Real-time Model Checking
— Timed Temporal Logics —

Nicolas MARKEY

Lav. Spécification & Vérification
CNRS & ENS Cachan – France

March 3, 2010
(Quantitative) Model checking

system:

⇒

property:

Always(safe)

model-checking algorithm

yes/no
(Quantitative) Model checking

system:

⇒

property:

⇒

always (safe)

model-checking algorithm

yes/no
(Quantitative) Model checking

system:

⇒

property:

Always (safe model-checking algorithm yes/no)

timed automata

reachability via regions

yes/no
(Quantitative) Model checking

system:

⇒

property:

⇒

timed automata

reachability via regions

yes/no

Always quantitative temporal logics
Quick reminder on untimed temporal logics

LTL \( \exists \varphi ::= \bigcirc \mid \neg \varphi \mid \varphi \land \varphi \mid X \varphi \mid \varphi U \varphi \)

CTL \( \exists \varphi ::= \bigcirc \mid \neg \varphi \mid \varphi \land \varphi \mid E \psi \mid A \psi \)

\[ \psi ::= X \varphi \mid \varphi U \varphi \]

Quick reminder on untimed temporal logics

LTL ∈ ϕ ::= ⊘ | ¬ϕ | ϕ ∧ ϕ | Xϕ | ϕ U ϕ

CTL ∈ ϕ ::= ⊘ | ¬ϕ | ϕ ∧ ϕ | Eψ | Aψ
ψ ::= Xϕ | ϕ U ϕ

Quick reminder on untimed temporal logics

LTL $\exists \varphi ::= \Diamond | \neg \varphi | \varphi \land \varphi | X \varphi | \varphi U \varphi$

CTL $\exists \varphi ::= \Diamond | \neg \varphi | \varphi \land \varphi | E\psi | A\psi$

$\psi ::= X \varphi | \varphi U \varphi$

Quick reminder on untimed temporal logics

\[
\text{LTL } \exists \varphi ::= \bigcirc \mid \neg \varphi \mid \varphi \land \varphi \mid X \varphi \mid \varphi U \varphi
\]

\[
\text{CTL } \exists \varphi ::= \bigcirc \mid \neg \varphi \mid \varphi \land \varphi \mid E\psi \mid A\psi
\]

\[
\psi ::= X \varphi \mid \varphi U \varphi
\]

Quick reminder on untimed temporal logics

\( \text{LTL} \ni \varphi ::= \bigcirc \mid \lnot \varphi \mid \varphi \land \varphi \mid X \varphi \mid \varphi U \varphi \)

\( \text{CTL} \ni \varphi ::= \bigcirc \mid \lnot \varphi \mid \varphi \land \varphi \mid E\psi \mid A\psi \)

\( \psi ::= X \varphi \mid \varphi U \varphi \)


Quick reminder on untimed temporal logics

**LTL**
\[ \varphi ::= \top | \neg \varphi | \varphi \land \varphi | X \varphi | \varphi \mathbf{U} \varphi \]

**CTL**
\[ \varphi ::= \top | \neg \varphi | \varphi \land \varphi | E \psi | A \psi \]
\[ \psi ::= X \varphi | \varphi \mathbf{U} \varphi \]

Quick reminder on untimed temporal logics

LTL \( \exists \varphi ::= \bigcirc | \neg \varphi | \varphi \land \varphi | X \varphi | \varphi U \varphi \)

CTL \( \exists \varphi ::= \bigcirc | \neg \varphi | \varphi \land \varphi | E\psi | A\psi \)

\( \psi ::= X \varphi | \varphi U \varphi \)

Quick reminder on untimed temporal logics

\[
\text{LTL \ } \exists \ \varphi ::= \bigcirc | \neg \varphi | \varphi \land \varphi | X \varphi | \varphi U \varphi
\]

\[
\text{CTL \ } \exists \ \varphi ::= \bigcirc | \neg \varphi | \varphi \land \varphi | E \psi | A \psi
\]

\[
\psi ::= X \varphi | \varphi U \varphi
\]

Quick reminder on untimed temporal logics

\[
\begin{align*}
\text{LTL} \ni \varphi & ::= \bigcirc | \neg \varphi | \varphi \land \varphi | X \varphi | \varphi U \varphi \\
\text{CTL} \ni \varphi & ::= \bigcirc | \neg \varphi | \varphi \land \varphi | E \psi | A \psi \\
\psi & ::= \varphi | X \varphi | \varphi U \varphi
\end{align*}
\]

Example

- \((\bigcirc U \bigcirc) \lor G \bigcirc\): weak until

Quick reminder on untimed temporal logics

LTL $\exists \varphi ::= \lnot \varphi \mid \varphi \land \varphi \mid X \varphi \mid \varphi U \varphi$

CTL $\exists \varphi ::= \lnot \varphi \mid \varphi \land \varphi \mid E\psi \mid A\psi$
$\psi ::= \varphi \mid X \varphi \mid \varphi U \varphi$

Example

- $(\varnothing U \varnothing) \lor G \varnothing$: weak until
- $G F \varnothing$: “infinitely often”

Quick reminder on untimed temporal logics

\[
\text{LTL} \ni \varphi ::= \top | \neg \varphi | \varphi \land \varphi | X \varphi | \varphi U \varphi
\]

\[
\text{CTL} \ni \varphi ::= \top | \neg \varphi | \varphi \land \varphi | E\psi | A\psi
\]

\[
\psi ::= \varphi | X \varphi | \varphi U \varphi
\]

Example

- \((\top U \top) \lor G \top\): weak until
- \(G F \top\): “infinitely often”
- \(A G(\top \Rightarrow A F \top)\): response property

Refs:
Quick reminder on untimed temporal logics

\[
\text{LTL } \varphi ::= \bigcirc | \neg \varphi | \varphi \land \varphi | X \varphi | \varphi U \varphi
\]

\[
\text{CTL } \varphi ::= \bigcirc | \neg \varphi | \varphi \land \varphi | E \psi | A \psi
\]

\[
\psi ::= \varphi | X \varphi | \varphi U \varphi
\]

Example

- \((\bigcirc U \bigcirc) \lor G \bigcirc\): weak until
- \(G F \bigcirc\): “infinitely often”
- \(A G(\bigcirc \Rightarrow A F \bigcirc)\): response property
- \(A(G F \bigcirc \Rightarrow G \bigcirc)\): fair runs are safe (not a CTL formula)

Outline of the talk

1 Introduction

2 Extending temporal logics with real-time constraints
   - Continuous and pointwise semantics
   - Expressiveness issues

3 Model checking timed linear-time logics
   - Undecidability of MTL and TPTL
   - Decidable fragments

4 Model checking timed branching-time logics

5 Conclusions and open problems
Outline of the talk

1. Introduction

2. Extending temporal logics with real-time constraints
   - Continuous and pointwise semantics
   - Expressiveness issues

3. Model checking timed linear-time logics
   - Undecidability of MTL and TPTL
   - Decidable fragments

4. Model checking timed branching-time logics

5. Conclusions and open problems
Extending temporal modalities with time

- decorating modalities with timing constraints:

\[ U \geq 5 \equiv \top \]

Extending temporal modalities with time

- decorating modalities with timing constraints:

\[ \xrightarrow{1.4} \xrightarrow{3.4} \xrightarrow{0.2} \xrightarrow{1.3} \xrightarrow{1.2} \models \quad \bigcirc \quad U_{=5} \quad \bigcirc \]

Refs:  
Extending temporal modalities with time

- decorating modalities with timing constraints:

\[
\begin{align*}
\text{\[1\]} \quad & 1.4 \quad 3.4 \quad 0.2 \quad 1.3 \quad 1.2 \\
\text{\[2\]} \quad & 1.4 \quad 3.5 \quad 1.8 \quad 3.6 \quad 0.9
\end{align*}
\]

\[\models \quad \text{U}_{\geq 5} \quad \text{U}_{\geq 6}\]

Extending temporal modalities with time

- decorating modalities with timing constraints:

\[ 1.4 \rightarrow 3.4 \rightarrow 0.2 \rightarrow 1.3 \rightarrow 1.2 \rightarrow \quad \models \quad \U_{\geq 5}\]

\[ 1.4 \rightarrow 3.5 \rightarrow 1.8 \rightarrow 3.6 \rightarrow 0.9 \rightarrow \quad \models \quad \F_{\geq 6} \equiv \top \U_{\geq 6}\]

Extending temporal modalities with time

- decorating modalities with timing constraints:

\[ U \geq 5 \]

\[ F \geq 6 \equiv T \quad U \geq 6 \]

\[ G \leq 7 \equiv \neg (F \leq 7 \neg \top) \]

Extending temporal modalities with time

- decorating modalities with timing constraints:

\[
\begin{align*}
\overset{1.4}{\longrightarrow} & \quad \overset{3.4}{\longrightarrow} & \quad \overset{0.2}{\longrightarrow} & \quad \overset{1.3}{\longrightarrow} & \quad \overset{1.2}{\longrightarrow} & \quad \overset{\Uparrow}{=} & \quad \overset{\mathbf{U}_{\geq 5}}{=} & \quad \overset{\mathbf{F}_{\geq 6}}{=} & \quad \overset{\equiv}{=} & \quad \top & \quad \overset{\Uparrow}{=} & \quad \overset{\mathbf{U}_{\geq 6}}{=} & \quad \overset{\mathbf{G}_{\leq 7}}{=} & \quad \equiv & \quad \neg (\mathbf{F}_{\leq 7} & \quad \neg \mathbf{U})
\end{align*}
\]

Extending temporal modalities with time

- decorating modalities with timing constraints:

\[ 1.4 \rightarrow 3.4 \rightarrow 0.2 \rightarrow 1.3 \rightarrow 1.2 \rightarrow \quad \models \quad \bigcirc \ U_{\geq 5} \bigcirc \]

\[ 1.4 \rightarrow 3.5 \rightarrow 1.8 \rightarrow 3.6 \rightarrow 0.9 \rightarrow \quad \models \quad \bigcirc \ F_{\geq 6} \bigcirc \equiv \top \ U_{\geq 6} \bigcirc \]

\[ 1.4 \rightarrow 1.7 \rightarrow 2.5 \rightarrow 0.7 \rightarrow 1.2 \rightarrow \quad \models \quad \bigcirc \ G_{\leq 7} \bigcirc \equiv \neg (F_{\leq 7} \neg \bigcirc) \bigcirc \]

- using formula clocks

Extending temporal modalities with time

- decorating modalities with timing constraints:

\[
\begin{align*}
\models U_{\geq 5} & \equiv F_{\geq 6} \equiv T U_{\geq 6} \\
\models G_{\leq 7} & \equiv \neg (F_{\leq 7} \neg \bigcirc)
\end{align*}
\]

- using formula clocks

\[
\models F(\bigcirc \land x.G(x \leq 5 \Rightarrow \neg \bigcirc))
\]

Extending temporal modalities with time

- decorating modalities with timing constraints:

\[ 1.4 \rightarrow 3.4 \rightarrow 0.2 \rightarrow 1.3 \rightarrow 1.2 \rightarrow \models \bigcirc U_{\geq 5} \bigcirc \]

\[ 1.4 \rightarrow 3.5 \rightarrow 1.8 \rightarrow 3.6 \rightarrow 0.9 \rightarrow \models \bigcirc F_{\geq 6} \bigcirc \equiv \top \bigcirc U_{\geq 6} \bigcirc \]

\[ 1.4 \rightarrow 1.7 \rightarrow 2.5 \rightarrow 0.7 \rightarrow 1.2 \rightarrow \models \bigcirc G_{\leq 7} \bigcirc \equiv \neg (\bigcirc F_{\leq 7} \neg \bigcirc) \bigcirc \]

- using formula clocks

\[ x := 0 \]

\[ x \leq 5 \]

\[ \models \bigcirc F (\bigcirc \land x, G (x \leq 5 \Rightarrow \neg \bigcirc)) \bigcirc \]


Timed words vs. timed state sequences

Example

```
Example

```

```
[Diagram with transitions labeled a, b, and c, with associated conditions on x and y.]

```

```
continuous semantics

```

```
pointwise semantics

```
Timed words vs. timed state sequences

Example

\[ a, \ x \leq 2, \ y := 0 \]
\[ b, \ y > 0, \ x := 0 \]
\[ c, \ y \leq 2, \ x := 0 \]
\[ a, \ x \geq 2, \ y := 0 \]

Pointwise semantics:
\[ x = 0, \ y = 0 \]

Continuous semantics:
\[ x = 1.5, \ y = 0.3 \]
\[ x = 2.6, \ y = 0 \]
Timed words vs. timed state sequences

Example

- **Continuous semantics**
  - $x = 1.5$
  - $y = 0$

- **Pointwise semantics**
  - $x = 1.5$
  - $y = 0$

Graph:
- **Node** $a$: $x \leq 2$, $y := 0$
- **Node** $b$: $y > 0$, $x := 0$
- **Node** $c$: $y \leq 2$, $x := 0$
- **Node** $a$: $x \geq 2$, $y := 0$
Timed words vs. timed state sequences

Example

**continuous semantics**

- $x = 0$
- $y = 1.3$

**pointwise semantics**

- $1.5$
- $2.8$
Timed words vs. timed state sequences

Example

\[ a, \quad x \leq 2 \quad y := 0 \]
\[ b, \quad y > 0 \quad x := 0 \]
\[ c, \quad y \leq 2 \quad x := 0 \]
\[ a, \quad x \geq 2 \quad y := 0 \]

**Continuous semantics**

\[ x = 2.6 \]
\[ y = 0 \]

**Pointwise semantics**

\[ a \quad 1.5 \quad b \quad 2.8 \quad a \quad 5.4 \]
Timed words vs. timed state sequences

Example

Continuous semantics

Pointwise semantics
Timed logics in the pointwise framework

**Definition**

MTL \( \in \varphi ::= \bigcirc \mid \neg \varphi \mid \varphi \lor \varphi \mid \varphi \cup_I \varphi \)

where \( \bigcirc \) ranges over \( \{\bigcirc, \bigcirc, \ldots\} \) and \( I \) is an interval with bounds in \( \mathbb{Q}^+ \cup \{+\infty\} \).
**Timed logics in the pointwise framework**

<table>
<thead>
<tr>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pointwise semantics of MTL:</strong> over $\pi = (w_i, t_i)_i$ with $t_0 = 0$:</td>
</tr>
<tr>
<td>- $\pi, i \models \varphi \mathbin{U}_I \psi$ iff there exists some $j &gt; 0$ s.t.</td>
</tr>
<tr>
<td>- $\pi, i + j \models \psi$,</td>
</tr>
<tr>
<td>- $\pi, i + k \models \varphi$ for all $0 &lt; k &lt; j$,</td>
</tr>
<tr>
<td>- $t_{i+j} - t_i \in I$.</td>
</tr>
</tbody>
</table>
Timed logics in the pointwise framework

**Definition**

Pointwise semantics of MTL: over $\pi = (w_i, t_i)_i$ with $t_0 = 0$:

- $\pi, i \models \varphi \mathbf{U}_1 \psi$ iff there exists some $j > 0$ s.t.
  - $\pi, i + j \models \psi$,
  - $\pi, i + k \models \varphi$ for all $0 < k < j$,
  - $t_{i+j} - t_i \in I$.

**Example**

\[
\begin{align*}
0 & \quad | & \quad 1 & \quad | & \quad 2 \\
\text{(init, 0)} & \quad | & \quad (a, 0.6) & \quad | & \quad (a, 1.2) & \quad | & \quad (c, 2.1) & \quad | & \quad a \mathbf{U}_{[2,3]} c
\end{align*}
\]
**Definition**

Pointwise semantics of MTL: over $\pi = (w_i, t_i)_i$ with $t_0 = 0$:

- $\pi, i \models \varphi \mathbf{U}_l \psi$ iff there exists some $j > 0$ s.t.
  - $\pi, i + j \models \psi$,
  - $\pi, i + k \models \varphi$ for all $0 < k < j$,
  - $t_{i+j} - t_i \in l$.

**Example**

$\mathbf{F}(b \land \bot \mathbf{U}_{[1,1]} a)$

(init,0)  (b,0.8)  (b,1.3)  (a,2.3)
Timed logics in the pointwise framework

**Definition**

Pointwise semantics of MTL: over $\pi = (w_i, t_i)_i$ with $t_0 = 0$:

- $\pi, i \models \varphi U_1 \psi$ iff there exists some $j > 0$ s.t.
  - $\pi, i + j \models \psi$,
  - $\pi, i + k \models \varphi$ for all $0 < k < j$,
  - $t_{i+j} - t_i \in I$.

**Example**

![Example Diagram]

$F[2,2]c$
Timed logics in the pointwise framework

**Definition**

Pointwise semantics of MTL: over $\pi = (w_i, t_i)_i$ with $t_0 = 0$:

- $\pi, i \models \varphi \mathbf{U}_1 \psi$ iff there exists some $j > 0$ s.t.
  - $\pi, i + j \models \psi$,
  - $\pi, i + k \models \varphi$ for all $0 < k < j$,
  - $t_{i+j} - t_i \in \mathbb{I}$.

**Example**

\[
\begin{align*}
&0 & 1 & 2 \\
& (\text{init}, 0) & (b, 0.9) & (c, 2) \\
& 0 & 1 & 2 \\
& F[2,2] C \overset{\text{def}}{=} F_{=2} C
\end{align*}
\]
Timed logics in the pointwise framework

**Definition**

Pointwise semantics of MTL: over $\pi = (w_i, t_i)_i$ with $t_0 = 0$:

- $\pi, i \models \varphi \mathbin{U}_j \psi$ iff there exists some $j > 0$ s.t.
  - $\pi, i + j \models \psi$,
  - $\pi, i + k \models \varphi$ for all $0 < k < j$,
  - $t_{i+j} - t_i \in I$.

**Example**

$\begin{align*}
0 & \quad 1 \quad 2 \\
\text{init,0} & \quad (b,0.9) & \quad (c,2) \\
\end{align*}$

$F_{[2,2]} c \not\equiv F_{=1} F_{=1} c$
Timed logics in the pointwise framework

Definition

\( \text{TPTL} \models \varphi ::= \bigcirc \mid x \sim c \mid \neg \varphi \mid \varphi \lor \varphi \mid \varphi \land \varphi \mid x. \varphi \)

where \( \bigcirc \) ranges over \{\bigcirc, \bigcirc, \ldots\}, \( x \) ranges over a set of formula clocks, \( c \in \mathbb{Q}^+ \) and \( \sim \in \{<, \leq, =, \geq, >\} \).
Timed logics in the pointwise framework

Definition

Pointwise semantics of TPTL: over $\pi = (w_i, t_i)_i$ with $t_0 = 0$, under some clock valuation $\tau$: :

- $\pi, i, \tau \models x \sim c$ iff $\tau(x) \sim c$
Timed logics in the pointwise framework

Definition

Pointwise semantics of TPTL: over \( \pi = (w_i, t_i)_i \) with \( t_0 = 0 \), under some clock valuation \( \tau \): :

- \( \pi, i, \tau \models x \sim c \) iff \( \tau(x) \sim c \)
- \( \pi, i, \tau \models x. \varphi \) iff \( \pi, i, \tau[x\leftarrow 0] \models \varphi \)
Timed logics in the pointwise framework

**Definition**

Pointwise semantics of TPTL: over $\pi = (w_i, t_i)_i$ with $t_0 = 0$, under some clock valuation $\tau$: 

- $\pi, i, \tau \models x \sim c$ iff $\tau(x) \sim c$
- $\pi, i, \tau \models x. \varphi$ iff $\pi, i, \tau[x \leftarrow 0] \models \varphi$
- $\pi, i, \tau \models \varphi \mathbf{U} \psi$ iff there exists some $j > 0$ s.t.
  - $\pi, i + j, \tau + t_{i+j} - t_i \models \psi$,
  - $\pi, i + k, \tau + t_{i+k} - t_i \models \varphi$ for all $0 < k < j$. 
Timed logics in the pointwise framework

**Definition**

Pointwise semantics of TPTL: over $\pi = (w_i, t_i)_i$ with $t_0 = 0$, under some clock valuation $\tau$: :

- $\pi, i, \tau \models x \sim c$ iff $\tau(x) \sim c$
- $\pi, i, \tau \models x. \varphi$ iff $\pi, i, \tau[x\leftarrow 0] \models \varphi$
- $\pi, i, \tau \models \varphi \mathbf{U} \psi$ iff there exists some $j > 0$ s.t.
  - $\pi, i + j, \tau + t_{i+j} - t_i \models \psi$,
  - $\pi, i + k, \tau + t_{i+k} - t_i \models \varphi$ for all $0 < k < j$.

**Example**

\[ x.(a \mathbf{U} (c \land x \in [2, 3])) \]

0 \quad 1 \quad 2

\((init,0)\) \quad \((a,0.6)\) \quad \((a,1.2)\) \quad \((c,2.1)\)
Timed logics in the pointwise framework

Definition

Pointwise semantics of TPTL: over $\pi = (w_i, t_i)_i$ with $t_0 = 0$, under some clock valuation $\tau$: :

- $\pi, i, \tau \models x \sim c$ iff $\tau(x) \sim c$
- $\pi, i, \tau \models x. \varphi$ iff $\pi, i, \tau[x\leftarrow 0] \models \varphi$
- $\pi, i, \tau \models \varphi \mathbf{U} \psi$ iff there exists some $j > 0$ s.t.
  - $\pi, i + j, \tau + t_{i+j} - t_i \models \psi$,
  - $\pi, i + k, \tau + t_{i+k} - t_i \models \varphi$ for all $0 < k < j$.

Example

$$F(b \land x.(\bot \mathbf{U} (a \land x = 1)))$$

(init,0) (a,0.6) (b,1.1) (a,2.1)
Timed logics in the pointwise framework

**Definition**

Pointwise semantics of TPTL: over \( \pi = (w_i, t_i)_i \) with \( t_0 = 0 \), under some clock valuation \( \tau: \)

- \( \pi, i, \tau \models x \sim c \) iff \( \tau(x) \sim c \)
- \( \pi, i, \tau \models x. \varphi \) iff \( \pi, i, \tau[x \leftarrow 0] \models \varphi \)
- \( \pi, i, \tau \models \varphi \mathbf{U} \psi \) iff there exists some \( j > 0 \) s.t.
  - \( \pi, i + j, \tau + t_{i+j} - t_i \models \psi \),
  - \( \pi, i + k, \tau + t_{i+k} - t_i \models \varphi \) for all \( 0 < k < j \).

**Example**

\( x. \mathbf{F}(a \land \mathbf{F}(b \land x \leq 1)) \)

\[
\begin{array}{cccc}
0 & 1 & 2 \\
\text{(init,0)} & \text{(a,0.5)} & \text{(b,0.9)} & \text{(c,2)}
\end{array}
\]
Timed logics in the continuous framework

Definition

Continuous semantics of MTL: over $\pi : \mathbb{R}^+ \rightarrow \{\bigcirc, \bigcirc, \ldots\}$:

- $\pi, t \models \varphi \mathbf{U} I \psi$ iff there exists some $u > 0$ s.t.
  - $\pi, t + u \models \psi$,
  - $\pi, t + v \models \varphi$ for all $0 < v < u$,
  - $u \in I$. 

Timed logics in the continuous framework

Definition

Continuous semantics of MTL: over $\pi : \mathbb{R}^+ \rightarrow \{\bigcirc, \bigcirc, \ldots\}$:

- $\pi, t \models \varphi \mathcal{U} I \psi$ iff there exists some $u > 0$ s.t.
  - $\pi, t + u \models \psi$,
  - $\pi, t + v \models \varphi$ for all $0 < v < u$,
  - $u \in I$.

- $\pi, t \models p$ iff $p \in \pi(t)$
Timed logics in the continuous framework

Definition

Continuous semantics of MTL: over $\pi : \mathbb{R}^+ \to \{\bigcirc, \diamond, \ldots\}$:

- $\pi, t \models \varphi \mathbf{U} \psi$ iff there exists some $u > 0$ s.t.
  - $\pi, t + u \models \psi$,
  - $\pi, t + v \models \varphi$ for all $0 < v < u$,
  - $u \in I$.

- $\pi, t \models p$ iff $p \in \pi(t)$

Example

```
0 1 2
(off \ or \ on) U_{\leq 2} (on)
```
Timed logics in the continuous framework

Definition

Continuous semantics of MTL: over $\pi : \mathbb{R}^+ \rightarrow \{\emptyset, \Diamond, \ldots\}$:

- $\pi, t \models \varphi U I \psi$ iff there exists some $u > 0$ s.t.
  - $\pi, t + u \models \psi$,
  - $\pi, t + v \models \varphi$ for all $0 < v < u$,
  - $u \in I$.

- $\pi, t \models p$ iff $p \in \pi(t)$

Example

Diagram showing a transition from 0 to 1 to 2 with $F_{\leq 2}$.
Timed logics in the continuous framework

**Definition**

Continuous semantics of MTL: over \( \pi : \mathbb{R}^+ \rightarrow \{\bigcirc, \circ, \ldots\} \):

- \( \pi, t \models \varphi U I \psi \) iff there exists some \( u > 0 \) s.t.
  - \( \pi, t + u \models \psi \),
  - \( \pi, t + v \models \varphi \) for all \( 0 < v < u \),
  - \( u \in I \).

- \( \pi, t \models p \) iff \( p \in \pi(t) \)

**Example**

\[
\begin{array}{ccc}
0 & 1 & 2 \\
\hline
\text{F} = 2 \bigcirc & \equiv & \text{F} = 1(\text{F} = 1 \bigcirc)
\end{array}
\]
Timed logics in the continuous framework

Definition

Continuous semantics of TPTL: over \( \pi : \mathbb{R}^+ \rightarrow \{\circ, \bullet, \ldots\} \):

- \( \pi, t, \tau \models x \sim c \iff \tau(x) \sim c \)
Timed logics in the continuous framework

Definition

Continuous semantics of TPTL: over $\pi : \mathbb{R}^+ \rightarrow \{\bigcirc, \bigcirc, \ldots\}$:

- $\pi, t, \tau \models x \sim c$ iff $\tau(x) \sim c$
- $\pi, t, \tau \models x. \varphi$ iff $\pi, i, \tau[x \leftarrow 0] \models \varphi$
Timed logics in the continuous framework

Definition

Continuous semantics of TPTL: over $\pi: \mathbb{R}^+ \rightarrow \{\bigcirc, \bigcirc, \ldots\}$:

- $\pi, t, \tau \models x \sim c$ iff $\tau(x) \sim c$
- $\pi, t, \tau \models x. \varphi$ iff $\pi, i, \tau[x\leftarrow 0] \models \varphi$
- $\pi, t, \tau \models \varphi \mathsf{U} \psi$ iff there exists some $u > 0$ s.t.
  - $\pi, t + u, \tau + u - t \models \psi$,
  - $\pi, i + k, \tau + v - t \models \varphi$ for all $0 < v < u$. 
Definition

Continuous semantics of TPTL: over $\pi : \mathbb{R}^+ \to \{\bigcirc, \bigcirc, \ldots\}$:

- $\pi, t, \tau \models x \sim c$ iff $\tau(x) \sim c$
- $\pi, t, \tau \models x. \varphi$ iff $\pi, i, \tau[x \leftarrow 0] \models \varphi$
- $\pi, t, \tau \models \varphi \mathbf{U} \psi$ iff there exists some $u > 0$ s.t.
  - $\pi, t + u, \tau + u - t \models \psi$,
  - $\pi, i + k, \tau + v - t \models \varphi$ for all $0 < v < u$.

Example

$0 \quad 1 \quad 2 \quad \leftarrow \quad x.((\bigcirc \lor \bigcirc) \mathbf{U} (\bigcirc \land x \leq 2))$
Timed logics in the continuous framework

Definition

Continuous semantics of TPTL: over $\pi : \mathbb{R}^+ \rightarrow \{\bigcirc, \bigcirc, \ldots\}$:

- $\pi, t, \tau \models x \sim c$ iff $\tau(x) \sim c$
- $\pi, t, \tau \models x. \varphi$ iff $\pi, i, \tau[x \leftarrow 0] \models \varphi$
- $\pi, t, \tau \models \varphi \U \psi$ iff there exists some $u > 0$ s.t.
  - $\pi, t + u, \tau + u - t \models \psi$,
  - $\pi, i + k, \tau + v - t \models \varphi$ for all $0 < v < u$.

Example

\[ x. F(\bigcirc \land F(\bigcirc \land x \leq 2)) \]
Relative expressiveness of TPTL and MTL

Lemma

MTL can be translated into TPTL.

Proof.

\[ \forall \ U I \ \psi \ \equiv \ \exists \ x. \ \forall \ U (\psi \ \land \ x \in I). \]
Relative expressiveness of TPTL and MTL

Lemma

**MTL can be translated into TPTL.**

*Proof.*

\[ \varphi \ U_I \psi \equiv x. \varphi \ U (\psi \land x \in I). \]

Conversely, consider the following TPTL formula:

\[ G[\bigcirc \Rightarrow x. F(\bigcirc \land F(\bigcirc \land x \leq 2))] \]

It characterizes the following pattern:
Relative expressiveness of TPTL and MTL

\[ \text{G} \left[ \text{G} \Rightarrow x. \text{F}(\text{G} \land \text{F}(\text{G} \land x \leq 2)) \right]. \]

Remark
This translation is only valid in the continuous semantics.
Relative expressiveness of TPTL and MTL

\[ \text{G} \left[ \varnothing \Rightarrow x \cdot F(\varnothing \land F(\varnothing \land x \leq 2)) \right]. \]
Relative expressiveness of TPTL and MTL

\[
G \left[ \begin{array}{c} \text{green} \\
\text{red} \\
\text{blue} \\
\end{array} \right] \Rightarrow \exists x. F(\text{red} \land F(\text{blue} \land x \leq 2))
\]
Relative expressiveness of TPTL and MTL

\[ G[\mathbb{G} \Rightarrow x. F(\mathbb{R} \land F(\mathbb{B} \land x \leq 2))] . \]

\[ G \mathbb{G} \Rightarrow \begin{cases} F_{[0,1]} \mathbb{R} \land F_{[1,2]} \mathbb{B} \\ \lor \\ F_{[0,1]}(\mathbb{R} \land F_{[0,1]} \mathbb{B}) \end{cases} \]

Remark: This translation is only valid in the continuous semantics.
Relative expressiveness of TPTL and MTL

\[ G[\mathbb{G}] \Rightarrow x. F(\mathbb{G} \land F(\mathbb{G} \land x \leq 2)). \]

\[ G \mathbb{G} \Rightarrow \begin{cases} F_{[0,1]} \mathbb{G} \land F_{[1,2]} \mathbb{G} \\ \lor \\ F_{[0,1]}(\mathbb{G} \land F_{[0,1]} \mathbb{G}) \\ \lor \\ F_{[0,1]}(F_{(0,1)} \mathbb{G} \land F_{=1} \mathbb{G}) \end{cases} \]

Remark
This translation is only valid in the continuous semantics
Relative expressiveness of TPTL and MTL

\[ G[\bigcirc \Rightarrow \ x. \ F(\bigcirc \land F(\bigcirc \land x \leq 2))]. \]

Remark
This translation is only valid in the continuous semantics
Relative expressiveness of TPTL and MTL

Theorem

*TPTL is strictly more expressive than MTL.*

Theorem

\textit{TPTL is strictly more expressive than MTL.}

\textbf{Proof.}

- In the pointwise semantics:

\[ G[\diamond \Rightarrow x. F(\diamond \land F(\diamond \land x \leq 2))] \]

cannot be expressed in MTL.

- In both semantics:

\[ \varphi = x. F(\diamond \land x \leq 1 \land G(x \leq 1 \Rightarrow \neg \diamond)) \]

cannot be expressed in MTL.

Outline of the talk

1. Introduction

2. Extending temporal logics with real-time constraints
   - Continuous and pointwise semantics
   - Expressiveness issues

3. Model checking timed linear-time logics
   - Undecidability of MTL and TPTL
   - Decidable fragments

4. Model checking timed branching-time logics

5. Conclusions and open problems
MTL model-checking

<table>
<thead>
<tr>
<th>Theorem</th>
</tr>
</thead>
<tbody>
<tr>
<td>**MTL model-checking and satisfiability are **undecidable <strong>under the continuous semantics.</strong></td>
</tr>
</tbody>
</table>

MTL model-checking

Theorem

MTL model-checking and satisfiability are **undecidable** under the 
continuous semantics.

Proof.

Encode the halting problem of a Turing machine:

One time-unit = one configuration of the Turing machine

MTL model-checking

Theorem

MTL model-checking and satisfiability are undecidable under the continuous semantics.

Proof.

Encode the halting problem of a Turing machine:

One time-unit = one configuration of the Turing machine

MTL model-checking

Theorem

MTL model-checking and satisfiability are **undecidable** under the continuous semantics.

Proof.

Encode the halting problem of a Turing machine:

One time-unit = one configuration of the Turing machine

MTL model-checking

**Theorem**

MTL model-checking and satisfiability are *undecidable* under the continuous semantics.

**Proof.**

Encode the halting problem of a Turing machine:

One time-unit = one configuration of the Turing machine

\[ G \left( (\square \land \neg (\square \ U \ \lozenge) \land \neg (\neg \square \land \neg \lozenge) \ U \ \lozenge) \right) \iff F_{=1} \lozenge \land \ldots \]

MTL model-checking

Remark

This reduction requires continuous semantics, or the use of past-time modalities:

\[ n \quad n+1 \quad n+2 \]

MTL model-checking

Remark

This reduction requires continuous semantics, or the use of past-time modalities:

![Diagram of time intervals and indices]

Theorem

Under pointwise semantics, MTL model-checking and satisfiability are undecidable over infinite timed words; are decidable (with non-primitive recursive complexity) over finite timed words.

Refs:
MTL model-checking

Remark

This reduction requires continuous semantics, or the use of past-time modalities:

=1

=1

“insertion errors”

MTL model-checking

Remark
This reduction requires continuous semantics, or the use of past-time modalities:

Theorem
Under pointwise semantics, MTL model-checking and satisfiability
- are undecidable over infinite timed words;
- are decidable (with non-primitive recursive complexity) over finite timed words.

Metric Interval Temporal Logic

**Definition**

MITL is the fragment of MTL where punctuality is not allowed:

\[
\text{MITL} \ni \varphi ::= \bigcirc | \neg \varphi | \varphi \lor \varphi | \varphi U I \varphi
\]

where \( \bigcirc \) ranges over \( \{\bigcirc, \infty, \ldots\} \) and \( I \) is a non-punctual interval with bounds in \( \mathbb{Q}^+ \cup \{+\infty\} \).

---

Metric Interval Temporal Logic

Definition

MITL is the fragment of MTL where punctuality is not allowed:

$$\text{MITL} \ni \varphi ::= \bigcirc \mid \neg \varphi \mid \varphi \lor \varphi \mid \varphi \Uparrow I, \varphi$$

where $\bigcirc$ ranges over $\{\bigcirc, \bigotimes, \ldots\}$ and $I$ is a non-punctual interval with bounds in $\mathbb{Q}^+ \cup \{+\infty\}$.

Example

- $G(\bigcirc \Rightarrow F_{[1,2]} \bigcirc)$ is an MITL formula;
- $G(\bigcirc \Rightarrow F_{=1} \bigcirc)$ is not.

Metric Interval Temporal Logic

Definition

MITL is the fragment of MTL where punctuality is not allowed:

\[ \text{MITL} \ni \varphi ::= \bigcirc | \neg \varphi | \varphi \lor \varphi | \varphi \ U I \varphi \]

where \( \bigcirc \) ranges over \( \{\bigcirc, \square, \ldots\} \) and \( I \) is a non-punctual interval with bounds in \( \mathbb{Q}^+ \cup \{+\infty\} \).

Example

- \( G(\bigcirc \Rightarrow F_{[1,2]} \bigcirc) \) is an MITL formula;
- \( G(\square \Rightarrow F_{=1} \bigcirc) \) is not.

Theorem

**MITL model checking and satisfiability are EXPSPACE-complete.**

**Definition**

**CoFlatMTL** is the fragment of MTL defined as:

\[
\text{CoFlatMTL} \ni \phi ::= \bigcirc | \neg \bigcirc | \phi \lor \phi | \phi \land \phi |
\]

\[
\phi \mathbf{U}_I \phi | \phi \mathbf{U}_J \psi | \phi \mathbf{R}_I \phi | \psi \mathbf{R}_J \phi
\]

where

- \( \bigcirc \) ranges over \( \{\bigcirc, \oplus, \ldots\} \),
- \( I \) ranges over *bounded* intervals with bounds in \( \mathbb{Q} \),
- \( J \) ranges over intervals with bounds in \( \mathbb{Q} \cup \{+\infty\} \), and
- \( \psi \) ranges over MITL.

(Co)Flat MTL

Definition

CoFlatMTL is the fragment of MTL defined as:

\[ \text{CoFlatMTL} \ni \varphi ::= \bigcirc | \neg \bigcirc | \varphi \lor \varphi | \varphi \land \varphi |
\]

\[ \varphi U_I \varphi | \varphi U_J \psi | \varphi R_I \varphi | \psi R_J \varphi \]

Remark

CoFlatMTL is not closed under negation.

(Co)Flat MTL

Definition

CoFlatMTL is the fragment of MTL defined as:

\[ \text{CoFlatMTL} \ni \varphi ::= \Diamond | \neg \Diamond | \varphi \lor \varphi | \varphi \land \varphi | \varphi \mathbin{U} I \varphi | \varphi \mathbin{U} J \psi | \varphi \mathbin{R} I \varphi | \psi \mathbin{R} J \varphi \]

Remark

CoFlatMTL is not closed under negation.

Example

- \( G(\Diamond \Rightarrow F_{=1} \Diamond) \) is in CoFlatMTL.
- \( F(\Diamond \land G_{=1} \Diamond) \) is in FlatMTL, but not in CoFlatMTL.

CoFlatMTL

Definition
CoFlatMTL is the fragment of MTL defined as:

CoFlatMTL ∋ φ ::= ⊗ | ¬ ⊗ | φ ∨ φ | φ ∧ φ |
φ U_I φ | φ U_J ψ | φ R_I φ | ψ R_J φ

Remark
CoFlatMTL is not closed under negation.

Theorem
CoFlatMTL model-checking is EXPSPACE-complete.
CoFlatMTL satisfiability is undecidable.

Outline of the talk

1 Introduction

2 Extending temporal logics with real-time constraints
   - Continuous and pointwise semantics
   - Expressiveness issues

3 Model checking timed linear-time logics
   - Undecidability of MTL and TPTL
   - Decidable fragments

4 Model checking timed branching-time logics

5 Conclusions and open problems
Branching-time logics with timing constraints – syntax

Definition

\[
TCTL \models \varphi ::= \bigcirc | \neg \varphi | \varphi \land \varphi | E\varphi \ U_{\sim c} \varphi | A\varphi \ U_{\sim c} \varphi
\]

where \( \bigcirc \in \{\bigcirc, \bigcirc, \bigcirc, ...\} \), \( \sim \in \{\leq, <, =, >, \geq\} \) and \( c \in \mathbb{N} \).
### Definition

\[ \text{TCTL} \ni \phi ::= \Box | \neg \phi | \phi \land \phi | E \phi U_{\sim c} \phi | A \phi U_{\sim c} \phi \]

where \( \Box \in \{\Box, \Diamond, \circ, \ldots\} \), \( \sim \in \{\leq, <, =, >, \geq\} \) and \( c \in \mathbb{N} \).

### Example

\[ A G(\Box \Rightarrow E F_{\leq 5} \circ) \]
Branching-time logics with timing constraints – syntax

Definition

\[
TCTL \ni \varphi ::= \Diamond \varphi \mid \neg \varphi \mid \varphi \land \varphi \mid E \varphi U_{\sim c} \varphi \mid A \varphi U_{\sim c} \varphi
\]

where \( \Diamond \in \{ \Box, \Diamond, \lozenge, \ldots \} \), \( \sim \in \{ \leq, <, =, >, \geq \} \) and \( c \in \mathbb{N} \).

Example

- \( A G(\Box \Rightarrow E F_{\leq 5} \Diamond) \)
- \( A F(A G_{\leq 5} \lozenge) \)

Branching-time logics with timing constraints – semantics

Definition

The semantics of TCTL is defined as follows: let \( \bigcirc \) be a location and \( \nu \) be a clock valuation.

- \( \bigcirc, \nu \models E(\bigcirc \mathbin{\bigcirc} U_{\sim c} \bigcirc) \) iff there is a run from \( (\bigcirc, \nu) \) such that

  \[
  \nu \mathbin{\bigcirc} \nu', \nu \models A(\bigcirc \mathbin{\bigcirc} U_{\sim c} \bigcirc)
  \]

is defined similarly.
Definition

The semantics of TCTL is defined as follows: let $\bigcirc$ be a location and $\nu$ be a clock valuation.

- $\bigcirc, \nu \models \text{E}(\bigcirc \mathbf{U}_{\sim c} \bigcirc)$ iff there is a run from $(\bigcirc, \nu)$ such that $\nu \sim c, \nu \models A(\bigcirc \mathbf{U}_{\sim c} \bigcirc)$ is defined similarly.

Remark

We could also define a pointwise semantics:
Branching-time logics with timing constraints – semantics

Example

\[
\begin{align*}
\text{Example} & \\
& y \leq 2, \quad x \geq 3 \\
& x \leq 2, \quad y := 0 \\
& x \leq 3, \quad y := 0 \\
& \bullet \quad (x = 1.2, y = 0.4) \models E \quad U_{\geq 1} \\
& \bullet \quad (x = 1.2, y = 0.4) \models A \quad G \\
& \bullet \quad (x = 1.2, y = 0.4) \models E \quad (E \ F = 1) \quad U = 3
\end{align*}
\]
Branching-time logics with timing constraints – semantics

Example

\[
\begin{align*}
& y \leq 2, x \geq 3 \\
& x \leq 2, x := 0 \\
& x \leq 3, y := 0
\end{align*}
\]

\[\begin{align*}
& \bullet \quad \bigcirc, \left( x = 1.2 \right) \models \text{E} \quad \bigcirc \quad \text{U}_{\geq 1} \quad \bigcirc \\
& \bullet \quad \bigcirc, \left( x = 1.2 \right) \models \text{AG} \quad \neg \quad \bigcirc \\
& \bullet \quad \bigcirc, \left( x = 0 \right) \models \text{EF}_1 \quad \bigcirc \quad \text{U}_{= 3} \quad \bigcirc
\end{align*}\]
TCTL model checking

Lemma

Let $\bigcirc$ be a location and $\varphi$ be a TCTL formula. For any two valuations $v$ and $v'$ that belong to the same region,

$$
\text{\bigcirc}, v \models \varphi \iff \text{\bigcirc}, v' \models \varphi.
$$

TCTL model checking

Lemma

Let \( \bigcirc \) be a location and \( \varphi \) be a TCTL formula. For any two valuations \( v \) and \( v' \) that belong to the same region,

\[
\begin{align*}
\bigcirc, v \models \varphi & \iff \bigcirc, v' \models \varphi.
\end{align*}
\]

Proof.

By induction on \( \varphi \).

**Lemma**

Let $\bigcirc$ be a location and $\varphi$ be a **TCTL formula**. For any two valuations $v$ and $v'$ that belong to the **same region**, 

\[ \bigcirc, v \models \varphi \iff \bigcirc, v' \models \varphi. \]

**Proof.**

By induction on $\varphi$.

**Theorem**

**TCTL model-checking** is **PSPACE-complete**.
TCTL model checking

Lemma

Let $\bigcirc$ be a location and $\varphi$ be a TCTL formula. For any two valuations $v$ and $v'$ that belong to the same region,

$$\bigcirc, v \models \varphi \iff \bigcirc, v' \models \varphi.$$ 

Proof.

By induction on $\varphi$. 

$\blacksquare$

Theorem

TCTL model-checking is PSPACE-complete.

Proof.

Space-efficient CTL labelling algorithm on the region graph. 

$\blacksquare$

Outline of the talk

1. Introduction

2. Extending temporal logics with real-time constraints
   - Continuous and pointwise semantics
   - Expressiveness issues

3. Model checking timed linear-time logics
   - Undecidability of MTL and TPTL
   - Decidable fragments

4. Model checking timed branching-time logics

5. Conclusions and open problems
Conclusions and perspectives

Real-time temporal logics have been much studied:
Conclusions and perspectives

Real-time temporal logics have been much studied:

- **linear-time:**
  - natural extensions of LTL are *undecidable*;
  - several restrictions lead to *decidability*;
  - however, model-checking linear-time logics is *hard*;
  - no implementation exists.

- Branching-time:
  - TCTL model-checking is in PSPACE;
  - can be made efficient in practice;
  - implemented in several tools (Uppaal, Kronos, ...)

Hot topics in real-time temporal logic model-checking:
- symbolic algorithms for linear-time temporal logics
- robust model-checking.
Conclusions and perspectives

Real-time temporal logics have been much studied:

- **linear-time:**
  - natural extensions of LTL are **undecidable**;
  - several restrictions lead to **decidability**;
  - however, model-checking linear-time logics **is hard**;
  - **no implementation** exists.

- **branching-time:**
  - TCTL model-checking is in PSPACE;
  - can be made **efficient in practice**;
  - implemented in **several tools** (Uppaal, Kronos, ...)

Hot topics in real-time temporal logic model-checking:
- symbolic algorithms for linear-time temporal logics
- robust model-checking
Conclusions and perspectives

Real-time temporal logics have been much studied:

- **linear-time:**
  - natural extensions of LTL are **undecidable**;
  - several restrictions lead to decidability;
  - however, model-checking linear-time logics is **hard**;
  - no implementation exists.

- **branching-time:**
  - TCTL model-checking is in PSPACE;
  - can be made **efficient in practice**;
  - implemented in several tools (Uppaal, Kronos, ...)

**Hot topics** in real-time temporal logic model-checking:

- **symbolic algorithms** for linear-time temporal logics;
- **robust** model-checking.