Semantics of intuitionistic propositional logic

Erik Palmgren
Department of Mathematics, Uppsala University

Lecture Notes for Applied Logic, Fall 2009

1 Introduction

Intuitionistic logic is a weakening of classical logic by omitting, most prominently, the principle of excluded middle and the reductio ad absurdum rule. As a consequence, this logic has a wider range of semantical interpretations. The motivating semantics is the so called Brouwer-Heyting-Kolmogorov interpretation of logic. The propositions $A, B, C, \ldots$ are regarded as problems or tasks to be solved, and their proofs $a, b, c, \ldots$ as methods or (computer) programs that solves them.

- A proof-object, or just proof, for $A \wedge B$ is a pair $\langle a, b \rangle$ where a is a proof for A and b is proof for B.
- A proof for $A \to B$ is a function f which to each proof a of A gives a proof $f(a)$ of B.
- A proof for $A \vee B$ is either an expression $\mathsf{inl}(a)$ where a is a proof of A or an expression $\mathsf{inr}(b)$ where b is proof of B.
- There is no proof of $\bot$ (falsity).
- A proof of $\top$ (truth) is a symbol t.

We use lambda-notation for functions. For an expression $a(x)$ in the variable x, $\lambda x.a(x)$ denotes the function which to t assigns $a(t)$. We also use the equivalent notation $x \mapsto a(x)$, familiar from mathematics.

We use the *sequent notation* $A \vdash B$ for B *follows from* A. We identify proof-objects for $A \vdash B$ with proof-objects for $A \to B$. Then we may find proof-objects for the following rules of *intuitionistic propositional logic* (IPC) listed below. Each rule is valid in the sense that if we find proof-objects for the premisses above the line, then there is a proof-object for the conclusion below the line. For example the $(\to E)$ rule below is verified thus. Suppose f is a proof-object of $A \to B$ and a is a proof-object of A. Then $\mathsf{apply}(f,a)$ is a proof-object of B.

Rules for IPC

$$\frac{A \quad B}{A \wedge B}\ (\wedge I) \qquad \frac{A \wedge B}{A}\ (\wedge E1) \qquad \frac{B}{A \wedge B}\ (\wedge E2)$$

$$\frac{\begin{array}{c}\overline{A}^{h}\\ \vdots\\ B\end{array}}{A \to B}\ (\to I, h) \qquad \frac{A \to B \quad A}{B}\ (\to E)$$

$$\frac{A}{A \vee B}\ (\vee I1) \qquad \frac{A}{A \vee B}\ (\vee I2) \qquad \frac{A \vee B \quad \begin{array}{c}\overline{A}^{h_1}\\ \vdots\\ C\end{array} \quad \begin{array}{c}\overline{B}^{h_2}\\ \vdots\\ C\end{array}}{C}\ (\vee E, h_1, h_2)$$

$$\frac{\perp}{A}\ (\perp E)$$

Negation is defined by $\neg A = (A \to \perp)$. To obtain classical propositional logic CPC we add the rule of *reductio ad absurdum* (RAA)

$$\frac{\begin{array}{c}\overline{\neg A}^{h}\\ \vdots\\ \perp\end{array}}{A}\ (RAA, h)$$

Equivalently we may add, as an axiom, the *principle of excluded middle* (PEM)

$$\overline{A \vee \neg A}\ ^{(PEM)}.$$

Exercises

1.1. Prove $A \to \neg\neg A$ in IPC.

1.2. Prove $A \to B \to (\neg B \to \neg A)$ in IPC.

1.3. Prove that adding all instances $(\neg B \to \neg A) \to A \to B$ as axioms to IPC makes RAA provable.

1.4. Prove that over IPC the rule reductio ad absurdum and principle of excluded middle are equivalent.

2 Algebraization of logic

Classical propositional logic was first described in an algebraic manner by George Boole. A *boolean algebra* is a distributive lattice with a complementation operation (see Grätzer 2003). The basic example is the power set $\mathcal{P}(X)$ of subsets of a fixed set X, with intersection $\cap$, union $\cup$ as the lattice operations, $\emptyset$ and X being the bottom and the top element respectively. The complementation operation $\overline{\cdot}$ is the complement relative to X:

$$\overline{A} = \{x \in X : x \notin A\}.$$

Recall that each finite boolean algebra is isomorphic to some power set $\mathcal{P}(\{1,\ldots,n\})$ where $n \geq 0$. However, infinite boolean algebras need not be isomorphic to power sets as the following example shows.

Example 2.1 Consider the set C which consists of the subsets S of $\mathbb{N}$ that are either finite, or whose complement $\overline{S}$ is finite. Notice that $\emptyset$ and $\mathbb{N} = \overline{\emptyset}$ are members of C. It is straightforward to check that C is closed under intersection, union and complementation. It is thus a boolean algebra, since the equations that hold in the boolean algebra $\mathcal{P}(\mathbb{N})$ also holds in C.

It is rather clear that the elements of C can be coded as strings as following kind

$$0 \qquad -0 \qquad 011010011 \qquad -1011$$

meaning $\emptyset$, $\overline{\emptyset} = \mathbb{N}$, $\{1,2,4,7,8\}$ and $\overline{\{0,2,3\}} = \{1,4,5,6,\ldots\}$, respectively. Thus C is countably infinite. However for any infinite boolean algebra of the power set form $\mathcal{P}(M)$, we must have that M is infinite. Thus $\mathcal{P}(M)$ is uncountable and cannot be isomorphic to C for size reasons.

We have seen that one of the characteristics of intuitionistic logic is that not every proposition is true or false. For subsets this means that not every subset has a complement.

Example 2.2 Let $L_3 = \{\emptyset, \{1\}, \{1,2\}\} \subseteq \mathcal{P}(\{1,2\})$. This is a distributive lattice with the operations $\cap$ and $\cup$, the bottom element $\bot = \emptyset$, and top element $\top = \{1,2\}$. However, $A = \{1\}$ lacks complement, i.e. there is no $C \in L_3$ with

$$A \cap C = \bot \qquad A \cup C = \top.$$

Example 2.3 A subset of the euclidean line $A \subseteq \mathbb{R}$ is said to be *open*, if for every point $x \in A$, there is an interval $(a,b) \subseteq A$ such that $x \in (a,b)$. For instance intervals of the form $(a,b),(a,+\infty),(-\infty,b)$ are open sets. However the intervals $[a,b],[a,+\infty),(-\infty,b]$ are not. It can be checked (Exercise) that the set O of such open subsets is a distributive lattice with operations $\cap,\cup$ and bottom and top elements $\bot=\emptyset$, $\top=\mathbb{R}$. In fact, any union of open sets is an open set. It can be shown (Exercise) that there are only two elements in O, which have complements, namely $\bot$ and $\top$. Define for $A,B\in O$ the open set

$$(A\to B)=\bigcup\{U\in O : U\cap A\subseteq B\}.$$

Now (almost) by definition, for all $U\in O$

$$U\cap A\subseteq B \Longleftrightarrow U\subseteq (A\to B)$$

Define the *pseudo-complement* $\neg A$ of A to be $(A\to\bot)$. Thus

$$\neg A=\bigcup\{U\in O : U\cap A=\emptyset\}.$$

Clearly $A\cap\neg A=\bot$, but not necessarily $A\cup\neg A=\top$. For instance, we have $\neg(1,2)=(-\infty,1)\cup(2,\infty)$, so $(1,2)\cup\neg(1,2)$ is the real line except the numbers 1 and 2. The pseudo-complement $\neg A$ is the largest open set which does not intersect A.

$$\begin{array}{ccc} \neg A & A & \neg A \\ \text{- - -}\,\rule{7em}{0.4pt}) & (\rule{4em}{0.4pt}) & (\rule{7em}{0.4pt}\,\text{- - -} \end{array}$$

Definition 2.4 An abstract *topology* is a set X together with a set O of subsets of X (conventionally called the *open sets* of the topology) satisfying the conditions

(O1) $\emptyset\in O$, $X\in O$,

(O2) if $U,V\in O$, then $U\cap V\in O$,

(O3) for any index set I, if $U_i\in O$ for all $i\in I$, then $\cup_{i\in I}U_i\in O$.

(Note that (O3) actually implies $\emptyset\in O$ by taking $I=\emptyset$.)

The definitions of $U\to V$ and $\neg U$ apply to the open sets of any topological space.

Example 2.5 The euclidean plane $\mathbb{R}^2$ has the standard topology given by: $U\subseteq\mathbb{R}^2$ is an *open set* iff for every point $p=(x,y)\in U$ there is a rectangle

$$(a,b)\times(c,d)\subseteq U$$

which contains the point p. Then we can, for instance, show that the disc $\{(x,y)\in\mathbb{R}^2 : x^2+y^2<1\}$ is open (Exercise).

Example 2.6 Let $P = (P, \leq)$ be a partially ordered set. Declare a subset $U \subseteq P$ to be open, if $y \in U$ whenever $x \in U$ and $x \leq y$. These sets, *upper sets*, form the so-called *Alexandrov topology* on P. (Exercise: check O1-3.)

Example 2.7 Every set X can be equipped with the *discrete topology*. In this topology every subset A of X is considered open.

We shall here to some extent follow the presentation of Troelstra and van Dalen 1988.

Definition 2.8 A *Heyting algebra* is a partially ordered set $(H, \leq)$ with a smallest element $\bot$ and a largest element $\top$ and three operations $\wedge$ and $\vee$ and $\to$ satisfying the following conditions, for all $x, y, z \in H$

(i) $x \leq \top$

(ii) $x \wedge y \leq x$

(iii) $x \wedge y \leq y$

(iv) $z \leq x$ and $z \leq y$ implies $z \leq x \wedge y$

(v) $\bot \leq x$

(vi) $x \leq x \vee y$

(vii) $y \leq x \vee y$

(viii) $x \leq z$ and $y \leq z$ implies $x \vee y \leq z$

(ix) $z \leq (x \to y)$ iff $z \wedge x \leq y$.

Define $\neg x = (x \to \bot)$.

A *distributive lattice* $L = (L, \leq, \wedge, \vee, \top, \bot)$ is a partial order with operations that satisfies (i) – (viii) above and the two distributive law

$$x \wedge (y \vee z) = x \wedge y \vee x \wedge z \qquad\qquad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

The second law is actually a consequence of the first.

Lemma 2.9 *Every Heyting algebra is a distributive lattice.*

Proof. We have by (vi): $y \wedge x \leq y \wedge x \vee z \wedge x$ and hence by (ix): $y \leq x \to y \wedge x \vee z \wedge x$. Similarly $z \leq x \to y \wedge x \vee z \wedge x$. Hence by (viii): $y \vee z \leq x \to y \wedge x \vee z \wedge x$ and using (ix)

$$(y \vee z) \wedge x \leq y \wedge x \vee z \wedge x.$$

From $y \leq y \vee z$ and $y \wedge x \leq y$ and $y \wedge x \leq x$ follows $y \wedge x \leq (y \vee z) \wedge x$. Similarly $y \wedge x \leq (y \vee z) \wedge x$. Thus $y \wedge x \vee z \wedge x \leq (y \vee z) \wedge x$. $\Box$

We leave the proofs of the following results to the reader, and only give some hints.

Theorem 2.10 *Every Boolean algebra is a Heyting algebra.*

Proof. Define $(x \to y) = \neg x \vee y$. $\Box$

Theorem 2.11 *Every Heyting algebra, where $x \vee \neg x = \top$ for all x, is a Boolean algebra.*

Theorem 2.12 *Every finite distributive lattice is a Heyting algebra.*

Proof. Let H be a finite distributive lattice. Define

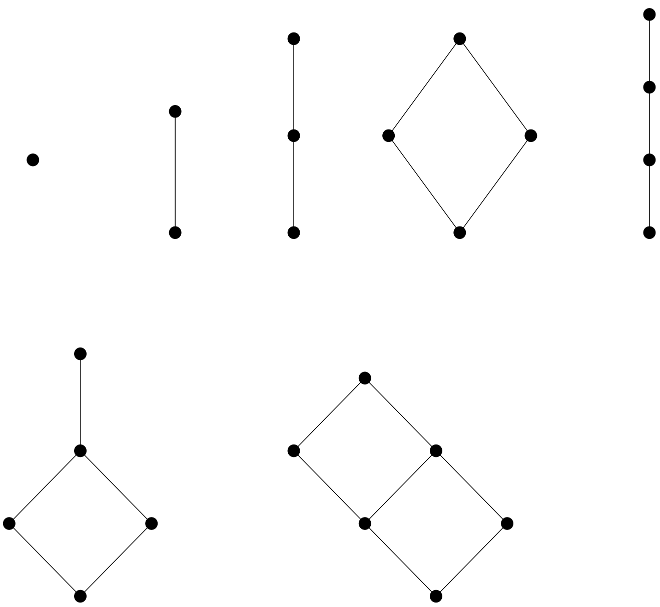
$$(x \to y) = \bigvee \{a \in H : a \wedge x \leq y\}, \tag{1}$$

and note that the join is finite. $\Box$

The formula (1) is very useful for computing implications in a finite lattice. Note the special case

$$\neg x = \bigvee \{a \in H : a \wedge x \leq \bot\}.$$

Example 2.13 Here are some examples of distributive lattices. The first, second and fourth lattices on the top row are boolean algebras, while the other lattices are not. (Exercise: in each such case find the elements which lack complements.)



Recall that the standard semantics of a formula of classical propositional logic is given by assigning the propositional variables a truth-value in $\mathbb{B}_2 = \{\bot, \top\}$ or $\{0,1\}$ or any other boolean algebra with two elements. Such an assignment $V : \mathbb{P} \to \{\bot, \top\}$ is called a *valuation*. (Here $\mathbb{P}$ is an infinite set of propositional variables, which we shall usually denote $P, Q, R, P', Q', R', \ldots$.) It is then extended to all formulas recursively

$$
\begin{array}{rcl}
V(\top) & = & \top \\
V(\bot) & = & \bot \\
V(A \wedge B) & = & V(A) \wedge V(B) \\
V(A \vee B) & = & V(A) \vee V(B) \\
V(A \to B) & = & V(A) \to V(B).
\end{array}
$$

The operations $\wedge, \vee, \to$ on the right hand side are given by the usual truth-tables for connectives. A formula A is *valid* if $V(A) = \top$, for all valuations $V : \mathbb{P} \to \mathbb{B}_2$. The completeness of propositional logic says that A is provable iff A is valid.

We may also replace $\mathbb{B}_2$ by an arbitrary boolean algebra B, and extend the notion of valuation to this algebra. We say that A is *B-valid* if $V(A) = \top$, for all valuations $V : \mathbb{P} \to B$.

By noting that the usual proof of soundness only depends on the abstract property we get

Theorem 2.14 *For any boolean algebra B, if A is provable in classical propositional logic, then A is B-valid.*

Thus we have the following version of the completeness theorem

Theorem 2.15 *The formula A is provable in classical propositional logic iff A is B-valid, for each boolean algebra B.*

Of course the usual version of the theorem states that we may restrict to checking validity for $B = \mathbb{B}_2$, the two-element boolean algebra.

Intuitionistic propositional logic (IPC) is given semantics in the same way, but the truth values belong to a Heyting algebra H instead of boolean algebra. An H-valuation is a function $V : \mathbb{P} \to H$, extended to all propositional formulas according the same recursive equations as above. A formula A is H-valid if $V(A) = \top$ for all H-valuations V. These notions are extended to sets of formulas in the obvious way. More generally, we say that A is an *H-consequence* of (a finite set of formulas) Γ if $V(\bigwedge \Gamma) \leq V(A)$. We denote this relation by $\Gamma \models_H A$

Lemma 2.16 (Soundness) *Let H be a Heyting algebra and let $V : \mathbb{P} \to H$ be a valuation. If $\Gamma \vdash A$ in IPC, then*

$$\Gamma \models_H A.$$

Proof. The lemma is proved by induction on the height of derivations in IPC. Thus we need to check that the rules of IPC preserve the order of H. Suppose the last rule in the derivation $\Gamma \vdash A$ was $(\wedge I)$. Then $A = B \wedge C$ and we have derivations $\Gamma_1 \vdash B$ and $\Gamma_2 \vdash C$ for subsets $\Gamma_1, \Gamma_2 \subseteq \Gamma$. By induction hypothesis we then have $V(\bigwedge \Gamma_1) \leq V(B)$ and $V(\bigwedge \Gamma_2) \leq V(C)$, whence $V(\bigwedge \Gamma) \leq V(\bigwedge \Gamma_1) \wedge V(\bigwedge \Gamma_2) \leq V(B) \wedge V(C) = V(B \wedge C)$ by the definition of valuation and meet in a Heyting algebra. Suppose the last rule applied in the derivation of $\Gamma \vdash A$ was $(\to I)$. Then $A = B \to C$ and $\Gamma \cup \{B\} \vdash C$ and so

$$V(\bigwedge \Gamma) \wedge V(B) = V(\bigwedge \Gamma \cup \{B\}) \leq V(C)$$

by the induction hypothesis. But then by the definition of $\to$ in H we have

$$V(\bigwedge \Gamma) \leq V(B) \to V(C) = V(B \to C),$$

where the equality holds by the definition of valuation. For one more example, suppose $\Gamma \vdash A$ is derived with last rule $(\vee E)$ so that there is a derivation $\Gamma \vdash B \vee C$ with $\Gamma \cup \{B\} \vdash A$ and $\Gamma \cup \{C\} \vdash A$. Then by induction hypothesis we have

$$V(\bigwedge \Gamma) \leq V(B \vee C) = V(B) \vee V(C),$$

and

$$V(\bigwedge \Gamma) \wedge V(B) \leq V(A), \quad V(\bigwedge \Gamma) \wedge V(C) \leq V(A).$$

That is,

$$\begin{array}{rcl} V(\bigwedge\Gamma) & \leq & V(\bigwedge\Gamma)\wedge(V(B)\vee V(C)) \\ & = & (V(\bigwedge\Gamma)\wedge V(B))\vee(V(\bigwedge\Gamma)\wedge V(C)) \\ & \leq & V(A). \end{array}$$

The other rules are immediately verified using the corresponding properties of a Heyting algebra. □

Interestingly, for intuitionistic logic it is not possible to restrict the truth-values to one fixed *finite* Heyting algebra to obtain the completeness. We have

Theorem 2.17 *The formula A is provable in IPC iff A is H-valid, for each Heyting algebra H.*

Proof. ($\Rightarrow$) If A is provable in IPC, this means there is a derivation of $\vdash A$. Hence $\top \leq V(A)$ for any H-valuation V, by Lemma 2.16. Thus A is H-valid.

($\Leftarrow$) (Outline of proof). Construct the following Heyting algebra. Let F be the set of IPC-formulas. Define an equivalence relation on F by

$$(A \sim B) \iff \vdash A \leftrightarrow B \text{ in IPC.}$$

Let $H = F/\sim$ be the set of equivalence classes $[A] = \{B \in F : A \sim B\}$ with respect to $\sim$. Partially order H by

$$[A] \leq [B] \iff \vdash A \to B \text{ in IPC.}$$

Set $\bot_H = [\bot]$ and $\top_H = [\top]$. Define operations by

$$[A] \wedge_H [B] = [A \wedge B] \qquad [A] \vee_H [B] = [A \vee B] \qquad [A] \to_H [B] = [A \to B].$$

Now one can check that $(H, \leq, \wedge_H, \vee_H, \to_H, \bot_H, \top_H)$ is a Heyting algebra. For example we verify the left to right direction of condition (ix) in the definition of Heyting algebra: Suppose $[A] \wedge [B] \leq [C]$, i.e. $[A \wedge B] \leq [C]$, i.e. $\vdash A \wedge B \to C$. Then we have a derivation

$$\dfrac{\begin{array}{c} \overline{A \wedge B}^{\,h} \\ \vdots \\ C \end{array}}{A \wedge B \to C}\ (\to I, h)$$

which we can change into a derivation

$$\dfrac{\dfrac{\dfrac{\dfrac{\overline{A}^{h_1} \quad \overline{B}^{h_2}}{A \wedge B}\ (\wedge I)}{\vdots}}{\dfrac{C}{B \to C}\ (\to I, h_2)}}{A \to (B \to C)}\ (\to I, h_1)$$

That is $\vdash A \to (B \to C)$, or $[A] \leq [B \to C] = [B] \to [C]$.

Now, we may define a valuation $V : P \to H$ by $V(Q) = [Q]$. Thus, by induction, for any formula

$$V(A) = [A].$$

If now $V(A) = \top_H$, we have that $\vdash A \leftrightarrow \top$ and thus $\vdash A$ in IPC. $\square$

A formula A is *intutionistically valid* if A is H-valid for each Heyting algebra H.

There is a sharpening of Theorem 2.17 which is useful for exhibiting counter-models.

Theorem 2.18 *The formula A is provable in IPC iff A is H-valid, for each finite Heyting algebra H.*

Proof. See Troelstra and van Dalen 1988. $\square$

Thus to prove that a particular A formula is unprovable in IPC, we may search for a finite Heyting algebra H and a valuation $V : \mathbb{P} \to H$ such that $V(A) \neq \top$. The pair H, V will then be a counter-model to A.

A crude decision method for intuitionistic validity of propositional formulas is thus to look in parallel for proofs, or finite counter-models, which may both be generated systematically. In fact, the decision problem for intuitionistic validity is much harder than for the classical case. We refer to (Troelstra and van Dalen 1988) and (Troelstra and Schwichtenberg 2000) for further reading.

Example 2.19 The formula $P \vee \neg P$ is not provable in IPC. Consider the lattice L_3 of Example 2.2. Assign $V(P) = \{1\}$. We have $V(\neg P) = \neg\{1\} = \emptyset$, so

$$V(P \vee \neg P) = \{1\} \cup \emptyset = \{1\} \neq \{1,2\} = \top.$$

Thus by the soundness part of the completeness theorem, the formula cannot be provable in IPC.

The same assignment shows also that

$$V(\neg\neg P \to P) = V(\neg\neg P) \to V(P) = \top \to V(P) = V(P) \neq \top$$

Thus $\neg\neg P \to P$ is not provable in IPC either. Note however that

$$V(\neg P \vee \neg\neg P) = \emptyset \cup \top = \top.$$

In fact, for any choice of L_3-valuation V, this holds. Hence $\neg P \vee \neg\neg P$ is L_3-valid.

Example 2.20 Let L_6 be the first lattice on the second row in Example 2.13. In this lattice there is an element a with $\neg a \vee \neg\neg a \neq \top$. This shows that $\neg P \vee \neg\neg P$ is not L_6-valid, and thus not provable in IPC.

Example 2.21 The two elements a and b just above $\perp$ in L_6 satisfies

$$\neg(a \wedge b) = \top \neq \neg a \vee \neg b.$$

Thus $\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)$ is unprovable in IPC.

Exercises

2.1. Do the exercise in Example 2.13.

2.2. For each lattice H in Example 2.13 find a finite set S and a subset $M \subseteq \mathcal{P}(S)$ such that the Hasse diagram of $(M, \subseteq)$ is the same as that of H. The third lattice in the first row corresponds to the set and subset given in Example 2.2.

2.3. Prove that in a Heyting algebra: if $a \wedge b = \perp$, $a \vee b = \top$, then $b = \neg a$. Thus every true complement is a pseudo-complement.

2.4*. Prove that the set of open sets, as defined in Example 2.3, form a distributive lattice. Prove that the union of any set of open sets is open. Conclude that O is Heyting algebra.

2.5. Show that the following formulas are unprovable in IPC. This may be done by finding a suitable Heyting algebra and a valuation which give a value $\neq \top$ to the formula. Another strategy is to try to show that the formula implies (in IPC) a formula which is already known to be unprovable.

(a) $\neg(P \to Q) \to P \wedge \neg Q$,

(b) $(\neg Q \to \neg P) \to (P \to Q)$,

(c) $(\neg\neg P \to \neg\neg Q) \to (P \to Q)$,

(d) $(P \to Q \vee R) \to (P \to Q) \vee (P \to R)$.

2.6* Complete the proofs of Lemma 2.16 and Theorem 2.17.

3 Kripke semantics

Kripke semantics or *possible worlds semantics* is another complete semantics for intuitionistic logic (van Dalen 1997; Troelstra and van Dalen 1988). It can be obtained as a special case of the Heyting-valued semantics as follows.

First we show how a partial order generates a Heyting algebra. Let $S = (S, \leq)$ be a partially ordered set. For $a \in S$ define

$$a\uparrow = \{b \in S : a \leq b\},$$

i.e. the set of elements above a. We say that a subset U of S is *upper closed* if $a\uparrow \subseteq U$ for any $a \in U$. For any partially ordered set S the set $\mathsf{UC}(S)$ of upper closed subsets of S ordered by inclusion form a Heyting algebra. Here $\cap$ and $\cup$ are meet and join operations respectively. For $A, B \in \mathsf{UC}(S)$ define the upper closed set

$$A \to B = \{x \in S : (x\uparrow) \cap A \subseteq B\}.$$

Then $\to$ satisfies 2.8.(viii): For $A, B, C \in \mathsf{UC}(S)$,

$$\begin{aligned} C \subseteq (A \to B) &\Leftrightarrow (\forall x \in C)(x\uparrow) \cap A \subseteq B \\ &\Leftrightarrow (\forall x \in C)(\forall y \in A)(x \leq y \Rightarrow y \in B) \\ &\Leftrightarrow (\forall x \in C \cap A)(x \in B) \\ &\Leftrightarrow C \cap A \subseteq B \end{aligned}$$

The third equivalence follows since A is upper closed.

Now several of the lattices encountered can be reconstructed as $(\mathsf{UC}(S), \subseteq)$ for some suitable chosen partial order S.

Example 3.1 1. The rightmost lattice in the top row of Example 2.13 is isomorphic to

$$\mathsf{UC}(\{1,2,3\}, \leq) = \{\emptyset, \{3\}, \{2,3\}, \{1,2,3\}\}.$$

Here $\leq$ is the usual order of natural numbers.

2. The leftmost lattice in the bottom row is isomorphic to

$$\mathsf{UC}(\{0,a,b\}, \leq) = \{\emptyset, \{a\}, \{b\}, \{a,b\}, \{0,a,b\}\}.$$

Here $0 \leq a$ and $0 \leq b$ and no other relations hold except reflexivity.

Next, for a first order formula A and a valuation $V : \mathbb{P} \to \mathsf{UC}(S)$ define the *forcing relation*

$$p \Vdash A \Longleftrightarrow_{\text{def}} p \in V(A).$$

Thus A is valid under the valuation V iff $p \Vdash A$ for all $p \in S$. Since $V(A)$ is upper closed we have the so-called *monotonicity property*

$$p \Vdash A \text{ and } p \leq q \Longrightarrow q \Vdash A.$$

Note that if S has a smallest element p_0 then validity under V is equivalent to $p_0 \Vdash A$, due to this property.

Remark 3.2 An intuitive reading of the above is to think of S as the set of possible worlds and the relation $p \Vdash A$ as *A is true in world p*. The judgement $p \leq q$ indicates that q is accessible from p. A further suggestive reading is to think of worlds as *states of knowledge*, and then $p \leq q$ indicates that q is a state of greater knowledge than p. This is in accordance with the monotonicty property.

Remark 3.3 The relation $\Vdash$ is most often written $\Vdash$, but we use this notation to distinguish from the notation for the Kripke models for *modal logics* in Huth and Ryan (2004). Their notion of model is more general since the "accessibility relation" between worlds may be an arbitrary relation.

The logical connectives are then interpreted as follows.

Theorem 3.4 *The forcing relation $(\Vdash) = (\Vdash_V)$ for a given valuation V satisfies the conditions:*

(i) $p \Vdash P$ *iff* $p \in V(P)$ *for propositional variables P.*

(ii) $p \Vdash \perp$ *never holds.*

(iii) $p \Vdash A \wedge B$ *iff* $p \Vdash A$ *and* $p \Vdash B$

(iv) $p \Vdash A \vee B$ *iff* $p \Vdash A$ *or* $p \Vdash B$

(v) $p \Vdash A \to B$ *iff* $(\forall q \geq p)(q \Vdash A \to q \Vdash B)$.

Proof. (i) is immediate by the definition. For (ii) note that $p \Vdash \perp$ is equivalent to $p \in V(\perp) = \emptyset$. (iii) and (iv) follows since $V(A \wedge B) = V(A) \cap V(B)$ and $V(A \vee B) = V(A) \cup V(B)$. To prove (v): We have $p \Vdash A \to B$ iff

$$p\!\uparrow \cap V(A) \subseteq V(B)$$

iff

$$(\forall q \geq p)(q \in V(A) \to q \in V(B)).$$

Then (v) follows by definition of the forcing relation. □

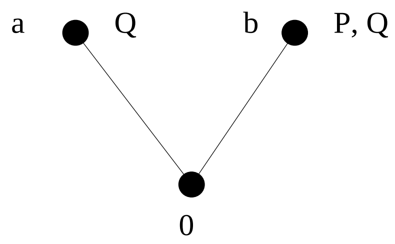
The following are especially noteworthy consequences which explains why negation does not have the classical meaning in Kripke models.

Corollary 3.5 *(i) $p \Vdash \neg A$ iff for all $q \geq p$, $q \Vdash A$ is false.*

(ii) $p \Vdash \neg\neg A$ iff for each $q \geq p$ there exists $r \geq q$ so that $r \Vdash A$.

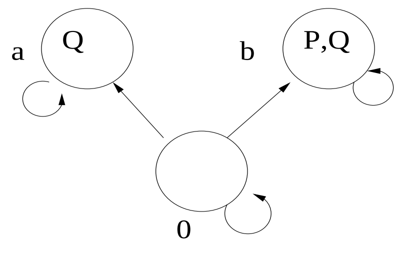
Remark 3.6 The common approach to Kripke models is to take the conditions (i)–(v) as a definition of $p \Vdash A$ by recursion on the formula A. Note that $V(P)$ determines in which "worlds" the propositional variable P is true. Under the reading as states-of-knowledge $V(P)$ tells at which states of knowledge P is known to be true.

Example 3.7 A Kripke model may be specified by drawing a Hasse diagram decorated with the propositional letters which are true at different nodes. Below is the Kripke model with partial order $S = \{0, a, b\}$ as in Example 3.1.2, and where $V(P) = \{b\}$ and $V(Q) = \{a, b\}$.



A formula A is thus valid in this model iff $0 \Vdash A$. We note the following: $0 \nVdash Q$, $0 \nVdash \neg Q$, $0 \Vdash \neg\neg Q$. Thus $0 \Vdash \neg Q \vee \neg\neg Q$ but $0 \nVdash Q \vee \neg Q$. We have $0 \nVdash \neg P$ and $0 \nVdash \neg\neg P$, so $0 \nVdash \neg P \vee \neg\neg P$.

In the style of Huth and Ryan (2004) the above model is graphically presented as follows.



Remark 3.8 The Kripke models presented here and those of Huth and Ryan (2004) may be related as follows. Define the labelling function as $L(x) = \{P \in \mathbb{P} : x \in V(P)\}$. Define a translation of IPC formulas into modal formulas by recursion:

$A^* = A$ for A propositional variable, $A = \perp$ or $A = \top$,

$(A \wedge B)^* = A^* \wedge B^*$,

$$(A \vee B)^* = A^* \vee B^*,$$

$$(A \to B)^* = \Box(A^* \to B^*).$$

As examples of translation, note that

$$(\neg P \vee P)^* = \Box(\neg P) \vee P \qquad\qquad (\neg P \to Q)^* = \Box(\Box(\neg P) \to Q).$$

The following is easily proved by induction on formulas A of IPC.

Theorem 3.9 *$x \Vdash A$ if, and only if, $x \Vdash A^*$*

Exercises

3.1* Let S be a partially ordered set. Show that $\mathsf{UC}(S)$ is a boolean algebra iff the partial order satisfies $p = q$ whenever $p \leq q$.

3.2* Does each finite distributive lattice have the form $\mathsf{UC}(S)$ for some partial order S?

4 Complete Heyting algebras

Existential and universal quantification over a set may be regarded as a (possibly) infinitary generalisation of the disjunction and conjunction operations. This is easy to describe algebraically.

A Heyting algebra H is *complete* (cHA) if each of its subsets has a supremum, that is if for any $A \subseteq H$ there is $\bigvee A \in H$ such that for all $b \in H$:

$$\bigvee A \leq b \iff (\forall a \in A)\, a \leq b.$$

(For $A = \{a_i : i \in I\}$ we write $\bigvee_{i \in I} a_i = \bigvee A$.)

Note that the supremum of $\emptyset$ in a Heyting algebra is $\bot$, and for $A = \{a_1, \ldots, a_n\}$, $\bigvee A = \bigvee_{i=1}^{n} a_i = a_1 \vee \cdots \vee a_n$. Thus each finite distributive lattice is a cHA.

Theorem 4.1 *The open sets of a topology (X, O) form a complete Heyting algebra, where inclusion is the order and*

$$\bigvee_{i \in I} U_i = \bigcup_{i \in I} U_i \qquad U \wedge V = U \cap V \qquad (U \to V) = \bigcup \{W \in O : W \cap U \subseteq V\}. \Box$$

Proposition 4.2 *In a cHA the infimum of a set A is given by*

$$\bigwedge A = \bigvee \{x \in H : (\forall a \in A) x \leq a\}.$$

Proof. Exercise. □

For complete Heyting algebras there is an infinitary generalisation of the distributive law

Proposition 4.3 *For a subset A of an cHA and any element b*

$$b \wedge (\bigvee A) = \bigvee \{b \wedge a : a \in A\}. \tag{2}$$

Proof. ($\geq$) follows since $b \wedge (\bigvee A) \geq b \wedge a$ for any $a \in A$.

($\leq$): To show the inequality

$$b \wedge (\bigvee A) \leq \bigvee \{b \wedge a : a \in A\},$$

note that it is equivalent to

$$(\bigvee A) \leq (b \to \bigvee \{b \wedge a : a \in A\}),$$

by the $\to$-axiom. This is in turn equivalent to

$$(\forall a \in A)\, a \leq (b \to \bigvee \{b \wedge a : a \in A\}),$$

which by the $\to$-axiom is equivalent to

$$(\forall a \in A)\, (a \wedge b \leq \bigvee \{b \wedge a : a \in A\}).$$

This is however obviously true, so we are done. □.

There is also a converse: any complete lattice L satisfying the infinite distributive law (2) becomes a cHA by letting

$$(a \to b) = \bigvee \{x \in X : x \wedge a \leq b\}.$$

This law is used to show that $c \leq a \to b$ implies $c \wedge a \leq b$ (Exercise).

Exercises

4.1. Prove Proposition 4.2. (It is easier if one notes that the result holds for any partial order which is complete in the sense that each of its subsets has supremum.)

4.2. Prove Theorem 4.1.

References

M.R.A. Huth and M.D. Ryan (2004). *Logic in Computer Science: Modelling and reasoning about systems. Second edition.* Cambridge University Press.

A.S Troelstra and H. Schwichtenberg (1996). *Basic Proof Theory,* Cambridge University Press.

A.S. Troelstra and D. van Dalen (1988). *Constructivism in Mathematics, Vol. I & II.* North-Holland.

G. Grätzer (2003). *General Lattice Theory.* Birkhäuser.

D. van Dalen (1997). *Logic and Structure.* Third edition. Springer.