Time Divergence, Timelock, and Zenoness

Lecture #14 of Advanced Model Checking

Joost-Pieter Katoen

Lehrstuhl 2: Software Modeling & Verification

E-mail: `katoen@cs.rwth-aachen.de`

June 24, 2009

Timed automata

- Timed automaton = finite-state automaton with clock variables
- Clocks take non-negative real values, i.e., in $\mathbb{R}_{\geqslant 0}$
- Clocks increase implicitly, i.e., clock updates are not allowed
- All clocks increase at the same pace, i.e., with rate one
- Clocks may only be inspected and reset to zero
- Boolean conditions on clocks are used as:
  - guards of edges: when is an edge enabled?
  - invariants of locations: how long is it allowed to stay?

Clock constraints

- A *clock constraint* over set C of clocks is formed according to:

$$g ::= \; x < c \;\Big|\; x \leqslant c \;\Big|\; x > c \;\Big|\; x \geqslant c \;\Big|\; g \wedge g \quad \text{where } c \in \mathbb{N} \text{ and } x \in C$$

- Let *CC*(C) denote the set of clock constraints over C
- Clock constraints without any conjunctions are *atomic*
  - let *ACC*(C) denote the set of atomic clock constraints over C

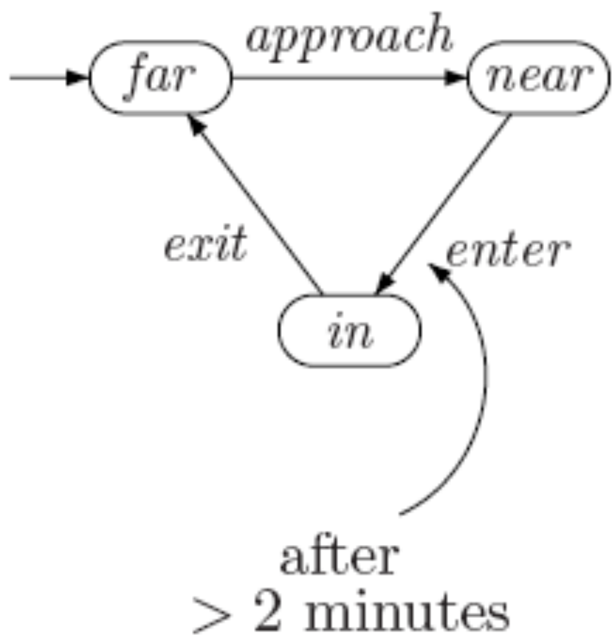
clock difference constraints such as $x - y < c$ can be added at expense of slightly more involved theory

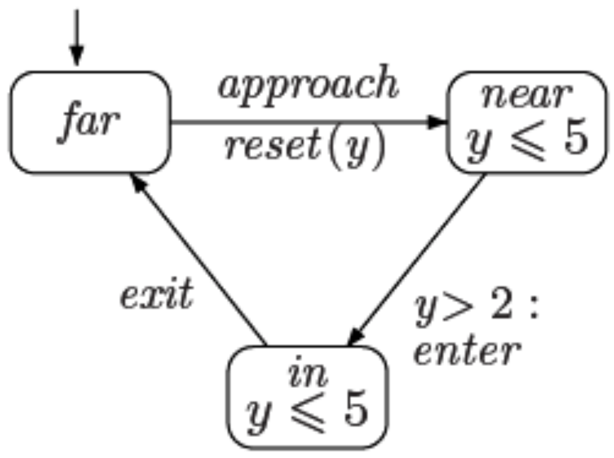
Timed automaton

A *timed automaton* *TA* $= \big(Loc, Act, C, \hookrightarrow, Loc_0, Inv, AP, L\big)$ where:

- *Loc* is a finite set of locations
- $Loc_0 \subseteq Loc$ is a set of initial locations
- C is a finite set of clocks
- $\hookrightarrow \subseteq Loc \times CC(C) \times Act \times 2^C \times Loc$ is a transition relation
- $Inv : Loc \to CC(C)$ is an invariant-assignment function, and
- $L : Loc \to 2^{AP}$ is a labeling function

Timed automata model of train





train is now also assumed to leave crossing within five time units

Clock valuations

- A *clock valuation* η for set C of clocks is a function $\eta : C \longrightarrow \mathbb{R}_{\geqslant 0}$
  - assigning to each clock $x \in C$ its current value $\eta(x)$
- Clock valuation $\eta{+}d$ for $d \in \mathbb{R}_{\geqslant 0}$ is defined by:
  - $(\eta{+}d)(x) = \eta(x) + d$ for all clocks $x \in C$
- Clock valuation reset x in η for clock x is defined by:

$$(\text{reset } x \text{ in } \eta)(y) = \begin{cases} \eta(y) & \text{if } y \neq x \\ 0 & \text{if } y = x \end{cases}$$

  - reset x in (reset y in η) is abbreviated by reset $\{ x, y \}$ in η

Timed automaton semantics

For timed automaton $\mathit{TA} = \big(\mathit{Loc}, \mathit{Act}, C, \hookrightarrow, \mathit{Loc}_0, \mathit{Inv}, \mathit{AP}, L\big)$:

Transition system $\mathit{TS}(\mathit{TA}) = (S, \mathit{Act}', \rightarrow, I, \mathit{AP}', L')$ where:

- $S = \mathit{Loc} \times \mathit{Eval}(C)$, so states are of the form $s = \langle \ell, \eta \rangle$
- $\mathit{Act}' = \mathit{Act} \cup \mathbb{R}_{\geqslant 0}$, (discrete) actions and time-passage actions
- $I = \{ \langle \ell_0, \eta_0 \rangle \mid \ell_0 \in \mathit{Loc}_0 \ \wedge \ \eta_0(x) = 0$ for all $x \in C \}$
- $\mathit{AP}' = \mathit{AP} \cup \mathit{ACC}(C)$
- $L'(\langle \ell, \eta \rangle) = L(\ell) \cup \{ g \in \mathit{ACC}(C) \mid \eta \models g \}$
- $\hookrightarrow$ is defined on the next slide

Timed automaton semantics

The transition relation $\rightarrow$ is defined by the following two rules:

- Discrete transition: $\langle \ell, \eta \rangle \xrightarrow{\alpha} \langle \ell', \eta' \rangle$ if all following conditions hold:
  - there is a transition labeled $(g : \alpha, D)$ from location ℓ to ℓ' such that:
  - g is satisfied by η, i.e., $\eta \models g$
  - $\eta' = \eta$ with all clocks in D reset to 0, i.e., $\eta' =$ reset D in η
  - η' fulfills the invariant of location ℓ', i.e., $\eta' \models \mathit{Inv}(\ell')$

- Delay transition: $\langle \ell, \eta \rangle \xrightarrow{d} \langle \ell, \eta{+}d \rangle$ for $d \in \mathbb{R}_{\geqslant 0}$ if $\eta{+}d \models \mathit{Inv}(\ell)$

Example

Timed paths

Delays may be realized in *TS*(*TA*) in uncountably many ways, e.g.:

$\langle \mathit{off}, 0\rangle \quad \langle \mathit{off}, 1\rangle \quad \langle on, 0\rangle \quad \langle on, 2\rangle \quad \langle \mathit{off}, 2\rangle \quad \ldots$

$\langle \mathit{off}, 0\rangle \quad \langle \mathit{off}, 0.5\rangle \quad \langle \mathit{off}, 1\rangle \quad \langle on, 0\rangle \quad \langle on, 1\rangle \quad \langle on, 2\rangle \quad \langle \mathit{off}, 2\rangle \quad \ldots$

$\langle \mathit{off}, 0\rangle \quad \langle \mathit{off}, 0.1\rangle \quad \langle \mathit{off}, 1\rangle \quad \langle on, 0\rangle \quad \langle on, 0.53\rangle \quad \langle on, 1.3\rangle \quad \langle on, 2\rangle \quad \langle \mathit{off}, 2\rangle \quad \ldots$

The effect of $\langle \ell, \eta\rangle \xrightarrow{d_1+d_2} \langle \ell, \eta+d_1+d_2\rangle$ corresponds to:

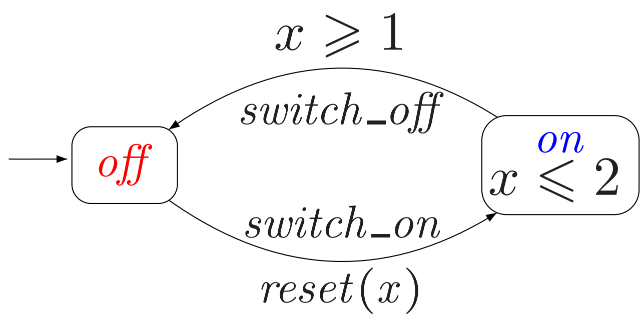
$$\langle \ell, \eta\rangle \xrightarrow{d_1} \langle \ell, \eta+d_1\rangle \xrightarrow{d_2} \langle \ell, \eta+d_1+d_2\rangle$$

Thus, uncountably many states of the form $\langle \ell, \eta+t\rangle$ with $0 \leqslant t \leqslant d_1+d_2$ are “visited”

Timed paths

- Paths through $TS(TA)$ model possible behaviours of TA
- But, not every path represents a realistic behaviour
- Some unrealistic phenomena that may occur:
  - time convergence: time converges to some value
  - timelock: the passage of time stops
  - zenoness: infinitely many actions take place in finite time
- Timelock and zenoness are modeling flaws and to be avoided
- Time-convergent paths will be excluded for model checking
  - they are treated similar as unfair paths in transition systems

Time divergence



The timed path:

$$\langle off, 0\rangle \xrightarrow{2^{-1}} \langle off, 1{-}2^{-1}\rangle \xrightarrow{2^{-2}} \langle off, 1{-}2^{-2}\rangle \xrightarrow{2^{-3}} \langle off, 1{-}2^{-3}\rangle \ \ldots\ldots$$

visits infinitely many states in the interval $[\frac{1}{2}, 1]$

Time divergence

- Let for any $t < d$, for fixed $d \in \mathbb{R}_{>0}$, clock valuation $\eta + t \models \mathit{Inv}(\ell)$

- A possible execution fragment starting from the location ℓ is:

$$\langle \ell, \eta \rangle \xrightarrow{d_1} \langle \ell, \eta + d_1 \rangle \xrightarrow{d_2} \langle \ell, \eta + d_1 + d_2 \rangle \xrightarrow{d_3} \langle \ell, \eta + d_1 + d_2 + d_3 \rangle \xrightarrow{d_4} \ldots$$

  - where $d_i > 0$ and the infinite sequence $d_1 + d_2 + \ldots$ *converges* towards d
  - such path fragments are called *time-convergent*

  $\Rightarrow$ time advances only up to a certain value

- Time-convergent execution fragments are unrealistic and *ignored*
  - much like unfair paths (as we will see later on)

Time divergence

- Infinite path fragment π is *time-divergent* if $ExecTime(\pi) = \infty$
- The function $ExecTime : \mathit{Act} \cup \mathbb{R}_{>0} \rightarrow \mathbb{R}_{\geqslant 0}$ is defined as:

$$ExecTime(\tau) \;=\; \begin{cases} 0 & \text{if } \tau \in \mathit{Act} \\ d & \text{if } \tau = d \in \mathbb{R}_{>0} \end{cases}$$

- For infinite execution fragment $\rho = s_0 \xrightarrow{\tau_1} s_1 \xrightarrow{\tau_2} s_2 \ldots$ in $\mathit{TS}(\mathit{TA})$ let:

$$ExecTime(\rho) \;=\; \sum_{i=0}^{\infty} ExecTime(\tau_i)$$

  - for path fragment π in $\mathit{TS}(\mathit{TA})$ induced by ρ: $ExecTime(\pi) = ExecTime(\rho)$
- For state s in $\mathit{TS}(\mathit{TA})$: $\mathit{Paths}_{\mathit{div}}(s) = \{ \pi \in \mathit{Paths}(s) \mid \pi \text{ is time-divergent} \}$

Example: light switch

The path π in *TS*$(Switch)$ in which on- and of-periods of one minute alternate:

$$\pi = \langle \mathit{off}, 0\rangle \, \langle \mathit{off}, 1\rangle \, \langle on, 0\rangle \, \langle on, 1\rangle \, \langle \mathit{off}, 1\rangle \, \langle \mathit{off}, 2\rangle \, \langle on, 0\rangle \, \langle on, 1\rangle \, \langle \mathit{off}, 2\rangle \ldots$$

is *time-divergent* as $ExecTime(\pi) = 1 + 1 + 1 + \ldots = \infty$

The path:

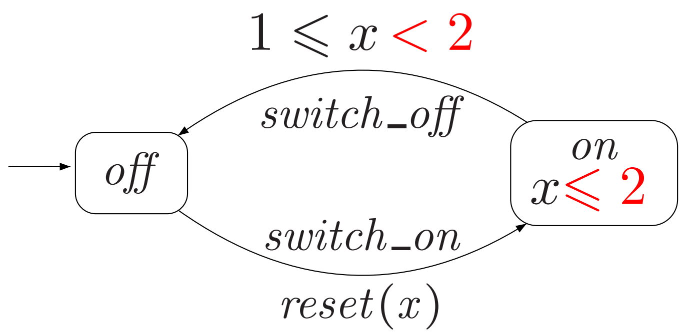
$$\pi' \;=\; \langle \mathit{off}, 0\rangle \, \langle \mathit{off}, 1/2\rangle \, \langle \mathit{off}, 3/4\rangle \, \langle \mathit{off}, 7/8\rangle \, \langle \mathit{off}, 15/16\rangle \ldots$$

is *time-convergent*, since $ExecTime(\pi') \;=\; \sum\limits_{i \geqslant 1} \left(\frac{1}{2}\right)^i = 1 < \infty$

Timelock

- State $s \in \mathit{TS}(\mathit{TA})$ contains a *timelock* if $\mathit{Paths}_{div}(s) = \varnothing$
  - there is no behavior in s where time can progress *ad infinitum*
  - any terminal state contains a timelock (but also non-terminal states may do)
  - terminal location does not necessarily yield a state with timelock (e.g. inv = true)
- *TA* is *timelock-free* if no state in $\mathit{Reach}(\mathit{TS}(\mathit{TA}))$ contains a timelock
- Timelocks are considered as *modeling flaws* that should be avoided
  - like deadlocks, we need mechanisms to check their presence

A non timelock-free timed automaton

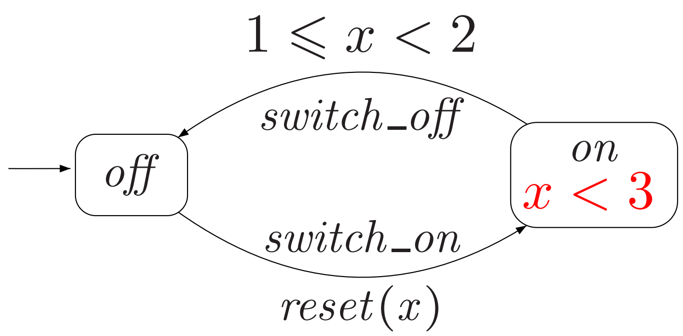


State $\langle on, 2 \rangle$ is reachable in transition system *TS*(*TA*), e.g., via:

$$\langle off, 0 \rangle \xrightarrow{switch\_on} \langle on, 0 \rangle \xrightarrow{2} \langle on, 2 \rangle$$

As $\langle on, 2 \rangle$ is a terminal state, $Paths_{div}(\langle on, 2 \rangle) = \varnothing$

Another non timelock-free timed automaton



State $\langle on, 2\rangle$ is not terminal, , e.g., the time-convergent path in:

$$\langle on, 2\rangle \; \langle on, 2.9\rangle \; \langle on, 2.99\rangle \; \langle on, 2.999\rangle \; \langle on, 2.9999\rangle \; \ldots$$

emanates from it. But, $\mathit{Paths}_{\mathit{div}}(\langle on, 2\rangle) = \varnothing$

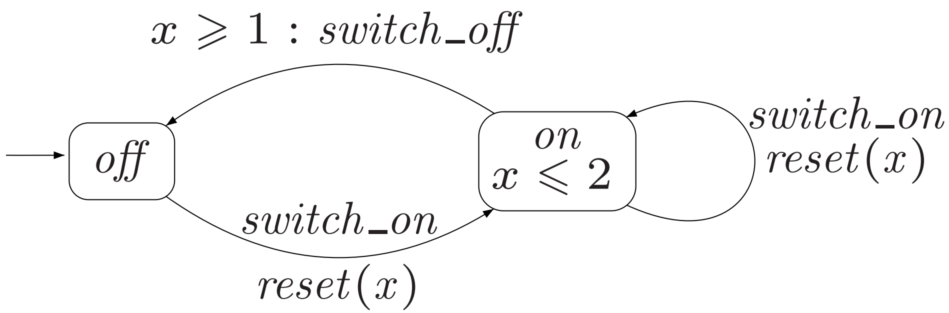
Zenoness

- A *TA* that performs infinitely many actions in finite time is *zeno*
- Path π in $TS(TA)$ is *zeno* if:

  it is time-convergent, and infinitely many actions $\alpha \in Act$ are executed along π

- *TA* is *non-zeno* if there does not exist a zeno path in $TS(TA)$
  - any π in $TS(TA)$ is time-divergent or
  - is time-convergent with nearly all (i.e., all except for finitely many) transitions being delay transitions
- Zeno paths are considered as *modeling flaws* that should be avoided
  - like timelocks (and deadlocks), we need mechanisms to check zenoness
  - this, however, turns out to be difficult $\Rightarrow$ resort to sufficient conditions

Zeno paths of a (yet another) light switch



The paths induced by the following execution fragments:

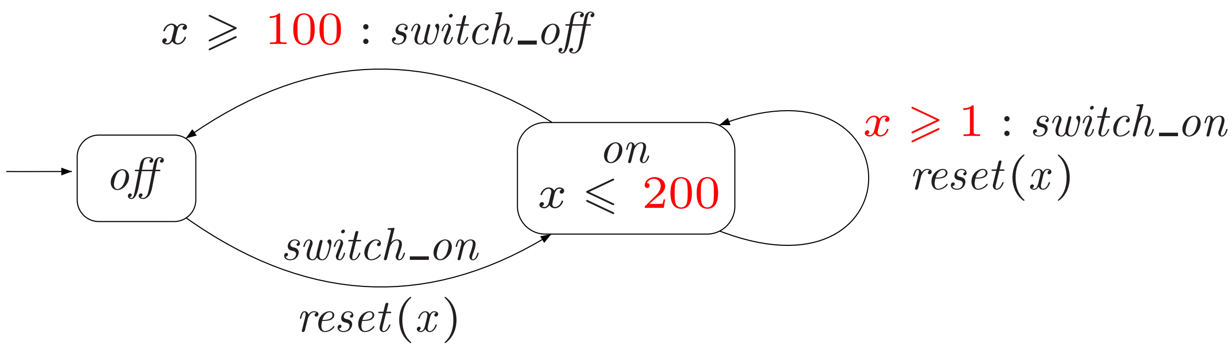
$$\langle off, 0\rangle \xrightarrow{\text{sw\_on}} \langle on, 0\rangle \xrightarrow{\text{sw\_on}} \langle on, 0\rangle \xrightarrow{\text{sw\_on}} \langle on, 0\rangle \xrightarrow{\text{sw\_on}} \ldots$$

$$\langle off, 0\rangle \xrightarrow{\text{sw\_on}} \langle on, 0\rangle \xrightarrow{0.5} \langle on, 0.5\rangle \xrightarrow{\text{sw\_on}} \langle on, 0\rangle \xrightarrow{0.25} \langle on, 0.25\rangle \xrightarrow{\text{sw\_on}} \ldots$$

are zeno paths during which the user presses the on button faster and faster

avoid by imposing a minimal delay, e.g., $\frac{1}{100}$, between successive on's

A non-zeno variant



Strong zenoness

Let *TA* with set C of clocks such that for every (control) cycle:

$$\ell_0 \xhookrightarrow{g_1:\alpha_1,C_1} \ell_1 \xhookrightarrow{g_2:\alpha_2,C_2} \ldots \xhookrightarrow{g_n:\alpha_n,C_n} \ell_n = \ell_0$$

there exists a clock $x \in C$ such that:

1. $x \in C_i$ for some $0 < i \leqslant n$, and
2. for all clock evaluations η there exists $c \in \mathbb{N}_{>0}$ such that

$$\eta(x) < c \quad \text{implies} \quad (\exists 0 < j \leqslant n.\, \eta \not\models g_j \ \text{ or } \ \eta \not\models \mathit{Inv}(\ell_j))$$

Then: *TA* is *non-zeno*

Proof

Example

Timelock, time-divergence and zenoness

- A timed automaton is adequately modeling a time-critical system whenever it is:

  non-zeno and timelock-free

- Time-divergent paths will be explicitly excluded for analysis purposes