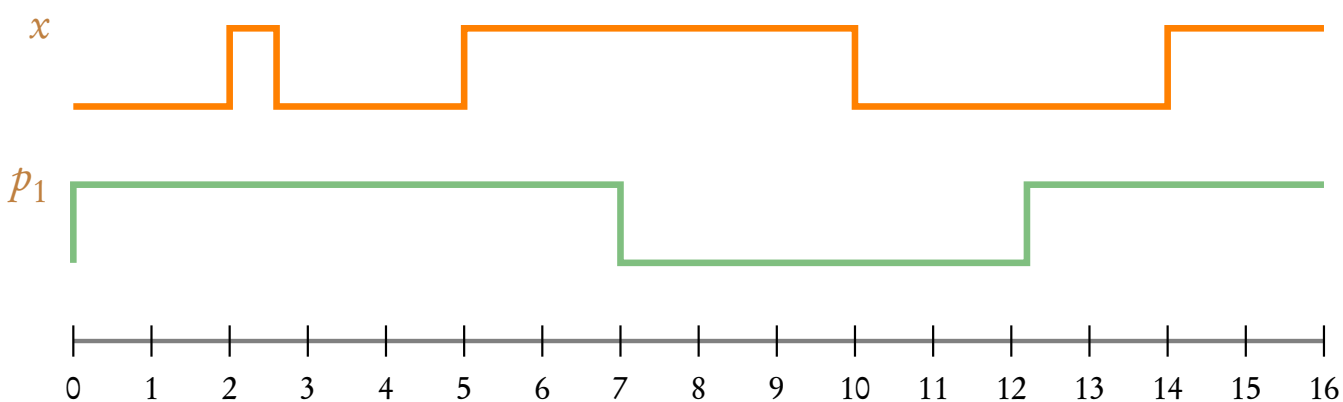

[1, 3]
Inertial delay
p_1
[1, 2]
p_3
x
y
p_2
[1, 3]
[1,3]
x
p_1
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

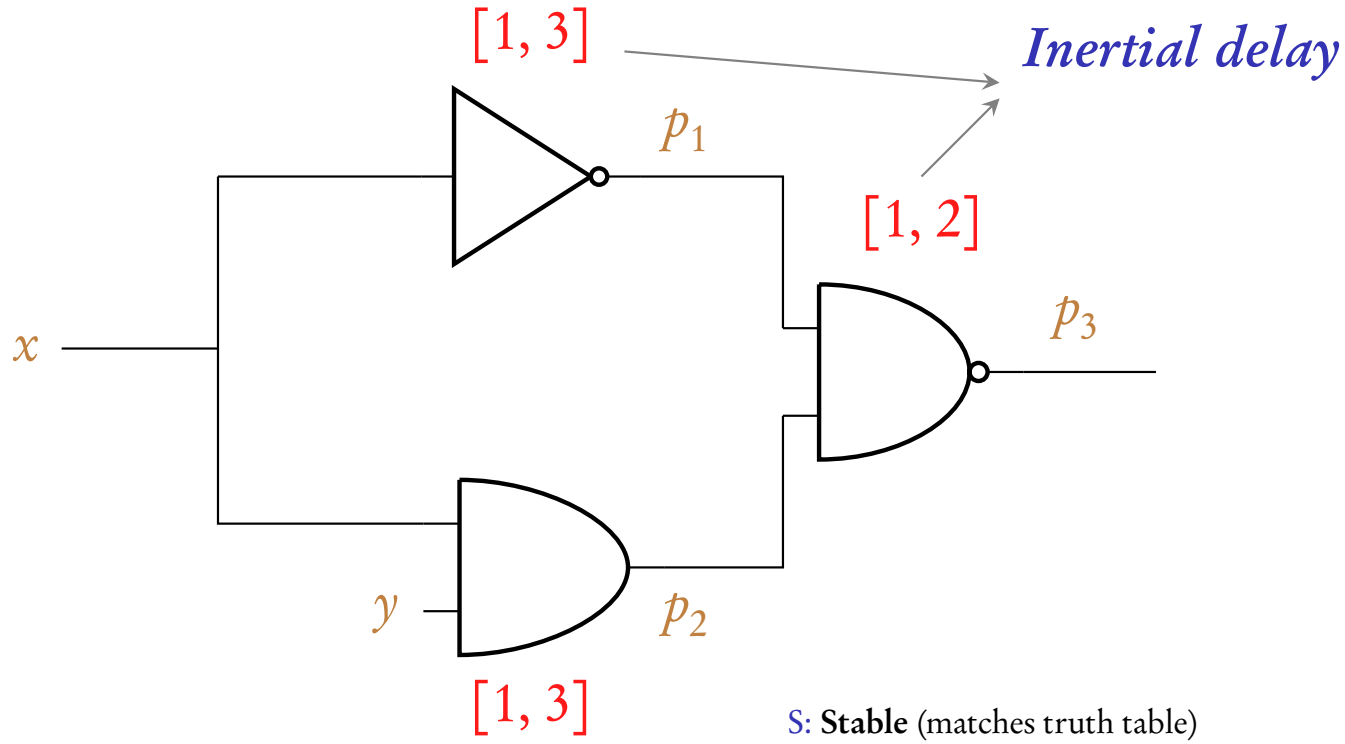


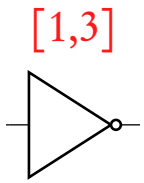
[1,3]

S: **Stable** (matches truth table)

U: **Unstable** (**does not** match truth table)

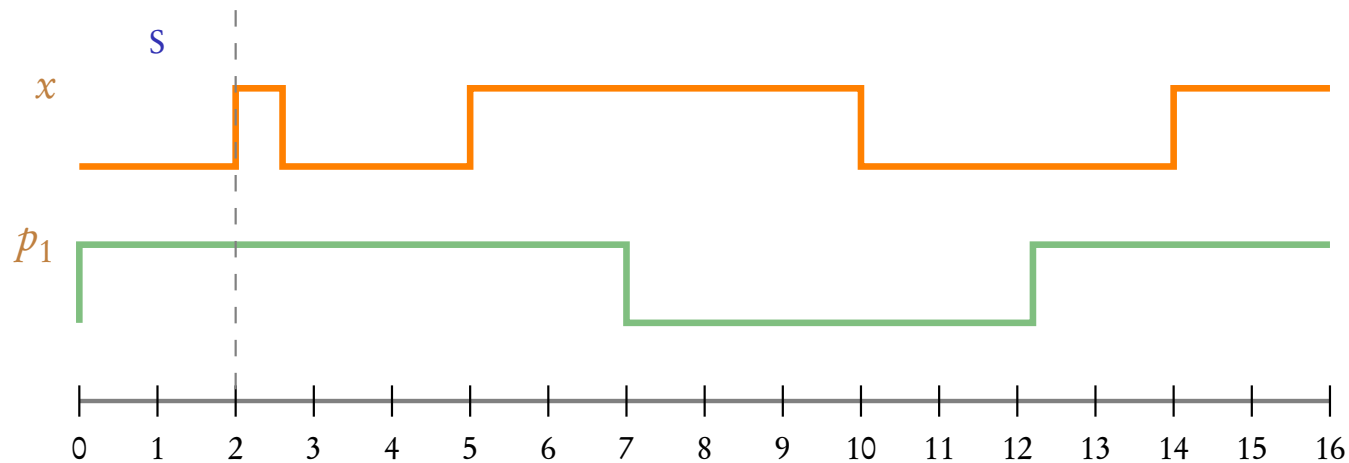


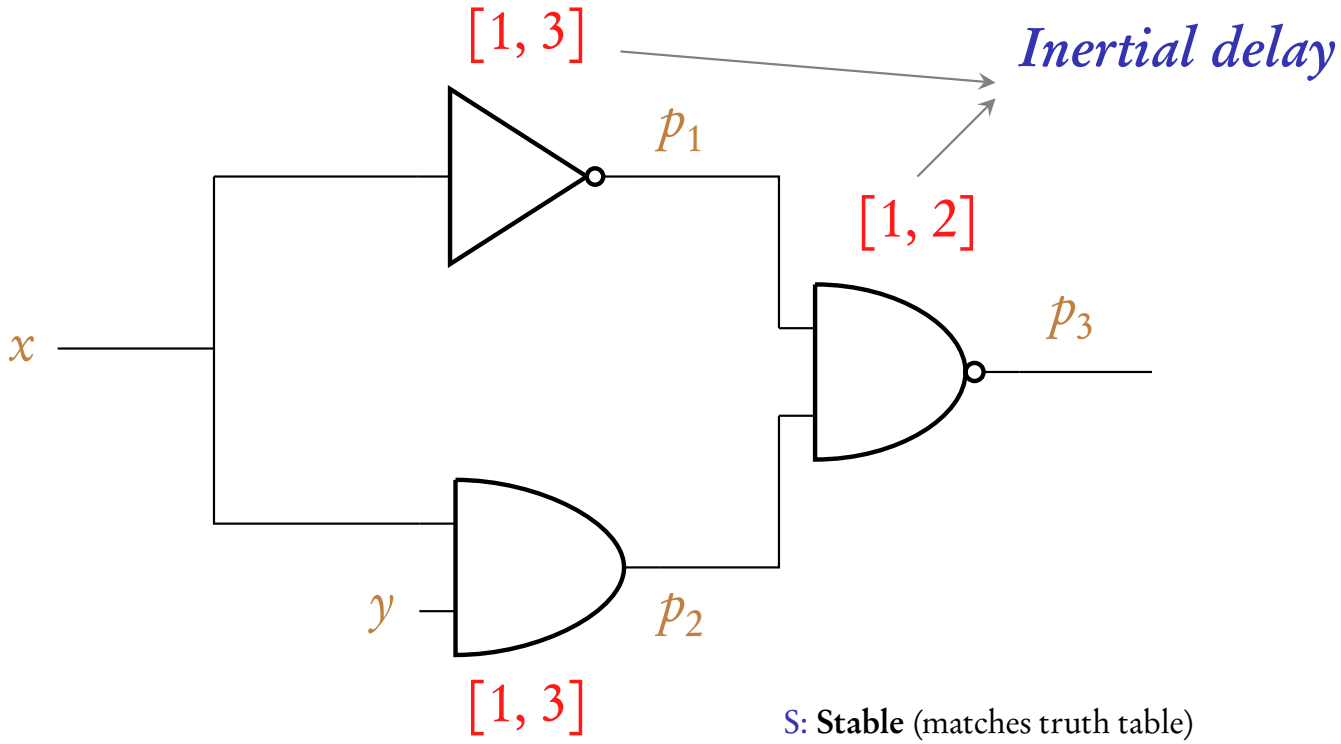


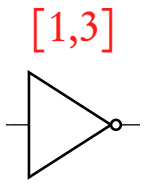


S: **Stable** (matches truth table)

U: **Unstable** (**does not** match truth table)

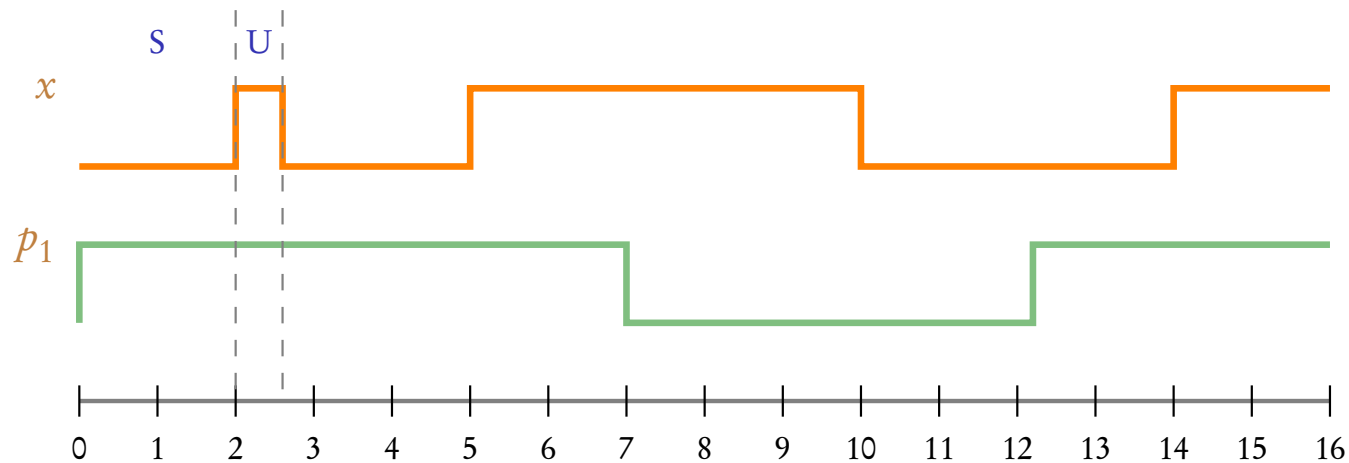


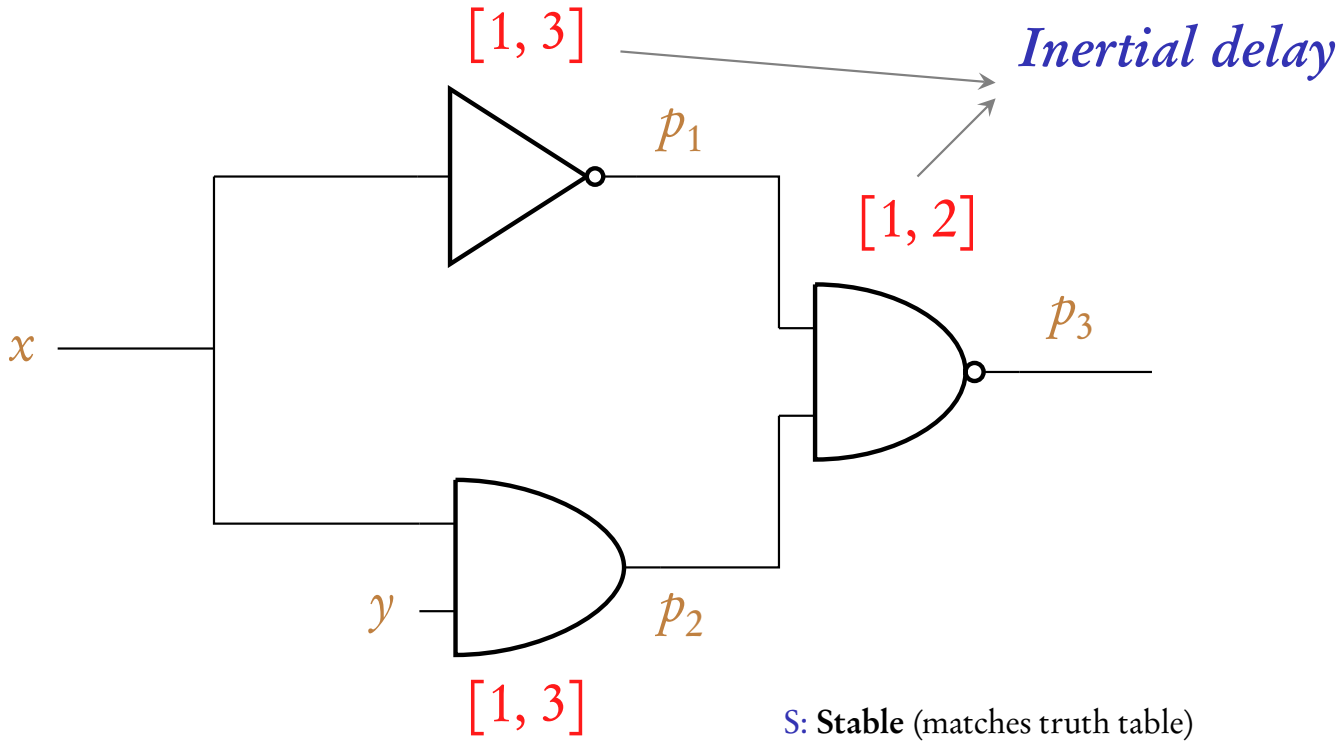


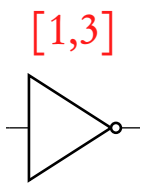


S: **Stable** (matches truth table)

U: **Unstable** (**does not** match truth table)

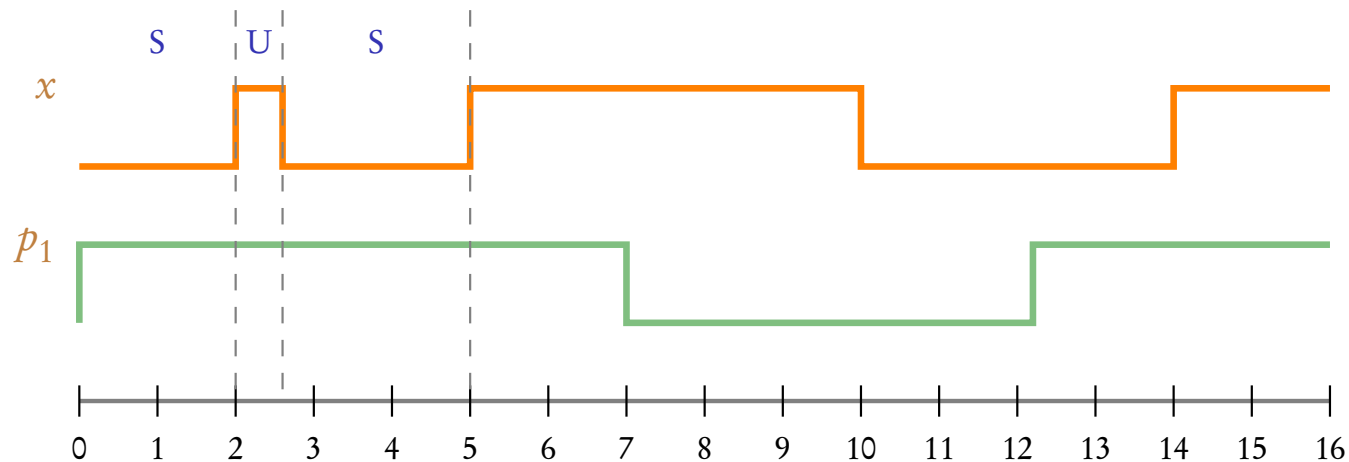


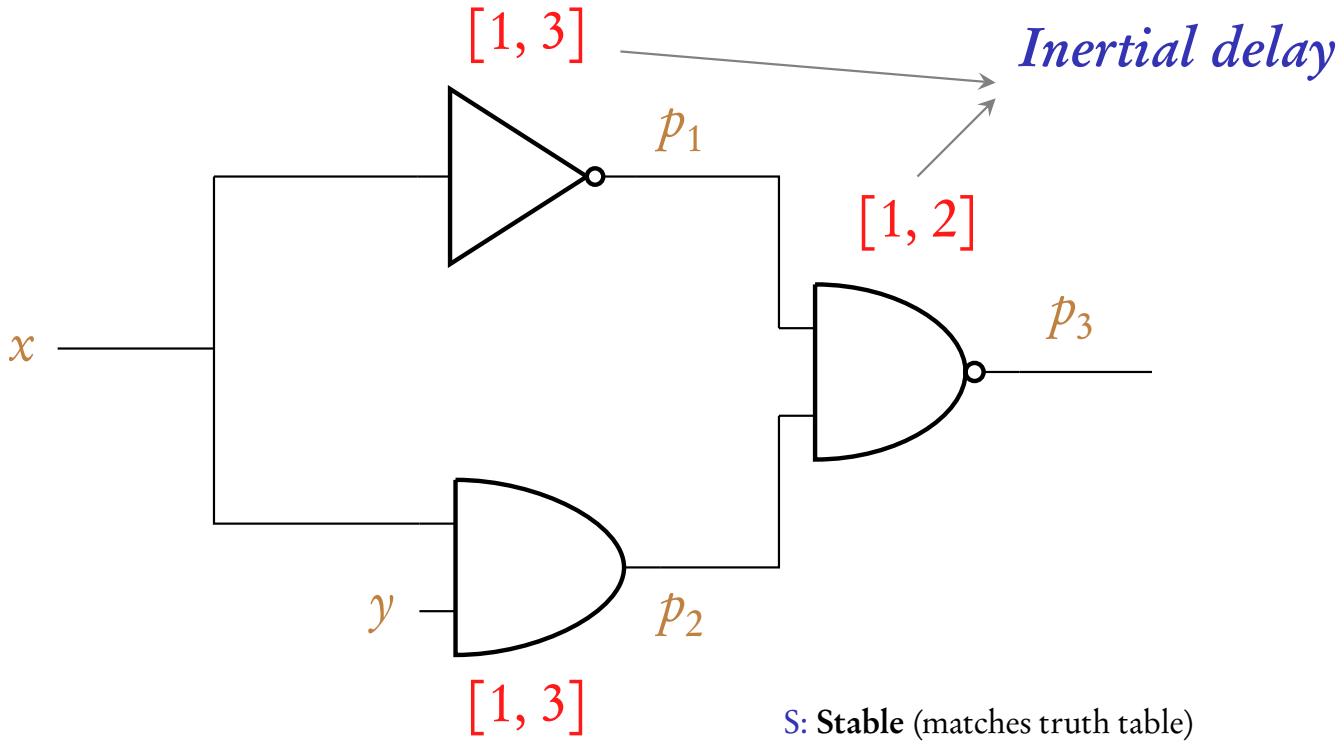


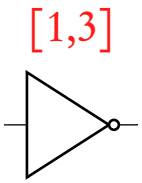


S: **Stable** (matches truth table)

U: **Unstable** (**does not** match truth table)

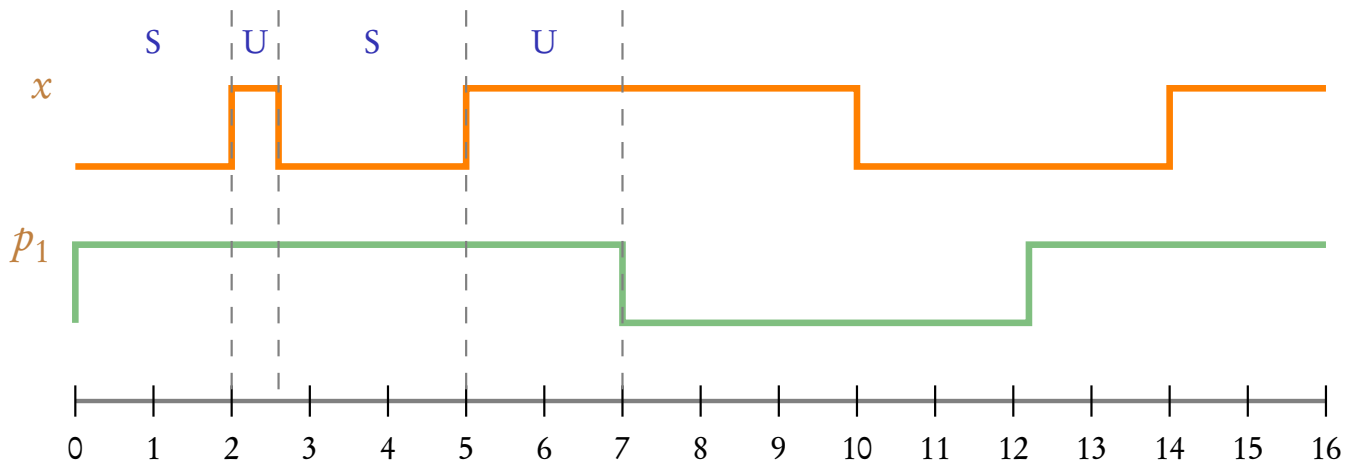


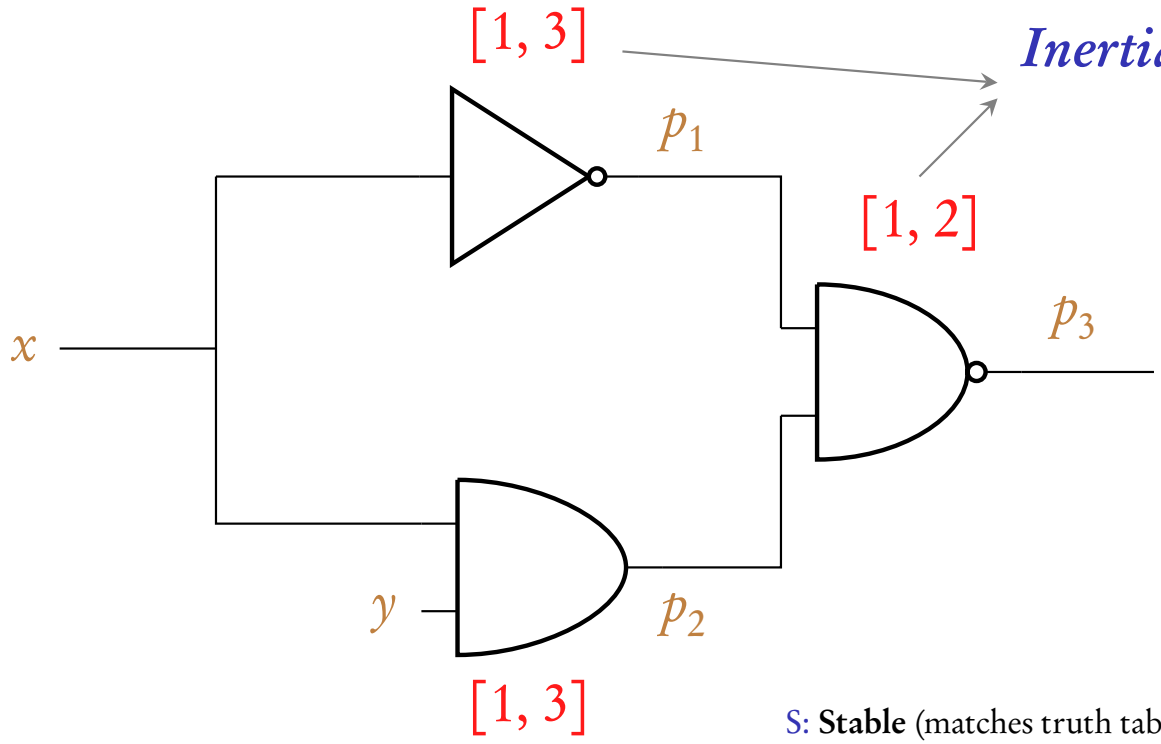


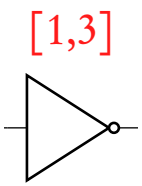


S: **Stable** (matches truth table)

U: **Unstable** (**does not** match truth table)

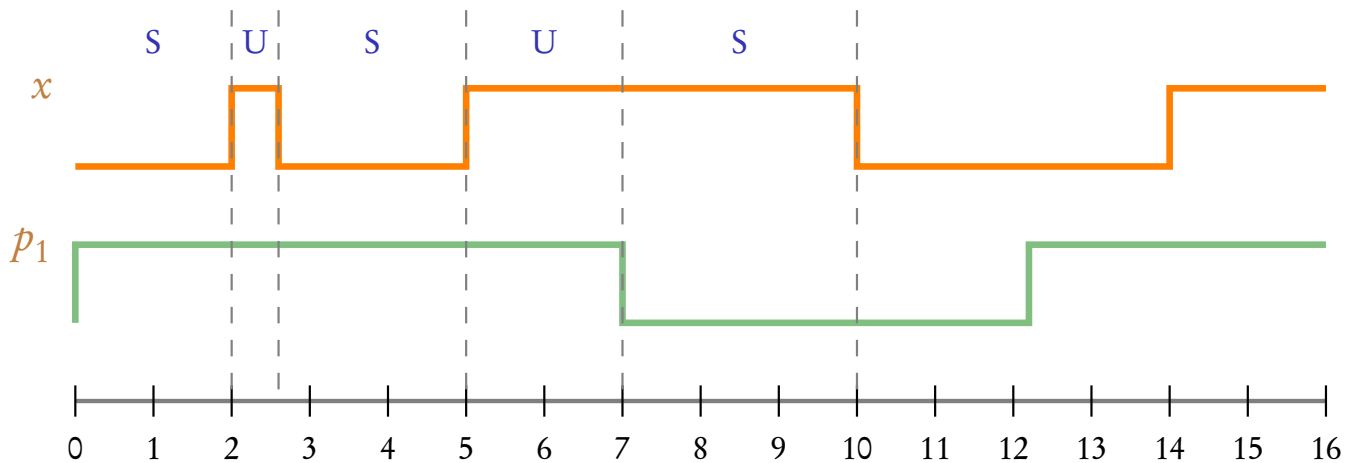


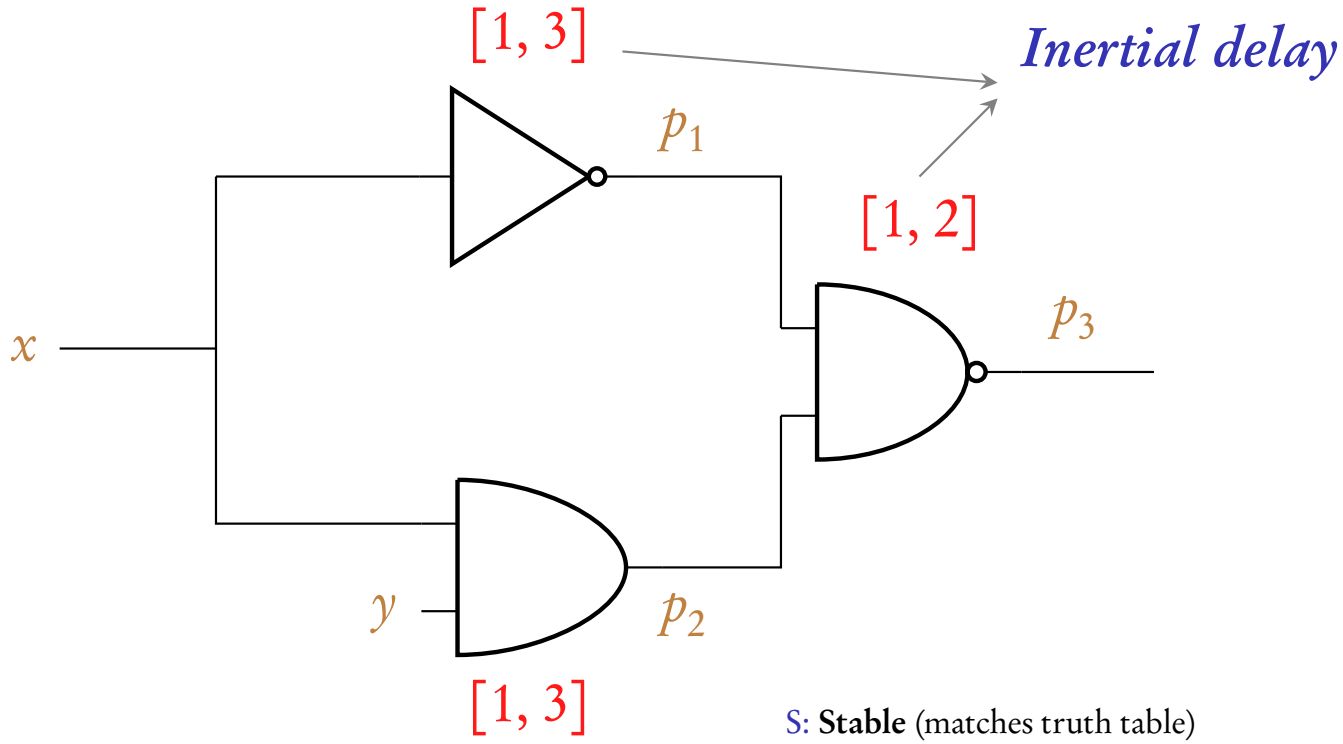


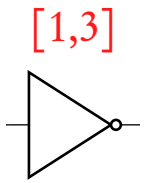


S: **Stable** (matches truth table)

U: **Unstable** (**does not** match truth table)

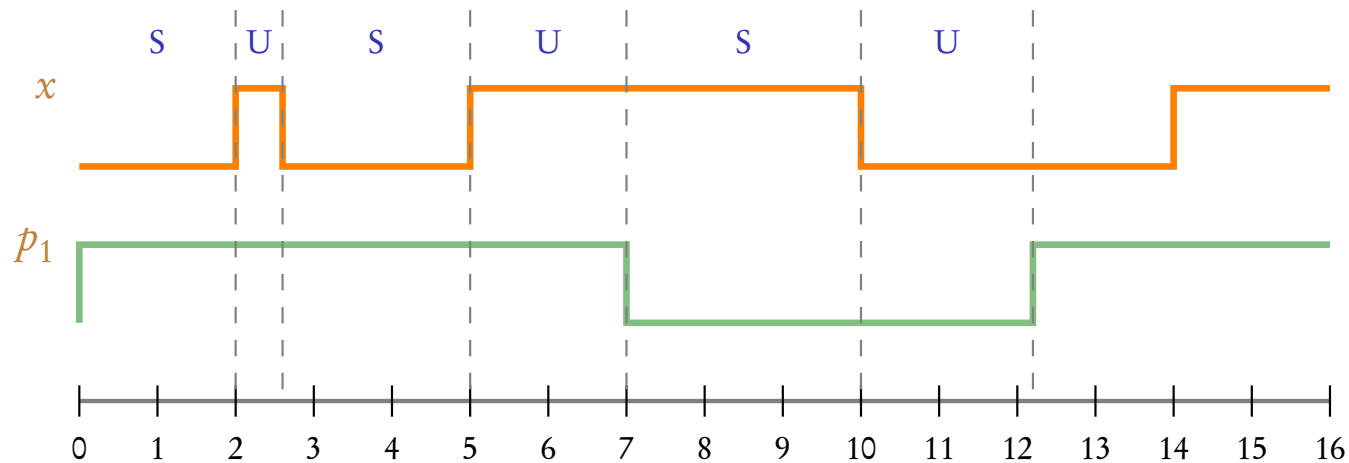


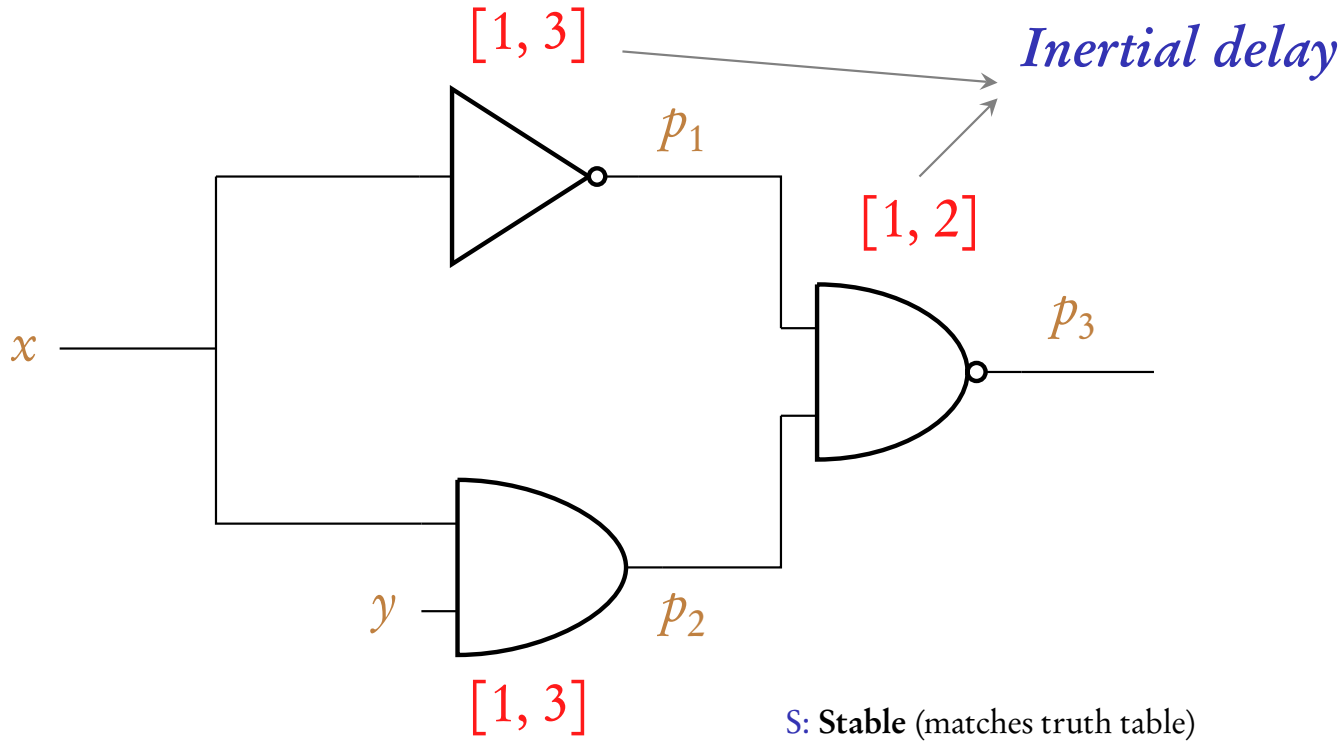


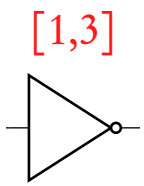


S: **Stable** (matches truth table)

U: **Unstable** (**does not** match truth table)

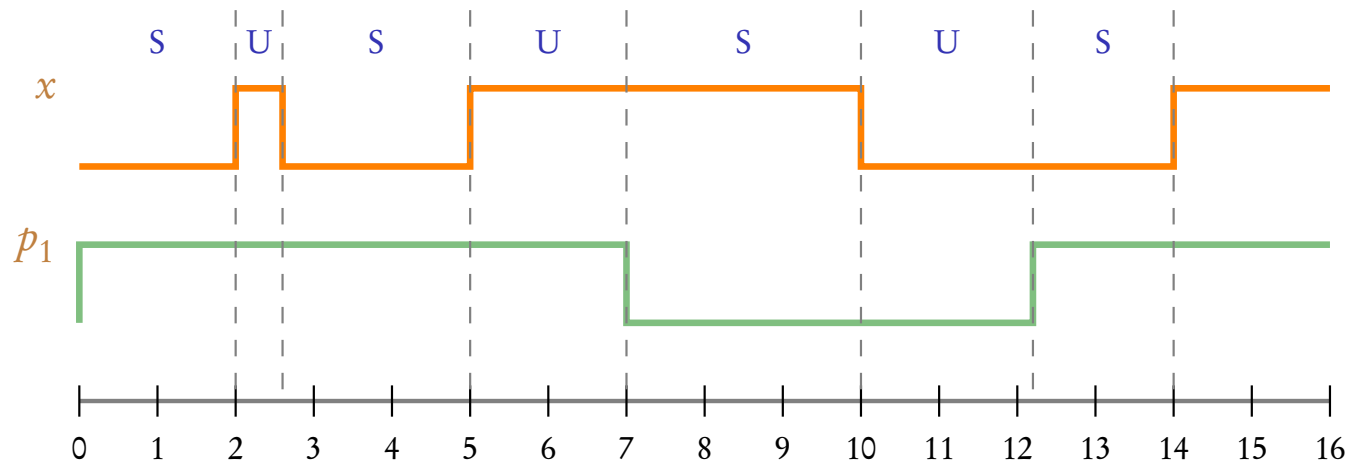


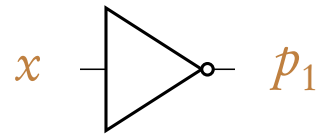




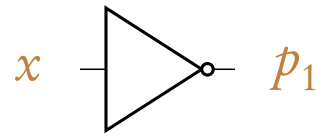
S: **Stable** (matches truth table)

U: **Unstable** (**does not** match truth table)





$$\langle\, x\,,\, p_1\,\rangle$$



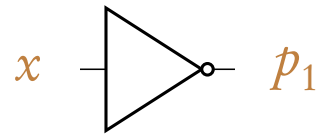
$$\langle\, x\,,\, p_1\,\rangle$$

$\langle 0, 1 \rangle$

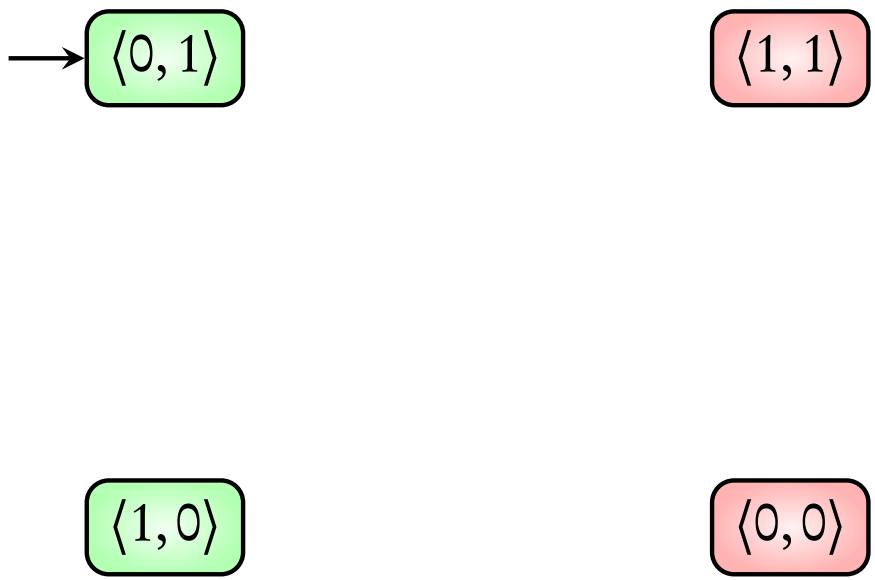
$\langle 1, 1 \rangle$

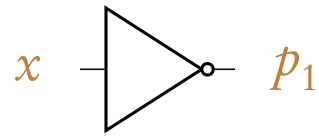
$\langle 1, 0 \rangle$

$\langle 0, 0 \rangle$

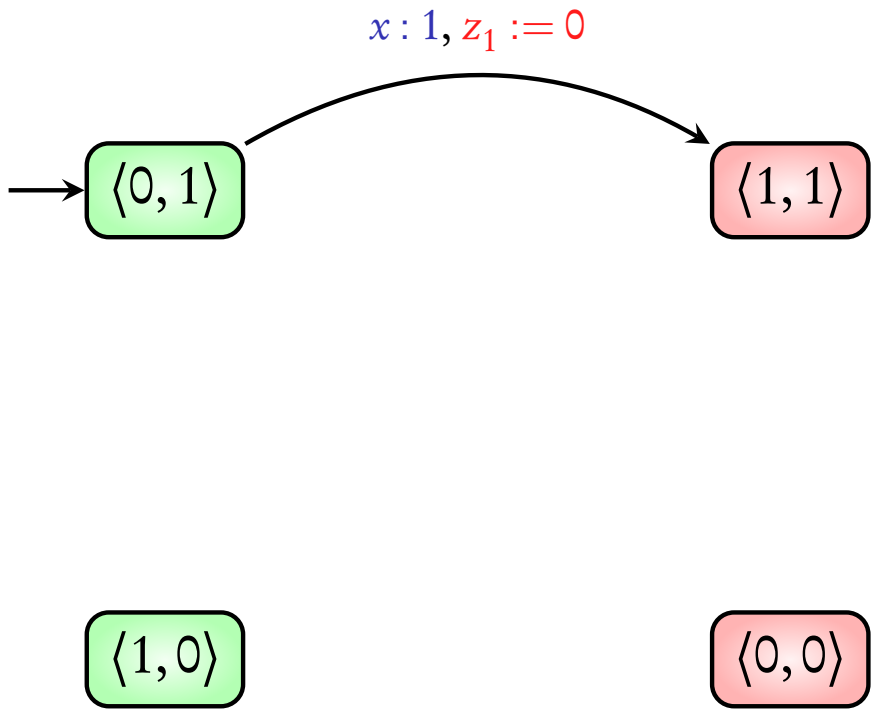


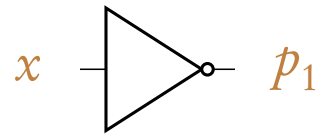
$$\langle\, x\,,\, p_1\,\rangle$$



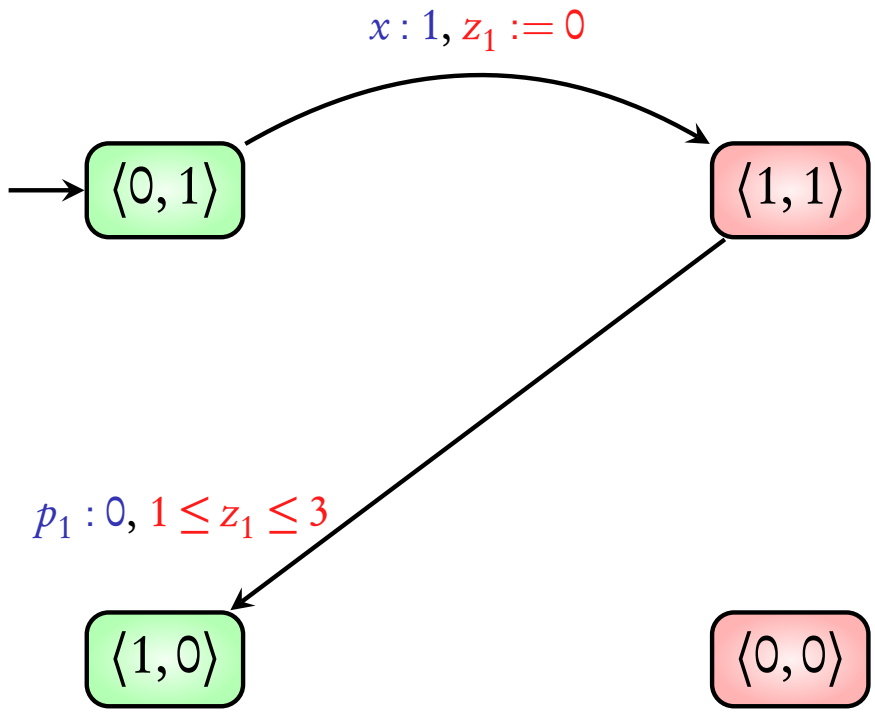


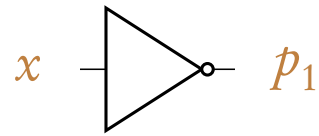
$$\langle\, x\,,\, p_1\,\rangle$$



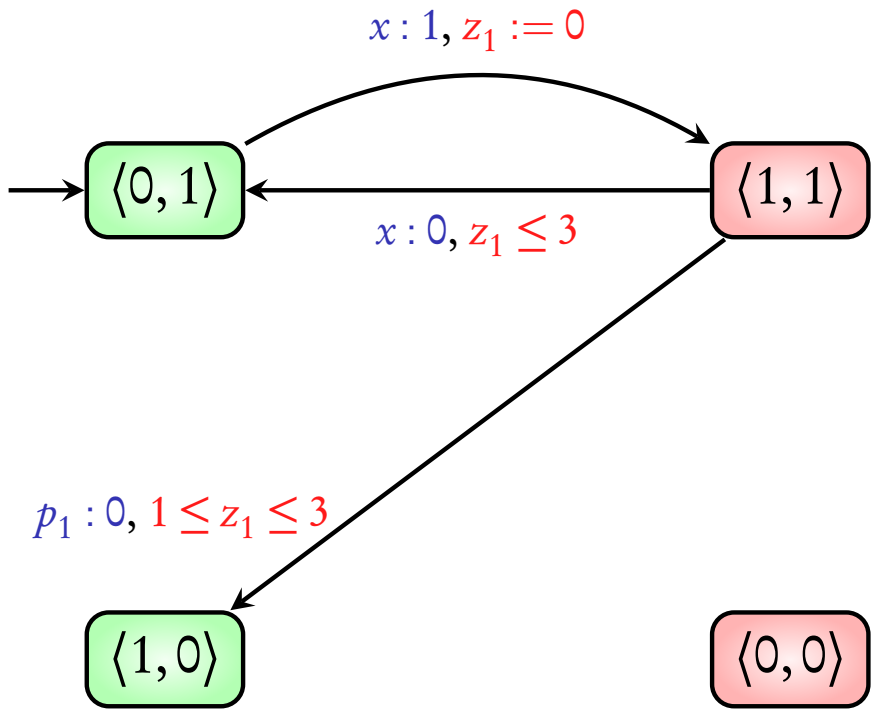


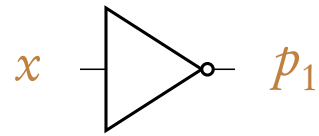
$$\langle\, x\,,\, p_1\,\rangle$$



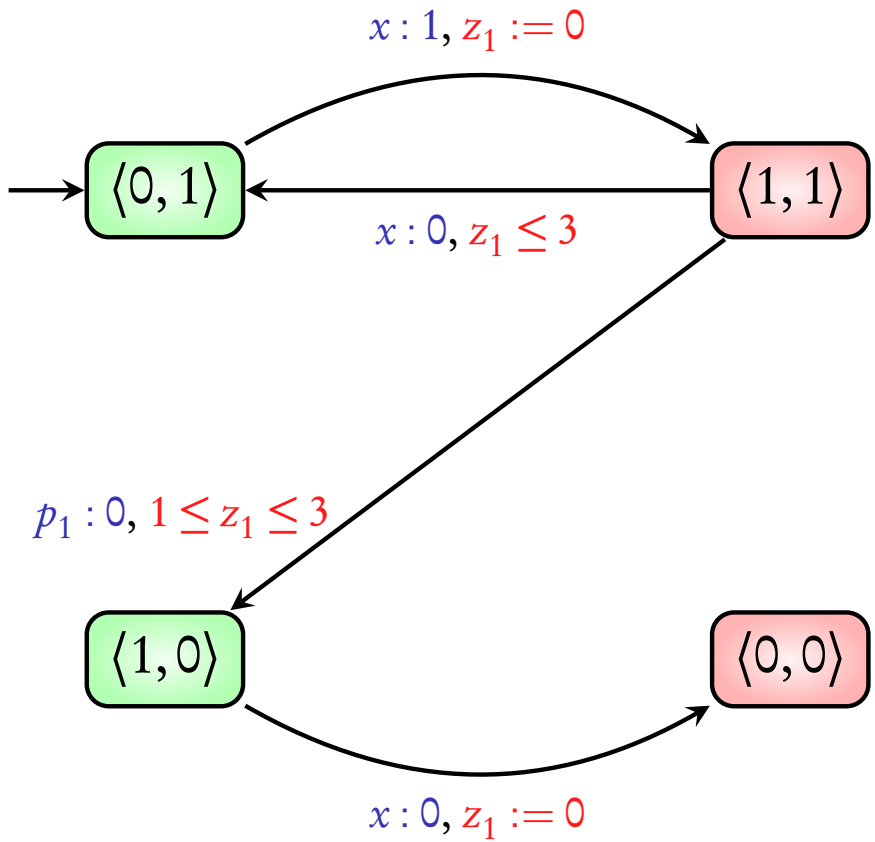


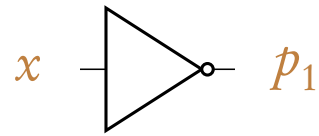
$$\langle\, x\,,\, p_1\,\rangle$$



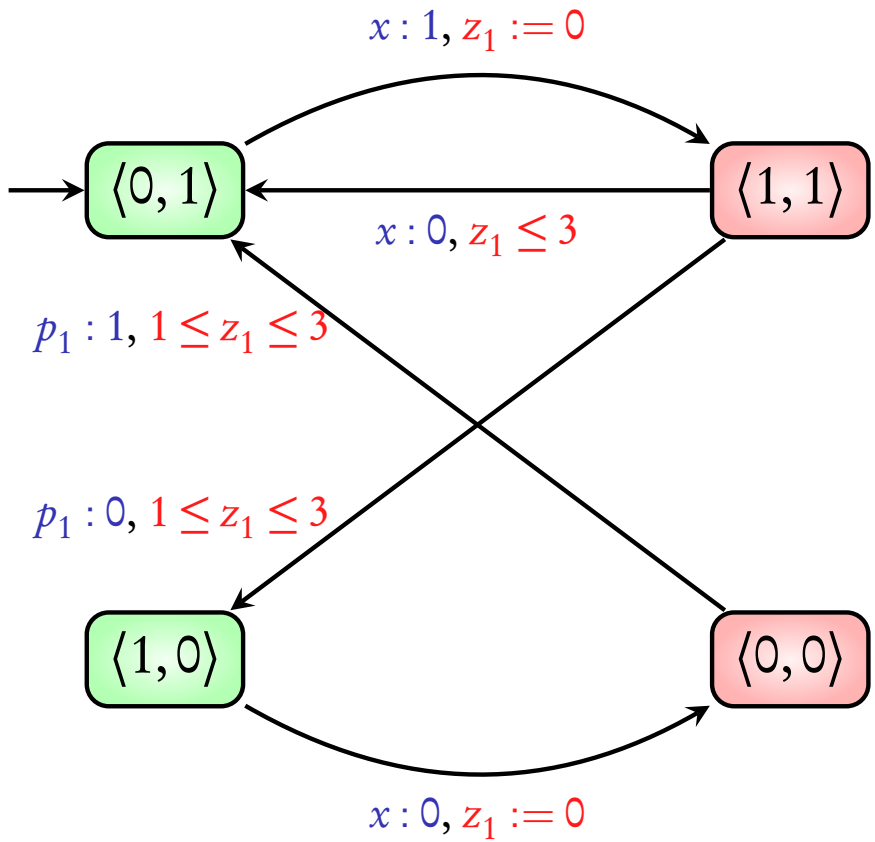


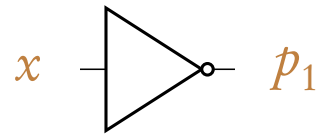
$$\langle\, x\,,\, p_1\,\rangle$$



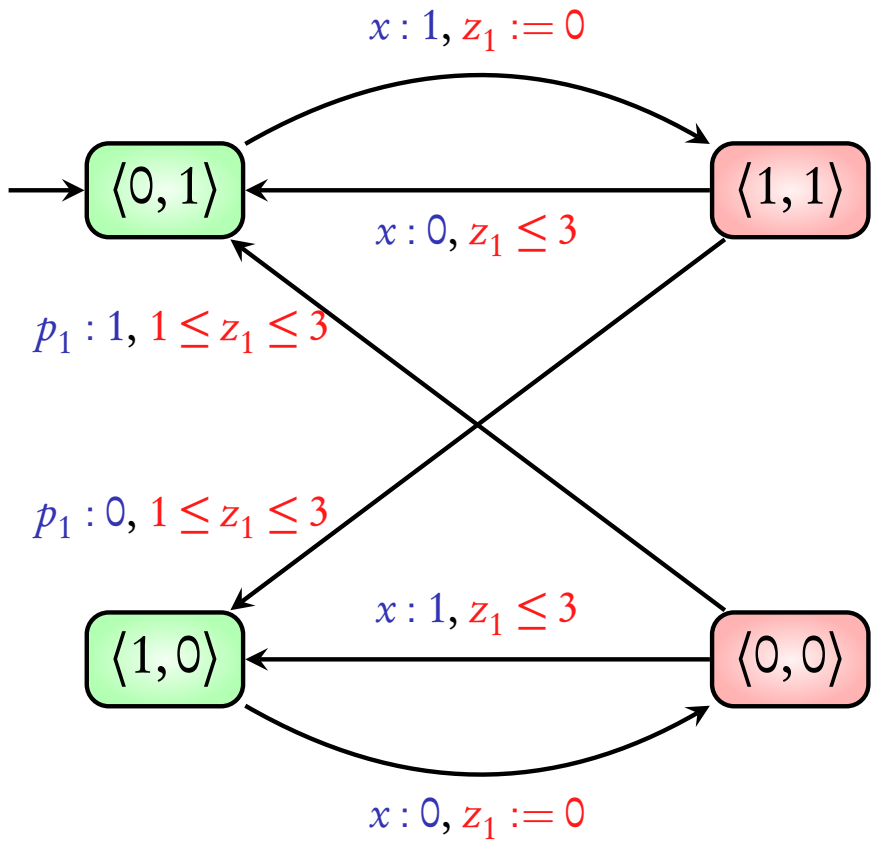


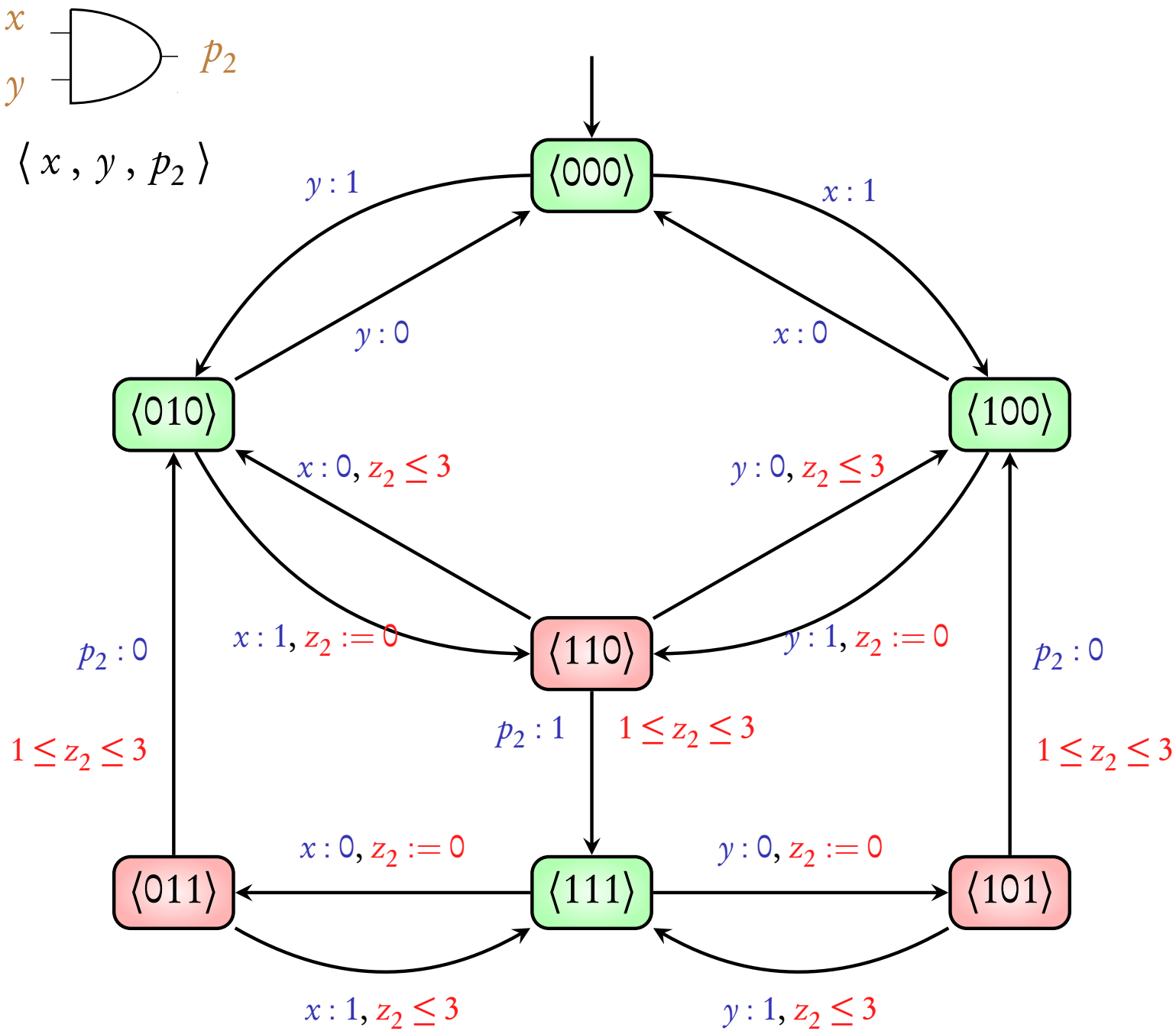
$$\langle\, x\,,\, p_1\,\rangle$$

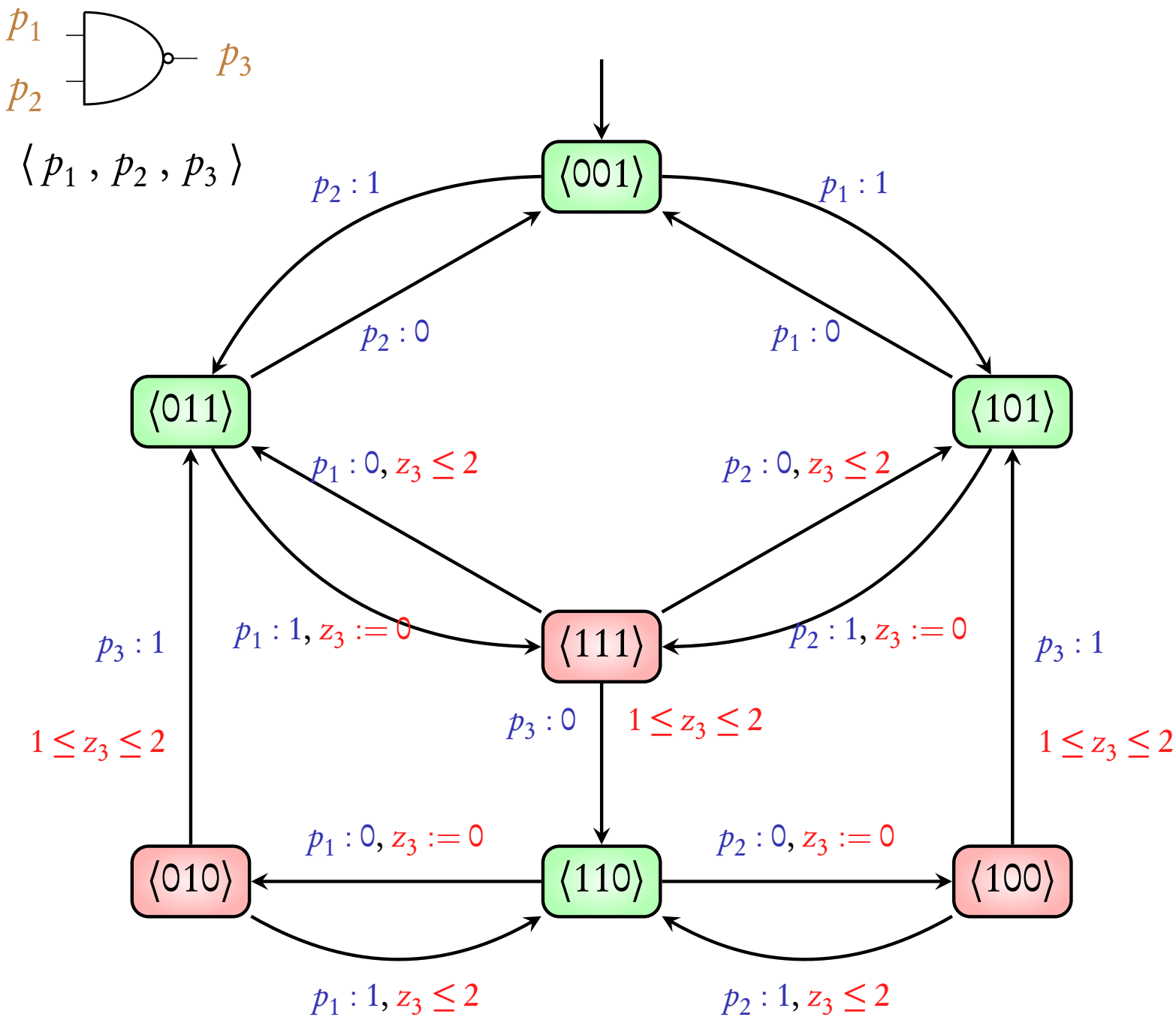


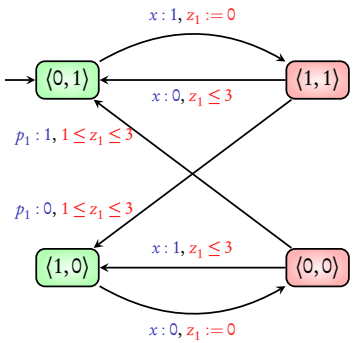


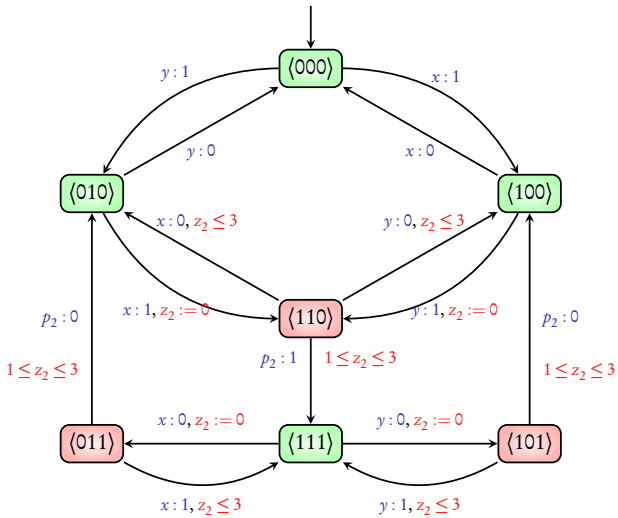
$$\langle\, x\,,\, p_1\,\rangle$$

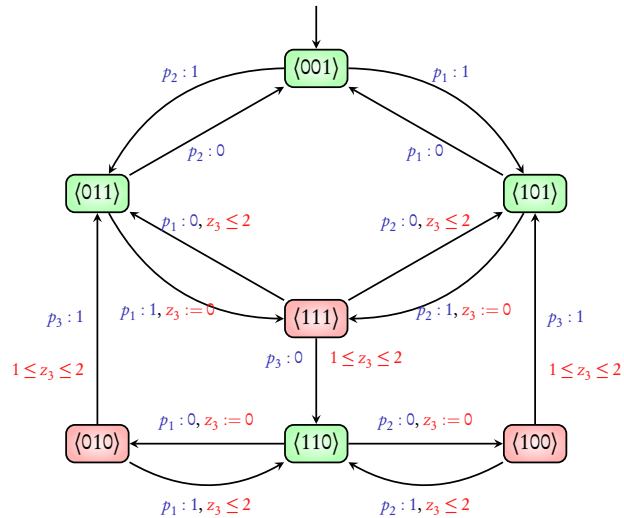



x
y
p_2
$\langle x , y , p_2 \rangle$
⟨000⟩
⟨010⟩
⟨100⟩
⟨110⟩
⟨011⟩
⟨111⟩
⟨101⟩
$y : 1$
$x : 1$
$y : 0$
$x : 0$
$x : 0, z_2 \leq 3$
$y : 0, z_2 \leq 3$
$x : 1, z_2 := 0$
$y : 1, z_2 := 0$
$p_2 : 0$
$1 \leq z_2 \leq 3$
$p_2 : 1$
$1 \leq z_2 \leq 3$
$p_2 : 0$
$1 \leq z_2 \leq 3$
$x : 0, z_2 := 0$
$y : 0, z_2 := 0$
$x : 1, z_2 \leq 3$
$y : 1, z_2 \leq 3$


p_1
p_2
p_3
$\langle p_1 , p_2 , p_3 \rangle$
$\langle 001 \rangle$
$\langle 011 \rangle$
$\langle 101 \rangle$
$\langle 111 \rangle$
$\langle 010 \rangle$
$\langle 110 \rangle$
$\langle 100 \rangle$
$p_2 : 1$
$p_1 : 1$
$p_2 : 0$
$p_1 : 0$
$p_1 : 0, z_3 \leq 2$
$p_2 : 0, z_3 \leq 2$
$p_3 : 1$
$1 \leq z_3 \leq 2$
$p_1 : 1, z_3 := 0$
$p_2 : 1, z_3 := 0$
$p_3 : 1$
$1 \leq z_3 \leq 2$
$p_3 : 0$
$1 \leq z_3 \leq 2$
$p_1 : 0, z_3 := 0$
$p_2 : 0, z_3 := 0$
$p_1 : 1, z_3 \leq 2$
$p_2 : 1, z_3 \leq 2$







Synchronous product of above will give timed transition system for circuit

Summary

- Modeling **timing constraints** in systems
- **Timed** transition systems
- Model-checker **UPPAAL**

Summary

- Modeling **timing constraints** in systems
- **Timed** transition systems
- Model-checker **UPPAAL**

A theory of timed automata, by *Alur and Dill*.
Theoretical Computer Science Journal, 1994