Propositions and Types, Proofs and Programs

Part I: Intuitionistic Logic

Ranald Clouston
School of Computing
Australian National University

ANU Logic Summer School 2023

Introduction

My name is **Ranald Clouston**

- Lecturer at Australian National University
- Teaching introductory programming (with the functional language Haskell), and the lambda-calculus
- Researching logics, proofs, types, and categories
- A student at the Logic Summer School 20 years ago!
- Formally of Victoria University of Wellington, University of Cambridge, and Aarhus University

Photos c/o Viator, Wikipedia, Condair

Overview

These lectures are about a remarkable connection between logic and computing known variously as…

- Curry–Howard isomorphism, Curry–Howard correspondence, Propositions-as-types, Proofs-as-programs, etc…

We will develop a deep correspondences between

- Propositions and Types;
- Proofs and Programs;
- Proof Normalisation and Computation

Resources

These lectures do not exactly follow any one reference, but two have been particularly inspiring:

- Phillip Wadler, ‘Propositions as Types’
  - Relatively non-technical introduction

- Jean-Yves Girard, ‘Proofs and Types’
  - Translated and with appendices by Paul Taylor and Yves Lafont
  - Book length
  - Very readable but also fine to dip into for proof details

Brouwer’s Intuitionism

L. E. J. Brouwer (1881-1966) challenged the mainstream of the philosophy of mathematics by challenging the centrality of the notion of ‘truth’

- He did not believe that ‘anything goes’!
- But did point out that mathematicians have no direct access to truth;
- The stuff of mathematics is **definition** and **proof**, constructed in the mathematician’s mind (intuition) or on paper.

This idea is known as **intuitionism**, or (more generally) **constructivism**.

Photo c/o Wikipedia

Logical Connectives in Intuitionism

Brouwer's arguments may seem rather abstract, but in fact have major impact on how we understand logical connectives.

With (propositional) **classical logic**, connectives combine **truth values**

- Easily summarised by **truth tables**

With **intuitionistic logic**, the point is that we have no truth values!

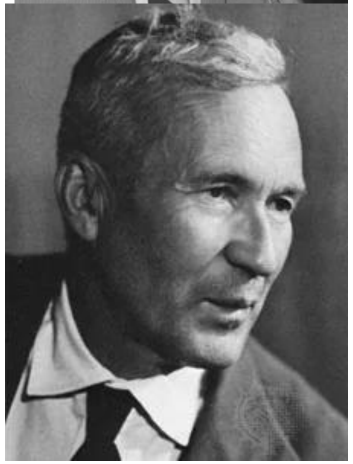
- Only **proofs**
- So logical connectives must be understood via combination of proofs

Brouwer-Heyting-Kolmogorov interpretation

The **BHK interpretation**, developed independently by Arend Heyting (1898-1980) and Andrey Kolmogorov (1903-87):

- A proof of A∧B is given by presenting a proof of A and a proof of B
- A proof of A∨B is given by presenting either a proof of A or a proof of B
- A proof of A→B is a construction which permits us to transform any proof of A into a proof of B
- ⊥ has no proof

We define ¬A as A→⊥, ⊤ as ¬⊥, ↔ as usual, and will look at quantifiers later.



Photos c/o Wikipedia, Britannica

Excluded Middle

Let p be the most famous unsolved problem in maths, the **Goldbach conjecture**:

- every even natural number greater than 2 is the sum of two prime numbers

A classical logician would affirm the 'law of excluded middle' (LEM):

$$p \vee \neg p$$

But consider the BHK interpretation:

- A proof of $p \vee \neg p$

Excluded Middle

Let p be the most famous unsolved problem in maths, the **Goldbach conjecture**:

- every even natural number greater than 2 is the sum of two prime numbers

A classical logician would affirm the ‘law of excluded middle’ (LEM):

$$p \vee \neg p$$

But consider the BHK interpretation:

- A proof of p, or a proof of ¬p

Excluded Middle

Let p be the most famous unsolved problem in maths, the **Goldbach conjecture**:

- every even natural number greater than 2 is the sum of two prime numbers

A classical logician would affirm the ‘law of excluded middle’ (LEM):

$$p \vee \neg p$$

But consider the BHK interpretation:

- A proof of p, or a construction which permits us to transform any proof of p into a proof of $\bot$

In Goldbach’s case, we obviously do not have either of these!

Excluded Middle, Excluded

So if we are to take Brouwer seriously, we must reject LEM, $A \vee \neg A$.

Many mathematicians were not keen on this!

“Taking the principle of excluded middle from the mathematician would be the same, say, as proscribing the telescope to the astronomer or to the boxer the use of his fists.” - David Hilbert (1862-1943)

The good news is that you do not have to choose sides in a century-old metamathematical flame war

- Merely recognize that the logic of **proof** is not the same as the logic of **truth**

The Value of Constructivism

Proof is an important human activity, worthy of study in its own right;

And **constructive** proofs are also often thought to be superior to non-constructive proofs, including by ‘mainstream’ mathematicians.

- They are clearly **valid**: all of intuitionistic logic is acceptable to the classical logician, but not vice versa;
- They tend to be more informative, because at no point do they rely on appeal to a ‘truth’ that cannot be directly demonstrated;
- In particular, requiring that everything be constructive allows algorithms to be extracted from proofs.
  - A link to computing already!
- Downside: constructive proofs are sometimes more complicated, harder to find, or do not exist at all.

Double Negation

Other than LEM, what is the intuitionist giving up?

Double negation: ¬¬A means

- a construction which permits us to transform any (construction which permits us to transform any proof of A into a proof of ⊥) into a proof of ⊥
- If we think of ¬A as ‘show there is no proof of A’, then ¬¬A is ‘show there is no proof that there is no proof of A’
- This is not the same as a proof of A!

Intuitionists accept double negation **introduction**, but not **elimination**:

- A→¬¬A always holds; ¬¬A→A does not

Proof By Contradiction

Mainstream mathematics makes a *lot* of use of double negation, disguised as proof by contradiction:

- To prove A, we assume ¬A. Some contradiction (⊥) follows, i.e. ¬A→⊥. This means ¬¬A. **Hence, by double negation elimination, A**.

This is not permitted to the intuitionist: to prove A, we must construct A directly, not merely show that ¬A leads to contradiction.

- Subtlety: the intuitionist *does* use something like proof by contradiction to prove a statement whose main connective is ¬: to prove ¬A we assume A and try to construct ⊥.

Interderivable Connectives

The connectives of classical logic can be defined in terms of each other in all sorts of ways, e.g.:

- $A \land B \quad \leftrightarrow \quad \neg(\neg A \lor \neg B) \quad \leftrightarrow \quad \neg(A \to \neg B)$
- $A \lor B \quad \leftrightarrow \quad \neg(\neg A \land \neg B) \quad \leftrightarrow \quad \neg A \to B$
- $A \to B \quad \leftrightarrow \quad \neg(A \land \neg B) \quad \leftrightarrow \quad \neg A \lor B$

These if-and-only-ifs *all* fail in intuitionistic logic

- Case by case, do both directions fail, or might one hold? A nice exercise.

Peirce’s Law

The slightly mysterious ((A→B)→A)→A is classically valid:

A	B	A→ B	(A → B) → A	((A→B)→A)→A
1	**1**	1	1	**1**
1	**0**	0	1	**1**
0	**1**	1	0	**1**
0	**0**	1	0	**1**

But not acceptable to intuitionists

- So classical vs intuitionistic is not just about negation and disjunction, but implication too!

Classical Logic, Hiding Inside

It seems obvious that intuitionistic logic is **weaker** than classical logic

- Its theorems are a strict subset of those of classical logic

But remarkably, classical logic can be seen to 'live inside' intuitionistic logic!

Glivenko's translation: A formula A is a theorem of classical logic iff ¬¬A is a theorem of intuitionistic logic

- So we can use intuitionistic logic to decide any classical logic question merely by adding double negation.
- Intuitionistic logic is not recoverable inside classical logic in this way.
- A slightly more sophisticated translation, also based on double negation, is needed if we add quantifiers.

Working with Intuitionistic Logic

Clearly we cannot keep working via the BHK interpretation alone.

We need better tools to determine which theorems are intuitionistically valid and which are not.

- Truth tables ✗
- Hilbert axiomatisation ✓
- Possible worlds semantics ✓
- Sequent calculus ✓
- Natural deduction ✓

This is not an exhaustive list, e.g. we could also talk about topological semantics and category theoretic semantics.

- One argument for intuitionistic logic is that it pops up in lots of different places!

Modus Ponens

The **Hilbert system** for classical propositional logic has only one rule of inference, modus ponens:

- If $A \to B$ is a theorem and A is a theorem, then B is a theorem

Is this intuitionistically acceptable?

- If we have a construction which permits us to transform any proof of A into a proof of B, and we have a proof of A, then we have a proof of B

Looks good!

- Indeed, looks suspiciously like feeding an input to a program…

This will, as with classical logic, be the only rule of inference we need.

Axioms for Implication

There is no one unique choice of Hilbert axioms, but we can make do with these two for implication:

- $A \to (B \to A)$
- $(A \to B) \to ((A \to (B \to C)) \to (A \to C))$
- Including all substitution instances, as usual.

A bunch of other useful theorems, like $A \to A$, follow from these.

Of course we cannot prove Peirce's law

- $((A \to B) \to A) \to A$

All Axioms

One presentation:

- $A \to (B \to A)$
- $(A \to B) \to ((A \to (B \to C)) \to (A \to C))$
- $A \to (B \to (A \land B))$
- $(A \land B) \to A$
- $(A \land B) \to B$
- $A \to (A \lor B)$
- $B \to (A \lor B)$
- $(A \to C) \to ((B \to C) \to ((A \lor B) \to C))$
- $\bot \to A$

Boosting to Classical Logic

Adding *any* of these axioms to the previous slide yields classical logic:

- $A \lor \neg A$
- $\neg\neg A \to A$
- $((A \to B) \to A) \to A$

Are there any propositions that are classically valid, not intuitionistically valid, and do *not* give us the full power of classical logic? Yes!

- e.g. $(A \to B) \lor (B \to A)$

In fact there are infinitely many different `intermediate logics' sitting between intuitionistic logic and classical logic.

Possible Worlds Semantics

The BHK interpretation gives a semantics (meaning) to intuitionistic logic, but is not (yet) completely formal

- What is a proof? A construction? A transformation?

The Curry-Howard isomorphism will sort this out, but before then it is good to know that a sound and complete semantics exists that can be stated in ordinary mathematics.

In fact, we will borrow Saul Kripke (1940-2022)'s notion of possible worlds semantics from modal logic, with slight modification.

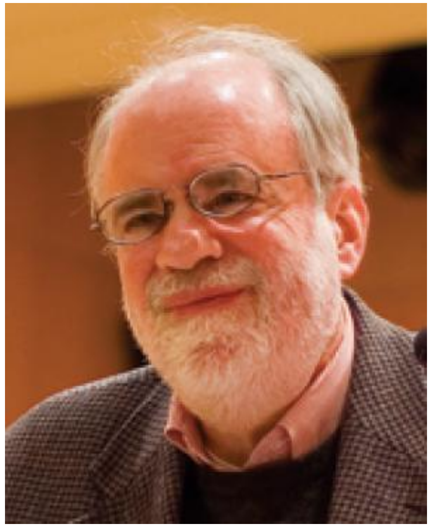


Photo c/o CUNY Graduate Centre

Intuitionistic Kripke Frames

An intuitionistic Kripke frame (from now, just ‘frame’) is a pair $\langle W, \leq \rangle$ where W is a set of worlds for which $\leq$ is a **preorder**:

- $\leq$ is **reflexive**: for all $w \in W$ we have $w \leq w$
- $\leq$ is **transitive**: if $w \leq x$ and $x \leq y$ then $w \leq y$
- It is harmless, but not necessary, to also ask that $\leq$ be antisymmetric, so that the frame is a poset.

Intuition: each world is a **state of knowledge**

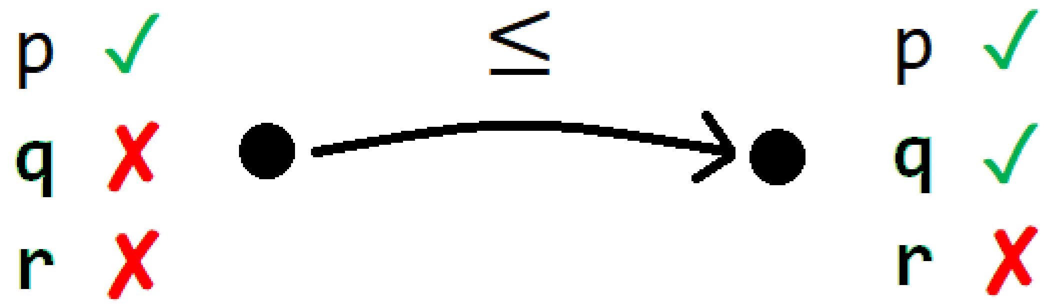
- As we prove new theorems, we move along the $\leq$ relation.

Intuitionistic Kripke Models

An intuitionistic Kripke model is a frame <W,≤> along with a **valuation** v from propositional variables to subsets of worlds that is

- **upwards-closed**: if $w \in v(p)$ and $w \leq x$ then $x \in v(p)$

Intuition: moving along the relation ≤ (proving a new theorem) can never falsify an existing proof, so if p is true at w then it is true at x.



Satisfaction

A world w in a model $\langle W,\leq,v\rangle$ satisfies a proposition A, written $\langle W,\leq,v,w\rangle \vDash A$, according to the following rules:

- $\langle W,\leq,v,w\rangle \vDash p$ if $w \in v(p)$
- $\langle W,\leq,v,w\rangle \vDash A \wedge B$ if $\langle W,\leq,v,w\rangle \vDash A$ and $\langle W,\leq,v,w\rangle \vDash B$
- $\langle W,\leq,v,w\rangle \vDash A \vee B$ if $\langle W,\leq,v,w\rangle \vDash A$ or $\langle W,\leq,v,w\rangle \vDash B$
- $\langle W,\leq,v,w\rangle \vDash A \to B$ if for all worlds x such that $w \leq x$, $\langle W,\leq,v,x\rangle \vDash A$ implies $\langle W,\leq,v,x\rangle \vDash B$
- $\langle W,\leq,v,w\rangle \vDash \bot$ never

$\langle W,\leq,v\rangle \vDash A$ if $\langle W,\leq,v,w\rangle \vDash A$ for all w;

$\langle W,\leq\rangle \vDash A$ if $\langle W,\leq,v\rangle \vDash A$ for all v;

A is **semantically valid** if $\langle W,\leq\rangle \vDash A$ for all $\langle W,\leq\rangle$.

Theorems

Truth preservation lemma: if $\langle W, \leq, v, w \rangle \vDash A$ and $w \leq x$ then $\langle W, \leq, v, x \rangle \vDash A$

- An important sanity check: ≤ does not destroy knowledge!

Soundness: if A is a theorem according to the Hilbert system, then A is semantically valid.

Completeness: if A is semantically valid, then A is a theorem according to the Hilbert system.

Understanding Negation

- $\langle W,\leq,v,w\rangle \vDash A \rightarrow B$ if for all worlds x such that $w \leq x$,
  $\langle W,\leq,v,x\rangle \vDash A$ implies $\langle W,\leq,v,x\rangle \vDash B$
- $\langle W,\leq,v,w\rangle \vDash \neg A$ if for all worlds x such that $w \leq x$,
  $\langle W,\leq,v,x\rangle \vDash A$ implies $\langle W,\leq,v,x\rangle \vDash \bot$
  iff for all worlds x such that $w \leq x$, $\langle W,\leq,v,x\rangle \nvDash A$

Hence

- $\langle W,\leq,v,w\rangle \vDash \neg\neg A$ iff for all worlds x such that $w \leq x$, there exists a world y such that $x \leq y$ and $\langle W,\leq,v,\mathbf{y}\rangle \vDash A$

So negation means ‘forever impossible’, while double negation means ‘forever possible’ – but does not necessarily mean `true right now’!

Frames for Intermediate and Classical Logics

As with modal logic we can restrict our set of frames to get different logics.

e.g. adding $(A \to B) \vee (B \to A)$ to the base axioms gives a logic sound and complete for the **linear** frames.

- For all worlds w and x, $w \leq x$ or $x \leq w$
- Known as Gödel–Dummett logic

If we restrict ourselves to the trivial frame with only one world, we get classical logic.

Structural Proof Theory

Proving things via a Hilbert system is a miserable experience.

- Exercise: prove $A \to A$ from $A \to (B \to A)$, and $(A \to B) \to ((A \to (B \to C)) \to (A \to C))$, and Modus Ponens

Working directly with semantics (BHK, possible worlds) is little better.

We want structural proof theory to help us lay out our proofs, and perhaps to help us find proofs, and to improve our proofs

- **Sequent calculus**
- **Natural deduction**
- Both invented by **Gerhard Gentzen** (1909-45)

Photo c/o Wikipedia

Sequent Calculus

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash B,\ A}\ \text{AX}}{\vdash A \to B,\ A}\ {\to}\text{R} \qquad \dfrac{}{A \vdash A}\ \text{AX}}{(A \to B) \to A \vdash A}\ {\to}\text{L}}{\vdash ((A \to B) \to A) \to A}\ {\to}\text{R}$$

This proof makes use of **multiple conclusions**.

If we allow **single conclusions** only, we get exactly intuitionistic logic!

Example Intuitionistic Sequent Calculus Proof

$$B, A \vdash B \qquad B, C, A \vdash C$$

$$B{\to}C, A \vdash A \qquad B, B{\to}C, A \vdash C$$

$$A{\to}B, A \vdash A \qquad A{\to}B, B{\to}C, A \vdash C$$

$$A{\to}B, A{\to}(B{\to}C), A \vdash C$$

$$A{\to}B, A{\to}(B{\to}C) \vdash A{\to}C$$

$$A{\to}B \vdash (A{\to}(B{\to}C)){\to}(A{\to}C)$$

$$\vdash (A{\to}B){\to}((A{\to}(B{\to}C)){\to}(A{\to}C))$$