

# Intuitionistic logic for dummies

Moritz Y. Becker

October 24, 2002

## **Structure**

1. Philosophical background
2. Proof theory
3. Algebraic semantics

## **What is Intuitionism?**

- Logic as part of Mathematics
- natural numbers are intuitively given to us
- Mathematics as mental constructions

### **Some related/opposing isms**

- Platonism/Realism
- Logicism
- Finitism
- Formalism

# Luitzen Egbertus Jan Brouwer

## (1881–1966)



"One cannot inquire into the foundations and nature of mathematics without delving into the question of the operations by which the mathematical activity of the mind is conducted. If one failed to take that into account, then one would be left studying only the language in which mathematics is represented rather than the essence of mathematics."

"It does not make sense to think of truth or falsity of a mathematical statement independently of our knowledge concerning the statement. A statement is true if we have a proof of it, and false if we can show that the assumption that there is a proof for the statement leads to a contradiction."

## David Hilbert

(1862–1943)



“Denying a mathematician use of the principle of excluded middle is like denying an astronomer his telescope or a boxer the use of his fists. To prohibit existence statements and the principle of excluded middle is tantamount to relinquishing the science of mathematics altogether.”

## What is truth? (in IPL)

- truth can only be established by *constructive proof*
- non-constructive proofs are a bit strange (philosophically): e.g. Tarski-Banach
- in particular, use of *tertium non datur* should be restricted

**But isn't  $A \vee \neg A$  intuitive?**

Okay for finite collections, but not for infinite ones.

## The BHK-interpretation

- A construction of  $A_1 \wedge A_2$  is a construction of  $A_1$  and a construction of  $A_2$
- A construction of  $A_1 \vee A_2$  is a number  $i \in \{1, 2\}$  together with a construction of  $A_i$
- A construction of  $A_1 \rightarrow A_2$  is a construction showing how to transform a construction of  $A_1$  into a construction of  $A_2$
- There is no construction of  $\perp$

$\neg A$  is shorthand for  $A \rightarrow \perp$

(that's stronger than "there's no construction for  $A$ "!)

All connectives are independent!

But what is actually a "construction"?

## **Why should a CompSci bother?**

- leads to modal logic
- Curry-Howard isomorphism (see my next talk)
- Proofs-as-Programs Paradigm / Proof Mining
- program verification



## Natural deduction

- due to Gerhard Gentzen (1909–1945)
- alternative to Hilbert style proof theory
- emphasis on inference (rules) rather than on truth (axioms)
- resembles “natural” reasoning
- but need to manage assumptions
- for each connective we have introduction and elimination rule
- sequent calculus is similar but quite different
- is there a coinciding algebraic semantics?

## Natural deduction – the rules

$$(\text{Ax}) \frac{}{\Gamma, A \vdash A}$$

$$(\wedge\text{I}) \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$$

$$(\wedge\text{E}) \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}$$

$$(\vee\text{I}) \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}$$

$$(\vee\text{E}) \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C \quad \Gamma \vdash A \vee B}{\Gamma \vdash C}$$

$$(\rightarrow\text{I}) \frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B}$$

$$(\rightarrow\text{E}) \frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}$$

$$(\perp\text{E}) \frac{\Gamma \vdash \perp}{\Gamma \vdash A}$$

## An algebraic semantics for Classical Propositional Logic (1/2)

A **Boolean Algebra** is a structure

$\mathcal{B} = (B, \cup, \cap, -, 0, 1)$  where:

- $\cup, \cap$  are associative, commutative and mutually distributive
- $\cup$  has identity (neutral element) 0:  $a \cup 0 = a$
- $\cap$  has identity (neutral element) 1:  $a \cap 1 = a$
- $-a \cup a = 1$
- $-a \cap a = 0$

Example: field of sets, algebra of truth values

## An algebraic semantics for Classical Propositional Logic (2/2)

Valuation  $v : PV \rightarrow B$

Define  $\llbracket - \rrbracket_v : \Phi \rightarrow B$  as:

$$\begin{aligned}\llbracket P \rrbracket_v &= v(P), & P \in PV \\ \llbracket \perp \rrbracket_v &= 0 \\ \llbracket A \vee B \rrbracket_v &= \llbracket A \rrbracket_v \cup \llbracket B \rrbracket_v \\ \llbracket A \wedge B \rrbracket_v &= \llbracket A \rrbracket_v \cap \llbracket B \rrbracket_v \\ \llbracket A \rightarrow B \rrbracket_v &= -\llbracket A \rrbracket_v \cup \llbracket B \rrbracket_v\end{aligned}$$

### The meaning of Truth

$A$  is a *tautology* iff

$\llbracket A \rrbracket_v = 1$  for all valuations  $v$

# **Arend Heyting**

## **1898–1980**



“What was specific to intuitionism, however, was the thesis that mathematics is an activity, a process of becoming, the exhaustive description of which is impossible, just as it is impossible to define once and for all its elementary concepts.”

## An algebraic semantics for IPL (1/3)

A **Heyting Algebra** is a structure

$\mathcal{H} = (H, \cup, \cap, \Rightarrow, -, 0, 1)$  where:

- $\cup, \cap$  are associative, commutative and mutually distributive
- $\cup$  has identity (neutral element) 0:  $a \cup 0 = a$
- $\cap$  has identity (neutral element) 1:  $a \cap 1 = a$
- $a \cup a = a$
- $-a = (a \Rightarrow 0)$
- $(a \cup c) \leq b$  iff  $c \leq (a \Rightarrow b)$ , where  
 $a \leq b \triangleq a \cup b = b$

In other words,  $\mathcal{H}$  is a distributive lattice with zero and relative pseudo-complement.

Examples:

$\mathcal{B}$  with  $a \Rightarrow b$  iff  $-a \cup b$

algebra of open sets of a topological space

## An algebraic semantics for IPL (2/3)

### Open sets of a topological space

Take any topological space, say  $\mathbb{R}^2$ .

**Def:**  $A \subseteq \mathbb{R}^2$  is *open* iff for every  $a \in A$  there is an  $r > 0$  such that  $\{b \in \mathbb{R}^2 \mid \delta(a, b) < r\} \subseteq A$

**Def:** If  $A \subseteq \mathbb{R}^2$  then  $Int(A)$  is the union of all open subsets of  $A$

The **algebra of open sets** of  $\mathbb{R}^2$ :

$$\mathcal{H}_O = (\mathcal{O}(\mathbb{R}^2), \cup, \cap, \Rightarrow, \sim, \emptyset, \mathbb{R}^2)$$

where

- $\mathcal{O}(\mathbb{R}^2)$  = family of all open subsets of  $\mathbb{R}^2$
- $A \Rightarrow B \triangleq Int(-A \cup B)$
- $\sim A \triangleq Int(-A)$

$\mathcal{H}_O$  is not a Boolean Algebra!

## An algebraic semantics for IPL (3/3)

Heyting Algebra  $\mathcal{H} = (H, \cup, \cap, \Rightarrow, -, 0, 1)$

Valuation  $v : PV \rightarrow H$

$$\llbracket P \rrbracket_v = v(p), \quad P \in PV$$

$$\llbracket \perp \rrbracket_v = 0$$

$$\llbracket A \vee B \rrbracket_v = \llbracket A \rrbracket_v \cup \llbracket B \rrbracket_v$$

$$\llbracket A \wedge B \rrbracket_v = \llbracket A \rrbracket_v \cap \llbracket B \rrbracket_v$$

$$\llbracket A \rightarrow B \rrbracket_v = \llbracket A \rrbracket_v \Rightarrow \llbracket B \rrbracket_v$$

**Def:**

- $\mathcal{H}, v \models A$  iff  $\llbracket A \rrbracket_v = 1$
- $\models A$  iff  $\mathcal{H}, v \models A$  for all  $\mathcal{H}, v$

**Soundness and completeness**

$$\Gamma \models A \text{ iff } \Gamma \vdash A$$

**Example:**

Pierce's law is not intuitionistically valid:

$$((P \rightarrow Q) \rightarrow P) \rightarrow P$$

Take  $v(P) = 1 - \{(x_0, y_0)\}$  and  $v(Q) = \emptyset$