Lecture 11: Intuitionistic Logic

Summary.
(1) Motivation: constructive logics and computation.

(2) Intuitionistic propositional logic: a proof system and a semantics.

Luís Soares Barbosa,
UNIV. MINHO *(Informatics Dep.)* & INL *(Quantum Software Engineering Group)*

Overview.

The principles of classical logic, based on a fundamental, Platonic notion of truth, are somehow inadequate to reason about computation. The reason is straightforward: classically, a statement holds independently of the way it was established, understood or, let us say, computed. Therefore, *false* stands for *not true*, as clearly expressed in the excluded middle principle[1], which states that $\phi \vee \neg\phi$ holds independently of what statement ϕ stands for.

The information content of $\phi \vee \neg\phi$ is, however, rather limited, in particular if one is unable to determine the value of ϕ through any reasonable means. Look at these two examples (from [3]):

- ϕ = *There are seven 7's in a row somewhere in the decimal representation of* π.
- ϕ = *There exist irrational numbers* x *and* y *such that* x^y *is rational.*

In the first case one is not able to determine its truth or falsity, thus being forced to accept that either the claim or its negation necessarily hold.

For the second, there is a simple proof: if $\sqrt{2}^{\sqrt{2}}$ is rational choose $x = y = \sqrt{2}$; otherwise, take $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. The proof, however, fails to show which of the two cases hold. For this reason it is qualified as *non constructive*.

This sort of reasoning fails to find (i.e. to compute) an actual solution to a problem — at best it says that some solution exists. A completely different argument proceeds constructively to provide an actual instance of x and y to prove the claim.

Intuitionistic logic, i.e the constructive approach to Logic, which goes back to the debates on the foundations of Mathematics in the first part of the 20^{th} century, is particularly relevant for Computer Science which deals with computational, constructive, essentially finite processes. The interested reader is referred to L. E. J. Brouwer and A. Heyting original texts [1, 2], or the excellent A.S. Troelstra and D. van Dalen monograph [4]. The survey [6] provides an historical overview, whereas connections to Computer Science are discussed in reference [5].

The basic principle of intuitionistic logic is that truth is not absolute: a statement holds only if there is an explicit, constructive proof of its correctness. This rules out reasoning principles as the excluded middle or the double negation. As J. Swift puts it in the wording of the famous

---

[1]The famous *tertium non datur*.

intelligent horses in the last part of Gulliver's *Travels into Several Remote Nations of the World* (1756, cited by [3]): *(...) reason taught us to affirm or deny only where we are certain; and beyond our knowledge we cannot do either*.

The logic.

The language of intuitionistic propositional logic is the same as the language of classical propositional logic. The validity of a statement is no longer based on any truth-value assigned to it, but on the mathematician's ability to provide an explicit (constructive) explanation (also said, a construction or a proof) for it. Propositional connectives are therefore specified by a constructive interpretation of their meaning when applied to constituent statements, rather by the usual truth tables used in classical logic. The BHK interpretation (after Brouwer, Heyting, and Kolmogorov) consists of the following set of (construction) rules:

- A construction of $\phi_1 \wedge \phi_2$ consists of a construction of ϕ_1 and a construction of ϕ_2.
- A construction of $\phi_1 \vee \phi_2$ consists of a construction of ϕ_1 or a construction of ϕ_2.
- A construction of $\phi_1 \Rightarrow \phi_2$ is a function mapping every construction of ϕ_1 into a construction of ϕ_2.
- There is no construction of $\bot$.

Note that negation $\neg$, $\Leftrightarrow$, and the constant $\top$ are, as usual, introduced by abbreviation:

- $\neg\phi \overset{\text{abv}}{=} \phi \Rightarrow \bot$
- $\phi \Leftrightarrow \psi \overset{\text{abv}}{=} (\phi \Rightarrow \psi) \wedge (\psi \Rightarrow \phi)$
- $\top \overset{\text{abv}}{=} \bot \Rightarrow \bot$

More important is the lack of any rule to form a construction of a propositional variable. Indeed, the meaning of a propositional variable becomes explicit only once the variable is replaced by a concrete statement.

Exercise 1

Give a BHK interpretation for the following formulas:

- $\bot \Rightarrow \phi$
- $\phi \Rightarrow \psi \Rightarrow \phi$
- $\phi \Rightarrow \neg\neg\phi$
- $\neg\neg(\phi \vee \neg\phi)$
- $(\phi \vee \neg\phi) \Rightarrow \neg\neg\phi \Rightarrow \phi$

Exercise 2

For the following formulas show that all of them are classical tautologies, but nevertheless fail to have a constructive interpretation:

- $((\phi \Rightarrow \psi) \Rightarrow \phi) \Rightarrow \phi$ (known as the Pierce's law)
- $\phi \vee \neg\phi$
- $\neg\neg\phi \Rightarrow \phi$
- $\neg(\phi \wedge \psi) \Leftrightarrow (\neg\phi \vee \neg\psi)$
- $((\phi \Leftrightarrow \psi) \Leftrightarrow \rho) \Leftrightarrow (\phi \Leftrightarrow (\psi \Leftrightarrow \rho))$

Note that the last example is the definition of classical implication in terms of negation and disjunction. In fact, from a constructive point of view none among $\wedge$, $\vee$, $\Rightarrow$ or $\neg$ connectives is definable from the others. Observe also that intuitionistic logic breaks the symmetry of classical logic, which is a consequence of negation not being an involution any more.

The BHK interpretation rules can be formalised in a *proof system*, presented in terms of natural deduction:

$$\frac{}{\Gamma, \phi \vdash \phi}\,(Ax) \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash \phi}\,(\bot out)$$

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \Rightarrow \psi}\,(\Rightarrow in) \qquad \frac{\Gamma \vdash \phi \Rightarrow \psi \quad \Gamma \vdash \phi}{\Gamma \vdash \psi}\,(\Rightarrow out)$$

$$\frac{\Gamma \vdash \phi \quad \Gamma \vdash \psi}{\Gamma \vdash \phi \wedge \psi}\,(\wedge in) \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi}\,(\wedge_1 out) \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi}\,(\wedge_2 out)$$

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi}\,(\vee in_1) \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi}\,(\vee in_2) \qquad \frac{\Gamma, \phi \vdash \rho \quad \Gamma, \psi \vdash \rho \quad \Gamma \vdash \phi \vee \psi}{\Gamma \vdash \rho}\,(\vee out)$$

Proof examples.

$$\frac{\dfrac{}{\phi \vdash \phi}\,(Ax)}{\vdash \phi \Rightarrow \phi}\,(\Rightarrow in) \qquad \frac{\dfrac{\dfrac{}{\phi, \psi \vdash \phi}\,(Ax)}{\phi \vdash \psi \Rightarrow \phi}\,(\Rightarrow in)}{\vdash \phi \Rightarrow \psi \Rightarrow \phi}\,(\Rightarrow in)$$

Exercise 3

Prove that

$$\phi \Rightarrow ((\psi \Rightarrow \rho),\ \phi \Rightarrow \psi,\ \phi\ \vdash\ (\phi \Rightarrow (\psi \Rightarrow \rho)) \Rightarrow (\phi \Rightarrow \psi) \Rightarrow (\phi \Rightarrow \rho)$$

Semantics.

The set $\mathbf{2}$ of Boolean values share a similar abstract structure with the powerset $\mathcal{P}X$ of a set X. Indeed the same structure is common to any non-empty family of subsets of X, closed under set-theoretic union, intersection and complement — which are typically known as a *field of sets*. The relevant structure is that of a Boolean algebra[2]:

A Boolean algebra $\mathcal{B} = (B, \sqcap, \sqcup, -, 1, 0)$ is a distributive lattice with top and bottom elements, such that every element has a complement. The underlying partial order is recoverd as $x \leq y$ iff $x \sqcap y = x$.

Classical propositional logic can be interpreted in any Boolean algebra, given a valuation v, i.e. a map relating propositional variables to elements of B. Thus,

$$\begin{aligned}
[\![p]\!]_v &= v(p) \quad \text{for any propositional variable } p \\
[\![\bot]\!]_v &= 0 \\
[\![\phi \wedge \psi]\!]_v &= [\![\phi]\!]_v \sqcap [\![\psi]\!]_v \\
[\![\phi \vee \psi]\!]_v &= [\![\phi]\!]_v \sqcup [\![\psi]\!]_v \\
[\![\phi \Rightarrow \psi]\!]_v &= -[\![\phi]\!]_v \sqcup [\![\psi]\!]_v
\end{aligned}$$

One writes $\mathcal{B}, v \models \phi$ when $[\![\phi]\!]v = 1$, and $\mathcal{B} \models \phi$ when $\mathcal{B}, v \models \phi$ for every valuation v. A folk result states that a propositional formula ϕ is a classical tautology if and only if $\mathcal{B} \models \phi$ for all Boolean algebras $\mathcal{B}$.

Can we play a similar game for intuitionistic logic?

First notice that, for every set Γ of formulas, implication provides a pre-order (i.e. a reflexive and transitive relation) over intuitionistic propositional formulas. To get anti-symmetry, one defines an equivalence relation

$$\phi \sim \psi \quad \text{iff} \quad \Gamma \vdash \phi \Rightarrow \psi \ \wedge\ \Gamma \vdash \psi \Rightarrow \phi$$

and takes its quotient $\mathcal{L} = \{[\phi]_\sim \mid \phi \text{ a formula}\}$. The order relation over $\mathcal{L}$ is defined by

$$[\phi]_\sim \leq [\psi]_\sim \quad \text{iff} \quad \Gamma \vdash \phi \Rightarrow \psi$$

[2] The fundamental result that every Boolean algebra is isomorphic to a field of sets is known as the Stone theorem, proved by M. H. Stone in 1934.

The pair $(\mathcal{L}, \leq)$ forms a distributive lattice by defining

$$0 \mathrel{\widehat{=}} [\bot]_\sim = \{\phi \mid \Gamma \vdash \neg\phi\} \qquad 1 \mathrel{\widehat{=}} [\top]_\sim = \{\phi \mid \Gamma \vdash \phi\}$$
$$[\phi]_\sim \sqcup [\psi]_\sim \mathrel{\widehat{=}} [\phi \vee \psi]_\sim \qquad [\phi]_\sim \sqcap [\psi]_\sim \mathrel{\widehat{=}} [\phi \wedge \psi]_\sim$$

The absence of the excluded middle principle precludes a proper definition of a complement. The best one can do is to define a *relative pseudo-complement*. Generically, in a lattice the relative pseudo-complement of x with respect to y, denoted by $x \to y$, is the greatest element in the lattice such that $x \sqcap (x \to y) \leq y$. In particular, $-a \mathrel{\widehat{=}} (a \to 0)$.

A distributive lattice, with top and bottom elements, such that the relative pseudo-complement exists for each pair of elements, is called an *Heyting* algebra. This is often presented as an algebraic structure $\mathcal{H} = (H, \sqcap, \sqcup, \to, -, 1, 0)$, where the underlying partial order is implicit and defined as before by $x \leq y = x \sqcap y = x$.

The algebraic semantics of intuitionistic propositional logic is defined as in the classical case, just replacing Boolean algebras by Heyting algebras, with

$$[\![\phi \Rightarrow \psi]\!]_v \;=\; [\![\phi]\!]_v \to [\![\psi]\!]_v$$

A formula ϕ is an intuitionistic tautology if $\models \phi$, i.e. it holds for every Heyting algebra $\mathcal{H}$ and valuation v, formally $\mathcal{H}, v \models \phi$. Similarly, given a set of formulas Γ, one writes

$$\Gamma \models \phi \quad \Longleftrightarrow \quad \mathcal{H}, v \models \Gamma \text{ implies } \mathcal{H}, v \models \phi \text{ for all } \mathcal{H} \text{ and } v$$

An important result states that the (syntactical) notion of a *theorem* and the (semantic) concept of a *tautology* coincide:

- $\Gamma \vdash \phi$ implies $\Gamma \models \phi$ — *soundness*
- $\Gamma \models \phi$ implies $\Gamma \vdash \phi$ — (semantic) *completeness*

The structure $(\mathcal{L}, \sqcap, \sqcup, \to, -, 1, 0)$, as defined above over the set of equivalence classes for $\sim$ forms a Heyting algebra[3] The most common example of an Heyting algebra (which is not a Boolean algebra) is provided by the family of open sets of a topological space. The complement of an open set in a topological space is usually not open. So, while union and intersection provides a way to interpret propositions as open sets, negation $\neg\phi$ cannot be taken as the complement of the interpretation of ϕ. It corresponds indeed to the *largest open set contained in the complement*, called its *interior* [4].

Formally, given a topological space $\mathcal{T}$, the structure $\mathcal{H} = (\mathcal{O}(\mathcal{T}), \cup, \cap, \to, -, \emptyset, \mathcal{T})$ is an Heyting algebra where $\cup, \cap$ are set union and intersection, $x \to y \mathrel{\widehat{=}} \mathcal{I}(-x \cup y)$, and $-x \mathrel{\widehat{=}} \mathcal{I}(-x)$, where the second symbol $-$ stands for set-theoretic complement.

[3] called the *Lindenbaum algebra* generated by a set of formulas Γ.

[4] In the real line, the interior $\mathcal{I}([0,1])$ of the interval $[0,1]$, is $\mathcal{I}([0,1]) =]0,1[$. Similarly, in the complex space, $\mathcal{I}(\{z \in C \mid |z| \leq 1\}) = \{z \in C \mid |z| < 1\}$.

Let us compute the interpretation of Peirce's law — $((\phi \Rightarrow \psi) \Rightarrow \phi) \Rightarrow \phi$ — over the algebra of open subsets of the real line. Consider $\nu(\phi) = \mathbb{R} - \{0\}$ and $\nu(\psi) = \emptyset$. Then,

$$[\![\phi \Rightarrow \psi]\!]_\nu = \mathcal{I}(\{0\} \cup \emptyset) = \emptyset \text{ and } [\![(\phi \Rightarrow \psi) \Rightarrow \phi]\!]_\nu = \mathcal{I}(\mathbb{R} \cup (\mathbb{R} - \{0\})) = \mathbb{R}$$

where we resorted tot he fact that in a Euclidean space the interior of a finite set is empty. Thus,

$$[\![((\phi \Rightarrow \psi) \Rightarrow \phi) \Rightarrow \phi]\!]_\nu \;=\; \mathcal{I}(\emptyset \cup (\mathbb{R} - \{0\})) \;=\; \mathbb{R} - \{0\}$$

which is different from $\mathbb{R}$. This means that the formula is not intuitionistically valid.

Exercise 4

Show that the principle of the excluded middle is not intuitionistically valid.

As a final observation, note that, unlike classical logic, intuitionistic logic is not finite-valued, i.e. there is no single finite Heyting algebra $\mathcal{H}$ such that $\vdash \phi$ is equivalent to $\mathcal{H} \models \phi$. A complete semantics can however be defined by an infinite Heyting algebra, for example the algebra of all open subsets of $\mathbb{R}$. This means that if a formula is not valid it is always possible to give a counterexample over the real line.

An alternative to an infinite Heyting algebra is to resort to the collection of all finite Heyting algebras. This is possible because intuitionistic logic has the *finite model property*, which may be stated as follows: A formula of length n is valid iff it is valid in all Heyting algebras of cardinality at most 2^{2^n}. Most importantly, this result implies that intuitionistic propositional logic is *decidable*. The rather unsatisfactory upper bound (double exponential space) can be improved down to polynomial space.

References

[1] L. E. J. Brouwer. *Collected Works: Philosophy and Foundations of Mathematics (volume 1)*. North-Holland, 1975.

[2] A. Heyting. *Intuitionism, An Introduction*. Studies in Logic and the Foundations of Mathematics. North-Holland, 1956.

[3] M. H. Sørensen and P. Urzyczyn. *Lectures on the Curry-Howard Isomorphism*. Studies in Logic and the Foundations of Mathematics (volume 149). North-Holland, 2006.

[4] A. Troelstra and D. van Dalen. *Constructivism in Mathematics. An Introduction*. Studies in Logic and the Foundations of Mathematics (volumes 121, 123). North-Holland, 1988.

[5] A. S. Troelstra. From constructivism to computer science. *Theoretical Computer Science*, 211(1):233 – 252, 1999.

[6] A. S. Troelstra. History of constructivism in the 20th century. In Juliette Kennedy and RomanEditors Kossak, editors, *Set Theory, Arithmetic, and Foundations of Mathematics: Theorems, Philosophies*, Lecture Notes in Logic, page 150?179. Cambridge University Press, 2011.