Verification

Lecture 24

Bernd Finkbeiner

UNIVERSITÄT
DES
SAARLANDES

Plan for today

- Timed model checking
  - Regions
  - Zones

REVIEW: Clock equivalence

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

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

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

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

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

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

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

REVIEW: 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 $s = \langle \ell, \eta \rangle \in \mathit{TS}(\mathit{TA})$ is defined by:

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

Preservation of atomic properties

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

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

2. For $s, s' \in TS(TA)$ such that $s \cong s'$:

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

where AP' includes all atomic propositions and atomic clock constraints in TA and Φ.

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 $\forall \eta \in r$:

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

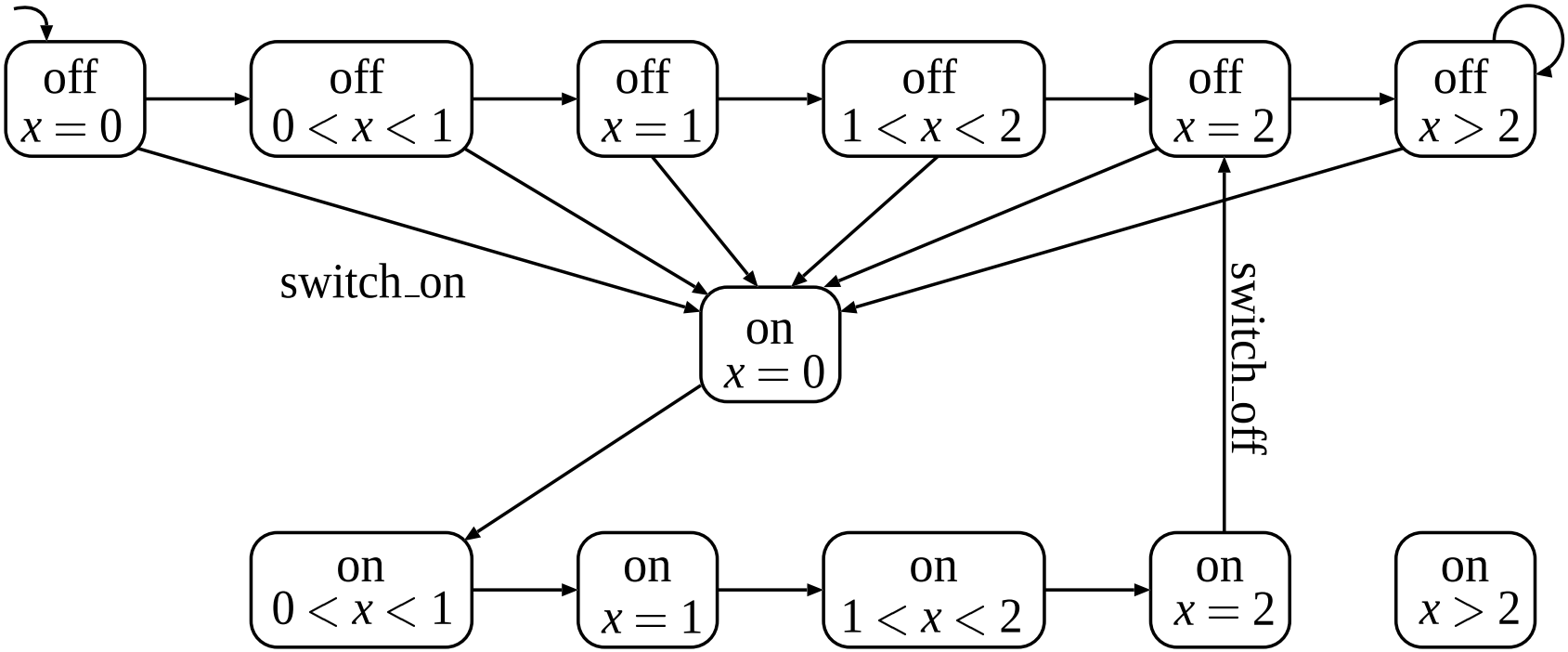
- The successor region: $\mathit{succ}(\langle \ell, r \rangle) = \langle \ell, \mathit{succ}(r) \rangle$

Region Graph

For non-Zeno $TA = (Loc, Act, C, \rightsquigarrow, Loc_0, inv, AP, L)$ with $TS(TA) = (Q, Q_0, E, L)$ let $RG(TA, \Phi) = (Q', Q'_0, E', L')$ with

- $Q' = Q/\cong = \{ [q] \mid q \in Q \}$ and $Q'_0 = \{ [q] \mid q \in Q_0 \}$,
- $L'(\langle \ell, r \rangle) = L(\ell) \cup \{ g \in AP' \setminus AP \mid r \models g \}$
- 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 $r \models inv(\ell')$;
  - Delay transitions: $\langle \ell, r \rangle \xrightarrow{\tau}' \langle \ell, succ(r) \rangle$ if $r \models inv(\ell)$ and $succ(r) \models inv(\ell)$

Example: simple light switch



Time convergence

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

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

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

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

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

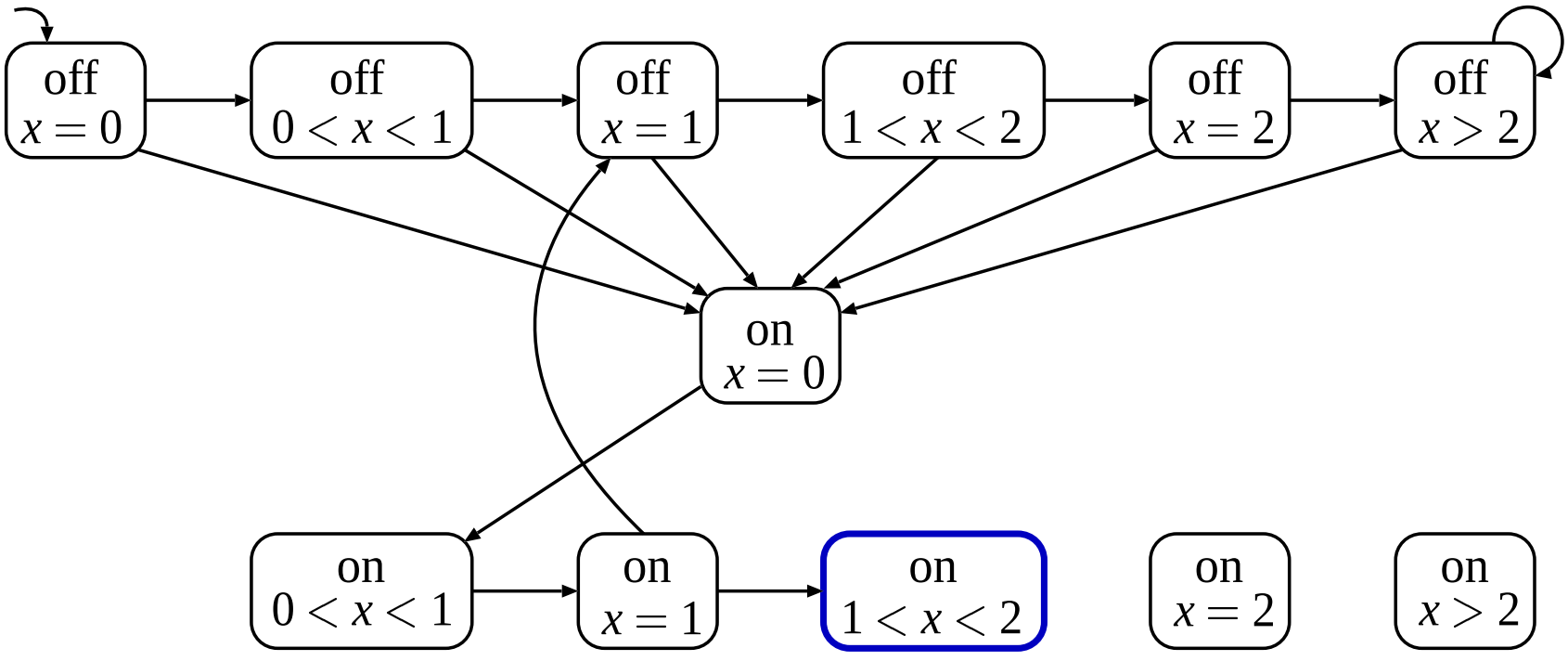
then π is time-convergent

Timelock freedom

For non-Zeno *TA*:

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

Example


off
$x = 0$
off
$0 < x < 1$
off
$x = 1$
off
$1 < x < 2$
off
$x = 2$
off
$x > 2$
on
$x = 0$
on
$0 < x < 1$
on
$x = 1$
on
$1 < x < 2$
on
$x = 2$
on
$x > 2$

Correctness theorem

Let *TA* be a non-Zeno timed automaton and Φ a TCTL$_\Diamond$ formula. Then:

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