

Modely konkurentných systémov

Formálne metódy tvorby softvéru

Damas Gruska

Katedra aplikovanej informatiky, I20, gruska@fmph.uniba.sk

State Transition Diagrams

State Transition Diagrams

- orientovaný graf,

State Transition Diagrams

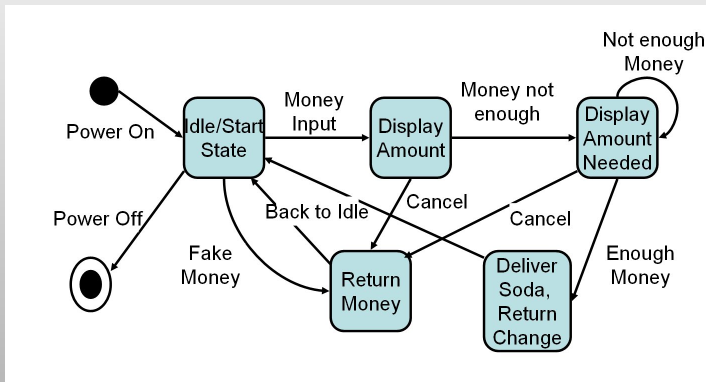
- orientovaný graf,
- vrcholy - stavy,

State Transition Diagrams

- orientovaný graf,
- vrcholy - stavy,
- hrany označujú prechody, môžu byť spojené s akciou alebo podmienkou.

State Transition Diagrams

Automat na predaj sódy



State Transition Diagrams

Nevýhody:

Nevýhody:

- počet stavov a prechodov sa zvyšuje zvyčajne exponencialne s nárastom zložitosti systému.

Nevýhody:

- počet stavov a prechodov sa zvyšuje zvyčajne exponencialne s nárastom zložitosti systému.
- neštrukturované diagramy

Nevýhody:

- počet stavov a prechodov sa zvyšuje zvyčajne exponencialne s nárastom zložitosti systému.
- neštrukturované diagramy

Jedno z riešení:

Nevýhody:

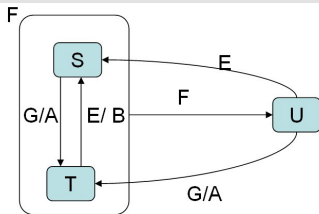
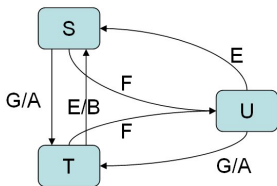
- počet stavov a prechodov sa zvyšuje zvyčajne exponencialne s nárastom zložitosti systému.
- neštrukturované diagramy

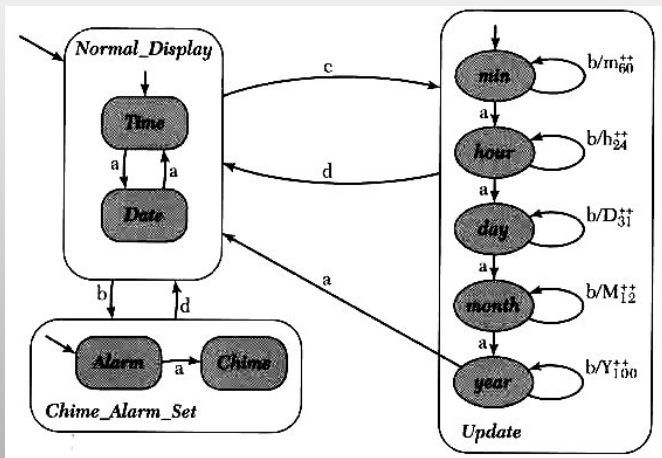
Jedno z riešení:

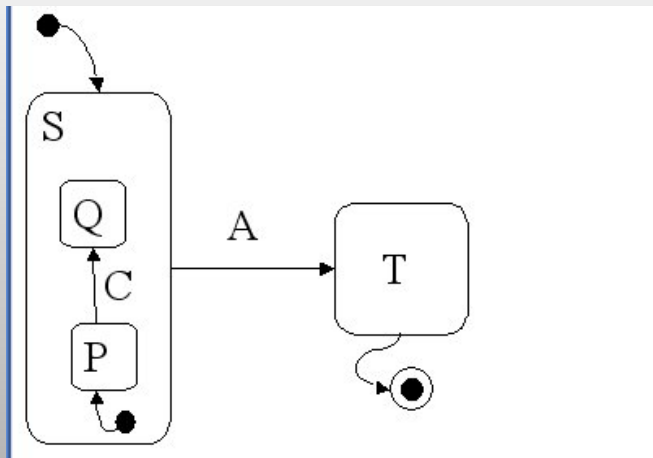
Statecharts, D. Harel, 1986

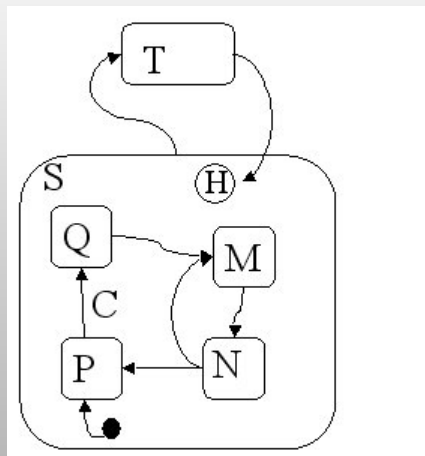
State-Transition Diagram vs Statechart

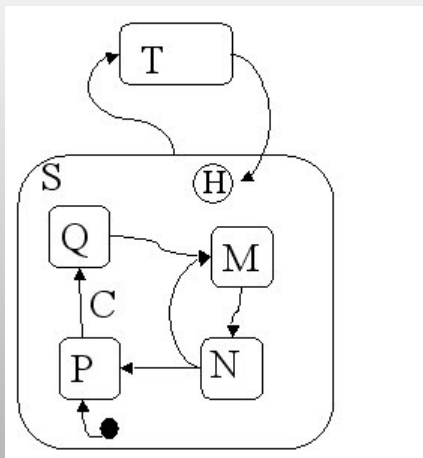
State-Transition Diagram vs Statechart





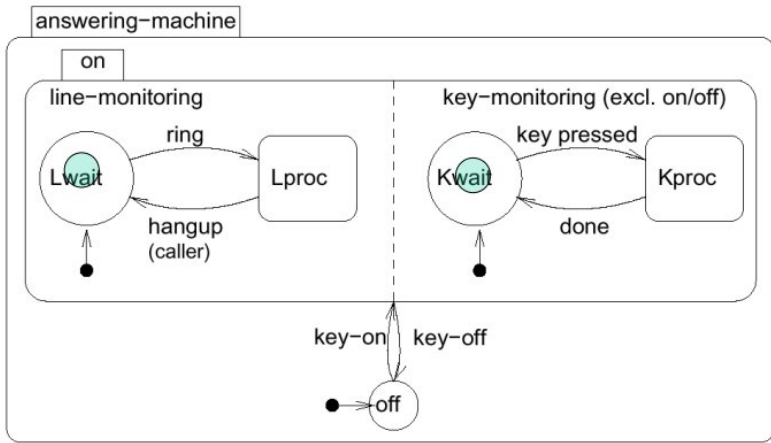




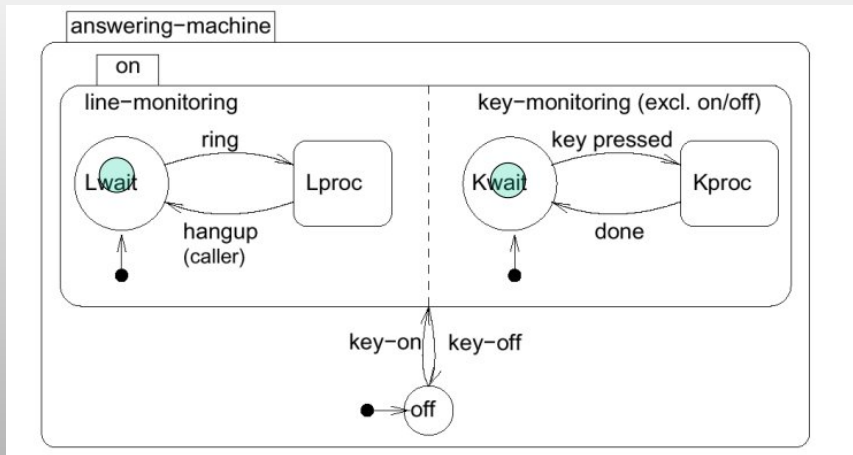


Stav môže mať svoj záznam histórie - miesta opustenia stavu.

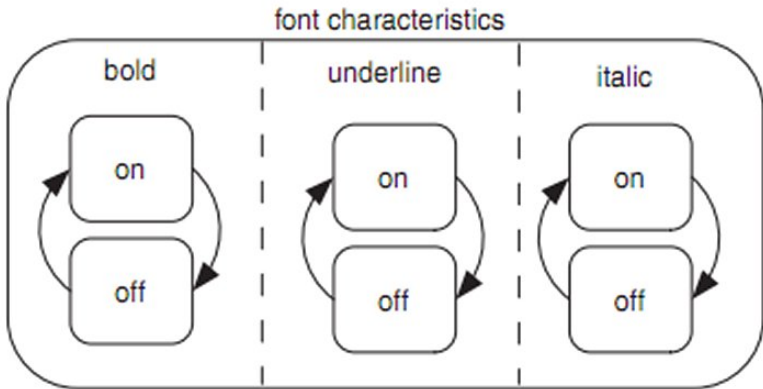
Satecharts - AND superstav



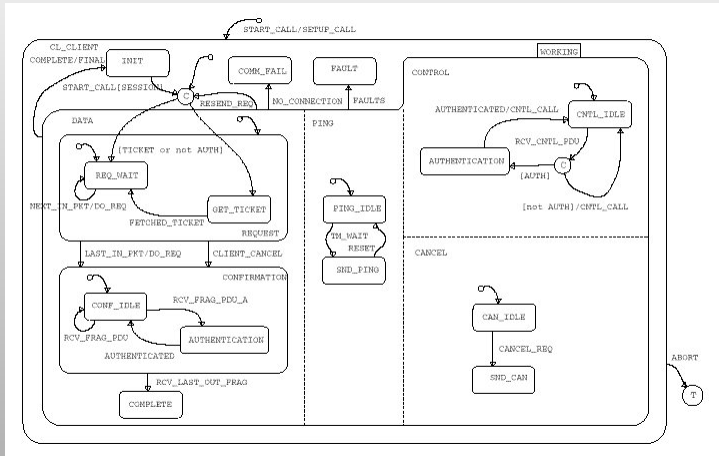
Satecharts - AND superstav



Vstupom do AND superstavu vchádzame do všetkých jeho podstavov.



Remote Procedure Call - protocol CLIENT Machine



Definition

ω -automat A je štvorica $\langle L, L^0, \Sigma, E \rangle$, kde

- L je množina miest,
- L^0 je množina počiatkových miest,
- Σ je konečná množina labelov, akcií,
- $E \subseteq L \times \Sigma \times L$ je množina prechodov - $\langle s, a, s' \rangle$ prechod z miesta s do s' , vykoná sa akcia a .

Definition

ω -automat A je štvorica $\langle L, L^0, \Sigma, E \rangle$, kde

- L je množina miest,
- L^0 je množina počiatkových miest,
- Σ je konečná množina labelov, akcií,
- $E \subseteq L \times \Sigma \times L$ je množina prechodov - $\langle s, a, s' \rangle$ prechod z miesta s do s' , vykoná sa akcia a .

pre $\sigma \in \Sigma^\omega$, $\sigma = a_1.a_2\dots$ je beh r

$$r : s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} \dots$$

kde $(s_i, a_{i+1}, s_{i+1}) \in E$ a $s_0 \in L_0$.

Predpokladajme množinu akceptačných miest $F \subseteq L$.

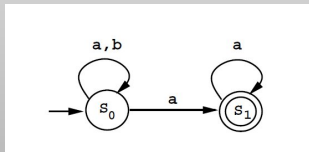
Predpokladajme množinu akceptačných miest $F \subseteq L$.

Büchiho akceptačná podmienka - beh je akceptovaný, ak aspoň jedno akceptačné miesto sa v ňom vyskytuje nekonečne veľa krát.

Predpokladajme množinu akceptačných miest $F \subseteq L$.

Büchiho akceptačná podmienka - beh je akceptovaný, ak aspoň jedno akceptačné miesto sa v ňom vyskytuje nekonečne veľa krát.

automat akceptujúci $(a + b)^* a^\omega$:



jazyk je ω -regulárny ak ho akceptuje ω -automat s Büchiho akceptačnou podmienkou

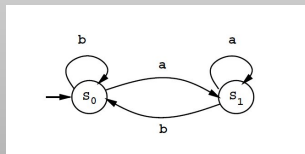
jazyk je ω -regulárny ak ho akceptuje ω -automat s Büchiho akceptačnou podmienkou

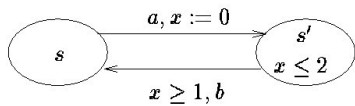
Mullerova akceptačná podmienka - nech $\mathcal{F} \subseteq 2^L$
beh je akceptovaný ak všetky miesta v F sa v ňom vyskytuje nekonečne veľa krát pre nejaké $F \in \mathcal{F}$.

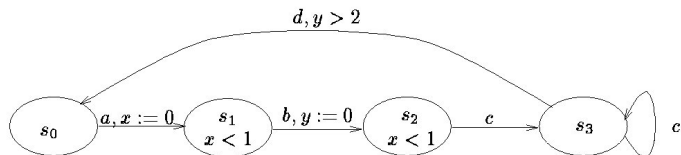
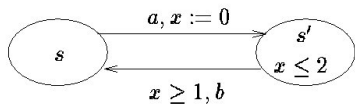
jazyk je ω -regulárny ak ho akceptuje ω -automat s Büchiho akceptačnou podmienkou

Mullerova akceptačná podmienka - nech $\mathcal{F} \subseteq 2^L$
beh je akceptovaný ak všetky miesta v F sa v ňom vyskytujú nekonečne veľa krát pre nejaké $F \in \mathcal{F}$.

deterministický Mullerov automat akceptujúci $(a + b)^* a^\omega$:







Predpokladajme množinu hodín X (clocks)

Předpokladajme množinu hodín X (clocks)

Všetky hodiny "rastú" rovnomerne (čas)

Předpokladajme množinu hodín X (clocks)

Všetky hodiny "rastú" rovnomerne (čas)

Jednotlivé hodiny značíme x, y, \dots

Predpokladajme množinu hodín X (clocks)

Všetky hodiny "rastú" rovnomerne (čas)

Jednotlivé hodiny značíme x, y, \dots

clock valuácia množiny hodín X : zobrazenie $v : X \rightarrow \mathbb{R}$

Predpokladajme množinu hodín X (clocks)

Všetky hodiny "rastú" rovnomerne (čas)

Jednotlivé hodiny značíme x, y, \dots

clock valuácia množiny hodín X : zobrazenie $v : X \rightarrow \mathbb{R}$

Pre clock valuácia v a čas t znamená $v + t$ clock valuácia takú, že
 $(v + t)(x) = v(x) + t$.

Predpokladajme množinu hodín X (clocks)

Všetky hodiny "rastú" rovnomerne (čas)

Jednotlivé hodiny značíme x, y, \dots

clock valuácia množiny hodín X : zobrazenie $v : X \rightarrow \mathbb{R}$

Pre clock valuáciu v a čas t znamená $v + t$ clock valuácia takú, že $(v + t)(x) = v(x) + t$.

Pre clock valuáciu v a podmnožinu hodín $Y \subseteq X$ bude $v[Y := 0]$ označovať clock valuáciu takú, že $v[Y := 0](x) = 0$ pre $x \in Y$ a inak $v[Y := 0](x) = v(x)$.

Predpokladajme množinu hodín X (clocks)

Všetky hodiny "rastú" rovnomerne (čas)

Jednotlivé hodiny značíme x, y, \dots

clock valuácia množiny hodín X : zobrazenie $v : X \rightarrow \mathbb{R}$

Pre clock valuáciu v a čas t znamená $v + t$ clock valuáciu takú, že $(v + t)(x) = v(x) + t$.

Pre clock valuáciu v a podmnožinu hodín $Y \subseteq X$ bude $v[Y := 0]$ označovať clock valuáciu takú, že $v[Y := 0](x) = 0$ pre $x \in Y$ a inak $v[Y := 0](x) = v(x)$.

Daná množina X , uvažujme množinu **clock obmedzení** hodín X , označenú $\Theta(X)$ definovanú gramatikou

$$\theta ::= x < c \mid x \leq c \mid c < x \mid c \leq x \mid \theta_1 \wedge \theta_2$$

kde $x \in X$ a $c \in \mathbb{Q}$

Definition

Časový automat A je šestica $\langle L, L^0, \Sigma, X, I, E \rangle$, kde

Definition

Časový automat A je šestica $\langle L, L^0, \Sigma, X, I, E \rangle$, kde

- L je množina miest,

Definition

Časový automat A je šestica $\langle L, L^0, \Sigma, X, I, E \rangle$, kde

- L je množina miest,
- L^0 je množina počiatočných miest,

Definition

Časový automat A je šestica $\langle L, L^0, \Sigma, X, I, E \rangle$, kde

- L je množina miest,
- L^0 je množina počiatočných miest,
- Σ je konečná množina labelov, akcií,

Definition

Časový automat A je šestica $\langle L, L^0, \Sigma, X, I, E \rangle$, kde

- L je množina miest,
- L^0 je množina počiatkových miest,
- Σ je konečná množina labelov, akcií,
- I zobrazenie, ktorá každému miestu priradí clock obmedzenie z $\Theta(X)$,

Definition

Časový automat A je šestica $\langle L, L^0, \Sigma, X, I, E \rangle$, kde

- L je množina miest,
- L^0 je množina počiatkových miest,
- Σ je konečná množina labelov, akcií,
- I zobrazenie, ktorá každému miestu priradí clock obmedzenie z $\Theta(X)$,
- $E \subseteq L \times \Sigma \times 2^X \times \Theta(X) \times L$ je množina prechodov - $\langle s, a, Y, \theta, s' \rangle$ prechod z miesta s do s' , vykoná sa akcia a , resetujú sa hodiny Y a celé sa to môže vykonať, ak platí θ .

Stav automatu $A - S_A$ je dvojica (s, v) kde s je mesto a v je clock valuácia.

Stav automatu A - S_A je dvojica (s, v) kde s je mesto a v je clock valuácia.

Zmena stavu:

Stav automatu $A - S_A$ je dvojica (s, v) kde s je mesto a v je clock valuácia.

Zmena stavu:

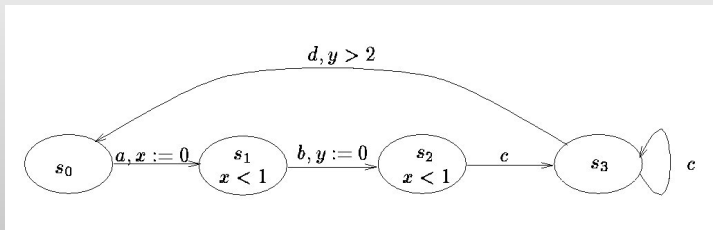
- v dôsledku plynutia času: $(s, v) \xrightarrow{\delta} (s, v + \delta)$, $\delta \geq 0$ ak
 $\forall \delta', 0 \leq \delta' \leq \delta$, $v + \delta'$ vyhovuje $I(s)$,

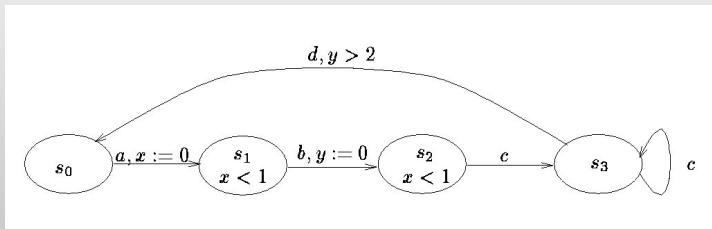
Stav automatu $A - S_A$ je dvojica (s, v) kde s je miesto a v je clock valuácia.

Zmena stavu:

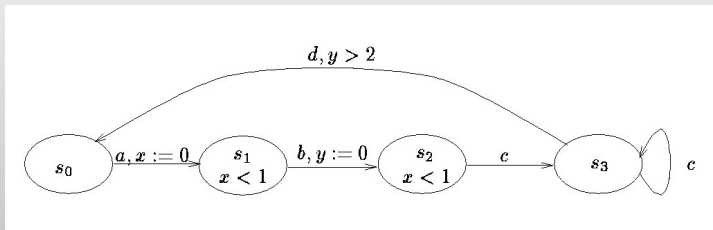
- v dôsledku plynutia času: $(s, v) \xrightarrow{\delta} (s, v + \delta)$, $\delta \geq 0$ ak $\forall \delta', 0 \leq \delta' \leq \delta$, $v + \delta'$ vyhovuje $I(s)$,

- v dôsledku zmeny miesta: $(s, v) \xrightarrow{a} (s', v[Y := 0])$ ak existuje hrana z s do s' s labelom $\langle s, a, Y, \theta, s' \rangle$ a valuácia v spĺňa θ .





$$(s_0, 0, 0) \xrightarrow{1.2} (s_0, 1.2, 1.2) \xrightarrow{a} (s_1, 0, 1.2) \xrightarrow{0.7} (s_1, 0.7, 1.9)$$



$$\begin{aligned} (s_0, 0, 0) &\xrightarrow{1.2} (s_0, 1.2, 1.2) \xrightarrow{a} (s_1, 0, 1.2) \xrightarrow{0.7} (s_1, 0.7, 1.9) \\ (s_1, 0.7, 1.9) &\xrightarrow{b} (s_2, 0.7, 0) \xrightarrow{0.1} (s_2, 0.8, 0.1) \end{aligned}$$

Súčin automatov

Nech $A_1 = \langle L_1, L_1^0, \Sigma_1, X_1, l_1, E_1 \rangle$ a

$A_2 = \langle L_2, L_2^0, \Sigma_2, X_2, l_2, E_2 \rangle$ sú dva časové automaty.

Súčin automatov

Nech $A_1 = \langle L_1, L_1^0, \Sigma_1, X_1, l_1, E_1 \rangle$ a

$A_2 = \langle L_2, L_2^0, \Sigma_2, X_2, l_2, E_2 \rangle$ sú dva časové automaty.

Nech majú disjunktné množinu hodín.

Súčin automatov

Nech $A_1 = \langle L_1, L_1^0, \Sigma_1, X_1, l_1, E_1 \rangle$ a

$A_2 = \langle L_2, L_2^0, \Sigma_2, X_2, l_2, E_2 \rangle$ sú dva časové automaty.

Nech majú disjunktné množinu hodín.

Definujeme časový automat

$A_1 || A_2 = \langle L_1 \times L_2, L_1^0 \times L_2^0, \Sigma_1 \times \Sigma_2, X_1 \cup X_2, l, E \rangle$ kde

$l(s_1, s_2) = l_1(s_1) \wedge l_2(s_2)$ a labely sú definované nasledovne

Súčin automatov

Nech $A_1 = \langle L_1, L_1^0, \Sigma_1, X_1, l_1, E_1 \rangle$ a

$A_2 = \langle L_2, L_2^0, \Sigma_2, X_2, l_2, E_2 \rangle$ sú dva časové automaty.

Nech majú disjunktné množinu hodín.

Definujeme časový automat

$A_1 || A_2 = \langle L_1 \times L_2, L_1^0 \times L_2^0, \Sigma_1 \times \Sigma_2, X_1 \cup X_2, l, E \rangle$ kde

$l(s_1, s_2) = l_1(s_1) \wedge l_2(s_2)$ a labely sú definované nasledovne

1. pre $a \in \Sigma_1 \cap \Sigma_2$ a pre $\langle s_1, a, Y_1, \theta_1, s'_1 \rangle \in E_1$,

$\langle s_2, a, Y_2, \theta_2, s'_2 \rangle \in E_2$, E obsahuje

$\langle (s_1, s_2), a, Y_1 \cup Y_2, \theta_1 \wedge \theta_2, (s'_1, s'_2) \rangle$

Súčin automatov

Nech $A_1 = \langle L_1, L_1^0, \Sigma_1, X_1, l_1, E_1 \rangle$ a

$A_2 = \langle L_2, L_2^0, \Sigma_2, X_2, l_2, E_2 \rangle$ sú dva časové automaty.

Nech majú disjunktné množinu hodín.

Definujeme časový automat

$A_1 || A_2 = \langle L_1 \times L_2, L_1^0 \times L_2^0, \Sigma_1 \times \Sigma_2, X_1 \cup X_2, l, E \rangle$ kde

$l(s_1, s_2) = l_1(s_1) \wedge l_2(s_2)$ a labely sú definované nasledovne

1. pre $a \in \Sigma_1 \cap \Sigma_2$ a pre $\langle s_1, a, Y_1, \theta_1, s'_1 \rangle \in E_1$,

$\langle s_2, a, Y_2, \theta_2, s'_2 \rangle \in E_2$, E obsahuje

$\langle (s_1, s_2), a, Y_1 \cup Y_2, \theta_1 \wedge \theta_2, (s'_1, s'_2) \rangle$

2. pre $a \in \Sigma_1 \setminus \Sigma_2$ a pre $\langle s_1, a, Y_1, \theta_1, s'_1 \rangle \in E_1$, $s_2 \in L_2$, E

obsahuje $\langle (s_1, s_2), a, Y_1, \theta_1, (s'_1, s_2) \rangle$

Súčin automatov

Nech $A_1 = \langle L_1, L_1^0, \Sigma_1, X_1, I_1, E_1 \rangle$ a

$A_2 = \langle L_2, L_2^0, \Sigma_2, X_2, I_2, E_2 \rangle$ sú dva časové automaty.

Nech majú disjunktné množinu hodín.

Definujeme časový automat

$A_1 || A_2 = \langle L_1 \times L_2, L_1^0 \times L_2^0, \Sigma_1 \times \Sigma_2, X_1 \cup X_2, I, E \rangle$ kde

$I(s_1, s_2) = I_1(s_1) \wedge I_2(s_2)$ a labely sú definované nasledovne

1. pre $a \in \Sigma_1 \cap \Sigma_2$ a pre $\langle s_1, a, Y_1, \theta_1, s'_1 \rangle \in E_1$,

$\langle s_2, a, Y_2, \theta_2, s'_2 \rangle \in E_2$, E obsahuje

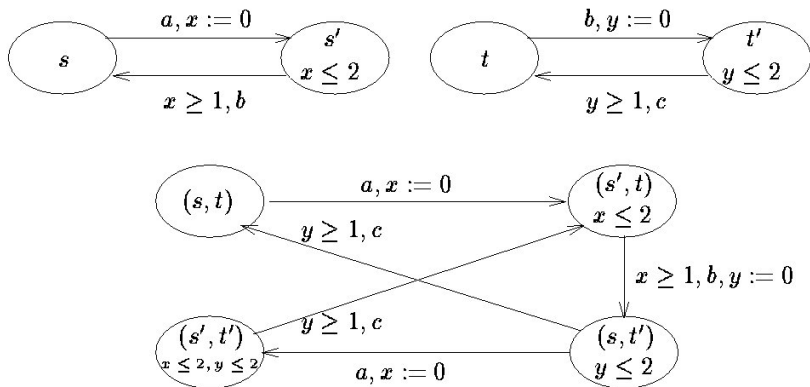
$\langle (s_1, s_2), a, Y_1 \cup Y_2, \theta_1 \wedge \theta_2, (s'_1, s'_2) \rangle$

2. pre $a \in \Sigma_1 \setminus \Sigma_2$ a pre $\langle s_1, a, Y_1, \theta_1, s'_1 \rangle \in E_1$, $s_2 \in L_2$, E

obsahuje $\langle (s_1, s_2), a, Y_1, \theta_1, (s'_1, s_2) \rangle$

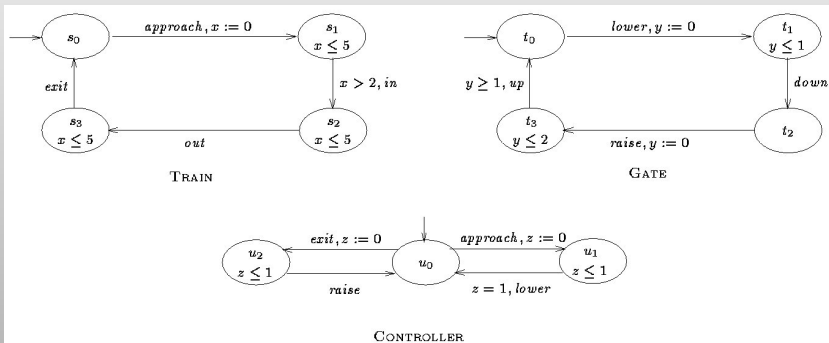
3. pre $a \in \Sigma_2 \setminus \Sigma_1$ a pre $\langle s_2, a, Y_2, \theta_2, s'_2 \rangle \in E_2$, $s_1 \in L_1$, E

obsahuje $\langle (s_1, s_2), a, Y_2, \theta_2, (s_1, s'_2) \rangle$



Vlak - závory - kontroler

Vlak - závory - kontroler



Miesto s časového automatu A je dosiahnuteľné ak nejaký stav q s miestom s je dosiahnuteľný pre A .

Miesto s časového automatu A je dosiahnuteľné ak nejaký stav q s miestom s je dosiahnuteľný pre A .

Vstup pre problém dosiahnuteľnosti je množina $L^F \subseteq L$ cieľových miest. Úlohou je zistiť, či nejaké z týchto miest je dosiahnuteľné.

Časová abstrakcia - abstrahujeme čas

Časová abstrakcia - abstrahujeme čas

predpokladáme, že všetky konštanty v $\Theta(X)$ sú celočíselné.

Časová abstrakcia - abstrahujeme čas

predpokladáme, že všetky konštanty v $\Theta(X)$ sú celočíselné.

nech najväčšia konštanta v obmedzeniach pre hodiny x je c_x .

Časová abstrakcia - abstrahujeme čas

predpokladáme, že všetky konštanty v $\Theta(X)$ sú celočíselné.

nech najväčšia konštanta v obmedzeniach pre hodiny x je c_x .

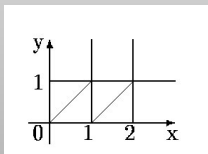
Príklad: nech $c_x = 2$, $c_y = 1$. Odpovedajúci clock región je:

Časová abstrakcia - abstrahujeme čas

predpokladáme, že všetky konštanty v $\Theta(X)$ sú celočíselné.

nech najväčšia konštanta v obmedzeniach pre hodiny x je c_x .

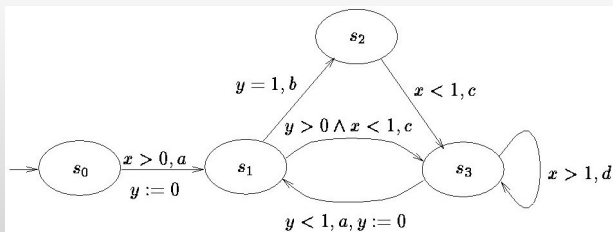
Príklad: nech $c_x = 2$, $c_y = 1$. Odpovedajúci clock región je:

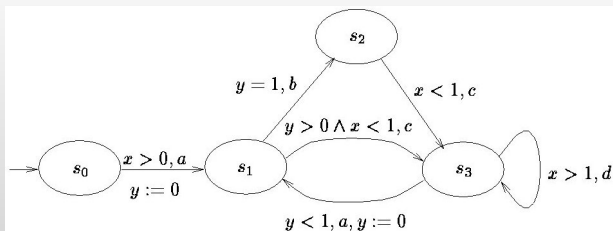


dva stavy (s, v) a (s', v') sú ekvivalentné $(s, v) \cong (s', v')$ ak $s = s'$ a v a v' patria do toho istého regiónu.

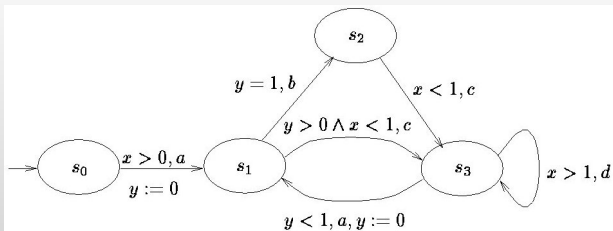
dva stavy (s, v) a (s', v') sú ekvivalentné $(s, v) \cong (s', v')$ ak $s = s'$ a v a v' patria do toho istého regiónu.

abstrahujme čas - bude reprezentovaným regiónom a vznikne
regiónový automat

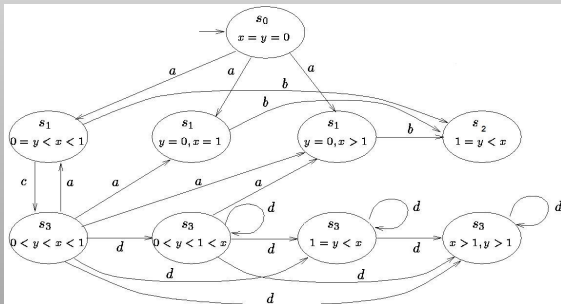




Odpovídající regionový automat.



Odpovedajúci regiónový automat.



Theorem

Nech A je časový automat s n miestami a k hodinami, pričom najväčšia konštanta v obmedzeniach pre hodiny je c . Potom problém dosiahnuteľnosti (A, L^F) je riešiteľný v čase $n \cdot 2^{O(k \log(kc))}$ a je PSPACE úplný.

Theorem

Nech A je časový automat s n miestami a k hodinami, pričom najväčšia konštanta v obmedzeniach pre hodiny je c . Potom problém dosiahnuteľnosti (A, L^F) je riešiteľný v čase $n \cdot 2^{O(k \log(kc))}$ a je PSPACE úplný.

ak by sme povolili obmedzenia pre hodiny napr. v tvare $x = 2y$ problém by sa stal nerozhodnuteľný.

časová postupnosť - monotónna neohraničená postupnosť reálnych čísiel $\tau - \tau_1, \tau_2, \dots$

časová postupnosť - monotónna neohraničená postupnosť reálnych čísiel $\tau - \tau_1, \tau_2, \dots$

postupnosť δ akcií zo $\Sigma - \delta_1, \delta_2, \dots$

časová postupnosť - monotónna neohraničená postupnosť reálnych čísiel $\tau - \tau_1, \tau_2, \dots$

postupnosť δ akcií zo $\Sigma - \delta_1, \delta_2, \dots$

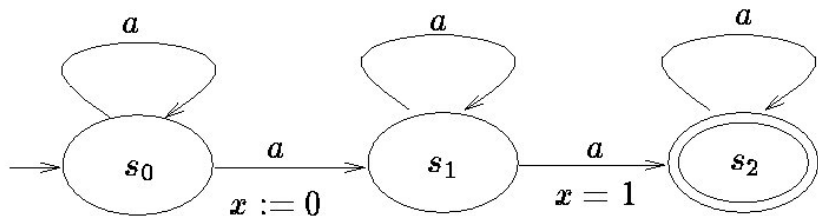
časové slová: $(\delta_1, \tau_1), (\delta_2, \tau_2), \dots$

časová postupnosť - monotónna neohraničená postupnosť reálnych čísiel $\tau - \tau_1, \tau_2, \dots$

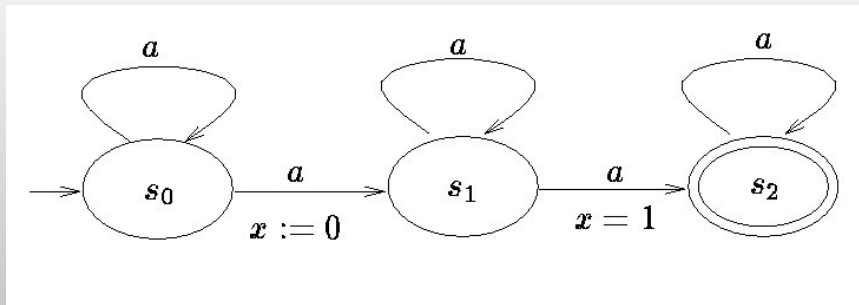
postupnosť δ akcií zo $\Sigma - \delta_1, \delta_2, \dots$

časové slová: $(\delta_1, \tau_1), (\delta_2, \tau_2), \dots$

Automat akceptuje časové slovo ak existuje taký výpočet, keď niektoré z koncových miest je nekonečne veľa krát navštívené (Büchi).

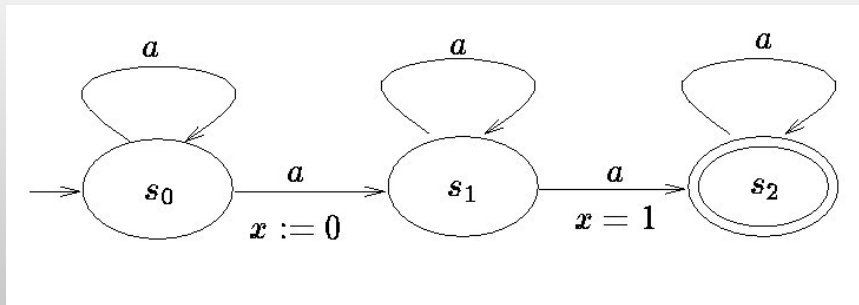


Jazyk akceptovaný tímto automatom:



Jazyk akceptovaný tímto automatom:

$$\{(a^\omega, \tau) \mid \text{existuje } i, j, 1 \leq i < j, \tau_j = \tau_i + 1\}$$



Jazyk akceptovaný týmto automatom:

$$\{(a^\omega, \tau) \mid \text{existuje } i, j, 1 \leq i < j, \tau_j = \tau_i + 1\}$$

Pre komplementárny jazyk neexistuje časový automat.

Theorem

Trieda časových jazykov je uzavretá vzhľadom na zjednotenie a prienik ale nie vzhľadom na komplement.

Deterministické časové automaty:

Deterministické časové automaty:

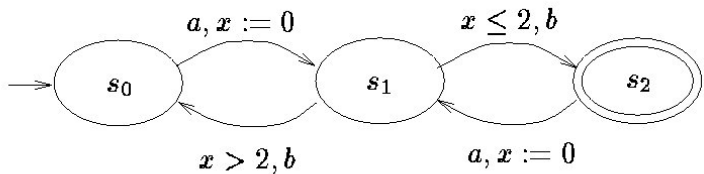
- len jedno počiatkové miesto

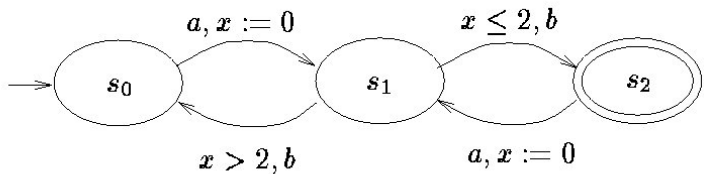
Deterministické časové automaty:

- len jedno počiatkové miesto
- ak sú dva prechody z toho istého miesta označené tou istou akciou, tak prienik clock obmedzení musí byť prázdny.

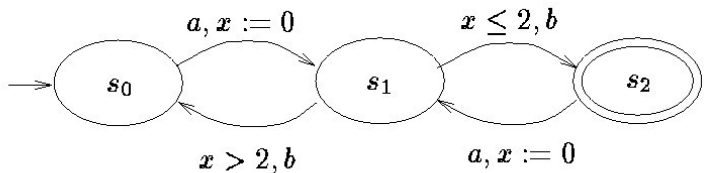
Deterministické časové automaty:

- len jedno počiatkové miesto
- ak sú dva prechody z toho istého miesta označené tou istou akciou, tak prienik clock obmedzení musí byť prázdny.





Jazyk akceptovaný tímto automatom:



Jazyk akceptovaný týmto automatom:

$$\{((ab)^\omega, \tau) \mid \text{pre nekonečne veľa } i, \tau_{2i} - \tau_{2i-1} \leq 2\}$$

Theorem

Trieda deterministických časových jazykov je uzavretá vzhľadom na komplement.