# Verifica di sistemi con proprietà temporali: materiale didattico

- J.-P. Katoen. Concepts, Algorithms and Tools for Model Checking, Capitolo 4 (introduzione, 4.1, 4.2 e 4.9).
- G. Behrmann, A. David, and K. G. Larsen. A Tutorial on Uppaal 4.0

(si possono scaricare dal sito del corso)

**UPPAAL** (tool di modellazione e verifica): http://www.uppaal.org/

# Time-critical systems

In molti sistemi reali gli **aspetti temporali** sono di importanza critica

- controllore del meccanismo d'atterraggio di un aereo, di un passaggio a livello, di un robot ...
- protocolli di comunicazione: dopo aver trasmesso un dato, si deve ritentare la trasmissione se non si riceve un acknowledgment della ricezione *entro un determinato tempo*
- controllo di un apparecchio per radioterapia: il paziente deve ricevere una data dose di radiazioni per un periodo limitato

**Time-critical systems:** sistemi la cui correttezza dipende non soltanto dal risultato logico del calcolo, ma anche dal tempo in cui è prodotto il risultato, cioè devono soddisfare dei requisiti temporali.

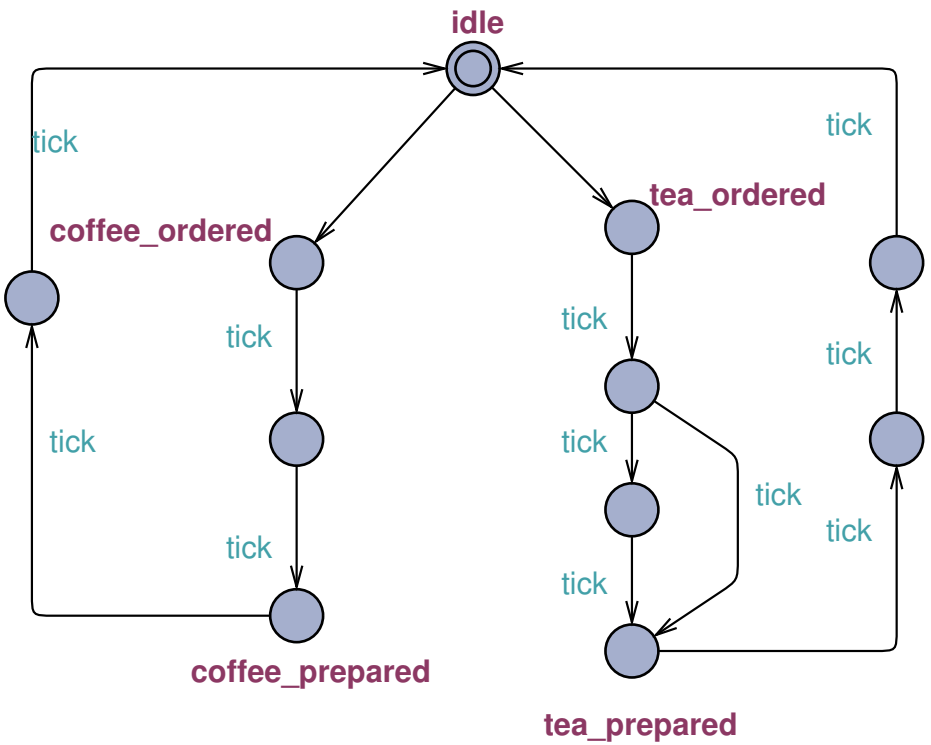
Normalmente, le proprietà temporali che collegano gli eventi e che devono essere soddisfatte sono **quantitative**.

# LTL: relazioni temporali qualitative e tempo discreto

Le relazioni temporali sono **qualitative**: $\Box(p \rightarrow \Diamond q)$ non dice nulla su quanto tempo passa tra il verificarsi di $p$ e quello di $q$.

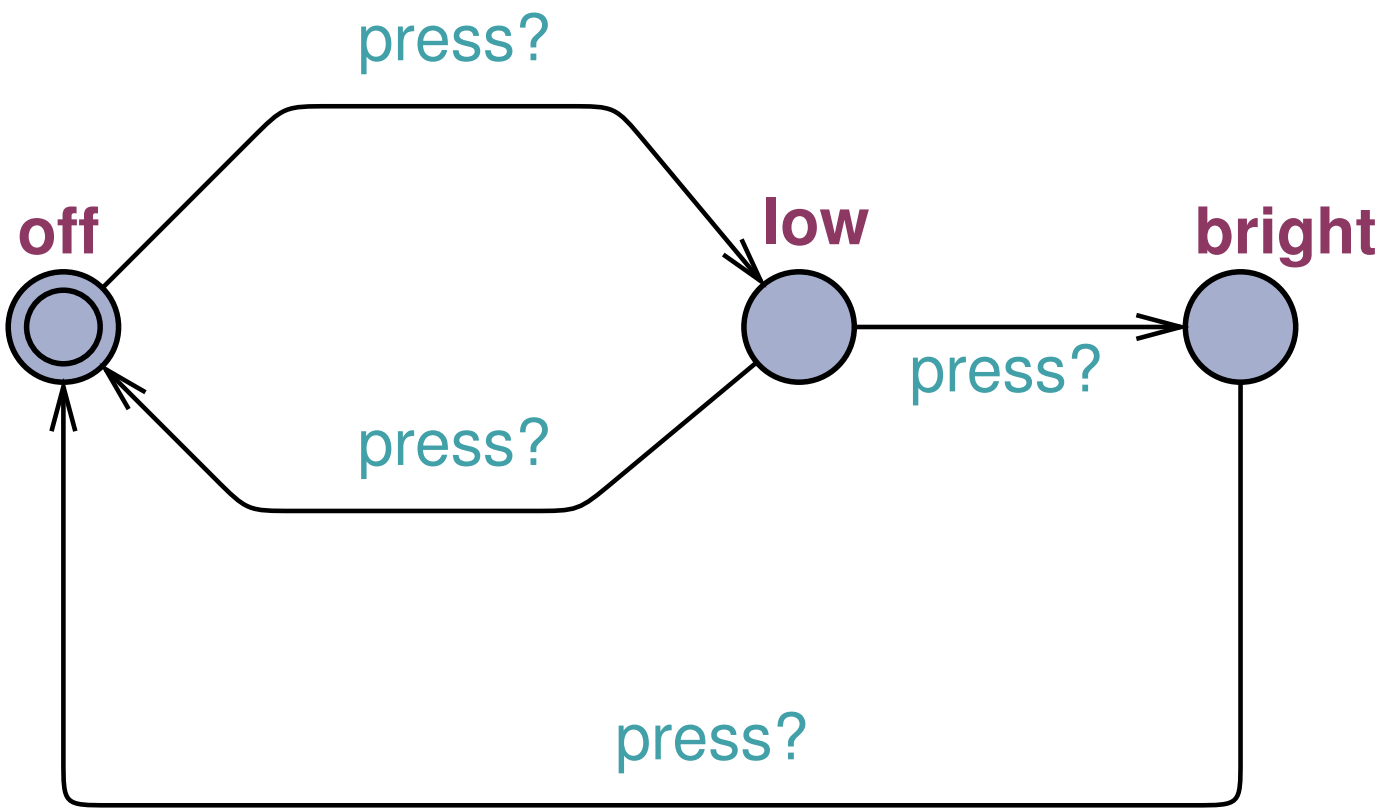
- **tempo discreto**: il tempo incrementa in passi discreti (di una **unità di tempo**)
  Si possono rappresentare alcune proprietà quantitative in LTL

$$\Box(\mathit{coffee\_ordered} \rightarrow \bigcirc\bigcirc \mathit{coffee\_prepared})$$
$$\Box(\mathit{tea\_ordered} \rightarrow \bigcirc\bigcirc \mathit{tea\_prepared} \vee \bigcirc\bigcirc\bigcirc \mathit{tea\_prepared})$$



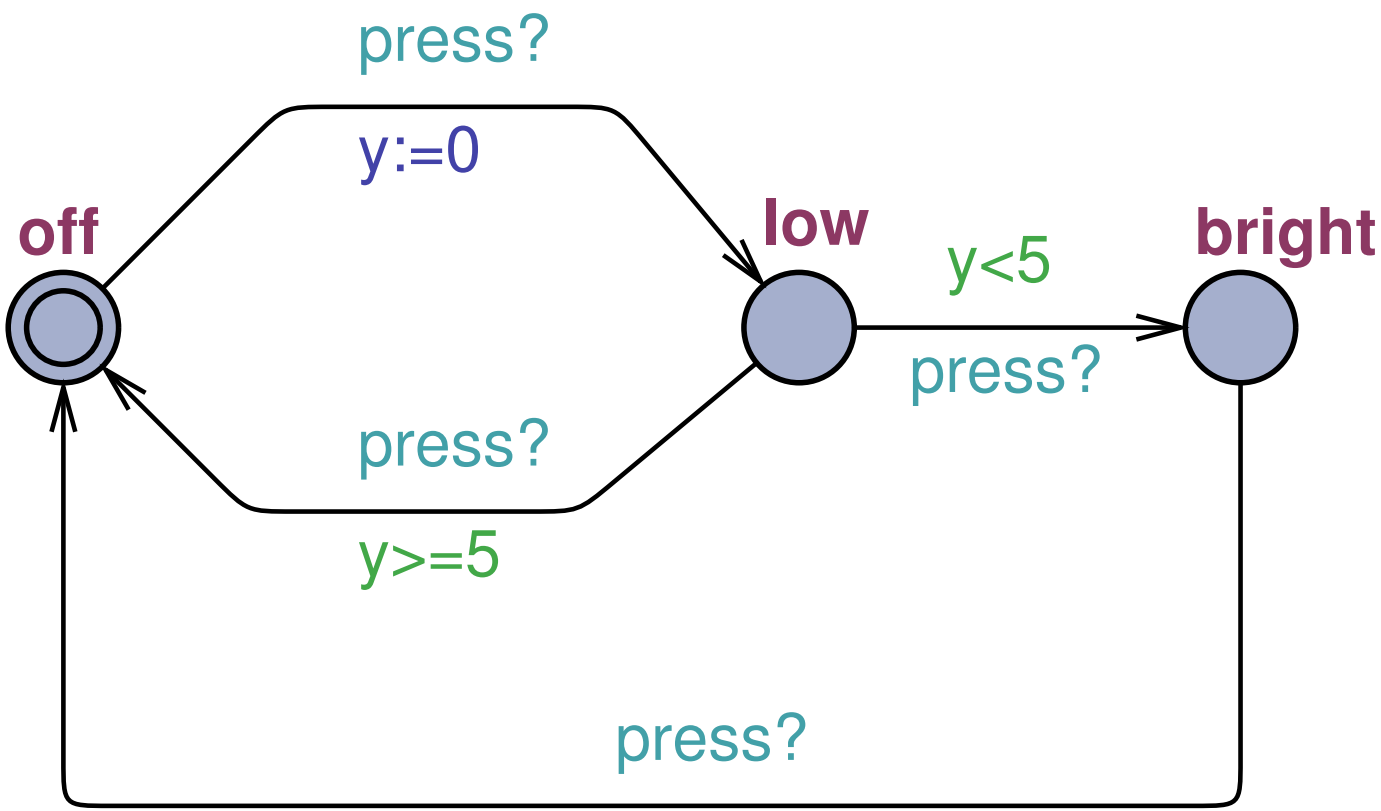
# Controllore di un interruttore della luce

**Nota:** lo stato iniziale è indicato con un doppio cerchio



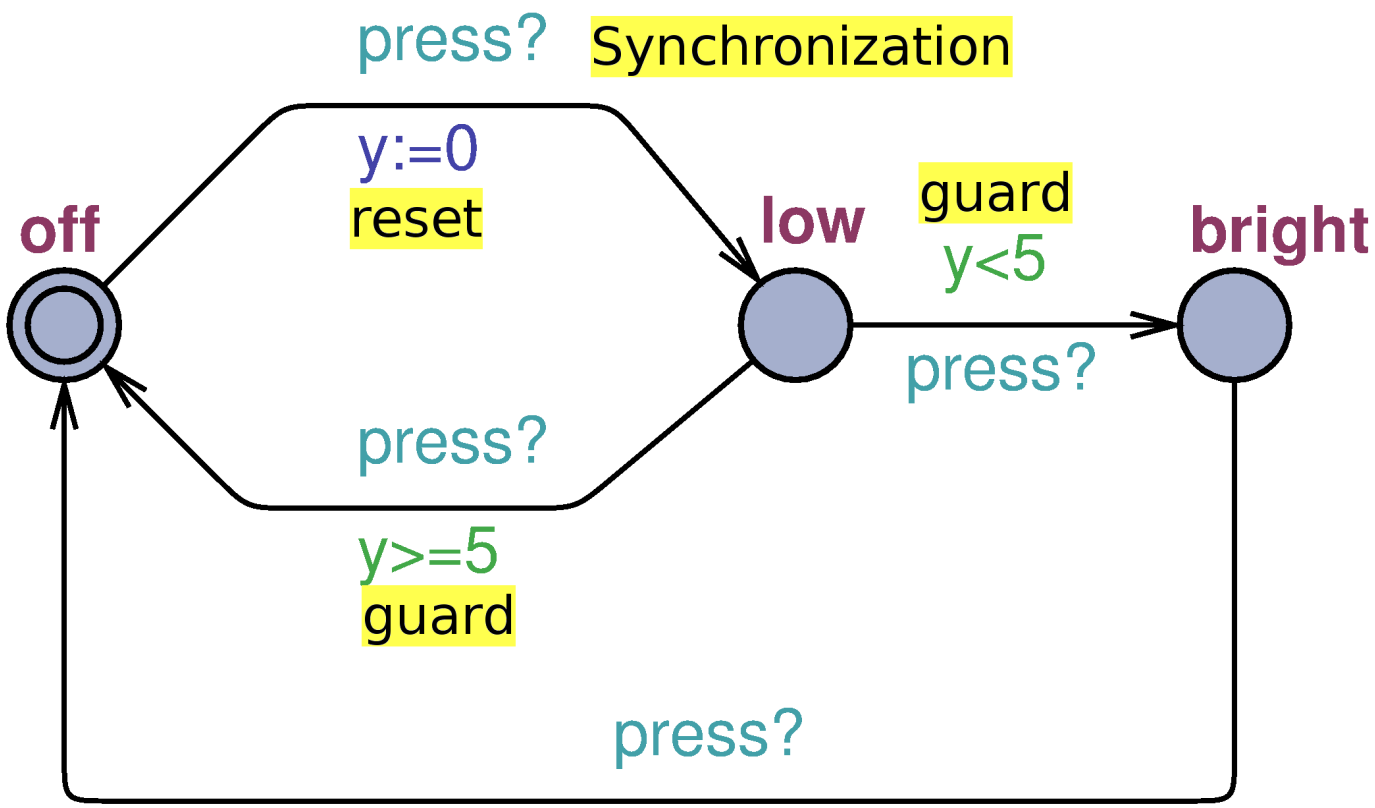

**Si vuole modellare** il fatto che: se l'interruttore viene premuto due volte di seguito **velocemente**, allora la lampadina diventa più luminosa, altrimenti si accende (low) e poi si spegne.

# Timed Automata [Alur & Dill '89]




**Soluzione:** aggiungere un **orologio** a valori reali

# Timed Automata [Alur & Dill '89]



# Timed Automata (TA): clocks

Formalismo di specifica per real-time systems, utilizzato per modellare diversi tipi di time-critical systems

Estendono gli automi a stati finiti mediante **orologi** (clock) usati per misurare il tempo.

Un **orologio** è una variabile con valori in $\mathbb{R}_{\geq 0}$ (reali non negativi).

Uno **stato** di un TA è costituito da una **locazione** + il valore corrente di tutti gli orologi.

Inizialmente il valore di tutti gli orologi è 0, e il loro valore aumenta alla stessa velocità.

Il valore di un orologio rappresenta il tempo che è trascorso da quando è stato inizializzato.

Un orologio può essere **reinizializzato** durante una transizione.

**Vincoli** sul valore di un orologio possono essere usati come **condizioni di abilitazione** di una transizione e come condizioni che devono essere soddisfatte per restare in una locazione (**invarianti**)

# Vincoli sugli orologi

Sia $C$ un insieme di orologi.

**$\Psi(C)$**: insieme dei **clock constraints** su $C$:

$$\alpha ::= x \bowtie c \mid x - y \bowtie c \mid \alpha \wedge \alpha$$

dove: $x, y \in C$, $c \in \mathbb{N}$ e $\bowtie \in \{<, \leq, =, \geq, >\}$.

Un TA è un grafo finito orientato, annotato da elementi di $\Psi(C)$ e reinizializzazioni di orologi

# TA: definizione formale

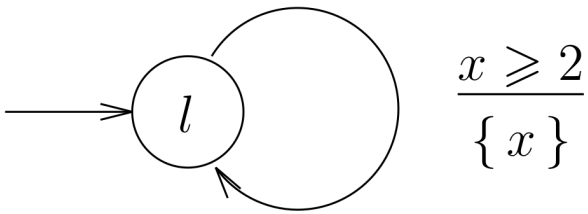
Un TA è una tupla $\langle L, l_0, C, A, E, \mathcal{I} \rangle$ dove:

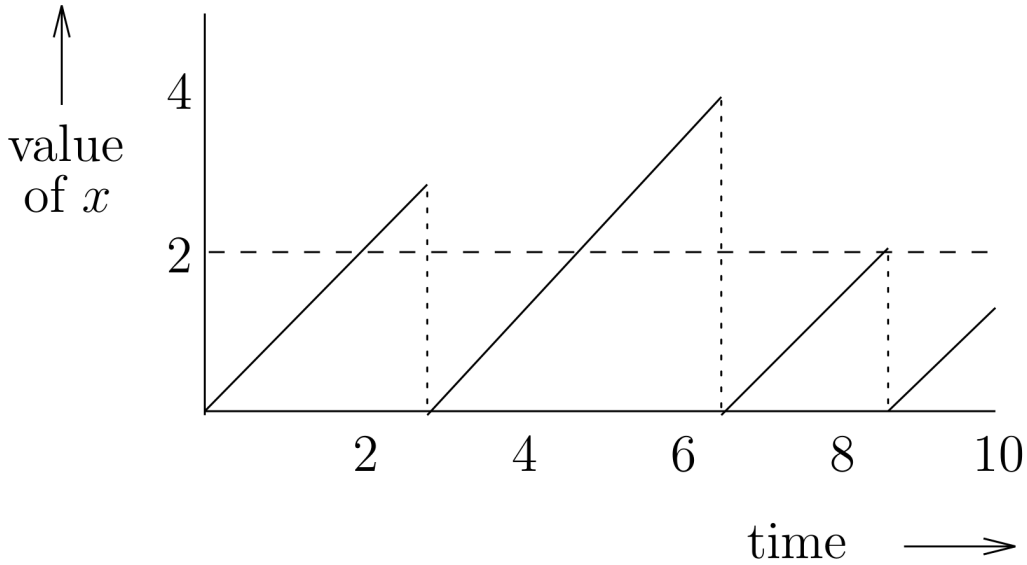
- $L$ è un insieme finito non vuoto di **locazioni** e $l_0 \in L$ è la **locazione iniziale**
- $C$ è un insieme finito di **orologi**
- $A$ è un insieme di **azioni** (usate per rappresentare le sincronizzazioni, quando si considerano **reti di TA**).
- $E \subseteq L \times A \times \Psi(C) \times 2^C \times L$ è l'insieme degli **archi**.
  Ogni arco ha la forma $(l, a, g, X, l')$

  $$l \xrightarrow{a,g,X} l'$$

  dove $a$ è l'azione dell'arco, $g$ la guardia e $X \subseteq C$ l'insieme degli orologi reinizializzati attraversando l'arco
- $\mathcal{I} : L \rightarrow \Psi(C)$ è una funzione che assegna a ogni locazione $l \in L$ un vincolo sugli orologi in $C$ (l'**invariante** della locazione).

# Esempio 1



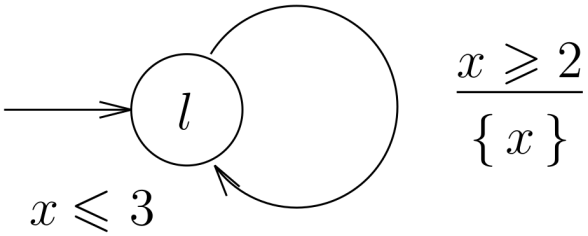



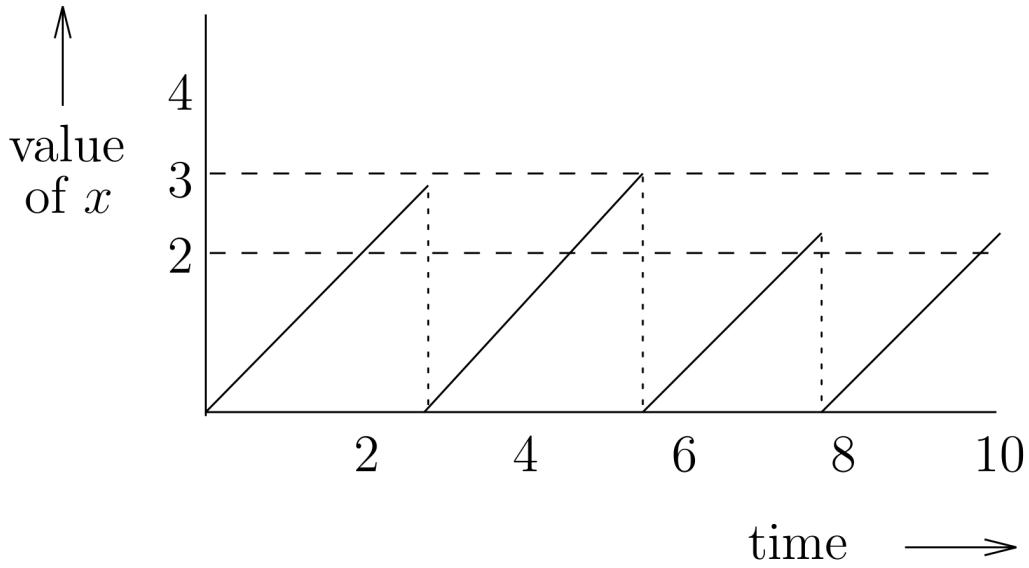

La transizione si può eseguire solo se $x \geq 2$, e quando viene eseguita, l'orologio viene reinizializzato a 0.

Si deve restare nella locazione $l$ **almeno** per 2 unità di tempo.

L'automa potrebbe non eseguire mai la transizione?

# Esempio 2



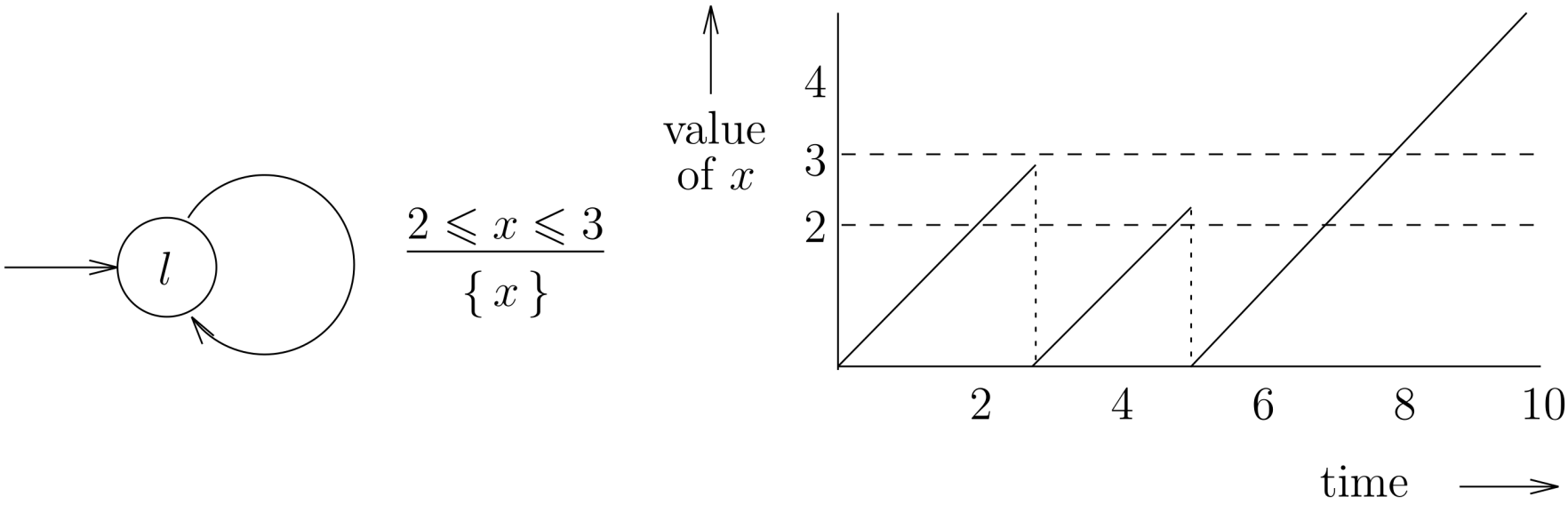

$\mathcal{I}(l) = x \leq 3$: **invariante**, proprietà che deve valere sempre quando si "sta" nella locazione $l$.

Appena l'invariante diventa falsa, si deve eseguire la transizione

Si può restare nella locazione $l$ **al massimo** per 3 unità di tempo.

In qualche istante, ogni volta che $x \geq 2$ (condizione di abilitazione) e $x \leq 3$ (invariante), si deve eseguire la transizione

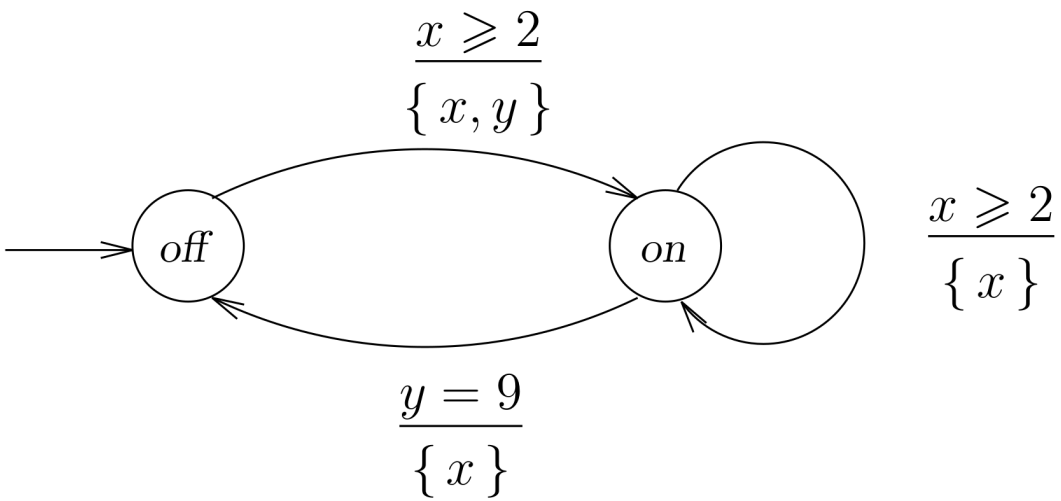
# Esempio 3




La transizione si **può** eseguire quando $x \in [2, 3]$, ma non deve essere eseguita per forza.

# Esempio 4: un interruttore

Come funziona?

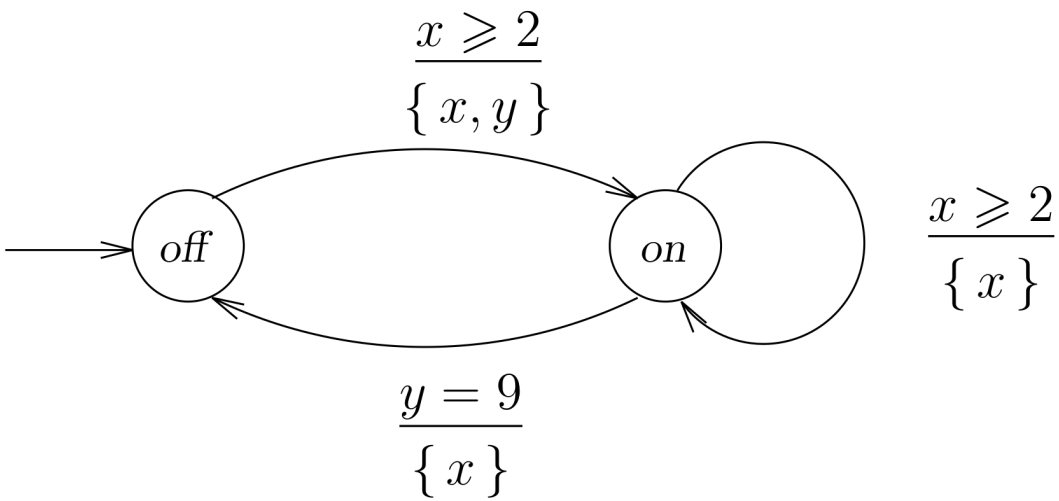



La luce potrebbe restare sempre spenta?

Dopo che è stata accesa, si spegne automaticamente quando $y = 9$?

# Esempio 4: un interruttore

Come funziona?




La luce potrebbe restare sempre spenta?

Dopo che è stata accesa, si spegne automaticamente quando $y = 9$?

Come fare per modellare un interruttore che fa spegnere automaticamente la luce dopo 9 unità di tempo?

# Verso la semantica dei TA: valutazioni e stati

**Clock evaluation** (valutazione degli orologi) ***v*** per un insieme di orologi $C$:

$$v : C \to \mathbb{R}_{\geq 0}$$

funzione che assegna un valore $v(x)$ a ogni orologio $x \in C$.

Insieme di tutte le clock evaluations per $C$: $\boldsymbol{V(C)}$.

$\boldsymbol{v_0}$: valutazione tale che $v_0(x) = 0$ per ogni $x \in C$

# Verso la semantica dei TA: valutazioni e stati

**Clock evaluation** (valutazione degli orologi) $v$ per un insieme di orologi $C$:

$$v : C \to \mathbb{R}_{\geq 0}$$

funzione che assegna un valore $v(x)$ a ogni orologio $x \in C$.

Insieme di tutte le clock evaluations per $C$: $V(C)$.

$v_0$: valutazione tale che $v_0(x) = 0$ per ogni $x \in C$

**Stato** di un TA con insieme $C$ di orologi e insieme $L$ di locazioni: $\langle l, v \rangle$ dove $l \in L$ e $v$ è una clock evaluation per $C$.

# Verso la semantica dei TA: valutazioni e stati

**Clock evaluation** (valutazione degli orologi) $v$ per un insieme di orologi $C$:

$$v : C \to \mathbb{R}_{\geq 0}$$

funzione che assegna un valore $v(x)$ a ogni orologio $x \in C$.

Insieme di tutte le clock evaluations per $C$: $V(C)$.

$v_0$: valutazione tale che $v_0(x) = 0$ per ogni $x \in C$

**Stato** di un TA con insieme $C$ di orologi e insieme $L$ di locazioni: $\langle l, v \rangle$ dove $l \in L$ e $v$ è una clock evaluation per $C$.

Se $v$ è una clock evaluation e $t \in \mathbb{R}_{\geq 0}$:

$$(v + t)(x) = v(x) + t \text{ per ogni } x \in C$$

# Verso la semantica dei TA: valutazioni e stati

**Clock evaluation** (valutazione degli orologi) $v$ per un insieme di orologi $C$:

$$v : C \to \mathbb{R}_{\geq 0}$$

funzione che assegna un valore $v(x)$ a ogni orologio $x \in C$.

Insieme di tutte le clock evaluations per $C$: $V(C)$.

$v_0$: valutazione tale che $v_0(x) = 0$ per ogni $x \in C$

**Stato** di un TA con insieme $C$ di orologi e insieme $L$ di locazioni: $\langle l, v \rangle$ dove $l \in L$ e $v$ è una clock evaluation per $C$.

Se $v$ è una clock evaluation e $t \in \mathbb{R}_{\geq 0}$:

$$(v + t)(x) = v(x) + t \text{ per ogni } x \in C$$

$$(v[x \mapsto 0])(y) = \begin{cases} v(y) & \text{se } y \neq x \\ 0 & \text{se } y = x \end{cases}$$

Abbreviazione: $v[x \mapsto 0][y \mapsto 0] \equiv_{def} v[x, y \mapsto 0]$

# Semantica dei vincoli sugli orologi

Se $x, y \in C$, $v \in V(C)$ e $\alpha, \beta \in \Psi(C)$:

- $v \models x \bowtie c$ sse $v(x) \bowtie c$;
- $v \models x - y \bowtie c$ sse $v(x) - v(y) \bowtie c$;
- $v \models \alpha \wedge \beta$ sse $v \models \alpha$ e $v \models \beta$.

**Esempio:** Sia $v$ tale che $v(x) = v(y) = 0$:

$$v \models x \leq 5 \quad \Leftrightarrow$$

# Semantica dei vincoli sugli orologi

Se $x, y \in C$, $v \in V(C)$ e $\alpha, \beta \in \Psi(C)$:

- $v \models x \bowtie c$ sse $v(x) \bowtie c$;
- $v \models x - y \bowtie c$ sse $v(x) - v(y) \bowtie c$;
- $v \models \alpha \wedge \beta$ sse $v \models \alpha$ e $v \models \beta$.

**Esempio:** Sia $v$ tale che $v(x) = v(y) = 0$:

$$\begin{aligned} v \models x \leq 5 \quad &\Leftrightarrow \quad v(x) = 0 \leq 5 \\ v \models x - y = 0 \quad &\Leftrightarrow \end{aligned}$$

# Semantica dei vincoli sugli orologi

Se $x, y \in C$, $v \in V(C)$ e $\alpha, \beta \in \Psi(C)$:

- $v \models x \bowtie c$ sse $v(x) \bowtie c$;
- $v \models x - y \bowtie c$ sse $v(x) - v(y) \bowtie c$;
- $v \models \alpha \wedge \beta$ sse $v \models \alpha$ e $v \models \beta$.

**Esempio:** Sia $v$ tale che $v(x) = v(y) = 0$:

$$\begin{array}{rcl} v \models x \leq 5 & \Leftrightarrow & v(x) = 0 \leq 5 \\ v \models x - y = 0 & \Leftrightarrow & v(x) - v(y) = 0 \\ v + 9 \not\models x \leq 5 & \Leftrightarrow & \end{array}$$

# Semantica dei vincoli sugli orologi

Se $x, y \in C$, $v \in V(C)$ e $\alpha, \beta \in \Psi(C)$:

- $v \models x \bowtie c$ sse $v(x) \bowtie c$;
- $v \models x - y \bowtie c$ sse $v(x) - v(y) \bowtie c$;
- $v \models \alpha \wedge \beta$ sse $v \models \alpha$ e $v \models \beta$.

**Esempio:** Sia $v$ tale che $v(x) = v(y) = 0$:

$$\begin{aligned} v \models x \leq 5 &\quad\Leftrightarrow\quad v(x) = 0 \leq 5 \\ v \models x - y = 0 &\quad\Leftrightarrow\quad v(x) - v(y) = 0 \\ v + 9 \not\models x \leq 5 &\quad\Leftrightarrow\quad (v+9)(x) = 9 > 5 \\ v + 9 \models x - y = 0 &\quad\Leftrightarrow \end{aligned}$$

# Semantica dei vincoli sugli orologi

Se $x, y \in C$, $v \in V(C)$ e $\alpha, \beta \in \Psi(C)$:

- $v \models x \bowtie c$ sse $v(x) \bowtie c$;
- $v \models x - y \bowtie c$ sse $v(x) - v(y) \bowtie c$;
- $v \models \alpha \wedge \beta$ sse $v \models \alpha$ e $v \models \beta$.

**Esempio:** Sia $v$ tale che $v(x) = v(y) = 0$:

$$
\begin{aligned}
v \models x \leq 5 &\quad\Leftrightarrow\quad v(x) = 0 \leq 5 \\
v \models x - y = 0 &\quad\Leftrightarrow\quad v(x) - v(y) = 0 \\
v + 9 \not\models x \leq 5 &\quad\Leftrightarrow\quad (v+9)(x) = 9 > 5 \\
v + 9 \models x - y = 0 &\quad\Leftrightarrow\quad (v+9)(x) - (v+9)(y) = 9 - 9 = 0 \\
(v + 9)[x \mapsto 0] \models x \leq 5 &\quad\Leftrightarrow
\end{aligned}
$$

# Semantica dei vincoli sugli orologi

Se $x, y \in C$, $v \in V(C)$ e $\alpha, \beta \in \Psi(C)$:

- $v \models x \bowtie c$ sse $v(x) \bowtie c$;
- $v \models x - y \bowtie c$ sse $v(x) - v(y) \bowtie c$;
- $v \models \alpha \wedge \beta$ sse $v \models \alpha$ e $v \models \beta$.

**Esempio:** Sia $v$ tale che $v(x) = v(y) = 0$:

$$
\begin{aligned}
v \models x \leq 5 &\quad\Leftrightarrow\quad v(x) = 0 \leq 5 \\
v \models x - y = 0 &\quad\Leftrightarrow\quad v(x) - v(y) = 0 \\
v + 9 \not\models x \leq 5 &\quad\Leftrightarrow\quad (v+9)(x) = 9 > 5 \\
v + 9 \models x - y = 0 &\quad\Leftrightarrow\quad (v+9)(x) - (v+9)(y) = 9 - 9 = 0 \\
(v + 9)[x \mapsto 0] \models x \leq 5 &\quad\Leftrightarrow\quad ((v+9)[x \mapsto 0])(x) = 0 \leq 5 \\
(v + 9)[x \mapsto 0] \not\models x - y = 0 &\quad\Leftrightarrow
\end{aligned}
$$

# Semantica dei vincoli sugli orologi

Se $x, y \in C$, $v \in V(C)$ e $\alpha, \beta \in \Psi(C)$:

- $v \models x \bowtie c$ sse $v(x) \bowtie c$;
- $v \models x - y \bowtie c$ sse $v(x) - v(y) \bowtie c$;
- $v \models \alpha \wedge \beta$ sse $v \models \alpha$ e $v \models \beta$.

**Esempio:** Sia $v$ tale che $v(x) = v(y) = 0$:

$$
\begin{aligned}
v \models x \leq 5 &\quad\Leftrightarrow\quad v(x) = 0 \leq 5 \\
v \models x - y = 0 &\quad\Leftrightarrow\quad v(x) - v(y) = 0 \\
v + 9 \not\models x \leq 5 &\quad\Leftrightarrow\quad (v+9)(x) = 9 > 5 \\
v + 9 \models x - y = 0 &\quad\Leftrightarrow\quad (v+9)(x) - (v+9)(y) = 9 - 9 = 0 \\
(v + 9)[x \mapsto 0] \models x \leq 5 &\quad\Leftrightarrow\quad ((v+9)[x \mapsto 0])(x) = 0 \leq 5 \\
(v + 9)[x \mapsto 0] \not\models x - y = 0 &\quad\Leftrightarrow\quad \\
&\quad ((v+9)[x \mapsto 0])(x) - ((v+9)[x \mapsto 0])(y) = 0 - 9 \neq 0
\end{aligned}
$$

# Semantica dei TA

La semantica di un TA $\mathcal{A} = \langle L, l_0, C, A, E, \mathcal{I} \rangle$ è definita in termini di un **sistema di transizioni** (infinito) $\langle S, s_0, \longrightarrow \rangle$ dove:

- $S = L \times V(C)$ è l'insieme degli stati
- $s_0 = \langle l_0, v_0 \rangle$ è lo stato iniziale (tutti gli orologi hanno valore 0)
- $\longrightarrow \subseteq S \times (\mathbb{R}_{>0} \cup A) \times S$ è la relazione di transizione, tale che:
  - $\langle l, v \rangle \xrightarrow{d} \langle l, v + d \rangle$,
    per $d \in \mathbb{R}_{>0}$ tale che per ogni $d'$, se $0 \leq d' \leq d$ allora $v + d' \models \mathcal{I}(l)$
    (l'automa resta nella stessa locazione lasciando passare il tempo, ma in modo che l'invariante sia sempre vera)
  - $\langle l, v \rangle \xrightarrow{a} \langle l', v' \rangle$,
    se esiste un arco $e \in E$, $e = l \xrightarrow{a,g,X} l'$, tale che:
    - $v \models g$
      (la guardia è soddisfatta nello stato di partenza),
    - $v' = v[X \mapsto 0]$
      (nello stato d'arrivo sono resettati gli orologi in $X$)
    - $v' \models \mathcal{I}(l')$
      (lo stato d'arrivo soddisfa l'invariante della sua locazione)

# Informalmente...

Gli **stati** sono tutte le coppie $\langle l, v \rangle$ dove $l$ è una locazione di $\mathcal{A}$ e $v$ una clock evaluation per gli orologi di $\mathcal{A}$.

Includono anche gli stati irraggiungibili

**Transizioni**

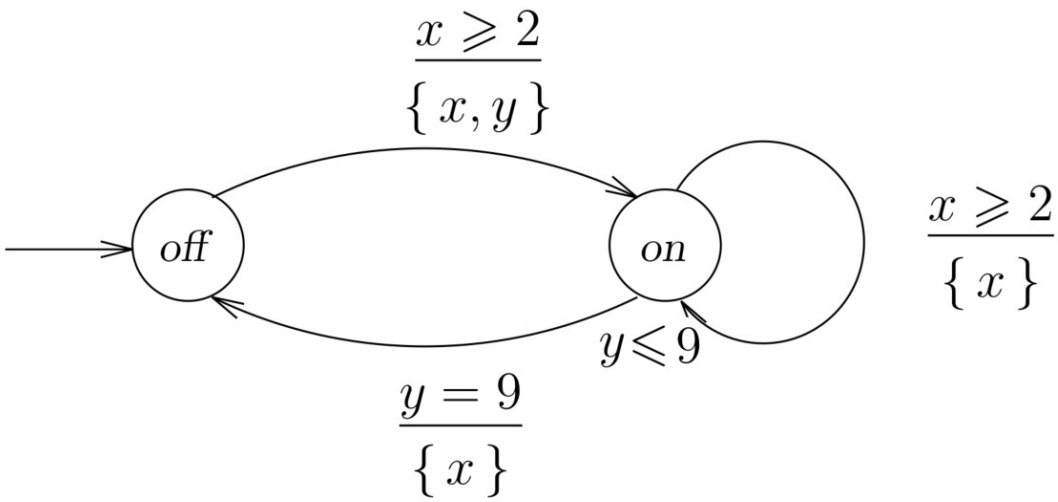
- **delay transition** (il valore degli orologi aumenta con la stessa velocità): si può restare nella stessa locazione per un determinato tempo purché resti sempre soddisfatta l'invariante della locazione
- **action transition** (il valore degli orologi non aumenta):

$$\langle l, v \rangle \xrightarrow{a} \langle l', v' \rangle$$

si attraversa un arco $e = l \xrightarrow{a,g,X} l'$ dell'automa.
L'attraversamento dell'arco è possibile se:

1. $v$ soddisfa la guardia di $e$ (altrimenti l'arco è disabilitato)
2. la nuova clock evaluation $v'$ si ottiene da $v$ resettando tutti gli orologi associati a $e$ e lasciando immutati gli altri
3. la nuova clock evaluation $v'$ soddisfa l'invariante della locazione d'arrivo

# Esempio (I)

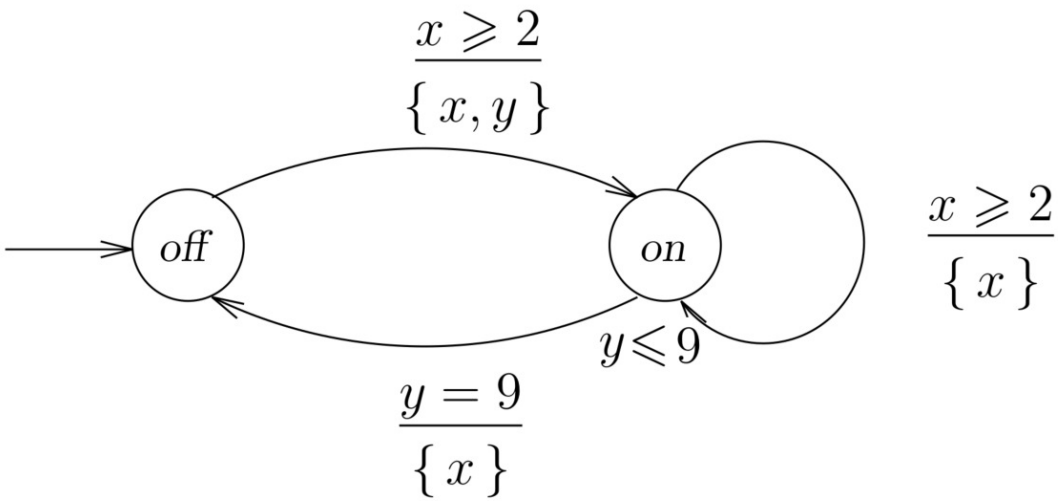



**Stato iniziale:** $s_0 = \langle off, v_0 \rangle$, con $v_0(x) = v_0(y) = 0$

**Delay transitions**

- $\langle off, v_0 \rangle \xrightarrow{100} \langle off, v_0 + 100 \rangle$:
  la locazione off non ha invarianti

# Esempio (I)

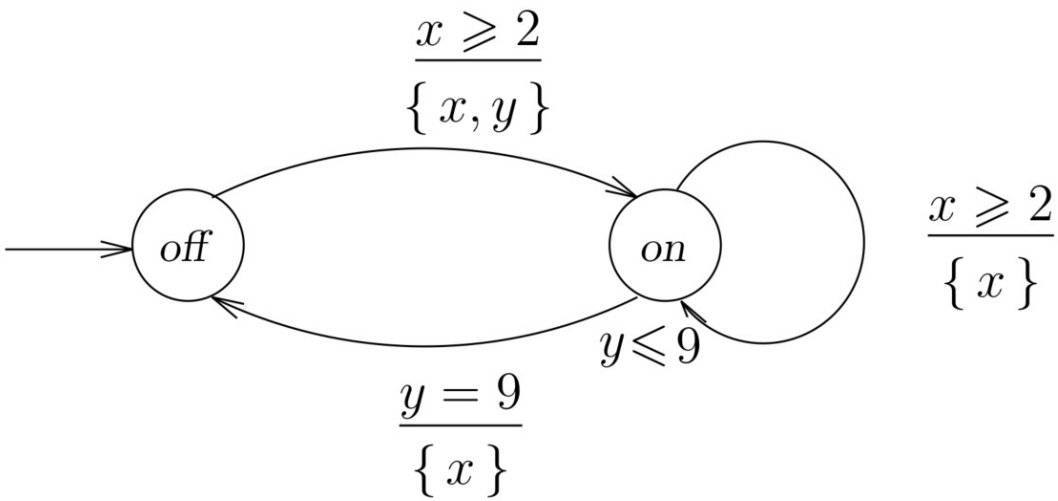



**Stato iniziale:** $s_0 = \langle off, v_0 \rangle$, con $v_0(x) = v_0(y) = 0$

**Delay transitions**

- $\langle on, v_0 \rangle \xrightarrow{4} \langle on, v_0 + 4 \rangle$:
  per ogni $d'$, se $0 \leq d' \leq 4$, allora $v_0 + d' \models y \leq 9$

# Esempio (I)

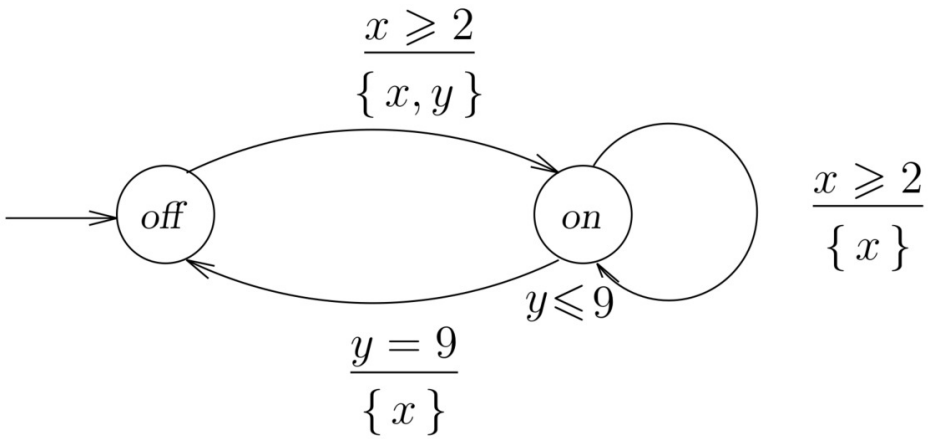



**Stato iniziale:** $s_0 = \langle off, v_0 \rangle$, con $v_0(x) = v_0(y) = 0$

**Delay transitions**

- **ma** $\langle on, v_0 \rangle \xrightarrow{10} \langle on, v_0 + 10 \rangle$ **non è una transizione**: $v_0 + 10 \not\models y \leq 9$

# Esempio (II)

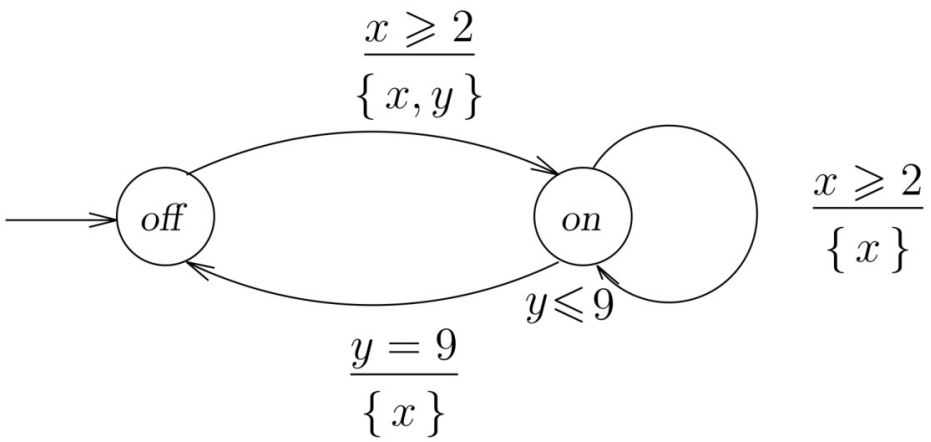



## Action transitions

Denotiamo con $v_{x=c,y=d}$ la clock evaluation che assegna $c$ a $x$ e $d$ a $y$

- $\langle off, v_0 + 3\rangle \longrightarrow \langle on, v_0\rangle$:
  $v_0 + 3 \models x \geq 2$, $v_0 = v_0 + 3[x, y \mapsto 0]$ e $v_0 \models y \leq 9$.

# Esempio (II)

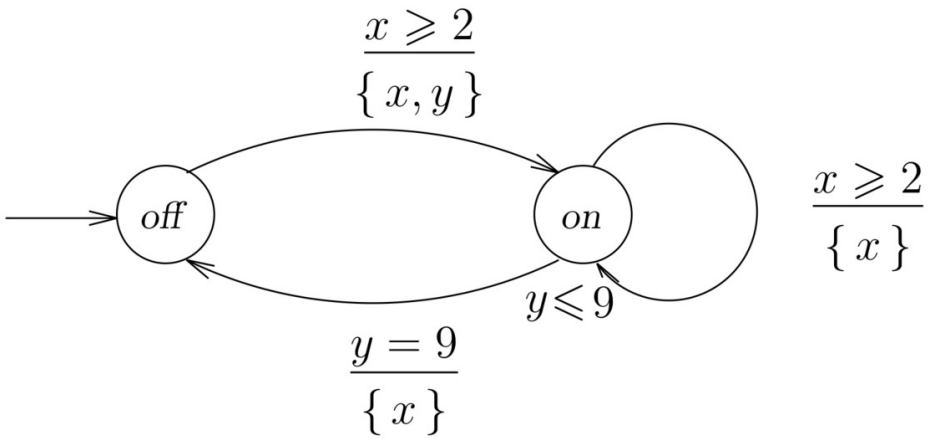



## Action transitions

Denotiamo con $v_{x=c,y=d}$ la clock evaluation che assegna $c$ a $x$ e $d$ a $y$

- $\langle off, v_{x=2,y=3} \rangle \longrightarrow \langle on, v_0 \rangle$:
  $v_{x=2,y=3} \models x \geq 2$, $v_0 = v_{x=2,y=3}[x, y \mapsto 0]$ e $v_0 \models y \leq 9$
  (anche se lo stato $\langle on, v_{x=2,y=3} \rangle$ non è raggiungibile dallo stato iniziale)

# Esempio (II)

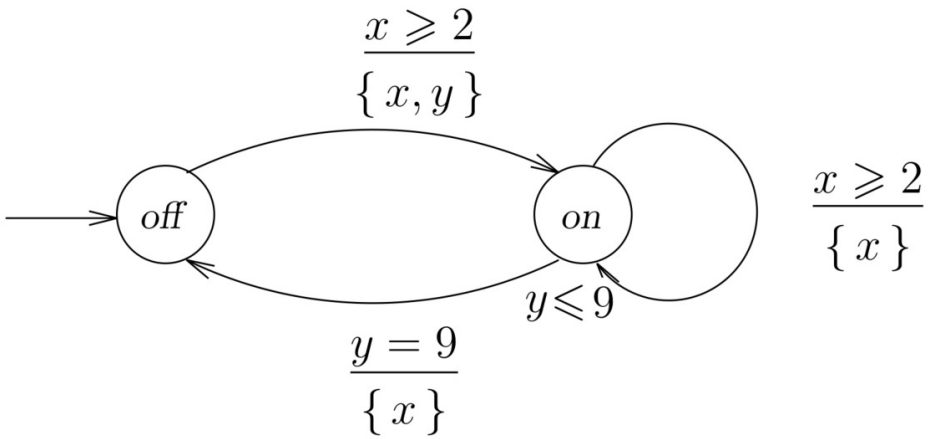



## Action transitions

Denotiamo con $v_{x=c,y=d}$ la clock evaluation che assegna $c$ a $x$ e $d$ a $y$

- $\langle on, v_0 + 3\rangle \longrightarrow \langle on, v_{x=0,y=3}\rangle$:
  $v_0 + 3 \models x \geq 2$, $v_{x=0,y=3} = v_0 + 3[x \mapsto 0]$ e $v_{x=0,y=3} \models y \leq 9$.

# Esempio (II)

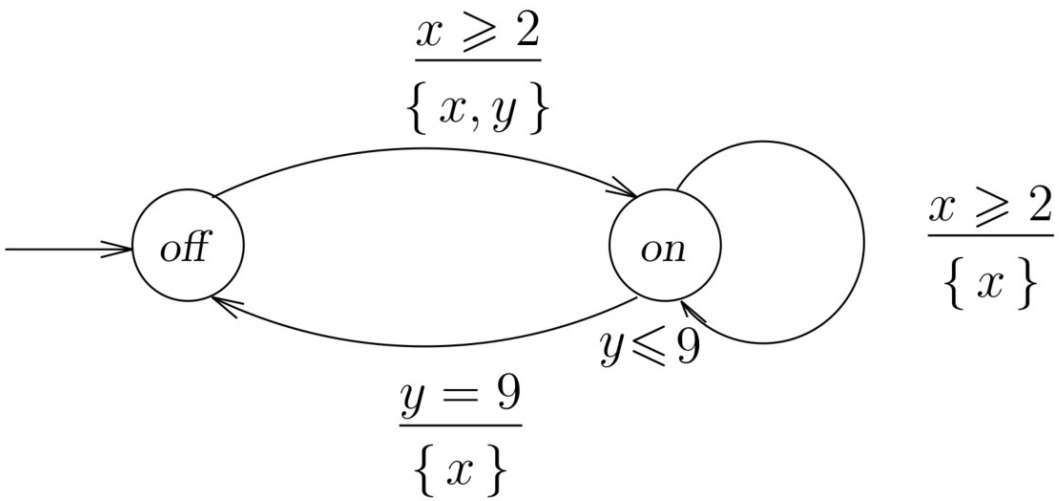



## Action transitions

Denotiamo con $v_{x=c,y=d}$ la clock evaluation che assegna $c$ a $x$ e $d$ a $y$

- $\langle on, v_{x=5,y=9} \rangle \longrightarrow \langle off, v_{x=0,y=9} \rangle$:
  $v_{x=5,y=9} \models y = 9$, $v_{x=0,y=9} = v_{x=5,y=9}[x \mapsto 0]$ e off non ha invarianti.

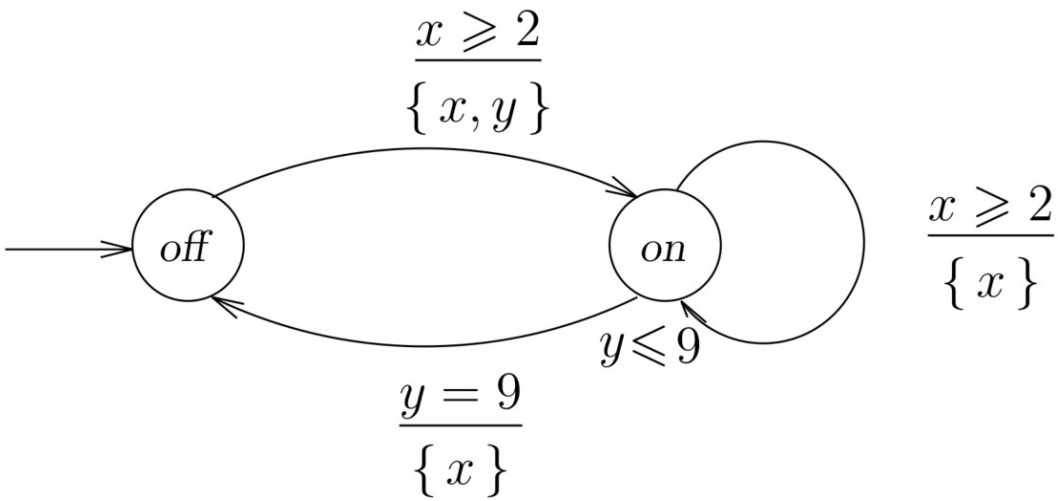
# Esempio (III)




**Non sono transizioni:**

- $\langle \mathit{off}, v_0 + 1 \rangle \longrightarrow \langle \mathit{on}, v_0 \rangle$, perché

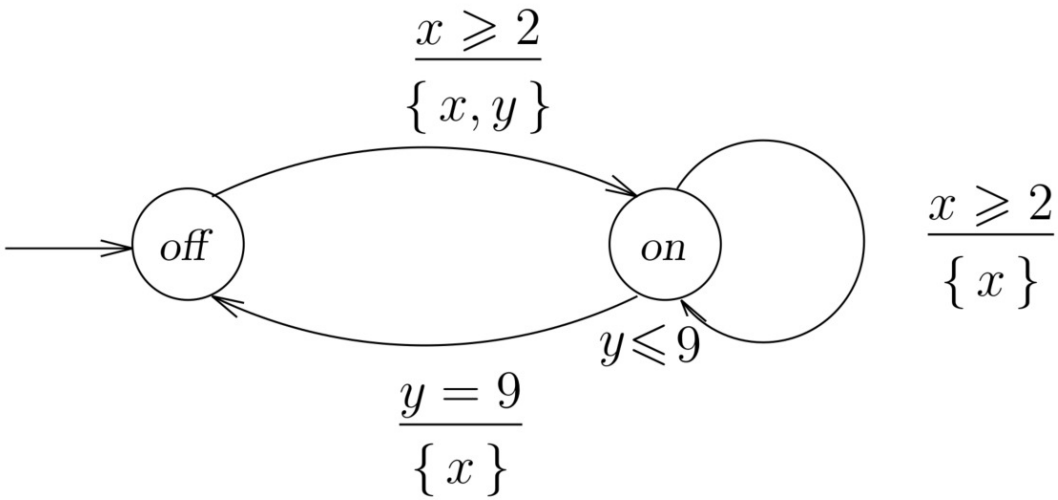
# Esempio (III)




**Non sono transizioni:**

- $\langle \mathit{off}, v_0 + 1 \rangle \longrightarrow \langle \mathit{on}, v_0 \rangle$, perché $v_0 + 1 \not\models x \geq 2$.
- $\langle \mathit{off}, v_0 + 3 \rangle \longrightarrow \langle \mathit{on}, v_{x=0,y=3} \rangle$, perché

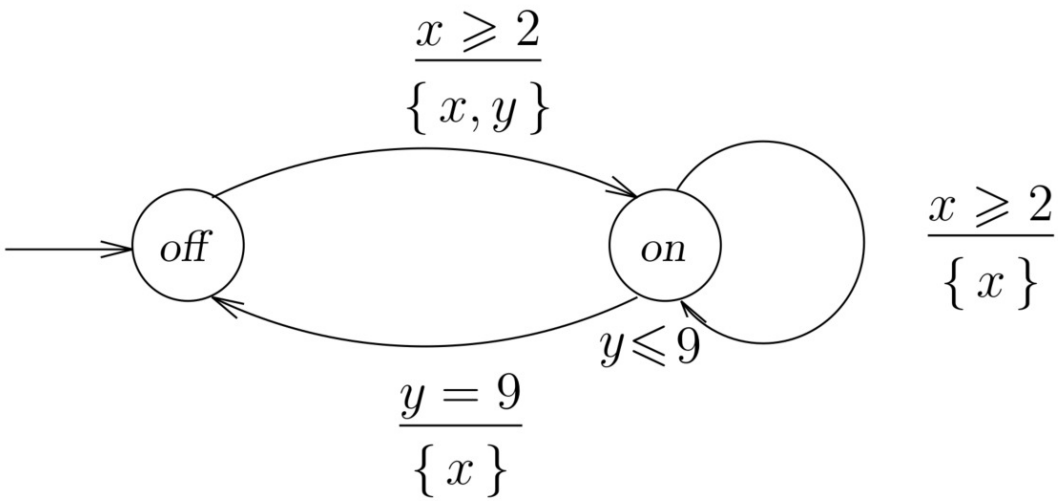
# Esempio (III)




**Non sono transizioni:**

- $\langle off, v_0 + 1 \rangle \longrightarrow \langle on, v_0 \rangle$, perché $v_0 + 1 \not\models x \geq 2$.
- $\langle off, v_0 + 3 \rangle \longrightarrow \langle on, v_{x=0,y=3} \rangle$, perché $v_{x=0,y=3} \neq v_0 + 3[x, y \mapsto 0]$.
- $\langle on, v_{x=3,y=10} \rangle \longrightarrow \langle on, v_{x=0,y=10} \rangle$ perché

# Esempio (III)




**Non sono transizioni:**

- $\langle \mathit{off}, v_0 + 1 \rangle \longrightarrow \langle \mathit{on}, v_0 \rangle$, perché $v_0 + 1 \not\models x \geq 2$.
- $\langle \mathit{off}, v_0 + 3 \rangle \longrightarrow \langle \mathit{on}, v_{x=0,y=3} \rangle$, perché $v_{x=0,y=3} \neq v_0 + 3[x, y \mapsto 0]$.
- $\langle \mathit{on}, v_{x=3,y=10} \rangle \longrightarrow \langle \mathit{on}, v_{x=0,y=10} \rangle$ perché $v_{x=0,y=10} \not\models y \leq 9$.

# Reti di TA (NTA)

Una rete di Timed Automata è la composizione parallela di un insieme di Timed Automata, chiamati **processi**.

La comunicazione asincrona avviene attraverso le variabili condivise.

La comunicazione sincrona tra i processi avviene mediante *hand-shake synchronization*, per mezzo di azioni di **input** e **output**.

Le azioni di output sono denotate da simboli della forma **a!** (**actions**), quelle di input hanno la forma **a?** (**co-actions**).

Le **azioni interne**, di cui non interessa il nome, sono denotate dal simbolo $\tau$.

Un automa della rete può effettuare una transizione per proprio conto oppure sincronizzarsi con un altro automa.

# NTA: definizione formale

Una rete di timed automata è un insieme $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ di TA con lo stesso insieme $C$ di orologi e azioni $A$:

$$\mathcal{A}_i = \langle L_i, l_i^0, C, A, E_i, \mathcal{I}_i \rangle$$

# NTA: definizione formale

Una rete di timed automata è un insieme $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ di TA con lo stesso insieme $C$ di orologi e azioni $A$:

$$\mathcal{A}_i = \langle L_i, l_i^0, C, A, E_i, \mathcal{I}_i \rangle$$

**Vettore di locazioni** $\bar{l} = \langle l_1, \ldots, l_n \rangle$.

Vettore **iniziale**: $\overline{l_0} = \langle l_1^0, \ldots, l_n^0 \rangle$.

# NTA: definizione formale

Una rete di timed automata è un insieme $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ di TA con lo stesso insieme $C$ di orologi e azioni $A$:

$$\mathcal{A}_i = \langle L_i, l_i^0, C, A, E_i, \mathcal{I}_i \rangle$$

**Vettore di locazioni** $\bar{l} = \langle l_1, \ldots, l_n \rangle$.

Vettore **iniziale**: $\overline{l_0} = \langle l_1^0, \ldots, l_n^0 \rangle$.

Composizione delle funzioni $\mathcal{I}_i$ in una funzione che assegna un'**invariante** a ogni vettore di locazioni

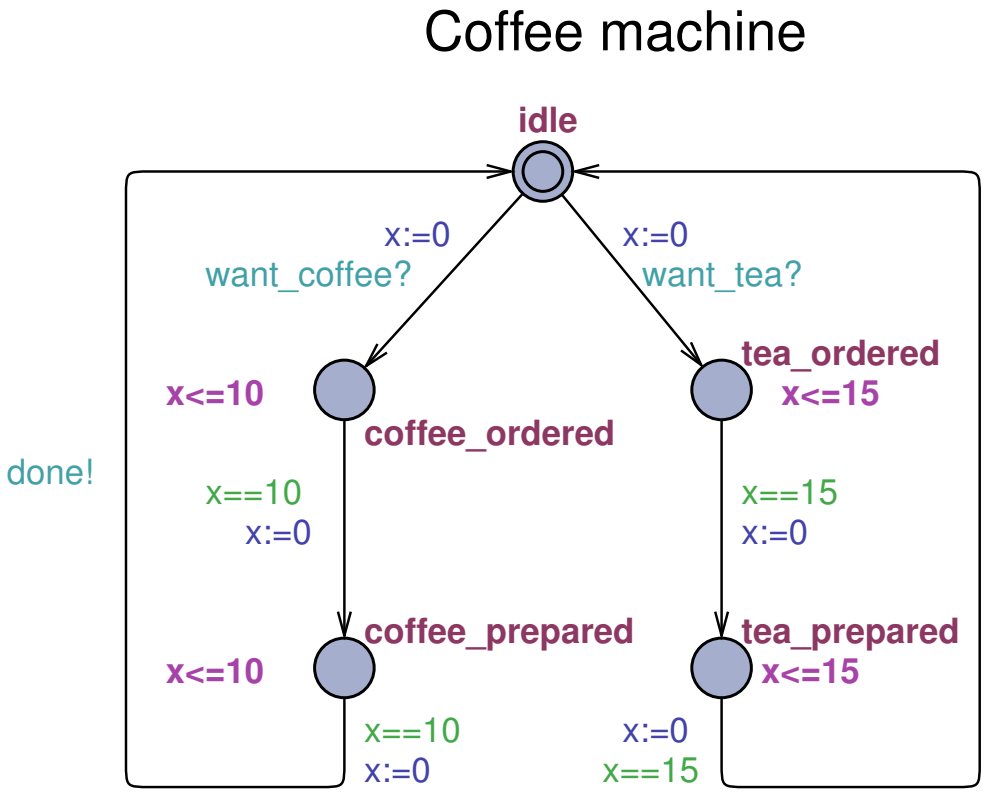
$$\mathcal{I}(\langle l_1, \ldots, l_n \rangle) = \mathcal{I}_1(l_1) \wedge \cdots \wedge \mathcal{I}_n(l_n)$$

Sostituzione di una locazione in un vettore:

$$\bar{l}[l_i'/l_i]$$

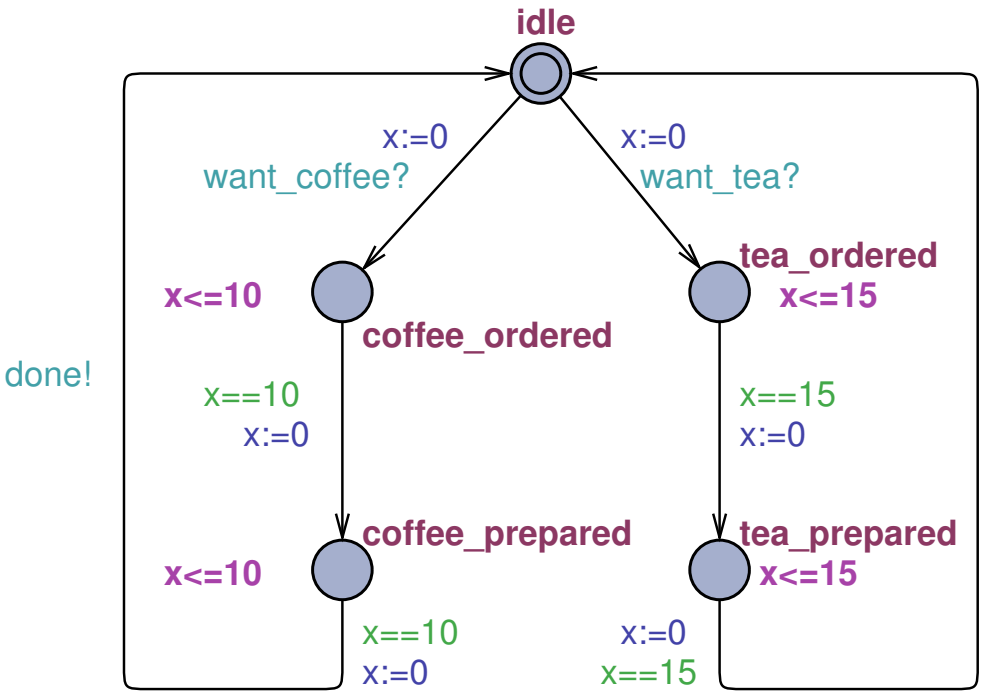
vettore che si ottiene da $\bar{l}$ sostituendo il suo $i$-esimo elemento $l_i$ con $l_i'$

# Esempio

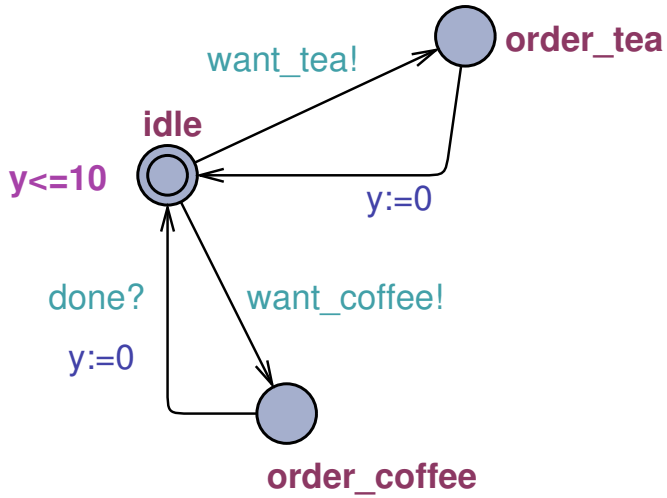

Coffee machine
idle
x:=0
want_coffee?
x:=0
want_tea?
x<=10
coffee_ordered
tea_ordered
x<=15
done!
x==10
x:=0
x==15
x:=0
coffee_prepared
x<=10
tea_prepared
x<=15
x==10
x:=0
x:=0
x==15

# Esempio

Coffee machine




Drinker




vettore iniziale: $\langle idle, idle \rangle$

$$I(\langle tea\_ordered, idle \rangle) = x \leq 15 \wedge y \leq 10$$

$$\langle tea\_ordered, order\_tea \rangle [tea\_prepared / tea\_ordered] = \langle tea\_prepared, order\_tea \rangle$$

# Semantica delle NTA

La semantica di una NTA $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$, con $\mathcal{A}_i = \langle L_i, l_i^0, C, A, E_i, \mathcal{I}_i \rangle$, è data da un sistema di transizioni $\langle S, s_0, \longrightarrow \rangle$, dove:

- $S = (L_1 \times \cdots \times L_n) \times V(C)$: uno stato è un vettore di locazioni + un clock assignment
- $s_0 = \langle \overline{l_0}, v_0 \rangle$
- $\longrightarrow \subseteq S \times S$ è tale che:
  - $\langle \bar{l}, v \rangle \longrightarrow \langle \bar{l}, v + d \rangle$, per $d \in \mathbb{R}_{>0}$ tale che per ogni $d'$, se $0 \leq d' \leq d$ allora $v + d' \models \mathcal{I}(\bar{l})$;

# Semantica delle NTA

La semantica di una NTA $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$, con $\mathcal{A}_i = \langle L_i, l_i^0, C, A, E_i, \mathcal{I}_i \rangle$, è data da un sistema di transizioni $\langle S, s_0, \longrightarrow \rangle$, dove:

- $S = (L_1 \times \cdots \times L_n) \times V(C)$: uno stato è un vettore di locazioni + un clock assignment
- $s_0 = \langle \overline{l_0}, v_0 \rangle$
- $\longrightarrow \subseteq S \times S$ è tale che:
  - $\langle \bar{l}, v \rangle \longrightarrow \langle \bar{l}, v + d \rangle$, per $d \in \mathbb{R}_{>0}$ tale che per ogni $d'$, se $0 \leq d' \leq d$ allora $v + d' \models \mathcal{I}(\bar{l})$;
  - $\langle \bar{l}, v \rangle \longrightarrow \langle \bar{l}[l_i'/l_i], v' \rangle$, se esiste $e \in E_i$, $e = l_i \overset{\tau, g, X}{\longrightarrow} l_i'$, tale che:

$$v \models g,$$

# Semantica delle NTA

La semantica di una NTA $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$, con $\mathcal{A}_i = \langle L_i, l_i^0, C, A, E_i, \mathcal{I}_i \rangle$, è data da un sistema di transizioni $\langle S, s_0, \longrightarrow \rangle$, dove:

- $S = (L_1 \times \cdots \times L_n) \times V(C)$: uno stato è un vettore di locazioni + un clock assignment
- $s_0 = \langle \overline{l_0}, v_0 \rangle$
- $\longrightarrow \subseteq S \times S$ è tale che:
  - $\langle \bar{l}, v \rangle \longrightarrow \langle \bar{l}, v + d \rangle$, per $d \in \mathbb{R}_{>0}$ tale che per ogni $d'$, se $0 \leq d' \leq d$ allora $v + d' \models \mathcal{I}(\bar{l})$;
  - $\langle \bar{l}, v \rangle \longrightarrow \langle \bar{l}[l_i'/l_i], v' \rangle$, se esiste $e \in E_i$, $e = l_i \overset{\tau, g, X}{\longrightarrow} l_i'$, tale che:

$$v \models g, \qquad v' = v[X \mapsto 0],$$

# Semantica delle NTA

La semantica di una NTA $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$, con $\mathcal{A}_i = \langle L_i, l_i^0, C, A, E_i, \mathcal{I}_i \rangle$, è data da un sistema di transizioni $\langle S, s_0, \longrightarrow \rangle$, dove:

- $S = (L_1 \times \cdots \times L_n) \times V(C)$: uno stato è un vettore di locazioni + un clock assignment
- $s_0 = \langle \overline{l_0}, v_0 \rangle$
- $\longrightarrow \subseteq S \times S$ è tale che:
  - $\langle \bar{l}, v \rangle \longrightarrow \langle \bar{l}, v + d \rangle$, per $d \in \mathbb{R}_{>0}$ tale che per ogni $d'$, se $0 \leq d' \leq d$ allora $v + d' \models \mathcal{I}(\bar{l})$;
  - $\langle \bar{l}, v \rangle \longrightarrow \langle \bar{l}[l_i'/l_i], v' \rangle$, se esiste $e \in E_i$, $e = l_i \overset{\tau, g, X}{\longrightarrow} l_i'$, tale che:

$$v \models g, \qquad v' = v[X \mapsto 0], \qquad v' \models \mathcal{I}(\bar{l}[l_i'/l_i])$$

# Semantica delle NTA

La semantica di una NTA $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$, con $\mathcal{A}_i = \langle L_i, l_i^0, C, A, E_i, \mathcal{I}_i \rangle$, è data da un sistema di transizioni $\langle S, s_0, \longrightarrow \rangle$, dove:

- $S = (L_1 \times \cdots \times L_n) \times V(C)$: uno stato è un vettore di locazioni + un clock assignment
- $s_0 = \langle \overline{l_0}, v_0 \rangle$
- $\longrightarrow \subseteq S \times S$ è tale che:
  - $\langle \bar{l}, v \rangle \longrightarrow \langle \bar{l}, v + d \rangle$, per $d \in \mathbb{R}_{>0}$ tale che per ogni $d'$, se $0 \leq d' \leq d$ allora $v + d' \models \mathcal{I}(\bar{l})$;
  - $\langle \bar{l}, v \rangle \longrightarrow \langle \bar{l}[l_i'/l_i], v' \rangle$, se esiste $e \in E_i$, $e = l_i \xrightarrow{\tau, g, X} l_i'$, tale che:

$$v \models g, \qquad v' = v[X \mapsto 0], \qquad v' \models \mathcal{I}(\bar{l}[l_i'/l_i])$$

  - $\langle \bar{l}, v \rangle \longrightarrow \langle \bar{l}[l_i'/l_i, l_j'/l_j], v' \rangle$, se esistono $e_i \in E_i$, $e_j \in E_j$:

$$e_i = l_i \xrightarrow{a?, g_i, X_i} l_i' \qquad e_j = l_j \xrightarrow{a!, g_j, X_j} l_j'$$

tali che:

$$v \models g_i \wedge g_j,$$

# Semantica delle NTA

La semantica di una NTA $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$, con $\mathcal{A}_i = \langle L_i, l_i^0, C, A, E_i, \mathcal{I}_i \rangle$, è data da un sistema di transizioni $\langle S, s_0, \longrightarrow \rangle$, dove:

- $S = (L_1 \times \cdots \times L_n) \times V(C)$: uno stato è un vettore di locazioni + un clock assignment
- $s_0 = \langle \overline{l_0}, v_0 \rangle$
- $\longrightarrow \subseteq S \times S$ è tale che:
  - $\langle \bar{l}, v \rangle \longrightarrow \langle \bar{l}, v + d \rangle$, per $d \in \mathbb{R}_{>0}$ tale che per ogni $d'$, se $0 \leq d' \leq d$ allora $v + d' \models \mathcal{I}(\bar{l})$;
  - $\langle \bar{l}, v \rangle \longrightarrow \langle \bar{l}[l_i'/l_i], v' \rangle$, se esiste $e \in E_i$, $e = l_i \xrightarrow{\tau, g, X} l_i'$, tale che:

$$v \models g, \qquad v' = v[X \mapsto 0], \qquad v' \models \mathcal{I}(\bar{l}[l_i'/l_i])$$

  - $\langle \bar{l}, v \rangle \longrightarrow \langle \bar{l}[l_i'/l_i, l_j'/l_j], v' \rangle$, se esistono $e_i \in E_i$, $e_j \in E_j$:

$$e_i = l_i \xrightarrow{a?, g_i, X_i} l_i' \qquad e_j = l_j \xrightarrow{a!, g_j, X_j} l_j'$$

tali che:

$$v \models g_i \wedge g_j, \qquad v' = v[X_i \cup X_j \mapsto 0],$$

# Semantica delle NTA

La semantica di una NTA $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$, con $\mathcal{A}_i = \langle L_i, l_i^0, C, A, E_i, \mathcal{I}_i \rangle$, è data da un sistema di transizioni $\langle S, s_0, \longrightarrow \rangle$, dove:

- $S = (L_1 \times \cdots \times L_n) \times V(C)$: uno stato è un vettore di locazioni + un clock assignment
- $s_0 = \langle \bar{l_0}, v_0 \rangle$
- $\longrightarrow \subseteq S \times S$ è tale che:
  - $\langle \bar{l}, v \rangle \longrightarrow \langle \bar{l}, v + d \rangle$, per $d \in \mathbb{R}_{>0}$ tale che per ogni $d'$, se $0 \leq d' \leq d$ allora $v + d' \models \mathcal{I}(\bar{l})$;
  - $\langle \bar{l}, v \rangle \longrightarrow \langle \bar{l}[l_i'/l_i], v' \rangle$, se esiste $e \in E_i$, $e = l_i \xrightarrow{\tau, g, X} l_i'$, tale che:

$$v \models g, \qquad v' = v[X \mapsto 0], \qquad v' \models \mathcal{I}(\bar{l}[l_i'/l_i])$$

  - $\langle \bar{l}, v \rangle \longrightarrow \langle \bar{l}[l_i'/l_i, l_j'/l_j], v' \rangle$, se esistono $e_i \in E_i$, $e_j \in E_j$:

$$e_i = l_i \xrightarrow{a?, g_i, X_i} l_i' \qquad e_j = l_j \xrightarrow{a!, g_j, X_j} l_j'$$

tali che:

$$v \models g_i \wedge g_j, \qquad v' = v[X_i \cup X_j \mapsto 0], \qquad v' \models \mathcal{I}(\bar{l}[l_i'/l_i, l_j'/l_j])$$

# Transizioni di stato


Transizioni non sincronizzate di due processi si alternano, non possono avvenire contemporaneamente.

| **Sono transizioni** | **Non sono transizioni** |
|---|---|
| $\langle A, uno\rangle \longrightarrow \langle B, uno\rangle$ | |
| $\langle A, uno\rangle \longrightarrow \langle A, due\rangle$ | $\langle A, uno\rangle \longrightarrow \langle B, due\rangle$ |
| $\langle B, uno\rangle \longrightarrow \langle B, due\rangle$ | |
| $\langle A, due\rangle \longrightarrow \langle B, due\rangle$ | |

# Transizioni di stato


Transizioni non sincronizzate di due processi si alternano, non possono avvenire contemporaneamente.

Transizioni sincronizzate di due processi possono solo avvenire contemporaneamente.

| **Sono transizioni** | **Non sono transizioni** |
|---|---|
| $\langle A, uno\rangle \longrightarrow \langle B, uno\rangle$ | |
| $\langle A, uno\rangle \longrightarrow \langle A, due\rangle$ | $\langle A, uno\rangle \longrightarrow \langle B, due\rangle$ |
| $\langle B, uno\rangle \longrightarrow \langle B, due\rangle$ | |
| $\langle A, due\rangle \longrightarrow \langle B, due\rangle$ | |
| $\langle B, due\rangle \longrightarrow \langle C, tre\rangle$ | $\langle B, due\rangle \longrightarrow \langle C, due\rangle$ |
| | $\langle B, due\rangle \longrightarrow \langle B, tre\rangle$ |

# Transizioni di stato

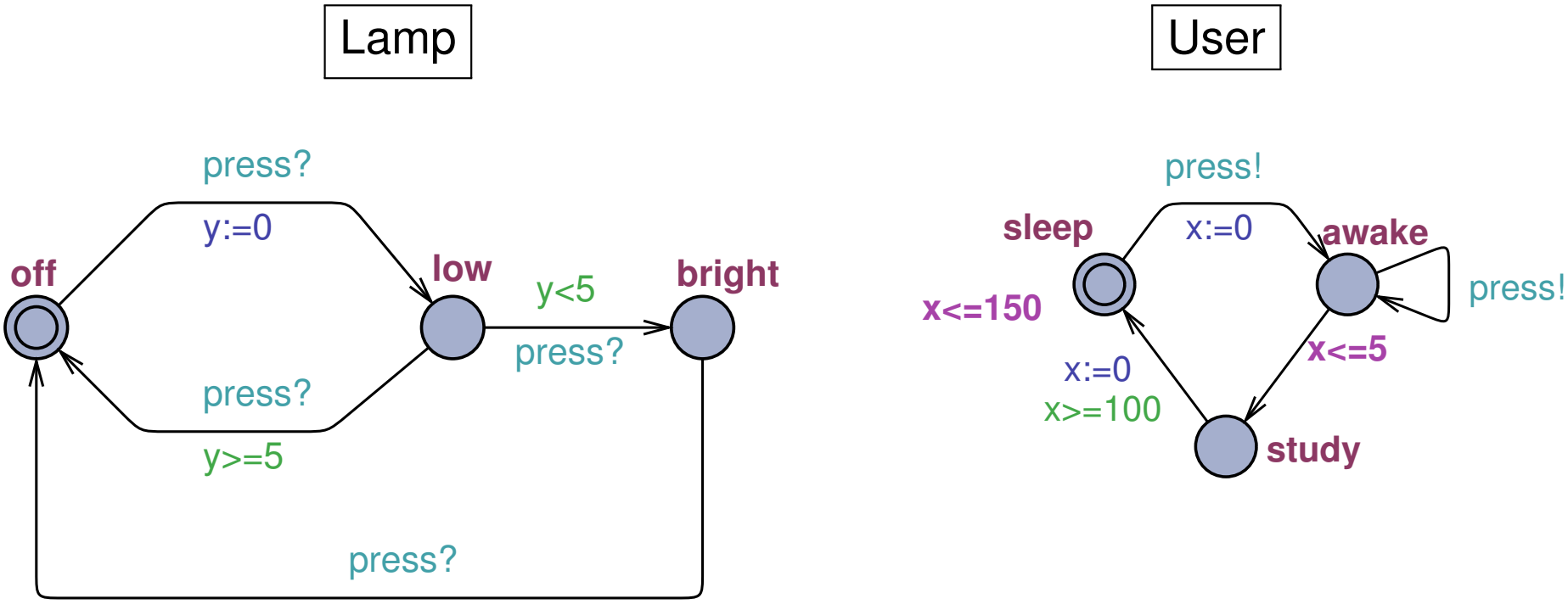

Transizioni non sincronizzate di due processi si alternano, non possono avvenire contemporaneamente.

Transizioni sincronizzate di due processi possono solo avvenire contemporaneamente.

Perché possa avvenire una transizione con azione di input/output, deve contemporaneamente avvenire la corrispondente azione di output/input

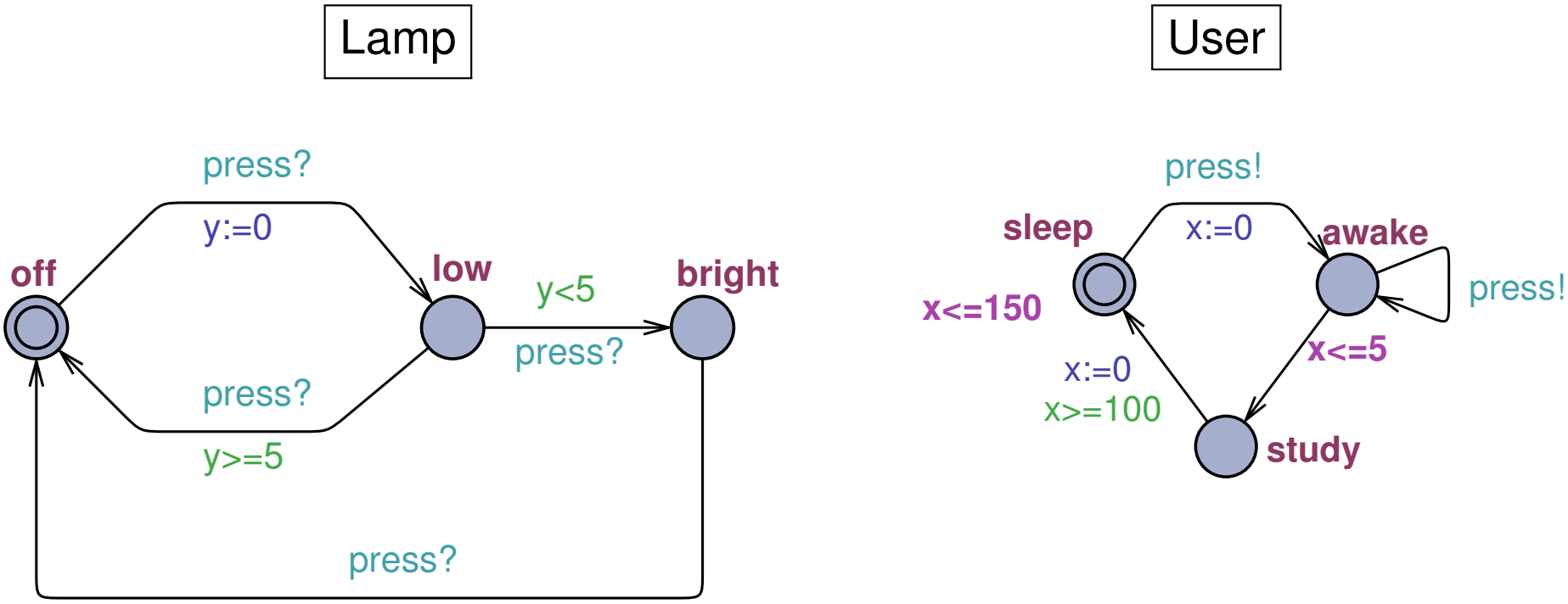
| **Sono transizioni** | **Non sono transizioni** |
|---|---|
| $\langle A, uno\rangle \longrightarrow \langle B, uno\rangle$<br>$\langle A, uno\rangle \longrightarrow \langle A, due\rangle$<br>$\langle B, uno\rangle \longrightarrow \langle B, due\rangle$<br>$\langle A, due\rangle \longrightarrow \langle B, due\rangle$ | $\langle A, uno\rangle \longrightarrow \langle B, due\rangle$ |
| $\langle B, due\rangle \longrightarrow \langle C, tre\rangle$ | $\langle B, due\rangle \longrightarrow \langle C, due\rangle$<br>$\langle B, due\rangle \longrightarrow \langle B, tre\rangle$ |
| | $\langle A, due\rangle \longrightarrow \langle A, tre\rangle$<br>$\langle B, uno\rangle \longrightarrow \langle C, uno\rangle$ |

# Esempio



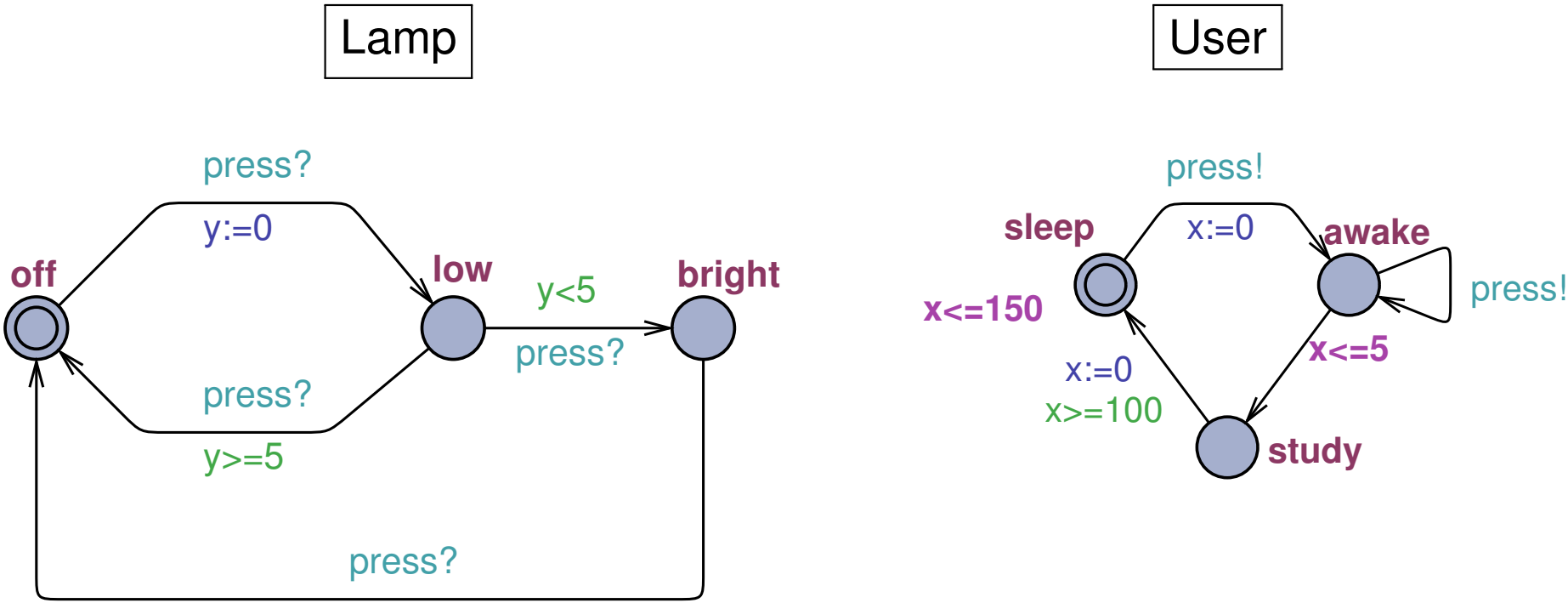

- $\langle (low, awake), v_{x=2,y=3} \rangle \longrightarrow \langle (low, awake), v_{x=5,y=6} \rangle$ perché per ogni $d'$, se $0 \leq d' \leq 3$ allora $v_{x=2+d',y=3+d'} \models x \leq 5$;
- **Ma** non esiste una transizione da $\langle (low, awake), v_{x=2,y=3} \rangle$ a $\langle (low, awake), v_{x=10,y=11} \rangle$ perché per $4 \leq d' \leq 8$, $v_{x=2+d',y=3+d'} \not\models x \leq 5$

# Esempio



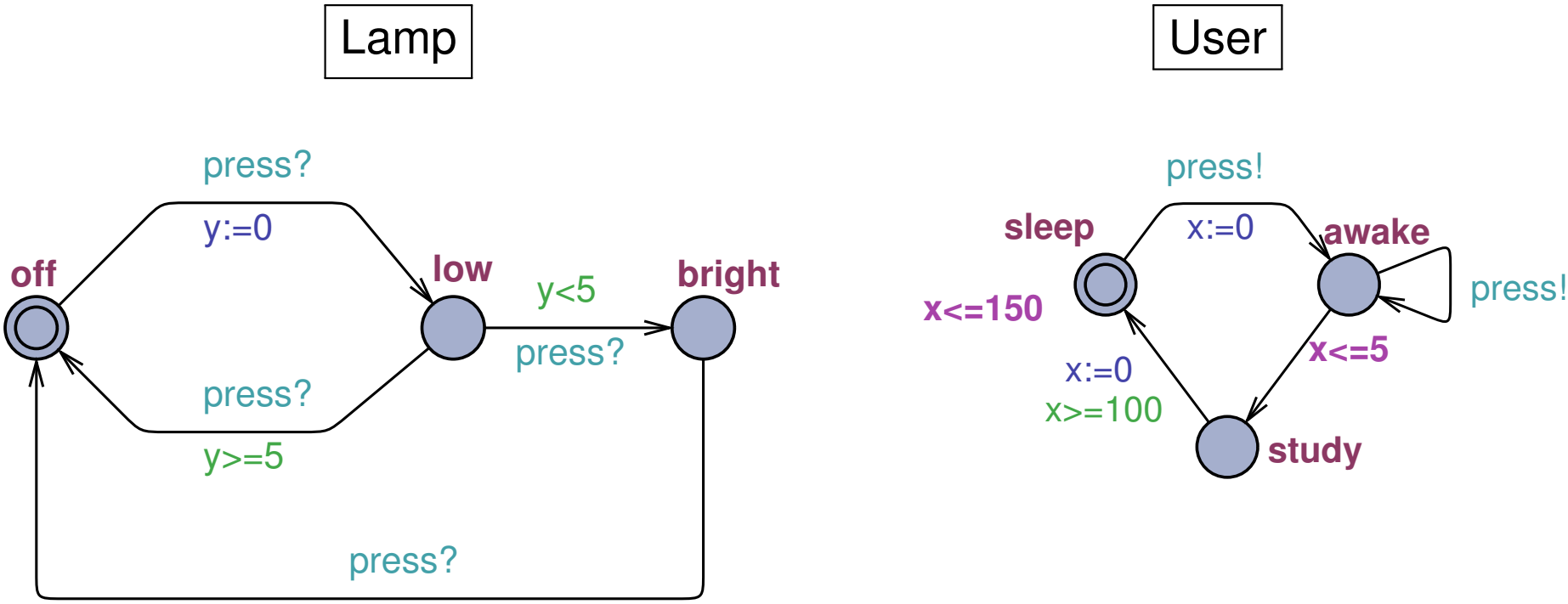

- $\langle (low, study), v_{x=110,y=8} \rangle \longrightarrow \langle (low, sleep), v_{x=0,y=8} \rangle$ perché la transizione da study a sleep è "interna" (azione $\tau$), $v_{x=110,y=8} \models x \geq 100$, $v_{x=0,y=8} = v_{x=110,y=8}[x \mapsto 0]$ e $v_{x=0,y=8} \models x \leq 150$
- **Ma** non esiste una transizione da $\langle (low, study), v_{x=50,y=8} \rangle$ a $\langle (low, sleep), v_{x=0,y=8} \rangle$ perché $v_{x=50,y=8} \not\models x \geq 100$

# Esempio




- $\langle (off, sleep), v_{x=100,y=10} \rangle \longrightarrow \langle (low, awake), v_{x=0,y=0} \rangle$ perché le transizioni $off \rightarrow low$ e $sleep \rightarrow awake$ sono sincronizzate, non ci sono guardie da soddisfare, $v_{x=0,y=0} = v_{x=100,y=10}[x, y \mapsto 0]$ e $v_{x=0,y=0} \models x \leq 5$
- **Ma** non esiste una transizione da $\langle (low, sleep), v_{x=100,y=10} \rangle$ a $\langle (bright, awake), v_{x=0,y=10} \rangle$ perché $v_{x=100,y=10} \not\models y < 5$

# Esempio




- **Non** esiste una transizione da $\langle (off, sleep), v_{x=100,y=10} \rangle \longrightarrow \langle (off, awake), v_{x=0,y=10} \rangle$ perché l'azione della transizione $sleep \rightarrow awake$ non è $\tau$, quindi l'automa User non può eseguire la action transition da solo, ma Lamp deve sincronizzarsi con User: quando User manda il messaggio press!, Lamp **deve** recepire il messaggio (press?) e eseguire la transizione $off \rightarrow low$.

# Esercizi

Esercizi proposti su automi temporizzati e Uppaal:

http://cialdea.dia.uniroma3.it/teaching/logica/slides/3-verifica/esercizi.pdf

Fare gli esercizi da 2 a 5, senza considerare le richieste relative alla formulazione di queries Uppaal.