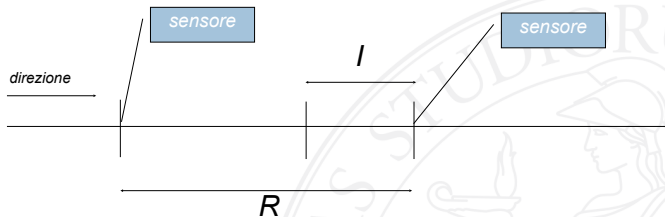
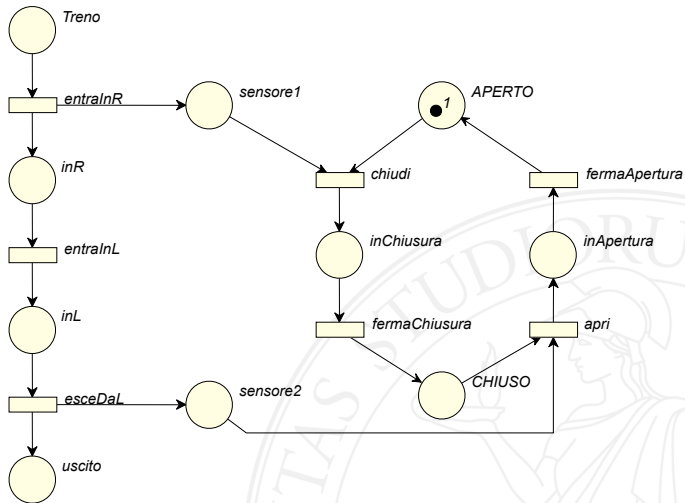


Modellare con reti TB

- Modellare un passaggio a livello con una rete di Petri

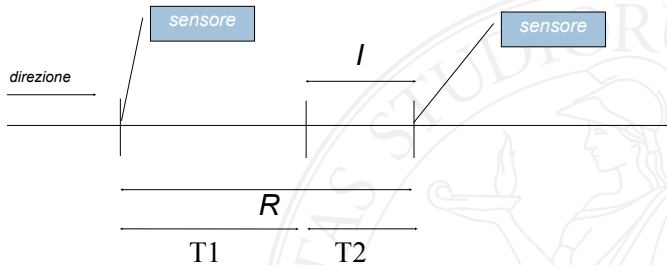


Soluzione

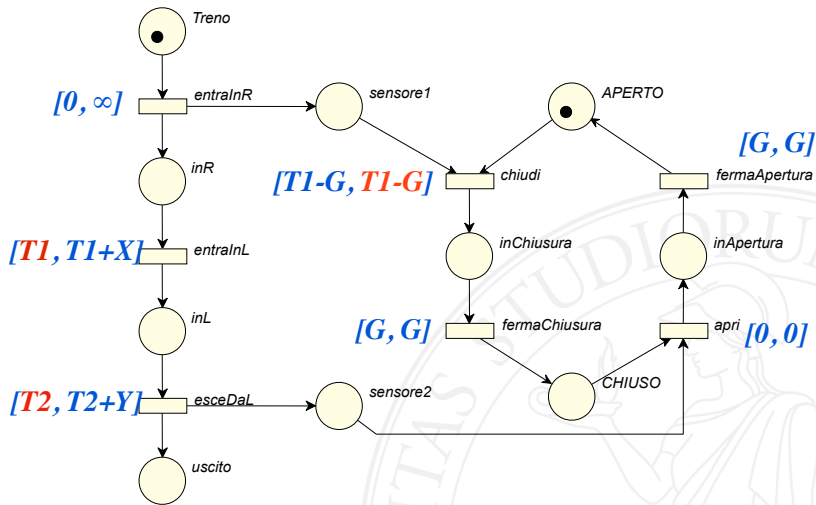


Aggiungere i tempi

- Modellare un passaggio a livello con una rete di Petri



Soluzione



Analisi

- È una soluzione corretta?
 - NO
- Perché si possono scontrare macchine e treni?
 - ipotesi non espresse o errori di specifica
 - Cosa succede se un secondo treno entra in R prima che il precedente esca da L?
 - Cosa succede se un secondo treno entra in R prima che il passaggio si sia riaperto completamente?

Tempo come concetto derivato

- Tempo = variabile associata ai gettoni (chronos)
- Predicati determinano la possibilità di scatto di una transizione a partire dai valori dei gettoni (incluso il chronos)
- Le azioni determinano i valori dei gettoni creati (incluso il valore della variabile chronos)
- NOTA: Le azioni devono produrre lo stesso valore per i chronos di tutti i gettoni creati (birth date) e devono essere non minori dei valori dei chronos dei gettoni rimossi.

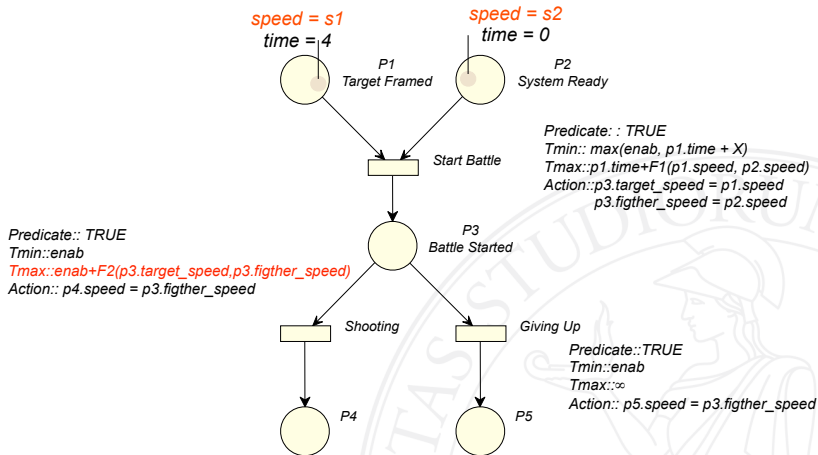
Semantiche temporali nelle ER nets

- $\text{chronos} + \text{assiomi } 1,3 = \text{WTS}$
- $\text{chronos} + \text{assiomi } 1, 2, 3 = \text{MWTS}$
- $\text{chronos} + \text{assiomi } 1, 2, 3, 4, 5 = \text{STS}$
- È possibile esprimerli?

Un modello completo: HLTPN (TER net)

- HLTPNs possono modellare:
 - Aspetti funzionali (high-level Petri nets: ER net)
 - Aspetti temporali (time Petri nets: TB net)
 - Dipendenze di aspetti funzionali da aspetti temporali
 - Dipendenze di aspetti temporali da aspetti funzionali
- Le reti HLTPN possono essere analizzate con gli stessi limiti delle reti TB

High-Level time Petri nets (HLTPNs)



Analisi di reti temporizzate

- Analisi di raggiungibilità
 - Enumerazione degli stati finiti raggiungibili
- PROBLEMI:
 - Lo scatto di una transizione può produrre infiniti stati che si differenziano tra loro per il tempo associato ai gettoni prodotti (tempo di scatto)
 - La rete può evolvere all'infinito
 - Il tempo avanza...
 - L'albero di raggiungibilità è infinito!!
 - Non è lo stesso problema delle reti non limitate, non si può usare l'albero di copertura

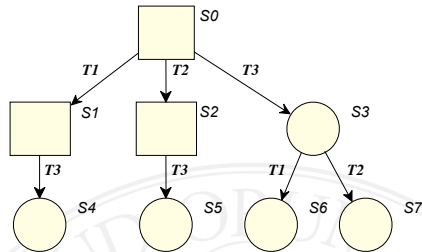
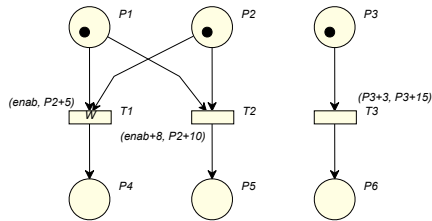
Analisi di raggiungibilità temporale per le reti TB

- Rappresentazione simbolica degli stati
- Uno stato simbolico rappresenta un insieme di possibili stati con in comune lo stesso numero di gettoni in ogni posto (marcatura P/T)
- Uno stato simbolico è una coppia $[\mu, C]$, dove
 - μ = marcatura simbolica: associa multiset di identificatori simbolici ai posti
 - C = vincoli: (dis)equazioni che rappresentano le relazioni tra gli identificatori simbolici

Funzioni temporali...

- Assumiamo che tf_t sia un intervallo con estremi inclusi esprimibili mediante espressioni lineari funzioni dei tempi dei token in ingresso e di tempi assoluti
 - $tmin_t$ limite inferiore
 - $tmax_t$ limite superiore
- $tf_t = \{ X \mid X \geq tmin_t \wedge X \leq tmax_t \}$

Sample Reachability Tree



S0 Marcatura: $\mu(P1) = \{\tau_1\}$ $\mu(P2) = \{\tau_0\}$ $\mu(P3) = \{\tau_0\}$
 $C_0 := 0 \leq \tau_0 \wedge \tau_0 \leq 10 \wedge \tau_0 \leq \tau_1 \wedge \tau_1 \leq \tau_0 + 15$

S1 Marcatura: $\mu(P3) = \{\tau_0\}$ $\mu(P4) = \{\tau_2\}$
 $C_1 := C_0 \wedge \tau_2 \leq \tau_0 + 5 \wedge \tau_1 \leq \tau_2$

S2 Marcatura: $\mu(P3) = \{\tau_0\}$ $\mu(P5) = \{\tau_3\}$
 $C_2 := C_0 \wedge \tau_3 \geq \tau_1 + 8 \wedge \tau_3 \leq \tau_0 + 10$

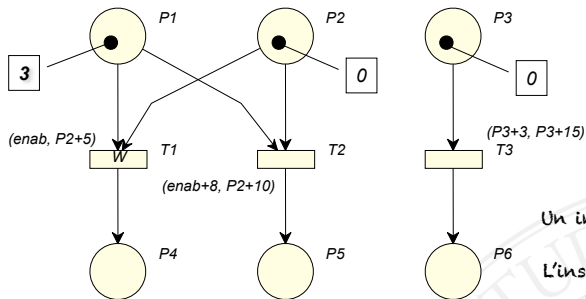
S3 Marcatura: $\mu(P1) = \{\tau_1\}$ $\mu(P2) = \{\tau_0\}$ $\mu(P6) = \{\tau_4\}$
 $C_3 := C_0 \wedge \tau_4 \geq \tau_0 + 3 \wedge \tau_4 \leq \tau_0 + 15 \wedge \tau_4 \geq \tau_1 \wedge (\tau_4 \leq \tau_0 + 10 \vee \tau_1 > \tau_0 + 2)$

Inizializzazione

Identificazione degli enabling

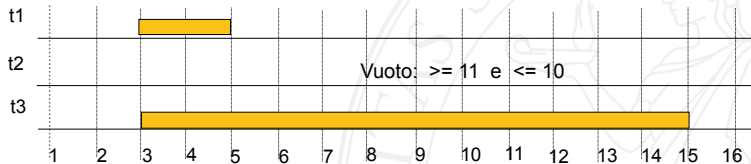
Aggiornamento di marcatura e vincoli

Che cosa è successo?



Un insieme infinito di marcature

L'insieme di transizioni abilitate potrebbe essere diverso...



Aggiornamento del constraint

- Allora lo scatto simbolico di una transizione t crea uno stato simbolico caratterizzato dal vincolo C_n :

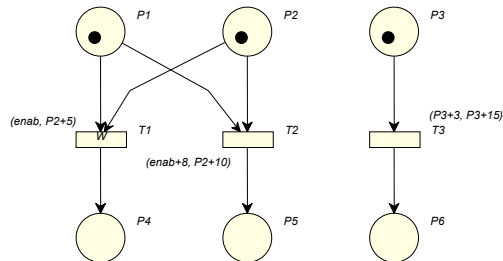
$$C_n = C_p \wedge t_n \geq \max T \wedge t_n \geq \min t \wedge t_n \leq \max t$$

$$\bigcap_{t_s} (t_{\max_s} < t_{\min_s} \vee t_{\max_s} < \max T \vee t_{\max_s} \geq t_n)$$

La soddisfacibilità del vincolo sopra stabilisce
anche la abilitazione della transizione

Rivediamo il calcolo

S0 Marcatura: $\mu(P1) = \{\tau_1\}$ $\mu(P2) = \{\tau_0\}$ $\mu(P3) = \{\tau_0\}$
 $C_0 := 0 \leq \tau_0 \wedge \tau_0 \leq 10 \wedge \tau_0 \leq \tau_1 \wedge \tau_1 \leq \tau_0 + 15$

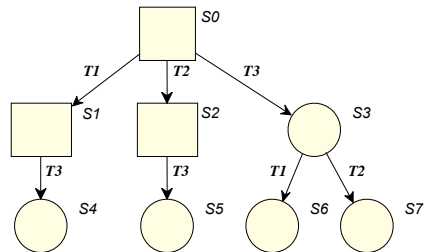
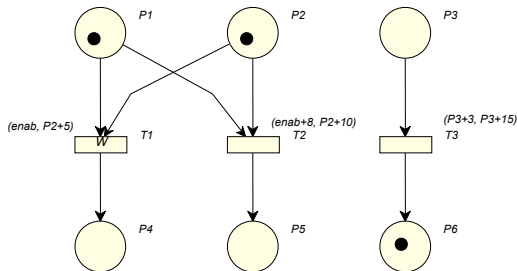


S1 Marcatura: $\mu(P3) = \{\tau_0\}$ $\mu(P4) = \{\tau_2\}$
 $C_1 := C_0 \wedge \tau_1 \leq \tau_2 \wedge \tau_2 \leq \tau_0 + 5 \wedge \tau_1 \leq \tau_2$
 $\wedge (\tau_2 \leq \tau_0 + 10 \vee \dots) \wedge (\tau_2 \leq \tau_0 + 15 \vee \dots)$

S2 Marcatura: $\mu(P3) = \{\tau_0\}$ $\mu(P5) = \{\tau_3\}$
 $C_2 := C_0 \wedge \tau_1 + 8 \leq \tau_3 \wedge \tau_3 \leq \tau_0 + 10 \wedge \tau_1 \leq \tau_3$
 $\wedge (\tau_3 \leq \tau_0 + 15 \vee \dots)$

S3 Marcatura: $\mu(P1) = \{\tau_1\}$ $\mu(P2) = \{\tau_0\}$ $\mu(P6) = \{\tau_4\}$
 $C_3 := C_0 \wedge \tau_4 \geq \tau_0 + 3 \wedge \tau_4 \leq \tau_0 + 15 \wedge \tau_4 \geq \tau_1$
 $\wedge (\tau_4 \leq \tau_0 + 10 \vee \tau_1 + 8 > \tau_0 + 10 \vee \tau_1 > \tau_0 + 10)$

Aggiornamento del constraint



Situazione in $S3$:

$$\mu(P1) = \{\tau_1\} \quad \mu(P2) = \{\tau_0\} \quad \mu(P6) = \{\tau_4\}$$

$$0 \leq \tau_0 \wedge \tau_0 \leq 10 \wedge \tau_0 \leq \tau_1 \wedge \tau_1 \leq \tau_0 + 15 \wedge \tau_4 \leq \tau_0 + 15 \wedge \tau_4 \geq \tau_1 \wedge \tau_4 \geq \tau_0 + 3 \wedge (\tau_1 > \tau_0 + 2 \vee \tau_4 \leq \tau_0 + 10)$$

$T1$ aggiunge $\tau_1 \leq \tau_n \wedge \tau_n \leq \tau_0 + 5 \wedge \tau_n \geq \tau_4 \wedge (\tau_n \leq \tau_0 + 10 \vee \tau_0 + 10 < \tau_1 + 8 \vee \tau_0 + 10 < \tau_4)$

$T2$ aggiunge $\tau_1 + 8 \leq \tau_n \wedge \tau_n \leq \tau_0 + 10 \wedge \tau_n \geq \tau_4$

$T1$ è abilitata se $\tau_4 \leq \tau_0 + 5$

$T2$ è abilitata se $\tau_1 \leq \tau_0 + 2$



abilitata solo $T1$: $\tau_0 = 6, \tau_1 = 9, \tau_4 = 10$

abilitata solo $T2$: $\tau_0 = 6, \tau_1 = 7, \tau_4 = 15$

abilitate entrambe: $\tau_0 = 6, \tau_1 = 7, \tau_4 = 10$

nessuna abilitata (deadlock) : $\tau_0 = 6, \tau_1 = 9, \tau_4 = 17$



Cosa abbiamo?

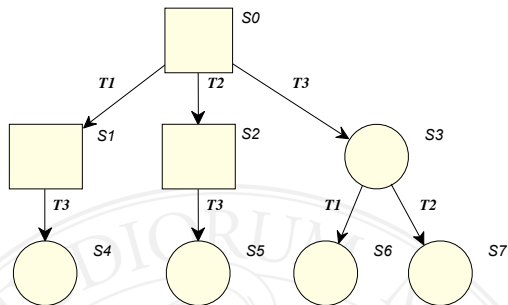
- Non abbiamo una forma normale
 - quindi non possiamo confrontare stati e scoprire se li abbiamo già visitati
 - ALBERO infinito
- Possiamo verificare proprietà entro un limite finito di tempo:
 - bounded invariance
 - bounded liveness

Verso grafo aciclico (DAG)

- Se riusciamo a scordarci la storia di come arriviamo a un nodo è possibile “ritrovare” degli stati.
- Possiamo sperare di arrivare a un grafo ciclico?

Semplificazione dei constraints

- Esprimere il constraint solo in termini della marcatura corrente, rimappando i constraint indiretti



S6

Marking: $\mu(P4) = \{\tau_7\}$ $\mu(P6) = \{\tau_4\}$

$$C_6 := 0 \leq \tau_0 \wedge \tau_0 \leq 10 \wedge \tau_0 \leq \tau_1 \wedge \tau_1 \leq \tau_0 + 15 \wedge \\ \tau_4 \leq \tau_0 + 15 \wedge \tau_1 \leq \tau_4 \wedge \tau_4 \geq \tau_0 + 3 \wedge (\tau_4 \leq \tau_0 + 10 \vee \tau_1 > \tau_0 + 2) \wedge \\ \tau_7 \leq \tau_0 + 5 \wedge \tau_4 \leq \tau_7$$

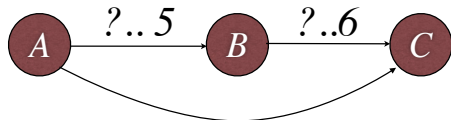


Marking: $\mu(P4) = \{\tau_2\}$ $\mu(P6) = \{\tau_1\}$

$$C_6' := \tau_1 \geq 3 \wedge \tau_1 \leq \tau_2 \wedge \tau_2 \leq \tau_1 + 2 \wedge \tau_2 \leq 15$$

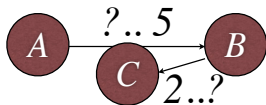
Algoritmo di Floyd

- $B-A \leq 5$ e $C-B \leq 6$



$C-A \leq 11$ e posso eliminare B

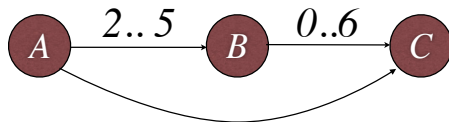
- $B-A \leq 5$ e $C-B \leq -2$ [$B-C \geq 2$]



$C-A \leq 3$ e posso eliminare B

Algoritmo di Floyd

- $A+2 \leq B \leq A+5$
- $B \leq C \leq B+6$



posso eliminare B e mantenere i vincoli?

\leq	A	B	C
A	0	-2	?
B	5	0	0
C	?	6	0

$$\begin{aligned}a-b &\leq -2 \\ b-c &\leq 0\end{aligned}$$

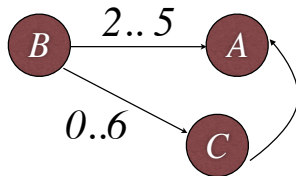
\leq	A	B	C
A	0	-2	-2
B	5	0	0
C	11	6	0

$$m[ij] \leq m[ik] + m[kj]$$



Algoritmo di Floyd

- $B + 2 \leq A \leq B + 5$
- $B \leq C \leq B + 6$



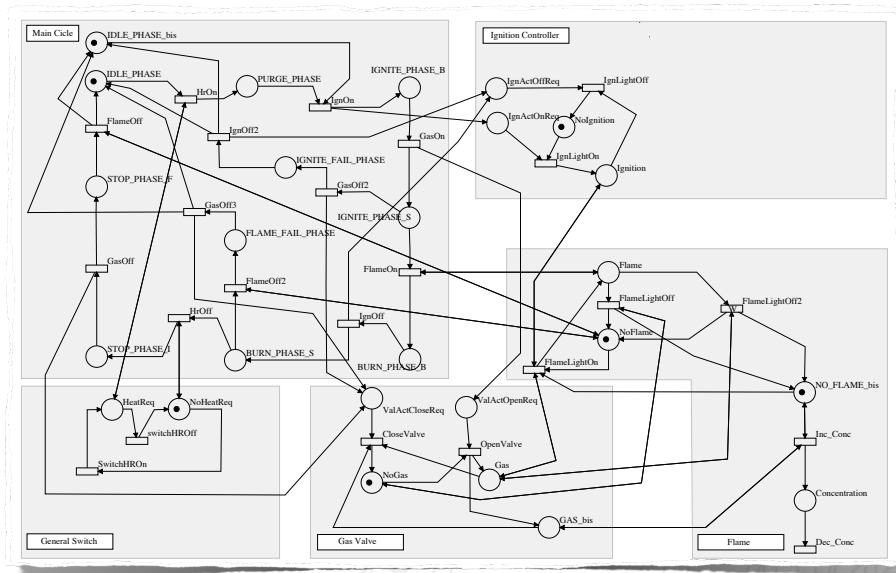
posso eliminare B e mantenere i vincoli?

\leq	A	B	C
A	0	5	?
B	-2	0	0
C	?	6	0

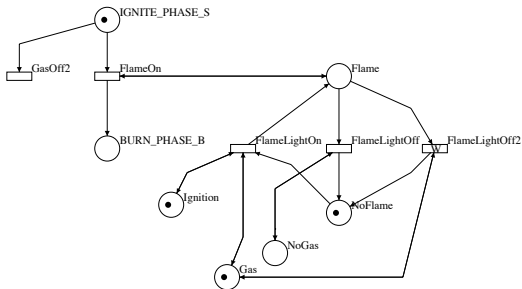
\leq	A	B	C
A	0	5	5
B	-2	0	0
C	4	6	0



The GasBurner example



... o solo una sua parte



Initial marking $IGNITE_PHASE_S\{T_0\}$ $Ignition\{T_0\}$ $Gas\{T_0\}$ $NoFlame\{T_0\}$
 Initial constraint $0 \leq T_0 \leq 10$

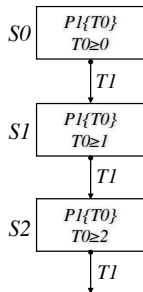
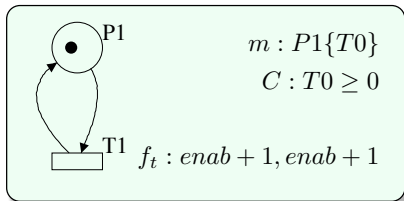
FlameOn	$[IGNITE_PHASE_S + 0.01, \max(\{Flame + 0.1, IGNITE_PHASE_S + 0.01\})]$	FlameLightOff	$[enab, NoGas + 0.1]$
FlameLightOn	$[enab + 0.5, enab + 0.5]$	GasOff2	$[enab + 2, enab + 2]$
FlameLightOff2	$[enab, enab + 100]$ with weak time semantic		

Relazione di inclusione tra stati

- Stato A è **contenuto** nello stato B se e solo se tutte le marcature rappresentate da A sono rappresentate anche da B
 - stesso assegnamento di timestamp
 - C_A implica C_B

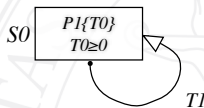


Esempio di inclusione semplice

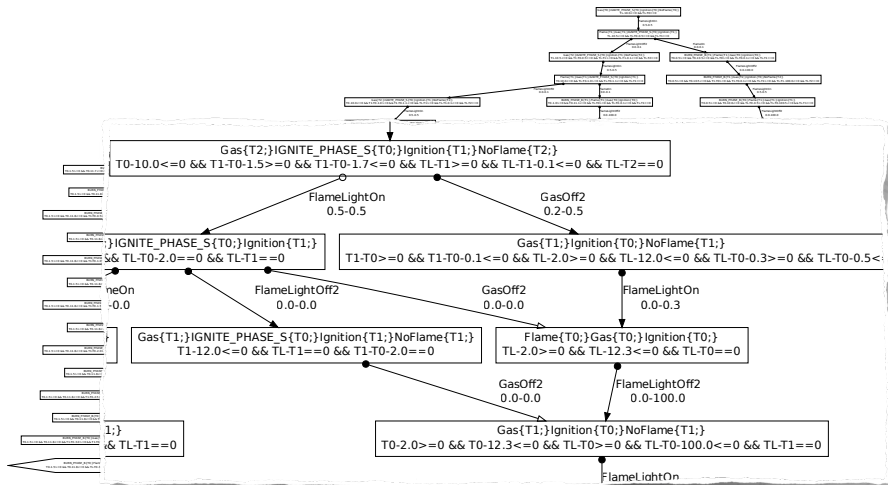


- Senza “inclusione” genererebbe infiniti stati (stessa marcatura ma con diversi vincoli)

- $C1: T0 \geq 1$
- $Cn: T0 \geq n$



Non è abbastanza per il gas burner

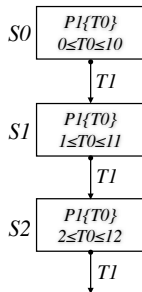
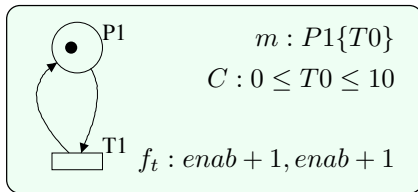


Tempi assoluti vs. Relativi

- Osservazione
 - Se le funzioni temporali non fanno riferimento a tempi assoluti
 - Per essere capace di identificare ciò che accade a partire da una marcatura bastano i constraint relativi tra i timestamp

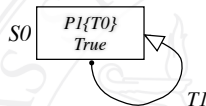


Esempio tempi relativi



- Mantenere i riferimenti ai tempi assoluti genererebbe infiniti stati

- $C1: 1 \leq T0 \leq 11$
- $Cn: n \leq T0 \leq n+10$



UNIVERSITÀ DEGLI STUDI
DI MILANO

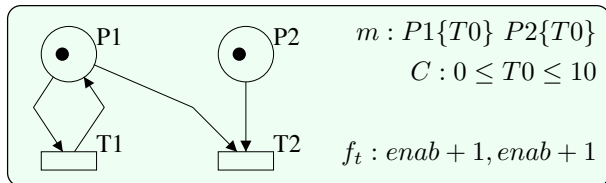
Time Anonymous Timestamp

- Se il timestamp associato a un gettone in una marcatura M non verrà mai usato per stabilire come evolverà la rete a partire da quella marcatura, allora è possibile anonimizzare il tempo di tale gettone

Definition 2 (valid TA-replacement): Given a state S , a timestamp occurrence $T_i : p$ is replaceable with $TA : p$ if and only if for each $S' = \langle M', C' \rangle \in \mathbf{R}(S)$ in which token $T_i : p$ is left (modulo timestamp renaming), for each symbolic enabling (en_s, t) in S' s.t. $en_s(p) = T_i$, $f_{t[\neg\{p\}]}$ is a well-defined erasure and

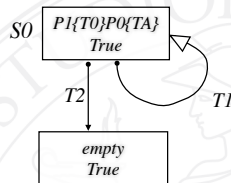
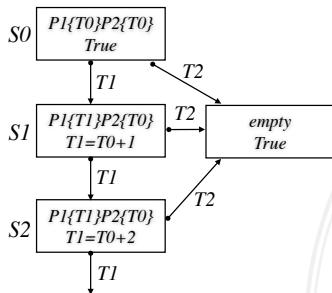
$$\begin{aligned} C' \wedge \max(\{TL, lb_t(en_s)\}) &\leq ub_t(en_s) \Leftrightarrow \\ C' \wedge \max(\{TL, lb_{t[\neg\{p\}]}(en_s)\}) &\leq ub_{t[\neg\{p\}]}(en_s) \end{aligned}$$

Esempio di Time Anonymous



- In P2 si può creare uno “zero relativo”

- $C1: T0+1 \leq T1 \leq T0+11$
- $Cn: T0+n \leq T1 \leq T0+n+10$



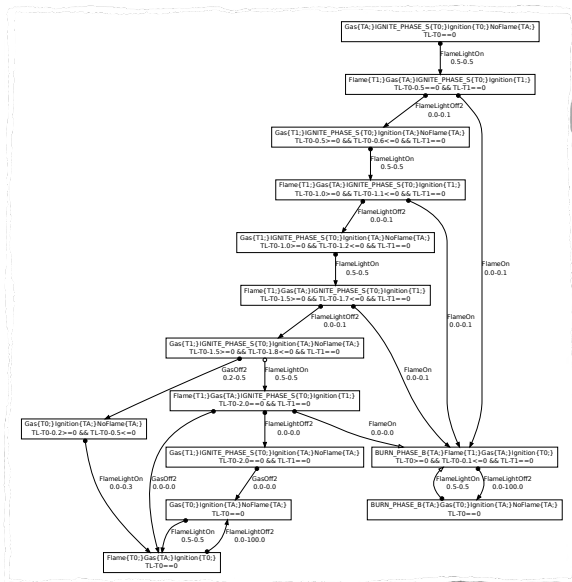
UNIVERSITÀ DEGLI STUDI
DI MILANO

Final Graph

● Inclusions

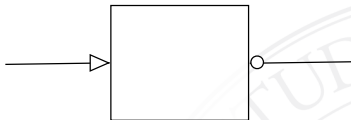
● Relative Times

● Anonymous Timestamp



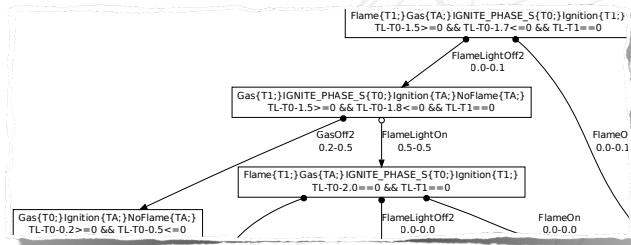
Perdita di informazioni

- inclusione
 - **possibile** presenza di cammini non percorribili



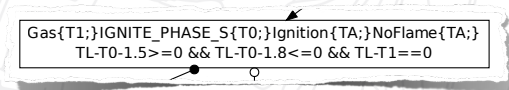
Perdita di informazioni

- inclusione
 - possibile presenza di cammini non percorribili
- relative constraints
 - Perdita di relazioni precise tra stati



Information Loss

- **inclusione**
 - possibile presenza di cammini non percorribili
- **relative constraints**
 - Perdita di relazioni precise tra stati
- **anonymous timestamps**
 - Non sempre possibile verificare raggiungibilità di una marcatura definita da vincoli sui timestamp



A diagram showing a state transition. A horizontal line has a solid black dot on the left and an open circle on the right. An arrow points from the solid dot to the right, passing through a rectangular box with a dashed border. The box contains two lines of text: 'Gas{T1;}|IGNITE_PHASE_S{T0;}|Ignition{TA;}|NoFlame{TA;}' and 'TL-T0-1.5>=0 && TL-T0-1.8<=0 && TL-T1==0'. The background of the slide features a large, faint watermark of the University of Milan seal.

```
Gas{T1;}|IGNITE_PHASE_S{T0;}|Ignition{TA;}|NoFlame{TA;}
TL-T0-1.5>=0 && TL-T0-1.8<=0 && TL-T1==0
```

Copertura temporale?

- Quale era il problema nell'uso della tecnica di copertura?
 - che i gettoni avevano una informazione che li rendeva distinguibili
- Ma i gettoni con tempo TA sono tutti “equivalenti” (anonimizzati) e quindi rappresentabili globalmente da un numero $\omega_{TA} (0 \leq \omega_{TA} < \infty)$