Potřeba zavedení prvků času

- Timeout v Alternating-bit protokolu:
  - V CCS jsme modelovali timeout využitím nedeterminismu.
  - To je dostatečné, abychom ověřili, že protokol je bezpečný.
  - Ale je to příliš abstraktní pro některé otázky
    (jako „Jaký je průměrný čas na doručení zprávy?“).
- Mnoho reálných systémů závisí na časování:
  - výrobní linky, řídící systémy v autech, železniční přejezdy
  - mobilní telefony, chytré hodinky
  - ...

Ohodnocené přechodové systémy s časem

Ohodnocené přechodové systémy s časem (Timed labelled transition system, TLTS)

TLTS je trojice $(Proc, Act, \{\xrightarrow{a} | \ a \in Act\})$ kde

- $Proc$ je množina stavů (nebo procesů),
- $Act = N \cup \mathbb{R}^{\geq 0}$ je množina akcí (skládající se z návěští (labels) a kroků plynutí času – time-elapsing steps), a
- pro každé $a \in Act$, je $\xrightarrow{a} \subseteq \ Proc \times Proc$ binární relace na stavech nazývaná přechodová relace (transition relation).

Píšeme

- $s \xrightarrow{a} s'$ pokud $a \in N$ a $(s, s') \in \xrightarrow{a}$, a
- $s \xrightarrow{d} s'$ pokud $d \in \mathbb{R}^{\geq 0}$ a $(s, s') \in \xrightarrow{d}$.

Přirozené požadavky na TLTS

- Sčítání času:
  pokud $s \xrightarrow{d} s'$ a $0 \leq d' \leq d$ potom $s \xrightarrow{d'} s'' \xrightarrow{d-d'} s'$ pro nějaký stav s'';
- Nulové plynutí času:
  $s \xrightarrow{0} s$ pro všechny stavy s;
- Časový determinismus:
  pokud $s \xrightarrow{d} s'$ a $s \xrightarrow{d} s''$ potom $s' = s''$.

Jak popsat přechodové systémy s časem?

Syntaxe		Sémantika
CCS	$\longrightarrow$	LTS
???	$\longrightarrow$	TLTS

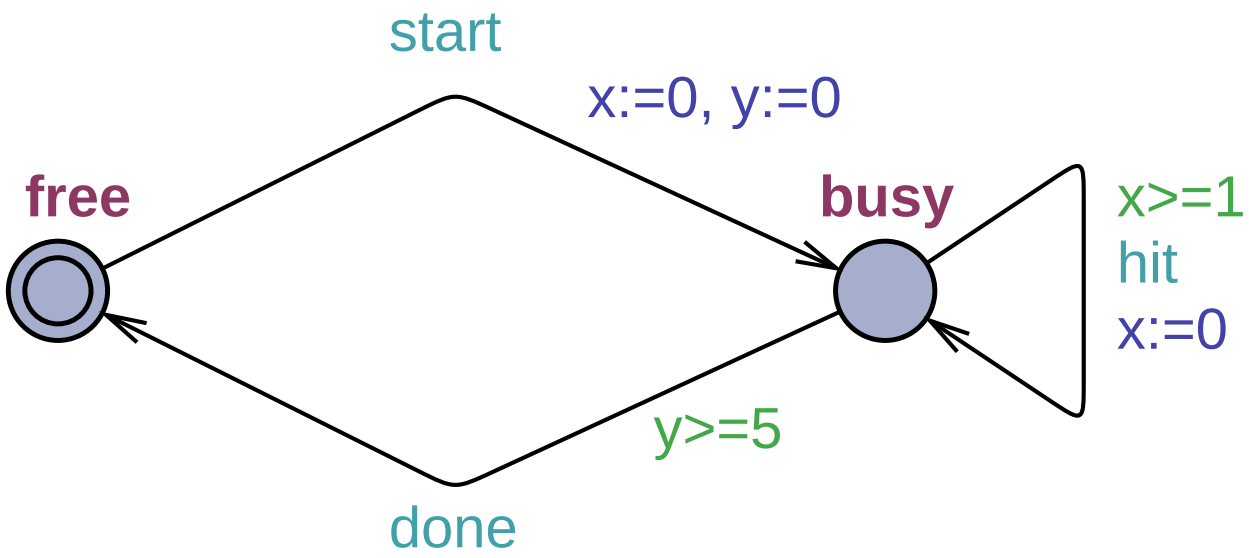
Jak popsat přechodové systémy s časem?

Syntaxe	⟶	Sémantika
CCS	⟶	LTS
???	⟶	TLTS

Možná odpověď

Časované automaty (Timed Automata) [Alur, Dill'90]
tj. konečně stavové automaty doplněné o hodiny s hodnotami v oboru reálných čísel.

Příklad: Kladivo



Některé důležité otázky:

- Jak modelovat systém pracující real-time?
- Jaké časové podmínky (guards) bychom měli povolit?
- ....

Definice časovaných automatů: omezení

Nechť $C = \{x, y, \ldots\}$ je konečná množina hodin.

$\mathcal{B}(C)$ ... množina časových omezení nad C

$\mathcal{B}(C)$ je definována následující abstraktní syntaxí

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

kde $x, y \in C$ jsou hodiny, $n \in \mathbb{N}$ a $\sim \in \{\leq, <, =, >, \geq\}$.

Příklad: $x \leq 3 \ \wedge \ y > 0$

Ohodnocení hodin

Ohodnocení hodin (Clock valuation)

Ohodnocení hodin v je funkce $v : C \rightarrow \mathbb{R}^{\geq 0}$.

Ohodnocení hodin

Ohodnocení hodin (Clock valuation)

Ohodnocení hodin v je funkce $v : C \to \mathbb{R}^{\geq 0}$.

Nechť v je ohodnocení hodin. Potom

- $v + d$ je ohodnocení hodin pro každé $d \in \mathbb{R}^{\geq 0}$ a je definováno jako

$$(v + d)(x) = v(x) + d \text{ pro všechna } x \in C$$

- $v[R]$ je ohodnocení hodiny pro každé $R \subseteq C$ a je definováno jako

$$v[R](x) \begin{cases} 0 & \text{když } x \in R \\ v(x) & \text{jinak.} \end{cases}$$

Vyhodnocení časových omezení

Vyhodnocení časových omezení ($v \models g$)

$v \models x < n$	právě, když $v(x) < n$
$v \models x \leq n$	právě, když $v(x) \leq n$
$v \models x = n$	právě, když $v(x) = n$
$\vdots$	
$v \models g_1 \wedge g_2$	právě, když $v \models g_1$ and $v \models g_2$

Syntaxe časovaných automatů

Definice

Časovaný automat (timed automaton, TA) nad množinou hodin C a množinou návěští (labels) N je čtveřice

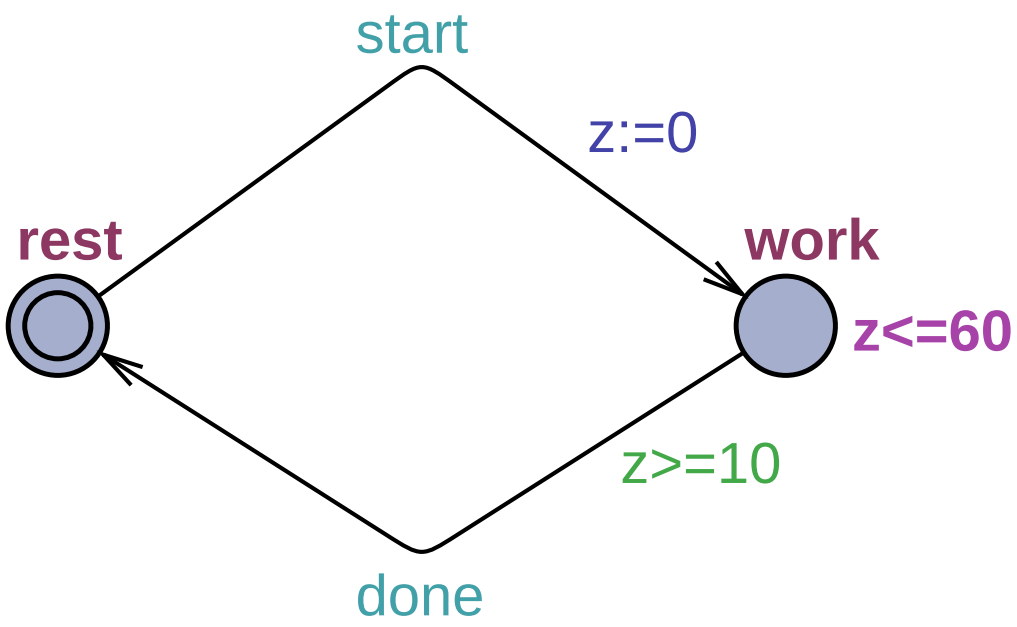
$$(L, \ell_0, E, I)$$

kde

- L je konečná množina lokací (locations)
- $\ell_0 \in L$ je počáteční lokace (initial location)
- $E \subseteq L \times \mathcal{B}(C) \times N \times 2^C \times L$ je množina hran (edges)
- $I : L \to \mathcal{B}(C)$ přiřazuje invarianty (invariants) lokacím.

Obvykle píšeme $\ell \xrightarrow{g,a,r} \ell'$ kdykoliv $(\ell, g, a, r, \ell') \in E$.

Příklad: Dělník



Co to znamená?

Sémantika časovaných automatů

Nechť $A = (L, \ell_0, E, I)$ je časovaný automat.

TLTS generovaný automatem A

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

- $Proc = L \times (C \to \mathbb{R}^{\geq 0})$, tj. stavy jsou tvaru (ℓ, v), kde ℓ je lokace a v valuace hodin taková, že $v \models I(\ell)$
- $Act = N \cup \mathbb{R}^{\geq 0}$
- $\longrightarrow$ je definována následovně:

$(\ell, v) \xrightarrow{a} (\ell', v')$, pokud existuje $(\ell \xrightarrow{g,a,r} \ell') \in E$ tž. $v \models g$, $v' = v[r]$, $v' \models I(\ell')$

$(\ell, v) \xrightarrow{d} (\ell, v + d)$ když $v + d' \models I(\ell)$ pro každé $d' \in [0, d]$.

Časovaná bisimilarita

Nechť A_1 a A_2 jsou časované automaty.

Časovaná bisimilarita

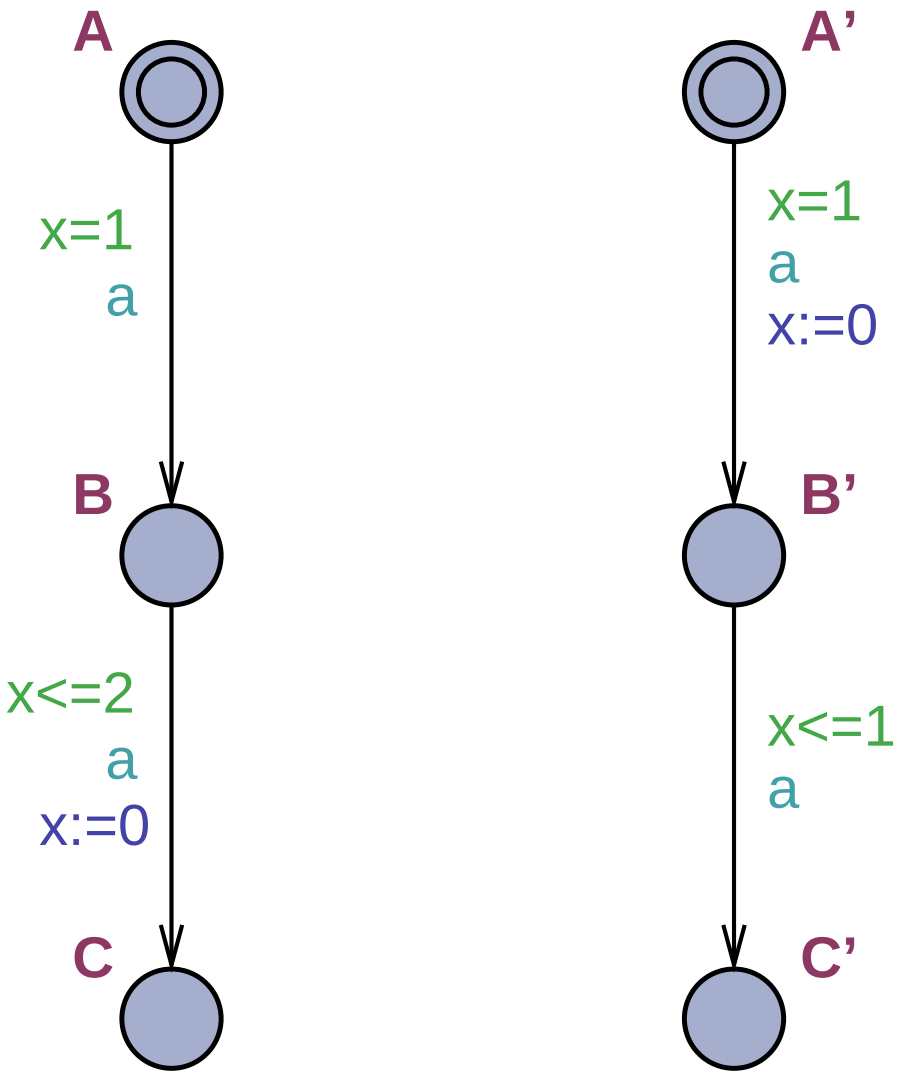
Řekneme, že A_1 a A_2 jsou časově bisimulačně ekvivalentní (timed bisimilar) právě tehdy, když přechodové systémy $T(A_1)$ a $T(A_2)$ generované automaty A_1 a A_2 jsou silně bisimulačně ekvivalentní.

Poznámka: oba typy přechodů

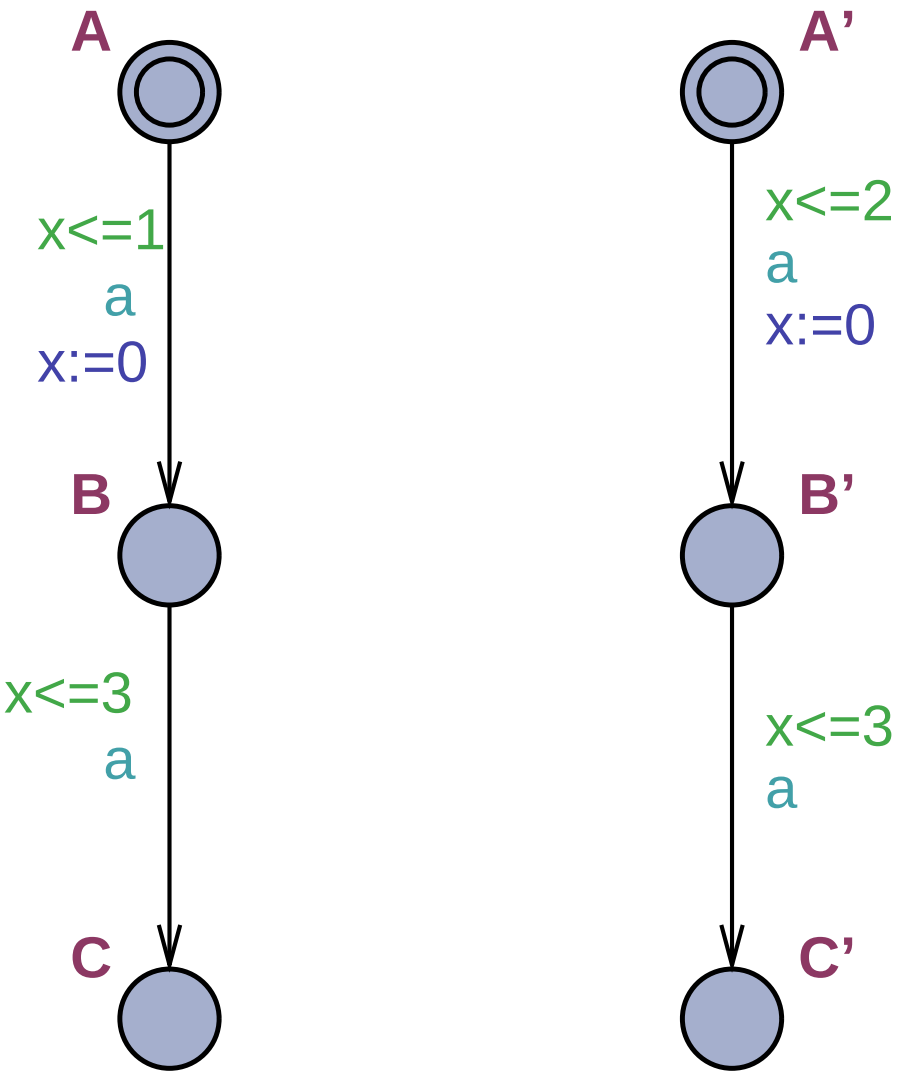
- $\xrightarrow{a}$ pro $a \in N$ a
- $\xrightarrow{d}$ pro $d \in \mathbb{R}^{\geq 0}$

jsou považovány za normální (viditelné) přechody.

Příklad časově bisimulačně ekvivalentních automatů



Příklad časově bisimulačně neekvivalentních automatů



Nečasovaná bisimulační ekvivalence

Nechť A_1 a A_2 jsou časované automaty. Uvažujme ε jako novou akci, která se v automatech A_1 a A_2 nevyskyje.

Nečasovaná bisimilarita (Untimed Bisimilarity)

Řekneme, že A_1 a A_2 jsou nečasově bisimulačně ekvivalentní (untimed bisimilar) právě tehdy, když přechodové systémy $T(A_1)$ and $T(A_2)$ generované automaty A_1 a A_2, kde každý přechod tvaru $\xrightarrow{d}$ pro $d \in \mathbb{R}^{\geq 0}$ je nahrazen přechodem $\xrightarrow{\varepsilon}$, jsou silně bisimulačně ekvivalentní.

Pozn.:

- S přechody $\xrightarrow{a}$ pro $a \in N$ zacházíme jako s viditelnými přechody,
- zatímco $\xrightarrow{d}$ pro $d \in \mathbb{R}^{\geq 0}$ jsou nahrazeny jednou viditelnou akcí $\xrightarrow{\varepsilon}$.

Nečasovaná bisimulační ekvivalence

Nechť A_1 a A_2 jsou časované automaty. Uvažujme ε jako novou akci, která se v automatech A_1 a A_2 nevyskyje.

Nečasovaná bisimilarita (Untimed Bisimilarity)

Řekneme, že A_1 a A_2 jsou nečasově bisimulačně ekvivalentní (untimed bisimilar) právě tehdy, když přechodové systémy $T(A_1)$ and $T(A_2)$ generované automaty A_1 a A_2, kde každý přechod tvaru $\xrightarrow{d}$ pro $d \in \mathbb{R}^{\geq 0}$ je nahrazen přechodem $\xrightarrow{\varepsilon}$, jsou silně bisimulačně ekvivalentní.

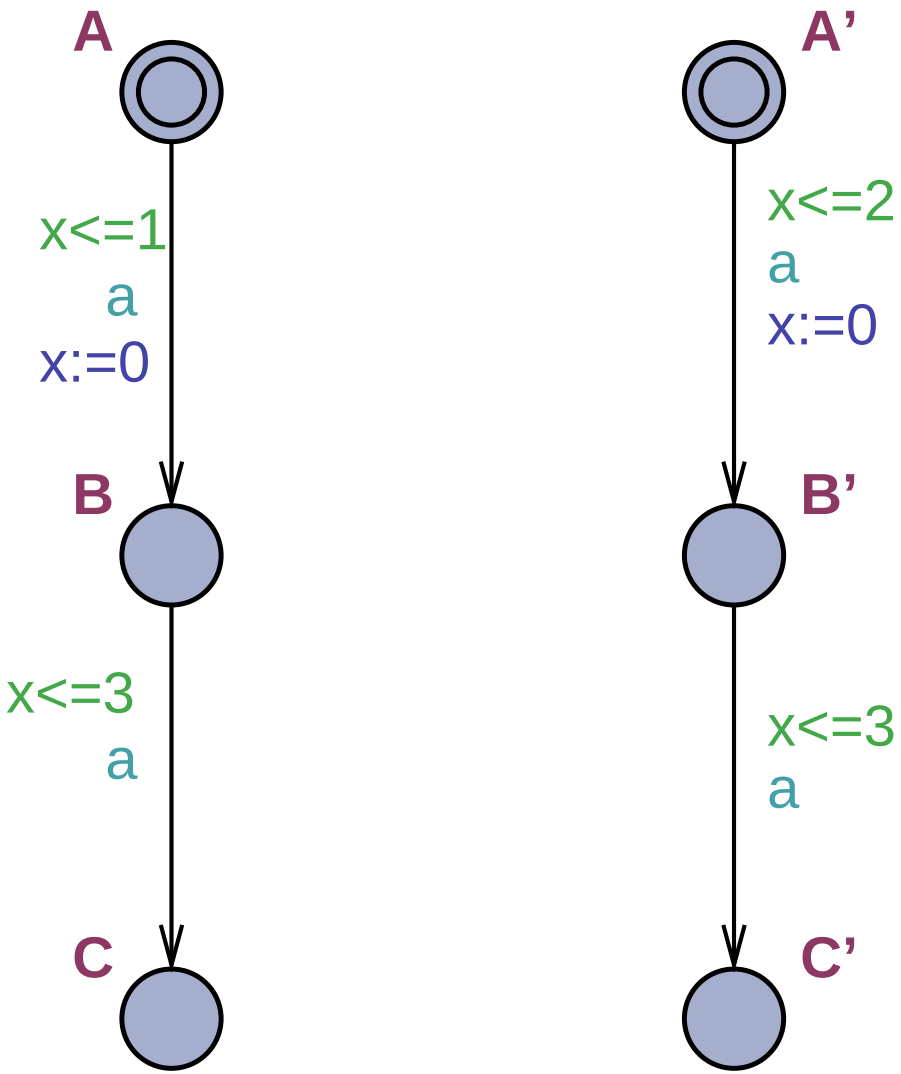
Pozn.:

- S přechody $\xrightarrow{a}$ pro $a \in N$ zacházíme jako s viditelnými přechody,
- zatímco $\xrightarrow{d}$ pro $d \in \mathbb{R}^{\geq 0}$ jsou nahrazeny jednou viditelnou akcí $\xrightarrow{\varepsilon}$.

Závěr

Každé dva časově bisimulačně ekvivalentní automaty jsou také nečasově bisimulačně ekvivalentní.

Automaty časově neekvivalentní a nečasově ekvivalentní



Rozhodnutelnost časované a nečasované bisimilarity

Věta [Cerans'92]

Časovaná bisimilarita pro časované automaty je v EXPTIME (rozhodnutelná deterministickým algoritmem v exponenciálním čase).

Věta [Larsen, Wang'93]

Nečasovaná bisimilarita pro časované automaty je v EXPTIME.

Časované stopy

Nechť $A = (L, \ell_0, E, I)$ je časovaný automat nad množinou hodin C a množinou návěští N.

Časované stopy (Timed Traces)

Sekvence $(t_1, a_1)(t_2, a_2)(t_3, a_3)\ldots$, kde $t_i \in \mathbb{R}^{\geq 0}$ a $a_i \in N$ se nazývá časovaná stopa automatu A (timed trace of A) právě tehdy, když existuje sekvence přechodů

$$(\ell_0, v_0) \xrightarrow{d_1} . \xrightarrow{a_1} . \xrightarrow{d_2} . \xrightarrow{a_2} . \xrightarrow{d_3} . \xrightarrow{a_3} \ldots$$

v A taková, že $v_0(x) = 0$ pro všechna $x \in C$ a

$$t_i = t_{i-1} + d_i \qquad \text{kde } t_0 = 0.$$

Intuice: t_i je absolutní čas (časové razítko - time-stamp), kdy se a_i stala od začátku běhu automatu A.

Časovaná and nečasovaná jazyková ekvivalence

Množinu všech časovaných stop automatu A označíme $L(A)$ a nazýváme časovaný jazyk automatu A (timed language of A).

Věta [Alur, Courcoubetis, Dill, Henzinger'94]

Časovaná jazyková ekvivalence (problém, jestli $L(A_1) = L(A_2)$ pro dané automaty A_1 a A_2) je nerozhodnutelný.

Časovaná and nečasovaná jazyková ekvivalence

Množinu všech časovaných stop automatu A označíme $L(A)$ a nazýváme časovaný jazyk automatu A (timed language of A).

Věta [Alur, Courcoubetis, Dill, Henzinger'94]

Časovaná jazyková ekvivalence (problém, jestli $L(A_1) = L(A_2)$ pro dané automaty A_1 a A_2) je nerozhodnutelný.

Řekneme, že $a_1 a_2 a_3 \ldots$ je nečasovaná stopa automatu A (untimed trace of A) právě tehdy, když existují $t_1, t_2, t_3, \ldots \in \mathbb{R}^{\geq 0}$ takové, že $(t_1, a_1)(t_2, a_2)(t_3, a_3)\ldots$ je časovaná stopa automatu A.

Theorem [Alur, Dill'94]

Nečasovaná jazyková ekvivalence pro časované automaty je rozhodnutelná.