Intuitionism*

Jaap van Oosten

Spring 1995
Revised, april 1996

1 What is Intuitionism?

Intuitionism originates with the Dutch mathematician L.E.J. Brouwer (1881-1966)[1], who developed, in the years following 1905, a completely new philosophy of mathematics. I'll try to outline two basic points here, without attempting to go too deeply into the quite sophisticated philosophical discussion which ensued [the curious reader is referred to the books and papers of Troelstra, Beeson, Bishop & Bridges and Smorynski in the references].

In order to understand these points it is perhaps useful to recall some developments in late 19th century mathematics which to some extent rocked the average mathematician's working intuition. These were the creation of set theory by Cantor, and the development of mathematical logic by Frege and Russell. Both were very successful attempts to codify mathematics and mathematical thinking, and Russell went so far as to propose that mathematics was not more than a deductive system, completely subsumed by logic. This view was also taken by his pupil Wittgenstein who taught that mathematical truths are vacuous tautologies.

Brouwer opposed this view vehemently. Against it he raised two related philosophical issues [this is an extremely simplified picture]: *solipsism* and *the role of language.*

- *Solipsism* states, in a crude form, that man is basically alone and has no way of firmly establishing the existence of an outside world, let alone facts about such a world.

  Mathematics can therefore not be concerned with the discovery of absolute truths which are, in some way or another, hidden 'out there'. The

*Text for a minicourse given at BRICS, spring 1995

[1] Apart from being, as we'll see, a very original character, Brouwer was an extremely gifted mathematician. He solved important open problems in topology, and the mathematical field known as *algebraic topology* is essentially due to him. It is therefore that his philosophical arguments carried authority, and that the debate about them raged so violently

mathematician [in this discussion there is often talk about 'the mathematician'. What is meant is an idealized mathematician, a representative of mathematics as a whole, who makes no mistakes] has as his sole tools some basic *intuitions* on which he can perform *constructions*.

What would such basic intuitions be? A 'logicist' as Russell might perhaps take the notion of 'set', or operations from logic, as basic. Brouwer accepted only one basic notion: *time*, mathematically seen as *the real line*. For a set theorist the real numbers are Dedekind cuts or equivalence classes of fundamental sequences, but for the intuitionist the reals are there without needing any further qualification.

- *Language* is our means of communication, and in Brouwer's view a very defective one. In order to communicate his constructions to others, the mathematician has to devise a codification of the mathematical notions and a concise way of getting an argument across. Logic provides an instrument for this, but it is very risky to generalize, by mere linguistic analogy, laws of thought which are valid for finite structures to infinite ones: such "laws" can easily be formulated is a system which then can be proved to be free of contradiction, but nothing guarantees that they represent valid inferences about the mathematical world.

One logical principle, obviously valid for statements about finite structures, which came under Brouwer's attack, was the principle of excluded middle (*principium tertii exclusi*): for any statement φ, either φ or its negation $\neg\varphi$ is true, often encountered in the following form of reductio ad absurdum: if $\neg\varphi$ leads to a contradiction, then φ must be true (the *other* form: if φ leads to contradiction then $\neg\varphi$ is true, is perfectly acceptable to intuitionists; in fact this is the definition of $\neg\varphi$).

In trying to follow Brouwer's main argument against this principle, bear in mind that in the solipsistic mathematician's universe a statement φ can only be true if *I* have a mathematical *construction* establishing φ!

It is very well possible that today's theoretical computer scientists, raised as they are with problems of decidability, have less problems than the mathematicians of 80 years ago, in understanding the so-called "weak counterexamples" with which Brouwer had in mind to refute the principle of excluded middle.

Let us then take an, as yet, undecided mathematical proposition (Fermat's last, that there are non nontrivial integer solutions to $x^n + y^n = z^n$ for $n > 2$, was popular in books on intuitionism, but alas...[2]). There is of course an infinity of them. For example:

1. Goldbach's conjecture: every even natural number is the sum of two prime numbers;
2. There is no sequence of 99 consecutive 9's in the decimal expansion of π.

[2] As you know, this was recently proved by Wiles

Note that in both cases a counterexample is a finite piece of data, and can be checked in finite time.

Now it is possible to define a real number α by the following Cauchy sequence $\langle a_k \rangle_{k\in\omega}$:

$$a_k = \begin{cases} 2^{-k_0} & \text{if } k \geq k_0 \text{ and } k_0 \text{ is the first} \\ & \text{counterexample to Goldbach's conjecture;} \\ 2^{-k} & \text{else} \end{cases}$$

Everyone will agree that $\langle a_k \rangle_{k\in\omega}$ is a Cauchy sequence, and thus represents a real number α.

Now in Brouwer's view it makes no sense to say that either $\alpha = 0$ or $\alpha > 0$ since both statements imply a decision of Goldbach's conjecture. The number α is a so-called 'floating number'.

Another example: take the sequence $\langle b_k \rangle_{k\in\omega}$ given by

$$b_k = \begin{cases} (-2)^{-k_0} & \text{if } k \geq k_0 \text{ and } k_0 \text{ is least such that after expanding } \pi \text{ in } k_0 \\ & \text{decimals, a sequence of 99 consecutive 9's has been found;} \\ (-2)^{-k} & \text{else} \end{cases}$$

Again, $\langle b_k \rangle_{k\in\omega}$ represents a real number β; but now we cannot say $\beta \geq 0$ or $\beta \leq 0$ since either statement implies an unfounded opinion on the parity of the length of a possible least expansion sequence of π exhibiting 99 9's. On the other hand, given two real numbers which are well apart, such as 0 and 1, it is always true for any real number x, that $x > 0$ or $x < 1$; this follows by just approximating them closely enough.

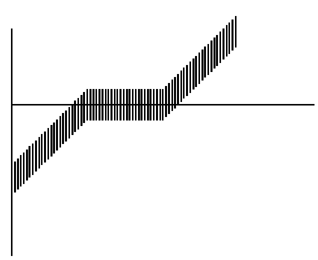
Once we take this kind of argument seriously, it has unexpected consequences. For example, the intermediate value theorem of analysis breaks down:

> INTERMEDIATE VALUE THEOREM
> For every continuous function f on $[0, a]$ with $f(0) < 0$ and $f(a) > 0$, there is $x \in [0, a]$ with $f(x) = 0$.

DISPROOF. Let, for β as defined above, f on [0,3] be defined by:

$$f(x) = \min\{x - 1, 0\} + \max\{0, x - 2\} + \beta$$

Roughly, f looks like this:



Now suppose f has a zero x. Then, as we have argued before, either $x < 2$ or $x > 1$ must hold; which implies respectively $\beta \geq 0$ or $\beta \leq 0$.

I mention two other, generally accepted, ideas in mathematics which are incompatible with the intuitionistic refusal of excluded middle as a valid law of thought: *cardinality of finite sets* and the *well orderedness of the natural numbers.*

- We call a set *finite* if it can be embedded into a set of the form $\{n \mid n < m\}$ for a natural number m (n also ranges over natural numbers). "Classically" (that is, in ordinary mathematics), every finite set can be assigned a unique natural number, its cardinality (number of elements). Not so intuitionistically: take the set $\{0, \alpha\}$. If it has a cardinality, then that must be 1 or 2. In the first case $\alpha = 0$, in the second case $\alpha > 0$; so in either case $\alpha = 0$ or $\alpha \geq 0$ holds.

- The well ordering principle for the natural numbers states that every nonempty subset of $\mathbb{N}$ has a least element. In fact, using excluded middle one can show that this is equivalent to the principle of mathematical induction over the natural numbers: if $X \subseteq \mathbb{N}$ is such that $0 \in X$ and for all $x \in \mathbb{N}$, $x \in X$ implies $x + 1 \in X$, then $X = \mathbb{N}$.

  Intuitionistically, neither principle implies the other. But whereas induction is a generally accepted principle, also among intuitionists, the well ordering principle implies the principle of excluded middle: let

  $$X = \{0 \mid \varphi\} \cup \{1\}$$

  where φ is some statement. Evidently, $1 \in X$ so X is nonempty; but if the least element of X is 0, then φ; if it's 1, then $\neg\varphi$. So in either case, $\varphi \vee \neg\varphi$.

2 Intuitionistic Logic

The codification in a logical system of those laws of thought which were valid in Brouwer's eyes, was carried out by his student A. Heyting and the Russian mathematician Kolmogorov. Given Brouwer's aversion to logic it is no more than natural that he thought this was a "sterile exercise".

Not, that at the time the discovery of the intuitionistically valid inferences was a trivial matter. For example, it was clear that for a proposition p, $\neg\neg p$ was not equivalent to p (because given this, one can derive the excluded middle); but what about $\neg\neg\neg p$, $\neg\neg\neg\neg p$ and so on? It seems to have been Heyting who discovered that this sequence ends, in fact that $\neg\neg\neg p$ is equivalent to $\neg p$.

Brouwer's proof of this goes wordly as follows (reflecting his horror of logical symbolism):

THEOREM. Absurdity of absurdity of absurdity is equivalent to absurdity.

PROOF. When property y follows from property x, then from the absurdity of y follows the absurdity of x. Therefore necessarily, since truth implies absurdity of absurdity, *absurdity of absurdity of absurdity implies absurdity.*

Conversely, because the correctness of an arbitrary property implies the absurdity of the absurdity of that property, so must absurdity of truth, that is *absurdity*, imply *absurdity of absurdity of absurdity.*

Poetic, isn't it?

One of the obstacles for a development of formal intuitionistic logic was the lack of a good understanding of how exactly Brouwer read the basic logical connectives. We have already seen that his interpretation of $\vee$ (or) is different from the usual one. Heyting formulated an interpretation of the symbols $\to$, $\wedge$, $\vee$, $\neg$ and $\bot$ (a special symbol, standing for "absurdity"), which later became known as the "Brouwer-Heyting-Kolmogorov interpretation". In this interpretation, one defines what it means to give an intuitionistic *proof* of a propositional formula φ (that is, a formula built up from these connectives and propositional variables) in terms of proofs of its constituents:

- A proof of $\varphi \wedge \psi$ is a pair consisting of a proof of φ and a proof of ψ;
- a proof of $\varphi \vee \psi$ is also a pair, the first component of which is a proof of φ or a proof of ψ, and the second component is information as to which is the case;
- a proof of $\varphi \to \psi$ is a construction which transforms any proof of φ into a proof of ψ;
- $\bot$ has no proof; and a proof of $\neg\varphi$ is a construction which transforms any proof of φ into a contradiction.

A derivation system, especially suited for intuitionistic logic, is *natural deduction*, invented by Gentzen in 1935.

In a *natural deduction tree*, we have the nodes labelled by formulas. The formal syntax is:

$$\text{Form} = \text{Var} \mid \bot \mid \text{Form} \oplus \text{Form} \mid \neg\text{Form}$$

where Var is a set of propositional variables $p, q, \ldots$ and $\oplus \in \{\wedge, \vee, \to\}$.

Formulas at the top nodes are numbered; they are called *assumptions*. The formula at the root is the *conclusion* of the tree. For example the tree

$$\frac{p^1 \quad q^2}{p \wedge q}$$

has two assumptions, p and q; and concludes $p \wedge q$. Assumptions can be *discharged*, for example in

$$\dfrac{\dfrac{p^1 \qquad\qquad q^2}{q}}{p \to q^1}$$

the assumption p has been discharged, which is made visible by its number at $p \to q$. The tree now has open (i.e. not discharged) assumption q, and concludes $p \to q$. Let's go one step further:

$$\dfrac{\dfrac{\dfrac{p^1 \qquad\qquad\qquad q^2}{q}}{p \to q^1}}{q \to (p \to q)^2}$$

concludes $q \to (p \to q)$ from no (open) assumptions at all.

A formula may occur more than once as assumption, and different occurrences may be discharged independently of each other:

$$\dfrac{\dfrac{q^1 \qquad\qquad\qquad q^2}{q \wedge q}}{q \to (q \wedge q)^1} \qquad \text{and} \qquad \dfrac{\dfrac{q^1 \qquad\qquad\qquad q^1}{q \wedge q}}{q \to (q \wedge q)^1}$$

are valid trees. The first derives $q \to (q \wedge q)$ from assumption q (numbered 2); the second one derives the same formula from no open assumptions. So different *occurrences* of the same formula may be numbered differently or alike; but we insist that different formulas be numbered differently. I now present a formal definition of natural deduction trees.

In the following list we denote by

$$\dfrac{\begin{array}{c}\{\varphi_i^{k_i} \mid 1 \leq i \leq n\} \\ \mathcal{D}\end{array}}{\psi}$$

a deduction tree with conclusion ψ and open assumptions φ_i $(i = 1, \ldots, n)$, where assumption φ_i is numbered k_i. The list is read in the following way: except for the first case, which is an axiom to start, each item is seen as a rule which permits the construction of the whole tree from its immediate subtrees. I also write $\vec{\varphi}$ for the assumption set, if the numbering plays no role in the rule.

We then have the following construction principles for deduction trees:

1. $$\dfrac{\{\varphi_i^{k_i} \mid 1 \leq i \leq n\}}{\varphi_j} \; (1 \leq j \leq n)$$
   is a valid tree (starting axiom);

2.

$$\dfrac{\dfrac{\begin{array}{c}\vec{\varphi}\\ \mathcal{D}\end{array}}{\psi} \qquad \dfrac{\begin{array}{c}\vec{\varphi}'\\ \mathcal{D}'\end{array}}{\psi'}}{\psi\wedge\psi'} \qquad\qquad \dfrac{\dfrac{\begin{array}{c}\vec{\chi}\\ \mathcal{D}\end{array}}{\varphi\wedge\psi}}{\varphi} \qquad\qquad \dfrac{\dfrac{\begin{array}{c}\vec{\chi}\\ \mathcal{D}\end{array}}{\varphi\wedge\psi}}{\psi}$$

3.

$$\dfrac{\dfrac{\begin{array}{c}\vec{\varphi}\\ \mathcal{D}\end{array}}{\psi\vee\chi} \qquad \dfrac{\begin{array}{c}\psi^k,\vec{\sigma}\\ \mathcal{D}_1\end{array}}{\alpha} \qquad \dfrac{\begin{array}{c}\chi^l,\vec{\tau}\\ \mathcal{D}_2\end{array}}{\alpha}}{\alpha^{k,l}}$$

In this rule, the assumptions ψ and χ are discharged.

$$\dfrac{\dfrac{\begin{array}{c}\vec{\chi}\\ \mathcal{D}\end{array}}{\varphi}}{\varphi\vee\psi} \qquad\qquad \dfrac{\dfrac{\begin{array}{c}\vec{\chi}\\ \mathcal{D}\end{array}}{\psi}}{\varphi\vee\psi}$$

4.

$$\dfrac{\dfrac{\begin{array}{c}\{\varphi_i^{k_i}\,|\,1\leq i\leq n\}\\ \mathcal{D}\end{array}}{\psi}}{\varphi_i\rightarrow\psi^{k_i}} \qquad\qquad \dfrac{\dfrac{\begin{array}{c}\vec{\omega}\\ \mathcal{D}\end{array}}{\varphi\rightarrow\psi} \qquad \dfrac{\begin{array}{c}\vec{\chi}\\ \mathcal{D}'\end{array}}{\varphi}}{\psi}$$

5.

$$\dfrac{\dfrac{\begin{array}{c}\varphi\\ \mathcal{D}\end{array}}{\bot}}{\psi} \qquad\qquad \dfrac{\dfrac{\begin{array}{c}\psi^i,\vec{\varphi}\\ \mathcal{D}\end{array}}{\bot}}{\neg\psi^i} \qquad\qquad \dfrac{\dfrac{\begin{array}{c}\vec{\varphi}\\ \mathcal{D}\end{array}}{\psi} \qquad \dfrac{\begin{array}{c}\vec{\varphi}'\\ \mathcal{D}'\end{array}}{\neg\psi}}{\bot}$$

Examples.

1. Let us show that, although intuitionism rejects $\varphi\vee\neg\varphi$, $\neg\neg(\varphi\vee\neg\varphi)$ is derivable (i.e. there is a natural deduction tree with no open assumptions, having it as its conclusion):

$$\dfrac{\dfrac{\neg(\varphi\vee\neg\varphi)^2 \qquad \dfrac{\dfrac{\dfrac{\neg(\varphi\vee\neg\varphi)^2 \qquad \dfrac{\varphi^1}{\varphi\vee\neg\varphi}}{\bot}}{\neg\varphi^1}}{\varphi\vee\neg\varphi}}{\bot}}{\neg\neg(\varphi\vee\neg\varphi)^2}$$

2. $\varphi\rightarrow\neg\neg\varphi$ is derivable:

$$\dfrac{\dfrac{\dfrac{\varphi^1 \qquad \neg\varphi^2}{\bot}}{\neg\neg\varphi^2}}{\varphi\rightarrow\neg\neg\varphi^1}$$

3. $\neg\neg\neg p \to \neg p$ (Compare with the part in Brouwer's verbal proof):

$$\dfrac{\dfrac{\dfrac{\neg\neg\neg p^3 \qquad \dfrac{\dfrac{p^1 \quad \neg p^2}{\bot}}{\neg\neg p^2}}{\bot}}{\neg p^1}}{\neg\neg\neg p \to \neg p^3}$$

Exercise 1. Construct natural deduction trees for the following formulas:

a) $(A \to B) \to (\neg B \to \neg A)$

b) $\neg\neg(A \to B) \to (\neg\neg A \to \neg\neg B)$

c) $(\neg A \vee B) \to (A \to B)$

We call two formulas φ and ψ *equivalent* if the formulas $\varphi \to \psi$ and $\psi \to \varphi$ are derivable.

Exercise 2. A formula φ is called *negative* if it contains no $\vee$ and all propositional variables p occur negated in φ. So, $\bot$ and $\neg p$ are negative, and the negative formulas are closed under application of $\wedge$, $\to$ and $\neg$.

Show that for negative φ, φ and $\neg\neg\varphi$ are equivalent.

Exercise 3.* Show that for negative φ, φ is derivable if and only if φ is classically true in the sense of truth-tables [for the meaning of this result, see section 4.1].

Exercise 4.* [The Rieger-Nishimura lattice] We consider formulas which only contain one propositional variable p, up to equivalence. We define, recursively, the following sequence $\langle A_n \rangle_{n\in\omega}$ of formulas in p:

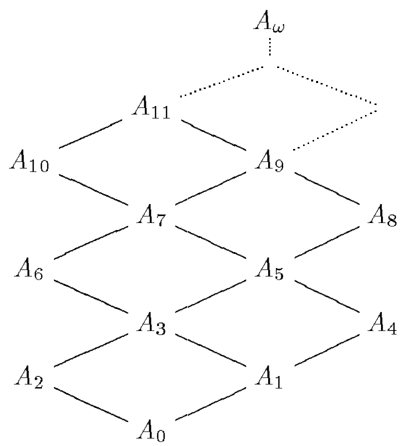
$$\begin{array}{ll} A_0 = p \wedge \neg p & \\ A_1 = p & A_{2n+1} = A_{2n-1} \vee A_{2n} \quad (n \geq 1) \\ A_2 = \neg p & A_{2n+2} = A_{2n} \to A_{2n-1} \quad (n \geq 1) \end{array}$$

Finally we set $A_\omega = p \to p$.

Show that every formula φ in the propositional variable p is equivalent to some A_n or to A_ω.

*Exercises so marked require some extra effort, or inventiveness

The implication ordering between the A_i's is as follows:



(This structure is called the "Rieger-Nishimura lattice" or the "free Heyting algebra on one generator") Show also that the implications between the A_i, the diagram suggests, are provable.

In fact, no other implications are provable. Quite in contrast to classical logic, where there are only 4 nonequivalent formulas in p, here there is an infinity of them.

Exercise 5.*["Formulas as Types"] The *typed λ-calculus* has the following types:

- Basic types $A_1, \ldots$; a type $\mathbf{0}$;
- Given types S, T, one has the types $S \times T$, $S + T$, $S \Rightarrow T$.

There are the following terms:

- For every type S there is a denumerably infinite set of variables of type S: $x_1^S, x_2^S, \ldots$;
- Given terms s of type S and t of type T, $\langle s, t\rangle$ is a term of type $S \times T$; given u of type $S \times T$, there is $p_0 u$ of type S and $p_1 u$ of type T;
- Given s of type S, there is $i_{S,T}(s)$ of type $S+T$ and $j_{S,T}(s)$ of type $T+S$; given u of type $S+T$, v of type $S \Rightarrow U$ and w of type $T \Rightarrow U$, there is $ex(u, v, w)$ of type U;
- Given u of type $S \Rightarrow T$ and s of type S, there is (us) of type T; given s of type S and a variable x of type T, there is $\lambda x.s$ of type $T \Rightarrow S$.

Now let N be the set of natural deduction trees which do not contain negations, and which are minimal, in the sense that there are no unused open assumptions. Let L be the set of terms of the typed λ-calculus modulo renaming of bound and free variables.

There is an obvious bijection between types and negation-free formulas; show that there is a bijection between L and N, such that a term t of type T is sent to a deduction of the formula corresponding to T.

Exercise 6. Find a deduction tree for

$$[A \to (B \vee (A \to C))] \to [A \to (B \vee C)]$$

and, if you've done the previous exercise, the λ-term corresponding to it.

3 Kripke models

To show that a formula is not provable, we often use models.

Definition 3.1 *A* Kripke model *is a finite tree K together with a function $[\![\cdot]\!]$ which assigns, to any propositional variable p, a subset $[\![p]\!]$ of K which is upwards closed, i.e. $x \in [\![p]\!]$ and $x \leq y$ imply $y \in [\![p]\!]$ (we take the order in this way, that the root is the least element).*

Given such $(K, [\![\cdot]\!])$ we define upwards closed subsets $[\![\varphi]\!]$ of K for any formula φ, by induction:

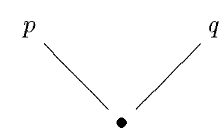
- $[\![\bot]\!] = \emptyset$;
- $[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\psi]\!]$;
- $[\![\varphi \vee \psi]\!] = [\![\varphi]\!] \cup [\![\psi]\!]$;
- $[\![\varphi \to \psi]\!] = \{x \in K \mid \forall y \geq x\, (y \in [\![\varphi]\!] \Rightarrow y \in [\![\psi]\!])\}$;
- $[\![\neg\varphi]\!] = \{x \in K \mid \forall y \geq x\; y \notin [\![\varphi]\!]\}$.

For $k \in K$ we say that k *satisfies* φ (written $k \models \varphi$) if $k \in [\![\varphi]\!]$. We say that $(K, [\![\cdot]\!])$ satisfies φ, or φ *is true in the model* $(K, [\![\cdot]\!])$, if the root of K satisfies φ. Let us note an evident fact: whether or not $x \models \varphi$ depends only on the set $\{y \in K \mid y \geq x\}$ and the sets $[\![p]\!]$ for those p which actually occur in φ.

The intuition behind Kripke models is as follows. We see a node of the tree as a "possible world"; the nodes branching out of that node, as possible future states. In the future, information can be gained, but cannot go lost; therefore, the sets $[\![\varphi]\!]$ are upwards closed.

We draw Kripke models like this, writing p at a node if that node is in $[\![p]\!]$:

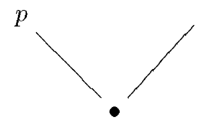
or



In the first model, $p \vee \neg p$ is not true; in the second model, $(p \to q) \vee (q \to p)$ fails.

Exercise 7. Prove this.

Exercise 8. Show that in:



$\neg p \vee \neg\neg p$ is not true.

Exercise 9. Construct models in which the following formulas are not true:

a) $((p \to q) \to p) \to p$ (Pierce's Law)

b) $(p \to (q \vee r)) \to ((p \to q) \vee (p \to r))$

We have the following important

SOUNDNESS THEOREM If φ is derivable, then φ is true in all Kripke models.

Exercise 10.* Prove this theorem [Hint: you have to devise the right induction hypothesis in order to carry induction over the height of deduction trees].

Conversely, there is the less trivial

COMPLETENESS THEOREM. If φ is true in all Kripke models, φ is derivable.

Bearing in mind that Kripke models are finite, we get:

COROLLARY. It is decidable whether φ is derivable or not.

Exercise 11. Give an intuitive proof of this corollary.

For the lovers of complexity results: R. Statman proved in 1979 that the above decision problem is PSPACE-complete.

The following exercises aim to give you an idea of different aspects of model theory: the first one shows preservation of a large class of formulas under a natural construction on trees (joining them together); the second one gives a proof theoretic result (disjunction property) by using models; the third introduces an important class of maps between models, which preserve the logic; and the fourth is of the kind which *characterizes* a type of models by the formulas which are true in them.

Exercise 12. The class $\mathcal{RH}$ of *Rasiowa-Harrop formulas* is defined as follows: $\bot \in \mathcal{RH}$, $p \in \mathcal{RH}$, $\varphi \to C \in \mathcal{RH}$ if $C \in \mathcal{RH}$, for any φ; and $\neg\varphi \in \mathcal{RH}$ for every φ.

Given a finite collection of Kripke models $(K_i, [\![\cdot]\!]_i)_{i \in I}$, we define a Kripke model $(\sum_{i \in I} K_i, [\![\cdot]\!])$, where $\sum_{i \in I} K_i$ is the union of all trees K_i with a new root k_0; $[\![\cdot]\!]$ is just $[\![\cdot]\!]_i$ when restricted to K_i, and we put $k_0 \in [\![p]\!]$ if and only if for all $i \in I$, p is true in $(K_i, [\![\cdot]\!]_i)$

Show the following: if C is a Rasiowa-Harrop formula, and for all i, C is true in $(K_i, [\![\cdot]\!]_i)$, then C is true in $(\sum_{i \in I} K_i, [\![\cdot]\!])$. Show also by a counterexample, that the condition that C is a Rasiowa-Harrop formula, can not be dropped.

Exercise 13. Show, using the preceding exercise and the completeness theorem, the *strong disjunction property* for intuitionistic propositional logic: if $C \to \varphi \vee \psi$ is derivable, with C Rasiowa-Harrop, then either $C \to \varphi$ or $C \to \psi$ is derivable. Conclude from this the ordinary disjunction property: if $\varphi \vee \psi$ is derivable, then φ or ψ is derivable.

Exercise 14. Let K and L be finite trees. A monotone function $f : L \to K$ is called an *open map* (or *p-morphism*) if for all $x \in L$ and $b \geq f(x)$ in K, there is $y \geq x$ in L with $f(y) = b$.

Now suppose that $(K, [\![\cdot]\!])$ is a Kripke model, L a tree and $f : L \to K$ an open map. We can define a Kripke model $(L, [\![\cdot]\!]_f)$ by putting

$$[\![p]\!]_f = f^{-1}([\![p]\!])$$

Show that for these two Kripke models, for all $x \in L$ and all formulas φ:

$$x \models \varphi \;\Leftrightarrow\; f(x) \models \varphi$$

Exercise 15. Show that the tree K is linear if and only if for all Kripke models $(K, [\![\cdot]\!])$ and for all formulas φ, ψ, the formula

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

is true in $(K, [\![\cdot]\!])$.

4 Further Perspectives

4.1 Constructive versus Nonconstructive Proofs

Is intuitionistic mathematics weaker than classical mathematics?

On the one hand: obviously. One has deleted an important logical principle. On the other hand, it is possible to embed classical logic into the so-called 'negative fragment' of intuitionistic logic; this is the meaning of exercise 3. So if you read all the connectives negatively (i.e. you interpret $\varphi \vee \psi$ as $\neg(\neg\varphi \wedge \neg\psi)$ throughout), everything which is provable classically is also provable intuitionistically.

Moreover, since the logic is weaker, there are more models and less equivalences. Usually, a classical notion 'splits' intuitionistically, in the sense that there are several notions, classically equivalent to the given one, but intuitionistically no one is equivalent to another. Proving anything about such a notion intuitionistically, usually gives you a stronger result than proving it classically. Let's see a simple example.

You know of course, that the cardinality of the powerset of a set A is strictly larger than that of A itself. Let's prove it:

THEOREM. There is no injective function $\mathcal{P}(A) \to A$, for any set A.

CLASSICAL PROOF. We identify $\mathcal{P}(A)$ with 2^A, the set of characteristic functions. Suppose $\Phi : 2^A \to A$ is injective. Let $f : A \to 2$ be defined as follows:

$$f(a) = \begin{cases} 0 & \text{if there is } g \in 2^A \text{ with } \Phi(g) = a \text{ and } g(a) = 1; \\ 1 & \text{else} \end{cases}$$

Let $\Phi(f) = N$ and consider $f(N)$. If $f(N) = 0$ then for some g, $\Phi(g) = N$ and $g(N) = 1$, so by injectivity of Φ, $g = f$ and $f(N) = 1$ contradiction; so $f(N) = 1$ whence by the very definition of f, $f(N) = 0$. Again contradiction.

Intuitionistically, there are two things wrong with this proof. First, the identification of $\mathcal{P}(A)$ with 2^A; and even assuming that that's OK, it is not clear that the function f defined in the proof, is a total function. But the general idea is perfectly all right, so:

INTUITIONISTIC PROOF. Again, suppose $\Phi : \mathcal{P}(A) \to A$ injective. We define the following subset of A:

$$\alpha = \{a \in A \mid \forall \beta \subseteq A(a \in \beta \Rightarrow a \neq \Phi(\beta))\}$$

Let $N = \Phi(\alpha)$. Instantiating α for β in the definition of α, one sees that N cannot be an element of α, but we're going to prove it anyway: if β satisfies $N \in \beta$ and $N = \Phi(\beta)$, then by injectivity of Φ, $\beta = \alpha$ so $N \in \alpha$, but that can't be! So, $N \in \alpha$.

What does this teach us? Well, intuitionistically we cannot repeat the trick with 2^A instead of $\mathcal{P}(A)$. Does that then mean that intuitionistically, we can have an injective function from 2^A into A? Yes, it does!

And this has important consequences for the semantics of programming languages; for example one can, in an intuitionistic universe, obtain models for an untyped language in which one has *all* functions from terms to Booleans, as terms.

4.2 Intuitionism and modern mathematics

The interest in intuitionism experienced a revival in the seventies, when it was discovered, by Lawvere and others, that structures which stood in the limelight of mathematical research, namely categories of sheaves (introduced to algebraic geometry by Grothendieck and Verdier) were, at the same time, models of intuitionistic logic.

This has two aspects: reasoning intuitionistically one could sometimes obtain results about these structures which would require a lot of calculations otherwise; on the other hand it provided intuitionism with a wealth of structures in which to test (in)equivalences, derivability questions, independence questions and so on.

The resulting field of "topos theory" unites intuitionism with category theory, and enjoys increasing interest from computer scientists. A good introductory text is the book by MacLane and Moerdijk in the references.

4.3 Intuitionism and computer science

Many programming languages are based on some form of type theory (like the typed λ-calculus). The intuition is that the types are sets, and the terms of an arrow type $S \Rightarrow T$ are functions between sets S and T. In many cases, this intuition can be given a precise meaning in models of intuitionistic set theory.

For example, if there is a type N of natural numbers, it is usually the case that the terms of type $N \Rightarrow N$ denote recursive functions. Yet we know that not all functions from $\mathbb{N}$ to $\mathbb{N}$ are recursive... Do we? In intuitionistic set theory, one often encounters the statement which is called "Church's Thesis", and which says that *all* functions from $\mathbb{N}$ to $\mathbb{N}$ are recursive. There are models of intuitionistic set theory, in which this statement is true. So the basic intuition can be vindicated.

Another example is "Brouwer's Theorem": *all* functions from $\mathbb{R}$ to $\mathbb{R}$ are continuous. The idea is, that in order to construct anything discontinuous, one has to make use of case distinctions like those we saw in section 1, and which are not valid intuitionistically. But we can say something more precise here. Suppose we have Church's thesis true. Set theoretically, the reals don't differ much from $\mathbb{N}^{\mathbb{N}}$. Now if the functions from $\mathbb{N}^{\mathbb{N}}$ to $\mathbb{N}^{\mathbb{N}}$ are also given recursively, then the Kreisel-Lacombe-Shoenfield theorem of recursion theory tells us that they must be continuous. Thus, also Brouwer's Theorem can be validated in models of intuitionistic set theory.

Acknowledgement. I'm grateful to Glynn Winskel and Vladi Sassone for reading through the manuscript, corrections, hints and discussions.

References

[1] M. Beeson, *Foundations of Constructive Mathematics*, Berlin (Springer) 1985

[2] E. Bishop & D. Bridges, *Constructive Analysis*, Berlin (Springer), 1985

[3] L.E.J. Brouwer, *Collected Works* (A. Heyting, ed.), Amsterdam (North Holland), 1975 (2 volumes)

[4] S. MacLane & I. Moerdijk, *Sheaves in Geometry and Logic*, Berlin (Springer), 1992

[5] C. Smorynski, *Logical Number Theory I, An Introduction*, Berlin (Springer), 1991

[6] R. Statman, *Intuitionistic propositional logic is polynomial space complete*, TCS **9** (1979), 67-72

[7] A.S. Troelstra, *Logic in the writings of Brouwer and Heyting*, in: Atti del Convegno Internazionale di Storia della Logica, San Gimignano, 1982, Bologna 1983

[8] A.S. Troelstra, *On the early history of intuitionistic logic*, ITLI Preprint ML-88-04, University of Amsterdam

[9] A.S.Troelstra, *History of constructivism in the twentieth century*, ITLI Preprint ML-91-05, University of Amsterdam

[10] A.S. Troelstra & D. van Dalen, *Constructivism in Mathematics*, Amsterdam (North Holland), 1988 (2 volumes)