

TCCS

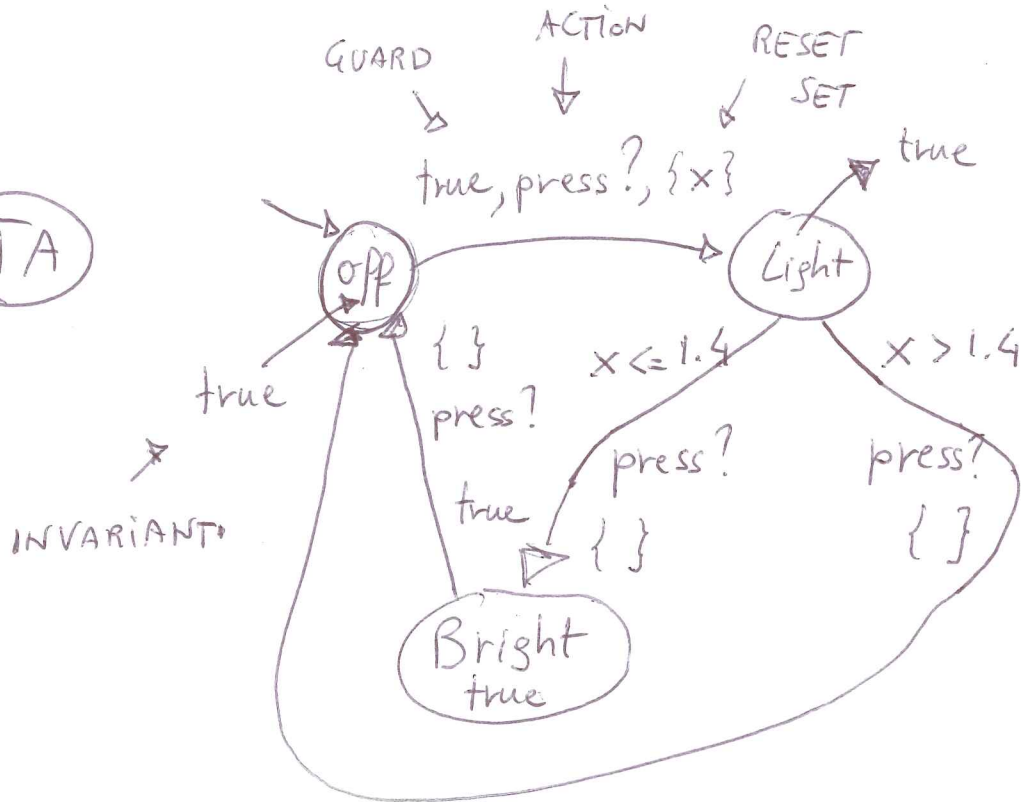
$\text{Off} \stackrel{\Delta}{=} \text{press. Light}$

$\text{Light} \stackrel{\Delta}{=} \text{press. Bright} + \varepsilon(1,4). \tau. \text{Off}$

$\text{Bright} \stackrel{\Delta}{=} \text{press. Off}$

14/12/16-1  
 LUCA TESEI  
 RPSV - 16-17  
 UNICAM

$\overline{IA}$



$x$  clock  $V: x \in \mathbb{R}^{\geq 0}$

$$\frac{\partial x}{\partial t} = 1$$

SINTASSI  $l_0,$

$\forall TA A = \langle L, Act, C, I, \rightarrow \rangle$

ALUR & DILL 1994 TCS


A THEORY OF TIMED AUTOMATA

L set of Locations FINITE

Act set of Actions  $Act = \{c? \mid c \text{ channel}\}$

C set of Clocks FINITE  $\cup \{c! \mid c \text{ channel}\}$

$I: L \rightarrow \Phi(c)$

$\uparrow$   
  
 CLOCK CONSTRAINTS

$\cup \{\tau\}$   
 $\equiv \cup N$  - names of non-communication actions  
 $\uparrow$  Non actions

Non necessario

14/12/16 - 2

$l_0 \in L$  INITIAL LOCATION

$\rightarrow \subseteq L \times \Phi(c) \times Act \times 2^C \times L$  EDGE  $e = (l_1, g, a, r, l_2)$

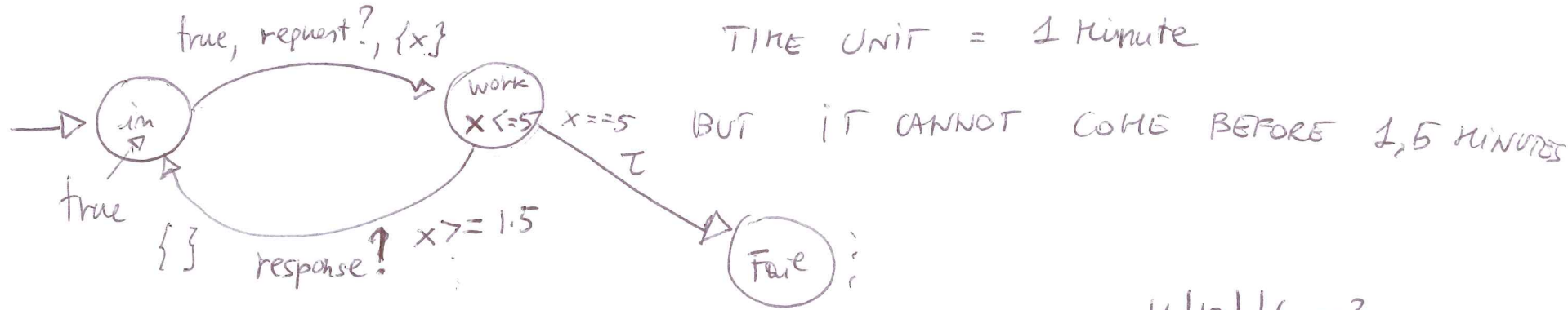
STATO •  
 LOCALIZIONE DI PARTENZA

RESET SET LOCALIZIONE DI ARRIVO

$l_1 \xrightarrow{g, a, r} l_2$

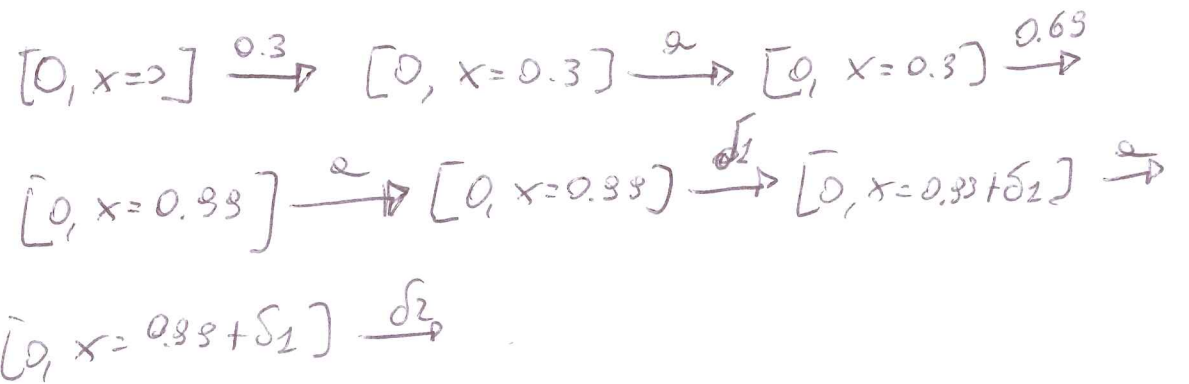
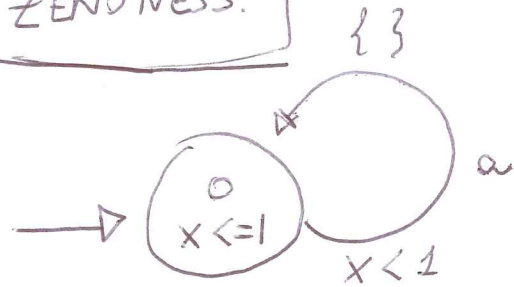
RESPONSE MUST COME BEFORE 5 minutes

TIME UNIT = 1 minute



14/12/16 -3

ZENONESS:



$$\sum \frac{1}{n^2} < \infty$$

$$0.99 + \sum_{i=1}^{\infty} \delta_i \leq 1$$

1) STANDALONE TA

# SEMANTICA

14/12/16 - 4

2) NETWORK OF TA ← UPPAAL

1) LA SEMANTICA DI

$$A = \langle L, Act, C, I, \rightarrow \rangle$$

SINTAX

è UN TLTS

$$\langle S, Act \cup \mathbb{R}^{\geq 0}, \rightarrow \rangle$$

SEMANTICS

$$\rightarrow S \times Act \cup \mathbb{R}^{\geq 0} \times S$$

~~SEMANTICO~~  $S = L \times [C \rightarrow \mathbb{R}^{\geq 0}]$

FUNZIONE DI VALUTAZIONE DEI CLOCK

$$(l; v)$$

SPAZIO DELLE FUNZIONI CON DOMINIO C E CODOMINIO  $\mathbb{R}^{\geq 0}$

e.g.  $v(x) = 1.4$

$$v(y) = 0.35$$

$$[0, x = 0.38]$$

$$l = 0$$

$$v = [x = 0.38]$$

$$C = \{x\}$$

→ SEMANTICA

2 REGOLE DI INFERENZA

L'INVARIANTE E'  
SODDISFATTO SE PASSA  
UN TEMPO d?

$$\frac{d \in \mathbb{R}^{\geq 0} \quad \cancel{V \models I(e)} \quad V+d \models I(e)}{(e, V) \xrightarrow{d} (e, V+d)} \quad \text{(TIME PASS)}$$

$$V+d \in [C \rightarrow \mathbb{R}^{\geq 0}]$$

$$V+d(x) = V(x) + d$$

$\forall x \in C$  (ACTION)

(SEMANTICA)  $V[e] \models I(e')$

$$\frac{d \in Act \quad e \xrightarrow{g, a, r} e' \in E \quad V \models g}{(e, V) \xrightarrow{a} (e', V[r])}$$

$$\frac{1}{V/r}$$

$$|4|12|16-5$$

e.g.

$$V = [x=0.3, y=1.4]$$

$$V+3.1 = [x=3.4, y=4.5]$$

$$V[r] \in [C \rightarrow \mathbb{R}^{\geq 0}]$$

$$V[r](x) = \begin{cases} 0 & \text{se } x \in r \\ V(x) & \text{se } x \notin r \end{cases}$$

e.p.  $V \models I(e)$

$$V[\{y\}] = [x=0.3, y=0]$$

Clock CONSTRAINTS

$$\bar{\Phi}(C) \triangleq$$

$$g ::= x \bowtie c \mid g \wedge g$$

$x \in \mathbb{C}$  clock

$c \in \mathbb{N}$

$\bowtie \in \{<, <=, =, >=, >\}$

SS2) non c'è  $\rightarrow$  e  $\vee$

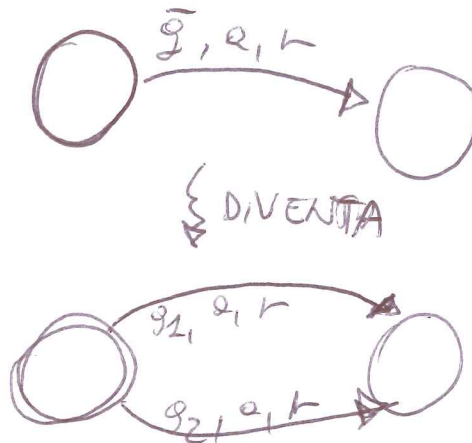
$$\bar{g} \vee = \neg (x > 3) \equiv x <= 3$$

$$\neg (x > 5 \wedge y < 4) \equiv$$

$$\begin{array}{l} g_1 \\ \text{---} \\ x <= 5 \vee \\ y >= 4 \end{array}$$

$$= g$$

$g_2$



14/12/16-6

SS2)  $c \in \mathbb{N}$

SE VOLESSI USARE IN UNA GUARDIA

$$x < 1.4$$

POSSO SEMPRE RIDEFINIRE LA TIME UNIT

$$1 \text{ TU} = 1/10 \text{ s} \Rightarrow \text{~~x < 1.4~~}$$

$$x < 1.4 \xrightarrow{\text{DIVENTA}} x < 14$$

$$x >= 3 \xrightarrow{\text{DIVENTA}} x >= 30$$

RELAZIONE  $F \subseteq \mathbb{R}^n \times \mathbb{R}^m$

~~xi~~  $V \subseteq \mathbb{R}^n \times \mathbb{R}^m$  iff  $V(x) \subseteq \mathbb{R}^m$

$V \subseteq g_1 \wedge g_2$  iff  $V \subseteq g_1$  and  $V \subseteq g_2$

---

~~inv.~~  $\Phi(K)$  è L'INSIEME DEI VINCOLI PER LE GUARDIE

PER GLI INVARIANTI CI SONO DELLE LIMITAZIONI

SI VUOLÈ CHE NEGLI INVARIANTI NON CI SIANO "BUCHI"

È CHE GLI INVARIANTI SIANO PAST-CLOSED

SI VEDA EX 10.3 pag. 178

14/12/16 - 7

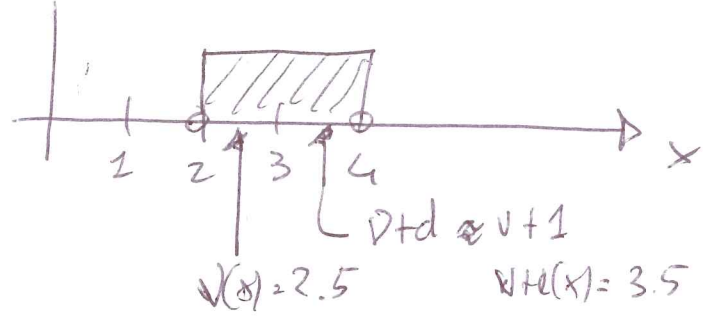


1) INVARIANTI

INTERVAL CLOSED

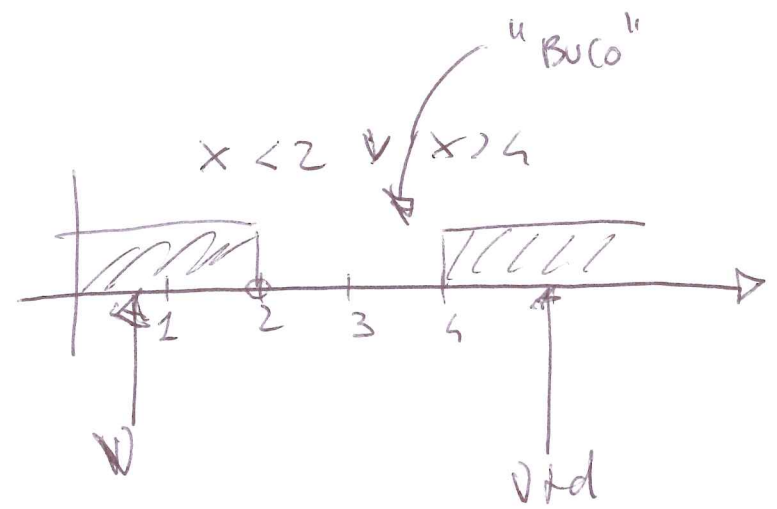
$g$  is int.-closed iff  $\left[ \begin{array}{l} (\forall \epsilon > 0 \wedge \forall d \in g) \\ \Rightarrow \\ \forall d' \leq d \quad \forall d' \in g \end{array} \right]$

$g = x < 4 \wedge x > 2$



OK

[4/12/16 - 8



NO  
 $\Rightarrow$   
 $\Rightarrow$  false

PER COME È FATTO

$\Phi(c)$

NON SI VERIFICA

MAI

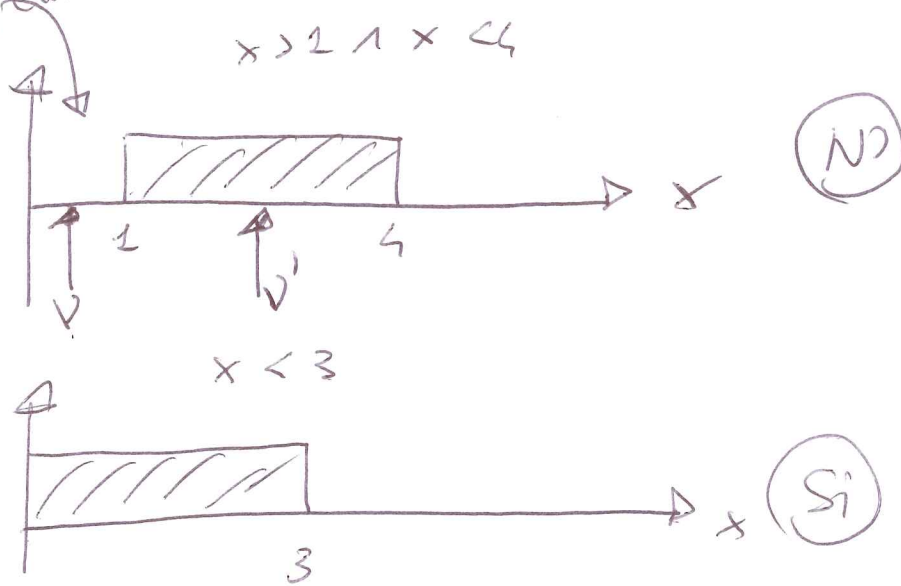


2)  $g$  PAST-CLOSED OR DOWNWARD CLOSED iff  $v \leq v'$  in  $[C \rightarrow \mathbb{R}^{\geq 0}]$

$\forall v, v'$  .  $(v \neq g \wedge v \leq v') \Rightarrow v \neq g$

$v \leq v'$  sse  
 $\forall x \in C \quad v(x) \leq v'(x)$   
 POINT WISE

"PASSATO NON CHIUSO"



14/12/16 - 9

$\Rightarrow x \leq 3$  OR INVARIANTE

$x \neq 2 \wedge x \neq 3$  NON OR COME INVARIANTE (non è intervallo-chiuso)

$x > 2 \wedge x < 3$  NON OR " " (non è DOWNWARD CLOSED)

# NETWORK OF TIMED AUTOMATA

15/12/16 - 10

$$N = A_1 \parallel A_2 \parallel \dots \parallel A_m \quad m > 1$$

$$A_i = \langle L_i, Act_i, C_i, I_i, l_0^i, \rightarrow_i \rangle$$

$$Act = \bigcup_{i=1}^m Act_i$$

TIMED AUTOMATA CHE COMUNICANO  
TRAMITE CANALI DI SINCRONIZZAZIONE  
INPUT/OUTPUT (PURE  
SYNCHRONIZATION)

$$\forall i, j \in \{1, \dots, m\}. i \neq j \Rightarrow C_i \cap C_j = \emptyset \quad (\text{NO SHARED CLOCKS})$$

$$C = \bigcup_{i=1}^m C_i$$

LA SEMANTICA È SEMPRE UN T LTS  $\langle S, Act, \rightarrow \rangle$  dove

$$S = \left( \prod_{i=1}^m L_i \right) \times [C \rightarrow \mathbb{R}^{\geq 0}]$$

$$\rightarrow \subseteq S \times Act \cup \mathbb{R}^{\geq 0} \times S$$

$$\downarrow$$

$$(l_1, l_2, \dots, l_m, v)$$

→ NELLO STATO SI RICORDA IL VALORE DI  
TUTTI I CLOCKS E LA LOCALIZIONE IN  
CUI SI TROVA CIASCUNA DELLA "RETE"

# REGOLE DI INFERENZA

GLI INVARIANTI DI TUTTE LE  
LOCALIZIONI SONO RISPETTATI

$$v+d \models \bigwedge_{i=1}^m I_i(l_i) \quad d \in \mathbb{R}^{\geq 0}$$

15/12/16 - 11

TIME-PASS

$$(l_1, \dots, l_m, v) \xrightarrow{d} (l_1, \dots, l_m, v+d)$$

NON AZIONE DI COMUNICAZIONE  
SODDISFO TUTTI GLI INV.

$$i \in \{1, \dots, m\}$$

$$\alpha \in \{\tau\} \cup N$$

ACTION-NO-SYNCH

$$l_i \xrightarrow{g_i, \alpha, r} l_i' \in \rightarrow_i \quad v \models g_i$$

$$v[r] \models \bigwedge_{j=1, j \neq i}^m I_j(l_j) \wedge I_i(l_i')$$

$$(l_1, \dots, l_m, v) \xrightarrow{\alpha} (l_1, \dots, l_i', \dots, l_m, v[r])$$

$$l_i \xrightarrow{g_i, \alpha, r_i} l_i'$$

$\alpha$  and  $\beta$  are COMPLEMENTARY (?/!)  $i \neq j$

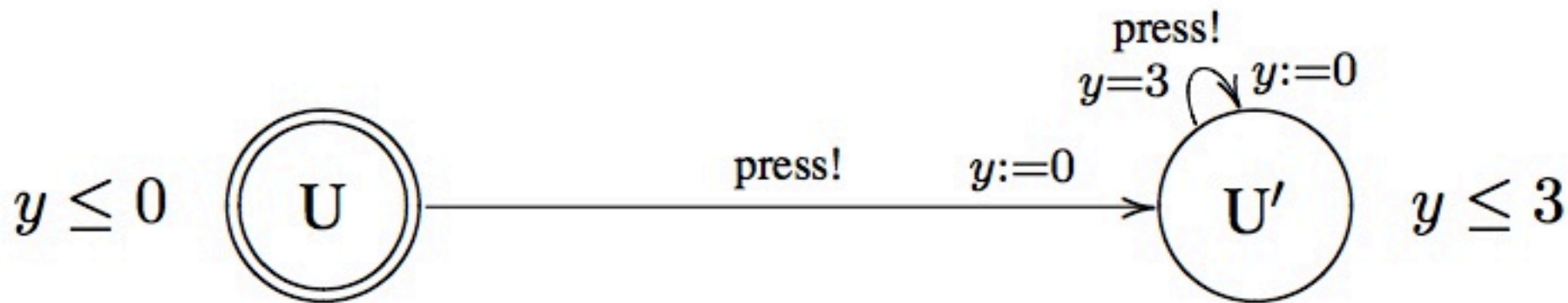
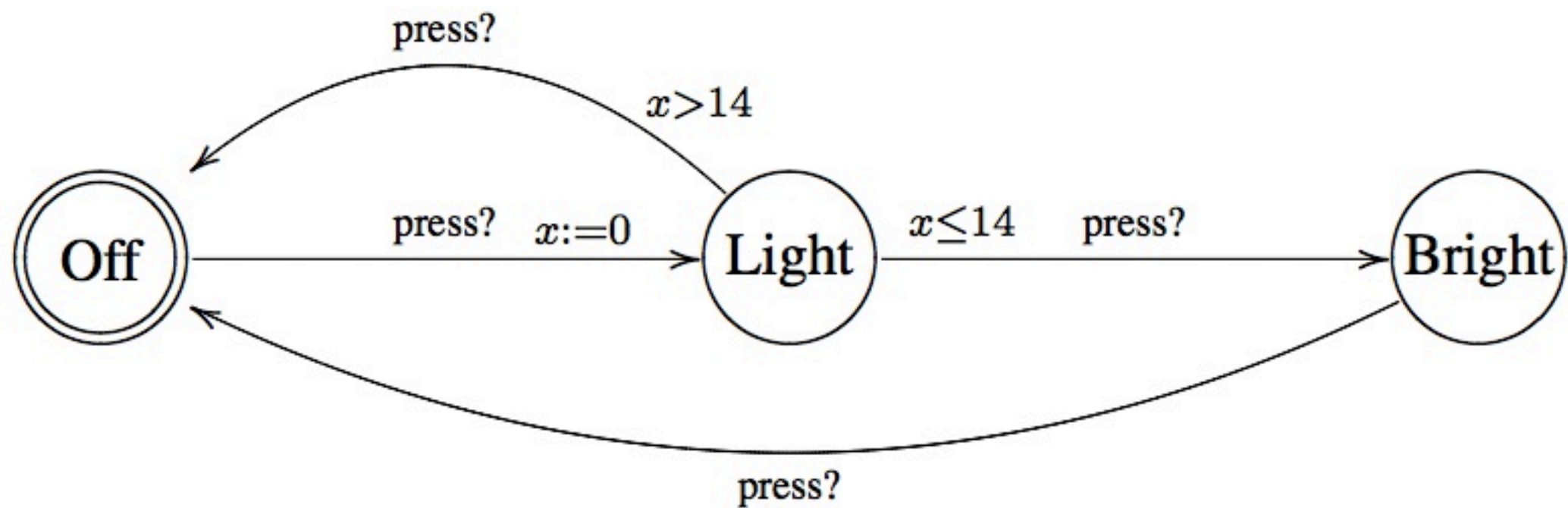
$$v \models g_i \quad v[\tau] \models \bigwedge_{\substack{k=1 \\ k \neq i \\ k \neq j}}^m I_k(l_k) \wedge I_i(l_i') \wedge I_j(l_j')$$

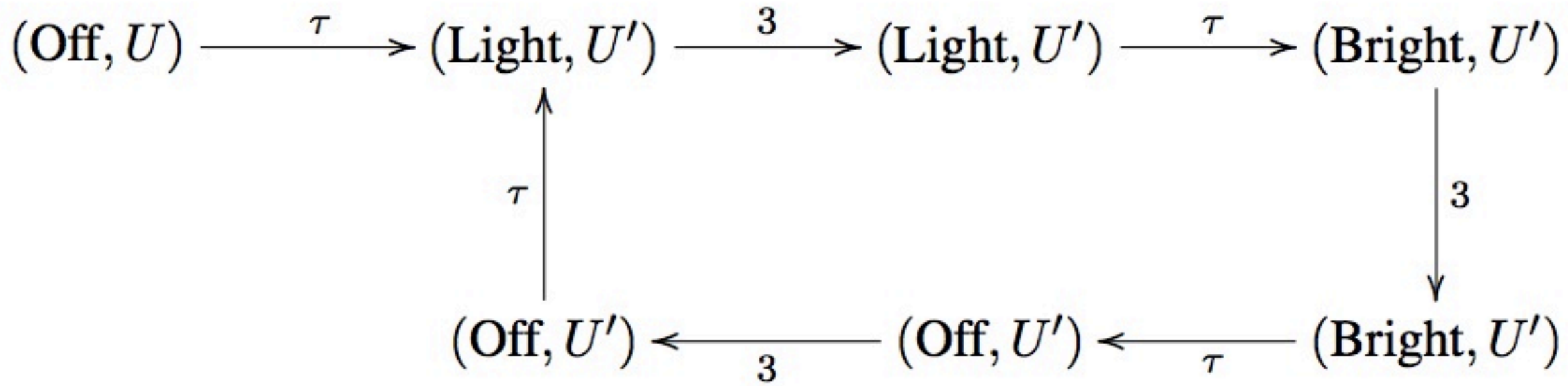
$$l_j \xrightarrow{g_j, \beta, r_j} l_j'$$

$$v \models g_j$$

ACTION-SYNCH

$$(l_1, \dots, l_i, \dots, l_j, \dots, l_m, v) \xrightarrow{\tau} (l_1, \dots, l_i', \dots, l_j', \dots, l_m, v[\tau])$$





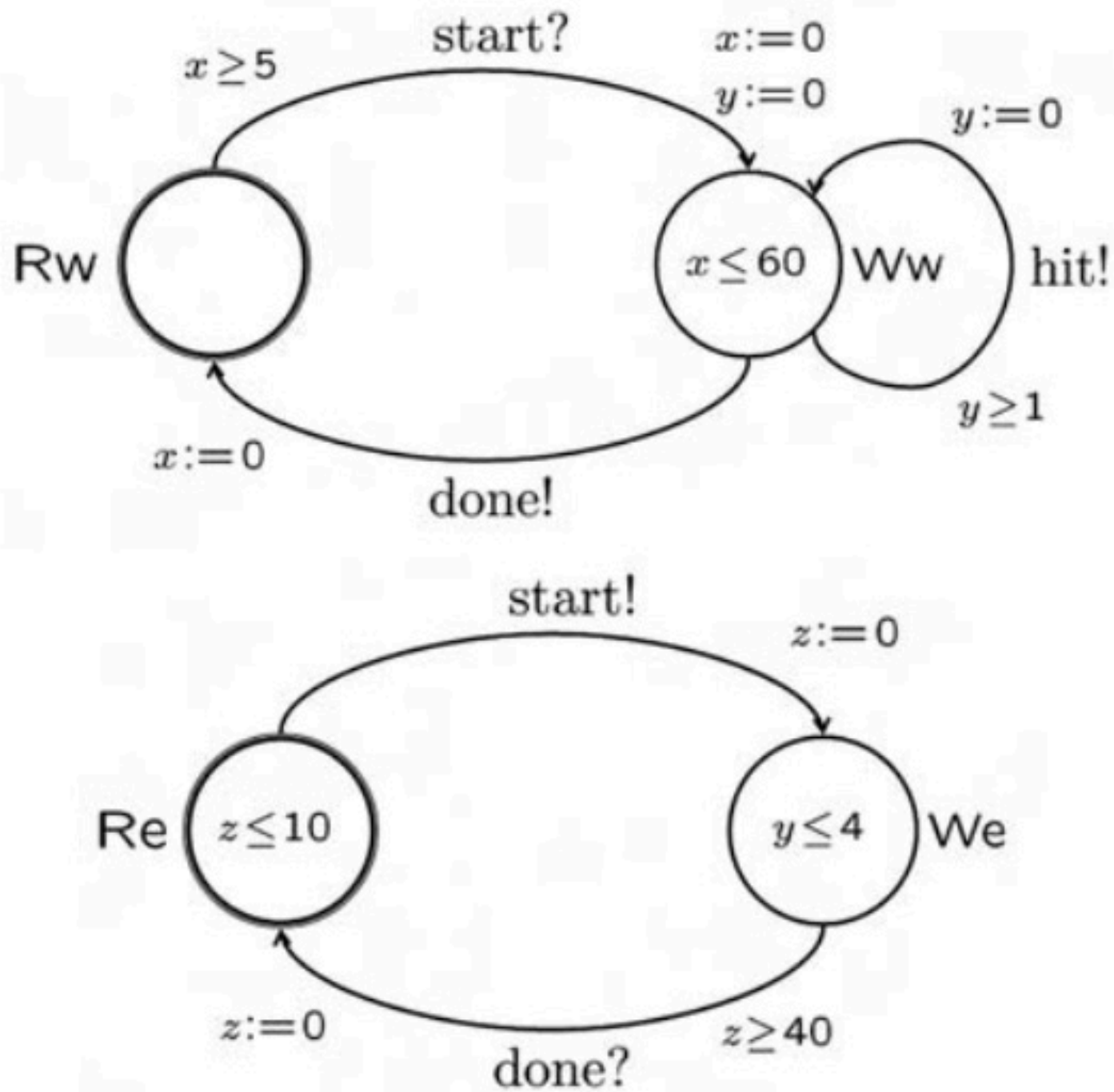


Figure 10.4 The lazy worker and his demanding employer.



**Exercise 10.17** *Implement the network of timed automata consisting of the fast user and the light switch in the verification tool UPPAAL available at*

*[www.uppaal.org](http://www.uppaal.org).*

*Simulate the behaviour of the system using the tool, and use the tool to check whether this network contains deadlocks. Similarly, implement and analyze the network of timed automata consisting of the lazy worker and the demanding employer from Exercise 10.16. Note that you will need to provide timed-automata models for hitting nails (for instance, a nail may need two hits before it is completely down) in order to have a closed system, as required by UPPAAL. ◆*