Temporal Reasoning on Incomplete Paths

Dana Fisman
Hillel Kugler
Temporal Reasoning on Incomplete Paths

Dana Fisman
Hillel Kugler
History

1977: LTL over infinite paths

1992: LTL also over finite paths

2003: LTL also over truncated paths

2018: LTL also over incomplete paths
The Next Operator

on an infinite path

\[ \sigma_1 \sigma_2 \sigma_3 \sigma_4 \sigma_5 \sigma_6 \sigma_7 \ldots \models X\varphi \iff \]

\[ \sigma_2 \sigma_3 \sigma_4 \sigma_5 \sigma_6 \sigma_7 \ldots \models \varphi \]
The Next Operator

on a finite path

\[ \sigma_1 \sigma_2 \sigma_3 \sigma_4 \sigma_5 \sigma_6 \sigma_7 \models X\varphi \iff \sigma_2 \sigma_3 \sigma_4 \sigma_5 \sigma_6 \sigma_7 \models \varphi \]

But what if the path is of length one?

Two versions: Strong Next \( \text{\underline{X}}\varphi \) Requires path to be of length greater than one

Weak Next \( \text{\underline{\text{\texttildetilde}}X}\varphi \) Holds also if the path is of length one

[Manna & Pnueli, 1992]
LTL on

infinite paths

\[ p \mid \neg \varphi \mid \varphi_1 \lor \varphi_2 \mid X \varphi \mid [\varphi_1 U \varphi_2] \]
\[ G \varphi \mid F \varphi \mid [\varphi_1 W \varphi_2] \]

finite/infinite paths

\[ p \mid \neg \varphi \mid \varphi_1 \lor \varphi_2 \mid \mathcal{X} \varphi \mid \mathcal{X} \varphi [\mathcal{X} \varphi \neg \varphi] \]
\[ G \varphi \mid F \varphi \mid [\varphi_1 W \varphi_2] \]

Decorations for Weak operators
Core ops:
Derived ops:

Decorations for Strong operators
One new op

\[ \mathcal{X} \varphi = \neg X \neg \varphi \]
The semantics of ELTL over truncated paths is given with respect to a path, a\_i of non-negative integers, so that 0 < p for i < with AP_{X < 0}.

Additional derived operators are defined as follows:

\[ p | \neg \varphi | \varphi_1 \lor \varphi_2 | X \varphi | [\varphi_1 U \varphi_2] \]

\[ G \varphi | F \varphi | [\varphi_1 W \varphi_2] \]

How do we evaluate p on an empty path?

p | 0 | 1 | X^i \varphi | [\varphi_1 U \varphi_2] \]

\[ G \varphi | F \varphi | [\varphi_1 W \varphi_2] | X^i \varphi \]

Generalization

i=1: Next
i=0: Now
Truncated Paths

- Prefixes of computations
- Not maximal, but truncated

Encountered in

- Bounded Model Checking
- Dynamic Verification
- Resets
- Clock Shifts

Do they require different semantics?
Truncated Paths

Hardware Resets

"p should hold until q does unless the reset signal r holds"

Answer should be True:
Up until the reset signal occurred, the path behaved correctly

Why not use Weak Until?
Because we allow q not to hold only if r did.

Why not $[p \dot{U} (q \lor r)]$?

The reset/truncation op
\[ \varphi_1 = \left[ (p_1 \land Xp_2 \land XXp_3) \cup (q \lor r) \right] \]

\[ \varphi_2 = \left[ (p_1 \land Xp_2 \land XXp_3) \cup q \right] \tilde{T} r \]

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p_1 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( p_2 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( p_3 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( q )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( r )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8</td>
</tr>
</tbody>
</table>

\( \not\models \varphi_1 \)

\( \models \varphi_2 \)
\( \varphi_1 = [(p_1 \land Xp_2 \land XXp_3) \lor (q \lor r)] \)

\( \varphi_2 = [(p_1 \land Xp_2 \land XXp_3) \lor q] \tilde{T} r \)

The reset op releases future obligations.

The until op does not!
Truncated Paths

Dynamic Verification

\[ p p p p p p p p \models [p U q] \]

If the test was designed to be long enough to exhibit \( q \) - False
If the test was not designed so - True (so far so good)

Should the verifier change the property when switching tools?

No!
Properties should state the desired behavior!

So???
Use Views!

The truncated semantics evaluates a formula wrt. (i) a path
(ii) a view

A view is one of the three:
(weak, neutral, strong)

Optimistic
accepts if nothing bad happened so far

Realistic
considers the truncated path as if it was maximal

Pessimistic
rejects if eventualities are not fulfilled

[Eisner et al. 03]
Views for Truncated Paths

Dynamic Verification

\[ \text{view in \{weak, neutral, strong\}} \]

\[ (p \ p \ p \ p \ p \ p \ p \ p, \text{weak}) \models pUq \]

\[ (p \ p \ p \ p \ p \ p \ p \ p, \text{neutral}) \models pUq \]

\[ (p \ p \ p \ p \ p \ p \ p \ p, \text{strong}) \models pUq \]
The Truncated Semantics

Given a finite/infinite word $w \in \Sigma^\infty$

a view $v \in \{+, \cdot, -\}

and a formula $\varphi$

$(w, v) \vDash \varphi$  \quad \text{formula $\varphi$ holds on path $w$ under the view $v$}$

$(w, -) \vDash \varphi$  \quad \varphi \text{ holds weakly on $w$}

$(w, \cdot) \vDash \varphi$  \quad \varphi \text{ holds neutrally on $w$}

$(w, +) \vDash \varphi$  \quad \varphi \text{ holds strongly on $w$}
ELTL Semantics

Semantics:

\[
\langle w, v \rangle \models \mathbf{X}^i p \iff \text{either } |w| > i \text{ and } w[i+1] \models p \text{ or } v = - \text{ and if } |w| > i \text{ then } w[i+1] \models p
\]

\[
\langle w, v \rangle \models \neg \varphi \iff \langle w, \bar{v} \rangle \not\models \varphi
\]

\[
\langle w, v \rangle \models \varphi_1 \lor \varphi_2 \iff \langle w, v \rangle \models \varphi_1 \text{ or } \langle w, v \rangle \models \varphi_2
\]

\[
\langle w, v \rangle \models [\varphi_1 \mathbf{U} \varphi_2] \iff \exists k. \langle w[k..], v \rangle \models \varphi_2 \text{ and } \forall j < k. \langle w[j..], v \rangle \models \varphi_1
\]

\[
\langle w, v \rangle \models [\varphi \mathbf{T} b] \iff \text{either } \langle w, v \rangle \models \varphi \text{ or } \exists j. \langle w[j], v \rangle \models b \text{ and } \langle w[..j-1], - \rangle \models \varphi
\]
ELTL Semantics

\[
\bar{v} = \begin{cases} 
+ & \text{if } v = - \\
\cdot & \text{if } v = \cdot \\
- & \text{if } v = + 
\end{cases}
\]

Semantics:

\[
\langle w, v \rangle \models X^i p \iff \text{either } |w| > i \text{ and } w[i+1] \models p \text{ or } v = - \text{ and if } |w| > i \text{ then } w[i+1] \models p
\]

\[
\langle w, v \rangle \models \neg \varphi \iff \langle w, \bar{v} \rangle \not\models \varphi
\]

\[
\langle w, v \rangle \models \varphi_1 \lor \varphi_2 \iff \langle w, v \rangle \models \varphi_1 \text{ or } \langle w, v \rangle \models \varphi_2
\]

\[
\langle w, v \rangle \models [\varphi_1 U \varphi_2] \iff \exists k. \langle w[k..], v \rangle \models \varphi_2 \text{ and } \forall j < k. \langle w[j..], v \rangle \models \varphi_1
\]

\[
\langle w, v \rangle \models [\varphi T b] \iff \text{either } \langle w, v \rangle \models \varphi \text{ or } \exists j. \langle w[j], v \rangle \models b \text{ and } \langle w[..j-1], \neg \rangle \models \varphi
\]
ELTL Semantics

Complementary view \( \overline{v} = \begin{cases} + & \text{if } v = - \\ \cdot & \text{if } v = \cdot \\ - & \text{if } v = + \end{cases} \)

Semantics:

\[ \langle w, v \rangle \models X^i p \iff \text{either } |w| > i \text{ and } w[i+1] \models p \text{ or } v = - \text{ and if } |w| > i \text{ then } w[i+1] \models p \]

\[ \langle w, v \rangle \models \neg \varphi \iff \langle w, \overline{v} \rangle \not\models \varphi \]

\[ \langle w, v \rangle \models \varphi_1 \lor \varphi_2 \iff \langle w, v \rangle \models \varphi_1 \text{ or } \langle w, v \rangle \models \varphi_2 \]

\[ \langle w, v \rangle \models [\varphi_1 U \varphi_2] \iff \exists k. \langle w[k..], v \rangle \models \varphi_2 \text{ and } \forall j < k. \langle w[j..], v \rangle \models \varphi_1 \]

\[ \langle w, v \rangle \models [\varphi T b] \iff \text{either } \langle w, v \rangle \models \varphi \text{ or } \exists j. \langle w[j], v \rangle \models b \text{ and } \langle w[..j-1], \overline{v} \rangle \models \varphi \]
The triggers operator adds expressiveness. While the expressive power of LTL most 3 cycles after

In PSL the triggers operators was added to PSL for ease of use. Indeed, the vast majority of properties written in PSL uses the trigger operator. On top of this, the semantics of the trigger operator is defined as follows.

Intuitively, $\text{req}()$ was acknowledged (or).

The strength relation theorem can be stated by the RELTL formula

For instance, the property

Theorem 2

Theorem 1

The logic RELTL, the core of PSL involving regular expressions, is an extended logic of LTL. The extension of ELTL with regular expressions is that of the full weak regular expressions.

For instance, the property

Theorem 2

Theorem 1

The logic RELTL, the core of PSL involving regular expressions, is an

For instance, the property

Theorem 2

Theorem 1

The logic RELTL, the core of PSL involving regular expressions, is an

For instance, the property

Theorem 2

Theorem 1

The logic RELTL, the core of PSL involving regular expressions, is an

For instance, the property

Theorem 2

Theorem 1

The logic RELTL, the core of PSL involving regular expressions, is an

For instance, the property

Theorem 2

Theorem 1

The logic RELTL, the core of PSL involving regular expressions, is an

For instance, the property

Theorem 2

Theorem 1

The logic RELTL, the core of PSL involving regular expressions, is an

For instance, the property

Theorem 2

Theorem 1

The logic RELTL, the core of PSL involving regular expressions, is an
The Prefix/Extension Theorem

Holds weakly

- $w \models \varphi \iff \forall w' \leq w. \ w' \models \varphi$

Holds weakly on all prefixes

Holds strongly

- $w \models^\pm \varphi \iff \forall w'' \geq w. \ w'' \models^\pm \varphi$

Holds strongly on all extensions

The Truncated Semantics is adopted by PSL and SVA (IEEE-1850, IEEE-1800).
Incomplete Paths

- A truncated path is just one type of incomplete path

- Other types:
  - Segmentally Broken Paths
  - Incomplete Ultimately Periodic Paths
  - Segmentally Broken Ultimately Periodically Periodic Paths
Segmentally Broken Path

Encountered when:
• Noise in observed paths
• Pieces of information
Incomplete Ultimately Periodic Paths

- Prefix of the transient part
- Infix of the periodic part
Segmentally Broken Ultimately Periodic Paths

- Segments of the transient part
- Segments of the periodic part
Semantics?

The semantics definition generalizes the $\top/\bot$ approach to the truncated semantics.
The $\top / \bot$ Semantics to the Truncated Semantics

Augment the alphabet $\Sigma = 2^{AP}$ with symbols $\{ \top, \bot \}$

$\top$ satisfies everything, even false
$\bot$ Satisfies nothing, not even true

**Neutral Semantics:**

\[
\begin{align*}
  w \models X^i p & \iff |w| > i \text{ and } w[i+1] \models p \\
  w \models \neg \varphi & \iff \bar{w} \not\models \varphi \\
  w \models \varphi_1 \lor \varphi_2 & \iff w \models \varphi_1 \text{ or } w \models \varphi_2 \\
  w \models [\varphi_1 \mathbf{U} \varphi_2] & \iff \exists k. w[k..] \models \varphi_2 \text{ and } \forall j < k. w[j..] \models \varphi_1 \\
  w \models [\varphi \mathbf{T} b] & \iff \text{either } \langle w \rangle \models \varphi \\
  & \text{or } \exists j. w[j] \models b \text{ and } w[..j-1] \models \varphi
\end{align*}
\]

**Weak & Strong Semantics:**

\[
\begin{align*}
  w \models \varphi & \iff w \top^\omega \models \varphi \\
  w \models \varphi & \iff w \bot^\omega \models \varphi \\
  \top^\omega & \text{satisfies everything} \\
  \bot^\omega & \text{satisfies nothing}
\end{align*}
\]
Incomplete Ultimately Periodically Paths

Semantics

Given $u, v \in \Sigma^*$

prefix of the transient part

infix of the periodic part

$(u, v) \models \varphi \iff \exists w \in (uT^*)(vT^*)^\omega. \ w \models \varphi$

$(u, v) \models \varphi \iff uv^\omega \models \varphi$

$(u, v) \models \varphi \iff \forall w \in (u\perp^*)(v\perp^*)^\omega. \ w \models \varphi$
Segmentally Broken Path

Semantics

Given \( u_1, u_2, \ldots, u_k \in \Sigma^* \)

\[ \langle u_1, u_2, \ldots, u_k \rangle \models \phi \iff \exists w \in u_1^*u_2^* \cdots T^*u_k T^\omega. \ w \models \phi \]

\[ \langle u_1, u_2, \ldots, u_k \rangle \models \phi \iff u_1u_2 \cdots u_k \models \phi \]

\[ \langle u_1, u_2, \ldots, u_k \rangle \models^\perp \phi \iff \forall w \in u_1^\perp u_2^\perp \cdots \perp u_k \perp^\omega. \ w \models \phi \]
Segmentally Broken Ultimately Periodic Paths

Semantics

Let \( u_1, u_2, \ldots, u_k \in \Sigma^* \) and \( v_1, v_2, \ldots, v_\ell \in \Sigma^* \).

\[
\begin{align*}
\langle \langle u_1, \ldots, u_k \rangle, \langle v_1, \ldots, v_\ell \rangle \rangle & \models \varphi \iff \exists w \in (u_1 T^* \ldots u_k T^*) (v_1 T^* \ldots v_\ell T^*) \omega. w \models \varphi \\
\langle \langle u_1, \ldots, u_k \rangle, \langle v_1, \ldots, v_\ell \rangle \rangle & \models \varphi \iff (u_1 u_2 \ldots u_k)(v_1 v_2 \ldots v_\ell) \omega \models \varphi \\
\langle \langle u_1, \ldots, u_k \rangle, \langle v_1, \ldots, v_\ell \rangle \rangle & \models \varphi \iff \forall w \in (u_1 r^* \ldots u_k r^*) (v_1 r^* \ldots v_\ell r^*) \omega. w \models \varphi
\end{align*}
\]
Properties of the Semantics on Segmentally Broken Ultimately Periodic Paths

- Generalizes the other semantics
  - Truncated Paths
  - Segmentally Broken Paths
  - Incomplete Ultimately Periodically Paths

- Strength Relation Theorem Holds

  \[ \text{Holds strongly} \implies \text{Holds Neutrally} \implies \text{Holds Weakly} \]

- The Prefix/Extension Theorem Holds

  \[ \text{Holds Weakly} \iff \text{Holds Weakly on All Prefixes} \]
  \[ \text{Holds Strongly} \iff \text{Holds Strongly on All Extensions} \]
What about Continuous Time?

- Signal Temporal Logic is an extension of LTL to reason on continuous time
- The models are non-Zeno Signals
- We define extension for the semantics of STL to
  - Truncated Signals
  - Segmentally Broken Signals
  - Incomplete Ultimately Periodically Signals
  - Segmentally Broken Ultimately Periodically Signals

\[(\langle \alpha_1, \ldots, \alpha_k \rangle, \langle \beta_1, \ldots, \beta_k \rangle) \models \varphi \iff \exists \gamma \in \langle \alpha_1 \mathbb{D}^T \ldots \alpha_k \mathbb{D}^T \rangle \langle \beta_1 \mathbb{D}^T \ldots \beta \mathbb{D}^T \rangle^\omega. \gamma \models \varphi\]

\[(\langle \alpha_1, \ldots, \alpha_k \rangle, \langle \beta_1, \ldots, \beta_k \rangle) \models \varphi \iff (\alpha_1 \ldots \alpha_k) \langle \beta_1 \ldots \beta_k \rangle^\omega \models \varphi\]

\[(\langle \alpha_1, \ldots, \alpha_k \rangle, \langle \beta_1, \ldots, \beta_k \rangle) \models \varphi \iff \forall \gamma \in \langle \alpha_1 \mathbb{D}^+ \ldots \alpha_k \mathbb{D}^+ \rangle \langle \beta_1 \mathbb{D}^+ \ldots \beta \mathbb{D}^+ \rangle^\omega. \gamma \models \varphi\]
Also skipped in the talk

- Reasoning on Incomplete Paths in System Biology

- Related Work:
  - $LTL_3$ [Bauer et al.]
  - $LTL_4$ [Bauer et al.]
  - $TLTL_3$ [Bauer et al.]
  - Counting Semantics for LTL [Bartocci et al.]
$\varphi = \tilde{G}(a \to \overline{Fb})$

- Holds weakly on both
- Doesn’t hold neutrally/strongly on both

[Bartocci et al. 2018] argue that it should hold weakly on the second but not on the first
We argue that it depends what is the periodic part.

\[ \varphi = \tilde{G}(a \rightarrow Fb) \]
To Conclude

- We propose a generalization of the semantics of LTL on truncated paths to other incomplete paths.
- We propose an orthogonal extension of STL to truncated and incomplete signals.
- We explored whether system biology can benefit from the suggested extensions.
Thanks for Listening!

Questions /
Comments?

Thanks to Guy Ofek for his help with the drawings!