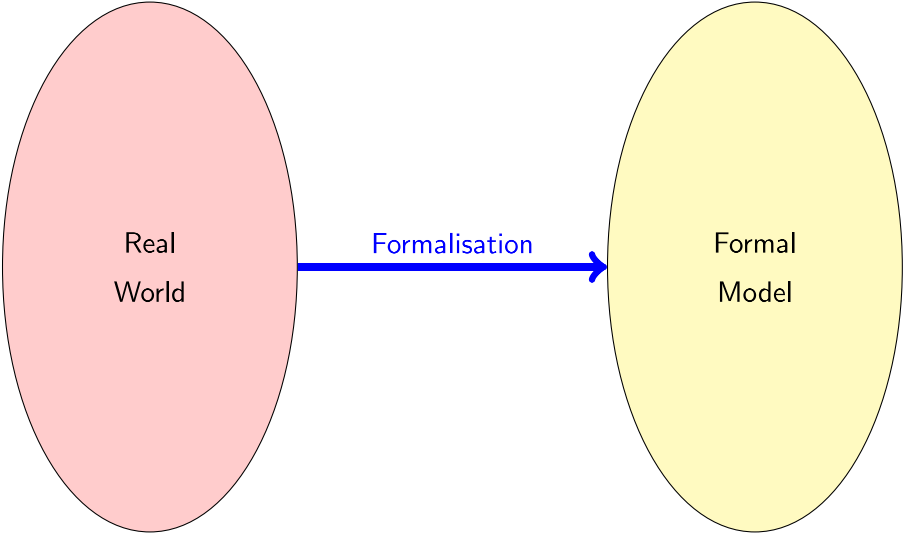
Formal Specification and Verification

Formal Modeling with Propositional Logic

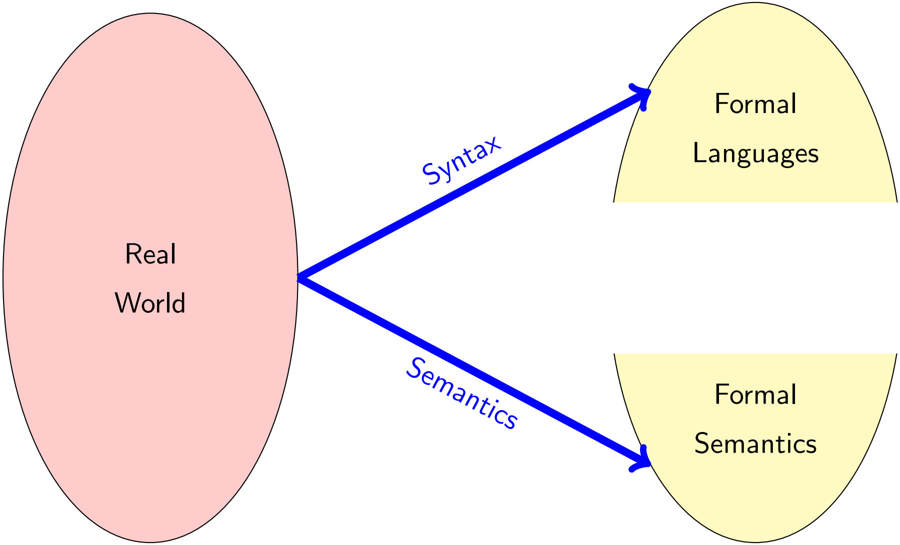
Bernhard Beckert

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

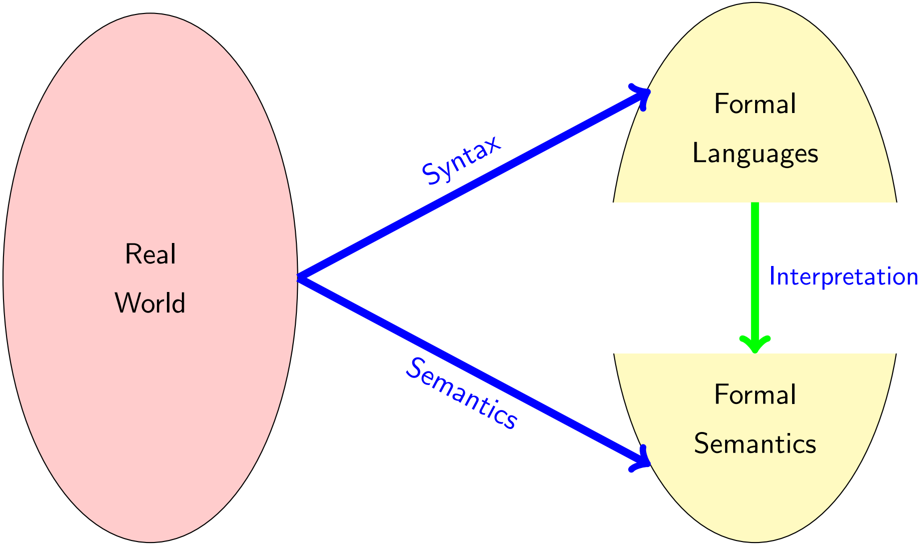
Formalisation



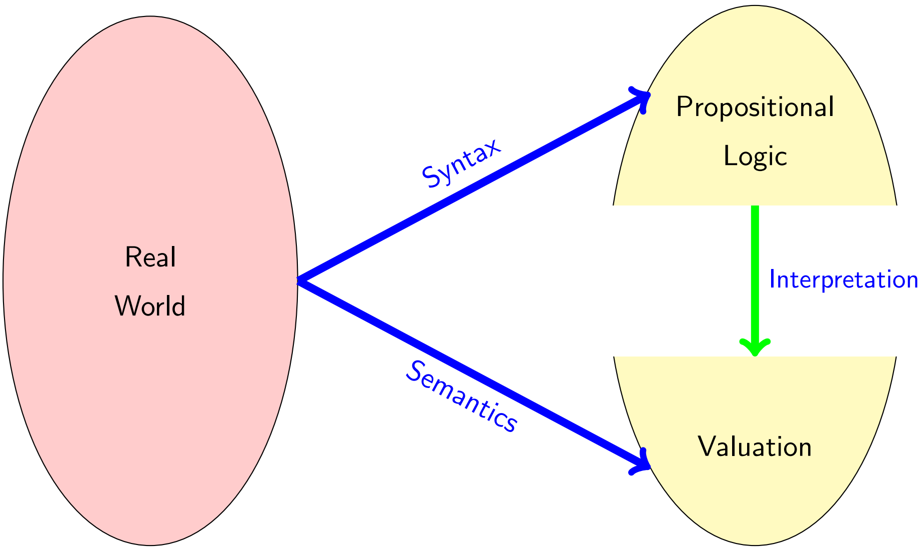
Formalisation: Syntax, Semantics



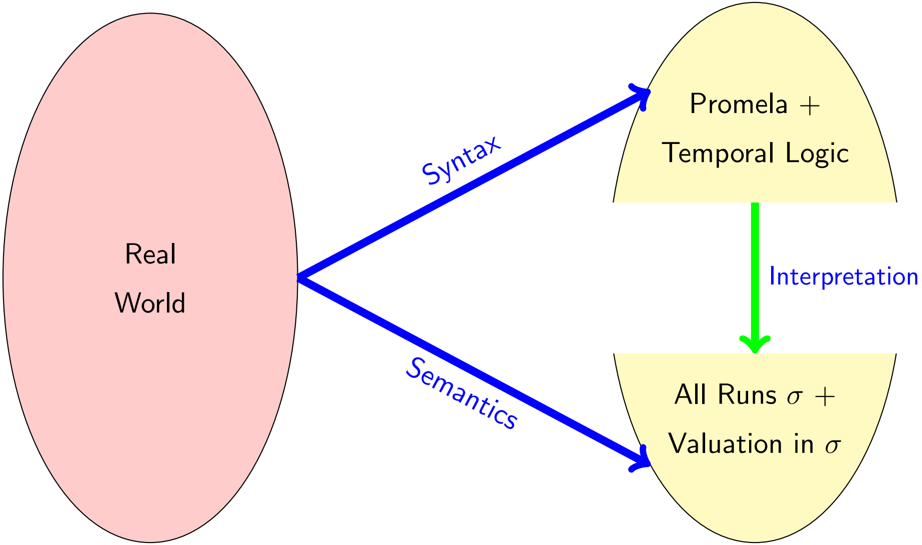
Formalisation: Syntax, Semantics



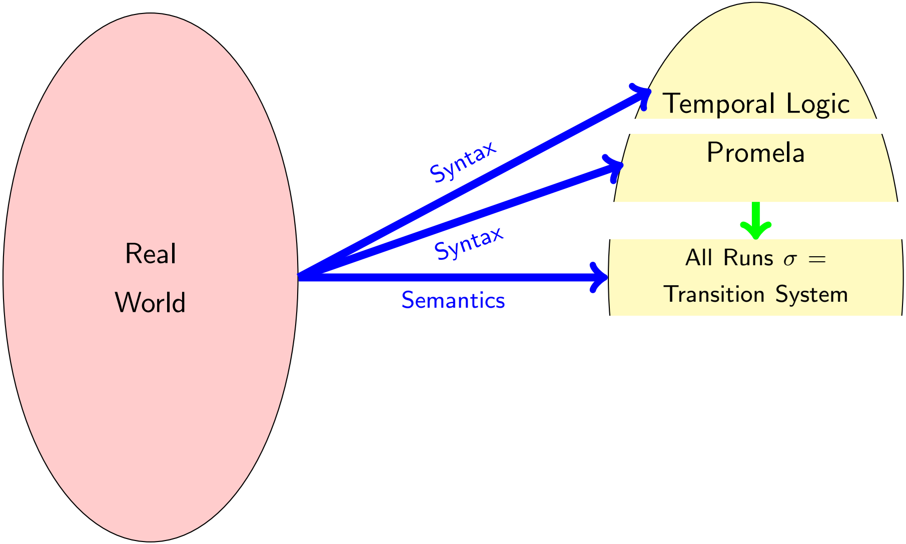
Formalisation: Syntax, Semantics



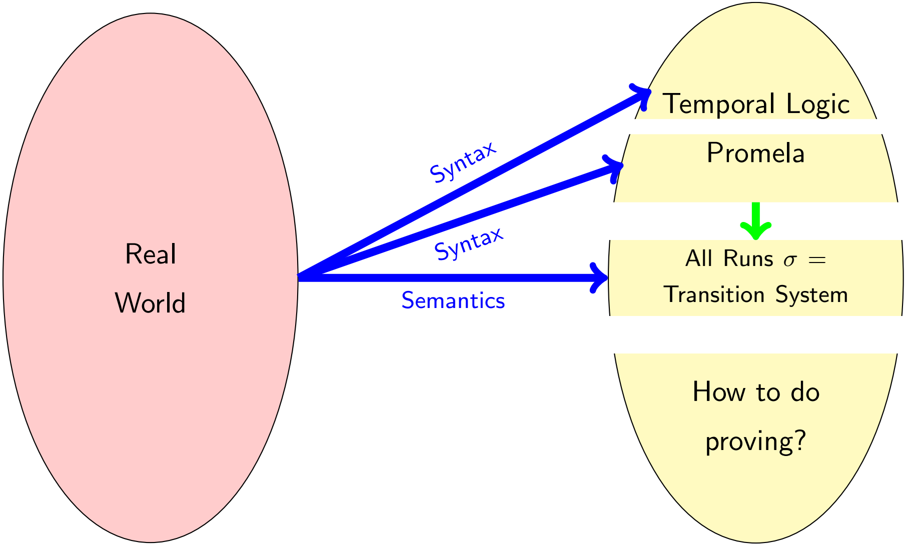
Formalisation: Syntax, Semantics



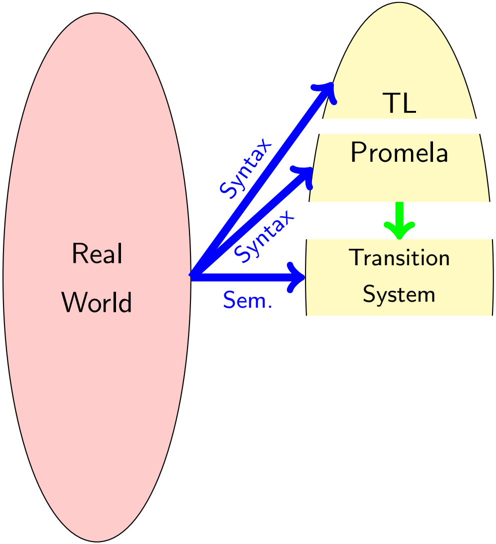
Formalisation: Syntax, Semantics



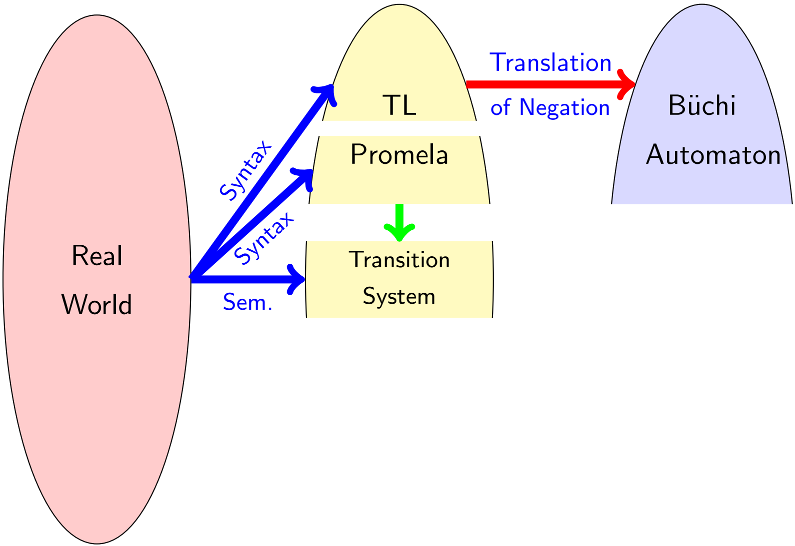
Formalisation: Syntax, Semantics, Proving



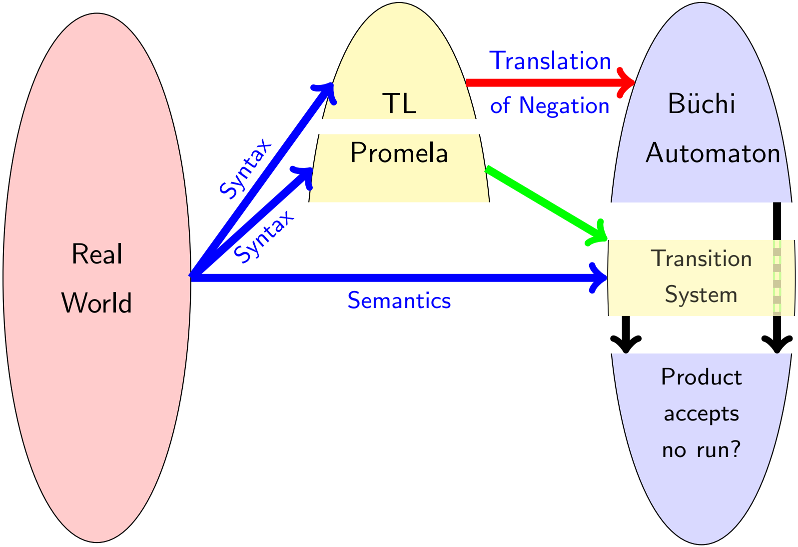
Formal Verification: Model Checking



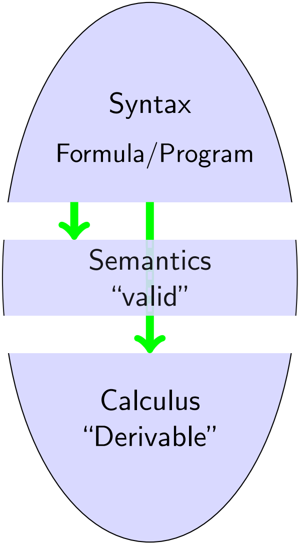
Formal Verification: Model Checking



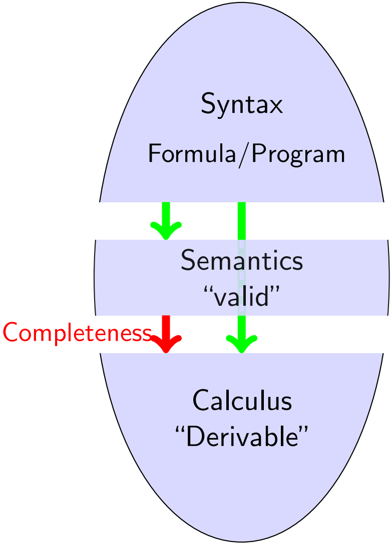
Formal Verification: Model Checking



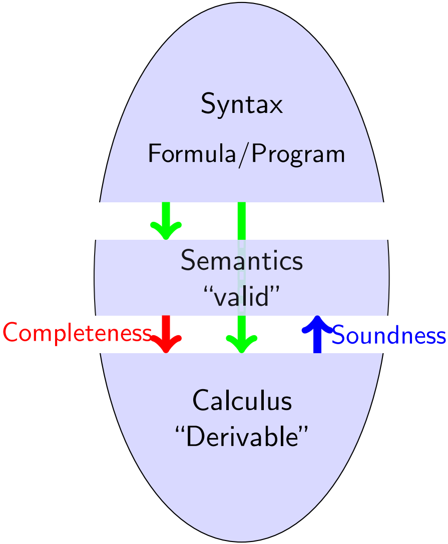
Syntax, Semantics, Calculus



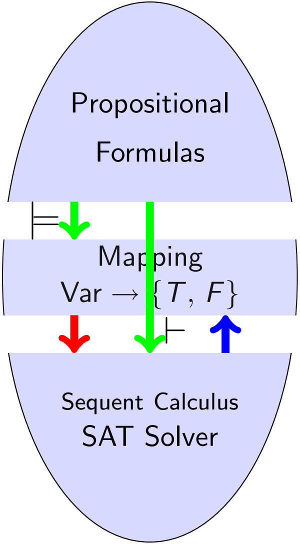
Syntax, Semantics, Calculus



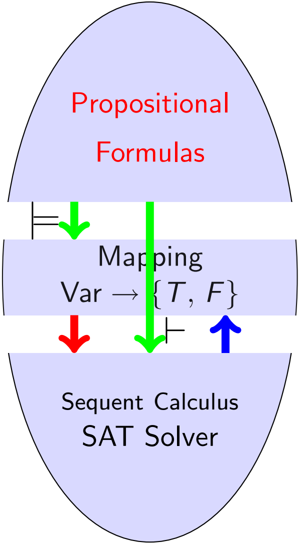
Syntax, Semantics, Calculus



Propositional Logic



Propositional Logic— Syntax



Syntax of Propositional Logic

Signature

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

Syntax of Propositional Logic

Signature

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

Propositional Connectives

true false & | ! -> <->

Syntax of Propositional Logic

Signature

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

Propositional Connectives

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

Set of Propositional Formulas For_0

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

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

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

Syntax of Propositional Logic

Signature

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

Propositional Connectives (KeY notation)

true false & | ! -> <->

Set of Propositional Formulas For_0

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

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

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

Remark on Concrete Syntax

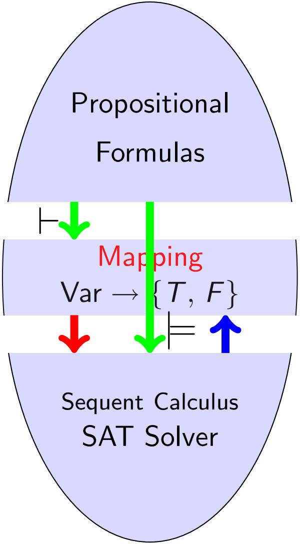
<table>
<tr><th></th><th>Text book</th><th>Spin</th><th>KeY</th></tr>
<tr><td>Negation</td><td>$\neg$</td><td>!</td><td>!</td></tr>
<tr><td>Conjunction</td><td>$\wedge$</td><td>&&</td><td>&</td></tr>
<tr><td>Disjunction</td><td>$\vee$</td><td>||</td><td>|</td></tr>
<tr><td>Implication</td><td>$\rightarrow$,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

Remark on Concrete Syntax

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

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

Propositional Logic— Semantics



Semantics of Propositional Logic

Interpretation $\mathcal{I}$

Assigns a truth value to each propositional variable

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

Semantics of Propositional Logic

Interpretation $\mathcal{I}$

Assigns a truth value to each propositional variable

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

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 (Cont'd)

Valuation function (Cont'd)

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

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

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

$$\mathit{val}_{\mathcal{I}}(\phi \;\texttt{->}\; \psi) = \begin{cases} T & \text{if } \mathit{val}_{\mathcal{I}}(\phi) = F \textbf{ or } \mathit{val}_{\mathcal{I}}(\psi) = T \\ F & \mathit{otherwise} \end{cases}$$

$$\mathit{val}_{\mathcal{I}}(\phi \;\texttt{<->}\; \psi) = \begin{cases} T & \text{if } \mathit{val}_{\mathcal{I}}(\phi) = \mathit{val}_{\mathcal{I}}(\psi) \\ F & \mathit{otherwise} \end{cases}$$

Examples

Formula

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

Examples

Formula

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

Interpretation

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

Examples

Formula

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

Interpretation

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

Valuation

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

Examples

Formula

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

Interpretation

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

Valuation

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

Examples

Formula

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

Interpretation

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

Valuation

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

Examples

Formula

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

Interpretation

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

Valuation

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

Semantic Notions of Propositional Logic

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

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

ϕ is true in $\mathcal{I}$ and $\mathcal{I}$ is a model of ϕ (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 (Model and Consequence Relation, overloading $\models$)

ϕ is true in $\mathcal{I}$ and $\mathcal{I}$ is a model of ϕ (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 true in some interpretation.
If ϕ is true in *every* interpretation, i.e.

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

then ϕ is called (logically) valid.

Examples

Formula (same as before)

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

Examples

Formula (same as before)

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

Is this formula valid?

$$\models p \;\texttt{->}\; (q \;\texttt{->}\; p)\;?$$

Examples

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

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

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

Satisfiable? ✔

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

Other Satisfying Interpretations? ✘

Therefore, also not valid!

Examples

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

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

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

Does it hold?

Examples

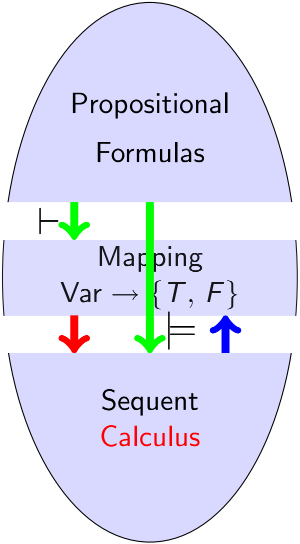
$$p \ \& \ ((!\, p) \ | \ q)$$

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

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

Does it hold? Yes. Why?

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

(Logic) Calculus

A set of syntactic transformation rules $\mathcal{R}$ defining a relation $\vdash \subseteq \mathit{For}_0$ such that $\vdash \phi$ implies $\models \phi$.

- $\vdash \phi$ 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

(Logic) Calculus

A set of syntactic transformation rules $\mathcal{R}$ defining a relation $\vdash \subseteq$ *For*$_0$ such that $\vdash \phi$ implies $\models \phi$.

- $\vdash \phi$ 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

$$\begin{array}{ccc} (\psi_1 \ \& \cdots \& \ \psi_m) & \texttt{->} & (\phi_1 \mid \cdots \mid \phi_n) \\ \{\psi_1, \ldots, \psi_m\} & \models & \phi_1 \mid \cdots \mid \phi_n \end{array}$$

Notation for Sequents

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

Consider antecedent/succedent as sets of formulas, may be empty

Notation for Sequents

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

Consider antecedent/succedent as sets of formulas, may be empty

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 $\Gamma, \phi \Longrightarrow \Delta, \phi$ 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): $\models (\Gamma_1 \Longrightarrow \Delta_1 \ \& \cdots \& \ \Gamma_r \Longrightarrow \Delta_r) \ {-}{>} \ (\Gamma \Longrightarrow \Delta)$

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	$$\frac{\Gamma \Longrightarrow \phi, \Delta}{\Gamma, !\,\phi \Longrightarrow \Delta}$$	$$\frac{\Gamma, \phi \Longrightarrow \Delta}{\Gamma \Longrightarrow !\,\phi, \Delta}$$
and	$$\frac{\Gamma, \phi,\ \psi \Longrightarrow \Delta}{\Gamma, \phi\ \&\ \psi \Longrightarrow \Delta}$$	$$\frac{\Gamma \Longrightarrow \phi, \Delta \qquad \Gamma \Longrightarrow \psi, \Delta}{\Gamma \Longrightarrow \phi\ \&\ \psi, \Delta}$$

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	$\dfrac{\Gamma \Longrightarrow \phi, \Delta \qquad \Gamma, \psi \Longrightarrow \Delta}{\Gamma, \phi \,\texttt{->}\, \psi \Longrightarrow \Delta}$	$\dfrac{\Gamma, \phi \Longrightarrow \psi, \Delta}{\Gamma \Longrightarrow \phi \,\texttt{->}\, \psi, \Delta}$

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	$\dfrac{\Gamma \Longrightarrow \phi, \Delta \qquad \Gamma, \psi \Longrightarrow \Delta}{\Gamma, \phi \mathbin{->} \psi \Longrightarrow \Delta}$	$\dfrac{\Gamma, \phi \Longrightarrow \psi, \Delta}{\Gamma \Longrightarrow \phi \mathbin{->} \psi, \Delta}$

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

Justification of Rules

Compute rules by applying semantic definitions

Justification of Rules

Compute 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

Compute 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

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

Γ -> $(\phi\ \&\ \psi) \mid \Delta$ iff Γ -> $\phi \mid \Delta$ and Γ -> $\psi \mid \Delta$

Distributivity of & over | and ->

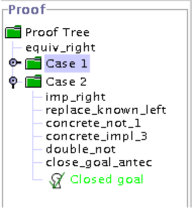
Sequent Calculus Proofs

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

- 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 $\mathcal{G}_1$, ..., $\mathcal{G}_r$
- tree structure with goal as root
- close proof branch when rule without premiss encountered

Goal-directed proof search

In KeY tool proof displayed as JAVA Swing tree



A Simple Proof

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

A Simple Proof

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

A Simple Proof

$$\dfrac{\dfrac{\dfrac{\text{—} \qquad \text{—}}{p,\ (p \mathbin{{-}{>}} q) \Longrightarrow q}}{p \ \&\ (p \mathbin{{-}{>}} q) \Longrightarrow q}}{\Longrightarrow (p \ \&\ (p \mathbin{{-}{>}} q)) \mathbin{{-}{>}} q}$$

A Simple Proof

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

A Simple Proof

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

A Simple Proof

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

A proof is closed iff all its branches are closed

Demo

`Examples/prop.key`

How Expressive is Propositional Logic?

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

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

We will see that Promela data structures are carefully designed such that computation states can be encoded in propositional logic

Limitations of Propositional Logic

Fixed, finite number of objects

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

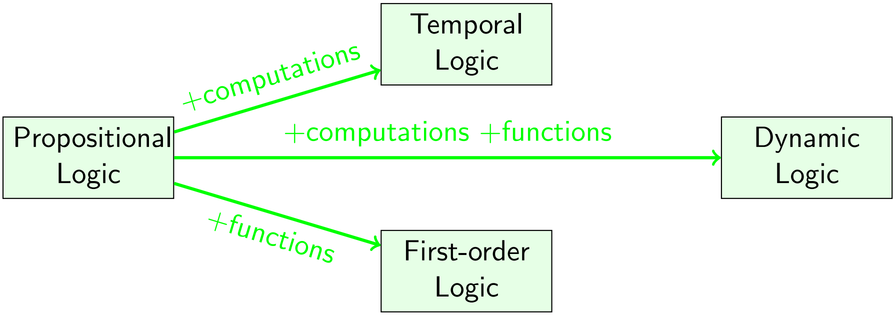
No functions or relations with arguments

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

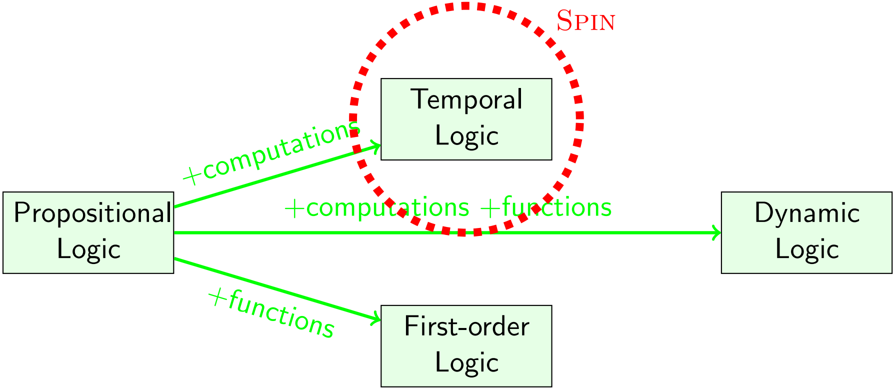
Static interpretation

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