Sítě časovaných automatů

Časované automaty paralelně

Intuice v CCS

$$(\overline{a}.Nil \mid a.Nil) \setminus \{a\}$$

Nechť C je množina hodin a $Chan$ množina kanálů.

Označíme $Act = N \cup \mathbb{R}^{\geq 0}$, kde

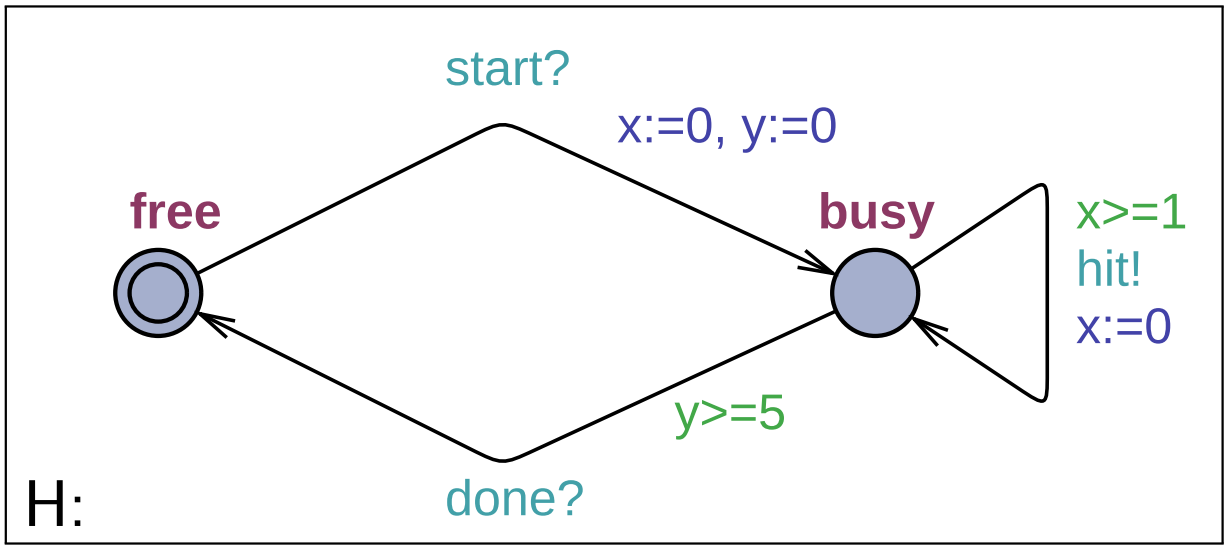
- $N = \{c! \mid c \in Chan\} \cup \{c? \mid c \in Chan\} \cup \{\tau\}$.

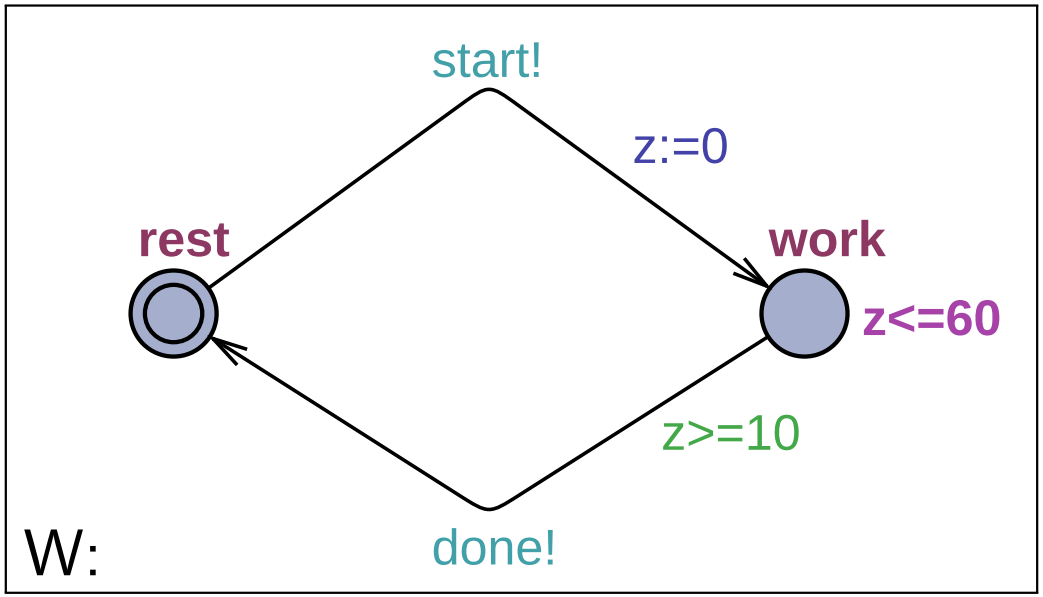
Nechť $A_i = (L_i, \ell_0^i, E_i, I_i)$ je časovaný automat pro $1 \leq i \leq n$.

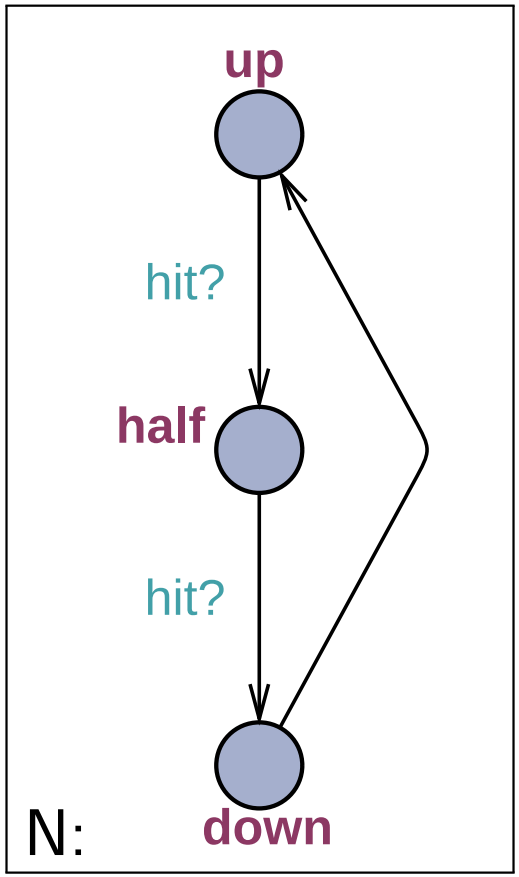
Sítě časovaných automatů (Networks of Timed Automata)

$A = A_1 | A_2 | \cdots | A_n$ nazýváme sítí časovaných automatů.

Příklad: kladivo, dělník, hřebík







TLTS generovaný sítí $A = A_1 | \cdots | A_n$

$T(A) = (Proc, Act, \{\xrightarrow{a} | \ a \in Act\})$, kde

- $Proc = (L_1 \times L_2 \times \cdots \times L_n) \times (C \to \mathbb{R}^{\geq 0})$, tj. stavy jsou tvaru $((\ell_1, \ell_2, \ldots, \ell_n), v)$ kde ℓ_i je lokace v A_i, $v \models I_i(\ell_i)$
- $Act = \{\tau\} \cup \mathbb{R}^{\geq 0}$
- $\longrightarrow$ je definováno následovně:

$((\ell_1, \ldots, \ell_i, \ldots, \ell_n), v) \xrightarrow{\tau} ((\ell_1, \ldots, \ell_i', \ldots, \ell_n), v')$ pokud existuje $(\ell_i \xrightarrow{g,\tau,r} \ell_i') \in E_i$ tž. $v \models g$ a $v' = v[r]$ a $v' \models I_i(\ell_i') \wedge \bigwedge_{k \neq i} I_k(\ell_k)$

$((\ell_1, \ldots, \ell_n), v) \xrightarrow{d} ((\ell_1, \ldots, \ell_n), v + d)$ pro každé $d \in \mathbb{R}^{\geq 0}$ tž. $v \models \bigwedge_k I_k(\ell_k)$ a $v + d \models \bigwedge_k I_k(\ell_k)$

. . . synchronizační krok . . .

$((\ell_1, \ldots, \ell_i, \ldots, \ell_j, \ldots, \ell_n), v) \xrightarrow{\tau} ((\ell_1, \ldots, \ell'_i, \ldots, \ell'_j, \ldots, \ell_n), v')$, pokud $i \neq j$ a existují $(\ell_i \xrightarrow{g_i, a!, r_i} \ell'_i) \in E_i$ a $(\ell_j \xrightarrow{g_j, a?, r_j} \ell'_j) \in E_j$ tž. $v \models g_i \wedge g_j$ and $v' = v[r_i \cup r_j]$ a $v' \models I_i(\ell'_i) \wedge I_j(\ell'_j) \wedge \bigwedge_{k \neq i,j} I_k(\ell_k)$

Automatizované verifikace časovaných automatů

Fakt

Již velmi jednoduché časované automaty generují časovaný přechodový systém s nekonečně (dokonce nespočetně) mnoha dosažitelnými stavy.

Otázka

Je nějaký přístup automatizované verifikace (jako ověřování bisimilarity, model checking nebo analýza dosažitelných stavů) vůbec možný?

Odpověď

Ano, díky využití techniky grafu regionů (region graph).

Klíčová myšlenka: nekonečně mnoho valuací hodin může být rozděleno do konečně mnoha tříd ekvivalence.

Intuitice

Nechť $v, v' : C \to \mathbb{R}^{\geq 0}$ jsou valuace hodin.
Nechť $\sim$ označuje nečasovanou bisimilaritu časovaných přechodových systémů.

Náš cíl

Definovat relaci ekvivalence $\equiv$ nad valuacemi hodin takovou, že

1. $v \equiv v'$ implikuje $(\ell, v) \sim (\ell, v')$ pro každou lokaci ℓ
2. $\equiv$ má jen konečně mnoho tříd ekvivalence.

Pomocné značení

Nechť $d \in \mathbb{R}^{\geq 0}$. Potom

- označíme $\lfloor d \rfloor$ celou část čísla d a
- označíme $frac(d)$ desetinnou část čísla d.

Každé $d \in \mathbb{R}^{\geq 0}$ tak můžeme psát jako $d = \lfloor d \rfloor + frac(d)$.

Například: $\lfloor 2.345 \rfloor = 2$ a $frac(2.345) = 0.345$.

Nechť A je časovaný automat a $x \in C$ jsou hodiny. Definujeme

$$c_x \in \mathbb{N}$$

jako největší konstantu, se kterou jsou hodiny x někdy porovnávány buď v podmínce přechodu nebo v invariantu v automatu A.

Ekvivalence hodin (regionů)

Relace ekvivalence na valuacích hodin

Valuace hodin v a v' jsou ekvivalentní ($v \equiv v'$) právě tehdy, když

1. pro všechna $x \in C$ taková, že $v(x) \leq c_x$ nebo $v'(x) \leq c_x$ máme

$$\lfloor v(x) \rfloor = \lfloor v'(x) \rfloor$$

2. pro všechna $x \in C$ taková, že $v(x) \leq c_x$ máme

$$frac(v(x)) = 0 \quad \text{právě tehdy, když} \quad frac(v'(x)) = 0$$

3. pro všechna $x, y \in C$ taková, že $v(x) \leq c_x$ a $v(y) \leq c_y$ máme

$$frac(v(x)) \leq frac(v(y)) \quad \text{právě, když} \quad frac(v'(x)) \leq frac(v'(y))$$

Regiony

Nechť v je valuace hodin. Třída ekvivalence $\equiv$ reprezentovaná prvkem v se označuje $[v]$ a je definovaná jako $[v] = \{v' \mid v' \equiv v\}$.

Definice regionu

Pro ekvivalenci $\equiv$ se třída $[v]$ reprezentovaná nějakou valuací hodin v nazývá region.

Věta

Pro každou lokaci ℓ a každé dvě valuace v a v' ze stejného regionu ($v \equiv v'$) platí, že

$$(\ell, v) \sim (\ell, v')$$

kde $\sim$ znamená nečasovanou bisimilaritu.

Symbolické stavy a graf regionů

stav (ℓ, v) $\rightsquigarrow$ symbolicky stav(symbolic state) $(\ell, [v])$

Pozn.: $v \equiv v'$ implikuje, že $(\ell, [v]) = (\ell, [v'])$.

Graf regionů (Region Graph)

Graf regionů časovaného automatu $A = (L, \ell_0, E, I)$ nad množinou hodin C a množinou akcí Act je (nečasovaný) ohodnocený přechodový systém $T_r(A) = (S, Act \cup \{\varepsilon\}, \{\stackrel{a}{\Longrightarrow} | \ a \in Act \cup \{\varepsilon\}\})$, kde

- stavy jsou výše uvedené symbolické stavy (tedy S je konečná)
- $(\ell, [v_1]) \stackrel{a}{\Longrightarrow} (\ell', [v_2])$ pro $a \in Act$ právě tehdy, když $(\ell, v_1') \stackrel{a}{\longrightarrow} (\ell', v_2')$ pro nějaké $v_1' \in [v_1]$, $v_2' \in [v_2]$
- $(\ell, [v_1]) \stackrel{\varepsilon}{\Longrightarrow} (\ell, [v_2])$ právě tehdy, když $(\ell, v_1') \stackrel{d}{\longrightarrow} (\ell, v_2')$ pro nějaké $v_1' \in [v_1]$, $v_2' \in [v_2]$ a $d \in \mathbb{R}^{\geq 0}$

Aplikace grafu regionů na dosažitelnost

Píšeme $(\ell, v) \longrightarrow (\ell', v')$, kdykoliv

- $(\ell, v) \xrightarrow{a} (\ell', v')$ pro nějaké návěští a nebo
- $(\ell, v) \xrightarrow{d} (\ell', v')$ pro nějaké $d \in \mathbb{R}^{\geq 0}$.

Problém dosažitelnosti pro časované automaty

Instance (vstup): Automat $A = (L, \ell_0, E, I)$ a stav (ℓ, v).

Otázka: Platí, že $(\ell_0, v_0) \longrightarrow^* (\ell, v)$?

(kde $v_0(x) = 0$ pro všechna $x \in C$)

Redukce dosažitelnosti pro časované automaty na grafy regionů

Dosažitelnost pro časované automaty je rozhodnutelná, protože

$(\ell_0, v_0) \longrightarrow^* (\ell, v)$ v časovaném automatu právě tehdy, když
$(\ell_0, [v_0]) \Longrightarrow^* (\ell, [v])$ v jeho (konečném) grafu regionů.

Aplikace grafu regionů

Výhody

Grafy regionů poskytují přirozenou abstrakci, která umožňuje dokázat rozhodnutelnost např.

- dosažitelnosti
- časované a nečasované bisimulační ekvivalence
- nečasovanou jazykovou ekvivalenci a prázdnost jazyka.

Nevýhody

Grafy regionů mají příliš velké stavové prostory. Exploze počtu stavů (state space explosion) je exponenciální vzhledem k

- počtu hodin
- maximálním konstantám vyskytujícím se v podmínkách.

Zóny a grafy zón

Zóny poskytují efektivnější reprezentaci symbolického stavového prostoru.
Mnoho regionů může být popsáno jednou zónou.

Zone

Zóna (zone) je popsána rozšířenými omezeními hodin $g \in \mathcal{B}^+(C)$.

$$g ::= x \sim n \mid x - y \sim n \mid g_1 \wedge g_2$$

(tedy tzv. diagonální omezení $x - y \sim n$ jsou nyní povolena)

Graf regionů

symbolický stav: $(\ell, [v])$,
kde v je valuace hodin

Graf zón

symbolický stav: $(\ell, [g])$,
kde g je rozšířené omezení hodin

Zóna je obvykle reprezentována (a uložena v paměti) jako
DBM (Difference Bound Matrix).

Logika pro časované automaty v UPPAALu

Nechť ϕ a ψ jsou lokální vlastnosti (ověřitelné lokálně v daném stavu).

Např.: $(\text{H.busy} \wedge \text{W.rest} \wedge \ 20 \leq z \leq 30)$

UPPAAL umí testovat následující formule (podmnožina TCTL)

- $\text{A}\Box\phi$ — stále (invariantly) ϕ
- $\text{E}\langle\rangle\phi$ — je možné (possibly) ϕ
- $\text{A}\langle\rangle\phi$ — vždy nakonec (always eventually) ϕ
- $\text{E}\Box\phi$ — je možné, že pořád (potentially always) ϕ
- $\phi \dashrightarrow \psi$ — ϕ vždy vede k (always leads to) ψ (stejné, jako $\text{A}\Box(\phi \Rightarrow \text{A}\langle\rangle\psi)$)

Vysvětlivky:

- A a E jsou tzv. kvantifikátory cesty (path quantifiers) a
- $\Box$ a $\langle\rangle$ kvantifikují nad stavy po zvolené cestě.