Formal Specification and Verification
Formal Modeling with Temporal Logic

Bernhard Beckert

Based on a lecture by Wolfgang Ahrendt and Reiner Hähnle at Chalmers University, Göteborg
Beyond the Limitations of Propositional Logic

Propositional Logic

Temporal Logic

First-order Logic

Dynamic Logic

+computations

+functions

+computations +functions

+functions
Beyond the Limitations of Propositional Logic
Beyond the Limitations of Propositional Logic

Propositional Logic

Temporal Logic

Dynamic Logic

+computations +functions

First-order Logic

+computations +functions

Spin

KeY

Formal Specification and Verification: Formal Modeling with TL
An extension of propositional logic that allows to specify properties of sets of runs
Temporal Logic—Syntax

An extension of propositional logic that allows to specify properties of sets of runs.

Syntax

Based on propositional signature and syntax. Extension with three connectives:

- **Always** If $\phi$ is a formula then so is $[\phi]$
- **Sometimes** If $\phi$ is a formula then so is $<>\phi$
- **Until** If $\phi$ and $\psi$ are formulas then so is $\phi U \psi$

Concrete Syntax

<table>
<thead>
<tr>
<th></th>
<th>textbook</th>
<th>SPIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>$\Box$</td>
<td>$[\ ]$</td>
</tr>
<tr>
<td>Sometimes</td>
<td>$\Diamond$</td>
<td>$&lt;&gt;\phi$</td>
</tr>
<tr>
<td>Until</td>
<td>$U$</td>
<td>$\bigcup$</td>
</tr>
</tbody>
</table>

Formal Specification and Verification: Formal Modeling with TL
A run $\sigma$ is an infinite chain of states

$s_0 I_0 \rightarrow s_1 I_1 \rightarrow s_2 I_2 \rightarrow s_3 I_3 \rightarrow s_4 I_4 \rightarrow \ldots$

$I_j$ propositional interpretation of variables in $j$-th state

Write more compactly $s_0 s_1 s_2 s_3 \ldots$
A run $\sigma$ is an infinite chain of states

$s_0$$\mathcal{I}_0$ $\rightarrow$ $s_1$$\mathcal{I}_1$ $\rightarrow$ $s_2$$\mathcal{I}_2$ $\rightarrow$ $s_3$$\mathcal{I}_3$ $\rightarrow$ $s_4$$\mathcal{I}_4$ $\rightarrow$ $\cdots$

$\mathcal{I}_j$ propositional interpretation of variables in $j$-th state
Write more compactly $s_0 s_1 s_2 s_3 \ldots$

If $\sigma = s_0 s_1 \ldots$, then $\sigma|_i$ denotes the suffix $s_i s_{i+1} \ldots$ of $\sigma$. 
Definition (Validity Relation)

Validity of temporal formula depends on runs $\sigma = s_0 s_1 \ldots$ for which the formula may, or may not, hold:

$\sigma \models p$ iff $I_0(p) = T$, for $p \in \mathcal{P}$.

$\sigma \models ! \phi$ iff not $\sigma \models \phi$ (write $\sigma \not\models \phi$)

$\sigma \models \phi & \psi$ iff $\sigma \models \phi$ and $\sigma \models \psi$

$\sigma \models \phi \mathcal{U} \psi$ iff $\sigma \not\models \phi$ or $\sigma \models \psi$
Definition (Validity Relation)

Validity of temporal formula depends on runs $\sigma = s_0 s_1 \ldots$ for which the formula may, or may not, hold:

- $\sigma \models p$ iff $I_0(p) = T$, for $p \in \mathcal{P}$.
- $\sigma \models !\phi$ iff not $\sigma \models \phi$ (write $\sigma \not\models \phi$)
Definition (Validity Relation)

Validity of temporal formula depends on runs $\sigma = s_0 s_1 \ldots$ for which the formula may, or may not, hold:

$\sigma \models p$ iff $I_0(p) = T$, for $p \in \mathcal{P}$.

$\sigma \models ! \phi$ iff not $\sigma \models \phi$ (write $\sigma \not\models \phi$)

$\sigma \models \phi \& \psi$ iff $\sigma \models \phi$ and $\sigma \models \psi$
Definition (Validity Relation)

Validity of temporal formula depends on runs $\sigma = s_0 s_1 \ldots$ for which the formula may, or may not, hold:

- $\sigma \models p$ iff $I_0(p) = T$, for $p \in \mathcal{P}$.
- $\sigma \models \neg \phi$ iff not $\sigma \models \phi$ (write $\sigma \not\models \phi$)
- $\sigma \models \phi \land \psi$ iff $\sigma \models \phi$ and $\sigma \models \psi$
- $\sigma \models \phi \lor \psi$ iff $\sigma \models \phi$ or $\sigma \models \psi$
- $\sigma \models \phi \to \psi$ iff $\sigma \not\models \phi$ or $\sigma \models \psi$
Definition (Validity Relation for Temporal Connectives)

Given a run $\sigma = s_0 \ s_1 \ldots$
Definition (Validity Relation for Temporal Connectives)

Given a run \( \sigma = s_0 s_1 \ldots \)
\[ \sigma \models [\ ]\phi \quad \text{iff} \quad \sigma_k \models \phi \quad \text{for all } k \geq 0 \]
Definition (Validity Relation for Temporal Connectives)

Given a run $\sigma = s_0 s_1 \ldots$

- $\sigma \models []\phi$ \iff $\sigma|_k \models \phi$ for all $k \geq 0$
- $\sigma \models <>\phi$ \iff $\sigma|_k \models \phi$ for some $k \geq 0$
Definition (Validity Relation for Temporal Connectives)

Given a run $\sigma = s_0 s_1 \ldots$

- $\sigma \models [\phi]$ if $\sigma|_k \models \phi$ for all $k \geq 0$
- $\sigma \models <>\phi$ if $\sigma|_k \models \phi$ for some $k \geq 0$
- $\sigma \models \phi U \psi$ if $\sigma|_k \models \psi$ for some $k \geq 0$, and $\sigma|_j \models \phi$ for all $0 \leq j < k$
## Safety Properties

Always-formulas called **safety property**: something bad never happens

Let $\text{mutex}$ be variable that is true when two processes do not access a critical resource at the same time

$\Box \text{mutex}$ expresses that simultaneous access never happens
Safety Properties

Always-formulas called **safety property**: something bad never happens

Let $mutex$ be variable that is true when two processes do not access a critical resource at the same time

$[\neg mutex]$ expresses that simultaneous access never happens

Liveness Properties

Sometimes-formulas called **liveness property**: something good happens eventually

Let $s$ be variable that is true when a process delivers a service

$<> s$ expresses that service is eventually provided
What does this mean?

\[ []<>\phi \]
Infinitely Often

\[ []<>\phi \]

During a run the formulas \( \phi \) will become true infinitely often.
Definition (Validity)

ϕ is valid, write ⊨ ϕ, iff ϕ is valid in all runs σ = s₀ s₁ ....

Recall that each run s₀ s₁ ... essentially is an infinite sequence of interpretations I₀ I₁ ....
Examples

Valid?

$<>[\ ]p$

No, there is a run in where it is not valid:

$(\neg p, \neg p, \neg p, ...)$

Valid in some run?

Yes: $(p, p, p, ...)$

$\phi \rightarrow \neg \phi$ $(\neg \phi)$

Both are valid!

$\square$ is reflexive

$\square$ and $<>$ are dual connectives
Examples

Valid?

No, there is a run in where it is not valid:

$<>[\neg p]$
Examples

$<>[]{p}$

Valid?

No, there is a run in where it is not valid:

$(!p, !p, !p, \ldots)$
Examples

<><[ ]>p

Valid?

No, there is a run in where it is not valid:
(! p, ! p, ! p, ...)

Valid in some run?
Examples

$<>[]p$

Valid?
No, there is a run in where it is not valid:
$(!p, !p, !p, \ldots)$

Valid in some run?
Yes: $(p, p, p, \ldots)$
Examples

\(<>[\!p]\)

Valid?
No, there is a run in where it is not valid:
\((\!p, \!p, \!p, \ldots)\)

Valid in some run?
Yes: \((p, p, p, \ldots)\)

\([\phi] -> \phi\) \hspace{1cm} (\! [\phi]) <-> (<> !\phi)

Both are valid!
Examples

$<>[]p$

Valid?
No, there is a run in where it is not valid:
$(!p, !p, !p, ...)$

Valid in some run?
Yes: $(p, p, p, ...)$

$[]\phi \rightarrow \phi \quad (![]\phi) \leftrightarrow (<>!\phi)$

Both are valid!

- [] is reflexive
- [] and <> are dual connectives
Definition (Transition System)

A Transition System $\mathcal{I} = (S, Ini, \delta, I)$ is given by a set of states $S$, a non-empty subset $Ini \subseteq S$ of initial states, and a transition relation $\delta \subseteq S \times S$, and $I$ labeling each state $s \in S$ with a propositional interpretation $I_s$.

Definition (Runs of Transition System)

A run of $\mathcal{I}$ is a run $\sigma = s_0 s_1 \ldots$, with $s_i \in S$, such that $s_0 \in Ini$ and $(s_i, s_{i+1}) \in \delta$ for all $i$. 
Validity of temporal formula is extended to transition systems in the following way:

**Definition (Validity Relation)**

Given a transition system $\mathcal{T} = (S, \text{Ini}, \delta, \mathcal{I})$, a temporal formula $\phi$ is valid in $\mathcal{T}$ (write $\mathcal{T} \models \phi$) iff $\sigma \models \phi$ for all runs $\sigma$ of $\mathcal{T}$. 

Ben-Ari  Section 5.2.1
(Promela examples on the surface only)