Verification

Lecture 22

Bernd Finkbeiner

UNIVERSITÄT
DES
SAARLANDES

Plan for today

- Timed model checking

REVIEW: Timed CTL

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

$$\Phi ::= \text{true} \;\Big|\; a \;\Big|\; g \;\Big|\; \Phi \wedge \Phi \;\Big|\; \neg\Phi \;\Big|\; \mathsf{E}\,\varphi \;\Big|\; \mathsf{A}\,\varphi$$

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

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

where $J \subseteq \mathbb{R}_{\geq 0}$ 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 $n \leq m$

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

REVIEW: Semantics of TCTL

For state $s = \langle \ell, \eta \rangle$ in $TS(TA)$ 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 $(s \models \Psi)$
$s \models \mathrm{E}\,\varphi$	iff	$\pi \models \varphi$ for some $\pi \in Paths_{div}(s)$
$s \models \mathrm{A}\,\varphi$	iff	$\pi \models \varphi$ for all $\pi \in Paths_{div}(s)$

path quantification over time-divergent paths only

REVIEW: Semantics of TCTL

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

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

iff

$\exists\, i \geq 0.\, s_i{+}d \models \Psi$ for some $d \in [0, d_i]$ with $\sum_{k=0}^{i-1} d_k + d \in J$
and
$\forall j \leq i.\, s_j{+}d' \models \Phi \vee \Psi$ for every $d' \in [0, d_j]$ with $\sum_{k=0}^{j-1} d_k + d' \leq \sum_{k=0}^{i-1} d_k + d$

TCTL-semantics for timed automata

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

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

- TA satisfies TCTL-formula Φ iff Φ holds in all initial states of TA:

$$TA \models \Phi \quad \text{if and only if} \quad \forall \ell_0 \in Loc_0 . \langle \ell_0, \eta_0 \rangle \models \Phi$$

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

Timed CTL versus CTL

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

$$\underbrace{TS(TA) \models_{\text{TCTL}} \mathrm{A}\,\varphi}_{\text{TCTL semantics}} \quad \text{but} \quad \underbrace{TS(TA) \not\models_{\text{CTL}} \mathrm{A}\,\varphi}_{\text{CTL semantics}}$$

  - CTL semantics considers all paths, timed CTL only time-divergent paths
- For $\Phi = \mathrm{A\,G}\left(on \longrightarrow \mathrm{A\,F}\,\mathit{off}\right)$ and the light switch

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

  - 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 E G true
  - some time-divergent path satisfies G true, i.e., there is ≥ 1 time-divergent path
  - note: for fair CTL, the states in which a fair path starts also satisfy E G true
- *TA* is timelock-free iff $\forall s \in \mathit{Reach}(\mathit{TS}(\mathit{TA})) \colon s \models \mathrm{E\,G\,true}$
- Timelocks can thus be checked by model checking

TCTL model checking

- TCTL model-checking problem: $TA \models \Phi$ for non-Zeno TA

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

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

Eliminating timing parameters: $\text{TCTL}_\diamond$

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

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

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

  - 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 Φ:

$$\eta \cong \eta' \Rightarrow \left(\eta \vDash g \quad \text{iff} \quad \eta' \vDash g\right)$$

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

(B) Time-divergent paths originating 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, $\lfloor \eta(x) \rfloor < c$
  - $\lfloor d \rfloor = \max\{ c \in \mathbb{N} \mid c \leq d \}$ and $\mathit{frac}(d) = d - \lfloor d \rfloor$
- $\eta \models x \leq c$ 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 η and η' 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 $x \leq c$, c is a natural

Second observation

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

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

Final observation

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

$\Rightarrow$ 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 $(\eta(x) \leq c_x) \wedge (\eta'(x) \leq c_x)$

(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:

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

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

Regions

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

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

- The state region of $s = \langle \ell, \eta \rangle \in TS(TA)$ 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:

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

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

the number of state regions is $|Loc|$ times larger