Intuitionistic Logic

Classical Logic Platonic notion truth

Law of Excluded Middle $p \vee \neg p$.

$$(P = NP) \vee (P \neq NP)$$

Non constructive proof.

Proposition There are irrational numbers x and y such that x^y is rational number.

Proof: Consider $\sqrt{2}^{\sqrt{2}}$

Case 1 $\sqrt{2}^{\sqrt{2}}$ is rational. Proposition is True $x = \sqrt{2}$; $y = \sqrt{2}$

Case 2 $\sqrt{2}^{\sqrt{2}}$ is irrational.

Take $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = (\sqrt{2})^2 = 2.$$

Theorem For any odd prime p, p is the sum of 2 squares iff $p \equiv 1 \bmod 4$.

Intuitionistic Logic

Truth is based on construction of an argument.

RHK interpretation

- $\psi_1 \wedge \psi_2$ can be proved if there is a proof of φ and a proof of ψ.
- $\psi_1 \vee \psi_2$ can be proved if you identify $i \in \{1, 2\}$ and present a proof of ψ_i.
- $\psi_1 \to \psi_2$ can be proved if there is an algorithm/function that takes a proof of ψ_1 and produces a proof of ψ_2.
- $\perp$ has a non-existent proof.

"$\neg\psi$" $= \psi \to \perp$: Given a proof for ψ we have an algorithm to transform it into a non-existent object.

$\psi \to (\neg\neg\psi) = \psi \to ((\psi \to \perp) \to \perp)$:

We have a proof of ψ.

Suppose I have a proof for $\psi \to \perp$ i.e. Algorithm that transforms proofs of ψ into a "proof for $\perp$".

Take the proof for ψ and use the

algorithm for $\psi \to \bot$ to construct a proof for $\bot$.

$\neg\neg\psi \to \psi$: does not hold.

Syntax

Assume a countable set of propositions P.

$$\varphi ::= \bot \mid p \mid (\varphi \vee \varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \to \varphi)$$

Proof System

Rule of inference $$\frac{\varphi \qquad \varphi \to \psi}{\psi} \ (MP)$$

Axioms

$$\frac{}{\varphi \to (\psi \to \varphi)} \qquad \boxed{\frac{}{((\varphi \to \bot) \to \bot) \to \varphi}}$$

$$\frac{}{(\varphi \to (\psi \to \rho)) \to ((\varphi \to \rho) \to (\psi \to \rho))}$$

$$\frac{}{(\varphi \wedge \psi) \to \varphi} \qquad \frac{}{(\varphi \wedge \psi) \to \psi}$$

$$\frac{}{\varphi \to (\psi \to (\varphi \wedge \psi))}$$

$$\frac{}{\varphi \to (\varphi \vee \psi)} \qquad \frac{}{\psi \to (\varphi \vee \psi)}$$

$\psi \to (\varphi \vee \psi)$

$$(\varphi \to \rho) \to ((\psi \to \rho) \to ((\varphi \vee \psi) \to \rho))$$

Definition $\Gamma \vdash \varphi$

"φ can be proved from Γ"

Deduction Theorem If $\Gamma \cup \{\varphi\} \vdash \psi$ then $\Gamma \vdash \varphi \to \psi$.

Example $\vdash \varphi \to \neg\neg\varphi$ or

$\vdash \varphi \to ((\varphi \to \bot) \to \bot)$

$\varphi, \varphi \to \bot \vdash \varphi \to \bot$ (hypothesis)

$\varphi, \varphi \to \bot \vdash \varphi$ (hypothesis)

$\varphi, \varphi \to \bot \vdash \bot$ (MP)

$\varphi, \vdash (\varphi \to \bot) \to \bot$ (Deduction Thm)

$\vdash \varphi \to ((\varphi \to \bot) \to \bot)$ (Deduction Thm)

Kripke Structure Semantics

Kripke Structure $\mathcal{K} = (W, \leq, \Vdash)$

- W is a set of "worlds"
- $\leq \subseteq W \times W$ that is a partial order.

$\leq \subseteq W \times W$ ...

(a) $\leq$ is reflexive $\forall w.\ w \leq w$.

(b) $\leq$ is transitive

$\forall w_1, w_2, w_3 \quad w_1 \leq w_2,\ w_2 \leq w_3 \Rightarrow w_1 \leq w_3$

(c) $\leq$ is antisymmetric

$\forall w_1, w_2, \quad w_1 \leq w_2$ and $w_2 \leq w_1 \Rightarrow w_1 = w_2$.

- $\Vdash \subseteq W \times P$.

  i.e. $w \Vdash p$ "p is true in w".

  Such that $\forall w_1, w_2 \quad w_1 \leq w_2$.

  $\forall p.\ w_1 \Vdash p \Rightarrow w_2 \Vdash p$.

Satisfaction "$K, w \models \varphi$" to mean that φ is true in world w of K.

- $K, w \models \bot$ is never true.

  (or $K, w \not\models \bot$)

- $K, w \models p$ iff $w \Vdash p$.

- $K, w \models \varphi \vee \psi$ iff $K, w \models \varphi$ or $K, w \models \psi$

- $K, w \models \varphi \wedge \psi$ iff $K, w \models \varphi$ and $K, w \models \psi$.

- $K, w \models \varphi \to \psi$ iff $\forall w' \geq w$

if $K, w' \models \varphi$ then $K, w' \models \psi$.

$K, w \models \neg \varphi$ iff $K, w \models \varphi \to \bot$

iff $\forall w' \geq w$, $K, w' \not\models \varphi$

"$K, w \not\models \varphi$" means "$K, w \models \varphi$ does not hold".

Proposition If $K, w \models \varphi$ and $w \leq w'$ then $K, w' \models \varphi$.

Definition For any set of formulas Γ and φ.

- $\Gamma \models \varphi$ iff $\forall K, w$ if $\underbrace{K, w \models \Gamma}_{\forall \psi \in \Gamma,\ K, w \models \psi}$ then $K, w \models \varphi$

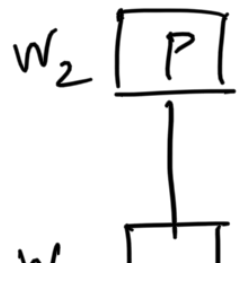
- φ is a tautology or $\models \varphi$ iff $\emptyset \models \varphi$.

Completeness Theorem

$\Gamma \vdash \varphi$ iff $\Gamma \models \varphi$

Example

K



$\{w_1, w_2\}$, $w_1 \leq w_2$

$w_1 \Vdash p$.

w_1

$\not\models (p \vee \neg p)$, $\boxed{K, w_1 \not\models p \vee \neg p.}$

$K, w_1 \not\models p.$

Since $K, w_2 \models p$ and $w_1 \leq w_2$

$K, w_1 \not\models \neg p.$

$K, w_1 \models ((p \to \bot) \to \bot) \to p)$

Theorem The problem of checking if $\models \varphi$ is PSPACE-complete.

Proof: $\models \varphi$ iff $K, w \models \varphi$ for all K of bounded size.

Implicational Fragment.

$$\varphi ::= \bot \mid p \mid \varphi \to \varphi$$

$$\frac{\varphi \qquad \varphi \to \psi}{\psi}$$

$$\frac{}{\varphi \to (\psi \to \varphi)}$$

$$\frac{}{(\varphi \to (\psi \to \rho)) \to ((\varphi \to \rho) \to (\psi \to \rho))}$$