# Time Divergence, Timelock, and Zenoness

## Lecture #17 of Advanced Model Checking

*Joost-Pieter Katoen*

Lehrstuhl 2: Software Modeling & Verification

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

January 18, 2017

# 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:

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

- 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 $C$

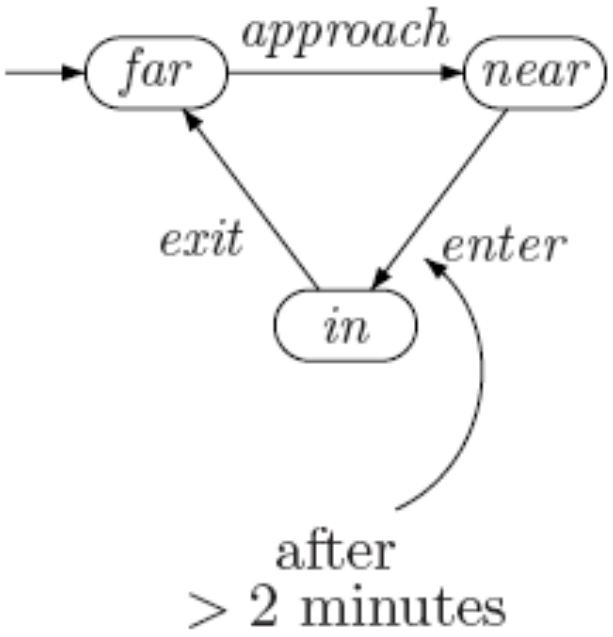
clock difference constraints such as $x - y < c$ can be added at expense of slightly more involved theory

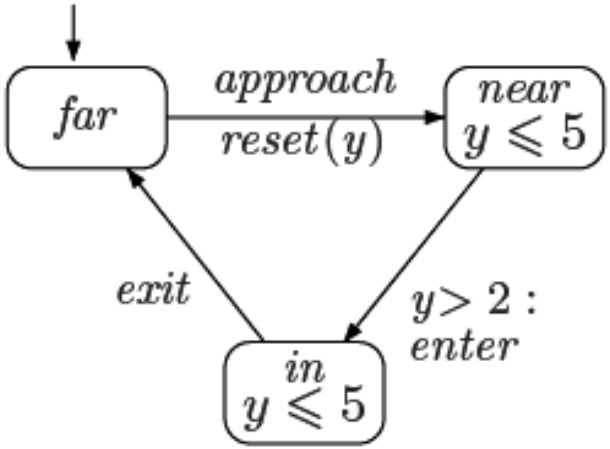
# Timed automaton

A *timed automaton* $TA = (Loc, Act, C, \hookrightarrow, Loc_0, Inv, AP, L)$ 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* $\eta$ 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 $\eta$ 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 $\eta$) is abbreviated by reset $\{ x, y \}$ in $\eta$

# Timed automaton semantics

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

Transition system $\mathit{TS}(\mathit{TA}) = (S, \mathit{Act}', \to, I, \mathit{AP}', L')$ 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
- $I = \{ \langle \ell_0, \eta_0 \rangle \mid \ell_0 \in \mathit{Loc}_0 \ \wedge \ \eta_0(x) = 0 \text{ for all } x \in C \}$
- $\mathit{AP}' = \mathit{AP} \cup \mathit{ACC}(C)$
- $L'(\langle \ell, \eta \rangle) = L(\ell) \cup \{ g \in \mathit{ACC}(C) \mid \eta \models g \}$
- $\hookrightarrow$ 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 $\ell$ to $\ell'$ such that:
  - $g$ is satisfied by $\eta$, i.e., $\eta \models g$
  - $\eta' = \eta$ with all clocks in $D$ reset to 0, i.e., $\eta' =$ reset $D$ in $\eta$
  - $\eta'$ fulfills the invariant of location $\ell'$, 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.:

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

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

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

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

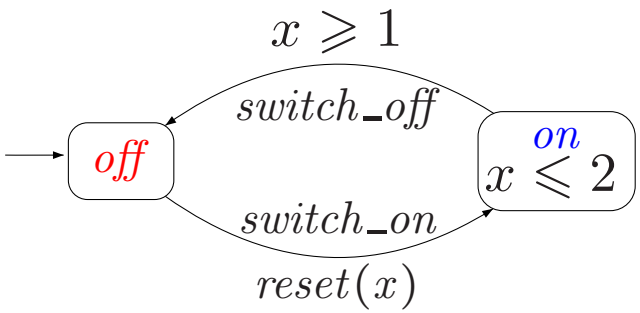
$$\langle \ell, \eta\rangle \xrightarrow{d_1} \langle \ell, \eta+d_1\rangle \xrightarrow{d_2} \langle \ell, \eta+d_1+d_2\rangle$$

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

# A sample time-divergent path




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 $\ell$ 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 $\pi$ is *time-divergent* if $ExecTime(\pi) = \infty$
- The function $ExecTime : \mathit{Act} \cup \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ is defined as:

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

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

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

  - for path fragment $\pi$ in *TS*(*TA*) induced by $\rho$: $ExecTime(\pi) = ExecTime(\rho)$

- For state $s$ in *TS*(*TA*): $\mathit{Paths}_{div}(s) = \{\, \pi \in \mathit{Paths}(s) \mid \pi \text{ is time-divergent} \,\}$

# Example: light switch

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

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

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

The path:

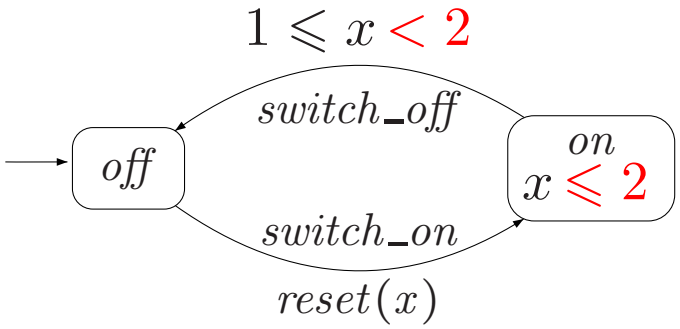
$$\pi' = \langle off, 0\rangle \langle off, 1/2\rangle \langle off, 3/4\rangle \langle off, 7/8\rangle \langle off, 15/16\rangle \ldots$$

is *time-convergent*, since $ExecTime(\pi') = \sum_{i \geqslant 1} \left(\frac{1}{2}\right)^i = \sum_{i=0} \left(\frac{1}{2}\right)^i - 1 = 1 < \infty$

# 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 timed automaton containing a timelock

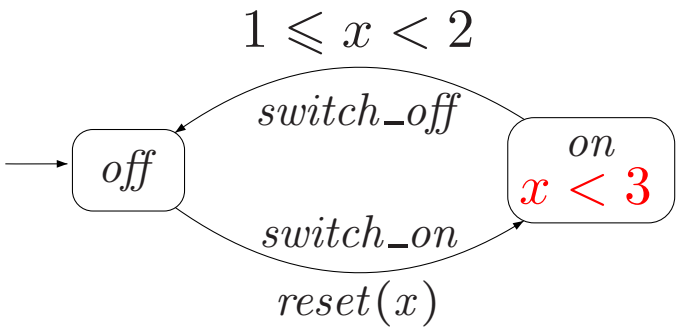



State $\langle on, 2 \rangle$ is reachable in transition system *TS*( *TA*), e.g., via:

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

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

# Another timed automaton with a timelock




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, $\mathit{Paths}_{\mathit{div}}(\langle on, 2 \rangle) = \varnothing$

# Timed reachability: the $\Longrightarrow$ relation

For infinite path fragments in *TS*(*TA*) performing $\infty$ many actions let:

$$s_0 \overset{d_0}{\Longrightarrow} s_1 \overset{d_1}{\Longrightarrow} s_2 \overset{d_2}{\Longrightarrow} \ldots \qquad \text{with } d_0, d_1, d_2 \ldots \geqslant 0$$

denote the equivalence class containing all infinite path fragments induced by execution fragments of the form:

$$s_0 \underbrace{\xrightarrow{d_0^1} \ldots \xrightarrow{d_0^{k_0}}}_{\substack{\text{time passage of} \\ d_0 \text{ time-units}}} s_0{+}d_0 \xrightarrow{\alpha_1} s_1 \underbrace{\xrightarrow{d_1^1} \ldots \xrightarrow{d_1^{k_1}}}_{\substack{\text{time passage of} \\ d_1 \text{ time-units}}} s_1{+}d_1 \xrightarrow{\alpha_2} s_2 \underbrace{\xrightarrow{d_2^1} \ldots \xrightarrow{d_2^{k_2}}}_{\substack{\text{time passage of} \\ d_2 \text{ time-units}}} s_2{+}d_2 \xrightarrow{\alpha_3} \ldots$$

where $k_i \in \mathbb{N}$, $d_i \in \mathbb{R}_{\geqslant 0}$ and $\alpha_i \in \mathit{Act}$ such that $\sum_{j=1}^{k_i} d_i^j = d_i$.

For $\pi \in s_0 \overset{d_0}{\Longrightarrow} s_1 \overset{d_1}{\Longrightarrow} \ldots$ we have $ExecTime(\pi) = \sum_{i \geqslant 0} d_i$

# Timed reachability

For time-divergent path $\pi \in s_0 \xrightarrow{d_0} s_1 \xrightarrow{d_1} \ldots$, we have

$$\pi \models \Diamond^J \Phi \quad \text{iff} \quad \exists\, i \geqslant 0.\, s_i{+}d \models \Phi \text{ for some } d \in [0, d_i] \text{ with}$$

$$\sum_{k=0}^{i-1} d_k{+}d \in J \qquad \text{and}$$

where for $s_i = \langle \ell_i, \eta_i \rangle$ and $d \geqslant 0$ we have $s_i{+}d = \langle \ell_i, \eta_i{+}d \rangle$

# Some abbreviations

"Always" is obtained in the following way:

$$\exists\Box^J \Phi \;=\; \neg\forall\Diamond^J \neg\Phi \quad \text{and} \quad \forall\Box^J \Phi \;=\; \neg\exists\Diamond^J \neg\Phi$$

$\exists\Box^J \Phi$ asserts that for some path during the interval $J$, $\Phi$ holds

$\forall\Box^J \Phi$ requires this to hold for all paths

Standard $\Box$ and $\Diamond$-operator are obtained as follows:

$$\Diamond \Phi = \Diamond^{[0,\infty)} \Phi \quad \text{and} \quad \Box \Phi = \Box^{[0,\infty)} \Phi$$

# Characterizing timelock

- Timed reachability is well-defined for *TA* with timelocks
- A state is *timelock-free* if and only if it satisfies $\exists\Box$true
  - some time-divergent path satisfies $\Box$true, i.e., there is $\geqslant 1$ time-divergent path
  - note: for fair CTL, the states in which a fair path starts also satisfy $\exists\Box$true
- *TA* is timelock-free iff $\forall s \in \mathit{Reach}(\mathit{TS}(\mathit{TA}))$: $s \models \exists\Box$true
- Timelocks can thus be checked by model checking

# Zenoness

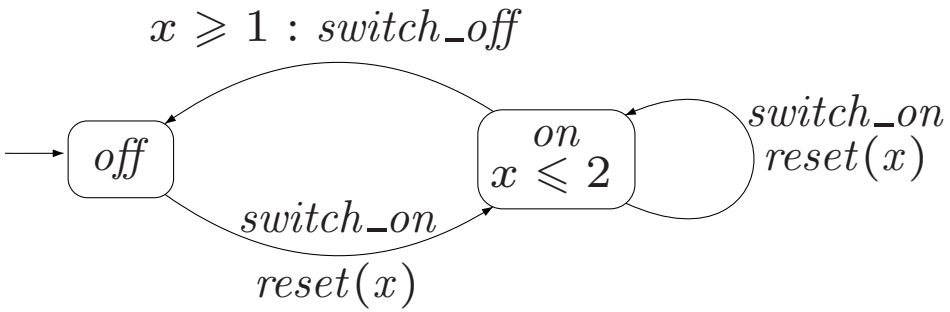
- A *TA* that performs infinitely many actions in finite time is *Zeno*
- Path $\pi$ in *TS*(*TA*) is *Zeno* if:

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

- *TA* is *non-Zeno* if there does not exist a Zeno path in *TS*(*TA*)
  - any $\pi$ 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

# A Zeno timed automaton




The paths induced by the following execution fragments:

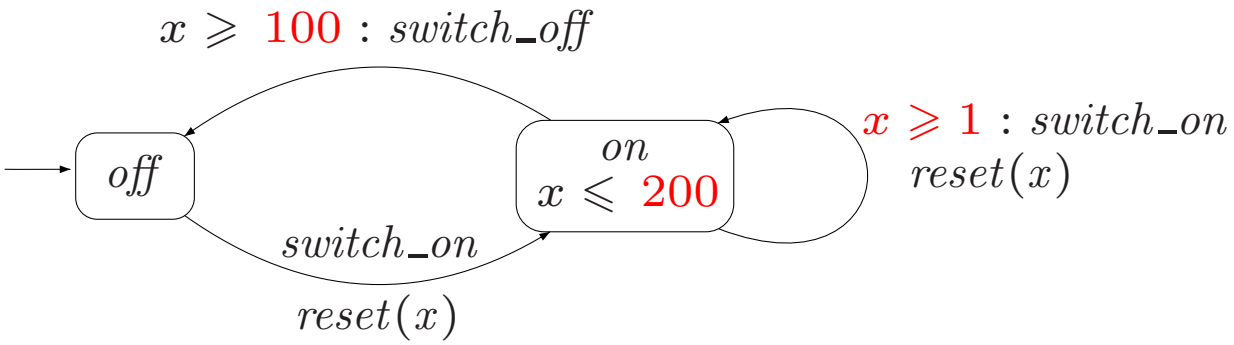
$$\langle off, 0\rangle \xrightarrow{sw\_on} \langle on, 0\rangle \xrightarrow{sw\_on} \langle on, 0\rangle \xrightarrow{sw\_on} \langle on, 0\rangle \xrightarrow{sw\_on} \ldots$$

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

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 actions

# A non-Zeno timed automaton



# Sufficient condition for non-Zenoness

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

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

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 $\eta$ of *TA* 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

# Strong Zenoness is compositional

# Timelock, time-divergence and Zenoness

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

  non-Zeno and timelock-free

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