TCCS

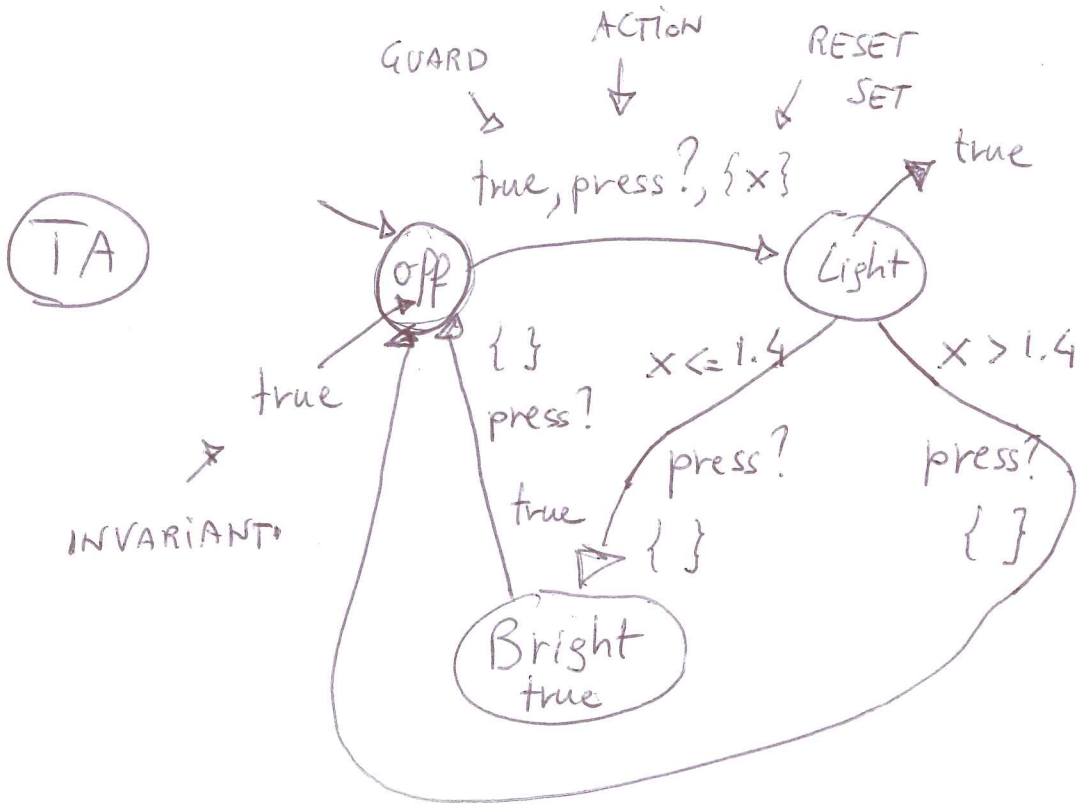
Off $\triangleq$ press. Light

Light $\triangleq$ press. Bright + $\varepsilon(1,4).\tau.Off$ **(errore)**

Bright $\triangleq$ press. Off

e(1.4).tau.press.Off

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



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

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

SINTASSI

TA $A = \langle L, Act, C, I, l_0, \rightarrow \rangle$ ≠ ALUR & DILL 1994 TCS — A THEORY OF TIMED AUTOMATA

L set of locations FINITE

Act set of Actions $Act = \{c? \mid c \text{ channel}\} \cup \{c! \mid c \text{ channel}\} \cup \{\tau\} \cup N$ — names of non-communication actions

C set of Clocks FINITE

$I : L \rightarrow \Phi(C)$ — CLOCK CONSTRAINTS

τ Non necessario

$l_0 \in L$ INITIAL LOCATION

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

- l_1: STATO o LOCAZIONE DI PARTENZA
- g: GUARDIA
- a: AZIONE
- r: RESET SET
- l_2: LOCAZIONE DI ARRIVO

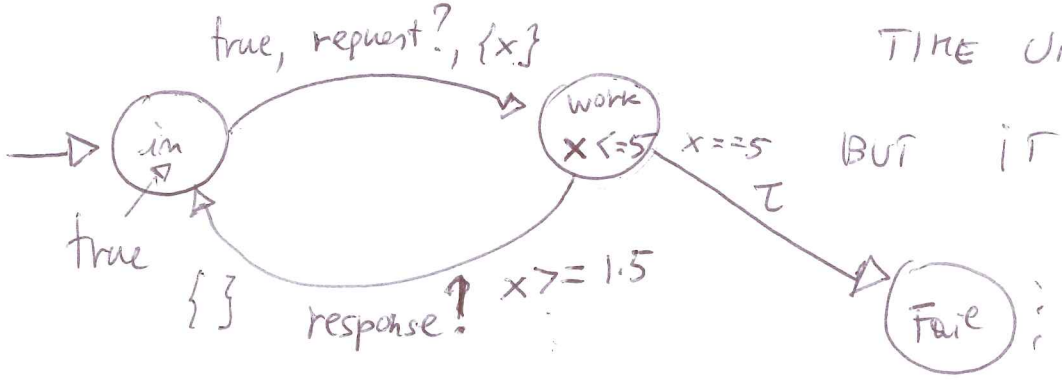
$l_1 \xrightarrow{g,a,r} l_2$

14/12/16 - 2

RESPONSE MUST COME BEFORE 5 Minutes

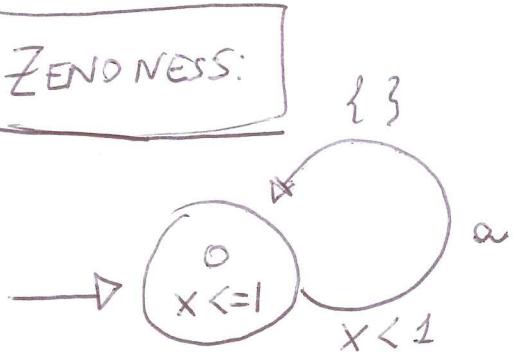
TIME UNIT = 1 Minute

BUT IT CANNOT COME BEFORE 1,5 MINUTES



14|12|16 -3

ZENONESS:



$[0, x=0] \xrightarrow{0.3} [0, x=0.3] \xrightarrow{a} [0, x=0.3] \xrightarrow{0.69}$

$[0, x=0.99] \xrightarrow{a} [0, x=0.99] \xrightarrow{\delta_1} [0, x=0.99+\delta_1] \xrightarrow{a}$

$[0, x=0.99+\delta_1] \xrightarrow{\delta_2}$

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

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

SEMANTICA

14/12/16 - 4

1) STANDALONE TA

2) NETWORK OF TA ← UPPAAL

1) LA SEMANTICA DI $A = \langle L, Act, C, I, \rightarrow \rangle$ (l: locazione; →: SINTAX)

è UN TLTS $\langle S, Act \cup \mathbb{R}^{\geq 0}, \rightarrow \rangle$ → SEMANTICS

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

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

$(l; v)$

$[0, x = 0.38]$

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

v FUNZIONE DI VALUTAZIONE DEI CLOCK

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

$v(y) = 0.3\overline{5}$

$l = 0$

$v = [x = 0.38)$

$C = \{x\}$

→ SEMANTICA

2 REGOLE DI INFERENZA

L'INVARIANTE È SODDISFATTO SE PASSA UN TEMPO d?

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

$\nu + d \in [C \to \mathbb{R}^{\geq 0}]$

$\nu + d\,(x) = \nu(x) + d \quad \forall x \in C$

$$\frac{a \in Act \quad \ell \xrightarrow{g,a,r} \ell' \in \to \quad \nu \models g}{(\ell, \nu) \xrightarrow{a} (\ell', \nu[r])} \text{(ACTION)}$$

(SINTATTICA) $\nu[r] \models I(\ell')$

ν / r 14/12/16 -5

e.g.

$\nu = [x = 0.3,\ y = 1.4]$

$\nu + 3.1 = [x = 3.4,\ y = 4.5]$

$\nu[r] \in [C \to \mathbb{R}^{\geq 0}]$

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

$\nu = [x = 0.3,\ y = 1.4]$

e.g. $\nu[\{y\}] = [x = 0.3,\ y = 0]$

CLOCK CONSTRAINTS

$\Phi(C) \triangleq$

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

$x \in C$ CLOCK

$c \in \mathbb{N}$

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

DSS2) $c \in \mathbb{N}$

SE VOLESSI USARE IN UNA GUARDIA

$x < 1.4$

POSSO SEMPRE RIDEFINIRE LA TIME UNIT

$1\,TU = 1/10\,s \Rightarrow$ [illegible]

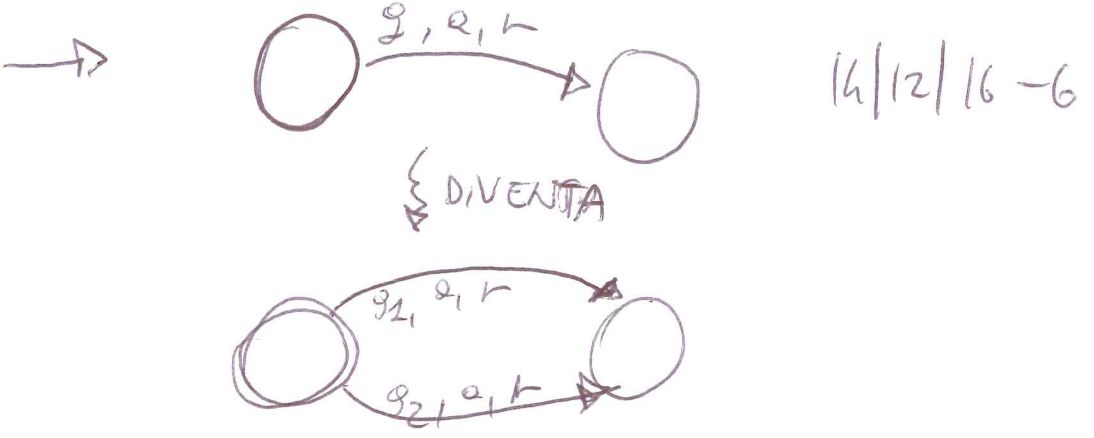
$x < 1.4$ DIVENTA $x < 14$

$x >= 3$ DIVENTA $x >= 30$

DSS2) non c'è $\dot{\neg}$ e $\vee$

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

$\neg(x > 5 \wedge y < 4) \equiv (\underbrace{x <= 5}_{g_1} \vee \underbrace{y >= 4}_{g_2}) = g$



14|12|16 −6

RELAZIONE $\models$

x SODDISFA $V \models x \bowtie c$ iff. $V(x) \bowtie c$

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

$\Phi(C)$ È L'INSIEME DEI VINCOLI PER LE GUARDIE

PER GLI INVARIANTI CI SONO DELLE <u>LIMITAZIONI</u>

SI VUOLE CHE NEGLI INVARIANTI NON CI SIANO "BUCHI"

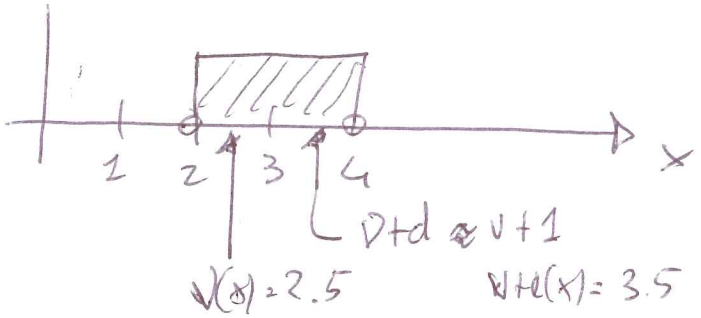
E CHE GLI INVARIANTI SIANO PAST-CLOSED

SI VEDA EX 10.3 pag. 178

1) INVARIANTI ⊗ INTERVAL CLOSED

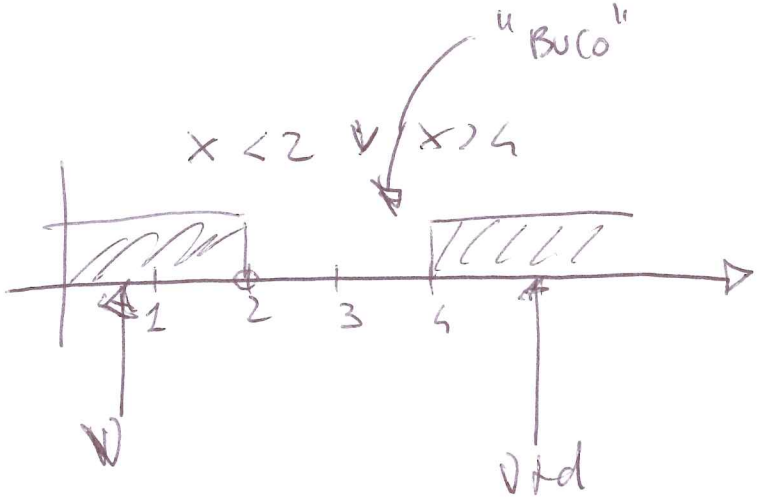
g is int.-closed iff $\left[(v \models g \wedge v+d \models g) \Rightarrow \forall d' \leq d \;\; v+d' \models g \right]$

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



OK

14|12|16 - 8



NO ⇒ PER COME È FATTO $\Phi(C)$

" ⇒ " falso

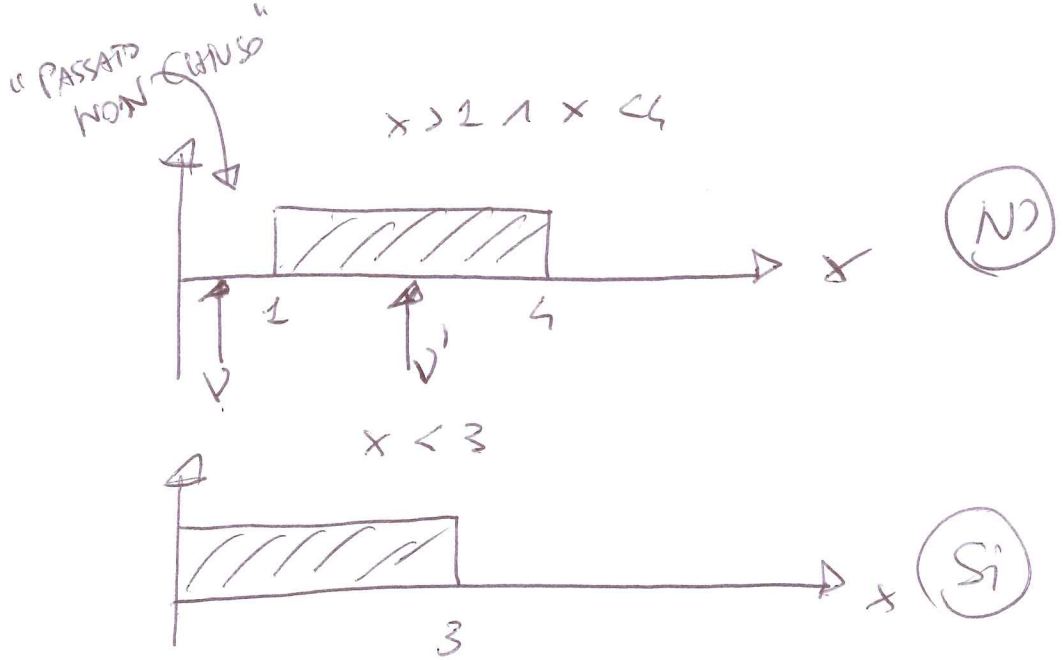
NON SI VERIFICA MAI

2) φ PAST-CLOSED OR DOWNWARD CLOSED iff $\forall \nu \leq \nu'$ in $[C \to \mathbb{R}^{\geq 0}]$

$\forall \nu, \nu' . \left(\nu' \models \varphi \wedge \nu \leq \nu' \right) \Rightarrow \nu \models \varphi$

$\nu \leq \nu'$ sse $\forall x \in C \quad \nu(x) \leq \nu'(x)$

POINT WISE



14/12/16 - 9

$\Rightarrow$ $x \leq 3$ OK INVARIANTE

$x \not\leq 2 \wedge x \not\leq 3$ NON OK COME INVARIANTE (non è interval-closed)

$x \geq 1 \wedge x < 3$ NON OK " " (non è DOWNWARD CLOSED)

NETWORK OF TIMED AUTOMATA

15/12/16 - 10

$N = A_1 \parallel A_2 \parallel \cdots \parallel A_m \qquad m > 1$

$A_i = \langle L_i, Act_i, C_i, I_i, l_0^i, \longrightarrow_i \rangle$ TIMED AUTOMATA CHE COMUNICANO TRAMITE CANALI DI SINCRONIZZAZIONE INPUT/OUTPUT (PURE SYNCHRONIZATION)

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

$\forall i, j \in \{1, \ldots, m\}.\ i \neq j \Rightarrow C_i \cap C_j = \phi$ (NO SHARED CLOCKS)

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

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

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

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

$(l_1, l_2, \ldots, l_m, v)$ → NELLO STATO SI RICORDA IL VALORE DI TUTTI I CLOCK E LA LOCAZIONE IN CUI SI TROVA CIASCUN TA DELLA "RETE"

REGOLE DI INFERENZA

GLI INVARIANTI DI TUTTE LE LOCAZIONI SONO RISPETTATI

15/12/16 - 11

TIME-PASS

$$\frac{\nu + d \models \bigwedge_{i=1}^{n} I_i(\ell_i) \qquad d \in \mathbb{R}^{\geq 0}}{(\ell_1, \dots, \ell_n, \nu) \xrightarrow{d} (\ell_1, \dots, \ell_n, \nu + d)}$$

NON AZIONE DI COMUNICAZIONE

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

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

SODDISFO TUTTI GLI INV.

ACTION-NO-SYNCH

$$\frac{\ell_i \xrightarrow{g, a, r} \ell_i' \in \longrightarrow_i \qquad \nu \models g \qquad \nu[r] \models \bigwedge_{\substack{j=1 \\ j \neq i}}^{n} I_j(\ell_j) \wedge I_i(\ell_i')}{(\ell_1, \dots, \ell_n, \nu) \xrightarrow{\alpha} (\ell_1, \dots, \ell_i', \dots, \ell_n, \nu[r])}$$

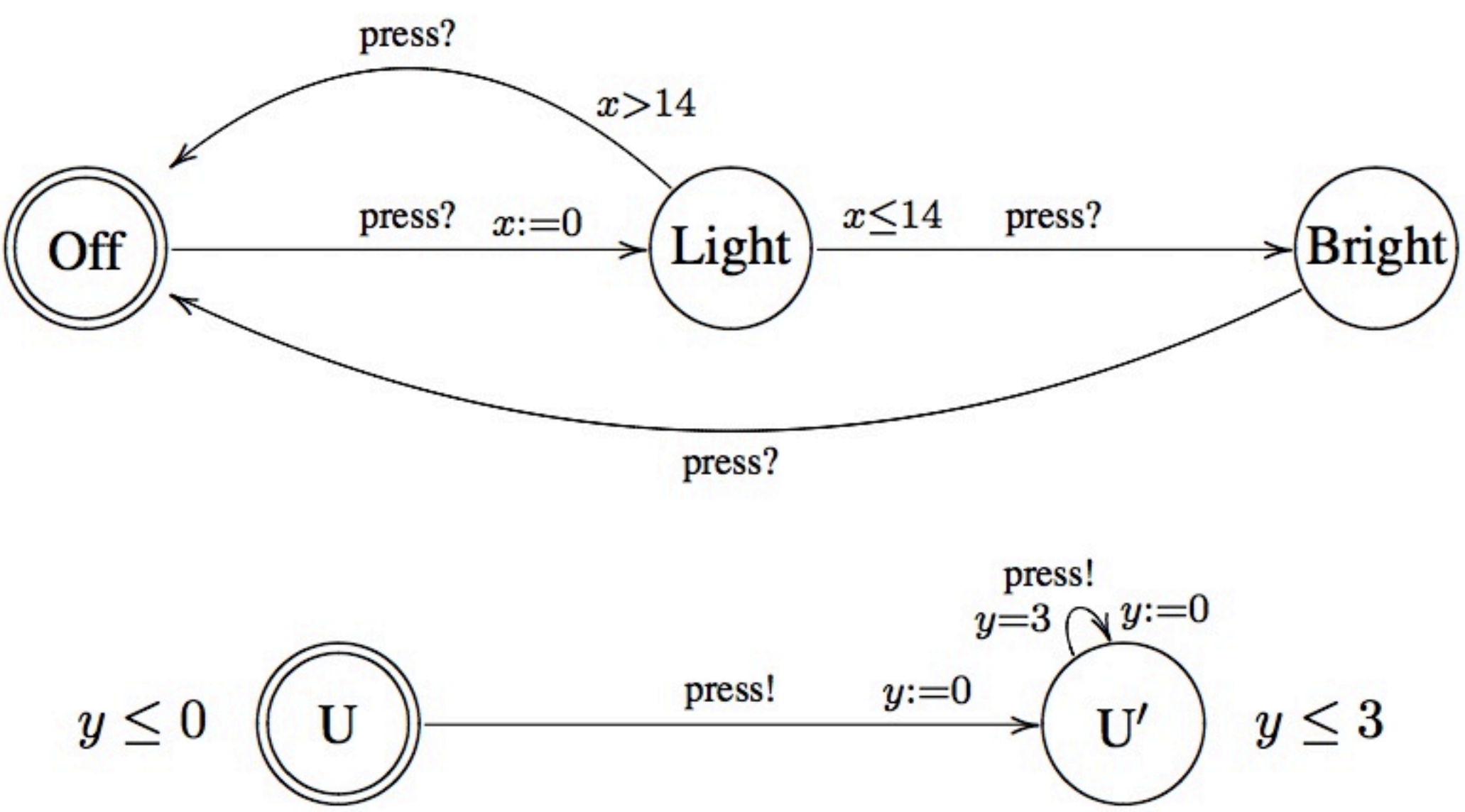
$r_i \cup r_j$

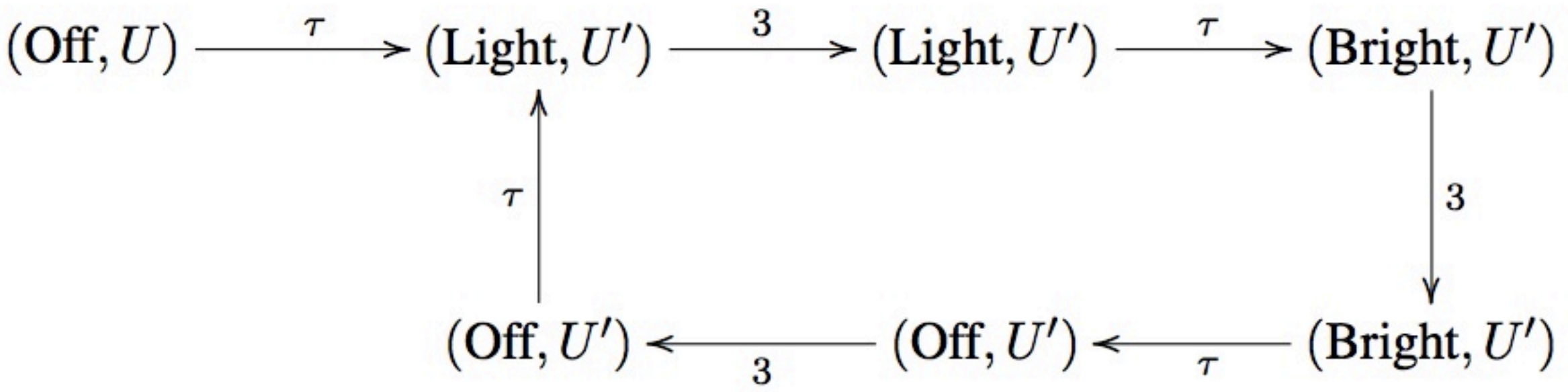
α and β are COMPLEMENTARY (?!) $\qquad i \neq j$

ACTION-SYNCH

$$\frac{\ell_i \xrightarrow{g_i, \alpha, r_i} \ell_i' \qquad \ell_j \xrightarrow{g_j, \beta, r_j} \ell_j' \qquad \nu \models g_i \qquad \nu \models g_j \qquad \nu[\,] \models \bigwedge_{\substack{k=1 \\ k \neq i \\ k \neq j}}^{n} I_k(\ell_k) \wedge I_i(\ell_i') \wedge I_j(\ell_j')}{(\ell_1, \dots, \ell_i, \dots, \ell_j, \dots, \ell_n, \nu) \xrightarrow{\tau} (\ell_1, \dots, \ell_i', \dots, \ell_j', \dots, \ell_n, \nu[\,])}$$

$r_i \cup r_j$


press?
x>14
Off
press?
x:=0
Light
x≤14
press?
Bright
press?
press!
y=3
y:=0
y ≤ 0
U
press!
y:=0
U′
y ≤ 3


(Off, U)
τ
(Light, U')
3
(Light, U')
τ
(Bright, U')
τ
3
(Off, U')
3
(Off, U')
τ
(Bright, U')

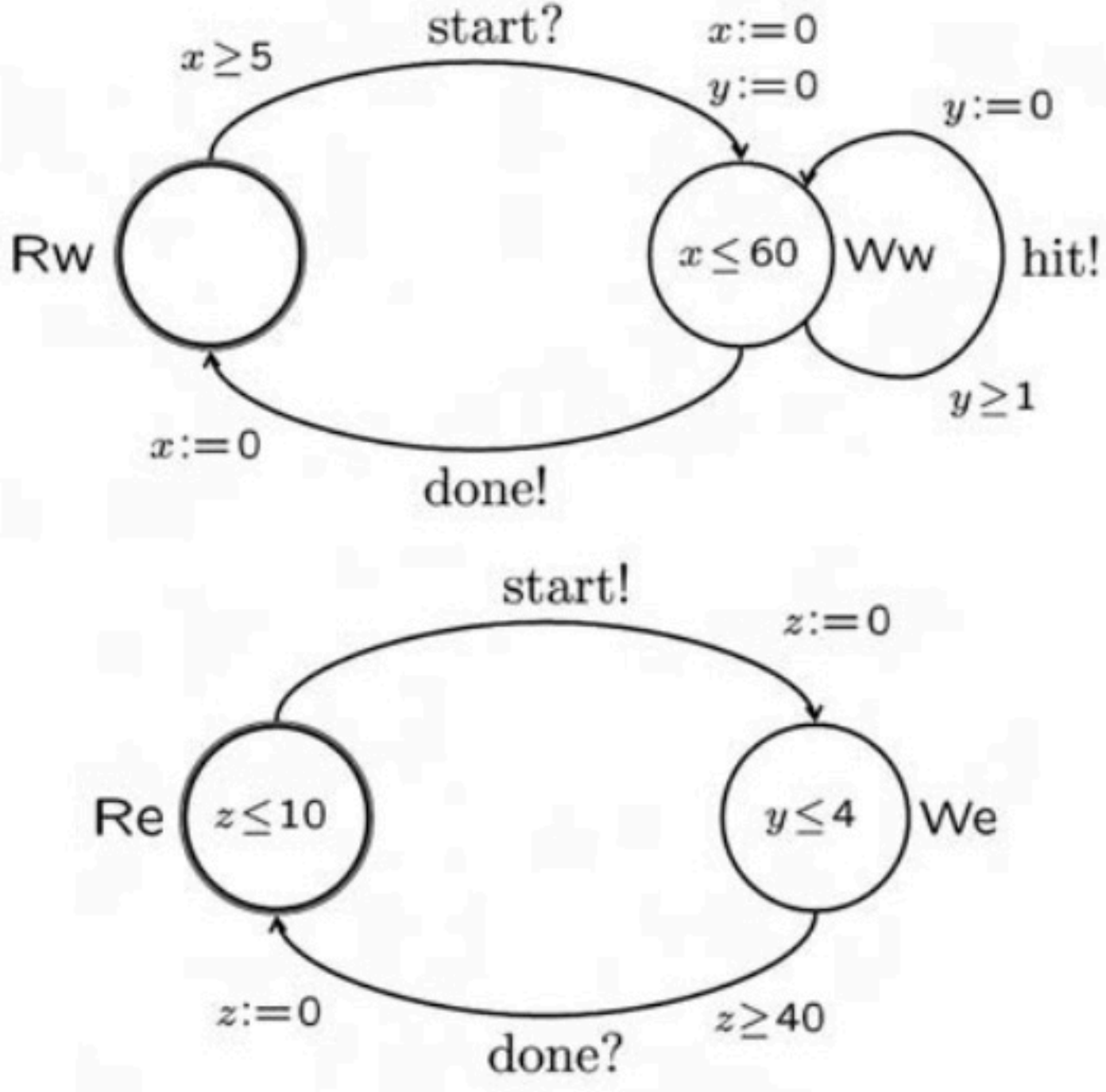


Figure 10.4 The lazy worker and his demanding employer.

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.~~com~~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. ♦