HyTech

Laboratorio di Sistemi in Tempo Reale

Corso di Laurea in Informatica Multimediale

13 Novembre 2008

Outline

1. Una breve introduzione ad HyTech
2. Il bruciatore che perde
3. Il passaggio a livello
4. Esercizio

HyTech è un pacchetto per la verifica di automi ibridi lineari

- sviluppato dall'Università di Berkeley, California
- permette di modellare sistemi più complessi di UPPAAL: automi ibridi lineari
- interfaccia di tipo testuale
- verifica di semplici proprietà di sicurezza e raggiungibilità
- sintesi automatica di parametri

Programma e documentazione:
`http://embedded.eecs.berkeley.edu/research/hytech/`

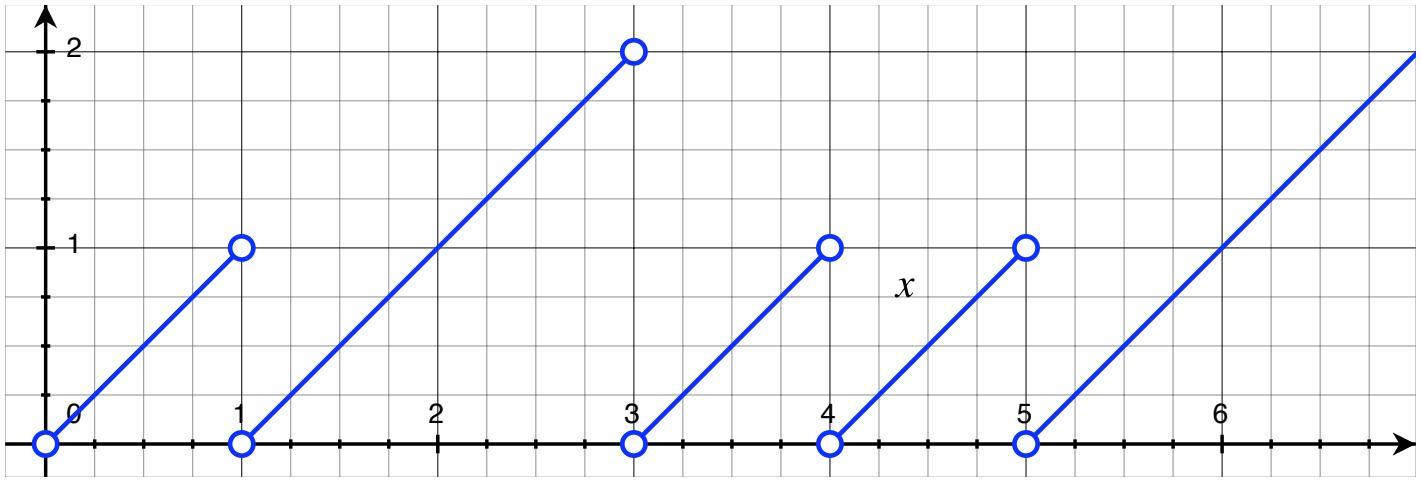
Automi ibridi lineari

Gli automi ibridi lineari estendono gli automi temporizzati:

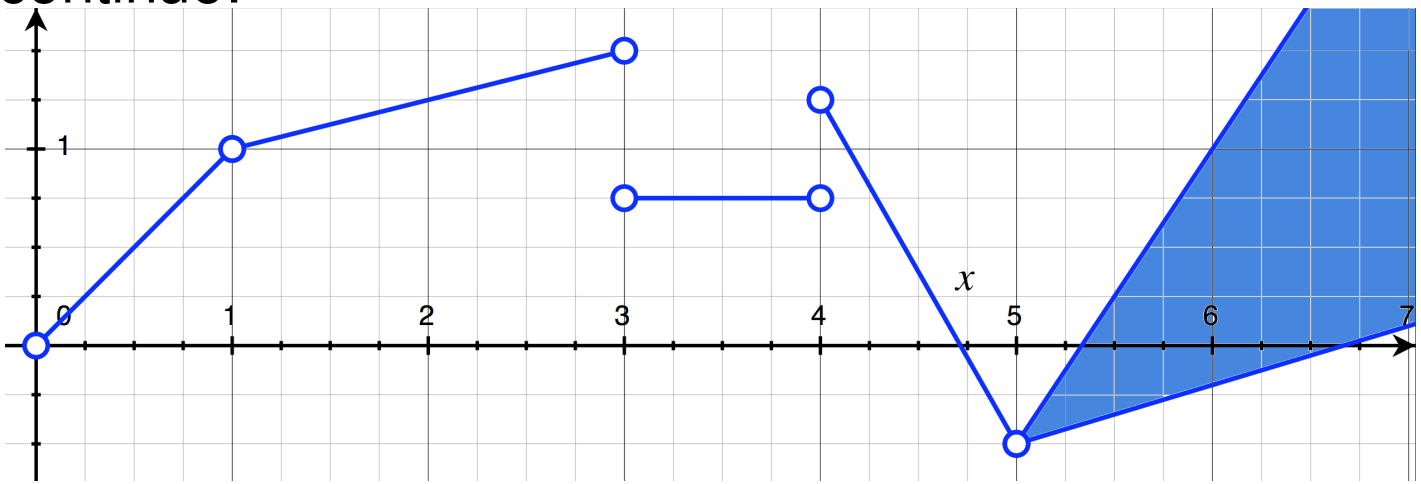
- **variabili continue** con derivata costante a tratti anziché orologi:
  $\dot{x} = 15, \quad \dot{y} = 0, \quad \dot{z} = -2, \quad \dot{t} \in [20, 50]$
- condizioni più complesse sui reset:
  $x' = 5, \quad y' <= 3, \quad z' = x + 5 - 2z$

Automi temporizzati vs. Automi Ibridi Lineari

Orologi:



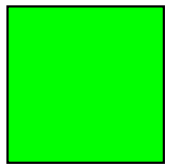
Variabili continue:



Funzionalità di HyTech

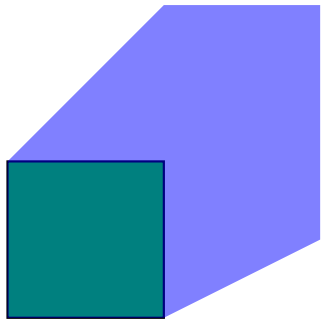
- **Variabili intere:** lo stato del sistema dipende anche da variabili intere che vengono modificate solamente dalle transizioni discrete.
- **Reti di automi:** un sistema può essere composto da più automi che evolvono in parallelo.
- **Sincronizzazione:** gli automi comunicano con segnali che etichettano le transizioni (no differenza ingresso/uscita).
- **Parametri:** alcune costanti del sistema possono essere lasciate come non specificate. HyTech permette di determinare i valori corretti.

Raggiungibilità in avanti



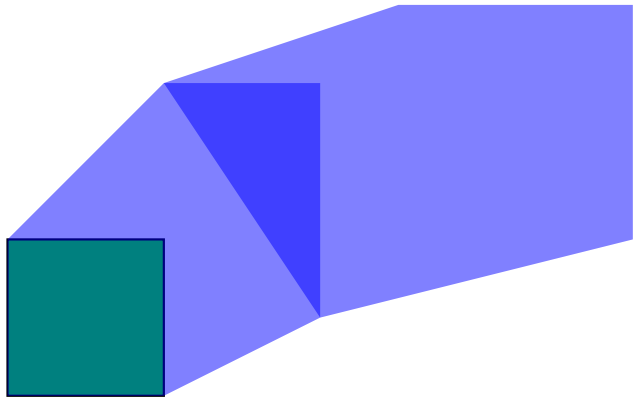
- si parte da un **insieme iniziale** di stati
- facendo scorrere il tempo in avanti, si calcola la **regione raggiunta** dal sistema.
- ci si ferma se e quando la regione si stabilizza.

Raggiungibilità in avanti



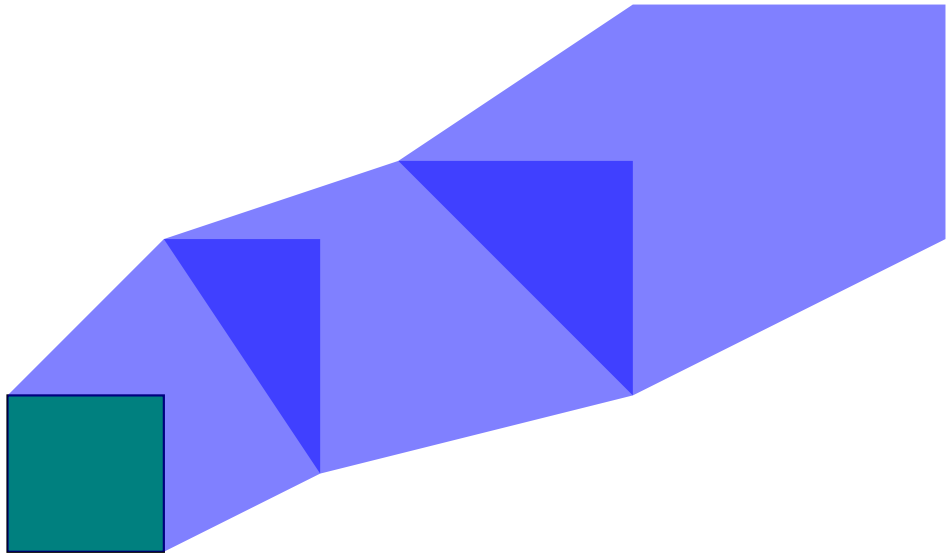
- si parte da un **insieme iniziale** di stati
- facendo scorrere il tempo in avanti, si calcola la **regione raggiunta** dal sistema.
- ci si ferma se e quando la regione si stabilizza.

Raggiungibilità in avanti



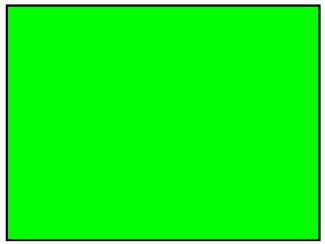
- si parte da un **insieme iniziale** di stati
- facendo scorrere il tempo in avanti, si calcola la **regione raggiunta** dal sistema.
- ci si ferma se e quando la regione si stabilizza.

Raggiungibilità in avanti



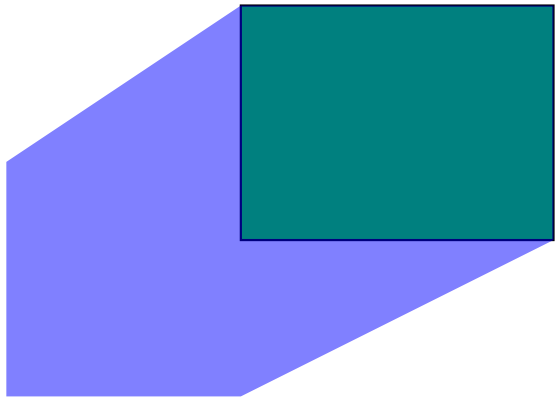
- si parte da un **insieme iniziale** di stati
- facendo scorrere il tempo in avanti, si calcola la **regione raggiunta** dal sistema.
- ci si ferma se e quando la regione si stabilizza.

Raggiungibilità all'indietro



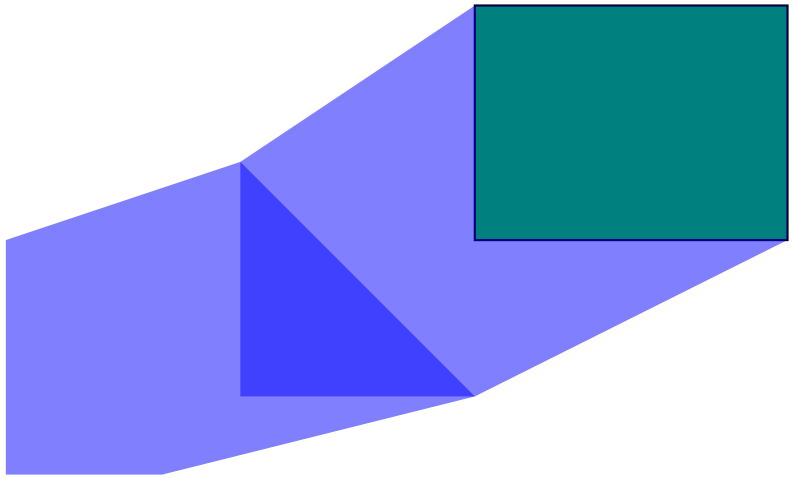
- si parte da un **insieme iniziale** di stati
- facendo scorrere il tempo all'indietro, si calcola la **regione raggiunta** dal sistema.
- ci si ferma se e quando la regione si stabilizza.

Raggiungibilità all'indietro



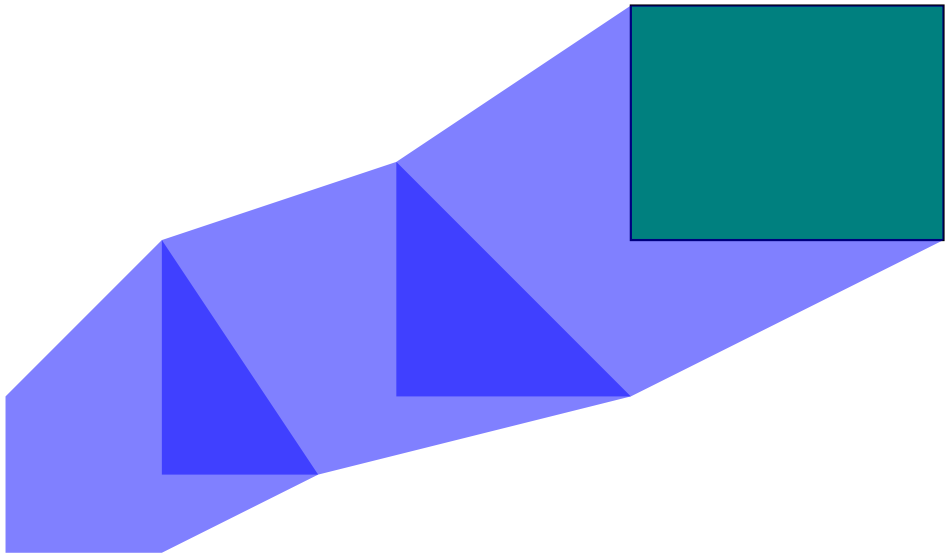
- si parte da un **insieme iniziale** di stati
- facendo scorrere il tempo all'indietro, si calcola la **regione raggiunta** dal sistema.
- ci si ferma se e quando la regione si stabilizza.

Raggiungibilità all'indietro



- si parte da un **insieme iniziale** di stati
- facendo scorrere il tempo all'indietro, si calcola la **regione raggiunta** dal sistema.
- ci si ferma se e quando la regione si stabilizza.

Raggiungibilità all'indietro



- si parte da un **insieme iniziale** di stati
- facendo scorrere il tempo all'indietro, si calcola la **regione raggiunta** dal sistema.
- ci si ferma se e quando la regione si stabilizza.

Attenzione!

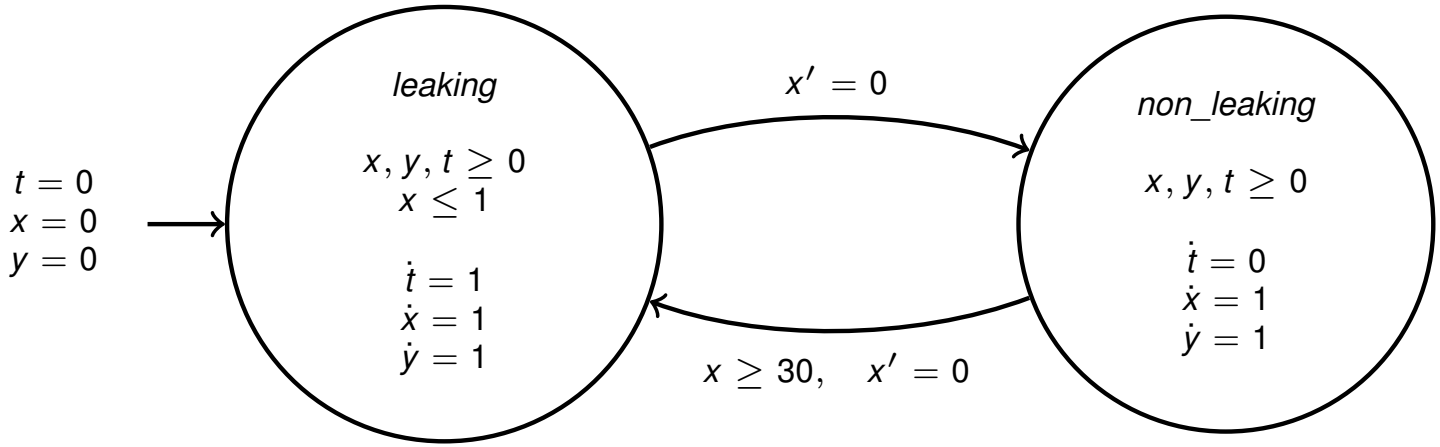
Le procedure di raggiungibilità in avanti/all'indietro non terminano sempre: può succedere che aggiungano sempre nuovi stati all'infinito.

- per alcuni sistemi, terminano tutte e due;
- per altri sistemi, ne termina solamente una;
- nei casi peggiori, nessuna delle due termina.

Outline

1. Una breve introduzione ad HyTech
2. Il bruciatore che perde
3. Il passaggio a livello
4. Esercizio

Esempio: un bruciatore che perde



- ogni perdita di gas viene identificata e fermata entro 1 secondo
- tra una perdita e la successiva trascorrono almeno 30 secondi
- x è un orologio locale usato per misurare 1 secondo oppure 30 secondi
- t misura il tempo complessivo di perdita di gas
- y misura il tempo totale

Verificare che, se sono trascorsi almeno 60 secondi, allora il bruciatore ha perso gas per meno di $1/20$ del tempo totale.

- Regione degli stati "cattivi": $y \geq 60$ e $t \geq 1/20y$;
- Calcoliamo la regione raggiungibile all'indietro dagli stati "cattivi";
- La regione calcolata contiene almeno uno stato iniziale?
  - **Si:** il sistema non rispetta la proprietà;
  - **No:** il sistema rispetta la proprietà.

Il codice HyTech per il problema del bruciatore (1)

```
-- leaking gas burner
var
     x,y: clock;
     t:stopwatch;

automaton gb
synclabs:;
initially leaking & t=0 & x=0 & y=0;
loc leaking:
  while x>=0 & y>=0 & t>=0 & x<=1 wait {dt=1}
  when True do {x' = 0} goto not_leaking;
loc not_leaking:
  while x>=0 & y>=0 & t>=0 wait {dt=0}
  when x>=30 do {x' = 0} goto leaking;
end
```

Il codice HyTech per il problema del bruciatore (2)

```
var init_reg, bad_reg, b_reachable: region;

init_reg := loc[gb]=leaking & x=0 & t=0 & y=0;

bad_reg :=  y>=60 & t >= 1/20 y;

b_reachable := reach backward from bad_reg endreach;

if empty( b_reachable & init_reg)
  then prints "System is safe";
  else prints "System is not safe";
endif;
```

- Il problema del bruciatore si trova negli esempi di HyTech: provatelo
- La proprietà si può verificare anche con la raggiungibilità in avanti:
  - ```
    f_reach := reach forward from init_reg endreach;
    if empty( f_reach & bad_reg)
      then prints "System is safe";
      else prints "System is not safe";
    endif;
    ```
  - per questo sistema, la raggiungibilità in avanti non termina
    ```

Outline

1. Una breve introduzione ad HyTech
2. Il bruciatore che perde
3. Il passaggio a livello
4. Esercizio

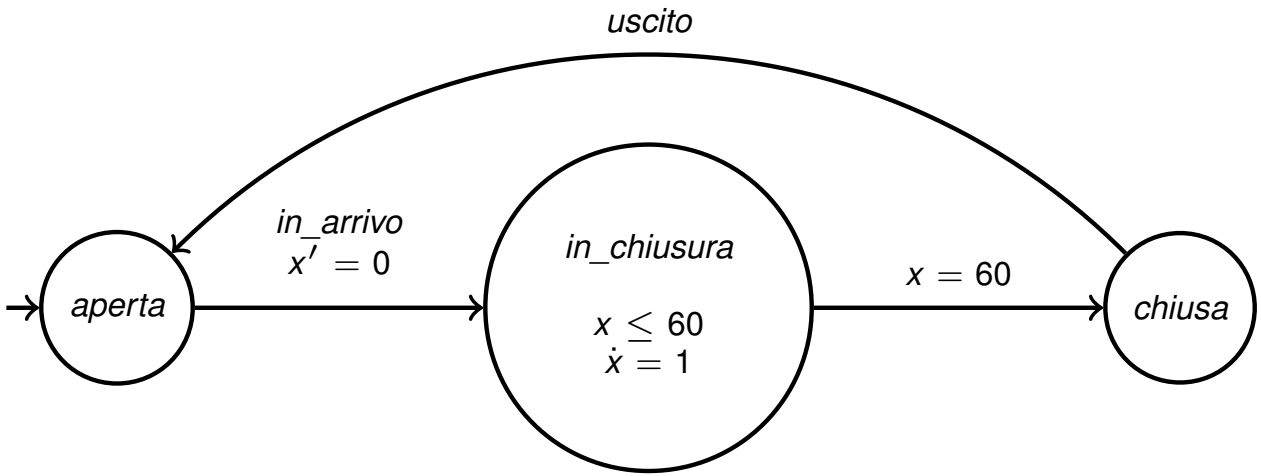
Problema:

progettare il controllore di un passaggio a livello

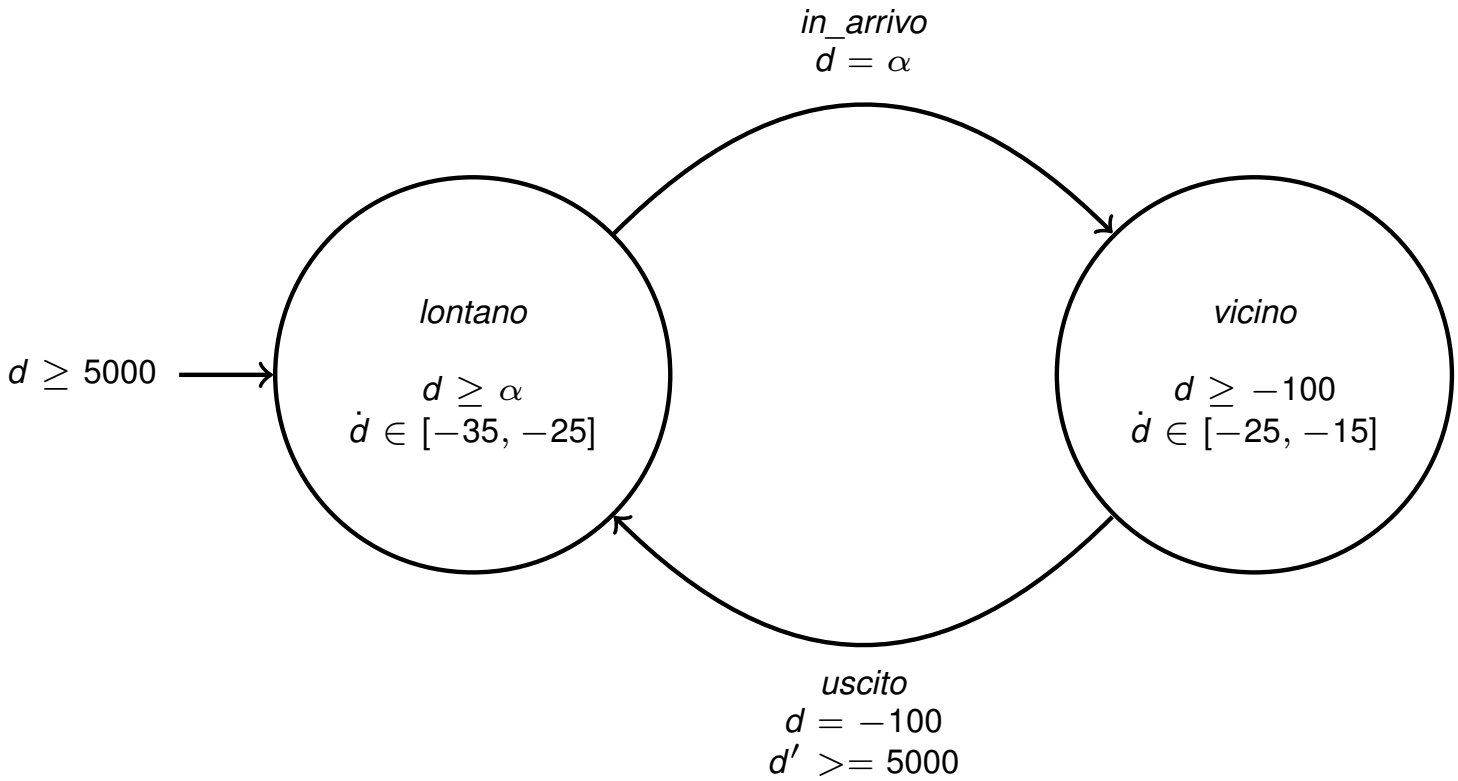
- il treno si avvicina al passaggio a livello con velocità tra i 25 e i 35 m/s;
- giunto ad una distanza α, segnala la sua presenza e riduce la velocità all'intervallo $[15, 25]$ m/s;
- $100m$ dopo il passaggio a livello, il treno segnala che è uscito dal passaggio a livello
- la sbarra impiega 60 secondi per chiudersi;

Garantire che la sbarra sia chiusa se il treno è a meno di $100m$

L'automa della sbarra



L'automa del treno



```
-- esempio del passaggio a livello
var
x: clock;
d: analog;
alpha: parameter;

automaton sbarra
synclabs: in_arrivo, uscito;
initially aperta;
loc aperta:
  while True wait {}
  when True sync in_arrivo do {x' = 0} goto in_chiusura;
loc in_chiusura:
  while x <= 60 wait {}
  when x = 60 goto chiusa;
loc chiusa:
  while True wait {}
  when True sync uscito goto aperta;
end -- sbarra
```

```
automaton treno
synclabs : in_arrivo, uscito;
initially lontano & d>=5000;
loc lontano:
  while d >= alpha wait {dd in [-35,-25]}
  when d = alpha sync in_arrivo goto vicino;
loc vicino:
  while d>=-100 wait {dd in [-25,-15]}
  when d=-100 sync uscito do {d' >= 5000} goto lontano;
end -- treno
```

```
-- comandi di analisi
var
   bad_reg, init_reg : region;

init_reg := loc[treno] = lontano & d>=5000
            & loc[sbarra] = aperta;
bad_reg := d >= -100 & d <= 100 &
   (loc[sbarra] = in_chiusura | loc[sbarra] = aperta);

-- stampa i valori dei parametri
print omit all locations
  hide non_parameters in
    reach forward from init_reg endreach
    & bad_reg
  endhide;
```

Risultati

Hytech calcola i valori del parametro `alpha` tali che il sistema non rispetta la proprietà voluta:

```
    alpha <= 100
|
    alpha <= 1600    & alpha + 100 >= 0
```

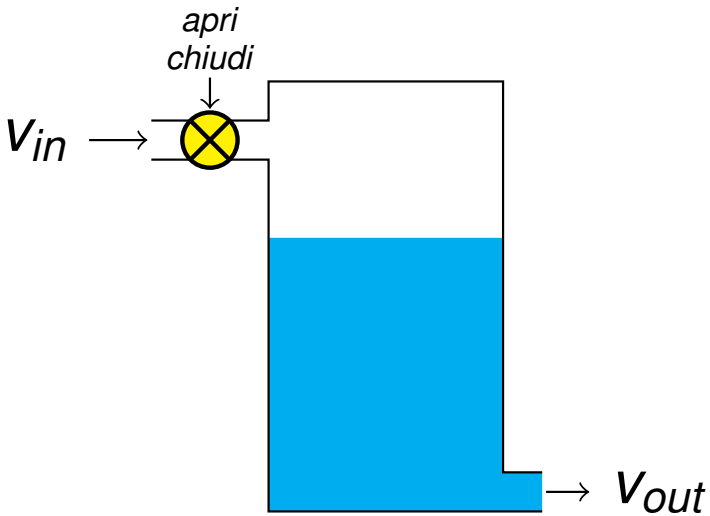
Conclusione

Il passaggio a livello è sicuro se il treno segnala il suo arrivo almeno 1600 metri prima.

Outline

1. Una breve introduzione ad HyTech
2. Il bruciatore che perde
3. Il passaggio a livello
4. Esercizio

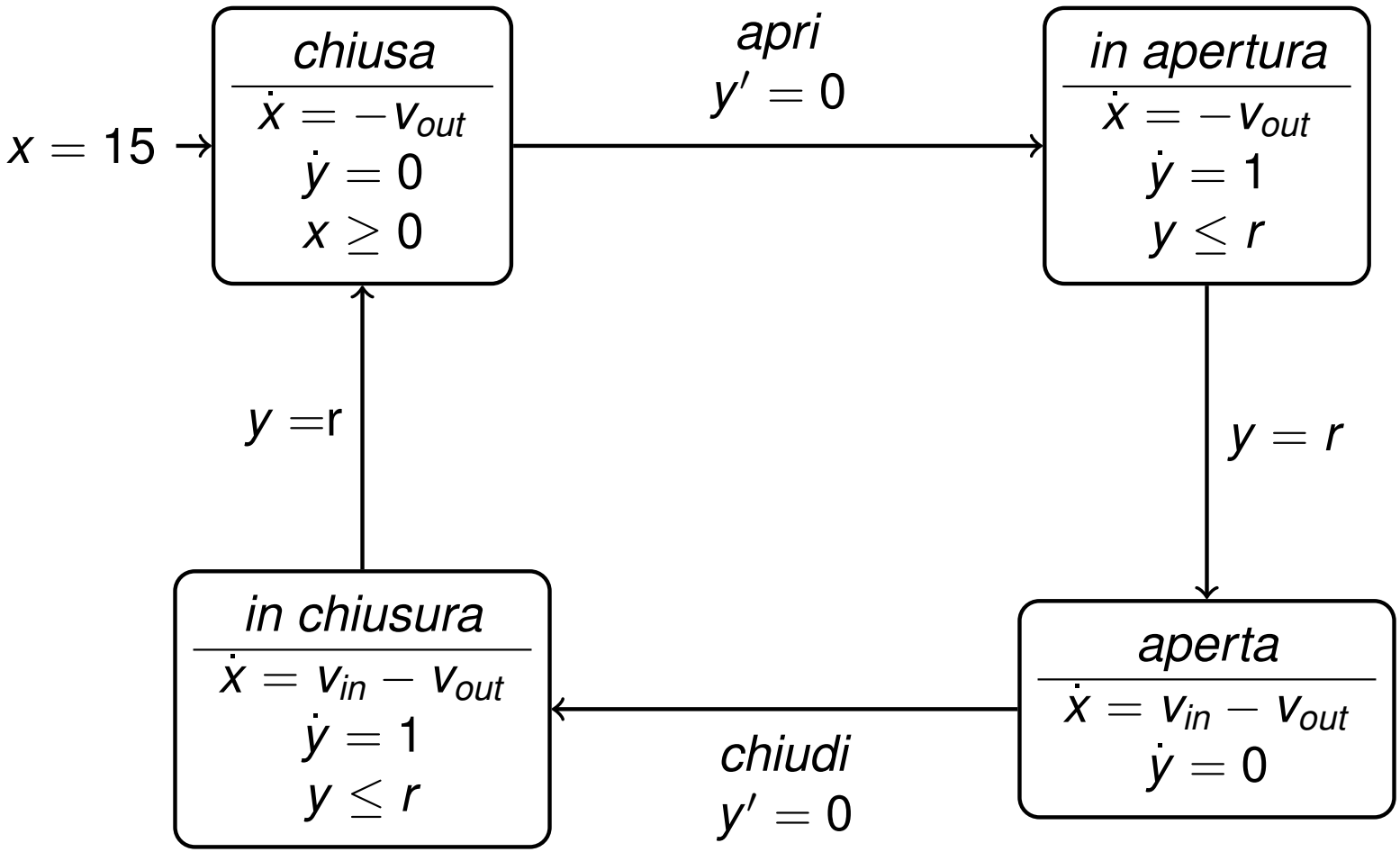
Progettare il controllore di una cisterna



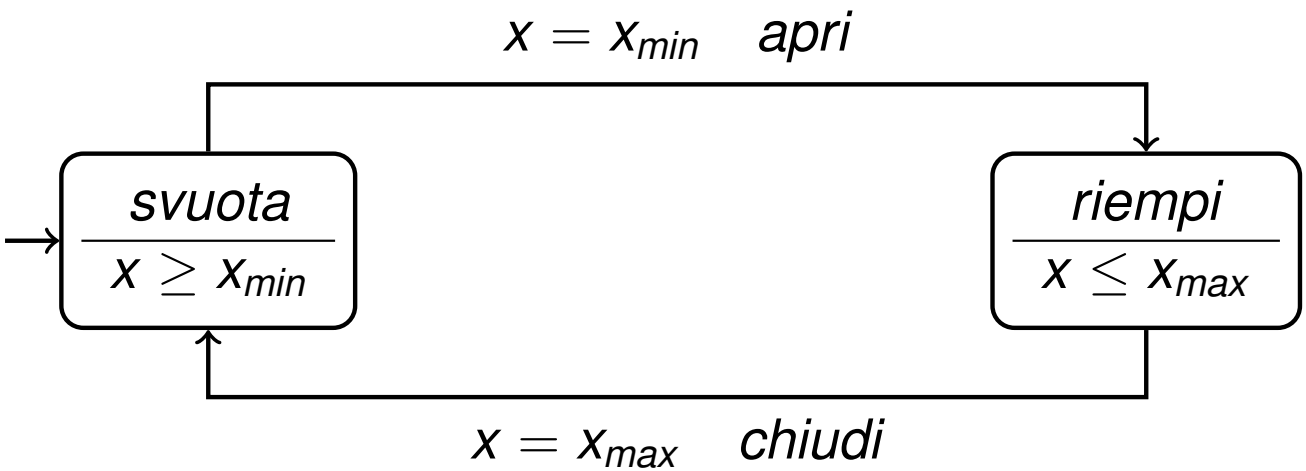
- l'acqua esce dalla cisterna con $v_{out} = 2$;
- se la valvola è aperta, l'acqua entra nella cisterna con $v_{in} = 5$;
- quando riceve un segnale, la valvola impiega un certo ritardo r per aprirsi/chiudersi;
- il controllore segnala alla valvola di aprirsi quando il livello è $x_{min} = 9$ e di chiudersi quando il livello è $x_{max} = 21$;
- il livello iniziale dell'acqua è 15;

Qual'è il ritardo massimo che la valvola può avere affinché il livello si mantenga tra 5 e 25?

L'automa della cisterna



L'automa del controllore



1. Implementare il sistema cisterna / controllore in HyTech;
2. determinare per quali valori di r il livello dell'acqua rimane all'interno dell'intervallo specificato;
3. considerare anche x_{min} e x_{max} come parametri, e determinare per quali valori di r, x_{min} e x_{max} il livello dell'acqua rimane nell'intervallo specificato.

http://profs.sci.univr.it/~bresolin/lab02.pdf