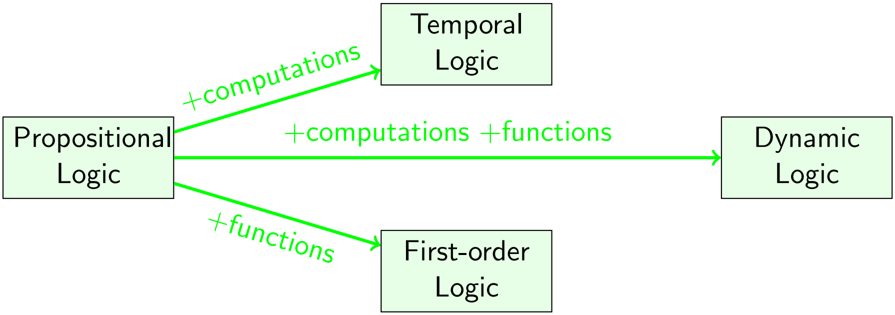
Formal Specification and Verification

Formal Modeling with Temporal Logic

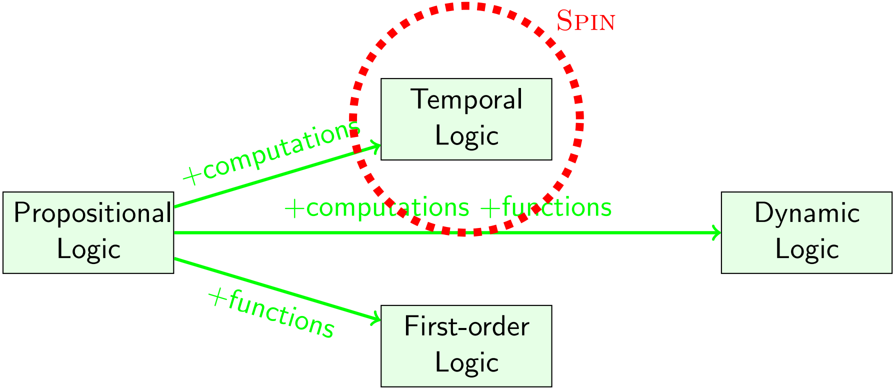
Bernhard Beckert

Based on a lecture by Wolfgang Ahrendt and Reiner Hähnle at Chalmers University, Göteborg

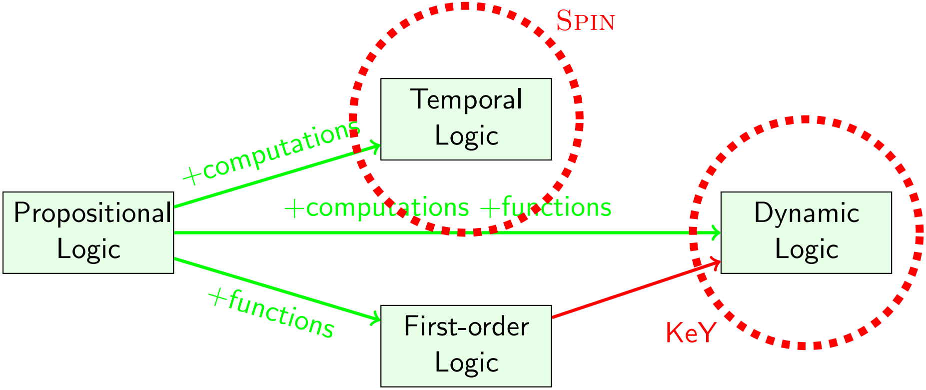
Beyond the Limitations of Propositional Logic



Beyond the Limitations of Propositional Logic



Beyond the Limitations of Propositional Logic



Temporal Logic

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

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 ϕ is a formula then so is $[]\phi$

Sometimes If ϕ is a formula then so is $<>\phi$

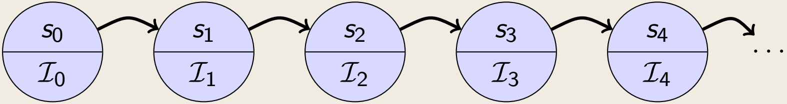
Until If ϕ and ψ are formulas then so is $\phi \, \mathtt{U} \, \psi$

Concrete Syntax

	text book	SPIN
Always	$\Box$	$[]$
Sometimes	$\Diamond$	$<>$
Until	$\mathcal{U}$	$\mathtt{U}$

Semantics of Temporal Logic

A run σ is an infinite chain of states

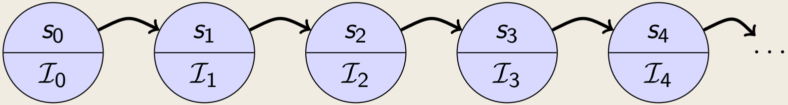


$\mathcal{I}_j$ propositional interpretation of variables in j-th state

Write more compactly $s_0\, s_1\, s_2\, s_3 \ldots$

Semantics of Temporal Logic

A run σ is an infinite chain of states



$\mathcal{I}_j$ 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 σ.

Semantics of Temporal Logic (Cont'd)

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 $\mathcal{I}_0(p) = T$, for $p \in \mathcal{P}$.

Semantics of Temporal Logic (Cont'd)

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 $\mathcal{I}_0(p) = T$, for $p \in \mathcal{P}$.

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

Semantics of Temporal Logic (Cont'd)

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	$\mathcal{I}_0(p) = T$, 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 $\sigma \models \psi$

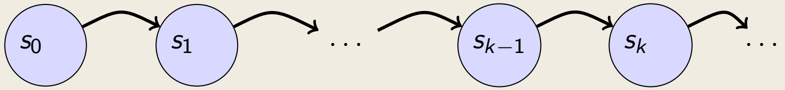
Semantics of Temporal Logic (Cont'd)

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	$\mathcal{I}_0(p) = T$, 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 $\sigma \models \psi$
$\sigma \models \phi \mid \psi$	iff	$\sigma \models \phi$ or $\sigma \models \psi$
$\sigma \models \phi \mathrel{-\!\!>} \psi$	iff	$\sigma \not\models \phi$ or $\sigma \models \psi$

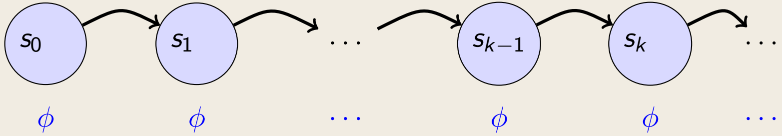
Semantics of Temporal Logic Cont'd



Definition (Validity Relation for Temporal Connectives)

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

Semantics of Temporal Logic Cont'd

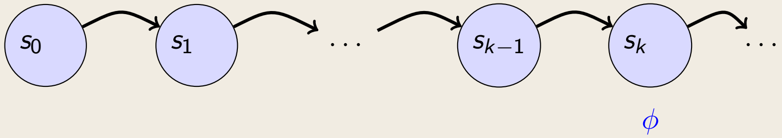


Definition (Validity Relation for Temporal Connectives)

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

$\sigma \models [\,]\phi$ iff $\sigma|_k \models \phi$ for all $k \geq 0$

Semantics of Temporal Logic Cont'd



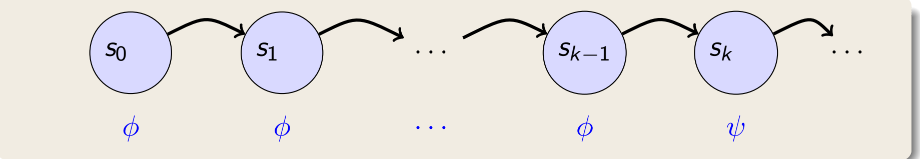
Definition (Validity Relation for Temporal Connectives)

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 $k \geq 0$

Semantics of Temporal Logic Cont'd



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 $k \geq 0$

$\sigma \models \phi\, \mathtt{U}\, \psi$ iff $\sigma|_k \models \psi$ for some $k \geq 0$, and $\sigma|_j \models \phi$ for all $0 \leq j < k$

Safety and Liveness Properties

Safety Properties

Always-formulas called safety property: something bad never happens

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

`[]mutex` expresses that simultaneous access never happens

Safety and Liveness Properties

Safety Properties

Always-formulas called safety property: something bad never happens

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

`[]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

Complex Properties

What does this mean?

$$[]<>\phi$$

Complex Properties

Infinitely Often

$$[\,]\!<\,>\phi$$

During a run the formulas ϕ will become true infinitely often.

Validity Temporal Logic

Definition (Validity)

ϕ is valid, write $\models \phi$, iff ϕ is valid in all runs $\sigma = s_0\, s_1 \ldots$.

Recall that each run $s_0\, s_1 \ldots$ essentially is an infinite sequence of interpretations $\mathcal{I}_0\, \mathcal{I}_1 \ldots$.

Examples

$$<>[]p$$

Valid?

Examples

$$<>[]p$$

Valid?

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

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

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: $(p,\ p,\ p, \ldots)$

$$[]\phi \;\text{->}\; \phi \qquad\qquad (!\,[]\phi) \;\text{<->}\; (<>!\,\phi)$$

Both are valid!

Examples

$$<>[]p$$

Valid?

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

Valid in some run?

Yes: $(p,\ p,\ p, \ldots)$

$$[\,]\phi \;{-}{>}\; \phi \qquad\qquad (!\,[\,]\phi) <{-}> (<>!\,\phi)$$

Both are valid!

- $[\,]$ is reflexive
- $[\,]$ and $<>$ are dual connectives

Transition systems revisited

Definition (Transition System)

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

Definition (Runs of Transition System)

A run of $\mathcal{T}$ is a is a run $\sigma = s_0\, s_1 \ldots$, with $s_i \in S$, such that $s_0 \in \mathit{Ini}$ and $(s_i, s_{i+1}) \in \delta$ for all i.

Semantics of Temporal Logic (Cont'd)

Validity of temporal formula is extended to transition systems in the following way:

Definition (Validity Relation)

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

Literature for this Lecture

KeY W. Ahrendt: Using KeY. In: B. Beckert, R. Hähnle, and P. Schmitt, editors. *Verification of Object-Oriented Software: The KeY Approach*, Chapter 10, only pp 409–424, vol 4334 of *LNCS*. Springer, 2006.
(Access to e-version via Chalmers Library)

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