Real-time and Probabilistic Systems Verification

Luca Tesei

MSc in Computer Science, University of Camerino

Topics

- Time Divergence
- Timelocks
- Zenoness

More:

The slides in the following pages are taken from the material of the course "Advanced Model Checking" held by Prof. Dr. Ir. Joost-Pieter Katoen at Aachen University.

Timed paths

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

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

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

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

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

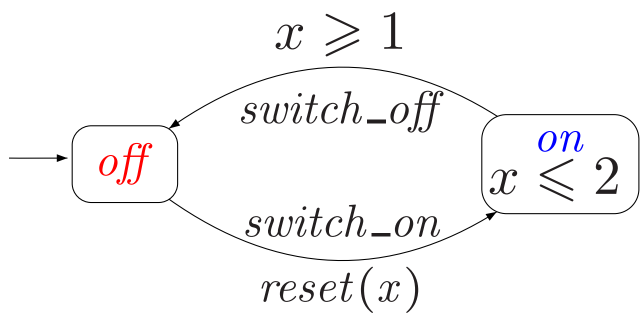
$$\langle \ell, \eta\rangle \xrightarrow{d_1} \langle \ell, \eta+d_1\rangle \xrightarrow{d_2} \langle \ell, \eta+d_1+d_2\rangle$$

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*
  ⇒ 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 *TS*(*TA*) let:

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

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

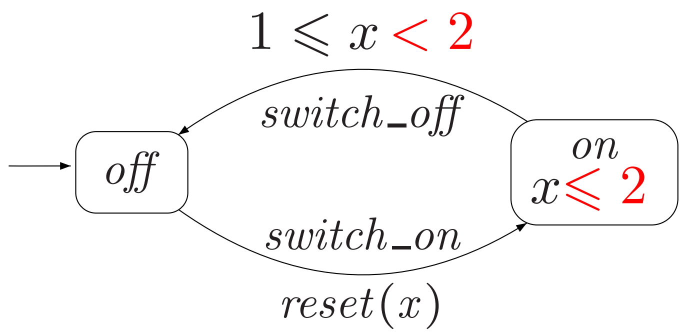
$$\pi' \;=\; \langle \mathit{off}, 0 \rangle \, \langle \mathit{off}, 1/2 \rangle \, \langle \mathit{off}, 3/4 \rangle \, \langle \mathit{off}, 7/8 \rangle \, \langle \mathit{off}, 15/16 \rangle \ldots$$

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

Timelock

- State $s \in$ *TS*(*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 *Reach*(*TS*(*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

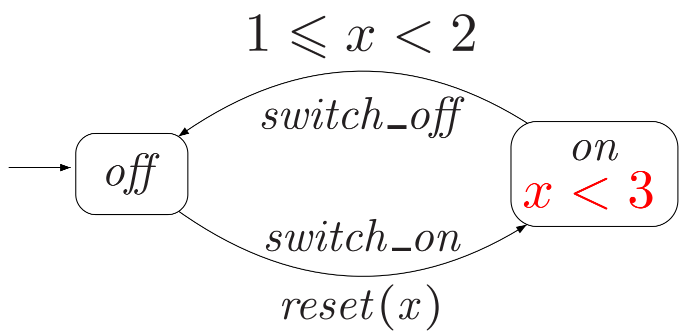


State $\langle on, 2\rangle$ is reachable in transition system *TS*(*TA*), e.g., via:

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

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, $Paths_{div}(\langle on, 2 \rangle) = \varnothing$

Zenoness

- A *TA* that performs infinitely many actions in finite time is *zeno*

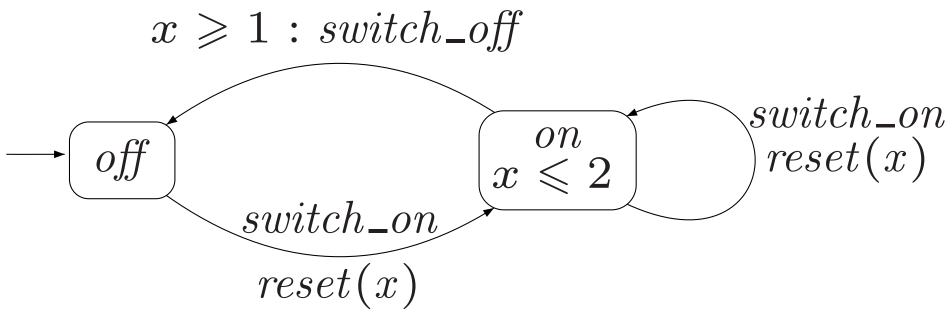
- Path π in *TS*(*TA*) is *zeno* if:

  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:

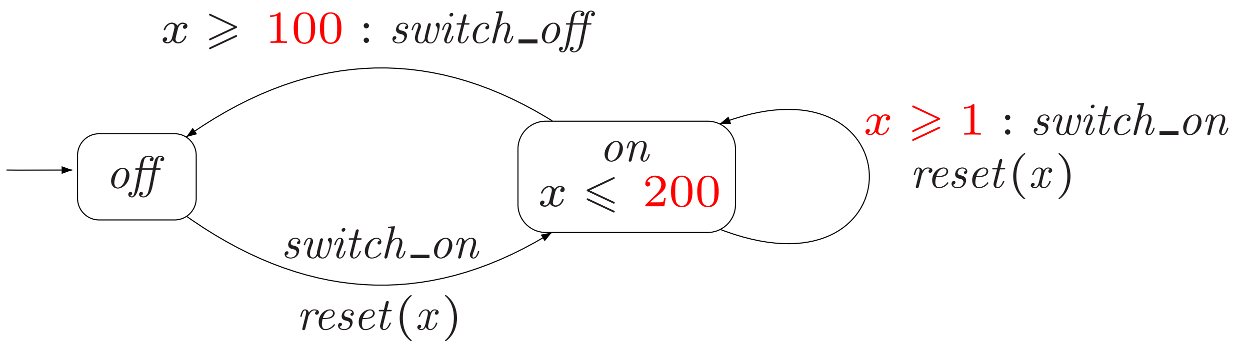
$$\langle \mathit{off}, 0\rangle \xrightarrow{\text{sw\_on}} \langle on, 0\rangle \xrightarrow{\text{sw\_on}} \langle on, 0\rangle \xrightarrow{\text{sw\_on}} \langle on, 0\rangle \xrightarrow{\text{sw\_on}} \ldots$$

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

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



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