# Verification – Lecture 25
# Region Graphs

Bernd Finkbeiner – Sven Schewe
Rayna Dimitrova – Lars Kuhtz – Anne Proetzsch

Wintersemester 2007/2008

REVIEW

## Timed automaton

A *timed automaton* is a tuple

$$TA = (Loc, Act, C, \rightsquigarrow, Loc_0, inv, AP, L) \quad \text{where:}$$

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

# Timed automaton semantics

For timed automaton *TA* $= \big(\textit{Loc}, \textit{Act}, C, \rightsquigarrow, \textit{Loc}_0, \textit{inv}, \textit{AP}, L\big)$:
state graph $S(\textit{TA}) = (Q, Q_0, E, L')$ over $\textit{AP}'$ where:

- $Q = \textit{Loc} \times \textit{val}(C)$, state $s = \langle \ell, v \rangle$ for location $\ell$ and clock valuation $v$
- $Q_0 = \{ \langle \ell_0, v_0 \rangle \mid \ell_0 \in \textit{Loc}_0 \ \wedge \ v_0(x) = 0 \text{ for all } x \in C \}$
- $\textit{AP}' = \textit{AP} \cup \textit{ACC}(C)$
- $L'(\langle \ell, v \rangle) = L(\ell) \cup \{ g \in \textit{ACC}(C) \mid v \models g \}$
- $E$ is the edge set defined on the next slide





# Timed automaton semantics

The edge set $E$ consist of the following two types of transitions:

- Discrete transition: $\langle \ell, v \rangle \xrightarrow{\alpha} \langle \ell', v' \rangle$ if all following conditions hold:
  - there is an edge labeled $(g : \alpha, D)$ from location $\ell$ to $\ell'$ such that:
  - $g$ is satisfied by $v$, i.e., $v \models g$
  - $v' = v$ with all clocks in $D$ reset to 0, i.e., $v' =$ reset $D$ in $v$
  - $v'$ fulfills the invariant of location $\ell'$, i.e., $v' \models \textit{inv}(\ell')$
- Delay transition: $\langle \ell, v \rangle \xrightarrow{d} \langle \ell, v{+}d \rangle$ for positive real $d$
  - if for any $0 \leqslant d' \leqslant d$ the invariant of $\ell$ holds for $v{+}d'$, i.e. $v{+}d' \models \textit{inv}(\ell)$

# Timelock

- State $s \in S(TA)$ contains a *timelock* if $Paths_{div}(s) = \varnothing$
  - there is no behavior in $s$ where time can progress *ad infinitum*
  - clearly: 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*$(S(TA))$ contains a timelock
- Timelocks are considered as *modeling flaws* that should be avoided





# Zenoness

- A *TA* that performs infinitely many actions in finite time is *Zeno*
- Path $\pi$ in $S(TA)$ 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 an initial Zeno path in $S(TA)$
  - any $\pi$ in $S(TA)$ 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

# Timed CTL

Syntax of TCTL *state-formulas* over *AP* and set $C$:

$$\Phi ::= \text{true} \;\Big|\; a \;\Big|\; g \;\Big|\; \Phi \wedge \Phi \;\Big|\; \neg\Phi \;\Big|\; \exists\varphi \;\Big|\; \forall\varphi$$

where $a \in$ *AP*, $g \in$ *ACC*$(C)$ and $\varphi$ is a path-formula defined by:

$$\varphi ::= \Phi \, \mathsf{U}^{J} \, \Phi$$

where $J \subseteq \mathbb{R}_{\geqslant 0}$ is an interval whose bounds are naturals

Forms of $J$: $[n, m]$, $(n, m]$, $[n, m)$ or $(n, m)$ for $n, m \in \mathbb{N}$ and $n \leqslant m$

for right-open intervals, $m = \infty$ is also allowed





# Some abbreviations

- $\Diamond^{J}\Phi \;=\; \text{true}\, \mathsf{U}^{J}\, \Phi$
- $\exists\Box^{J}\,\Phi \;=\; \neg\forall\Diamond^{J}\,\neg\Phi$ and $\forall\Box^{J}\,\Phi \;=\; \neg\exists\Diamond^{J}\,\neg\Phi$
- $\Diamond\,\Phi = \Diamond^{[0,\infty)}\,\Phi$ and $\Box\,\Phi = \Box^{[0,\infty)}\,\Phi$

# Semantics of TCTL

For state $s = \langle \ell, \eta \rangle$ in $S(TA)$ the satisfaction relation $\models$ is defined by:

| | | |
|---|---|---|
| $s \models \text{true}$ | | |
| $s \models a$ | iff | $a \in L(\ell)$ |
| $s \models g$ | iff | $\eta \models g$ |
| $s \models \neg \Phi$ | iff | not $s \models \Phi$ |
| $s \models \Phi \wedge \Psi$ | iff | $(s \models \Phi)$ and $(s \models \Psi)$ |
| $s \models \exists \varphi$ | iff | $\pi \models \varphi$ for some $\pi \in \mathit{Paths}_{div}(s)$ |
| $s \models \forall \varphi$ | iff | $\pi \models \varphi$ for all $\pi \in \mathit{Paths}_{div}(s)$ |

path quantification over time-divergent paths only





# Semantics of TCTL

For time-divergent path $\pi \in s_0 \stackrel{d_0}{\Longrightarrow} s_1 \stackrel{d_1}{\Longrightarrow} \ldots$:

$\pi \models \Phi \, \mathsf{U}^{J} \, \Psi$

iff

$\exists\, i \geqslant 0.\, s_i{+}d \models \Psi$ for some $d \in [0, d_i]$ with $\sum_{k=0}^{i-1} d_k + d \in J$

and

$\forall j \leqslant i.\, s_j{+}d' \models \Phi \vee \Psi$ for every $d' \in [0, d_j]$ with $\sum_{j=0}^{j-1} d_k + d' \leqslant \sum_{k=0}^{i-1} d_k + d$

# TCTL-semantics for timed automata

- Let *TA* be a timed automaton with clocks $C$ and locations *Loc*
- For TCTL-state-formula $\Phi$, the *satisfaction set* *Sat*$(\Phi)$ is defined by:

$$\mathit{Sat}(\Phi) \;=\; \{\, s \in \mathit{Loc} \times \mathit{Eval}(C) \mid s \models \Phi \,\}$$

- *TA* satisfies TCTL-formula $\Phi$ iff $\Phi$ holds in all initial states of *TA*:

$$\mathit{TA} \models \Phi \quad \text{if and only if} \quad \forall \ell_0 \in \mathit{Loc}_0.\, \langle \ell_0, \eta_0 \rangle \models \Phi$$

where $\eta_0(x) = 0$ for all $x \in C$



# Timed CTL versus CTL

- Due to ignoring time-convergent paths in TCTL semantics, possibly:

$$\underbrace{S(\mathit{TA}) \models_{\text{TCTL}} \forall\varphi}_{\text{TCTL semantics}} \quad \text{but} \quad \underbrace{S(\mathit{TA}) \not\models_{\text{CTL}} \forall\varphi}_{\text{CTL semantics}}$$

  - CTL semantics considers all paths, timed CTL only time-divergent paths

- For $\Phi \;=\; \forall\Box\big(on \;\longrightarrow\; \forall\Diamond \mathit{off}\big)$ and the light switch

$$S(\mathit{Switch}) \models_{\text{TCTL}} \Phi \quad \text{whereas} \quad S(\mathit{TA}) \not\models_{\text{CTL}} \Phi$$

  - there are time-convergent paths on which location *on* is never left

# Characterizing timelock

- TCTL semantics is also well-defined for *TA* with timelock
- 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 $\forall s \in \mathit{Reach}(S(\mathit{TA}))$: $s \models \exists\Box$true
- Timelocks can thus be checked by model checking



# TCTL model checking

- TCTL model-checking problem: $\mathit{TA} \models \Phi$ for non-Zeno *TA*

$$\underbrace{\mathit{TA} \models \Phi}_{\text{timed automaton}} \quad \text{iff} \quad \underbrace{S(\mathit{TA}) \models \Phi}_{\text{infinite state graph}}$$

- Idea: consider a finite region graph $RG(\mathit{TA})$
- Transform TCTL formula $\Phi$ into an "equivalent" CTL-formula $\widehat{\Phi}$
- Then: $\mathit{TA} \models_{\text{TCTL}} \Phi \quad \text{iff} \quad \underbrace{RG(\mathit{TA})}_{\text{finite state graph}} \models_{\text{CTL}} \widehat{\Phi}$

# Eliminating timing parameters

- Eliminate all intervals $J \neq [0, \infty)$ from TCTL formulas
  - introduce a fresh clock, $z$ say, that does not occur in *TA*
  - $s \models \exists \Diamond^{J} \Phi$ iff reset $z$ in $s \models \Diamond(z \in J \wedge \Phi)$
- Formally: for any state $s$ of $S(TA)$ it holds:

$$s \models \exists \Phi \,\mathsf{U}^{J}\, \Psi \quad \text{iff} \quad \underbrace{s\{z := 0\}}_{\text{state in } S(TA \oplus z)} \models \exists \big( (\Phi \vee \Psi) \,\mathsf{U}\, (z \in J) \wedge \Psi \big)$$

$$s \models \forall \Phi \,\mathsf{U}^{J}\, \Psi \quad \text{iff} \quad \underbrace{s\{z := 0\}}_{\text{state in } S(TA \oplus z)} \models \forall \big( (\Phi \vee \Psi) \,\mathsf{U}\, (z \in J) \wedge \Psi \big)$$

  - where $TA \oplus z$ is *TA* (over $C$) extended with $z \notin C$



# Clock equivalence

Impose an equivalence, denoted $\cong$, on the clock valuations such that:

(A) Equivalent clock valuations satisfy the same clock constraints $g$ in *TA* and $\Phi$:

$$\eta \cong \eta' \;\Rightarrow\; (\eta \models g \quad \text{iff} \quad \eta' \models g)$$

  - no diagonal clock constraints are considered
  - all the constraints in *TA* and $\Phi$ are thus either of the form $x \leqslant c$ or $x < c$

(B) Time-divergent paths emanating from equivalent states are equivalent

  - this property guarantees that equivalent states satisfy the same path formulas

(C) The number of equivalence classes under $\cong$ is finite

# First observation

- $\eta \models x < c$ whenever $\eta(x) < c$, or equivalently, $\lfloor \eta(x) \rfloor < c$
  - $\lfloor d \rfloor \; = \; \max\{ c \in \mathbb{N} \mid c \leqslant d \}$ and $\mathit{frac}(d) \; = \; d - \lfloor d \rfloor$
- $\eta \models x \leqslant c$ whenever $\lfloor \eta(x) \rfloor < c$ or $\lfloor \eta(x) \rfloor = c$ and $\mathit{frac}(\eta(x)) = 0$

$\Rightarrow$ $\eta \models g$ only depends on $\lfloor \eta(x) \rfloor$, and whether $\mathit{frac}(\eta(x)) = 0$

- Initial suggestion: clock valuations $\eta$ and $\eta'$ are equivalent if:

$$\lfloor \eta(x) \rfloor \; = \; \lfloor \eta'(x) \rfloor \quad \text{and} \quad \mathit{frac}(\eta(x)) = 0 \text{ iff } \mathit{frac}(\eta'(x)) = 0$$

- Note: it is crucial that in $x < c$ and $x \leqslant c$, $c$ is a natural



# Second observation

- Consider location $\ell$ with *inv*$(\ell) =$ true and only outgoing transitions:
  - one guarded with $x \geqslant 2$ (action $\alpha$) and $y > 1$ (action $\beta$)
- Let state $s = \langle \ell, \eta \rangle$ with $1 < \eta(x) < 2$ and $0 < \eta(y) < 1$
  - $\alpha$ and $\beta$ are disabled, only time may elapse
- Transition that is enabled next depends on $x < y$ or $x \geqslant y$
  - e.g., if $\mathit{frac}(\eta(x)) \geqslant \mathit{frac}(\eta(y))$, action $\alpha$ is enabled first
- Suggestion for strengthening of initial proposal for all $x, y \in C$ by:

$$\mathit{frac}(\eta(x)) \leqslant \mathit{frac}(\eta(y)) \quad \text{if and only if} \quad \mathit{frac}(\eta'(x)) \leqslant \mathit{frac}(\eta'(y))$$

# Final observation

- So far, clock equivalence yield a denumerable though not finite quotient
- For *TA* $\models \Phi$ only the clock constraints in *TA* and $\Phi$ are relevant
  - let $c_x \in \mathbb{N}$ the *largest constant* with which $x$ is compared in *TA* or $\Phi$

$\Rightarrow$ If $\eta(x) > c_x$ then the actual value of $x$ is irrelevant

- constraints on $\cong$ so far are only relevant for clock values of $x$ ($y$) up to $c_x$ ($c_y$)



# Clock equivalence

Clock valuations $\eta, \eta' \in$ *Eval*$(C)$ are *equivalent*, denoted $\eta \cong \eta'$, if:

(1) for any $x \in C$: $(\eta(x) > c_x) \wedge (\eta'(x) > c_x)$ or $(\eta(x) \leqslant c_x) \wedge (\eta'(x) \leqslant c_x)$

(2) for any $x \in C$: if $\eta(x), \eta'(x) \leqslant c_x$ then:

$$\lfloor \eta(x) \rfloor = \lfloor \eta'(x) \rfloor \quad \text{and} \quad \mathit{frac}(\eta(x)) = 0 \text{ iff } \mathit{frac}(\eta_2(x)) = 0$$

(3) for any $x, y \in C$: if $\eta(x), \eta'(x) \leqslant c_x$ and $\eta(y), \eta'(y) \leqslant c_y$, then:

$$\mathit{frac}(\eta(x)) \leqslant \mathit{frac}(\eta(y)) \quad \text{iff} \quad \mathit{frac}(\eta'(x)) \leqslant \mathit{frac}(\eta'(y)).$$

$$s \cong s' \quad \text{iff} \quad \ell = \ell' \quad \text{and} \quad \eta \cong \eta'$$

# Regions

- The *clock region* of $\eta \in \mathit{Eval}(C)$, denoted $[\eta]$, is defined by:

$$[\eta] \ = \ \{\, \eta' \in \mathit{Eval}(C) \mid \eta \cong \eta' \,\}$$

- The *state region* of $s = \langle \ell, \eta \rangle \in S(\mathit{TA})$ is defined by:

$$[s] \ = \ \langle \ell, [\eta] \rangle \ = \ \{\, \langle s, \eta' \rangle \mid \eta' \in [\eta] \,\}$$



# Number of regions

The *number of clock regions* is bounded from below and above by:

$$|C|! * \prod_{x \in C} c_x \ \leqslant \ \big| \underbrace{\mathit{Eval}(C)/\cong}_{\text{number of regions}} \big| \ \leqslant \ |C|! * 2^{|C|-1} * \prod_{x \in C} (2c_x + 2)$$

where for the upper bound it is assumed that $c_x \geqslant 1$ for any $x \in C$

the number of state regions is $|\mathit{Loc}|$ times larger

## Preservation of atomic properties

1. For $\eta, \eta' \in \mathit{Eval}(C)$ such that $\eta \cong \eta'$:

$$\eta \models g \quad \text{if and only if} \quad \eta' \models g \text{ for any } g \in \mathit{AP}' \setminus \mathit{AP}$$

2. For $s, s' \in S(\mathit{TA})$ such that $s \cong s'$:

$$s \models a \quad \text{if and only if} \quad s' \models a \text{ for any } a \in \mathit{AP}'$$

where *AP'* includes all atomic propositions and atomic clock constraints in *TA* and $\Phi$.



## Clock equivalence is a bisimulation

Clock equivalence is a bisimulation equivalence over *AP'*

# Unbounded and successor regions

- Clock region $r_\infty = \{ \eta \in \mathit{Eval}(C) \mid \forall x \in C.\, \eta(x) > c_x \}$ is *unbounded*
- $r'$ is the *successor (clock) region* of $r$, denoted $r' = \mathit{succ}(r)$, if either:

1. $r = r_\infty$ and $r = r'$, or

2. $r \neq r_\infty$, $r \neq r'$ and $\forall \eta \in r$:

$$\exists d \in \mathbb{R}_{>0}.\ (\eta{+}d \in r' \quad \text{and} \quad \forall 0 \leqslant d' \leqslant d.\, \eta{+}d' \in r \cup r')$$

- The *successor region*: $\mathit{succ}(\langle \ell, r \rangle) \ = \ \langle \ell, \mathit{succ}(r) \rangle$

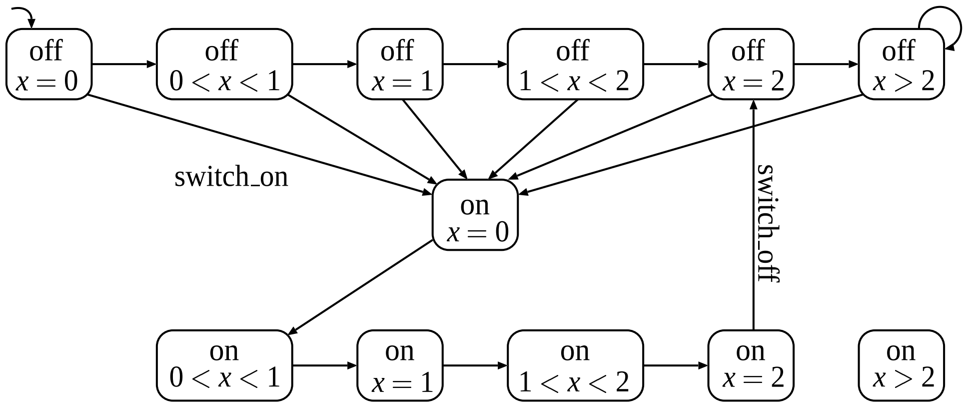


# Region Graph

For non-Zeno $\mathit{TA} = (\mathit{Loc}, \mathit{Act}, C, \rightsquigarrow, \mathit{Loc}_0, \mathit{inv}, \mathit{AP}, L)$ with $S(\mathit{TA}) = (Q, Q_0, E, L)$ let $\mathit{RG}(\mathit{TA}, \Phi) = (Q', Q'_0, E', L')$ with

- $Q' = Q/\cong = \{ [q] \mid q \in Q \}$ and $Q'_0 = \{ [q] \mid q \in Q_0 \}$,
- $L'(\langle \ell, r \rangle) = L(\ell) \cup \{ g \in \mathit{AP}' \setminus \mathit{AP} \mid r \models g \}$
- $E'$ consists of two types of edges:
  - Discrete transitions: $\langle \ell, r \rangle \xrightarrow{\alpha}{}' \langle \ell', \text{reset } D \text{ in } r \rangle$ if $\ell \overset{g:\alpha,D}{\rightsquigarrow} \ell'$ and $r \models g$ and reset $D$ in $r \models \mathit{inv}(\ell')$;
  - Delay transitions: $\langle \ell, r \rangle \xrightarrow{\tau}{}' \langle \ell, \mathit{succ}(r) \rangle$ if $r \models \mathit{inv}(\ell)$ and $\mathit{succ}(r) \models \mathit{inv}(\ell)$

# Example: simple light switch






# Time convergence

For non-Zeno *TA* and $\pi = s_0\, s_1\, s_2 \ldots$ an initial, infinite path in *S*(*TA*):

(a) $\pi$ is *time-convergent* $\Rightarrow$ $\exists$ state region $\langle \ell, r \rangle$ such that for some $j$:

$$s_i \in \langle \ell, r \rangle \text{ for all } i \geqslant j$$

(b) If $\exists$ state region $\langle \ell, r \rangle$ with $r \neq r_\infty$ and an index $j$ such that:

$$s_i \in \langle \ell, r \rangle \text{ for all } i \geqslant j$$

then $\pi$ is *time-convergent*

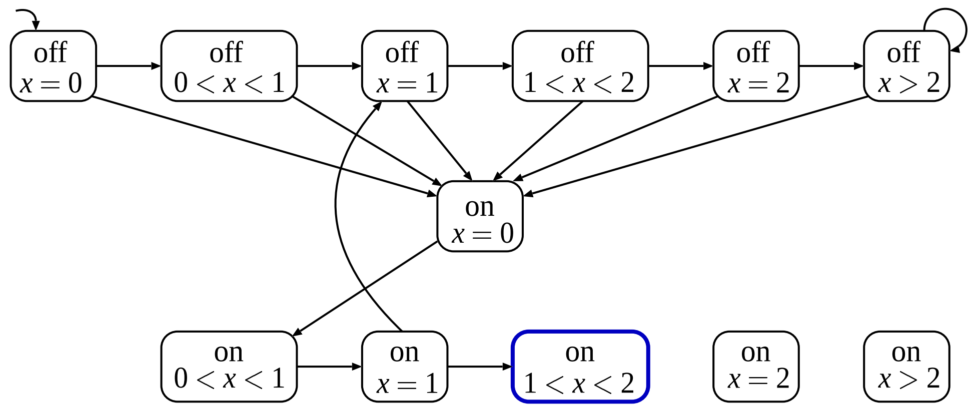
# Timelock freedom

For non-Zeno *TA*:

*TA* is timelock-free iff no reachable state in *RG*(*TA*) is terminal



# Example



# Correctness theorem

Let *TA* be a non-Zeno timed automaton and $\Phi$ a $\text{TCTL}_\diamond$ formula. Then:

$$\underbrace{TA \models \Phi}_{\text{TCTL semantics}} \quad \text{iff} \quad \underbrace{RG(TA, \Phi) \models \Phi}_{\text{CTL semantics}}$$



# Zones

- Clock constraints are *conjunctions* of atomic constraints
  - $x \prec c$ and $x - y \prec c$ for $\prec \in \{ <, \leqslant, =, \geqslant, > \}$
  - restrict to *TA* with *only conjunctive clock constraints*
  - and (as before) assume no difference clock constraints
- A *clock zone* is the set of clock valuations that satisfy a clock constraint
  - a clock zone for $g$ is the maximal set of clock valuations satisfying $g$
- Clock zone of $g$: $[\![ g ]\!] = \{ \eta \in Eval(C) \mid \eta \models g \}$
  - use $z, z'$ and so on to range over zones
- The *state zone* of $s = \langle \ell, \eta \rangle \in S(TA)$ is $\langle \ell, z \rangle$ with $\eta \in z$

# Zone automaton: intuition