Model Checking Timed Automata

Material from "Principles of Model Checking" by C. Baier and J-.P Katoen

Borzoo Bonakdarpour

School of Computer Science
University of Waterloo

November 24, 2013

Outline

1. Timed Computation Tree Logic (TCTL)

2. TCTL Model Checking

Presentation outline

1. Timed Computation Tree Logic (TCTL)

2. TCTL Model Checking

Timed Computation Tree Logic (TCTL)

Definition (Syntax of TCTL)

Formulae in TCTL are either state or path formulae. TCTL state formulae over the set AP of atomic propositions and set C of clocks are formed according to the following grammar:

$$\Phi ::= \mathit{true} \mid a \mid g \mid \Phi \wedge \Phi \mid \mathbf{E}\varphi \mid \mathbf{A}\varphi$$

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

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

where $J \subseteq \mathbb{R}_{\geq 0}$ is an interval whose bounds are natural numbers.

Timed Computation Tree Logic (TCTL)

TCTL Tempral Abbreviations

$$\Diamond^J \Phi = true\,\mathbf{U}^J\,\Phi$$

$$\mathbf{E}\Box^J \Phi = \neg \mathbf{A} \Diamond^J \neg \Phi$$

$$\mathbf{A}\Box^J \Phi = \neg \mathbf{E} \Diamond^J \neg \Phi$$

Timed Computation Tree Logic (TCTL)

TCTL Tempral Abbreviations

$$\Diamond^J \Phi = \mathit{true}\,\mathbf{U}^J\,\Phi$$

$$\mathbf{E}\Box^J \Phi = \neg\mathbf{A}\Diamond^J \neg\Phi$$

$$\mathbf{A}\Box^J \Phi = \neg\mathbf{E}\Diamond^J \neg\Phi$$

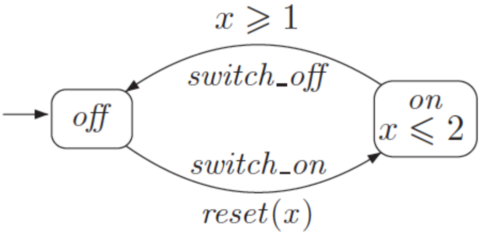
TCTL Interval Abbreviations

Intervals are often denoted by shorthand, e.g., $\Diamond^{\leq 2}$ denotes $\Diamond^{[0,2]}$ and $\Box^{>8}$ denotes $\Box^{(8,\infty)}$

Example

Example

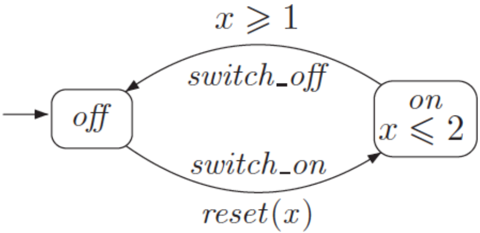
Consider the following timed automata



Example

Example

Consider the following timed automata



Example

The property:

> *"the light cannot be continously switched on for more than 2 minutes"*

is expressed by the TCTL formula:

$$\mathbf{A}\Box(on \rightarrow \mathbf{A}\Diamond^{>2}\neg on)$$

Semantics of TCTL

Definition (Satisfaction relation for TCTL)

Let $TA = (L, \Sigma, E, C, L^0, I)$ be a timed automaton, $a \in AP$, $g \in ACC(C)$, and $J \subseteq \mathbb{R}_{\geq 0}$. For state $s = \langle l, \nu \rangle$ in $TS(TA)$ and TCTL formulea Φ and Ψ, and TCTL path formula φ, the satisfaction relation $\models$ is defined for state formulae by

$s \models true$		
$s \models a$	iff	$a \in Label(l)$
$s \models g$	iff	$\nu \models g$
$s \models \neg\Phi$	iff	not $s \models \Phi$
$s \models \Phi \wedge \Psi$	iff	$(s \models \Phi) \wedge (s \models \Psi)$
$s \models \mathbf{E}\varphi$	iff	$\pi \models \varphi$ for some $\pi \in Paths_{div}(s)$
$s \models \mathbf{A}\varphi$	iff	$\pi \models \varphi$ for all $\pi \in Paths_{div}(s)$

Semantics of TCTL (cont'd)

Definition (Satisfaction relation for TCTL (con'd))

For a time-divergent path $\pi = s_0 \xrightarrow{d_0} s_1 \xrightarrow{d_1} \ldots$, the satisfaction relation $\models$ for path formulae is defined by:

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

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

$$\forall j \leq i . s_j + d' \models \Phi \vee \Psi \text{ for any } d' \in [0, d_j] \text{ with}$$

$$\sum_{k=0}^{j-1} d_k + d' \leq \sum_{k=0}^{i-1} d_k + d$$

where for $s_i = \langle l_i, \nu_i \rangle$ and $d \geq 0$, we have $s_i + d = \langle l_i, \nu_i + d \rangle$

Semantics of TCTL (cont'd)

Definition (TCTL Semantics fot Timed Automata)

A timed automaton *TA* satisfies a TCTL formula Φ iff $s_0 \models \Phi$ for each initial state s_0 of *TA*.

Presentation outline

Reduction to CTL Model Checking

Idea

Given a time automaton TA and a TCTL formula Φ, our goal is to find a finite transition system S and an CTL formula $\hat{\Phi}$, such that

$$TA \models_{TCTL} \Phi \quad \text{iff} \quad R(TA, \Phi) \models_{CTL} \hat{\Phi}$$

Input: timed automaton TA and TCTL formula Φ (both over propositions AP and clocks C.

Output: $TA \models \Phi$

$\hat{\Phi}$:= eliminate the timing parameters from Φ;

determine the clock equivalence classes under $\cong$;

construct the region transition system $TS = R(TA, \Phi)$;

apply the CTL model checking algorithm to check $TS \models \hat{\Phi}$

$TA \models \Phi$ if and only if $TS \models \hat{\Phi}$

Algorithm 1: A recipe for TCTL model checking

Elimination of Timing Parameters

Notation

For clock evaluation ν, $z \notin C$, and $d \in \mathbb{R}_{\geq 0}$, let $\nu\{z := d\}$ denote the clock valuation for $C \cup \{z\}$ that extends ν by setting z to d while keeping the value of all other clocks unchanged:

$$\nu\{z := d\}(x) = \begin{cases} \nu(x) & \text{if} \quad x \in C \\ d & \text{if} \quad x = z \end{cases} \tag{1}$$

Elimination of Timing Parameters

Notation

For clock evaluation ν, $z \notin C$, and $d \in \mathbb{R}_{\geq 0}$, let $\nu\{z := d\}$ denote the clock valuation for $C \cup \{z\}$ that extends ν by setting z to d while keeping the value of all other clocks unchanged:

$$\nu\{z := d\}(x) = \begin{cases} \nu(x) & \text{if} \quad x \in C \\ d & \text{if} \quad x = z \end{cases} \tag{1}$$

Notation

Let TA be a timed automaton over clocks C. For state $s = \langle l, \nu \rangle$ in $TS(TA)$ let $s\{z := d\}$ denote the state, $\nu\{z := d\}$. Note that $s\{z := d\}$ is a state in $TS(TA \oplus z)$ where $TA \oplus z$ is the timed automaton TA with the set of clocks $C \cup \{z\}$.

Elimination of Timing Parameters

Theorem

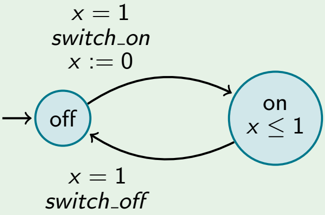
Let TA be timed automaton $(L, \Sigma, C, E, L^0, I)$, *and* $\Phi\,\mathbf{U}^J\,\Psi$ *a TCTL formula over C and AP. For clock* $z \notin C$ *and for any state s of* $TS(TA)$ *it holds that*

1. $s \models_{TCTL} \mathbf{E}(\Phi\,\mathbf{U}^J\,\Psi)$ *iff* $s\{z := 0\} \models_{CTL} \mathbf{E}((\Phi \vee \Psi)\,\mathbf{U}\,((z \in J) \wedge \Psi))$.
2. $s \models_{TCTL} \mathbf{A}(\Phi\,\mathbf{U}^J\,\Psi)$ *iff* $s\{z := 0\} \models_{CTL} \mathbf{A}((\Phi \vee \Psi)\,\mathbf{U}\,((z \in J) \wedge \Psi))$.

Example

Example

Light Switch Consider the following timed automaton TA and the TCTL formula $\Phi = \mathbf{E}\Diamond^{\leq 1} on$.

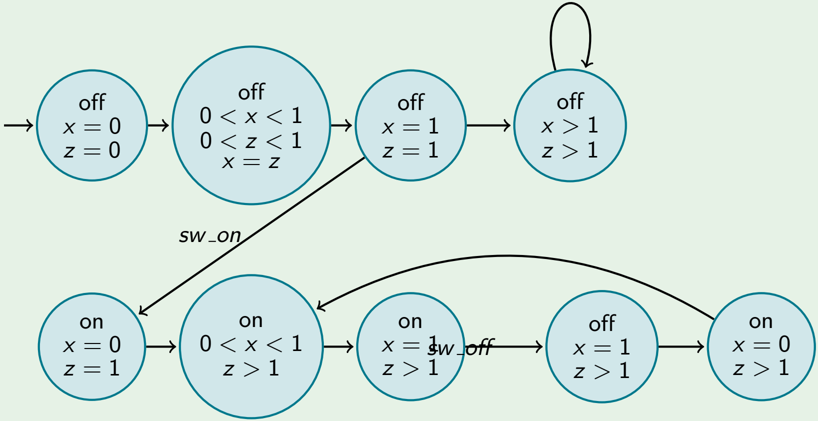


As a first step, Φ is replaced by $\hat{\Phi} = \mathbf{E}\Diamond((z \leq 1) \wedge on)$ and TA is equipped with an additional clock z. The maximal constants for the clocks x and z are $c_x = 1$ and $c_z = 1$. The region transition system $TS = R(TA \oplus z, \Phi)$ is on the next slide.

Example (con'd)

Example

Light Switch (cont'd)



Example (con'd)

Example

Light Switch (cont'd) The state region

$$\langle on, [x = 0, z = 1] \rangle \models (z \leq 1) \wedge on$$

and is reachable from the initial state region. Therefore,

$$TS \models_{CTL} \mathbf{E}\Diamond((z \leq 1) \wedge on)$$

and thus

$$TA| = \mathbf{E}\Diamond^{\leq 1} on$$

Handling Multiple Clocks

Eliminating Multiple Clocks

A simple way of treating formulae with nested time bounds is to introduce a fresh clock for each subformula.

Example

For example, the followling TCTL formula

$$\Phi = \mathbf{A}\Box^{\geq 3}\mathbf{E}\Diamond^{]1,2]} on$$

is transformed into:

$$\hat{\Phi} = \mathbf{A}\Box((z_1 \geq 3) \Rightarrow \mathbf{E}\Diamond(z_2 \in]1,2]) \wedge on))$$