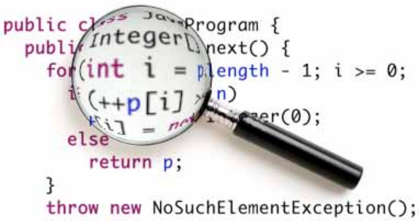
15-819M: Data, Code, Decisions

02: Formal Modeling with Propositional Logic

André Platzer

aplatzer@cs.cmu.edu
Carnegie Mellon University, Pittsburgh, PA

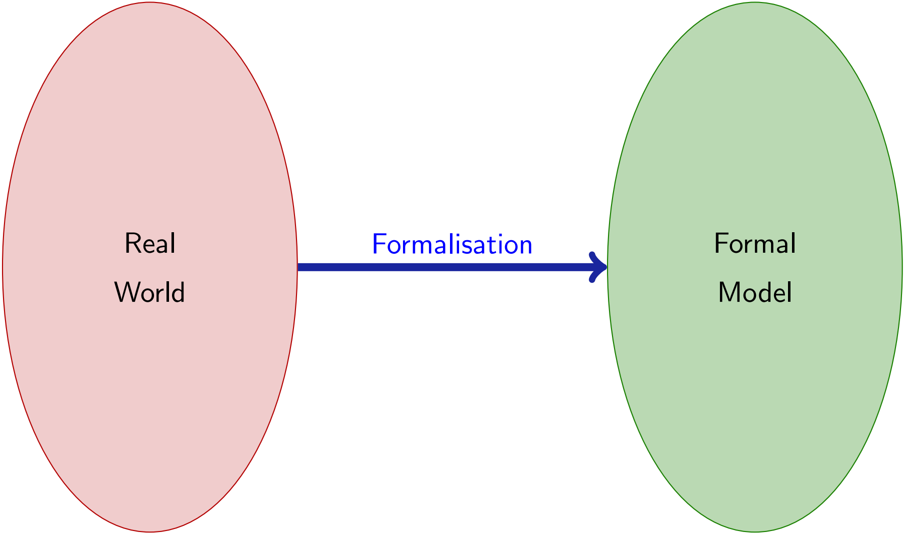


Outline

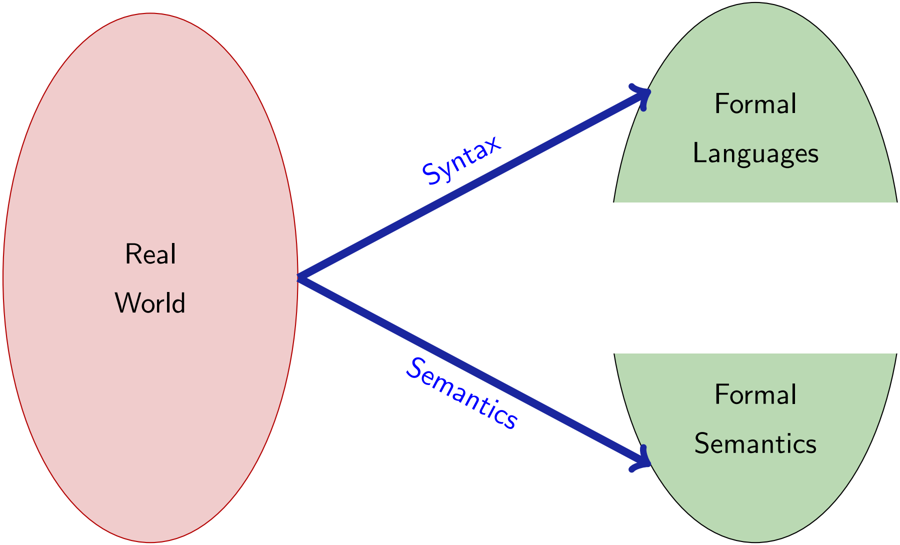
1. Formal Modeling
2. Propositional Logic
   - Syntax
   - Semantics
   - Sequent Calculus
   - DPLL
   - Expressiveness
3. Temporal Logic

Outline

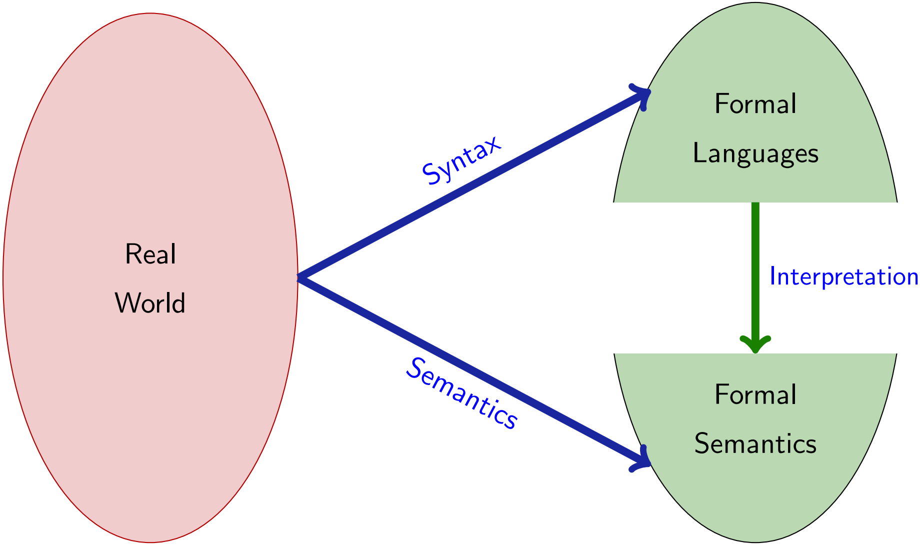
Formalisation



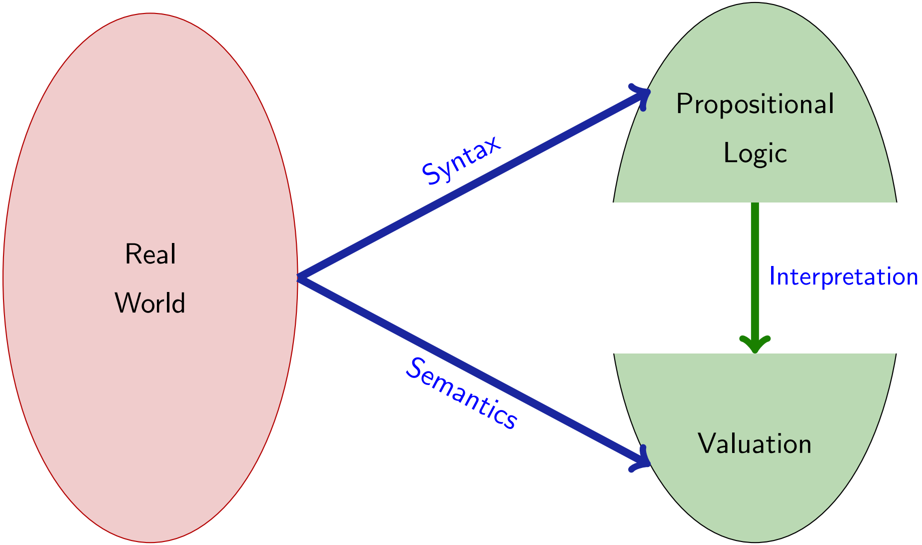
Formalisation: Syntax, Semantics



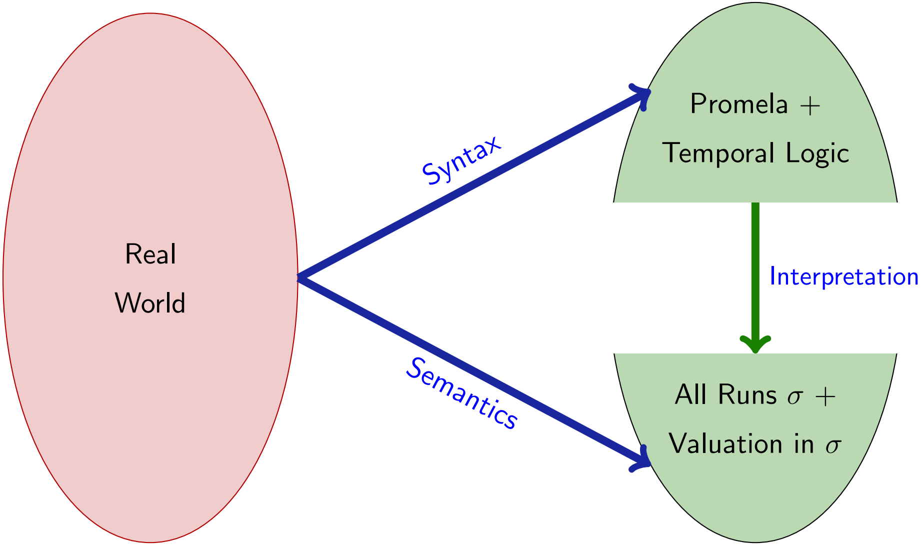
Formalisation: Syntax, Semantics



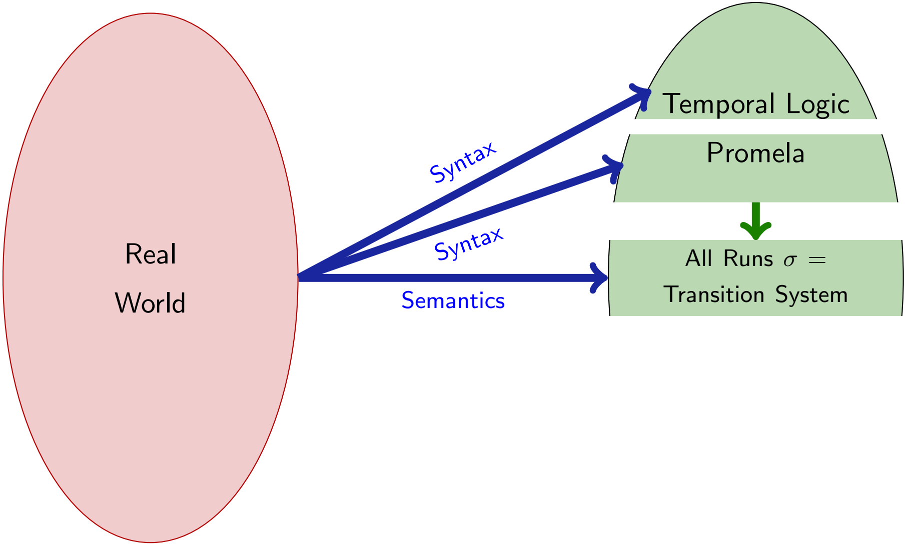
Formalisation: Syntax, Semantics



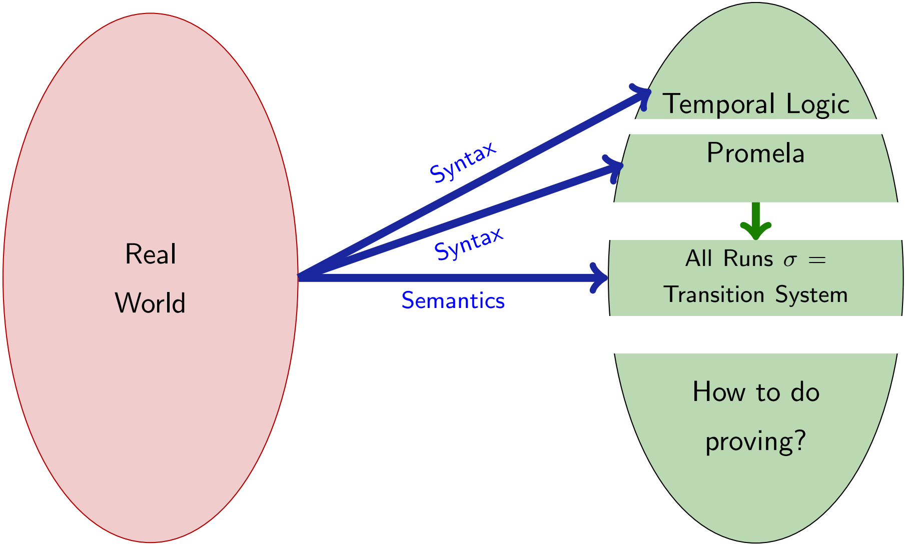
Formalisation: Syntax, Semantics



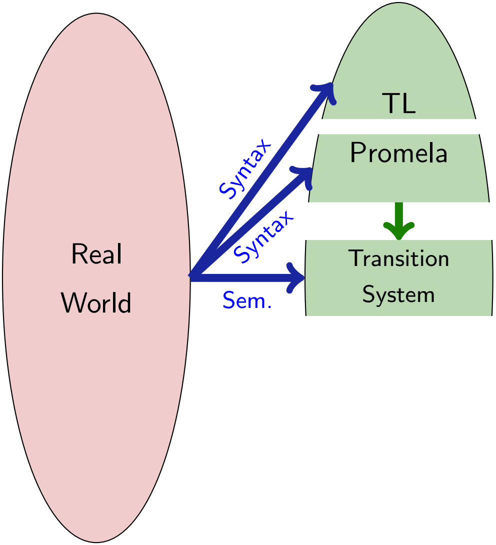
Formalisation: Syntax, Semantics



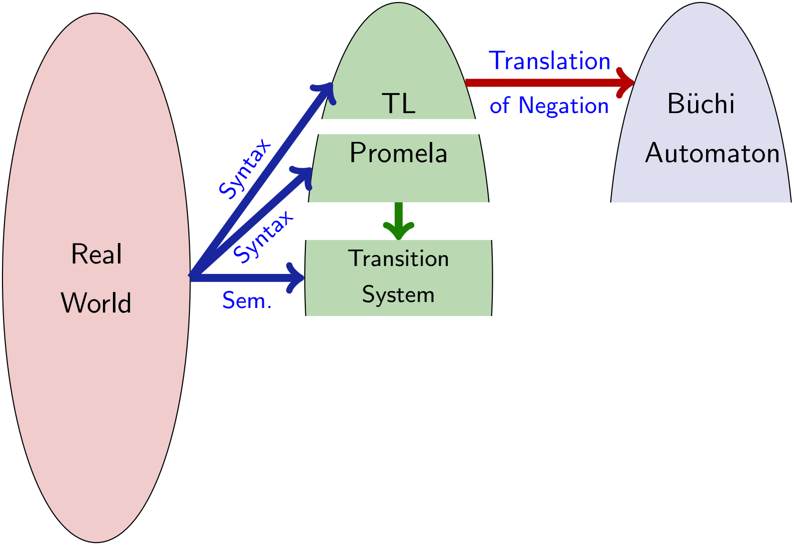
Formalisation: Syntax, Semantics, Proving



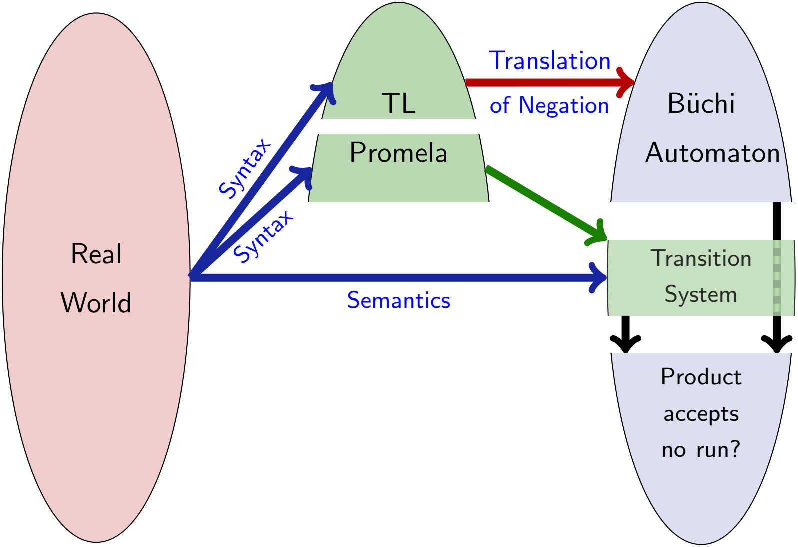
Formal Verification: Model Checking



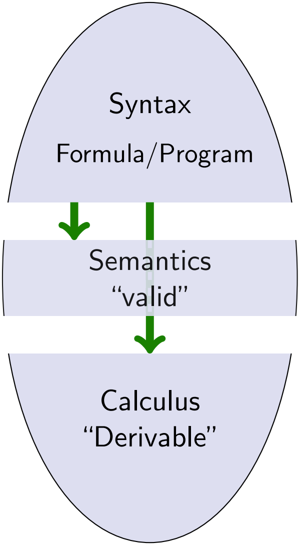
Formal Verification: Model Checking



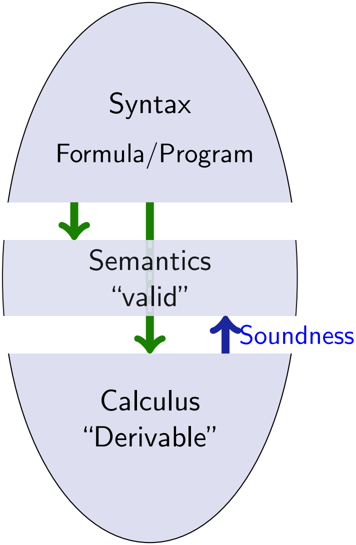
Formal Verification: Model Checking



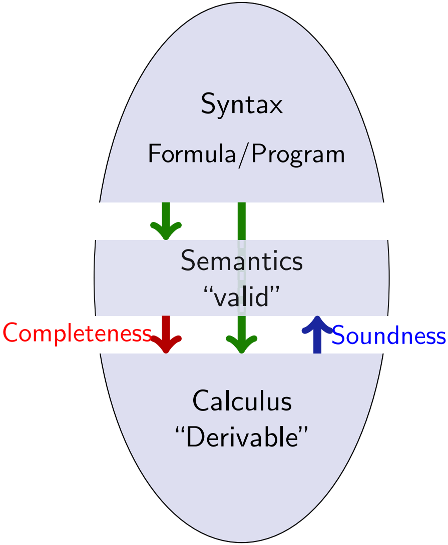
Syntax, Semantics, Calculus



Syntax, Semantics, Calculus

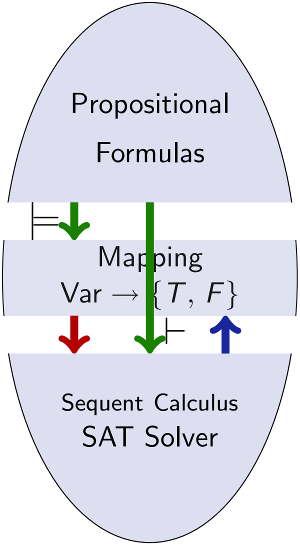


Syntax, Semantics, Calculus

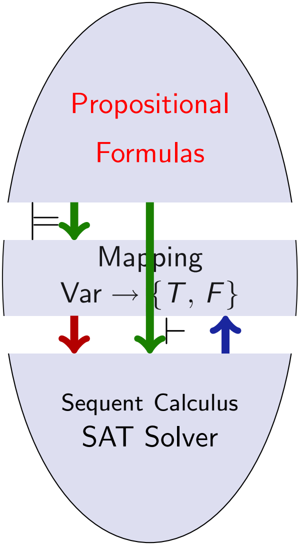


Outline

Propositional Logic



Propositional Logic: Syntax



Syntax of Propositional Logic

Definition (Signature)

A set of Propositional Variables $\mathcal{P}$ (with typical elements $p, q, r, \ldots$)

Syntax of Propositional Logic

Definition (Signature)

A set of Propositional Variables $\mathcal{P}$ (with typical elements $p, q, r, \ldots$)

Propositional Connectives

true false & | ! -> <->

Syntax of Propositional Logic

Definition (Signature)

A set of Propositional Variables $\mathcal{P}$ (with typical elements $p, q, r, \ldots$)

Propositional Connectives

$\mathrm{true} \quad \mathrm{false} \quad \& \quad | \quad ! \quad -> \quad <->$

Definition (Propositional Formulas For_0)

- Truth constants true, false and variables $\mathcal{P}$ are formulas
- If ϕ and ψ are formulas then

  $$!\,\phi, \quad (\phi \ \& \ \psi), \quad (\phi \mid \psi), \quad (\phi \ -> \ \psi), \quad (\phi \ <-> \ \psi)$$

  are also formulas
- There are no other formulas (inductive definition)

Syntax of Propositional Logic

Definition (Signature)

A set of Propositional Variables $\mathcal{P}$ (with typical elements $p, q, r, \ldots$)

Propositional Connectives (KeY notation)

$\mathrm{true} \quad \mathrm{false} \quad \& \quad | \quad ! \quad -\!\!> \quad <\!\!-\!\!>$

Definition (Propositional Formulas For_0)

- Truth constants true, false and variables $\mathcal{P}$ are formulas
- If ϕ and ψ are formulas then

  $$!\,\phi, \quad (\phi \;\&\; \psi), \quad (\phi \mid \psi), \quad (\phi \;-\!\!>\; \psi), \quad (\phi \;<\!\!-\!\!>\; \psi)$$

  are also formulas
- There are no other formulas (inductive definition)

Remark on Concrete Syntax

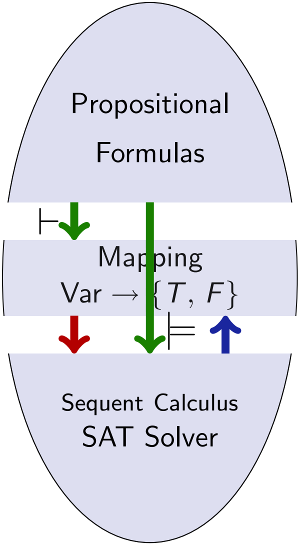
	Text book	KeY	SPIN
Negation	$\neg$	!	!
Conjunction	$\wedge$	&	&&
Disjunction	$\vee$	|	||
Implication	$\rightarrow, \supset$	->	->
Equivalence	$\leftrightarrow$	<->	<->

Remark on Concrete Syntax

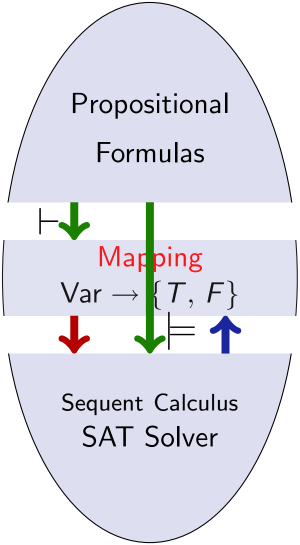
<table>
<tr><th></th><th>Text book</th><th>KeY</th><th>SPIN</th></tr>
<tr><td>Negation</td><td>$\neg$</td><td>!</td><td>!</td></tr>
<tr><td>Conjunction</td><td>$\wedge$</td><td>&</td><td>&&</td></tr>
<tr><td>Disjunction</td><td>$\vee$</td><td>|</td><td>||</td></tr>
<tr><td>Implication</td><td>$\rightarrow$, $\supset$</td><td>-></td><td>-></td></tr>
<tr><td>Equivalence</td><td>$\leftrightarrow$</td><td><-></td><td><-></td></tr>
</table>

Today, we use KeY notation.
Be flexible during the course!

Propositional Logic: Semantics



Propositional Logic: Semantics



Semantics of Propositional Logic

Definition (Interpretation $\mathcal{I}$)

Assigns a truth value to each propositional variable

$$\mathcal{I} : \mathcal{P} \to \{T, F\}$$

Semantics of Propositional Logic

Definition (Interpretation $\mathcal{I}$)

Assigns a truth value to each propositional variable

$$\mathcal{I} : \mathcal{P} \rightarrow \{T, F\}$$

Definition (Valuation function)

$val_{\mathcal{I}}$: Continuation of $\mathcal{I}$ on For_0

$$val_{\mathcal{I}} : For_0 \rightarrow \{T, F\}$$

$val_{\mathcal{I}}(p_i) = \mathcal{I}(p_i)$
$val_{\mathcal{I}}(\mathrm{true}) = T$
$val_{\mathcal{I}}(\mathrm{false}) = F$

(cont'd next page)

Semantics of Propositional Logic

Definition (Valuation function ...)

$$val_{\mathcal{I}}(!\,\phi) = \begin{cases} T & \text{if } val_{\mathcal{I}}(\phi) = F \\ F & \text{otherwise} \end{cases}$$

$$val_{\mathcal{I}}(\phi \,\&\, \psi) = \begin{cases} T & \text{if } val_{\mathcal{I}}(\phi) = T \textbf{ and } val_{\mathcal{I}}(\psi) = T \\ F & \text{otherwise} \end{cases}$$

$$val_{\mathcal{I}}(\phi \mid \psi) = \begin{cases} T & \text{if } val_{\mathcal{I}}(\phi) = T \textbf{ or } val_{\mathcal{I}}(\psi) = T \\ F & \text{otherwise} \end{cases}$$

$$val_{\mathcal{I}}(\phi \mathrel{-\!\!>} \psi) = \begin{cases} T & \text{if } val_{\mathcal{I}}(\phi) = F \textbf{ or } val_{\mathcal{I}}(\psi) = T \\ F & \text{otherwise} \end{cases}$$

$$val_{\mathcal{I}}(\phi \mathrel{<\!\!-\!\!>} \psi) = \begin{cases} T & \text{if } val_{\mathcal{I}}(\phi) = val_{\mathcal{I}}(\psi) \\ F & \text{otherwise} \end{cases}$$

Examples

Example (Formula)

$$p \ \text{->}\ (q \ \text{->}\ p)$$

Examples

Example (Formula)

$$p \ \text{->}\ (q \ \text{->}\ p)$$

Example (Interpretation)

One of four different ones on $\mathcal{P} = \{p, q\}$ that are possible:
$\mathcal{I}(p) = T$
$\mathcal{I}(q) = F$

Examples

Example (Formula)

$$p \;\text{->}\; (q \;\text{->}\; p)$$

Example (Interpretation)

One of four different ones on $\mathcal{P} = \{p, q\}$ that are possible:
$\mathcal{I}(p) = T$
$\mathcal{I}(q) = F$

Example

$val_{\mathcal{I}}(\; q \;\text{->}\; p \;) \quad =$

Examples

Example (Formula)

$$p \;{-}{>}\; (q \;{-}{>}\; p)$$

Example (Interpretation)

One of four different ones on $\mathcal{P} = \{p, q\}$ that are possible:
$\mathcal{I}(p) = T$
$\mathcal{I}(q) = F$

Example

$val_{\mathcal{I}}(\ q \;{-}{>}\; p\ ) \quad = \quad T$

Examples

Example (Formula)

$$p \ -\!\!> \ (q \ -\!\!> \ p)$$

Example (Interpretation)

One of four different ones on $\mathcal{P} = \{p, q\}$ that are possible:
$\mathcal{I}(p) = T$
$\mathcal{I}(q) = F$

Example

$val_{\mathcal{I}}(\ q \ -\!\!> \ p\ ) \quad = \quad T$
$val_{\mathcal{I}}(\ p \ -\!\!> \ (q \ -\!\!> \ p)\ ) \quad =$

Examples

Example (Formula)

$$p \ {->}\ (q \ {->}\ p)$$

Example (Interpretation)

One of four different ones on $\mathcal{P} = \{p, q\}$ that are possible:
$\mathcal{I}(p) = T$
$\mathcal{I}(q) = F$

Example

$val_{\mathcal{I}}(\ q \ {->}\ p\ ) \quad = \quad T$
$val_{\mathcal{I}}(\ p \ {->}\ (q \ {->}\ p)\ ) \quad = \quad T$

Semantic Notions of Propositional Logic

Let $\phi \in For_0$, $\Gamma \subset For_0$

Definition (Validity and Consequence Relation, overloading $\models$)

ϕ is valid in $\mathcal{I}$ (write: $\mathcal{I} \models \phi$) iff $val_{\mathcal{I}}(\phi) = T$

ϕ follows from Γ (write: $\Gamma \models \phi$) iff for all interpretations $\mathcal{I}$:

$$\text{If } \mathcal{I} \models \psi \text{ for all } \psi \in \Gamma \text{ then also } \mathcal{I} \models \phi$$

Semantic Notions of Propositional Logic

Let $\phi \in For_0$, $\Gamma \subset For_0$

Definition (Validity and Consequence Relation, overloading $\models$)

ϕ is valid in $\mathcal{I}$ (write: $\mathcal{I} \models \phi$) iff $val_{\mathcal{I}}(\phi) = T$

ϕ follows from Γ (write: $\Gamma \models \phi$) iff for all interpretations $\mathcal{I}$:

$$\text{If } \mathcal{I} \models \psi \text{ for all } \psi \in \Gamma \text{ then also } \mathcal{I} \models \phi$$

Definition (Satisfiability, Validity)

A formula is satisfiable if it is valid in some interpretation.
If ϕ is valid in *every* interpretation, i.e

$$\emptyset \models \phi \quad (\text{short: } \models \phi)$$

then ϕ is called logically valid.

Examples

Example (Formula)

$$p \; {-}{>} \; (q \; {-}{>} \; p)$$

Examples

Example (Formula)

$$p \; -\!\!> \; (q \; -\!\!> \; p)$$

Is this formula valid?

$$\models p \; -\!\!> \; (q \; -\!\!> \; p) \;?$$

Examples

$$p \ \& \ ((!\, p) \mid q)$$

Satisfiable?

Examples

$$p \ \& \ ((!\, p) \ | \ q)$$

Satisfiable? ✔

Examples

$$p \ \& \ ((!\, p) \ | \ q)$$

Satisfiable? ✔
Satisfying Interpretation?

Examples

$$p \ \& \ ((!\,p) \ | \ q)$$

Satisfiable? ✔

Satisfying Interpretation? $\mathcal{I}(p) = T, \mathcal{I}(q) = T$

Examples

$$p \ \& \ ((!\,p) \ | \ q)$$

Satisfiable? ✔
Satisfying Interpretation? $\mathcal{I}(p) = T, \mathcal{I}(q) = T$
Other Satisfying Interpretations?

Examples

$$p \ \& \ ((!\, p) \ | \ q)$$

Satisfiable?	✔
Satisfying Interpretation?	$\mathcal{I}(p) = T, \mathcal{I}(q) = T$
Other Satisfying Interpretations?	✘

Examples

$$p \ \& \ ((!\, p) \ | \ q)$$

Satisfiable? ✔
Satisfying Interpretation? $\mathcal{I}(p) = T, \mathcal{I}(q) = T$
Other Satisfying Interpretations? ✘
Therefore, also not valid!

Examples

$$p \;\&\; ((!\,p) \mid q)$$

Satisfiable? ✔
Satisfying Interpretation? $\mathcal{I}(p) = T, \mathcal{I}(q) = T$
Other Satisfying Interpretations? ✘
Therefore, also not valid!

$$p \;\&\; ((!\,p) \mid q) \models q \mid r$$

Does it hold?

Examples

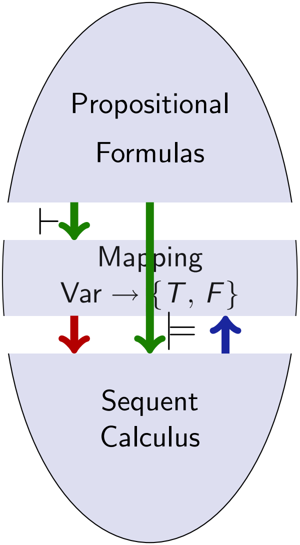
$$p \ \& \ ((!\, p) \mid q)$$

Satisfiable? ✔
Satisfying Interpretation? $\mathcal{I}(p) = T, \mathcal{I}(q) = T$
Other Satisfying Interpretations? ✘
Therefore, also not valid!

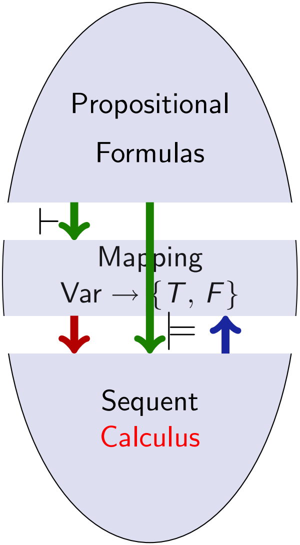
$$p \ \& \ ((!\, p) \mid q) \models q \mid r$$

Does it hold? Yes. Why?

Propositional Logic: Calculus



Propositional Logic: Calculus



Reasoning by Syntactic Transformation

Establish $\models \phi$ by finite, syntactic transformation of ϕ

Reasoning by Syntactic Transformation

Establish $\models \phi$ by finite, syntactic transformation of ϕ

Definition ((Logic) Calculus)

A set of (decidable) syntactic transformation rules $\mathcal{R}$ defining a relation $\vdash \subseteq \mathit{For}_0$ such that

- $\vdash \phi$ implies $\models \phi$: Soundness (required)
- $\models \phi$ implies $\vdash \phi$: Completeness (desirable)

Reasoning by Syntactic Transformation

Establish $\models \phi$ by finite, syntactic transformation of ϕ

Definition ((Logic) Calculus)

A set of (decidable) syntactic transformation rules $\mathcal{R}$ defining a relation $\vdash \subseteq \mathit{For}_0$ such that

- $\vdash \phi$ implies $\models \phi$: Soundness (required)
- $\models \phi$ implies $\vdash \phi$: Completeness (desirable)

Sequent Calculus based on notion of sequent

$$\underbrace{\psi_1, \ldots, \psi_m}_{\text{Antecedent}} \quad \Longrightarrow \quad \underbrace{\phi_1, \ldots, \phi_n}_{\text{Succedent}}$$

has same semantics as

$$(\psi_1 \;\&\; \cdots \;\&\; \psi_m) \quad \texttt{->} \quad (\phi_1 \mid \cdots \mid \phi_n)$$
$$\{\psi_1, \ldots, \psi_m\} \quad \models \quad \phi_1 \mid \cdots \mid \phi_n$$

Notation for Sequents

$$\psi_1, \ldots, \psi_m \quad \Longrightarrow \quad \phi_1, \ldots, \phi_n$$

Consider antecedent/succedent as sets of formulas, possibly empty

Notation for Sequents

$$\psi_1, \ldots, \psi_m \quad \Longrightarrow \quad \phi_1, \ldots, \phi_n$$

Consider antecedent/succedent as sets of formulas, possibly empty

Definition (Schema Variables)

$\phi, \psi, \ldots$ match formulas, $\Gamma, \Delta, \ldots$ match sets of formulas
Characterize infinitely many sequents with a single schematic sequent

$$\Gamma \quad \Longrightarrow \quad \Delta, \phi \;\&\; \psi$$

Matches any sequent with occurrence of conjunction in succedent

Call $\phi \;\&\; \psi$ main formula and Γ, Δ side formulas of sequent

Any sequent of the form $\Gamma, \phi \implies \Delta, \phi$ is logically valid: axiom

Sequent Calculus Rules of Propositional Logic

Write syntactic transformation schema for sequents that reflects semantics of connectives as closely as possible

$$\text{RuleName}\ \frac{\overbrace{\Gamma_1 \Longrightarrow \Delta_1 \quad \cdots \quad \Gamma_r \Longrightarrow \Delta_r}^{\text{Premisses}}}{\underbrace{\Gamma \Longrightarrow \Delta}_{\text{Conclusion}}}$$

Sequent Calculus Rules of Propositional Logic

Write syntactic transformation schema for sequents that reflects semantics of connectives as closely as possible

$$\text{RuleName}\ \frac{\overbrace{\Gamma_1 \Longrightarrow \Delta_1 \quad \cdots \quad \Gamma_r \Longrightarrow \Delta_r}^{\text{Premisses}}}{\underbrace{\Gamma \Longrightarrow \Delta}_{\text{Conclusion}}}$$

Example

$$\text{andRight}\ \frac{\Gamma \Longrightarrow \phi, \Delta \qquad \Gamma \Longrightarrow \psi, \Delta}{\Gamma \Longrightarrow \phi \ \& \ \psi, \Delta}$$

Sequent Calculus Rules of Propositional Logic

Write syntactic transformation schema for sequents that reflects semantics of connectives as closely as possible

$$\text{RuleName}\ \frac{\overbrace{\Gamma_1 \Longrightarrow \Delta_1 \quad \cdots \quad \Gamma_r \Longrightarrow \Delta_r}^{\text{Premisses}}}{\underbrace{\Gamma \Longrightarrow \Delta}_{\text{Conclusion}}}$$

Example

$$\text{andRight}\ \frac{\Gamma \Longrightarrow \phi, \Delta \qquad \Gamma \Longrightarrow \psi, \Delta}{\Gamma \Longrightarrow \phi\ \&\ \psi, \Delta}$$

Sound rule (essential): $\models (\Gamma_1 \Longrightarrow \Delta_1\ \&\ \cdots\ \&\ \Gamma_r \Longrightarrow \Delta_r) \rightarrow (\Gamma \Longrightarrow \Delta)$

Sequent Calculus Rules of Propositional Logic

Write syntactic transformation schema for sequents that reflects semantics of connectives as closely as possible

$$\text{RuleName}\ \frac{\overbrace{\Gamma_1 \Longrightarrow \Delta_1 \quad \cdots \quad \Gamma_r \Longrightarrow \Delta_r}^{\text{Premisses}}}{\underbrace{\Gamma \Longrightarrow \Delta}_{\text{Conclusion}}}$$

Example

$$\text{andRight}\ \frac{\Gamma \Longrightarrow \phi, \Delta \qquad \Gamma \Longrightarrow \psi, \Delta}{\Gamma \Longrightarrow \phi\ \&\ \psi, \Delta}$$

Sound rule (essential): $\models (\Gamma_1 \Longrightarrow \Delta_1\ \&\ \cdots\ \&\ \Gamma_r \Longrightarrow \Delta_r) \mathrel{{-}{>}} (\Gamma \Longrightarrow \Delta)$

Complete rule (desirable): $\models (\Gamma \Longrightarrow \Delta) \mathrel{{-}{>}} (\Gamma_1 \Longrightarrow \Delta_1\ \&\ \cdots\ \&\ \Gamma_r \Longrightarrow \Delta_r)$

Admissible to have no premisses (iff conclusion is valid, eg axiom)

Rules of Propositional Sequent Calculus

main	left side (antecedent)	right side (succedent)
not	$\dfrac{\Gamma \Longrightarrow \phi, \Delta}{\Gamma, !\,\phi \Longrightarrow \Delta}$	$\dfrac{\Gamma, \phi \Longrightarrow \Delta}{\Gamma \Longrightarrow !\,\phi, \Delta}$

Rules of Propositional Sequent Calculus

main	left side (antecedent)	right side (succedent)
not	$\dfrac{\Gamma \Longrightarrow \phi, \Delta}{\Gamma, !\,\phi \Longrightarrow \Delta}$	$\dfrac{\Gamma, \phi \Longrightarrow \Delta}{\Gamma \Longrightarrow !\,\phi, \Delta}$
and	$\dfrac{\Gamma, \phi, \psi \Longrightarrow \Delta}{\Gamma, \phi \ \&\ \psi \Longrightarrow \Delta}$	$\dfrac{\Gamma \Longrightarrow \phi, \Delta \qquad \Gamma \Longrightarrow \psi, \Delta}{\Gamma \Longrightarrow \phi \ \&\ \psi, \Delta}$

Rules of Propositional Sequent Calculus

main	left side (antecedent)	right side (succedent)
not	$\dfrac{\Gamma \Longrightarrow \phi, \Delta}{\Gamma, !\,\phi \Longrightarrow \Delta}$	$\dfrac{\Gamma, \phi \Longrightarrow \Delta}{\Gamma \Longrightarrow !\,\phi, \Delta}$
and	$\dfrac{\Gamma, \phi, \psi \Longrightarrow \Delta}{\Gamma, \phi \ \&\ \psi \Longrightarrow \Delta}$	$\dfrac{\Gamma \Longrightarrow \phi, \Delta \qquad \Gamma \Longrightarrow \psi, \Delta}{\Gamma \Longrightarrow \phi \ \&\ \psi, \Delta}$
or	$\dfrac{\Gamma, \phi \Longrightarrow \Delta \qquad \Gamma, \psi \Longrightarrow \Delta}{\Gamma, \phi \mid \psi \Longrightarrow \Delta}$	$\dfrac{\Gamma \Longrightarrow \phi, \psi, \Delta}{\Gamma \Longrightarrow \phi \mid \psi, \Delta}$

Rules of Propositional Sequent Calculus

main	left side (antecedent)	right side (succedent)
not	$\dfrac{\Gamma \Longrightarrow \phi, \Delta}{\Gamma, !\,\phi \Longrightarrow \Delta}$	$\dfrac{\Gamma, \phi \Longrightarrow \Delta}{\Gamma \Longrightarrow !\,\phi, \Delta}$
and	$\dfrac{\Gamma, \phi, \psi \Longrightarrow \Delta}{\Gamma, \phi \;\&\; \psi \Longrightarrow \Delta}$	$\dfrac{\Gamma \Longrightarrow \phi, \Delta \qquad \Gamma \Longrightarrow \psi, \Delta}{\Gamma \Longrightarrow \phi \;\&\; \psi, \Delta}$
or	$\dfrac{\Gamma, \phi \Longrightarrow \Delta \qquad \Gamma, \psi \Longrightarrow \Delta}{\Gamma, \phi \mid \psi \Longrightarrow \Delta}$	$\dfrac{\Gamma \Longrightarrow \phi, \psi, \Delta}{\Gamma \Longrightarrow \phi \mid \psi, \Delta}$
imp	$\dfrac{\Gamma \Longrightarrow \phi, \Delta \qquad \Gamma, \psi \Longrightarrow \Delta}{\Gamma, \phi \text{ -> } \psi \Longrightarrow \Delta}$	$\dfrac{\Gamma, \phi \Longrightarrow \psi, \Delta}{\Gamma \Longrightarrow \phi \text{ -> } \psi, \Delta}$

Rules of Propositional Sequent Calculus

main	left side (antecedent)	right side (succedent)
not	$\dfrac{\Gamma \Longrightarrow \phi, \Delta}{\Gamma, !\,\phi \Longrightarrow \Delta}$	$\dfrac{\Gamma, \phi \Longrightarrow \Delta}{\Gamma \Longrightarrow !\,\phi, \Delta}$
and	$\dfrac{\Gamma, \phi, \psi \Longrightarrow \Delta}{\Gamma, \phi \ \&\ \psi \Longrightarrow \Delta}$	$\dfrac{\Gamma \Longrightarrow \phi, \Delta \qquad \Gamma \Longrightarrow \psi, \Delta}{\Gamma \Longrightarrow \phi \ \&\ \psi, \Delta}$
or	$\dfrac{\Gamma, \phi \Longrightarrow \Delta \qquad \Gamma, \psi \Longrightarrow \Delta}{\Gamma, \phi \mid \psi \Longrightarrow \Delta}$	$\dfrac{\Gamma \Longrightarrow \phi, \psi, \Delta}{\Gamma \Longrightarrow \phi \mid \psi, \Delta}$
imp	$\dfrac{\Gamma \Longrightarrow \phi, \Delta \qquad \Gamma, \psi \Longrightarrow \Delta}{\Gamma, \phi \mathrel{-\!>} \psi \Longrightarrow \Delta}$	$\dfrac{\Gamma, \phi \Longrightarrow \psi, \Delta}{\Gamma \Longrightarrow \phi \mathrel{-\!>} \psi, \Delta}$

close $\dfrac{}{\Gamma, \phi \Longrightarrow \phi, \Delta}$ true $\dfrac{}{\Gamma \Longrightarrow \mathrm{true}, \Delta}$ false $\dfrac{}{\Gamma, \mathrm{false} \Longrightarrow \Delta}$

Justification of Rules

Justify rules by applying semantic definitions

Justification of Rules

Justify rules by applying semantic definitions

$$\text{orRight}\ \frac{\Gamma \Longrightarrow \phi,\ \psi, \Delta}{\Gamma \Longrightarrow \phi \mid \psi, \Delta}$$

Follows directly from semantics of sequents

Justification of Rules

Justify rules by applying semantic definitions

$$\text{orRight}\ \frac{\Gamma \Longrightarrow \phi,\ \psi, \Delta}{\Gamma \Longrightarrow \phi \mid \psi, \Delta}$$

Follows directly from semantics of sequents

$$\text{andRight}\ \frac{\Gamma \Longrightarrow \phi, \Delta \qquad \Gamma \Longrightarrow \psi, \Delta}{\Gamma \Longrightarrow \phi \ \&\ \psi, \Delta}$$

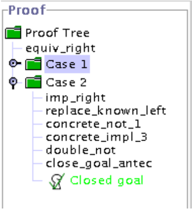
$\Gamma \texttt{->} (\phi \ \&\ \psi) \mid \Delta$ iff $\Gamma \texttt{->} \phi \mid \Delta$ and $\Gamma \texttt{->} \psi \mid \Delta$

Distributivity of & over | and ->

Sequent Calculus Proofs

Goal to prove: $\mathcal{G} \equiv \quad \psi_1, \ldots, \psi_m \implies \phi_1, \ldots, \phi_n$

- find rule $\mathcal{R}$ whose conclusion matches $\mathcal{G}$
- instantiate $\mathcal{R}$ such that conclusion identical to $\mathcal{G}$
- recursively find proofs for resulting premisses $\mathcal{G}_1, \ldots, \mathcal{G}_r$
- tree structure with goal as root
- close proof branch when rule without premiss encountered



Goal-directed proof search

In KeY tool proof displayed as a tree

A Simple Proof

$$\overline{\qquad\qquad} \qquad \overline{\qquad\qquad}$$

$$\overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}$$

$$\overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}$$

$$\overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}$$

$$\Longrightarrow (p \ \& \ (p \ {-}{>} \ q)) \ {-}{>} \ q$$

A Simple Proof

$$\dfrac{\dfrac{\dfrac{\dfrac{\quad\quad\quad\quad}{}\qquad\dfrac{\quad\quad\quad\quad}{}}{}}{p \,\&\, (p \mathrel{-\!\!>} q) \Longrightarrow q}}{\Longrightarrow (p \,\&\, (p \mathrel{-\!\!>} q)) \mathrel{-\!\!>} q}$$

A Simple Proof

$$\dfrac{\dfrac{\dfrac{\overline{} \qquad \overline{}}{p, (p -> q) \Longrightarrow q}}{p \;\&\; (p -> q) \Longrightarrow q}}{\Longrightarrow (p \;\&\; (p -> q)) -> q}$$

A Simple Proof

$$\dfrac{\dfrac{\dfrac{\dfrac{}{p \Longrightarrow q,\ p} \qquad \dfrac{}{p,\ q \Longrightarrow q}}{p,\ (p \mathrel{-\!\!>} q) \Longrightarrow q}}{p \ \& \ (p \mathrel{-\!\!>} q) \Longrightarrow q}}{\Longrightarrow (p \ \& \ (p \mathrel{-\!\!>} q)) \mathrel{-\!\!>} q}$$

A Simple Proof

$$
\dfrac{\dfrac{\overline{p \Longrightarrow q,\ p}^{\,*}\ \textsc{Close} \qquad \overline{p,\ q \Longrightarrow q}^{\,*}\ \textsc{Close}}{\dfrac{p,\ (p \mathbin{{-}{>}} q) \Longrightarrow q}{\dfrac{p\ \&\ (p \mathbin{{-}{>}} q) \Longrightarrow q}{\Longrightarrow (p\ \&\ (p \mathbin{{-}{>}} q)) \mathbin{{-}{>}} q}}}}
$$

A Simple Proof

$$\dfrac{\textsc{Close}\dfrac{*}{p \Longrightarrow q,\ p} \qquad \dfrac{*}{p,\ q \Longrightarrow q}\textsc{Close}}{\dfrac{p,\ (p \mathrel{-\!\!>} q) \Longrightarrow q}{\dfrac{p\ \&\ (p \mathrel{-\!\!>} q) \Longrightarrow q}{\Longrightarrow (p\ \&\ (p \mathrel{-\!\!>} q)) \mathrel{-\!\!>} q}}}$$

A proof is closed iff all its branches are closed

Demo

`Examples/prop.key`

DPLL: Davis-Putnam-Logeman-Loveland

Basis for fast SAT solving in propositional logic

```
refute(S):
    while false ∉ S do
        if S=∅ then return sat
        if S does not contain unit clause then
            P := choose variable
            /* split on P */
            refute(S with P:=false);
            refute(S with P:=true);
        else
            K := choose unit clause from S
            /* propagate K */
            drop all clauses containing K
            drop complement of K from all clauses
        end if
    end while
    return unsat
```

$A \mid B \mid C$

$!\,A \mid B \mid !\,D$

$!\,A \mid C$

$!\,A \mid !\,C \mid D$

$A \mid !\,C$

$!\,B$

$A \mid B \mid C$
$!A \mid B \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$
$!B$

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

propagate($!B$)

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

propagate($!B$)

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

refute(with A:=true)

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

propagate(C)

refute(with A:=false)

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

$A \mid C$
$!\,A \mid !\,D$
$!\,A \mid C$
$!\,A \mid !\,C \mid D$
$A \mid !\,C$

propagate($!\,B$)

$A \mid C$
$!\,A \mid !\,D$
$!\,A \mid C$
$!\,A \mid !\,C \mid D$
$A \mid !\,C$

refute(with A:=true)

$A \mid C$
$!\,A \mid !\,D$
$!\,A \mid C$
$!\,A \mid !\,C \mid D$
$A \mid !\,C$

propagate(C)

refute(with A:=false)

$A \mid C$
$!\,A \mid !\,D$
$!\,A \mid C$
$!\,A \mid !\,C \mid D$
$A \mid !\,C$

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

propagate($!B$)

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$

refute(with A:=true)

$!D$
C
$!C \mid D$

propagate(C)

refute(with A:=false)

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

propagate($!B$)

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

refute(with A:=true)

$!D$
C
$!C \mid D$

propagate(C)

$!D$
C
$!C \mid D$

refute(with A:=false)

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

propagate($!B$)

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$

refute(with A:=true)

$!D$
C
$!C \mid D$

propagate(C)

$!D$

D

propagate($!D$)

$!D$
D

refute(with A:=false)

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

propagate($!B$)

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

refute(with A:=true)

$!D$
C
$!C \mid D$

propagate(C)

$!D$
D

propagate($!D$)

unsat! empty clause

refute(with A:=false)

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

propagate($!B$)

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

refute(with A:=true)

$!D$
C
$!C \mid D$

propagate(C)

$!D$

D

propagate($!D$)

unsat! empty clause

refute(with A:=false)

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

propagate($!B$)

$A \mid C$
$!A \mid !D$
$!A \mid C$
$!A \mid !C \mid D$
$A \mid !C$

refute(with A:=true)

$!D$
C
$!C \mid D$

propagate(C)

$!D$
D

propagate($!D$)

unsat! empty clause

refute(with A:=false)

C
$!C$

propagate(C)

C
$!C$

$A \mid C$
$!\, A \mid !\, D$
$!\, A \mid C$
$!\, A \mid !\, C \mid D$
$A \mid !\, C$

propagate($!\, B$)

$A \mid C$
$!\, A \mid !\, D$
$!\, A \mid C$
$!\, A \mid !\, C \mid D$
$A \mid !\, C$

refute(with A:=true)

$!\, D$
C
$!\, C \mid D$

propagate(C)

$!\, D$
D

propagate($!\, D$)

unsat! empty clause

refute(with A:=false)

C
$!\, C$

propagate(C)

unsat! empty clause

How Expressive is Propositional Logic?

Finite set of elements $N = \{1, \ldots, n\}$

Let p_{ij} denote $p(i) = j$. p is a permutation on N is expressible ...
Groups, Latin squares, Sudoku, ...
Even finite numbers (e.g., bitwise encoding)

Limitations of Propositional Logic

Fixed, finite number of objects

Cannot express: let g be group with arbitrary number of elements

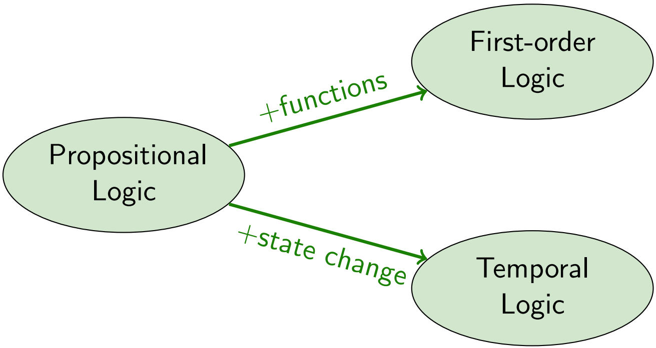
No functions or relations with arguments

Can express: finite function/relation table p_{ij}
Cannot express: properties of function/relation on all arguments, e.g., $+$ is associative

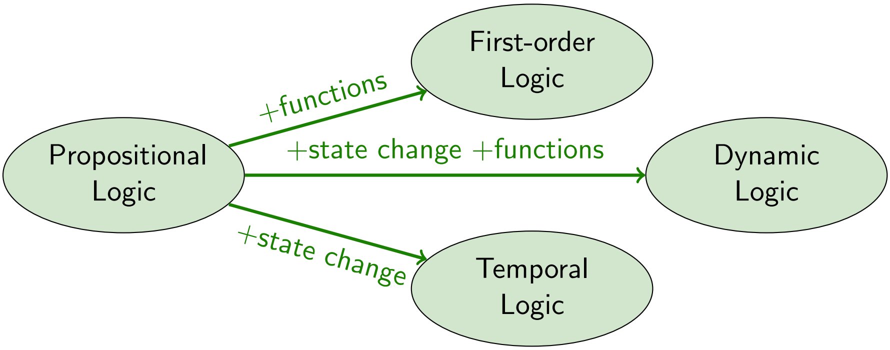
Static interpretation

Programs change value of their variables, e.g., via assignment, call, etc.
Propositional formulas look at one single interpretation at a time

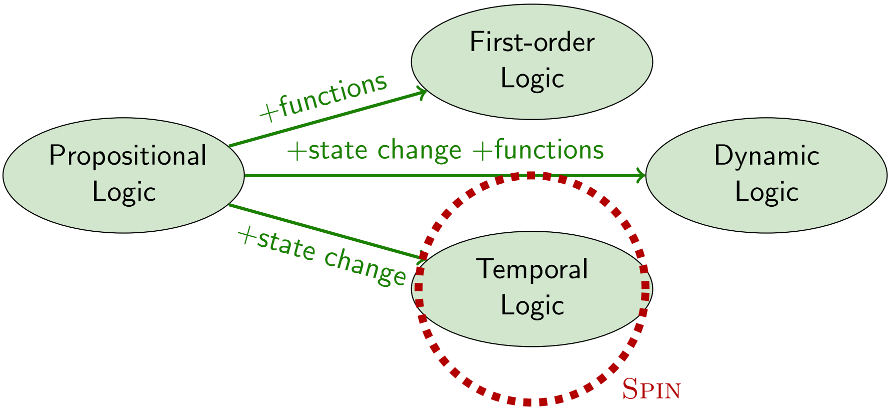
Beyond the Limitations of Propositional Logic



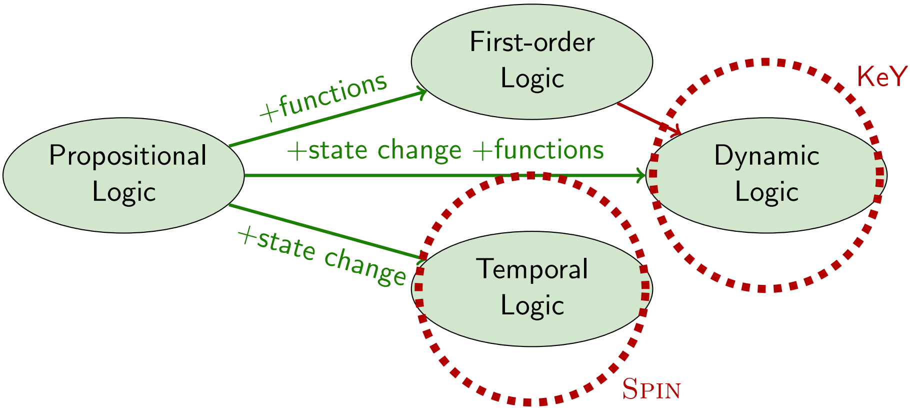
Beyond the Limitations of Propositional Logic



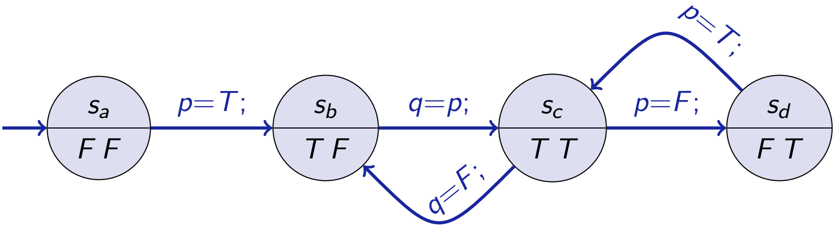
Beyond the Limitations of Propositional Logic



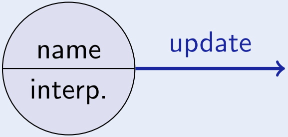
Beyond the Limitations of Propositional Logic



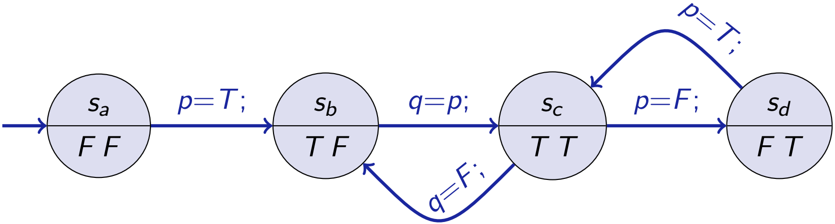
Outline



Notation



Transition Systems / Kripke Structures



- Each state has its own propositional interpretation!
- Computations, or *runs*, are infinite paths through states
- Infinitely many different runs
- How to express (for example) that either p or q changes its value infinitely often in each run?

Linear Temporal Logic

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

Linear 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:

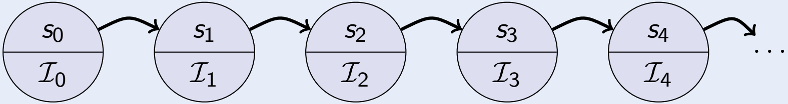
- **Always** If ϕ is a formula then so is $[\,]\phi$
- **Sometimes** If ϕ is a formula then so is $<>\phi$
- **Until** If ϕ and ψ are formulas then so is $\phi\,\mathtt{U}\,\psi$

Concrete Syntax

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

Semantics of Temporal Logic

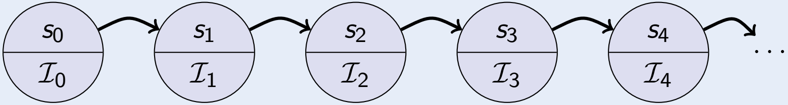
A run σ is an infinite chain of states



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

Semantics of Temporal Logic

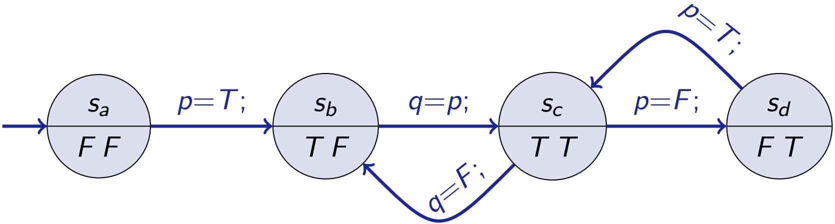
A run σ is an infinite chain of states



$\mathcal{I}_j$ 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

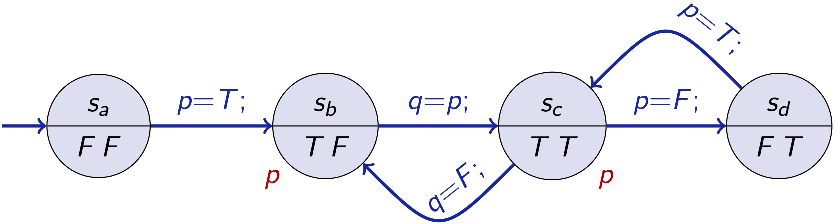


Definition (Validity Relation)

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

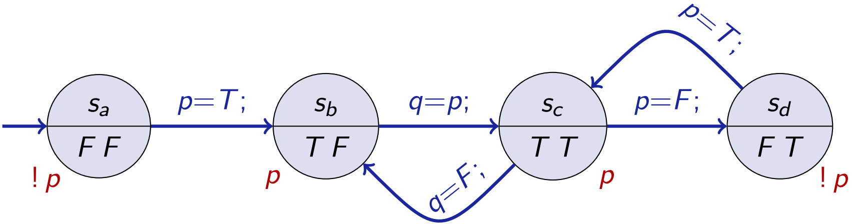


Definition (Validity Relation)

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



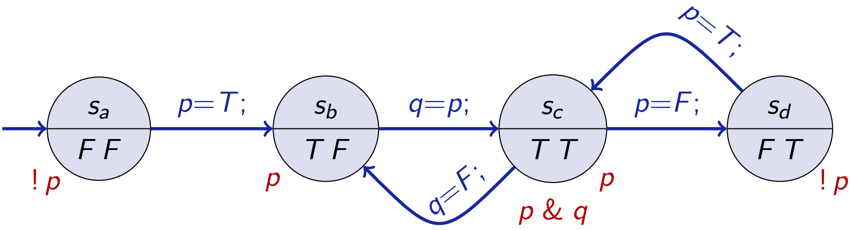
Definition (Validity Relation)

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

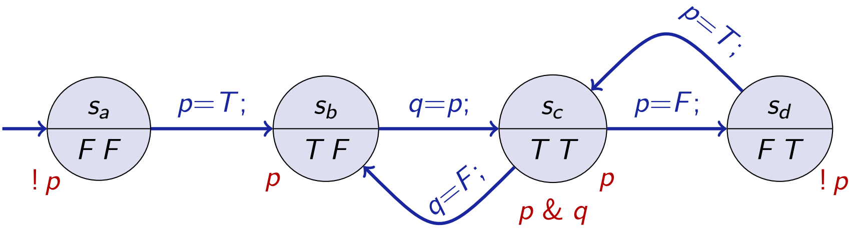


Definition (Validity Relation)

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



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 $p \in \mathcal{P}$.

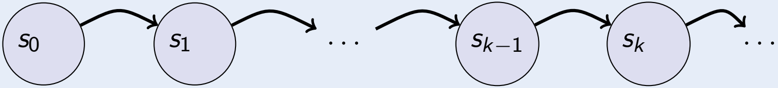
$\sigma \models\ !\phi$ iff not $\sigma \models \phi$ (write $\sigma \not\models \phi$)

$\sigma \models \phi \,\&\, \psi$ 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 $\sigma \models \psi$

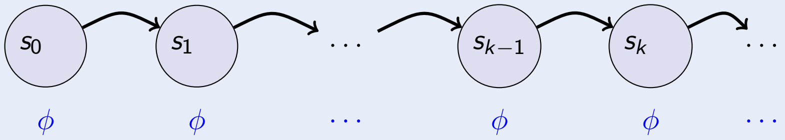
Semantics of Temporal Logic



Definition (Validity Relation for Temporal Connectives)

Given a run $\sigma = s_0\, s_1, s_2 \ldots$

Semantics of Temporal Logic

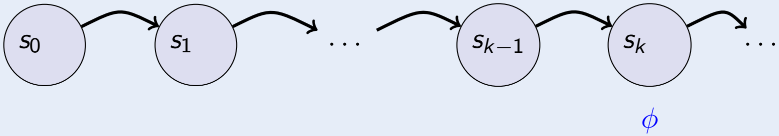


Definition (Validity Relation for Temporal Connectives)

Given a run $\sigma = s_0\, s_1, s_2 \dots$

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

Semantics of Temporal Logic



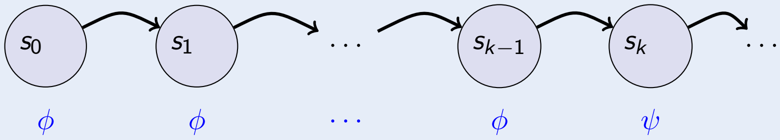
Definition (Validity Relation for Temporal Connectives)

Given a run $\sigma = s_0\, s_1, s_2 \ldots$

$\sigma \models []\phi$ 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



Definition (Validity Relation for Temporal Connectives)

Given a run $\sigma = s_0\, s_1, s_2 \dots$

$\sigma \models [\,]\phi$ 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.

Complex Properties

Infinitely Often

$$[]<>\phi$$

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

What does this mean?

$$<>[]\phi$$

Complex Properties

Infinitely Often

$$[]<>\phi$$

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

Finally Always

$$<>[]\phi$$

During a run the formulas ϕ will become eventually stay true indefinitely.

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

$$<>[]\phi$$

Valid?

Examples

$$<>[]\phi$$

Valid?

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

Examples

$$<>[]\phi$$

Valid?

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

Examples

$$<>[]\phi$$

Valid?

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

Valid in some run?

Examples

$$<>[]\phi$$

Valid?

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

Valid in some run?

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

Examples

$$<>[]\phi$$

Valid?

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

Valid in some run?

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

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

Both are valid!

Examples

$$<>[]\phi$$

Valid?

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

Valid in some run?

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

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

Both are valid!

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

Transition systems revisited

Definition (Transition System)

A Transition System $\mathcal{T} = (S, Ini, \delta, \mathcal{I})$ 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 $\mathcal{I}$ 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 $s_0 \in Ini$ and $(s_i, s_{i+1}) \in \delta$ for all i.

Semantics of Temporal Logic

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 $\mathcal{T}$.

Background Literature

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.

Ben-Ari Mordechai Ben-Ari: *Principles of the Spin Model Checker*, Springer, 2008(!). Section 5.2.1 (PROMELA examples briefly)