Chapter 2

Intuitionistic logic

The word "logic" is used with a variety of meanings, from common sense reasoning to sophisticated formal systems. In most cases, logic is used to classify statements as "true" or "false". That is, what we mean by logic is usually one of the many possible variants of two-valued *classical logic*.

Indeed, classical logic can by all means be seen as a standard wherever there is a need for precise reasoning, especially in mathematics and computer science. The principles of classical logic are extremely useful as a tool to describe and classify the reasoning patterns occurring both in everyday life and in mathematics.

It is however important to understand the following. First of all, no system of rules can capture all of the rich and complex world of human thoughts, and thus every logic can merely be used as a limited-purpose tool rather than as an ultimate oracle, responding to all possible questions.

In addition, the principles of classical logic, although easily acceptable by our intuition, are not the only possible reasoning principles. It can be argued that from certain points of view (likely to be shared by the reader with a computing background) it is actually better to use other principles. Let us have a closer look at this.

Classical logic is based on the fundamental notion of *truth*. The truth of a statement is an "absolute" property of this statement, in that it is independent of any reasoning, understanding, or action. A well-formed and unambiguous declarative statement is either true or false, whether or not we (or anybody else) know it, prove it, or verify it in any possible way. Here "false" means the same as "not true", and this is expressed by the *excluded middle* principle (also known as *tertium non datur*) stating that $p \vee \neg p$ holds no matter what the meaning of p is.

Needless to say, the information contained in the claim $p \vee \neg p$ is quite limited. Take the following sentence as an example:

There are seven 7's in a row somewhere in the decimal
representation of the number π.

It may very well happen that nobody will ever be able to determine the truth or falsity of the sentence above. Yet we are forced to accept that either the claim or its negation must necessarily hold. Another well-known example is:

There exist irrational numbers x and y, such that x^y is rational.

The proof of this fact is very simple: if $\sqrt{2}^{\sqrt{2}}$ is a rational number then we can take $x = y = \sqrt{2}$; otherwise take $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$.

The problem with this proof is that we do not know which of the two possibilities is the right one. But here is a different argument: For $x = \sqrt{2}$ and $y = 2\log_2 3$, we have $x^y = 3 \in \mathbb{Q}$. We say the latter proof is *constructive* while the former is not.

Such examples demonstrate some of the drawbacks of classical logic. Indeed, in many applications we want to find an actual solution to a problem, and not merely to know that some solution exists. We thus want to sort out the proof methods that provide the actual solutions from those that do not. Therefore, from a very pragmatic point of view, it makes sense to consider a constructive approach to logic.

The logic that meets our expectations and accepts only "constructive" reasoning is traditionally known under the (slightly confusing) name of *intuitionistic logic*. To explain this name, one has to recall the philosophical foundations of intuitionistic logic. These may be expressed concisely and very simplified by the following principle: There is no absolute truth, there is only the knowledge and intuitive construction of the idealized mathematician, the *creative subject*. A logical judgement is only considered "true" if the creative subject can verify its correctness. Accepting this point of view inevitably leads to the rejection of the excluded middle as a uniform principle. As we learned from the noble Houyhnhnms [464]:

(...) reason taught us to affirm or deny only where we are certain;
and beyond our knowledge we cannot do either.

2.1. The BHK interpretation

The language of *intuitionistic propositional logic*, also called *intuitionistic propositional calculus* (abbreviated IPC), is the same as the language of classical propositional logic.

2.1.1. DEFINITION. We assume an infinite set PV of *propositional variables* and we define the set Φ of *formulas* as the least set such that:

- Each propositional variable and the constant $\bot$ are in Φ;
- If $\varphi, \psi \in \Phi$ then $(\varphi \to \psi), (\varphi \vee \psi), (\varphi \wedge \psi) \in \Phi$.

Variables and $\bot$ are called *atomic* formulas. A *subformula* of a formula φ is a (not necessarily proper) part of φ, which itself is a formula.

That is, our basic connectives are: implication $\to$, disjunction $\vee$, conjunction $\wedge$, and the constant $\bot$ (absurdity). Negation $\neg$ and equivalence $\leftrightarrow$ are abbreviations, as well as the constant $\top$ (truth):

- $\neg\varphi$ abbreviates $\varphi \to \bot$;
- $\varphi \leftrightarrow \psi$ abbreviates $(\varphi \to \psi) \wedge (\psi \to \varphi)$;
- $\top$ abbreviates $\bot \to \bot$.

2.1.2. CONVENTION.

1. We often use the convention that implication is right associative, i.e. we write e.g. $\varphi \to \psi \to \vartheta$ instead of $\varphi \to (\psi \to \vartheta)$.
2. We assume that negation has the highest priority, and implication the lowest, with no preference between $\vee$ and $\wedge$. That is, $\neg p \wedge q \to r$ means $((\neg p) \wedge q) \to r$.
3. And of course we skip the outermost parentheses.

In order to understand intuitionistic logic, one should forget the classical notion of "truth". Now our judgements about a logical statement are no longer based on any truth-value assigned to that statement, but on our ability to justify it via an explicit proof or "construction". As a consequence of this we should not attempt to define propositional connectives by means of truth-tables (as it is normally done for classical logic). Instead, we should explain the meaning of compound formulas in terms of their constructions.

Such an explanation is often given by means of the so-called *Brouwer-Heyting-Kolmogorov interpretation*, in short *BHK interpretation*. One can formulate the BHK interpretation as the following set of rules, the algorithmic flavor of which will later lead us to the Curry-Howard isomorphism.

- *A construction of* $\varphi_1 \wedge \varphi_2$ *consists of a construction of* φ_1 *and a construction of* φ_2*;*
- *A construction of* $\varphi_1 \vee \varphi_2$ *consists of an indicator* $i \in \{1, 2\}$ *and a construction of* φ_i*;*
- *A construction of* $\varphi_1 \to \varphi_2$ *is a method (function) transforming every construction of* φ_1 *into a construction of* φ_2*;*
- *There is no construction of* $\bot$.[1]

[1] According to the Houyhnhnms (a construction of) a lie is "the thing which is not".

We do not specify what a construction of a propositional variable is. This is because the meaning of a propositional variable becomes only known when the variable is replaced by a concrete statement. Then we can ask about the construction of that statement. In contrast, the constant $\perp$ represents a statement with no possible construction at all.

Negation $\neg\varphi$ is understood as the implication $\varphi \to \perp$. That is, we may assert $\neg\varphi$ when the assumption of φ leads to absurdity. In other words:

- *A construction of $\neg\varphi$ is a method that turns every construction of φ into a nonexistent object.*

The equivalence of $\neg\varphi$ and $\varphi \to \perp$ holds also in classical logic. But note that the intuitionistic $\neg\varphi$ is stronger than just "there is no construction of φ".

The reader should be aware that the BHK interpretation is by no means intended to make a precise and complete description of constructive semantics. The very notion of "construction" is informal and can be understood in a variety of ways.

2.1.3. EXAMPLE. Consider the following formulas:

(i) $\perp \to p$;

(ii) $p \to q \to p$;

(iii) $(p \to q \to r) \to (p \to q) \to p \to r$;

(iv) $p \to \neg\neg p$;

(v) $\neg\neg\neg p \to \neg p$;

(vi) $(p \to q) \to (\neg q \to \neg p)$;

(vii) $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$;

(viii) $((p \wedge q) \to r) \leftrightarrow (p \to (q \to r))$;

(ix) $\neg\neg(p \vee \neg p)$;

(x) $(p \vee \neg p) \to \neg\neg p \to p$.

All these formulas can be given a BHK interpretation. For instance, a construction for formula (i) is based on the safe assumption that a construction of $\perp$ is impossible. (In contrast, we do not have a construction of $q \to p$, because we cannot generally rule out the existence of a construction of q.) A construction for formula (iv), that is, for $p \to ((p \to \perp) \to \perp)$, is as follows:

> *Given a construction of p, here is a construction of $(p \to \perp) \to \perp$: Take a construction of $p \to \perp$. It is a method to translate constructions of p into constructions of $\perp$. As we have a construction of p, we can use this method to obtain a construction of $\perp$.*

The reader is invited to discover the BHK interpretation of the other formulas (Exercise 2.2).

Of course all the formulas of Example 2.1.3 are classical tautologies. But not every classical tautology can be given a construction.

2.1.4. Example. Each of the formulas below is a classical tautology. Yet none appears to have a construction, despite the fact that some of them are similar or "dual" to certain formulas of the previous example.

(i) $((p \to q) \to p) \to p$;

(ii) $p \vee \neg p$;

(iii) $\neg\neg p \to p$;

(iv) $(\neg q \to \neg p) \to (p \to q)$;

(v) $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$;

(vi) $(p \to q) \to (\neg p \to q) \to q$;

(vii) $((p \leftrightarrow q) \leftrightarrow r) \leftrightarrow (p \leftrightarrow (q \leftrightarrow r))$;

(viii) $(p \to q) \leftrightarrow (\neg p \vee q)$;

(ix) $(p \vee q \to p) \vee (p \vee q \to q)$;

(x) $(\neg\neg p \to p) \to p \vee \neg p$.

For instance, formula (iii) seems to express the same principle as Example 2.1.3(iv). Similarly, formula (iv) and Example 2.1.3(vi) are often treated as two equivalent patterns of a proof by contradiction. Formula (v) and Example 2.1.3(vii) are both known as *De Morgan's laws*, and express the classical duality between conjunction and disjunction.

Such examples show that the symmetry of classical logic disappears when we turn to constructive semantics, and this is obviously due to the fact that negation is no longer an *involution*, i.e. φ and $\neg\neg\varphi$ cannot be identified with each other anymore. Note however that formula (iii) expresses a property weaker than (ii), because we do not have a construction of (x).

Not very surprisingly, proofs by cases (vi) are not constructive. Indeed, this is a simple consequence of the unavailability of the excluded middle—we just cannot a priori split the argument into cases. But it may be a surprise to observe that not only negation or falsity may cause difficulties. Formula (i), known as *Peirce's law*, is purely implicational, but still we are unable to find a construction. Another example of this kind is formula (vii) expressing the classical associativity of equivalence. One can verify it using a binary truth-table, but from the constructive point of view this associativity property seems to be purely accidental.

Formula (viii) can be seen as a definition of classical implication in terms of negation and disjunction. Constructively, this definition does not work. We can say more: None among $\to$, $\bot$, $\vee$, $\wedge$ is definable from the others (see Exercise 2.26).

2.2. Natural deduction

In order to formalize the intuitionistic propositional logic, we define a proof system, called *natural deduction*, and denoted by $\mathrm{NJ}(\to, \bot, \wedge, \vee)$, or simply NJ. The rules of natural deduction express in a precise way the ideas of the informal semantics of Section 2.1.

2.2.1. DEFINITION.

(i) A *judgement* in natural deduction is a pair, written $\Gamma \vdash \varphi$ (and read "Γ proves φ") consisting of a finite set of formulas Γ and a formula φ.

(ii) We use various simplifications when we deal with judgements. For instance, we write $\varphi_1, \varphi_2 \vdash \psi$ instead of $\{\varphi_1, \varphi_2\} \vdash \psi$, or Γ, Δ instead of $\Gamma \cup \Delta$, or Γ, φ instead of $\Gamma \cup \{\varphi\}$. In particular, the notation $\vdash \varphi$ stands for $\varnothing \vdash \varphi$.

(iii) A formal *proof* or *derivation* of $\Gamma \vdash \varphi$ is a finite tree of judgements satisfying the following conditions:

- The root label is $\Gamma \vdash \varphi$;
- All the leaves are *axioms*, i.e. judgements of the form $\Gamma, \varphi \vdash \varphi$;
- The label of each mother node is obtained from the labels of the daughters using one of the rules in Figure 2.1.

If such a proof exists, we say that the judgement $\Gamma \vdash \varphi$ is *provable* or *derivable*, and we write $\Gamma \vdash_N \varphi$. For infinite Γ, we write $\Gamma \vdash_N \varphi$ to mean that $\Gamma_0 \vdash_N \varphi$, for some finite subset Γ_0 of Γ.

(iv) It is customary to omit the index $_N$ in $\vdash_N$. Note that in this way the notation $\Gamma \vdash \varphi$ becomes overloaded. It expresses the provability of a judgement and also denotes the judgement itself. However, the intended meaning is usually clear from the context.

(v) If $\vdash \varphi$ then we say that φ is a *theorem*.[2]

The proof system consists of an axiom scheme and rules. For each logical connective (except $\bot$) we have one or two *introduction* rules and one or two *elimination* rules. An introduction rule for a connective $\circ$ tells us how a conclusion of the form $\varphi \circ \psi$ can be derived. An elimination rule describes the

[2] In general, a *theorem* is a formula provable in a logical system.

$$\Gamma, \varphi \vdash \varphi \ (\mathrm{Ax})$$

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}\ (\to\mathrm{I}) \qquad \frac{\Gamma \vdash \varphi \to \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}\ (\to\mathrm{E})$$

$$\frac{\Gamma \vdash \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}\ (\wedge\mathrm{I}) \qquad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi}\ (\wedge\mathrm{E})\ \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}$$

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}\ (\vee\mathrm{I})\ \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi} \qquad \frac{\Gamma, \varphi \vdash \vartheta \quad \Gamma, \psi \vdash \vartheta \quad \Gamma \vdash \varphi \vee \psi}{\Gamma \vdash \vartheta}\ (\vee\mathrm{E})$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}\ (\bot\mathrm{E})$$

Figure 2.1: Intuitionistic natural deduction NJ

way in which $\varphi \circ \psi$ can be used to derive other formulas. Observe that the natural deduction rules can be seen as a formalization of the BHK interpretation, where "construction" should be read as "proof". Indeed, consider for instance the implication. The premise $\Gamma, \varphi \vdash \psi$ of rule ($\to$I) can be understood as the ability to infer ψ from Γ if a proof of φ is provided. This is enough to derive the implication. The elimination rule ($\to$E) corresponds to the same idea: if we have a proof of $\varphi \to \psi$ then we can turn a proof of φ into a proof of ψ. In a sense, rule ($\to$E) can be seen as a converse of rule ($\to$I), and a similar observation (called the *inversion principle*, see Prawitz [403]) can be made about the other connectives. Rule ($\bot$E), called *ex falso sequitur quodlibet* (or simply *ex falso*) is an exception, because there is no matching introduction rule.

2.2.2. Notation. It is sometimes useful to consider fragments of propositional logic where some connectives do not occur. For instance, in Section 2.6 we discuss the implicational fragment IPC($\to$) of the intuitionistic propositional logic. The subsystem of NJ consisting of the axiom scheme and rules for implication is then denoted by NJ($\to$). This convention applies to other fragments, e.g. IPC($\to, \wedge, \vee$) is the positive fragment, called also *minimal logic*, and NJ($\to, \wedge, \vee$) stands for the appropriate part of NJ.

2.2.3. Example. We give example proofs of our favourite formulas. Below, formulas φ, ψ and ϑ can be arbitrary:

(i)
$$\dfrac{\varphi \vdash \varphi}{\vdash \varphi \to \varphi}\,(\to \mathrm{I})$$

(ii)
$$\dfrac{\dfrac{\varphi, \psi \vdash \varphi}{\varphi \vdash \psi \to \varphi}\,(\to \mathrm{I})}{\vdash \varphi \to (\psi \to \varphi)}\,(\to \mathrm{I})$$

(iii) Here, Γ abbreviates $\{\varphi \to (\psi \to \vartheta), \varphi \to \psi, \varphi\}$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma \vdash \varphi \to (\psi \to \vartheta) \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi \to \vartheta}\,(\to \mathrm{E}) \qquad \dfrac{\Gamma \vdash \varphi \to \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}\,(\to \mathrm{E})}{\Gamma \vdash \vartheta}\,(\to \mathrm{E})}{\varphi \to (\psi \to \vartheta), \varphi \to \psi \vdash \varphi \to \vartheta}\,(\to \mathrm{I})}{\varphi \to (\psi \to \vartheta) \vdash (\varphi \to \psi) \to (\varphi \to \vartheta)}\,(\to \mathrm{I})}{\vdash (\varphi \to (\psi \to \vartheta)) \to (\varphi \to \psi) \to (\varphi \to \vartheta)}\,(\to \mathrm{I})$$

2.2.4. LEMMA. *Intuitionistic propositional logic is closed under weakening and substitution, that is,* $\Gamma \vdash \varphi$ *implies* $\Gamma, \psi \vdash \varphi$ *and* $\Gamma[p := \psi] \vdash \varphi[p := \psi]$, *where* $[p := \psi]$ *denotes a substitution of* ψ *for all occurrences of the propositional variable* p.

PROOF. Induction with respect to the size of proofs (Exercise 2.3). □

Results like the above are sometimes expressed by saying that the following are *derived* (or *admissible*) rules of propositional intuitionistic logic:

$$\dfrac{\Gamma \vdash \varphi}{\Gamma, \psi \vdash \varphi} \qquad\qquad \dfrac{\Gamma \vdash \varphi}{\Gamma[p := \psi] \vdash \varphi[p := \psi]}$$

2.3. Algebraic semantics of classical logic

In the next section we shall introduce an algebraic semantics for intuitionistic logic. To help the reader understand it better, let us begin with classical logic. Usually, semantics of classical propositional formulas is defined so that each connective is seen as an operation acting on the set $\mathbb{B} = \{0, 1\}$ of truth values. That is, we actually deal with an algebraic system

$$\langle \mathbb{B}, \vee, \wedge, \to, -, 0, 1 \rangle$$

where $0 \vee 1 = 1$, $0 \wedge 1 = 0$, $0 \to 1 = 1$ etc. This system is easily ordered so that $0 < 1$, and we have the following property:

$$a \le b \quad \text{iff} \quad a \to b = 1.$$

There is an obvious similarity between the algebra of truth values and the algebra of sets. The logical operations $\vee$ and $\wedge$ behave very much like the set-theoretical $\cup$ and $\cap$. The equation $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$ states one of many analogies. In a similar way negation corresponds to the complement $-A$ (with respect to a fixed domain) and implication to $-A \cup B$.

The notion of a *Boolean algebra* we are now going to introduce is a generalization of both the algebra of truth values and the algebra of sets. We begin though with a weaker and thus more general notion of a *lattice*.

2.3.1. Definition. A *lattice* is a partial order $\langle A, \le\rangle$ such that every two-element subset $\{a, b\}$ of A has both a least upper bound and a greatest lower bound in A. We use the notation $a \sqcup b$ for $\sup_A\{a, b\}$ and $a \sqcap b$ for $\inf_A\{a, b\}$. By analogy with set-theoretic operations, we refer to $\sqcup$ as *union* (or *join*) and to $\sqcap$ as *intersection* (or *meet*). A top (resp. bottom) element in a lattice (if it exists) is usually denoted by 1 (resp. 0).

2.3.2. Lemma. *In a lattice, the following conditions are equivalent:*

(i) $a \le b$;

(ii) $a \sqcap b = a$;

(iii) $a \sqcup b = b$.

Proof. Immediate. □

2.3.3. Example. Every linear order, in particular the set $\mathbb{B}$ of truth values, is a lattice. Every family of sets closed under set union and intersection is also a lattice. But the closure with respect to $\cup$ and $\cap$ is not a necessary condition for a family of sets to be a lattice. A good example is the family of all convex subsets of the Euclidean plane. (A set A is *convex* iff for all $a, b \in A$ the straight line segment joining a and b is contained in A.)

2.3.4. Lemma. *The following equations are valid in every lattice:*

(i) $a \sqcup a = a$ *and* $a \sqcap a = a$;

(ii) $a \sqcup b = b \sqcup a$ *and* $a \sqcap b = b \sqcap a$;

(iii) $(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$ *and* $(a \sqcap b) \sqcap c = a \sqcap (b \sqcap c)$;

(iv) $(a \sqcup b) \sqcap a = a$ *and* $(a \sqcap b) \sqcup a = a$.

Proof. A routine application of the definitions. □

In fact, the properties listed in Lemma 2.3.4 give an axiomatization of lattices as algebraic systems of the form $\langle A, \sqcup, \sqcap \rangle$, cf. Exercise 2.6. We are mostly interested in lattices satisfying some additional properties.

2.3.5. Definition.

(i) A lattice A is *distributive* iff the following equations hold in A:

   (1) $(a \sqcup b) \sqcap c = (a \sqcap c) \sqcup (b \sqcap c)$;

   (2) $(a \sqcap b) \sqcup c = (a \sqcup c) \sqcap (b \sqcup c)$.

(ii) Assume that a lattice A has a top element 1 and a bottom element 0. We say that b is a *complement* of a iff $a \sqcup b = 1$ and $a \sqcap b = 0$.

2.3.6. Lemma. *Let b be a complement of a in a distributive lattice. Then b is the greatest element of A satisfying $a \sqcap b = 0$. In particular, a has at most one complement.*

Proof. Suppose that $a \sqcap c = 0$. Then $c \leq b$, because

$$c = 1 \sqcap c = (a \sqcup b) \sqcap c = (a \sqcap c) \sqcup (b \sqcap c) = 0 \sqcup (b \sqcap c) = b \sqcap c. \qquad \square$$

2.3.7. Definition. A *Boolean algebra* is a distributive lattice B with top and bottom elements, such that every element a of B has a complement (denoted by $-a$).

Boolean algebras are often presented as algebraic structures of the form $\mathcal{B} = \langle B, \sqcup, \sqcap, -, 0, 1 \rangle$. In this case the underlying partial order can be reconstructed with the help of the equivalence: $a \leq b$ iff $a \sqcap b = a$ (cf. Lemma 2.3.2).

2.3.8. Example. Let X be any set. A *field of sets* (*over* X) is a non-empty family $\mathcal{R}$ of subsets of X, closed under set-theoretic union, intersection and complement (to X). Every field of sets is a Boolean algebra. Examples of fields of sets are:

(i) $\mathcal{P}(X)$, the power set of X;

(ii) $\{\varnothing, X\}$;

(iii) $\{A \subseteq X : A \text{ finite or } X - A \text{ finite}\}$.

Observe that the algebra $\mathbb{B}$ of truth values (forget about $\to$ for a moment) is isomorphic to (ii).

The following result is known as *Stone's representation theorem*.

2.3.9. Theorem (M.H. Stone, 1934). *Every Boolean algebra is isomorphic to a field of sets.*

We omit the proof of Stone's theorem, as it would distract us too much from the mainstream of our considerations. The reader may spend some of her spare time doing Exercise 2.15, but we now turn to the Boolean algebra semantics for classical propositional logic.

2.3.10. Definition. A *valuation* in a Boolean algebra $\mathcal{B} = \langle B, \sqcup, \sqcap, -, 0, 1\rangle$ is any map v from the set PV of propositional variables to B. The *value* (in $\mathcal{B}$) of a formula φ with respect to a valuation v is defined by induction.

$$\begin{array}{lcl} [\![p]\!]_v & = & v(p), \quad \text{for } p \in \mathrm{PV}; \\ [\![\bot]\!]_v & = & 0; \\ [\![\varphi \vee \psi]\!]_v & = & [\![\varphi]\!]_v \sqcup [\![\psi]\!]_v; \\ [\![\varphi \wedge \psi]\!]_v & = & [\![\varphi]\!]_v \sqcap [\![\psi]\!]_v; \\ [\![\varphi \to \psi]\!]_v & = & -[\![\varphi]\!]_v \sqcup [\![\psi]\!]_v. \end{array}$$

One writes $\mathcal{B}, v \models \varphi$ when $[\![\varphi]\!]_v = 1$, and $\mathcal{B} \models \varphi$ when $\mathcal{B}, v \models \varphi$, for all v.

It should be clear that the Boolean algebra semantics is a generalization of the ordinary two-valued semantics. Indeed, a formula is a classical tautology if and only if $\mathbb{B} \models \varphi$. In fact, this generalization is not essential.

2.3.11. Theorem. *A propositional formula is a classical tautology if and only if $\mathcal{B} \models \varphi$, for all Boolean algebras $\mathcal{B}$.*

Proof. The implication from right to left is immediate. To prove the other implication suppose that $\mathcal{B} \not\models \varphi$ for some $\mathcal{B}$. By Stone's representation theorem[3] we can assume that $\mathcal{B}$ is a field of sets over some X.

Since $\mathcal{B} \not\models \varphi$, there exists a valuation v in $\mathcal{B}$ with $[\![\varphi]\!]_v \neq X$. Thus, there is $x \in X$ such that $x \notin [\![\varphi]\!]_v$. Define a binary valuation w (a valuation in $\mathbb{B}$) so that $w(p) = 1$ iff $x \in [\![p]\!]_v$. Prove by induction that for all formulas ψ:

$$[\![\psi]\!]_w = 1 \quad \text{iff} \quad x \in [\![\psi]\!]_v.$$

Then $[\![\varphi]\!]_w \neq 1$. □

2.4. Heyting algebras

We will now develop a semantics for intuitionistic propositional logic. For this we analyze the algebraic properties of formulas with respect to provability. We begin by observing that provable implication behaves almost like an ordering relation on formulas, i.e. it is reflexive and transitive. More exactly, for every Γ we have:

[3] A hint for a direct proof is given in Exercise 2.14.

- $\Gamma \vdash \varphi \to \varphi$;
- If $\Gamma \vdash \varphi \to \psi$ and $\Gamma \vdash \psi \to \vartheta$ then $\Gamma \vdash \varphi \to \vartheta$.

This relation is however not anti-symmetric. But we can turn it into a partial order if we identify equivalent formulas. To make this precise, let Γ be a fixed set of propositional formulas (in particular Γ may be empty). We define a relation $\sim_\Gamma$ as follows:

$$\varphi \sim_\Gamma \psi \quad \text{iff} \quad \Gamma \vdash \varphi \to \psi \text{ and } \Gamma \vdash \psi \to \varphi.$$

It is not difficult to see that $\sim_\Gamma$ is an equivalence relation on the set Φ of all formulas, and that (we omit the subscript $_\Gamma$ in $\sim_\Gamma$):

$$[\bot]_\sim = \{\varphi \mid \Gamma \vdash \neg\varphi\} \qquad \text{and} \qquad [\top]_\sim = \{\varphi \mid \Gamma \vdash \varphi\}.$$

Let $\mathcal{L}_\Gamma = \Phi/_\sim = \{[\varphi]_\sim \mid \varphi \in \Phi\}$. It should now be obvious that the relation $\leq_\Gamma$, defined by

$$[\varphi]_\sim \leq_\Gamma [\psi]_\sim \quad \text{iff} \quad \Gamma \vdash \varphi \to \psi$$

is a well-defined partial order over $\mathcal{L}_\Gamma$. We have the equivalence:

$$[\varphi]_\sim = [\psi]_\sim \qquad \text{iff} \qquad [\varphi]_\sim \leq_\Gamma [\psi]_\sim \quad \text{and} \quad [\psi]_\sim \leq_\Gamma [\varphi]_\sim.$$

Our next step is to discover that the partial order $\langle \mathcal{L}_\Gamma, \leq \rangle$ is a lattice. Define

$$\begin{aligned} [\varphi]_\sim \sqcup [\psi]_\sim &= [\varphi \vee \psi]_\sim \,; \\ [\varphi]_\sim \sqcap [\psi]_\sim &= [\varphi \wedge \psi]_\sim \,. \end{aligned}$$

The operations $\sqcup$ and $\sqcap$ are well-defined, because the following are provable:

$$\begin{aligned} (\varphi \leftrightarrow \varphi') &\to ((\psi \leftrightarrow \psi') \to ((\varphi \vee \psi) \leftrightarrow (\varphi' \vee \psi'))); \\ (\varphi \leftrightarrow \varphi') &\to ((\psi \leftrightarrow \psi') \to ((\varphi \wedge \psi) \leftrightarrow (\varphi' \wedge \psi'))). \end{aligned}$$

The reader can easily check that $[\varphi]_\sim \sqcup [\psi]_\sim$ (resp. $[\varphi]_\sim \sqcap [\psi]_\sim$) is the supremum (resp. infimum) of the set $\{[\varphi]_\sim, [\psi]_\sim\}$. Having observed that, the next step is to see that the lattice is distributive and that $[\top]_\sim$ is the top and $[\bot]_\sim$ is the bottom. An optimistic reader might now pose the conjecture that $\mathcal{L}_\Gamma$ is a Boolean algebra with $-[\varphi]_\sim$ defined as $[\neg\varphi]_\sim$.

It would be exactly the case if we dealt with classical logic. But we do not have the excluded middle and there are (not unexpected) difficulties with this complement operation. We have $a \sqcap -a = 0$, but not necessarily $a \sqcup -a = 1$.

The best we can assert about $-a$ is that it is *the greatest element such that* $a \sqcap -a = 0$, and we can call it a *pseudo-complement*. Since negation is a special kind of implication, the above calls for a generalization.

2.4.1. DEFINITION. An element c of a lattice is called a *relative pseudo-complement* of a with respect to b, iff c is the greatest element such that $a \sqcap c \leq b$. The relative pseudo-complement, if exists, is denoted $a \Rightarrow b$, and one defines $-a$ as a special case: $-a = a \Rightarrow 0$.

For example, in our algebra $\mathcal{L}_\Gamma$, often called the *Lindenbaum algebra*, the relative pseudo-complement always exists:

$$[\varphi]_\sim \Rightarrow [\psi]_\sim = [\varphi \to \psi]_\sim.$$

We have just discovered a new type of algebra, called *Heyting algebra* or *pseudo-Boolean algebra*.

2.4.2. DEFINITION. A *Heyting algebra* is a distributive lattice H with top and bottom elements, such that the relative pseudo-complement $a \Rightarrow b$ exists for all $a, b \in H$.

In fact the word "distributive" in the definition above is redundant, see Exercise 2.9. Heyting algebras are typically taken as algebraic structures of the form $\mathcal{H} = \langle H, \sqcup, \sqcap, \Rightarrow, -, 0, 1\rangle$, where the underlying partial order is implicit and defined as usual by the clause $a \leq b$ iff $a \sqcap b = a$ (see Lemma 2.3.2). We often ignore the notational difference between $\mathcal{H}$ and H.

2.4.3. LEMMA.

(i) *The Lindenbaum algebra $\mathcal{L}_\Gamma$ is a Heyting algebra.*

(ii) *Each Boolean algebra is a Heyting algebra with $a \Rightarrow b$ defined as $-a \sqcup b$.*

(iii) *Every finite distributive lattice is a Heyting algebra.*

PROOF. Part (i) has already been shown. For part (ii) first observe that $(-a \sqcup b) \sqcap a = (-a \sqcap a) \sqcup (b \sqcap a) = 0 \sqcup (b \sqcap a) = b \sqcap a \leq b$. Then assume that $c \sqcap a \leq b$. We have $c = c \sqcap 1 = c \sqcap (-a \sqcup a) = (c \sqcap -a) \sqcup (c \sqcap a) \leq (c \sqcap -a) \sqcup b = (c \sqcup b) \sqcap (-a \sqcup b) \leq -a \sqcup b$. Part (iii) follows from the simple fact that, for any given a and b, the set $A = \{c \mid c \sqcap a \leq b\}$ is finite, and thus it has a supremum. Because of distributivity, $\sup A$ itself belongs to A and thus $\sup A = a \Rightarrow b$. □

The following easy observations are often useful:

2.4.4. LEMMA. *In every Heyting algebra,*

(i) *$a \leq b \Rightarrow c$ is equivalent to $a \sqcap b \leq c$;*

(ii) *$a \leq b$ is equivalent to $a \Rightarrow b = 1$.*

The algebraic semantics of intuitionistic propositional logic is defined in a similar style as for classical logic (cf. Definition 2.3.10). We only need to replace Boolean algebras by Heyting algebras.

2.4.5. DEFINITION. Let $\mathcal{H} = \langle H, \sqcup, \sqcap, \Rightarrow, -, 0, 1\rangle$ be a Heyting algebra. A *valuation* in $\mathcal{H}$ is a map $v : \mathrm{PV} \to H$. Given a valuation v in $\mathcal{H}$, we define the *value* $[\![\varphi]\!]_v$ of a formula φ with respect to v (written more precisely as $[\![\varphi]\!]_v^{\mathcal{H}}$).

$$\begin{array}{lcl}
[\![p]\!]_v & = & v(p), \quad \text{for } p \in \mathrm{PV};\\
[\![\bot]\!]_v & = & 0;\\
[\![\varphi \vee \psi]\!]_v & = & [\![\varphi]\!]_v \sqcup [\![\psi]\!]_v\,;\\
[\![\varphi \wedge \psi]\!]_v & = & [\![\varphi]\!]_v \sqcap [\![\psi]\!]_v\,;\\
[\![\varphi \to \psi]\!]_v & = & [\![\varphi]\!]_v \Rightarrow [\![\psi]\!]_v\,.
\end{array}$$

2.4.6. NOTATION. Let $\mathcal{H}$ be a Heyting algebra. We write:

- $\mathcal{H}, v \models \varphi$, when $[\![\varphi]\!]_v = 1$;
- $\mathcal{H} \models \varphi$, when $\mathcal{H}, v \models \varphi$, for all v;
- $\mathcal{H}, v \models \Gamma$, when $\mathcal{H}, v \models \varphi$, for all $\varphi \in \Gamma$;
- $\mathcal{H} \models \Gamma$, when $\mathcal{H}, v \models \Gamma$, for all v;
- $\models \varphi$, when $\mathcal{H}, v \models \varphi$, for all $\mathcal{H}, v$;
- $\Gamma \models \varphi$, when $\mathcal{H}, v \models \Gamma$ implies $\mathcal{H}, v \models \varphi$, for all $\mathcal{H}$ and v.

If $\models \varphi$ holds, we say that φ is *intuitionistically valid* or that is an *intuitionistic tautology.* It follows from the following that the notions of a theorem and a tautology coincide for intuitionistic propositional calculus.

2.4.7. THEOREM (Completeness). *The following are equivalent:*[4]

(i) $\Gamma \vdash \varphi$;

(ii) $\Gamma \models \varphi$.

PROOF. (i) $\Rightarrow$ (ii): Let $\Gamma = \{\vartheta_1, \ldots, \vartheta_n\}$. If v is a valuation in a Heyting algebra $\mathcal{H}$, then $[\![\Gamma]\!]_v$ stands for $[\![\vartheta_1]\!]_v \sqcap \cdots \sqcap [\![\vartheta_n]\!]_v$ (which is 1 when $\Gamma = \varnothing$). By induction with respect to derivations we prove that, for all v:

$$\textit{If } \Gamma \vdash \varphi \textit{ then } [\![\Gamma]\!]_v \leq [\![\varphi]\!]_v.$$

[4]Part (i) $\Rightarrow$ (ii) is called *soundness*, while (ii) $\Rightarrow$ (i) is the proper *completeness*.

The statement of the theorem follows from the special case when $[\![\Gamma]\!]_v = 1$.

We proceed by cases depending on the last rule used in the proof. For instance, consider the case of ($\to$I). We need to show that $[\![\Gamma]\!]_v \leq [\![\varphi_1 \to \varphi_2]\!]_v$ follows from the induction hypothesis $[\![\Gamma]\!]_v \sqcap [\![\varphi_1]\!]_v \leq [\![\varphi_2]\!]_v$. But that is an easy consequence of $[\![\varphi_1 \to \varphi_2]\!]_v = [\![\varphi_1]\!]_v \Rightarrow [\![\varphi_2]\!]_v$. For the case of ($\vee$E) observe that $[\![\Gamma]\!]_v \leq [\![\varphi_1 \vee \varphi_2]\!]_v$ implies

$$[\![\Gamma]\!]_v = [\![\Gamma]\!]_v \sqcap ([\![\varphi_1]\!]_v \sqcup [\![\varphi_2]\!]_v) = ([\![\Gamma]\!]_v \sqcap [\![\varphi_1]\!]_v) \sqcup ([\![\Gamma]\!]_v \sqcap [\![\varphi_2]\!]_v).$$

If both components of $\sqcup$ are less than or equal to $[\![\varphi]\!]_v$ then so is $[\![\Gamma]\!]_v$.

(ii) $\Rightarrow$ (i): This follows from our construction of the Lindenbaum algebra. Indeed, suppose that $\Gamma \models \varphi$, but $\Gamma \nvdash \varphi$. Then $\varphi \not\sim_\Gamma \top$, i.e. $[\varphi]_\sim \neq 1$ in $\mathcal{L}_\Gamma$. Define a valuation v in $\mathcal{L}_\Gamma$ by $v(p) = [p]_\sim$, and prove by induction that $[\![\psi]\!]_v = [\psi]_\sim$, for all ψ. It follows that $[\![\varphi]\!]_v \neq 1$, a contradiction. $\square$

The completeness proof above can easily be adapted to classical logic, if we expand our natural deduction system by appropriate rules to account for the extension (we do it later in Chapter 6). The Lindenbaum algebra $\mathcal{L}_\Gamma$ is then a Boolean algebra and we conclude that classical propositional logic is sound and complete with respect to the general Boolean algebra semantics, as defined in Section 2.3. To obtain a completeness result for the two-valued semantics, one then uses Theorem 2.3.11. For an alternative approach see the proof of Theorem 6.1.10.

So far, Heyting algebras remain a nice but abstract notion. In order to actually make use of our algebraic semantics, we need concrete examples of such algebras. And these are not hard to find. The most prominent example of a Heyting algebra which is not a Boolean algebra is the family of open sets of a topological space.

An important difference between a topological space and a field of sets is that a complement of an open set is usually not open. If we want to interpret propositions as open sets, we can easily do it for conjunctions and disjunctions, using sums and intersections. But we cannot in general interpret a negation $\neg p$ as the complement of the value of p. The best we can do is to take the largest open set contained in the complement—the interior. This is exactly the Heyting algebra pseudo-complement.

2.4.8. Proposition. *Let $\mathcal{H} = \langle \mathcal{O}(\mathcal{T}), \cup, \cap, \Rightarrow, \sim, \varnothing, \mathcal{T} \rangle$, where $\mathcal{T}$ is a topological space and*

- *the operations $\cap$, $\cup$ are set-theoretic;*
- *$A \Rightarrow B = \mathrm{Int}(-A \cup B)$, for arbitrary open sets A and B;*
- *$\sim A = \mathrm{Int}(-A)$, where $-$ is the set-theoretic complement.*

Then $\mathcal{H}$ is a Heyting algebra.

PROOF. Exercise 2.16. □

2.4.9. EXAMPLE. To see that Peirce's law $((p \to q) \to p) \to p$ is not intuitionistically valid, consider the algebra of open subsets of the real line. Take $v(p) = \mathbb{R} - \{0\}$ and $v(q) = \varnothing$. Then $[\![p \to q]\!]_v = \mathrm{Int}(\{0\} \cup \varnothing) = \varnothing$, and $[\![(p \to q) \to p]\!]_v = \mathrm{Int}(\mathbb{R} \cup (\mathbb{R} - \{0\})) = \mathbb{R}$. The value of the whole formula is thus the set $\mathrm{Int}(\varnothing \cup (\mathbb{R} - \{0\})) = \mathbb{R} - \{0\} \neq \mathbb{R}$.

Consider now the *tertium non datur* principle in the form $p \vee \neg p$. If we take $v(p) = (0, \infty)$ then $[\![p \vee \neg p]\!]_v = \mathbb{R} - \{0\}$. Again, only one point is missing.

That the border between "yes" and "no" in the example above is so thin is not just a coincidence. By the following result, a classical tautology must always be represented in a topological space by a *dense* set, i.e. one whose complement has an empty interior.

2.4.10. THEOREM (Glivenko). *A formula φ is a classical tautology iff $\neg\neg\varphi$ is an intuitionistic tautology.*

PROOF. Exercise 2.34. □

WARNING. The above does not hold for first-order logic, cf. Example 8.2.2(i).

Intuitionistic logic, unlike classical logic, is not finite-valued. There is no single finite Heyting algebra $\mathcal{H}$ such that $\vdash \varphi$ is equivalent to $\mathcal{H} \models \varphi$. Indeed, consider the formula $\bigvee\{p_i \leftrightarrow p_j \mid i, j = 0, \ldots, n \text{ and } i \neq j\}$. (Here the symbol $\bigvee$ abbreviates the disjunction of all members of the set.) This formula is not valid in general (Exercise 2.19), although it is valid in all Heyting algebras of cardinality at most n.

A complete semantics can however be defined by an infinite Heyting algebra. Some of these are quite familiar.

2.4.11. THEOREM. *Let $\mathcal{H}$ be the algebra of all open subsets of*

- *the set $\mathbb{R}$ of reals, or*
- *the set $\mathbb{Q}$ of rationals, or*
- *any Cartesian product of the above, in particular $\mathbb{R}^2$.*

Then $\mathcal{H} \models \varphi$ iff φ is valid.

PROOF. Exercise 2.30. □

Theorem 2.4.11 may be interpreted as follows. If a formula φ is not valid intuitionistically, it is always possible to give a counterexample over the real line. The same holds for the Euclidean plane $\mathbb{R}^2$. The latter has the following nice consequence: One can always expect to produce a counterexample by drawing pictures on paper. (A similar property holds of course for classical logic. In Exercise 2.14 take $\mathcal{B} = \mathcal{P}(\mathbb{R}^2)$, the power set of the real plane.)

An alternative to one infinite algebra is the collection of all finite models.

2.4.12. Theorem (Finite model property). *A formula φ of length n is valid iff it is valid in all Heyting algebras of cardinality at most 2^{2^n}.*

Proof. Assume that φ is not valid, i.e. that $\mathcal{H}, v \not\models \varphi$, for some algebra $\mathcal{H} = \langle H, \sqcup, \sqcap, \Rightarrow, -, 0, 1\rangle$. We show how to replace $\mathcal{H}$ by a finite algebra. Let $\varphi_1, \ldots, \varphi_m$ be all subformulas of φ. (Note that $m \leq n$.) Let $a_i = [\![\varphi_i]\!]_v$, for $i = 1, \ldots, m$, and consider the subalgebra L of $\langle H, \sqcup, \sqcap, 0, 1\rangle$ generated by $a_1, \ldots, a_m$. Observe that L has at most 2^{2^m} elements, namely all possible unions of the 2^m possible intersections of the generators. (We get 0 if the union has no components and 1 if there is one component of length zero. The closure under $\sqcap$ follows from distributivity.) In addition, L is a Heyting algebra, because of Lemma 2.4.3(iii). But L is not necessarily a Heyting subalgebra of $\mathcal{H}$, i.e. the definition of $\Rightarrow$ in L and in $\mathcal{H}$ may be different. To distinguish the two, let us use the notation $\Rightarrow_L$ and $\Rightarrow_{\mathcal{H}}$, respectively.

Thus it is not necessarily the case that $[\![\psi]\!]_v^L = [\![\psi]\!]_v^{\mathcal{H}}$ for arbitrary ψ. However, this equation holds for all subformulas of φ, including φ itself. This is shown by induction, using the following observation: If $\psi_1 \to \psi_2$ is a subformula of φ then $[\![\psi_1]\!]_v^{\mathcal{H}} \Rightarrow_{\mathcal{H}} [\![\psi_2]\!]_v^{\mathcal{H}} = [\![\psi_1 \to \psi_2]\!]_v^{\mathcal{H}} \in L$. This implies $[\![\psi_1]\!]_v^{\mathcal{H}} \Rightarrow_{\mathcal{H}} [\![\psi_2]\!]_v^{\mathcal{H}} = [\![\psi_1]\!]_v^{\mathcal{H}} \Rightarrow_L [\![\psi_2]\!]_v^{\mathcal{H}}$. Details are left to the reader, and the conclusion is that $[\![\varphi]\!]_v^L \neq 1$ and thus $L, v \not\models \varphi$. □

From the finite model property it follows that intuitionistic propositional logic is decidable. The upper bound obtained this way (double exponential space) is unsatisfactory. But it can be improved down to polynomial space, see Lemma 4.2.3 and Exercise 7.13.

2.5. Kripke semantics

We now introduce another semantics of intuitionistic propositional logic. This semantics reflects the following idea. From the constructive point of view, we can assert the truth only of the propositions of which we are certain. But by learning about new facts we gain more information, and we can add new propositions to our state of knowledge. We should however not lose our knowledge. In other words, what is true now will remain true forever, but what is not recognized today as true may become true tomorrow. Because of that we have to be careful and assert "*not A*" only when it is entirely impossible that we might ever assert A.

2.5.1. Definition. A *Kripke model* is a triple of the form

$$\mathcal{C} = \langle C, \leq, \Vdash\rangle,$$

where C is a non-empty set, whose elements are called *states* or *possible worlds*, $\leq$ is a partial order in C, and $\Vdash$ is a binary relation between elements of C and propositional variables. The relation $\Vdash$ (read "forces") must satisfy the following monotonicity condition.

$$\text{If } c \leq c' \text{ and } c \Vdash p \text{ then } c' \Vdash p.$$

The intuition is that elements of the model represent states of knowledge. The relation $\leq$ corresponds to extending states by gaining more knowledge, and the relation $\Vdash$ determines which propositional variables are assumed to be true in a given state. We extend this relation to provide meaning for propositional formulas as follows.

2.5.2. DEFINITION. If $\mathcal{C} = \langle C, \leq, \Vdash\rangle$ is a Kripke model, then

- $c \Vdash \varphi \vee \psi$ iff $c \Vdash \varphi$ or $c \Vdash \psi$;
- $c \Vdash \varphi \wedge \psi$ iff $c \Vdash \varphi$ and $c \Vdash \psi$;
- $c \Vdash \varphi \to \psi$ iff $c' \Vdash \psi$ for all $c' \geq c$ with $c' \Vdash \varphi$;
- $c \Vdash \bot$ does not hold.

Note that the definition above implies the following rule for negation:

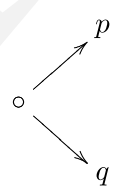
- $c \Vdash \neg\varphi$ iff $c' \nVdash \varphi$, for all $c' \geq c$.

The notation $\Vdash$ can be used in various ways. Sometimes we write $\mathcal{C}, c \Vdash \varphi$ to make it clear which model is being used. We write $\mathcal{C} \Vdash \varphi$ when $c \Vdash \varphi$, for all $c \in C$. The notation $c \Vdash \Gamma$ means that $c \Vdash \varphi$ for all $\varphi \in \Gamma$, and similarly for $\mathcal{C} \Vdash \Gamma$. Finally, $\Gamma \Vdash \varphi$ that for every Kripke model $\mathcal{C}$ and every state c of $\mathcal{C}$, the condition $\mathcal{C}, c \Vdash \Gamma$ implies $\mathcal{C}, c \Vdash \varphi$.

The following generalized monotonicity follows by easy induction:

2.5.3. LEMMA. *If $c \leq c'$ and $c \Vdash \varphi$ then $c' \Vdash \varphi$.*

2.5.4. EXAMPLE. Let $C = \{c, c', c''\}$ where $c \leq c', c''$ and c', c'' are incomparable. A Kripke model $\mathcal{C} = \langle C, \leq, \Vdash\rangle$, where $c' \Vdash p$ and $c'' \Vdash q$ and $c \nVdash p, q$ can be represented by the following graph:



In this model we have e.g. $c \Vdash \neg\neg(p \vee q)$ and $c \Vdash (p \to q) \to q$, but $c \nVdash p \vee \neg p$.

We now want to show completeness of Kripke semantics. For this, we transform every Heyting algebra into a Kripke model.

2.5.5. DEFINITION. A *filter* in a Heyting algebra $\mathcal{H} = \langle H, \sqcup, \sqcap, \Rightarrow, -, 0, 1\rangle$ is a non-empty subset F of H, such that[5]

- $a, b \in F$ implies $a \sqcap b \in F$;
- $a \in F$ and $a \leq b$ implies $b \in F$.

A filter F is *proper* iff $F \neq H$. A proper filter F is *prime* iff $a \sqcup b \in F$ implies that either $a \in F$ or $b \in F$.

2.5.6. LEMMA. *Let A be any subset of a Heyting algebra $\mathcal{H}$. Then the set $F = \{a \in \mathcal{H} \mid a \geq a_1 \sqcap \ldots \sqcap a_k,$ for some $a_1, \ldots, a_k \in A\}$ is the least filter containing A. The filter F is proper iff $a_1 \sqcap \ldots \sqcap a_k \neq 0$, for all finite sets $\{a_1, \ldots, a_k\} \subseteq A$.*

PROOF. Left to the reader. $\Box$

2.5.7. LEMMA. *Let F be a proper filter in $\mathcal{H}$ and let $a \notin F$. There exists a prime filter G such that $F \subseteq G$ and $a \notin G$.*

PROOF. Let $\mathcal{F} = \{E \mid E$ is a filter and $F \subseteq E$ and $a \notin E\}$. One shows that the union of an arbitary chain in $\mathcal{F}$ is itself a member of $\mathcal{F}$. Thus every chain in $\mathcal{F}$ has an upper bound in $\mathcal{F}$. We can apply the Kuratowski-Zorn Lemma A.1.1 to conclude that $\mathcal{F}$ has a maximal element G with respect to inclusion. We show that G is a prime filter.

For $y \in \mathcal{H}$, let $G_y = \{x \mid x \geq g \sqcap y$, for some $g \in G\}$. By Lemma 2.5.6, each G_y is a filter. We claim that if $b \sqcup c \in G$ then either G_b or G_c must belong to $\mathcal{F}$. Thus $b \in G$ or $c \in G$ by the maximality of G.

Suppose otherwise, i.e. neither G_b nor G_c is in $\mathcal{F}$. That is, $a \in G_b \cap G_c$ and there are $g_1, g_2 \in G$ with $g_1 \sqcap b \leq a$ and $g_2 \sqcap c \leq a$. Then $(g_1 \sqcap g_2) \sqcap (b \sqcup c) \in G$, and we have $a = a \sqcup a \geq (g_1 \sqcap g_2 \sqcap b) \sqcup (g_1 \sqcap g_2 \sqcap c) = (g_1 \sqcap g_2) \sqcap (b \sqcup c)$, so that $a \in G$, a contradiction. $\Box$

2.5.8. LEMMA. *Let v be a valuation in a Heyting algebra $\mathcal{H}$, where $0 \neq 1$. There is a Kripke model $\mathcal{C} = \langle C, \leq, \Vdash\rangle$, such that the conditions $\mathcal{H}, v \models \varphi$ and $\mathcal{C} \Vdash \varphi$ are equivalent for all φ.*

PROOF. We take C to be the set of all prime filters in $\mathcal{H}$. The relation $\leq$ is inclusion, and we define $F \Vdash p$ iff $v(p) \in F$. For all formulas ψ we prove

$$F \Vdash \psi \quad \text{iff} \quad [\![\psi]\!]_v \in F, \qquad (*)$$

by induction with respect to ψ. The only non-trivial case is $\psi = \psi' \to \psi''$. Suppose that $F \Vdash \psi' \to \psi''$, but $[\![\psi' \to \psi'']\!]_v = [\![\psi']\!]_v \Rightarrow [\![\psi'']\!]_v \notin F$. Take the least filter G' containing $F \cup \{[\![\psi']\!]_v\}$. Lemma 2.5.6 implies that

$$G' = \{b \mid b \geq f \sqcap [\![\psi']\!]_v \text{ for some } f \in F\},$$

[5]Exercises 2.11 and 2.12 explain the intuition of a filter: It is an algebraic model of a "state of knowledge", closed under logical consequence.

and we have $[\![\psi'']\!]_v \notin G'$, in particular G' is proper. Indeed, otherwise there is an $f \in F$, with $[\![\psi'']\!]_v \geq f \sqcap [\![\psi']\!]_v$, and thus $f \leq [\![\psi']\!]_v \Rightarrow [\![\psi'']\!]_v \in F$.

Using Lemma 2.5.7, we extend G' to a prime filter G, not containing $[\![\psi'']\!]_v$. By the induction hypothesis $G \Vdash \psi'$, because $[\![\psi']\!]_v \in G$. Since $F \Vdash \psi' \to \psi''$, it follows that $G \Vdash \psi''$. That is, $[\![\psi'']\!]_v \in G$, which is not true.

For the converse, assume that $[\![\psi' \to \psi'']\!]_v \in F$ and $F \subseteq G \Vdash \psi'$. From the induction hypothesis we have $[\![\psi']\!]_v \in G$ and since $F \subseteq G$ we obtain $[\![\psi']\!]_v \Rightarrow [\![\psi'']\!]_v \in G$. Thus $[\![\psi'']\!]_v \geq [\![\psi']\!]_v \sqcap ([\![\psi']\!]_v \Rightarrow [\![\psi'']\!]_v) \in G$, so that $[\![\psi'']\!]_v \in G$. Apply again the induction hypothesis to conclude $G \Vdash \psi''$.

The other cases are easy. Note that primality is essential for disjunction. Having shown $(*)$, assume that $\mathcal{H}, v \not\models \varphi$, i.e. $[\![\varphi]\!]_v \notin \{1\}$. The filter $\{1\}$ extends to a prime filter G such that $[\![\varphi]\!]_v \notin G$, and thus $\mathcal{C}, G \not\Vdash \varphi$. On the other hand, if $\mathcal{H}, v \models \varphi$, then $[\![\varphi]\!]_v = 1$ and 1 belongs to all filters in $\mathcal{H}$. □

2.5.9. THEOREM (Completeness). *The conditions*

$$\Gamma \vdash \varphi \qquad \Gamma \models \varphi \qquad \Gamma \Vdash \varphi$$

are equivalent to each other.

PROOF. To show that $\Gamma \vdash \varphi$ implies $\Gamma \Vdash \varphi$ we proceed by induction. As an example consider the induction step for rule $(\to\mathrm{I})$. Assume that we have derived $\Gamma \vdash \varphi_1 \to \varphi_2$ from $\Gamma, \varphi_1 \vdash \varphi_2$. Let $c \Vdash \Gamma$, and let $c' \geq c$ be such that $c' \Vdash \varphi_1$. By the monotonicity we have $c' \Vdash \Gamma, \varphi_1$, and from the induction hypothesis we obtain $c' \Vdash \varphi_2$ as desired. We leave the other cases to the reader. (In the case of $(\bot\mathrm{E})$ observe that $\Gamma \Vdash \bot$ simply means that $c \Vdash \Gamma$ is impossible, and thus $\Gamma \Vdash \varphi$ can be safely concluded.)

By Theorem 2.4.7 it now remains to prove that $\Gamma \Vdash \varphi$ implies $\Gamma \models \varphi$. Assume the contrary. Then $\mathcal{H}, v \models \Gamma$ but $\mathcal{H}, v \not\models \varphi$, for some $\mathcal{H}, v$. From the previous lemma we have a Kripke model $\mathcal{C}$ with $\mathcal{C} \Vdash \Gamma$ and $\mathcal{C} \not\Vdash \varphi$. □

The Kripke model of Example 2.5.4 shows that the excluded middle principle is not Kripke valid. Here is another nice application of Kripke semantics.

2.5.10. PROPOSITION (Disjunction property). *If* $\vdash \varphi \vee \psi$ *then* $\vdash \varphi$ *or* $\vdash \psi$.

PROOF. Assume $\nvdash \varphi$ and $\nvdash \psi$. There are Kripke models $\mathcal{C}_1 = \langle C_1, \leq_1, \Vdash_1 \rangle$ and $\mathcal{C}_2 = \langle C_2, \leq_2, \Vdash_2 \rangle$ and states $c_1 \in C_1$ and $c_2 \in C_2$, such that $c_1 \not\Vdash \varphi$ and $c_2 \not\Vdash \psi$. Without loss of generality we can assume that c_1 and c_2 are least elements of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, and that $C_1 \cap C_2 = \varnothing$. Define a new model $\mathcal{C} = \langle C_1 \cup C_2 \cup \{c_0\}, \leq, \Vdash \rangle$, where $c_0 \notin C_1 \cup C_2$ and the order is the union of $\leq_1$ and $\leq_2$, extended by c_0 taken as the least element. The relation $\Vdash$ is simply the sum of $\Vdash_1$ and $\Vdash_2$. In particular $c_0 \not\Vdash p$, for all variables p. It is easy to see that $\mathcal{C}$ is a Kripke model. In addition we have $\mathcal{C}, c_1 \Vdash \vartheta$ iff $\mathcal{C}_1, c_1 \Vdash \vartheta$, for all formulas ϑ, and a similar property holds for c_2.

Now suppose that $\vdash \varphi \vee \psi$. By soundness, we have $c_0 \Vdash \varphi \vee \psi$, and thus either $c_0 \Vdash \varphi$ or $c_0 \Vdash \psi$, by definition of $\Vdash$. Then either $c_1 \Vdash \varphi$ or $c_2 \Vdash \psi$, because of monotonicity. ☐

2.6. The implicational fragment

The most important logical connective is the implication. Thus, it is meaningful to study *implicational formulas*, built with only this connective. The natural deduction system NJ($\to$) for this restricted calculus consists of rules ($\to$E), ($\to$I) and the axiom scheme (Ax).

2.6.1. THEOREM. *The natural deduction system* NJ($\to$) *is complete with respect to Kripke models, i.e. if $\to$ is the only connective occurring in in Γ and φ then the conditions $\Gamma \vdash \varphi$ and $\Gamma \Vdash \varphi$ are equivalent.*

PROOF. The implication from left to right follows from soundness of the full natural deduction system. For the proof in the other direction, let us assume that $\Gamma \nvdash \varphi$. Define $Con(\Delta) = \{\psi \mid \Delta \vdash \psi\}$ and consider a Kripke model $\mathcal{C} = \langle C, \subseteq, \Vdash \rangle$, where

$$C = \{\Delta \mid \Gamma \subseteq \Delta, \text{ and } Con(\Delta) = \Delta\}.$$

The order is by inclusion and $\Delta \Vdash p$ holds for a propositional variable p if and only if $p \in \Delta$. By induction we show the following claim:

$$\Delta \Vdash \psi \quad \text{iff} \quad \psi \in \Delta, \tag{$*$}$$

for all implicational formulas ψ and all states Δ. The case of a variable is immediate from the definition. Let ψ be $\psi_1 \to \psi_2$ and let $\Delta \Vdash \psi$. To show that $\psi \in \Delta$, take $\Delta' = \{\vartheta \mid \Delta, \psi_1 \vdash \vartheta\}$. Then $\psi_1 \in \Delta'$ and, by the induction hypothesis, $\Delta' \Vdash \psi_1$. Thus $\Delta' \Vdash \psi_2$, because $\Delta \subseteq \Delta'$, and we get $\psi_2 \in \Delta'$, again by the induction hypothesis. Thus, $\Delta, \psi_1 \vdash \psi_2$, and by ($\to$ I) we get what we want.

Now assume $\psi_1 \to \psi_2 \in \Delta$ (in particular $\Delta \vdash \psi_1 \to \psi_2$) and take $\Delta' \supseteq \Delta$ with $\Delta' \Vdash \psi_1$. Then $\psi_1 \in \Delta'$, so $\Delta' \vdash \psi_1$. But also $\Delta' \vdash \psi_1 \to \psi_2$, because $\Delta \subseteq \Delta'$. By ($\to$ E) we can derive $\Delta' \vdash \psi_2$, which means, by the induction hypothesis, that $\Delta' \Vdash \psi_2$. This completes the proof of ($*$).

Now let $\Delta = \{\psi \mid \Gamma \vdash \psi\}$. Then $\Delta \in C$ and from ($*$) we have $\Delta \Vdash \gamma$ for all $\gamma \in \Gamma$, but $\Delta \nVdash \varphi$. ☐

It follows from Theorems 2.5.9 and 2.6.1 that the three conditions $\Gamma \vdash \varphi$, $\Gamma \models \varphi$, and $\Gamma \Vdash \varphi$ are equivalent for implicational formulas. The completeness theorem has a very important consequence: the *conservativity* of IPC over its implicational fragment.

2.6.2. THEOREM. *Let φ be an implicational formula, and let Γ be a set of implicational formulas. If $\Gamma \vdash_N \varphi$ then $\Gamma \vdash \varphi$ in* NJ($\to$).

2.7. Notes

The roots of constructivism in mathematics reach deeply into the 19th century, or even further into the past. Intuitionists themselves admitted for instance the inspiration of the philosophy of Immanuel Kant (1724–1804). According to Kant, such areas of mathematical cognition as time and space, are directly accessible to the *human intuition* rather than empirically "observed". Mathematics can thus be seen as a purely mental construction.

Leopold Kronecker (1823–1891) is usually cited as the first author who explicitly applied constructive ideas in mathematics. A correct definition of a number, according to Kronecker, was one which could be verified in a finite number of steps. And a proof of an existential statement should provide an explicit object witnessing that statement.

In the search for a firm basis of mathematics, Kronecker was soon joined by many others. In the second half of the 19th century mathematics was changing in a quite important way. With development of new branches, including mathematical logic, the subject of mathematical research was becoming more and more abstract and unrelated to physical experience. The mathematician's activity changed from *discovering* properties of the "real" world into *creating* an abstract one. This raised important questions concerning the foundations of mathematics. With the discovery of paradoxes, notably the well-known paradox due to Russell, these questions became really urgent.

The end of the 19th and beginning of the 20th century was a period of an intensive development and competition of ideas and trends aiming at explaining the conceptual basis of the modern mathematics. Some of these trends created the background for the philosophical school known as *intuitionism*. For instance, Poincaré emphasized the role of intuition in mathematics and Lebesgue denied the existence of objects (like number sequences) unless they were explicitly defined.

But the principles of intuitionism were first formulated in the works of the Dutch mathematician and philosopher Luitzen Egbertus Jan Brouwer (1881–1966). Beginning with his thesis of 1907, the subject was developed in subsequent works into a general and consistent exposition of a philosophy of science [56, 112, 320]. Brouwer is also the inventor of the term "intuitionism", which was originally meant to denote a philosophical approach to the foundations of mathematics, being in opposition to Hilbert's *formalism*. Here, formalism is understood as an attempt to describe mathematics within the framework of formal manipulation of symbols. By restriction to finitary methods, formalists hoped to achieve a rigorous proof of consistency of mathematics and to develop mechanical tools to verify mathematical truth. As we know, *Hilbert's programme*, as this endeavour was called, failed after Gödel's results, but formalism contributed a lot to the development of contemporary logic.

Brouwer rejected the idea that mathematics be reduced to some kind of formal game. But he also rejected the idea of mathematics as a natural science. Instead, intuitionists insisted that the human mind (the intuition), and not the external world, is the source of mathematical notions. That is, mathematical objects exist only as the creations of a mathematician, and mathematical truth is only achieved by means of proof, a mental activity. Quoting Brouwer after van Dalen [111]: *"There are no non-experienced truths"*.

Brouwer did not intend to make intuitionistic logic a part of formal logic. The intuitionistic propositonal calculus was developed between 1925 and 1930 by Kolmogorov [273], Glivenko [190], and Heyting [227]. Their research in intuitionistic proof theory turned Brouwer's idealistic philosophy into a branch of mathematical logic. The interest in this logic has since then largely been motivated by its constructive character.

To explain what intuitionistic logic is about, one usually refers to the Brouwer-Heyting-Kolmogorov interpretation, as we did in Section 2.1. Only implicitly present in Brouwer's work, this explanation is due to Heyting [228, 229, 230] and Kolmogorov [274]. Although intuitively convincing and useful, the BHK interpretation causes also some misunderstanding. This is obviously due to the imprecise character of the rules and also to the numerous differences between their variants. For instance, we use the word *construction*, following Heyting [230, p. 102], Prawitz [405], and Howard [247], while other authors talk about *proofs* [189, 488, 489], *realizers* [346], *evidence* [311], etc. Kolmogorov's original paper was about *problems* and their *solutions*. Some of Heyting's informal explanations are about *fulfillment* of an *intention* expressed by a proposition [228] or about *conditions* under which a proposition can be *asserted* [230].

The way the rules are stated varies too. For instance, our interpretation of disjunction requires that a construction explicitly determines which component is taken into account. This variant is common nowadays (as it might make a difference even in the case of $\varphi \vee \varphi$), but the following would be closer to the original formulation of Heyting and Kolmogorov:

A construction of $\varphi_1 \vee \varphi_2$ *is either a construction of* φ_1 *or a construction of* φ_2.

Another possible extension of BHK (cf. [278, 462, 487]) is to require that a construction of $\varphi_1 \to \varphi_2$ should include a verification of correctness.

Various other approaches to intuitionistic semantics, most notably Kleene's realizability (see Chapter 9) are often compared to the BHK interpretation, and then obvious similarities as well as important differences are found. See for instance [15, 134, 377, 486, 488]. But a liberal understanding of the BHK rules may also lead to topological semantics [436], or even classical two-valued semantics [134].

Begining with Gödel, many authors considered various formalizations of the BHK interpretation in terms of classical logic, for instance by introducing a formal notion of "provability". In particular, one can think of *modal logic* (see [68]) as a form of provability logic. A recent development is the logic LP of Artemov [15, 16].

The natural deduction system for propositional intuitionistic logic is usually attributed to the work of Gentzen [171] but one can find a similar system in an independent paper by Jaśkowski [254]. The algebraic approach to formal semantics originated with the work of Łukasiewicz on many-valued logic. Semantic properties of intuitionistic logic were initially formulated in terms of "matrices". This includes, for instance, the solution to our Exercise 2.19 given by Gödel in 1932, and a completeness theorem and an initial version of the finite model property (Theorem 2.4.12) published by Jaśkowski in 1936. The topological semantics originated in the late 1930's with papers by Stone and Tarski. A completeness theorem (*Zweiter Hauptsatz*) in Tarski's paper [473] implies our Theorem 2.4.11. Exercise 2.30 is based on Mints and Zhang [347]. See also [47].

Heyting algebras emerged from the "closure algebras" and "Brouwerian algebras" investigated in 1944–1948 by McKinsey and Tarski,[6] who also gave the double-

[6]Interestingly, they initially used closed sets, rather than open sets, so that $\wedge$ was interpreted by $\cup$ and $\vee$ by $\cap$.

exponential bound of Theorem 2.4.11.

In 1956, Beth proposed a semantics ("Beth models") very similar to Kripke semantics. The latter dates from 1959, and was first designed for modal logic. The completeness of intuitionistic logic with respect to Kripke models was shown in 1963 and published in [283]. Our Lemma 2.5.8 and Exercise 2.28 are based on Fitting's [151], who attributes the translation to Beth.

Decidability of intuitionistic logic is of course a consequence of the finite model property, but the first (syntactical) proof of decidability was derived by Gentzen from his cut-elimination theorem of 1935 (see Corollary 7.3.9).

For the interested reader, let us also mention that the first proof of the independence of intuitionistic propositional connectives (Exercise 2.26) is due to Wajsberg [505], and was published in 1938. An independent solution was given next year by McKinsey [334]. Later, Prawitz [403] derived yet another solution from proof normalization. The example about $\sqrt{2}$, mentioned at the beginning of this chapter, probably appeared first in print in [253]. Since first used by Hindley in 1970, it is now obligatory in every introduction to intuitionistic logic. (In fact, there is a Gelfond-Schneider theorem which implies that $\sqrt{2}$ raised to the power $\sqrt{2}$ is irrational, but the proofs we have seen in [168, 296] do not qualify as strictly constructive.)

In this short survey we have only recalled the very basic facts about the initial history of intuitionistic logic. To learn more about the history and motivations see the books [112, 136, 230, 320, 488] and articles [111, 483, 484, 487].

For a general introduction to intuitionistic logic we recommend the article [110] of van Dalen, and also the books of Mints [346], Dragalin [134] and Fitting [151, 152]. A comprehensive study of the algebraic semantics for intuitionistic (and classical) logic is the book of Rasiowa and Sikorski [410]. See also Chapter 13 of [488, vol. II].

Although the subject of a large part of the present book is constructive logic, our approach is entirely classical, or *naive common sense*, as we perhaps should prefer to say. We do not restrict our apparatus to intuitionistic logic, accepting proofs by contradiction with no reservations. But the reader should be aware that there is a broad and active area of research, called *constructive mathematics*, aiming at re-building classical mathematics on the basis of constructive reasoning. This is far beyond the scope of this book, and the reader is referred to [38, 48, 343, 426, 488].

2.8. Exercises

2.1. (From [78].) Prove that at least one of $e + \pi$ and $e\pi$ is not algebraic.

2.2. Find constructions for the formulas in Example 2.1.3, and do not find constructions for the formulas in Example 2.1.4.

2.3. Prove Lemma 2.2.4 about weakening and substitution.

2.4. Give formal proofs of the formulas in Example 2.1.3.

2.5. Show that intuitionistic propositional logic is *consistent*, that is $\nvdash \bot$. (Note that consistency is equivalent to "There exists φ with $\nvdash \varphi$".)

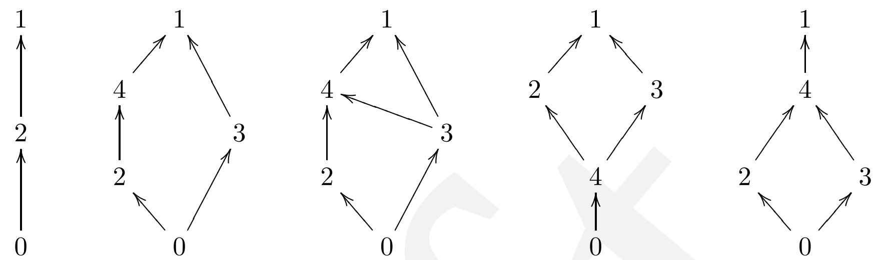
2.6. Let $\langle A, \sqcup, \sqcap \rangle$ be an algebra with two binary operations (written in infix notation). Assume that the equations (i)–(iv) of Lemma 2.3.4 hold for all elements of A. Define $a \leq b$ by $a \sqcup b = b$. Prove that $\langle A, \leq \rangle$ is a lattice, where suprema and infima are given by $\sqcup$ and $\sqcap$.

2.7. Show that the family of all convex subsets of a plane is a lattice but not a distributive one.

2.8. Let A be a lattice satisfying $(a \sqcup b) \sqcap c \leq (a \sqcap c) \sqcup (b \sqcap c)$, for all a, b, c. Show that A is distributive.

2.9. Assume that $a \Rightarrow b$ exists for all elements a, b of a lattice L. Prove that L is distributive. *Hint:* Use Exercise 2.8.

2.10. Consider the partial orders represented below as directed graphs where an edge from a to b means that $a < b$ (edges implied by transitivity not shown). Which of these are lattices? Heyting algebras? Boolean algebras?



(a) (b) (c) (d) (e)

2.11. For $\Gamma \subseteq \Delta$ show that the set $F_\Delta = \{[\varphi]_\sim \mid \Delta \vdash \varphi\}$ is a filter in the Lindenbaum algebra $\mathcal{L}_\Gamma$.

2.12. Let F be a filter in a Heyting algebra $\mathcal{H}$ and let v be a valuation in $\mathcal{H}$. Define $\Gamma = \{\varphi \mid [\![\varphi]\!]_v \in F\}$. Show that Γ is closed under $\vdash$, i.e. $\Gamma \vdash \varphi$ implies $\varphi \in \Gamma$.

2.13. Assume that $\mathcal{B}, v \not\models \varphi$, for some Boolean algebra $\mathcal{B}$ and some φ and v. Show that there exists a prime filter F in $\mathcal{B}$, with $[\![\neg\varphi]\!]_v \in F$. Then define a binary valuation by $w(p) = 1$ iff $v(p) \in F$ and show that $[\![\varphi]\!]_w = 0$.

2.14. Let $\mathcal{B}_0$ be a Boolean algebra with $0 \neq 1$, and let $\mathbb{B}$ be the two-element Boolean algebra of truth values. Show that the following three conditions are equivalent:

(i) $\mathbb{B} \models \varphi$;

(ii) $\mathcal{B}_0 \models \varphi$;

(iii) $\mathcal{B} \models \varphi$, for all Boolean algebras $\mathcal{B}$.

Do not use Stone's Theorem 2.3.9. *Hint:* Apply Exercise 2.13 to prove (i)$\Rightarrow$(iii).

2.15. For a Boolean algebra $\mathcal{B}$, let $\mathcal{Z}$ be the set of all prime filters in $\mathcal{B}$. Show that $\mathcal{B}$ is isomorphic to a subalgebra of $\mathcal{P}(\mathcal{Z})$, consisting of all sets of the form $Z_a = \{F \in \mathcal{Z} \mid a \in F\}$, for $a \in \mathcal{B}$.

2.16. Prove Proposition 2.4.8 (topological spaces regarded as Heyting algebras).

2.17. Prove that if $\not\Vdash \varphi$ then $\mathcal{C} \not\Vdash \varphi$ for a finite Kripke model $\mathcal{C}$. *Hint:* Turn an infinite counterexample into a finite one using a quotient construction.

2.18. Show that the formulas in Example 2.1.4 are not intuitionistically valid. (Use open subsets of $\mathbb{R}^2$ or construct Kripke models.)

2.19. Show that the formula $\bigvee\{p_i \leftrightarrow p_j \mid i, j = 0, \ldots, n \text{ and } i \neq j\}$ is not intuitionistically valid.

2.20. Which of the following judgements are provable?

(i) $p \to \neg p \vdash \neg p$;

(ii) $\neg p \to p \vdash p$;

(iii) $\neg p \to \neg q, p \to \neg q \vdash \neg q$.

(iv) $\neg p \to q, p \to q \vdash q$.

2.21. Which of the following formulas are intuitionistically valid?

(i) $((p \to q) \to p) \to \neg\neg p$;

(ii) $((((p \to q) \to p) \to p) \to q) \to q$;

(iii) $\neg p \vee \neg\neg p$;

(iv) $\neg p \vee \neg q \to \neg(p \wedge q)$;

(v) $(p \to p \wedge q) \vee (q \to p \wedge q)$;

(vi) $(p \to q \vee r) \to (p \to q) \vee r$;

(vii) $(p \to q \vee r) \to (p \to q) \vee (p \to r)$;

(viii) $((p \vee \neg p) \to \neg q) \to \neg q$;

(ix) $(p \to \neg p) \to \neg(\neg p \to p)$;

2.22. Which of the following equivalences are correct intuitionistically?

(i) $p \vee q \leftrightarrow (\neg p \to q)$;

(ii) $p \wedge q \leftrightarrow \neg(p \to \neg q)$;

(iii) $p \wedge q \leftrightarrow (p \leftrightarrow (p \to q))$;

(iv) $(p \to q) \leftrightarrow ((p \vee q) \leftrightarrow q)$.

2.23. Which of the following are intuitionistic tautologies?

(i) $\neg\neg(\varphi \to \psi) \to (\neg\neg\varphi \to \neg\neg\psi)$.

(ii) $\neg\neg(\varphi \wedge \psi) \to (\neg\neg\varphi \wedge \neg\neg\psi)$.

(iii) $\neg\neg(\varphi \vee \psi) \to (\neg\neg\varphi \vee \neg\neg\psi)$.

(iv) $(\neg\neg\varphi \to \neg\neg\psi) \to \neg\neg(\varphi \to \psi)$.

(v) $(\neg\neg\varphi \wedge \neg\neg\psi) \to \neg\neg(\varphi \wedge \psi)$.

(vi) $(\neg\neg\varphi \vee \neg\neg\psi) \to \neg\neg(\varphi \vee \psi)$.

2.24. Show that the following formulas are intuitionistic tautologies:

(i) $\neg\neg(\neg\neg\varphi \to \neg\neg\psi) \to \neg\neg\varphi \to \neg\neg\psi$;

(ii) $(\varphi \to \neg\psi) \to \neg\neg\varphi \to \neg\psi$.

2.25. A propositional formula is *negative* iff every propositional variable p occurs only in the form $p \to \bot$ in φ, and φ contains no occurrence of $\vee$. Show that $\neg\neg\varphi \to \varphi$ is intuitionistically valid for negative φ. *Hint:* Use Exercise 2.23.

2.26. In classical logic some propositional connectives are *definable* from the others. For instance, we say that $\vee$ is definable from $\to$ and $\bot$, because $\alpha \vee \beta$ is equivalent to $(\alpha \to \bot) \to \beta$. Show that none of the connectives $\vee$, $\wedge$, $\to$, $\bot$ is definable from the others in propositional intuitionistic logic.

2.27. Show that $\vee$, $\wedge$, $\to$ and $\bot$ are definable from the ternary connective given by the following *Kuznetsov formula* [291]:

$$((p \vee q) \wedge \neg r) \vee (\neg p \wedge (q \leftrightarrow r)).$$

2.28. In the proof of Lemma 2.5.8 we have shown how to translate every Heyting algebra into a Kripke model. A translation in the other direction is also possible. Let $\mathcal{C} = \langle C, \leq, \Vdash \rangle$ be a Kripke model and let H be the set of all upward-closed subsets of C. Show that H is a Heyting algebra with

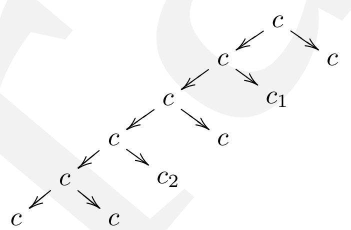
$$X \Rightarrow Y = \{c \mid \forall c' \in X(c \leq c' \to c' \in Y)\}.$$

Then prove that $\mathcal{C} \Vdash \varphi$ implies $H, v \models \varphi$, where $v(p) = \{c \in C \mid c \Vdash p\}$, for $p \in \mathrm{PV}$. *Hint:* Show that $[\![\varphi]\!]_v = \{c \in C \mid c \Vdash \varphi\}$ for all formulas φ.

2.29. In this exercise we fix a finite Kripke model $\mathcal{C} = \langle C, \leq, \Vdash \rangle$, with a least element c_0, and we define a certain function $\pi : (0,1) \to C$. First we associate a "label" $\ell(w) \in C$ to every word $w \in \{0,1\}^*$. We begin with $\ell(\varepsilon) = c_0$ and proceed by induction. Assume that $\ell(w) = c$ and that $\ell(w')$ has not yet been defined for any word w' extending w. Let c have m immediate successors in C, say $c_1, \ldots, c_m$. Then we extend the labeling by:

$$\begin{array}{lcll} \ell(w0^{2i}1) & = & c, & \text{for } i = 0, \ldots, m; \\ \ell(w0^{2i-1}1) & = & c_i, & \text{for } i = 1, \ldots, m; \\ \ell(w0^{i}) & = & c, & \text{for } i = 1, \ldots, 2m+1. \end{array}$$

This definition is illustrated, for $m = 2$, by the figure below.



If a number $x \in (0,1)$ is written in binary as $x = 0.b_1b_2 \ldots b_n1$, or equivalently as $x = 0.b_1b_2 \ldots b_n100\ldots$ with an infinite sequence of zeros (we do not allow infinite sequences of 1's), then define $\pi(x) = \ell(b_1b_2 \ldots b_n)$. Note that $\pi(x) \leq \ell(b_1b_2 \ldots b_n1)$, and that the inequality may happen to be strict. Now assume that x has an infinite binary representation $x = 0.b_1b_2b_3\ldots$ Since the model is finite, there is $c \in C$ such that $\ell(b_1b_2 \ldots b_n) = c$, for almost all n. In this case we take $\pi(x) = c$. Prove that π is a surjective map such that

1. If $X \subseteq C$ is upward-closed then $\pi^{-1}(X)$ is open.
2. If $A \subseteq (0,1)$ is open then $\pi(A)$ is upward-closed;

Hint: First prove the following statements:[7]

[7]Note that ε_x in (i) depends on x, and that y may require an ε_y different than ε_x.

(i) $\forall x \in (0,1)\, \exists \varepsilon_x > 0\, \forall y \in (0,1)[|x-y| < \varepsilon_x \to \pi(x) \le \pi(y)]$;

(ii) $\forall x \in (0,1)\, \forall c \in C\, \forall \varepsilon > 0\, [\pi(x) \le c \to \exists y \in (0,1)[|x-y| < \varepsilon \wedge \pi(y) = c]]$.

2.30. Let $\mathcal{C}$ and $\pi : (0,1) \to \mathcal{C}$ be as in Exercise 2.29. Define a valuation v in the algebra $\mathcal{O}((0,1))$ by $v(p) = \pi^{-1}(\{c \in C \mid c \Vdash p\})$. (Observe that $v(p)$ is open by Exercise 2.29.) Prove that $[\![\varphi]\!]_v = \pi^{-1}(\{c \in C \mid c \Vdash \varphi\})$ holds for all φ.

2.31. Derive Theorem 2.4.11 (completeness for $\mathbb{R}$ etc.) from Exercises 2.17 and 2.30.

2.32. A state c in a Kripke model $\mathcal{C}$ *determines* p iff either $c \Vdash p$ or $c \Vdash \neg p$. Define a binary valuation v_c by $v_c(p) = 1$ iff $c \Vdash p$. Show that if c determines all propositional variables in φ then $[\![\varphi]\!]_{v_c} = 1$ implies $c \Vdash \varphi$. Conclude that a formula is a classical tautology if and only if it is forced in all one-element models.

2.33. Let φ be a classical tautology such that all propositional variables in φ are among $p_1, \ldots, p_n$. Show that the formula $(p_1 \vee \neg p_1) \to \cdots \to (p_n \vee \neg p_n) \to \varphi$ is intuitionistically valid. *Hint:* Use Exercise 2.32.

2.34. Prove Glivenko's Theorem 2.4.10: A double negation of a classical tautology is intuitionistically valid. *Hint:* Use Exercise 2.32.