Stone and Heyting duality for classical and intuitionistic propositional logic

Author:
Laura van Schijndel

Supervisor:
Prof. dr. N. P. Landsman

Bachelor thesis
FNWI
Radboud University
August 2017

Abstract

This thesis proves M. H. Stone's representation theorem for Boolean algebras and Stone spaces and L. Esakia's generalisation to Heyting algebras and spaces. It presents, to my knowledge, the first self-contained overview of the necessary theory explained at the level of a bachelor student. The material of this thesis is mainly based on the books by S. Givant and P. Halmos, and B. A. Davey and H. A. Priestley, and on notes by P. J. Morandi.

Contents

1 Introduction

When I was younger, I was one of those children that never stopped asking why. I also loved looking for patterns. A few of the questions that I asked myself over and over were: Why is $1 + 1 = 2$? Why are $+$ and - opposites, and $\times$ and $\div$? Are there other such opposites?

Through my study of mathematics, at school and at university, I gradually received answers to many of these questions. Yet, I wanted to dig deeper. The answers to my questions were proven using the reasoning of (classical) logic, often viewed as the foundation of mathematics. Hence, I caught myself wondering: why does logic work the way it does? What changes in mathematics if we change the logical axioms?

Thus, when I learned of the existence of different types of logic, my interest was sparked. For this thesis, I focused on the two types that were most well-known to me: classical and intuitionistic logic. To keep it manageable, I restricted myself to propositional logic.

This thesis studies Stone's representation theorem, an essential building block in the algebraic approach to studying classical propositional logic. The obvious question to ask was: is there an analogue of this theorem for intuitionistic propositional logic? There proves to be one, however, it is usually presented using concepts which are not introduced yet at the bachelor level. Therefore, this thesis aims to write a comprehensive overview of the material needed to understand these theorems, using only material understandable for a bachelor student.

This thesis begins with an introduction in lattice theory. The development of this theory ultimately begins with the development of Boolean algebras, about which more will follow below. Another important step in the discovery of lattice theory was the work of R. Dedekind in the second half of the 19th century. He effectively studied lattices applied to number theory, calling them dual groups. The time was not yet ripe, however, for the connection between these ideas formed by lattice theory.

At the end of the 1920s, the study of lattice theory started in earnest. One of the first who studied lattices was K. Menger, who presented a set of axioms for projective geometries which were in essence complemented modular lattices. (Modular lattices will not be presented in this thesis. For more information about modular lattices, see [1].) Other areas where lattices appeared were formal logic, in the work of F. Klein, and algebra, in the work of R. Remak and O. Ore.

The work of G. Birkhoff was of the utmost importance in the early development of lattice theory: he united the applications, approaching lattices from the side of algebra. He independently rediscovered Dedekind's results: it only became known after publication that his approach matched the study of dual groups. He also coined the English term lattice. The German term Verband had been coined before by Klein.

In these early years, there were great hopes for lattice theory as a universal algebra. As lattice theory became an accomplished part of modern algebra in the 1940s, this optimism died out. Although lattice theory has become an important part of algebra, it has not overtaken group theory in its importance. Birkhoff, amongst others, originally expected this to happen. Yet, lattice theory has steadily developed further every decade of the 20th century since its birth.

One class of lattices which plays an important role in this thesis are the Boolean algebras mentioned earlier. These will appear in our dealings with classical propositional logic. We will now look at its history in more detail.

The discipline of Boolean algebras was founded by G. Boole in 1847. He wished to analyse logic using mathematical means, and created Boolean algebras as a calculus or arithmetic suitable for this goal. However, their form was still very different from the one we know today.

Between 1864 and 1895, W. S. Jevons, A. De Morgan, C. S. Peirce, and E. Schröder created the modern version. Peirce improved Boole's axiomatisation, and Schröder showed the independency of the distributive law from the other axioms. However, Boolean algebras were still only a set of tools to analyse logic.

The first step in transforming Boolean algebra into an abstract algebraic discipline, was made by E. Huntington in 1904. This transformation was completed in the 1930s by M. H. Stone and A. Tarski.

The most fundamental result about Boolean algebras is Stone's representation theorem, which Stone proved in 1936. To understand the effect of this theorem, accept for now that every Boolean algebra can be transformed into a specific topological space, its dual, and vice versa. Now imagine taking the dual of an algebra, then of the resulting topological space, then of the resulting algebra, and so on, infinitely many times. Stone's representation theorem states that we will end up switching between a single algebra and a single topological space: all others are isomorphic incarnations of either one.

Stone's representation theorem can be applied to classical propositional logic to show that the Lindenbaum algebra of a set of propositions is isomorphic to the clopen subsets of the set of its valuations: a proposition can be identified with those truth functions that render it true.

In this thesis, we will be concerned with two different types of propositional logic. Classical propositional logic relies on the assumption that every proposition has a predetermined truth value: it is either true or false, regardless of whether it has already been proven. Intuitionistic propositional logic is concerned with whether a proposition has been proven or disproven at this moment, or is still an open problem.

The history of intuitionistic propositional logic begins with the intuitionistic philosophy of L.E.J. Brouwer (1881–1966), which he introduced in his dissertation of 1907. For Brouwer, to do mathematics is to make mental constructions. These can be mathematical objects, or proofs.

In his vision, whilst language is a useful tool to remember and communicate ideas, doing mathematics is not dependent on language. Therefore, axioms may describe a mathematical object, but one cannot conclude that a mathematical object exists by simply stating the axioms it satisfies.

Moreover, Brouwer views logic as the application of mathematics to the language of mathematics. He assumes mathematics to be independent of language, and therefore formalisation. In his view, logic cannot dictate mathematical reasoning, only describe it. This makes logic a part of mathematics instead of its foundation.

A year later, Brouwer stated one important aspect of intuitionism that he neglected in his dissertation: that the *law of the excluded middle*, $p \vee \neg p$, is not valid in intuitionism.

Over the years, Brouwer reproved many classical mathematical results using intuitionism, yet he never formalised intuitionistic logic. Although this may seem contradictory, remember that to an intuitionist, logic is not necessary to do mathematics. Indeed, it is impossible to capture all intuitionistically valid reasoning in a single set of axioms.

Nonetheless, parts of intuitionistic thinking can be formalised, and this was done between 1925 and 1930, mainly by A. Kolmogorov, A. Heyting and V. Glivenko.

In his 1925 article, Kolmogorov showed that classical propositional logic is interpretable in an intuitionistically acceptable fragment of it. At the time, his article was unknown outside of the Soviet Union, and therefore did not influence either Heyting's or Glivenko's thinking until after 1930.

Heyting wrote an article in 1928 for a contest of the Dutch Mathematical Society in which he formalised intuitionistic propositional logic, predicate logic, arithmetic, set theory and analysis. He was the only contestant, yet his win was not undeserved: the jury praised his thoroughness and insight. The revised version was published in 1930. It contained the first conception of Heyting algebras, which will be treated in this thesis.

In 1927, Barzin and Errera questioned the validity of intuitionism, arguing that it had 3 truth values and that this implied that it was inconsistent. In 1928, Glivenko foiled this attack by proving that intuitionistic propositional logic is not 3-valued. Four years later, Gödel would prove that there is no natural number n such that intuitionistic propositional logic has n truth values.

In 1929, just before Heyting's revised article was published, Glivenko showed that if p can be proven in classical propositional logic, then $\neg\neg p$ can be proven in intuitionistic propositional logic. Thus classical and intuitionistic propositional logic are equiconsistent, that is, they are as consistent as each other. In addition, if $\neg p$ can be proven in classical propositional logic, it can also be proven in intuitionistic propositional logic.

In 1930, Heyting published three articles, one of which was his revised 1928 submission. In these articles, he set the standard formalisation of intuitionism still used today. Nonetheless, his formalisation of analysis garnered no general interest. This is explained by the fact that it was neither in the intended interpretation, nor when taken formally, a subsystem of classical analysis.

The most important part of the theory still missing was the precise meaning of the connectives, which Heyting and Kolmogorov arrived at in the next few years. Although there were renewed, independent attempts at formalising intuitionism in the 1950s and later, Heyting's formalism remains dominant.

Unfortunately for intuitionists, the formalisation of intuitionism directed attention away from the underlying ideas. Moreover, it gave an incorrect sense of finality: as human thinking develops, it is entirely possible that there will be found extra axioms which fit the intuitionistic view. To reflect this, the formalisation of intuitionism would have to be expanded.

Heyting's formalisation also gave rise to a persistent misunderstanding of intuitionism. It is possible to distill subsystems of the classical counterparts to intuitionistic propositional and predicate logic, arithmetic and set theory. These subsystems only miss the law of the excluded middle or the equivalent *double negation elimination*, $\neg\neg p \to p$. Distilling these subsystems, however, requires disregarding the intended meaning of the intuitionistic axioms.

This led to the misunderstanding that intuitionistic logic, arithmetic and set theory are subsystems of their classical counterparts, whilst in reality the two are founded on very different principles.

To generalise Stone's representation theorem to intuitionistic propositional logic, we need to find the algebraic structure corresponding to the intuitionistic Lindenbaum algebra. We will show that this is a Heyting algebra. L. Esakia proved the generalisation of Stone's representation theorem to Heyting algebras in 1974. We will also see that the intuitionistic Lindenbaum algebra cannot be represented in terms of valuations, in contrast to the classical case.

This thesis will provide a self-contained exposition of Stone's representation theorem and its generalisation to Heyting algebras, and their application to classical and intuitionistic propositional logic, respectively. Although all these results are already mentioned in the literature, they are scattered throughout multiple articles and books. There is no comprehensive overview, let alone one understandable for a bachelor student. This thesis aspires to fill that gap.

We assume knowledge of naive set theory, topology and logic which a third-year bachelor student should possess.

Since this is a literature thesis, this work relies heavily on several sources. This introduction uses material from [2, 3, 4]. I have adapted Sections 2 to 6 from [1]. In addition, Section 3 contains material from [3]. Section 7 is based on both [1] and [3]. I have adapted Section 8 from [5]. In addition, it contains material from [1, 6]. Section 9 is adapted from [1], and also contains material from [3]. Sections 10 to 12 are adapted from [5]. In addition, Sections 10 and 11 contain material from [3]. Section 13 is based on [7, 8, 2, 9], and Section 14 is based on [1, 8, 9, 10] and personal communications with N. Bezhanishvili.

2 Ordered sets

In this thesis, we will use ordered sets regularly. Therefore, we start out with some definitions and results about ordered sets. The natural numbers begin with 0 in this thesis.

2.1 Definition. An **ordered set**, also called a **partially ordered set** or **poset**, $\langle P, \leq \rangle$, is a set P with a reflexive, antisymmetric and transitive relation $\leq$. Usually, we denote $\langle P, \leq \rangle$ by its set, and only use the full notation when it is unclear what is the order relation on P.

Let P be an ordered set with $x, y \in P$. If $x \leq y$, we say that x **is less than** y or y **is greater than** x. If $x \not\leq y$, then x and y are **incomparable**. P is a **chain**, also called a **linearly ordered set** or **totally ordered set**, if, for all $x, y \in P$, either $x \leq y$ or $y \leq x$.

Several examples of chains are $\mathbb{N}, \mathbb{Z}, \mathbb{Q},$ and $\mathbb{R}$ with the usual order. A poset which is not a chain is the power set of $\{0, 1\}$, ordered by inclusion: the elements $\{0\}$ and $\{1\}$ are incomparable. Throughout the text, subsets of $\mathcal{P}(X)$ will be used often as an example. They are ordered by inclusion, unless stated otherwise.

For every ordered set $\langle P, \leq \rangle$, its **dual** is $\langle P, \geq \rangle$, where $x \leq y$ in $\langle P, \leq \rangle$ if and only if $y \leq x$ in $\langle P, \geq \rangle$. Because of this, every statement about $\langle P, \leq \rangle$ can be translated into a statement about its dual. We can use this duality to reduce work in proofs.

In the next definition, we give more basic definitions of elements of an ordered set. Note the duality present in the definitions.

2.2 Definition. Let P be an ordered set, and $x \in P$. If $y \leq x$ for all $y \in P$, then x is the **top element** or **greatest element** of P. Dually, if $x \leq y$ for all $y \in P$, then x is the **bottom element** or **least element** of P. We may denote the top element of P by $\top$, and the bottom element of P by $\bot$.

Let $Q \subseteq P$. An **upper bound** of Q is an $x \in P$ with $y \leq x$ for all $y \in Q$. If the set of upper bounds of Q has a least element, then this is the **least upper bound** or **supremum**. We denote this as $\sup Q$. Dually, a **lower bound** of Q is an $x \in P$ with $x \leq y$ for all $y \in Q$. If the set of lower bounds of Q has a greatest element, then this is the **greatest lower bound** or **infimum**.

A **maximal element** is an $x \in Q$ for which $y \in Q$ and $x \leq y$ imply $x = y$. If Q has a top element (with the order inherited from P), then this top element is the **maximum element** of Q. Dually, a **minimal element** is an $a \in Q$ for which $x \in Q$ and $a \geq x$ imply $a = x$. If Q has a bottom element (with the order inherited from P), then this bottom element is the **minimum element** of Q.

The next lemma is equivalent to the Axiom of Choice. We will use it without proof.

2.3 Lemma (Zorn's lemma)**.** *Let P be a non-empty ordered set in which every non-empty chain has an upper bound. Then P has a maximal element.*

The ascending and descending chain conditions defined below are useful aids for proving several results throughout this thesis.

2.4 Definition. Let P be an ordered set, and let $\{a_n\}_{n\in\mathbb{N}}$ be a sequence of elements of P, where $a_n \leq a_{n+1}$ for every $n \in \mathbb{N}$. P satisfies the **ascending chain condition** (ACC) if there exists an $k \in \mathbb{N}$ such that $a_k = a_{k+i}$ for every $i \in \mathbb{N}$.

Dually, let $\{a_n\}_{n\in\mathbb{N}}$ be a sequence of elements of P, where $a_n \geq a_{n+1}$ for every $n \in \mathbb{N}$. P satisfies the **descending chain condition** (DCC) if there exists an $k \in \mathbb{N}$ such that $a_k = a_{k+i}$ for every $i \in \mathbb{N}$.

Our first result about the ascending chain condition is a useful auxiliary lemma, which will be used later.

2.5 Lemma. *An ordered set P satisfies ACC if and only if every non-empty subset Q of P has a maximal element.*

Proof. Let P be an ordered set. We will prove the contrapositive of both implications. For the first implication, let $\{x_n\}_{n\in\mathbb{N}}$, with $x_i < x_j$ if $i < j$, be an infinitely ascending chain in P. Then $Q = \{x_n : n \in \mathbb{N}\}$ is a non-empty subset of P without a maximal element.

For the other implication, assume Q is a non-empty subset of P without a maximal element. The contrapositive of Zorn's lemma now states that there is a non-empty chain C in Q with no upper bound. Therefore, we can construct a sequence $\{x_n\}_{n\in\mathbb{N}}$, with $x_i < x_j$ if $i < j$, as follows: first let x_0 be an element of C. Now, given x_i, choose x_{i+1} such that $x_i < x_{i+1}$. We see that $\{x_n\}_{n\in\mathbb{N}}$ is a sequence in $C \subseteq Q \subseteq P$. Thus, P does not satisfy ACC. □

Now that we have seen some basic results about posets, the next step is to define structure-preserving maps of posets.

2.6 Definition. Let $f : P \to Q$ be a map between ordered sets.

f **is order-preserving** or **monotone** if $x \leq y$ in P implies $f(x) \leq f(y)$ in Q.

f **is an order-embedding** if $x \leq y$ in P if and only if $f(x) \leq f(y)$ in Q.

f **is an order-isomorphism** if f is a surjective order-embedding.

The difference between an order-preserving map and an order-embedding can form a pitfall for the unwary. Therefore, we will give an example of an order-preserving map which is not an order-embedding. Order $P = \{\varnothing, \{1\}, \{2\}, \{1, 2\}, \{1, 2, 3\}\}$ by inclusion and order $Q = \{0, 1, 2\}$ by the standard order. Let $f : P \to Q$ send $\varnothing$ and $\{1\}$ to 0, and all other elements of P to 2. Then $f(\{1\}) \leq f(\{2\})$, but $\{1\}$ is incomparable to $\{2\}$.

If f is an order-embedding, it is injective. To see this, take $x, y \in P$ with $f(x) = f(y)$. Then both $f(x) \leq f(y)$ and $f(y) \leq f(x)$. Because f is an order-embedding, these are equivalent with $x \leq y$ and $y \leq x$, respectively. Thus, $x = y$.

Next, we will define some of the most important concepts about posets in this thesis.

2.7 Definition. Given an ordered set P, a subset Q of P is a **down-set** (also called **decreasing set** or **order ideal**) if $x \in Q$ implies $y \in Q$ for all $y \in P$ for which $y \leq x$. Dually, a subset R of P is an **up-set** (also called **increasing set**, or **order filter**) if $x \in R$ implies $y \in R$ for all $y \in P$ for which $x \leq y$.

Next, let S be an arbitrary subset of P. We define the **down-set generated by** S as $\downarrow S := \{x \in P : x \leq y \text{ for a } y \in S\}$, and the **up-set generated by** S as $\uparrow S := \{x \in P : y \leq x \text{ for a } y \in S\}$, respectively.

Let $x \in P$. We define the **down-set generated by** x as $\downarrow x := \{y \in P : y \leq x\}$, and the **up-set generated by** b as $\uparrow x := \{y \in P : x \leq y\}$. Down-sets and up-sets of the form $\downarrow b$ and $\uparrow b$ are called **principal**.

Note that the term order ideal is misleading: an order ideal is defined differently than a ring ideal, or, as we will see later, a lattice ideal. The latter two are both closed under an operation. An order ideal, however, is not defined by any operation.

As we would expect, the operation of taking the down-set of an element preserves order.

2.8 Lemma. *Let P be an ordered set and $x, y \in P$. Then $x \leq y$ if and only if $\downarrow x \subseteq \downarrow y$.*

Proof. First, assume $x \leq y$ and let z be an element of $\downarrow x$. Then $z \leq x$. By transitivity, we have $z \leq y$, which gives $z \in \downarrow y$.

Now, assume $\downarrow x$ to be a subset of $\downarrow y$. By reflexivity, x is an element of $\downarrow x$, so $x \in \downarrow y$. Therefore, $x \leq y$. □

3 Lattices

We can define lattices in two equivalent ways: as ordered sets and as algebraic structures. We will start by taking the algebraic viewpoint.

3.1 Lattices as algebraic structures

In set theory, every set X has the power set $\mathcal{P}(X)$ with the operations of union and intersection. In propositional logic, a formal language has a set of propositions p_i which can be manipulated by logical operations, such as logical or ($\vee$) and logical and ($\wedge$). Some of these are essentially the same, as they are simultaneously true or simultaneously false. We call these logically equivalent. The equivalence classes of these propositions with $\vee$ and $\wedge$ form a structure that resembles a power set.

The generalisation of these examples leads us to the algebraic structure called a lattice. The operations of union and logical or are generalised to join, and those of intersection and logical and are generalised to meet.

3.1 Definition. A **lattice** $\langle L; \vee, \wedge \rangle$ is a non-empty set L with two binary operations **join** $\vee$ and **meet** $\wedge$ that satisfy the following axioms for all $a, b, c \in L$:

(Ass)	$(a \vee b) \vee c$	$= a \vee (b \vee c)$	$(a \wedge b) \wedge c$	$= a \wedge (b \wedge c)$
$(Comm)$	$a \vee b$	$= b \vee a$	$a \wedge b$	$= b \wedge a$
$(Idem)$	$a \vee a$	$= a$	$a \wedge a$	$= a$
(Abs)	$a \vee (a \wedge b)$	$= a$	$a \wedge (a \vee b)$	$= a$

We call (Ass) the **associative laws**, (Comm) the **commutative laws**, (Idem) the **idempotency laws**, and (Abs) the **absorption laws**. Note that each of the idempotency laws can be deduced from both absorption laws together. However, it is standard to state these laws as axioms.

We define an **order relation** $\preccurlyeq$ on L by $a \preccurlyeq b$ if $a \vee b = b$, or equivalently $a \wedge b = a$. This last equivalence relation is easily seen by using the absorption axiom. We see that $\preccurlyeq$ is an order relation because it is reflexive (use (Idem)), transitive (use (Ass)) and antisymmetric (use (Comm)). We will call this the **algebraic definition of order** on a lattice.

Note that in each case, the right equations of the axioms are the same as the left equations, only with $\vee$ and $\wedge$ reversed. We also say that the right equations are **dual to** the left equations. To get the dual of an expression, we should also invert 0 and 1. Since the axioms of lattices (and as we see later, bounded and distributive lattices) come in dual pairs, so do the theorems that follow from them. Therefore, we only need to prove half of those: the other half can be proven by a dual proof. We will make use of that fact quite often.

For counterexamples, we will look at the subsets of the lattice $L = \{\varnothing, x, y, \{x, y\}\}$ with union as join and intersection as meet. Examine the set $A = \{\varnothing, x, y\}$. Then A is not a lattice, because $x \vee y$ does not exist in A. Dually, $B = \{x, y, \{x, y\}\}$ with the same meet and join is not a lattice, because $x \wedge y$ does not exist in B.

We will now examine another example of a lattice. Let X be a set, and let Y be the set of finite subsets of X. If X is finite, then Y is the power set of X and thus a lattice. If X is infinite, then Y still satisfies all axioms. However, there is no single greatest element of Y, like X would be if X was finite. There is still a least element of Y in both cases, namely the empty set. This difference in structure leads us to the next definition.

3.2 Definition. Let L be a lattice. A **bounded lattice** is a lattice L with a **zero** element $0 \in L$ such that $a = a \vee 0$ for all $a \in L$, and a **one** (or **unit**) element $1 \in L$ such that $a = a \wedge 1$ for all $a \in L$.

So, in our last example Y is bounded if and only if X is finite. The power set of an arbitrary set X also forms a bounded lattice, as well as the set of propositions with the operations of logical or and logical and. In this case, the zero element is the equivalence class of always false propositions, and the unit element is the equivalence class of always true propositions. We will further examine this in our chapters on logic.

3.2 Lattices as ordered sets

As we saw, the duality of the lattice axioms makes the algebraic approach an attractive one. There are, however, also advantages to a different approach. If we define lattices as ordered sets, we can use our knowledge of upper and lower bounds to prove many results. The ordering relation can also serve to gain a geometric understanding of the lattice structure.

3.3 Definition. A **lattice** $\langle L; \leq \rangle$ is a non-empty set L with an order relation imposed, such that for all $a, b \in L$, the least upper bound $\sup(\{a, b\})$ and greatest lower bound $\inf(\{a, b\})$ exist. We define **a join b**, $a \vee b := \sup(\{a, b\})$ and **a meet b**, $a \wedge b := \inf(\{a, b\})$.

Our modified examples of lattices are now the power set $\mathcal{P}(X)$, ordered by inclusion, and the set of logically equivalent propositions, where $p \leq q$ if $p \to q$.

The order relation induces a few other examples of lattices. For example, every totally ordered set is a lattice. Thus, $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ are all lattices when ordered with the standard order. Also, every closed interval $[a, b] \subseteq \mathbb{R}$ with the standard order is a lattice.

We can once again define a bounded lattice. Let us take a look at Definition 3.2, and apply our new definitions of join and meet to them. We find that for all elements a of the lattice, we should have $\inf\{a, 1\} = a = \sup\{a, 0\}$. To accomplish that, we should have $0 \leq a \leq 1$ for all elements a of the lattice. To emphasise that these constants are defined differently than before, they have a different name and notation.

3.4 Definition. A **bounded lattice** is a lattice L with a **top** element $\top$ such that for all $a \in L$ we have $a \leq \top$ and a **bottom** element $\bot$ such that for all $a \in L$ we have $\bot \leq a$.

In this case, the **dual** of a lattice $\langle L; \leq \rangle$ is the lattice $\langle L; \geq \rangle$ where $a \geq b$ if and only if $b \leq a$. Again, we can use this duality to avoid unnecessary work. Observe that the term duality has several different meanings featuring in this thesis. The context will clarify which one we are dealing with.

Remark (A note on suprema and infima). Let L be a lattice. If L has a top element $\top$, then this is the only upper bound of L, so $\sup L = \top$. Dually, if L has a bottom element $\bot$, then $\inf L = \bot$. If L has no top element, then it has no upper bounds. Thus, $\sup L$ does not exist. Dually, if L has no bottom element, $\inf L$ does not exist.

Next, observe the empty set. Every element $a \in L$ vacuously satisfies $b \leq a$ for all $b \in \varnothing$. Therefore, every element in L is an upper bound of $\varnothing$, which means that there is a least upper bound of $\varnothing$ if and only if L has a bottom element, and then $\sup \varnothing = \bot$. Dually, $\inf \varnothing = \top$ if L has a top element, and does not exist otherwise.

3.3 Equivalence of lattice definitions

We will denote a lattice L as an algebraic structure by $\langle L; \vee, \wedge \rangle$. If the lattice L is defined as an ordered set, we denote it by $\langle L; \leq \rangle$. Now, we show that both

definitions are equivalent.

3.5 Lemma. *A set L is a lattice $\langle L; \vee, \wedge\rangle$ if and only if it is a lattice $\langle L; \leq\rangle$.*

Proof. Let $\langle L; \vee, \wedge\rangle$ be an algebraically defined lattice. We will show that it is also an ordered set lattice. To do so, we need to show that the order relation $\preccurlyeq$ defined in Definition 3.1 on $\langle L; \vee, \wedge\rangle$ makes $\langle L; \preccurlyeq\rangle$ a lattice. Therefore, we have to show that $\sup\{a, b\} = a \vee b$. The assertion $\inf\{a, b\} = a \wedge b$ will then follow from order duality.

Firstly, we will show that $a \vee b$ is an upper bound of $\{a, b\}$, so $a \preccurlyeq a \vee b$ and $b \preccurlyeq a \vee b$. By definition of $\preccurlyeq$, we have $a \preccurlyeq a \vee b$ if and only if $a \vee (a \vee b) = a \vee b$. We have

$$a \vee (a \vee b) = (a \vee a) \vee b = a \vee b.$$

We used (Ass) in the first equality and (Idem) in the second.

Next, we prove that $a \vee b$ is in fact the least upper bound. Let c be an upper bound for $\{a, b\}$, so $a \preccurlyeq c$ and $b \preccurlyeq c$. We need to show that $a \vee b \preccurlyeq c$. So

$$(a \vee b) \vee c = a \vee (b \vee c) = a \vee c = c.$$

The first equality uses (Ass), the second $b \preccurlyeq c$, and the third uses $a \preccurlyeq c$. Thus, for each upper bound c of a and b, we have $a \vee b \preccurlyeq c$. Therefore, $a \vee b$ is the least upper bound of $\{a, b\}$.

Now let $\langle L; \leq\rangle$ be a lattice. We will show that the join and meet of $\langle L; \leq\rangle$ satisfy the axioms (Ass), (Comm), (Idem) and (Abs) in Definition 3.1. Because of duality, we only need to prove the left equations.

It is clear that the supremum of a set does not depend on the order of the elements. Therefore, the definition of join, $a \vee b = \sup\{a, b\}$, directly implies the commutative law.

To prove the idempotency law, we use the definition of join once again. This shows that $a \vee a = sup\{a, a\}$ is an upper bound of a. Therefore, we have $a \leq a \vee a$. However, reflexivity of $\leq$ shows us that a is also an upper bound of $\{a, a\}$, so $a \vee a \leq a$. Therefore, we have $a = a \vee a$. This proves the idempotency law.

We prove the associative law using an intermediate step: we will prove that $(a \vee b) \vee c = \sup\{a, b, c\}$ and that $a \vee (b \vee c) = \sup\{a, b, c\}$. To do so, we have to show that the set of upper bounds of $\{a \vee b, c\}$ equals the set of upper bounds of $\{a, b, c\}$, and the set of upper bounds of $\{a, b \vee c\}$ also equals the set of upper bounds of $\{a, b, c\}$.

Let d be an upper bound of $\{a, b, c\}$. This is equivalent to stating that d is an upper bound of $\{a, b\}$ and $c \leq d$, which can be rewritten as $a \vee b \leq d$ and $c \leq d$. This is equivalent to stating that d is an upper bound of $\{a \vee b, c\}$. So the upper bounds of $\{a \vee b, c\}$ and $\{a, b, c\}$ are the same.

By an analogous argument we find that the upper bounds of $\{a, b \vee c\}$ and $\{a, b, c\}$ are the same. Therefore, their suprema must also be equal, which gives us

$$(a \vee b) \vee c = \sup\{a \vee b, c\} = \sup\{a, b, c\} = \sup\{a, b \vee c\} = a \vee (b \vee c).$$

This proves (Ass).

To prove (Abs), observe that $a \vee (a \wedge b) = \inf\{a, \sup\{a, b\}\} \leq a$, because of the infimum. Moreover, $a \leq \sup\{a, b\}$ and $a \leq a$, so $a \leq \inf\{a, \sup\{a, b\}\}$. This gives

$$a = \inf\{a, \sup\{a, b\}\} = a \vee (a \wedge b),$$

so we have (Abs). □

As both notions of lattice are equivalent, we will simply denote a lattice by its underlying set, only using the full algebraic or order notations for emphasis.

We will now prove a simple property of join and meet which will be useful for later chapters.

3.6 Lemma. *Let L be a lattice with $a, b, c, d \in L$. If $a \leq c$ and $b \leq d$, then $a \wedge b \leq c \wedge d$ and $a \vee b \leq c \vee d$. These inequalities are called the* ***monotony laws****.*

Proof. We will prove this from an order-theoretic viewpoint.

For the first inequality, recall that $a \wedge b$ is the greatest lower bound of $\{a, b\}$, and $c \wedge d$ is the greatest lower bound of $\{c, d\}$. Since $a \leq c$, we find $a \wedge b \leq c$. As $b \leq d$, we find $a \wedge b \leq d$. Therefore, $a \wedge b$ is a lower bound of $\{c, d\}$, which gives $a \wedge b \leq c \wedge d$.

For the second inequality, an analogous argument shows that $c \vee d$ is an upper bound of $\{a, b\}$, and therefore $a \vee b \leq c \vee d$. □

4 Lattice maps

Now that we have explored some of the different types of lattice, it is high time to examine the different structure-preserving maps for lattices. Most of this should be no surprise.

4.1 Definition. Let $f : L \to K$ be a map between lattices.

f **is a (lattice) homomorphism** if $f(a \vee b) = f(a) \vee f(b)$ and $f(a \wedge b) = f(a) \wedge f(b)$.

f **is an embedding** if f is an injective lattice homomorphism.

f **is a (lattice) isomorphism** if f is a bijective lattice homomorphism.

f **is a $\{0, 1\}$-homomorphism** if L and K are bounded, f is a homomorphism and $f(0) = 0$ and $f(1) = 1$.

In this thesis, from now on, we will understand a (lattice) homomorphism between bounded lattices to be a $\{0, 1\}$-homomorphism. As a lattice is an ordered set, there could be a conflict between the different definitions of isomorphism on lattices. The following lemma shows that all is as it should be.

4.2 Lemma. *Let $f : L \to K$ be a map between lattices.*

1. *If f is an order-embedding, then f is injective.*

2. *Let $a, b \in L$. The following are equivalent:*

   (a) *f is order-preserving;*

   (b) *$f(a) \vee f(b) \leq f(a \vee b)$;*

   (c) *$f(a \wedge b) \leq f(a) \wedge f(b)$.*

   In particular, if f is a homomorphism, then f is order-preserving.

3. *f is a lattice isomorphism if and only if it is an order-isomorphism.*

Proof. For the first statement, let $f : L \to K$ be an order-embedding, and let $a, b \in L$ with $f(a) = f(b)$. We can rewrite this as $f(a) \leq f(b) \text{and} f(b) \leq f(a)$. Because f is an order-embedding, this is equivalent to $a \leq b$ and $b \leq a$, which we can rewrite as $a = b$. So f is injective.

Now, let $a, b \in L$. We will prove the equivalence of (a) and (b), from which the equivalence of (a) and (c) will automatically follow.

We start by proving that (a) implies (b). Let $a \leq b$. We know that $a \leq a \vee b$. This implies $f(a) \leq f(a \vee b)$, because f is order-preserving. We also know that $b \leq a \vee b$, which again implies $f(b) \leq f(a \vee b)$, because f is order-preserving. Therefore, $f(a \vee b)$ is an upper bound of $\{f(a), f(b)\}$, which gives $f(a) \vee f(b) \leq f(a \vee b)$.

To prove the reverse implication, let $a, b \in L$ with $a \leq b$. The algebraic definition of order dictates that $a \vee b = b$. We use our assumption of (b) to find $f(b) = f(a \vee b) \geq f(a) \vee f(b)$. This gives $f(b) = f(a) \vee f(b)$. Again using the algebraic definition of order, we find $f(a) \leq f(b)$. □

5 Complete lattices

We saw before that both $\mathbb{Q}$ and the closed interval $[a, b]$ with $a, b \in \mathbb{R}$ are lattices, when equipped with the standard order. There is, however, a major difference in their structure.

For $[a, b]$ not only the supremum of every two-element set, but the supremum of every set exists in $[a, b]$. In $\mathbb{Q}$, however, it is well known that not all suprema exist: the set $\{q \in \mathbb{Q} : q^2 < 2\}$ has no supremum in $\mathbb{Q}$. Moreover, as $\mathbb{Q}$ lacks a top and bottom, $\mathbb{Q}$ itself and the empty set have no supremum in $\mathbb{Q}$.

To differentiate between lattices like $[a, b]$ and lattices like $\mathbb{Q}$, we have the following definition.

5.1 Definition. Let L be a lattice. L is a **complete lattice** if the **join of S** $\bigvee S := \sup S$ and the **meet of S** $\bigwedge S := \inf S$ exist for all $S \subseteq L$.

Note that although it seems the definition of a complete lattice is dependent on a lattice being an ordered set, the equivalence of lattice definitions means that this definition serves equally well if we regard the lattice as an algebraic structure.

We will now prove some basic properties about joins and meets of subsets. To start with, we show that taking a meet or join of a finite union of sets works as expected.

5.2 Lemma. *Let L be a lattice.*

1. *Let J and K be subsets of L and assume that $\bigvee J$, $\bigvee K$, $\bigwedge J$, and $\bigwedge K$ exist in L. Then*
$$\bigvee (J \cup K) = \left(\bigvee J\right) \vee \left(\bigvee K\right), \text{ and } \bigwedge (J \cup K) = \left(\bigwedge J\right) \vee \left(\bigwedge K\right).$$
2. *For every finite, non-empty subset F of L, $\bigvee F$ and $\bigwedge F$ exist in L.*

Proof. To prove the first part, we only need to prove the left equation. The right equation will then follow by duality. Denote $j = \bigvee J$, $k = \bigvee K$, and $m = \bigvee(J \cup K)$.

Firstly, we show that $j \vee k \leq m$. Because m is an upper bound of $J \cup K$, it is an upper bound of J and of K, so $j \leq m$ and $k \leq m$. Then we see that m is an upper bound of $\{j, k\}$, so $j \vee k = \sup\{j, k\} \leq m$.

Secondly, we show that $m \leq j \vee k$. We know that $j \leq j \vee k$ and $k \leq j \vee k$, so $j \vee k$ is an upper bound of both J and K. This makes it an upper bound of $J \cup K$, so $m = \sup J \cup K \leq j \vee k$. Therefore, we have $m = j \vee k$.

The second statement follows by induction from the first statement and the definition of join and meet. We will not give a detailed proof here. □

The next lemma is an auxiliary lemma; the subsequent lemma establishes equivalent conditions to completeness.

5.3 Lemma. *Let L be a lattice. For every non-empty subset S of L, let $\bigwedge S$ exist in L. Then, for every subset S of L which has an upper bound in L, $\bigvee S$ exists in L. Moreover, $\bigvee S = \bigwedge\{a \in L : a \text{ is an upper bound of } S\}$.*

Proof. Let $S \subseteq L$ and assume that S has an upper bound in L. Then the set of upper bounds of S is a non-empty subset of L. Hence $s = \bigwedge\{a \in L : a \text{ is an upper bound of } S\}$ exists. As it is the infimum of the set of upper bounds of S, it is the least upper bound of S. Therefore, $s = \bigvee S$. □

5.4 Lemma. *Let L be a lattice. Then the following are equivalent:*

1. *L is complete;*
2. *$\bigwedge S$ exists in L for every subset S of L;*
3. *L has a top element $\top$, and $\bigwedge S$ exists in L for every non-empty subset S of L.*

Proof. That the first statement implies the second, follows directly from the definition of completeness.

As the meet of $\varnothing$ exists precisely if L has a top element, the second statement implies the third.

Now assume the third statement. By Lemma 5.3, $\bigvee S$ exists in L for every $S \subseteq L$ with an upper bound in L. But as L has a top element, every subset S of L has an upper bound. Therefore, L is complete. □

The next lemma yields another equivalent condition for completeness. It uses the ascending chain condition (ACC), which we saw before in Definition 2.4.

5.5 Lemma. *Let L be a lattice.*

1. *If L satisfies ACC, then for every non-empty subset A of L there exists a finite subset F of A such that $\bigvee A = \bigvee F$ (the latter exists by Lemma 5.2).*

2. *If L has a bottom element and satisfies ACC, then L is complete.*

Proof. Firstly, we prove the first statement. Let L satisfy ACC, and let A be a non-empty subset of L. Then, by the second statement of Lemma 5.2, $B := \{\bigvee F : F \text{ is a finite non-empty subset of } A\}$ is a well-defined subset of L. Because A is non-empty, $\bigvee A \in B$. Therefore, B is non-empty as well. Thus, by Lemma 2.5, there is a finite subset F of A, for which $m := \bigvee F$ is a maximal element of B.

Let $a \in A$. Then $F \cup \{a\}$ is a subset of A, and therefore $\bigvee(F \cup \{a\}) \in B$. Moreover, $m \leq \bigvee(F \cup \{a\})$. As m is maximal in B, we find $m = \bigvee(F \cup \{a\})$. Therefore, m is an upper bound of a. As a was an arbitrary element of A, m is an upper bound of A.

Now, let $x \in L$ be an upper bound of A. As F is a subset of A, we find that x is an upper bound of F. Therefore, $m \leq x$. Thus, m is the least upper bound of A, so $\bigvee A = m$ and the first statement holds.

For the second statement, let L have a bottom element and satisfy ACC. Because L satisfies ACC, we can apply the first statement. We then find that for every non-empty subset S of L, $\bigvee A$ exists. The dual of Lemma 5.4 tells us that if L has a bottom element, and $\bigvee A$ exists in L for every non-empty subset A of L, then L is complete. Therefore, L must be complete. □

6 Distributive lattices

The distributive law of sets $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and its dual $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ characterise an important property of power sets. This property, generalised to join and meet, can also be found in an important class of lattices. We call these distributive lattices. A full definition is given below.

6.1 Definition. A **distributive lattice** is a lattice L which satisfies the distributive law: For all $a, b, c \in L$, we have $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ and its equivalent dual $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

In a distributive lattice, in a sense, the converse of the monotony laws (see Lemma 3.6) also hold. We call these the **cancellation laws**.

6.2 Lemma. *Let L be a distributive lattice, $a, b, c \in L$ with $a \wedge b = a \wedge c$, and $a \vee b = a \vee c$. Then $b = c$.*

Proof. Using the axioms of a distributive lattice, we find

$$\begin{aligned} b = b \vee (b \wedge a) = b \vee (c \wedge a) = (b \vee c) \wedge (b \vee a) = (b \vee c) \wedge (b \vee a) \wedge (b \vee a) \\ = (b \vee c) \wedge (b \vee a) \wedge (c \vee a) = (c \vee b) \wedge (c \vee a) \wedge (c \vee a) = (c \vee b) \wedge (c \vee a) \\ = c \vee (b \wedge a) = c \vee (c \wedge a) = c. \end{aligned}$$

The first equation uses the absorption law, and the second uses $a \wedge b = a \wedge c$. The third equation uses distributivity, and the fourth the idempotency law. The fifth and sixth equations use $a \vee b = a \vee c$, and the seventh equation uses idempotency. The eighth equation uses distributivity, the ninth $a \wedge b = a \wedge c$, and the tenth uses the absorption law. Commutativity laws are used freely throughout. □

We can use induction to expand the distributive law to finite joins and meets. There are various laws for infinite joins and meets, which only hold for certain complete lattices. We will take a closer look in the next subsection.

6.1 Infinite distributive laws

We will begin with the simplest infinite distributive laws. These have infinite joins or infinite meets, but not both.

6.3 Definition. Let L be a complete lattice, and J be an arbitrary index set. L satisfies the **Join-Infinite Distributive law** (JID) if for any subset $\{b_j\}_{j \in J}$ of L and any $a \in L$, we have

$$a \wedge \bigvee_{j \in J} b_j = \bigvee_{j \in J} a \wedge b_j.$$

L satisfies the **Meet-Infinite Distributive law** (MID) if for any subset $\{b_j\}_{j \in J}$ of L and any $a \in L$, we have

$$a \vee \bigwedge_{j \in J} b_j = \bigwedge_{j \in J} a \vee b_j.$$

Note that whereas for many other laws the dual expressions were equivalent, here this is not the case. The next lemma investigates the conditions in which JID and MID hold in bounded distributive lattices.

6.4 Lemma. *Any bounded distributive lattice which satisfies ACC satisfies JID, and any bounded distributive lattice that satisfies DCC satisfies MID.*

Proof. Let L be a bounded distributive lattice which satisfies ACC. Let $\{b_j\}_{j \in J}$ be a subset of L and $a \in L$. By the first statement of Lemma 5.5 there is a finite subset $\{b_j\}_{j \in F}$ of $\{b_j\}_{j \in J}$ with $\bigvee\{b_j\}_{j \in J} = \bigvee\{b_j\}_{j \in F}$. Therefore

$$a \wedge \bigvee_{j \in J} \{b_j\} = a \wedge \bigvee_{j \in F} \{b_j\} = \bigvee_{j \in F} a \wedge \{b_j\} \leq \bigvee_{j \in J} a \wedge \{b_j\}.$$

The second equality uses the finite distributive law, and the last inequality follows from the fact that F is a subset of J.

As $\{a \vee b_j\}_{j\in J}$ is also a subset of L, there is a finite subset $\{a \vee b_j\}_{j\in G}$ of $\{a \vee b_j\}_{j\in J}$ such that $\bigvee\{a \vee b_j\}_{j\in J} = \bigvee\{a \vee b_j\}_{j\in G}$. Therefore

$$\bigvee_{j\in J} a \wedge b_j = \bigvee_{j\in G} a \wedge b_j = a \wedge \bigvee_{j\in G} b_j \leq a \wedge \bigvee_{j\in J} b_j.$$

Again, the second equality uses the finite distributive law, and the last inequality follows from the fact that F is a subset of J.

These two inequalities give the required equality. The statement about DCC and MID follows by duality.

□

Note that these lattices are automatically complete. To see this, use Lemma 5.5 and its dual.

7 Boolean algebras

Throughout this thesis, we have repeatedly used the example of the power set of X as a motivating example to define a certain structure. We have already generalised the operations of union, intersection and inclusion, but there is another important operation on the power set of X: taking the complement.

In this section, we generalise this operation to lattices. To do so, we require boundedness: we cannot take the complement of a subset of X without using X. Analogously, we cannot take a complement without using the top element, or dually, the bottom element, of a lattice.

7.1 Definition. Let L be a bounded lattice and $a \in L$. Then $b \in L$ is a **complement** of a if $a \wedge b = 0$ and $a \vee b = 1$. If a has a *unique* complement, we denote it by a'.

It is quite easy to think of a lattice L and an element $a \in L$ where a has a non-unique complement. Take the lattice $L = \{0, a, b, c, 1\}$ with $0 \leq a \leq 1$, $0 \leq b \leq 1$, and $0 \leq c \leq 1$. The elements a, b, and c are incomparable. The join of any two of a, b, and c is 1, and their meet is 0. Therefore, both b and c are complements of a.

However, if a lattice is distributive, every element has at most one complement. To see this, let L be a distributive lattice and $b_1, b_2 \in L$ both complements of $a \in L$. Then

$$b_1 = b_1 \wedge 1 = b_1 \wedge (a \vee b_2) = (b_1 \wedge a) \vee (b_1 \wedge b_2) = b_1 \wedge b_2.$$

The algebraic definition of order implies that $b_1 \leq b_2$. An analogous argument gives $b_2 \leq b_1$, so $b_1 = b_2$. Note that a lattice element does not need to have a complement.

We can now define the lattice structure that most resembles a power set, the Boolean lattice.

7.2 Definition. A lattice L is called **Boolean** if L is bounded, distributive and each $a \in L$ has a (unique) complement $a' \in L$.

In the next lemma we will study some basic properties of the complement in a Boolean lattice.

7.3 Lemma (Properties of the complement)**.** *Let L be a Boolean lattice. Then for all $a, b \in L$:*

1. $0' = 1$ *and* $1' = 0$*;*
2. $a'' := (a')' = a$*;*
3. $(a \vee b)' = a' \wedge b'$ *and* $(a \wedge b)' = a' \vee b'$ *(De Morgan's laws);*
4. $a \vee b = (a' \wedge b')'$ *and* $a \wedge b = (a' \vee b')'$*;*
5. $a \wedge b' = 0$ *if and only if* $a \leq b$.

Proof. Because a Boolean lattice is distributive, each element has a unique complement. Therefore, to prove $k = l'$ in L it is sufficient to prove that $p \vee q = 1$ and $p \wedge q = 0$.

Now the proof of the first, second, and third statement is obtained by straightforward manipulation of equations. The fourth statement follows by combining the second and third.

To prove the fifth statement, we see by joining with b on both sides that $a \wedge b' = 0$ if and only if $(a \wedge b') \vee b = 0 \vee b$. Using the distributivity law and the properties of 0, we see that this is equivalent with $(a \vee b) \wedge (b' \vee b) = b$. Next, use the properties of 1 to rewrite this to $(a \vee b) \wedge 1 = b$, and again to $a \vee b = b$. Per definition of order, this is equivalent to $a \leq b$. □

Given a Boolean lattice L, we usually take the view that 0, 1 and $'$ are an integral part of the structure. We call the structure a **Boolean algebra**. We usually denote it by its set.

As we saw, the standard example of a Boolean algebra is the power set of a set S, with union as join, intersection as meet, and set-theoretic complement as complement, $\varnothing$ as 0, and S as 1.

$\{0\}$ is the **trivial** or **degenerate** Boolean algebra. The simplest non-trivial or non-degenerate Boolean algebra is $\mathbf{2} := \{0, 1\}$. It plays a special role in classical propositional logic, as we will see later.

The structure-preserving maps of Boolean algebras are $\{0, 1\}$-homomorphisms: the conservation of $0, 1$, and $\leq$ ensures the conservation of $\vee, \wedge$ and $'$. You can see this easily by regarding join and meet as suprema and infima. The preservation of the complement follows from the preservation of join and meet. We will call these maps **Boolean homomorphisms**.

8 Heyting algebras

To generalise the concept of a Boolean algebra, we need to weaken the concept of complement. One way to do this is by introducing the pseudocomplement. Let L be a lattice with 0, and let $a \in L$. Let $a^* = \max\{b \in L : b \wedge a = 0\}$ be the **pseudocomplement** of a.

The next definition introduces Heyting algebras. Their operation of implication can easily be linked to the concept of pseudocomplement: $a^* = a \to 0$ in a Heyting algebra.

8.1 Definition. A **Heyting lattice** or **Heyting algebra** is a bounded distributive lattice H with a binary operation $\to$, called **implication**, such that $c \leq (a \to b)$ if and only if $(a \wedge c) \leq b$.

To get some feel for Heyting algebras and the operation of implication, below are some examples of Heyting algebras.

- finite distributive lattices;
- Boolean algebras, with $a \to b = a' \vee b$;
- bounded chains, with $a \to b = \begin{cases} 1 & \text{if } a \leq b, \\ b & \text{if } a > b. \end{cases}$

We see from the definition that $a \to b = \bigvee\{c \in H : a \wedge c \leq b\}$. As arbitrary joins of elements need not exist in a lattice, the existence of an implication is not automatic. If H is a lattice in which joins of arbitrary subsets exist, then H is a Heyting algebra if and only if H satisfies JID (see Definition 6.3).

There is also way to define Heyting algebras that relies on equations only. In the next lemma, we show that the two definitions are equivalent.

8.2 Lemma. *Let L be a (distributive) lattice. L is a Heyting algebra if and only if there is a binary operation $\to$ on L such that for every $a, b, c \in L$:*

1. $a \to a = 1$;
2. $a \wedge (a \to b) = a \wedge b$;
3. $b \wedge (a \to b) = b$;
4. $a \to (b \wedge c) = (a \to b) \wedge (a \to c)$.

Proof. Let us assume that L is a Heyting algebra, and let $a, b, c \in L$. We have to prove that axioms *1* to *4* hold.

Firstly, we prove axiom *1*. Let $c \in L$. It is evident that $a \wedge c \leq a$. Per definition of implication, this can be rewritten as $c \leq a \to a$. This is equivalent to $a \to a = 1$. For the other three axioms, we will prove both inequalities to arrive at the equality.

Secondly, let us prove axiom *2*. It is easily seen that $a \wedge b \leq b$. By definition of implication, this is equivalent to $b \leq a \to b$. This implies by monotony (see

Lemma 3.6) that $a \wedge b \leq a \wedge (a \to b)$. For the other inequality, the definition of supremum together with $a \to b = \bigvee\{c \in H : a \wedge c \leq b\}$ gives $a \to b \leq b$. Monotony implies that $a \wedge (a \to b) \leq a \wedge b$.

Thirdly, we prove *3*. It is easily seen that $b \wedge (a \to b) \leq b$. To show that $b \leq b \wedge (a \to b)$, we need to show that b is a lower bound of $\{b, a \to b\}$. It is evident that $b \leq b$. Per definition of implication, $b \leq a \to b$ is equivalent with $a \wedge b \leq b$. This last inequality is certainly true, therefore, $b \leq b \wedge (a \to b)$.

Finally, let us prove axiom *4*. We see that $a \to (b \wedge c) \leq (a \to b) \wedge (a \to c)$ if and only if both $a \to (b \wedge c) \leq (a \to b)$ and $a \to (b \wedge c) \leq (a \to c)$. Both claims are proven analogously; we will prove the first one. By definition of implication, $a \to (b \wedge c) \leq (a \to b)$ if and only if $a \wedge (a \to (b \wedge c)) \leq b$. Using *2*, we can rewrite this last inequality as $a \wedge b \wedge c \leq b$, which is true.

For the reverse inequality, we use the definition of implication to rewrite $(a \to b) \wedge (a \to c) \leq a \to (b \wedge c)$ as

$$a \wedge (a \to b) \wedge (a \to c) \leq b \wedge c,$$

using the definition of implication. By applying *2* twice, we find this to be equivalent to $a \wedge b \wedge (a \to c) \leq b \wedge c$ if and only if $b \wedge a \wedge c \leq b \wedge c$. Thus, we have proven *4*.

Now assume that L is a lattice in which axioms *1* to *4* hold, and let $a, b, c \in L$. To start with, we assume $c \leq a \to b$, and want to prove that $a \wedge c \leq b$. By monotony, $c \leq a \to b$ implies $a \wedge c \leq a \wedge (a \to b) = a \wedge b$. Here, we applied *2* to derive the last equality. It is clear that $a \wedge b \leq b$, therefore, $a \wedge c \leq b$.

For the reverse inequality, assume $a \wedge c \leq b$. We want to prove $c \leq a \to b$. Subsequently apply idempotency, monotony, and *2* on $a \wedge c \leq b$ to get

$$a \wedge c = a \wedge a \wedge c \leq a \wedge b = a \wedge (a \to b).$$

Application of the cancellation laws (see Lemma 6.2) gives us $c \leq a \to b$. □

Note that the lemma does not need to assume distributivity explicitly: any lattice in which these four equalities hold, is automatically distributive. We will not prove this here.

The structure-preserving maps of Heyting algebras are lattice homomorphisms which preserve implication.

9 Sublattices, ideals and filters

In this section, we explore some subsets of lattices which have additional structure. The first subset of this kind is the sublattice.

9.1 Definition. Let L be a lattice, and let A be a non-empty subset of L. Then A is a **sublattice** of L if A is closed under joins and meet. If L has additional structure, e.g. L is bounded, distributive, Boolean or Heyting, then this additional structure should also be preserved in A: it should be closed under any operations, and contain any special elements such as 0 and 1. If L is a Boolean or Heyting algebra, we call A a **subalgebra**.

Note that this definition of sublattice is not standard: the customary definition merely requires closedness under joins and meets. The alternative definition is advantageous because it mirrors the customary definition of a subalgebra by preserving all structural properties.

Some straightforward examples of sublattices are the singletons, and any chain in a lattice (provided that 0 and 1 are included if the lattice is bounded).

A subset of a lattice may be a lattice in its own right without being a sublattice. For example, take the power set of $\{1, 2, 3\}$, ordered by inclusion. The subset $A = \{\varnothing, \{1\}, \{1, 2\}, \{2, 3\}, \{1, 2, 3\}\}$, ordered by inclusion, is a lattice. However, it is not a sublattice of $\mathcal{P}(\{1, 2, 3\})$, because $\{1, 2\} \wedge \{2, 3\} = \varnothing$ in A, but $\{1, 2\} \wedge \{2, 3\} = \{2\}$ in $\mathcal{P}(\{1, 2, 3\})$. In other words, A is not closed under meets, because $\{2\} \notin A$.

An important concept in lattice theory is that of an ideal, and its dual concept of a filter. These subsets of a lattice play a major role in many results, amongst which the representation theorems that are the heart of this thesis.

9.2 Definition. Let L be a lattice, and let J be a non-empty subset of L. We call J an **ideal** if J is a down-set closed under joins. We can rewrite this as $a, b \in J$ implies $a \vee b \in J$. Moreover, $a \in L$, $b \in J$ and $a \leq b$ imply $a \in J$.

The dual concept of an ideal is a filter. Let G be non-empty. Then, G is a **filter** if G is an up-set closed under meets. We can rewrite this as $a, b \in G$ implies $a \wedge b \in G$. Moreover, $a \in L$, $b \in G$ and $a \geq b$ imply $a \in G$.

An ideal or filter is called **proper** if it strictly included in L.

We see that since an ideal is a down-set, it must always contain 0, and since a filter is an up-set, it must always contain 1. $\{0\}$ and $\{1\}$ are the smallest ideal and filter, respectively.

An ideal is proper if and only if it does not contain 1 and a filter is proper if and only if it does not contain 0. One direction is trivial. For the other, it is routine to prove the contraposition.

In the Boolean case, there is a one-to-one correspondence between ideals and filters. Given an ideal J of a Boolean algebra B, the corresponding filter would be $\{a' : a \in J\}$. Conversely, given a filter G of B, the corresponding ideal is $\{a' : a \in G\}$. Because of this correspondence, every statement about ideals translates automatically into one about filters.

It is often useful to find the smallest ideal containing a certain subset S or element of the lattice. It follows from the definitions of an ideal that the intersection T of all ideals containing S is an ideal, the smallest ideal to contain S. Dually, the intersection R of all filters containing S is a filter, the smallest filter to contain S.

Moreover, let a be an arbitrary element of a lattice. Then it follows directly from the definitions that $\downarrow a$ is an ideal, and $\uparrow a$ is a filter.

9.3 Definition. Let $S \subseteq L$ be an arbitrary subset. We call the intersection T of all ideals containing S the **ideal generated by** S. Analogously, we call the intersection R of all filters containing S the **filter generated by** S.

Let $a \in L$. We call $\downarrow a$ the **principal ideal** generated by a, and $\uparrow a$ the **principal filter** generated by a. This coincides with the ideal or filter generated by $\{a\}$.

Many results about lattice ideals and filters require additional conditions, making the ideals or filters prime or maximal. We define these below.

9.4 Definition. A proper ideal J of L is **prime** if $a, b \in L$ and $a \wedge b \in J$ imply $a \in J$ or $b \in J$. Dually, a proper filter G of L is prime if $a, b \in L$ and $a \vee b \in G$ imply $a \in G$ or $b \in G$.

A proper ideal J (proper filter G) of L is **maximal** if the only ideal (filter) which properly contains J (G) is L itself. A maximal filter is more commonly called an **ultrafilter**.

The next lemma proves some basic relations between prime and maximal ideals in a distributive or Boolean lattice.

9.5 Lemma. *Let L be a lattice, and let B be a Boolean lattice.*

1. *Let L be a distributive lattice with 1. Then every maximal ideal in L is prime. Dually, in a distributive lattice with 0, every ultrafilter is a prime filter.*
2. *Now let K be a proper ideal (filter) in B. Then the following are equivalent:*
   (a) *K is a maximal ideal (filter);*
   (b) *K is a prime ideal (filter);*
   (c) *for each $a \in B$, we have $a \in K$ if and only if $a' \notin K$.*

Proof. To prove the first statement, let J be a maximal ideal. Let $a, b \in L$ with $a \wedge b \in J$ and $a \notin J$. We want to prove that $b \in J$. Define $J_a := \downarrow\{a \vee c : c \in J\}$. Then J_a is an ideal containing J and a: that J_a is an ideal follows directly from the definition of an ideal.

Since J_a is an ideal, it contains 0. It follows from the definition of J_a that $J \subseteq J_a$ and $a \in J_a$, therefore, J is strictly included in J_a. Because J is maximal, we conclude $J_a = L$.

In particular, we have $1 \in J_a$, so $1 = a \vee c$ for some $c \in J$. As $a \wedge b, c \in J$, we have $(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c) = b \vee c \in J$. Since $b \leq b \vee c$, we have $b \in J$. So J is prime. The statement about filters follows by duality.

Next, we prove the second statement. Firstly, let K be a maximal ideal. Because B is distributive, K is a prime ideal.

Secondly, let K be a prime ideal, and let a be an element of B. Because $a \wedge a' = 0$, we have $a \wedge a' \in K$. As K is prime, this implies $a \in K$ or $a' \in K$. If both a and a' belong to K, then we would also have $1 = a \vee a' \in K$, which would mean that K is not proper. This is in contradiction with the definition of a prime ideal. Therefore, precisely one of a and a' is an element of K.

Lastly, assume (c), and let H be an ideal properly containing K. Let a be a fixed element of $H \setminus K$. Then $a' \in K$, which implies $a' \in H$. Therefore, $a \vee a' = 1 \in H$. Thus, $H = B$, which shows that K is maximal.

The dual statements about filters follow by duality. □

10 Preliminaries for the proofs

First, we define some topological concepts which we will need. The finite intersection property is a useful aid in our proofs, whereas the concept of a Stone space is central to Stone duality.

10.1 Definition. Let (X, τ) be a topological space, and let $A = \{A_i\}_{i \in I}$ be a collection of subsets of X. We say that A has the **finite intersection property** if any finite subcollection $J \subseteq I$ has a non-empty intersection $\bigcap_{i \in J} A_i$.

10.2 Definition. We say that a topological space (X, τ) is **totally disconnected** if τ has a basis of clopen sets. A **Stone space** is a totally disconnected compact Hausdorff space. Stone spaces are also called **Boolean spaces** in some literature.

Note that although there are different definitions of totally disconnected spaces, they are all equivalent in compact Hausdorff spaces. Since we only need total disconnectedness in compact Hausdorff spaces, we have chosen the most convenient option for our purposes.

Because Stone spaces are topological spaces, their structure is preserved by homeomorphisms.

For Heyting duality (also named Esakia duality in some literature), we need an analogue of Stone spaces. These are aptly named Heyting spaces.

10.3 Definition. Let $(X, \tau, \leq)$ be a Stone space with a partial order defined on X, and let $x, y \in X$ with $x \not\leq y$. If there is a clopen up-set U with $x \in U$ and $y \notin U$, we say that $(X, \tau, \leq)$ satisfies the **Priestley separation axiom**. If, in addition, for every clopen $U \subseteq X$ the set $\downarrow U$ is clopen, we call $(X, \tau, \leq)$ a **Heyting space**. Heyting spaces are also called **Esakia spaces** in the literature.

To preserve the structure of a Heyting space, we need to preserve both the topological and the ordered structure. The topological structure is preserved by continuous maps. To preserve the order and algebraic structure (including implication), we need a new kind of map.

10.4 Definition. Let $f : (X, \tau, \leq) \to (Y, \sigma, \preccurlyeq)$ be an order-preserving map. We call f a **p-morphism** if for every $x \in X, y \in Y$ with $f(x) \leq y$, there is a $z \in X$ with $x \leq z$ and $f(z) = y$.

The structure-preserving maps of Heyting spaces are continuous p-morphisms.

Now that we have all our required knowledge in order, we can define basic notation for the proofs.

10.5 Definition. For L a bounded distributive lattice, let $PF(L)$ be the set of prime filters. For $a \in L$, let $F_a \in PF(L)$ be defined as

$$F_a := \{P \in PF(L) : a \in P\}.$$

Let $F : L \to PF(L)$ be the map sending a to F_a. Equip $PF(L)$ with the topology τ as follows: Let $S := \{F_a : a \in L\} \cup \{(F_b)' : b \in L\}$ be a subbasis. Then $T := \{F_a \cap (F_b)' : a, b \in L\}$ is a basis of τ. For X a topological space, let $Cl(X)$ be the set of clopen sets of X, and $CU(X)$ the set of clopen up-sets of X. These sets are ordered by inclusion.

Note that both F_a and $(F_a)'$ are in the basis for all $a \in L$. To see why, observe that $F_a = F_a \cap (F_0)' = F_a \cap PF(L)$ and $(F_a)' = F_1 \cap (F_a)' = PF(L) \cap (F_a)'$. Moreover, since L is bounded, 0 and 1 are elements of L. Therefore, for every element a of L, F_a is clopen.

The map F will be central to our efforts, so it pays to prove a few basic results about it. First we prove that it is a homomorphism:

10.6 Lemma. *Let L be a bounded distributive lattice. Then F preserves join, meet, 0 and 1. If L is a Boolean algebra, F also preserves complement.*

Proof. $F_0 = \varnothing$ because no prime filter contains 0. $F_1 = PF(L)$ because every prime filter contains 1. Thus, the map preserves 0 and 1.

Next, we prove $F_a \cup F_b \subseteq F_{a \vee b}$ to see that F preserves join. As filters are up-sets, $a \in P$ or $b \in P$ implies $a \vee b \in P$. Moreover, we have $F_{a \vee b} \subseteq F_a \cup F_b$ because $P \in F_{a \vee b}$ is prime, so $a \vee b \in P$ implies $a \in P$ or $b \in P$.

Now we prove that F preserves meet: $F_a \cap F_b \subseteq F_{a \wedge b}$ because filters are closed under finite meets. $F_{a \wedge b} \subseteq F_a \cap F_b$ because filters are up-sets, so $a \wedge b \in P$ implies $a \in P$ and $b \in P$.

Now let L be a Boolean algebra. We want to prove that $(F_b)' = F_{b'}$. Because $P \in PF(L)$ is proper, it does not contain both b and b'. Because P is prime, and thus an ultrafilter, it contains either b or b'. So the set of prime filters containing b' is precisely the set of prime filters not containing b. □

Due to the dual nature of lattices, it would have been equivalent to prove that F preserves supremum and infimum, rather than join and meet.

The next lemma is an auxiliary lemma, which we will use several times throughout the proofs. If we do not explicitly name an ideal, we can assume it is any ideal which fulfills the conditions. There is always one such ideal if G is a proper filter: the trivial ideal, $\{0\}$.

10.7 Lemma. *Let G be a filter and I an ideal of a bounded distributive lattice L. If $G \cap I = \varnothing$, then there is a prime filter P of L such that $G \subseteq P$ and $P \cap I = \varnothing$.*

Proof. Let A be the set of all filters of L containing G and disjoint from I. Then A is nonempty since it contains G. Let $C = \{A_i : i \in K\}$ be an arbitrary chain in A, with K an arbitrary index set.

Then $\bigcup_i A_i$ is a filter: it is closed under meets because for all $i, j \in K$, we have $A_i \wedge A_j = A_i$ if $A_i \leq A_j$ and A_j otherwise. Because C is a chain, $\bigcup_i A_i$ is certainly an up-set.

Also, $\bigcup_i A_i \cap I = \varnothing$, as $A_i \cap I = \varnothing$ for all $i \in K$. Thus, $\bigcup_i A_i \in A$, and it is clearly an upper bound for C. We can now apply Zorn's lemma (Lemma 2.3),

which gives us that A has a maximal element P. To verify that this indeed the P we want, we still need to prove that P is prime.

Suppose $a, b \in L$ with $a \vee b \in P$. Let G_1 and G_2 be the filters generated by $P \cup \{a\}$ and $P \cup \{b\}$, respectively. Suppose that $a, b \notin P$. Then P is properly contained in both G_1 and G_2. As P is a maximal element of A, this must mean that G_1 and G_2 are not elements of A. As G_1 and G_2 are filters of L and contain F (as P does), we must have that $G_i \cap I \neq \varnothing$ for $i = 1, 2$.

Let $x_i \in G_i \cap I$ for each i. Because G_1 and G_2 are the smallest up-sets closed under meets which includes $P \cup \{a\}$ and $P \cup \{b\}$, respectively, there are $p_1, p_2 \in P$ with $p_1 \wedge a \leq x_1$ and $p_2 \wedge b \leq x_2$. This gives

$$x_1 \vee x_2 \geq (p_1 \wedge a) \vee (p_2 \wedge b) = (p_1 \vee p_2) \wedge (p_1 \vee a) \wedge (p_2 \vee b) \wedge (a \vee b).$$

The left inequality follows from the previous statement, the rightmost equality from repeated application of the distributive laws. Because $p_1, p_2 \in P$ and $p_1 \vee p_2, p_1 \vee a, p_2 \vee b$ are each greater than either p_1 or p_2, and because we assumed $a \vee b \in P$, all four terms are in P. As P is a filter, their meet is in P, which implies that $x_1 \vee x_2 \in P$.

However, we had both $x_1, x_2 \in I$. As I is an ideal, we find $x_1 \vee x_2 \in I$. Therefore, $x_1 \vee x_2 \in P \cap I$, which contradicts $P \in A$. Thus, we must have either $a \in P$ or $b \in P$, so P is a prime filter. □

We can use our auxiliary lemma for the first time to prove that F is injective.

10.8 Lemma. *Let L be a bounded distributive lattice. Then F is injective.*

Proof. Suppose $a \neq b$. We want to show that $F_a \neq F_b$. Since $a \neq b$, we have either $a \not\leq b$ or $b \not\leq a$. Without loss of generality, we may assume $a \not\leq b$. Let $G = {\uparrow}a$ be the filter generated by a and $I = {\downarrow}b$ be the ideal generated by b. Because $a \not\leq b$, we must have $G \cap I = \varnothing$. By applying Lemma 10.7, we obtain a prime filter P with $G \subseteq P$ and $P \cap I = \varnothing$. Therefore, $a \in P$ and $b \notin P$, so $P \in F_a$ and $P \notin F_b$. From this it follows that $F_a \neq F_b$, so F is injective. □

11 Stone Duality

We begin with the Boolean case, as we can use some of the results again later on. We will show that, in a sense, taking the set of prime filters of a Boolean algebra, and taking the clopen subsets of a Stone space are opposite operations.

In the next lemma, we prove that if L is a Boolean algebra, then forming the set of prime filters gives a Stone space. However, it is a surprising and less well known fact that we can weaken the requirement to L being a distributive lattice.

11.1 Lemma. *Let L be a distributive lattice. Then $PF(L)$ with the topology defined before is a Stone space. We call it the **dual space** of L.*

Proof. First we prove that $PF(L)$ has a basis of clopen sets. Let A be in T, the basis of τ. By definition of the topology, $A = F_a \cap F_b'$ for certain $a, b \in L$. Since A is in the basis of τ, A is certainly open. To prove that A is closed, we have to show that the complement of A is also open. By definition of A and application of the de Morgan's laws, we can write $A' = (F_a \cap F_b')' = F_a' \cup F_b$. As both F_a' and F_b are in the basis, their union A' is open, so A is closed.

Next, we show that $PF(L)$ is Hausdorff. Let P and Q be prime filters with $P \neq Q$. Then either $P \nsubseteq Q$ or $Q \nsubseteq P$. Without loss of generality, we may assume $P \nsubseteq Q$. Then there is an $a \in L$ with $a \in P, a \notin Q$. Therefore, $P \in F_a$ and $Q \in (F_a)'$. So P and Q are separated by disjoint open sets of $PF(L)$. Therefore, $PF(L)$ is Hausdorff.

Lastly, we claim that $PF(L)$ is compact. Let $\mathcal{U}$ be an open cover of PF(L). We have to show that $\mathcal{U}$ has a finite subcover. Since every $U \in \mathcal{U}$ is open, $\mathcal{U}$ is a union of sets of the form $\{F_a \cap F_b'\}$ for $a, b \in A$ where A is a fixed subset of L. In short, we can write $\mathcal{U} = \bigcup_{a,b \in A} \{F_a \cap F_b'\}$. Since F_a and F_b' are in the subbasis of τ, they are open.

Because $\mathcal{U}$ is a cover of $PF(L)$, we can write

$$PF(L) \subseteq \bigcup_{a,b \in A} \{F_a \cap F_b'\} \subseteq \bigcup_{a \in A_1} \{F_a\} \cup \bigcup_{b \in A_2} \{F_b'\}.$$

Here A_1 and A_2 are fixed subsets of A. We see that $\bigcup_{a \in A_1} \{F_a\} \cup \bigcup_{b \in A_2} \{F_b'\}$ is also an open cover of $PF(L)$. It follows that $\bigcap_{b \in A_2} F_b \subseteq \bigcup_{a \in A_1} F_a$.

Let I be the ideal generated by the $a \in A_1$ and G the filter generated by the $b \in A_2$. We will show by contradiction that $G \cap I \neq \varnothing$. Let us assume that $G \cap I = \varnothing$. Lemma 10.7 gives us a prime filter P with $G \subseteq P$ and $G \cap I = \varnothing$. Since $A_2 \subseteq G \subseteq P$, we have $P \in F_b$ for all $b \in A_2$. So $P \in \bigcap_{b \in A_2} F_b$. We saw before that $\bigcap_{b \in A_2} F_b \subseteq \bigcup_{a \in A_1} F_a$, so we have $P \in F_a$ for an $a_0 \in A_1$, which means $a_0 \in P$. However, as a_0 is also an element of $A_1 \subseteq I$, this implies $P \cap I \neq \varnothing$, which contradicts our assumption. This contradiction tells us that $G \cap I \neq \varnothing$.

Let $x \in G \cap I$. Because G is the filter generated by A_2 and $x \in G$ we have, per definition of G, $x \geq b_* := b_1 \wedge \cdots \wedge b_n$ for certain $b_1, \ldots, b_n \in A_2$. Similarly, as I is the ideal generated by A_1 and $x \in I$ we have, per definition of I, $x \leq a_* = a_1 \vee \cdots \vee a_m$ for certain $a_1, \ldots, a_m \in A_1$. So

$$b_1 \wedge \cdots \wedge b_n \leq x \leq a_1 \vee \cdots \vee a_m.$$

Any prime filter containing all of $b_1, \ldots, b_n$ contains b_*, because a filter is closed under meets. Moreover, as a filter is an up-set, any prime filter containing b_* will contain a_* as well. Finally, any prime filter containing a_* must contain one of $a_1, \ldots, a_m$, because it is prime. Therefore, we have

$$F_{b_1} \cap \cdots \cap F_{c_n} \subseteq F_{c_*} \subseteq F_{a_*} \subseteq F_{a_1} \cup \cdots \cup F_{a_m}.$$

We now see that the open sets $F_{a_1}, \ldots, F_{a_m}, F_{b_1}', \ldots, F_{b_n}'$ cover $PF(B)$, so $PF(B)$ is compact. $\square$

We can now turn a Boolean algebra into a Stone space by finding the set of prime filters with the correct topology. We also want to turn a Stone space into a Boolean algebra by taking the set of clopen subsets. The following lemma asserts that this works.

11.2 Lemma. *Let X be a Stone space. Then $Cl(X)$ is a Boolean algebra, called the **dual algebra** of X.*

The lemma can be proven routinely by checking the axioms of a Boolean algebra, most of which follow directly from set theory and the preservation of clopenness by intersection, union and complement. We leave the proof as an exercise for the reader.

We now know that we can switch between Boolean algebras and Stone spaces by taking the dual space or algebra. The next question to ask is whether we create a new Boolean algebra or Stone space every time, or whether we eventually come back to the same one. The next two theorems together form **Stone's representation theorem**, which asserts that after two steps we have, up to isomorphism, the same Boolean algebra or Stone space that we started with. We first prove this result for Boolean algebras.

11.3 Theorem (Stone's representation theorem, part 1)**.** *Let B be a Boolean algebra. Then the map*

$$f : B \to Cl(PF(B)), \text{ given by } b \mapsto F_b$$

is an isomorphism of Boolean algebras.

Proof. First we show that f is well-defined. Because $PF(B)$ is a Stone space (Lemma 11.1) we see that $Cl(PF(B))$ is a Boolean algebra (Lemma 11.2), and therefore a subalgebra of the power set of $PF(B)$. Because F_b is an element of the subbase S of τ, it is open. As $(F_b)'$ is also an element of S, F_b) is closed, thus clopen. So every image of b is an element of $Cl(PF(B))$.

The next thing to show is that f is surjective. Let C be a clopen subset of $PF(B)$. Because C is open,

$$C = \bigcup_{b\in B_1, c\in B_2} \{F_b \cap F_c'\}, \text{ where } B_1 \text{ and } B_2 \text{ are certain fixed subsets of } B.$$

We can rewrite this to

$$C = \bigcup_{b\in B_1, c\in B_2} \{P \in PF(B) : b \in P \text{ and } c \notin P\}.$$

Since every prime filter is an ultrafilter (see Lemma 9.5), $c \notin P$ implies $c' \in P$. Because P is a filter, and thus closed under meets, we have $b \wedge c' \in P$ for all prime filters in C. So

$$C = \bigcup_{b\in B_1, c\in B_2} \{P \in PF(B) : b\wedge c' \in P\} = \bigcup_{d\in B_3} \{P \in PF(B) : d \in P\} = \bigcup_{d\in B_3} F_d$$

with $b \wedge c'$ an element of B_3 if and only if $b \in B_1$ and $c \in B_2$.

Because F_d is open for each d, $\{F_d : d \in B_3\}$ is an open cover of C. Since C is closed and $PF(B)$ is compact, C is also compact. Therefore, $C = F_{d_1} \cup \cdots \cup F_{d_n}$ for some $d_1, \ldots, d_n \in B_3$. From Lemma 10.6 we therefore have $C = F_{d_1 \vee \cdots \vee d_n}$. Therefore, C is in the image of f.

We proved that f is a homomorphism in Lemma 10.6, and that f is injective in Lemma 10.8. □

Now we prove Stone's representation theorem for Stone spaces.

11.4 Theorem (Stone's representation theorem, part 2)**.** *Let X be a Stone space. Then the map*

$$g : X \to PF(Cl(X)), \text{ given by } x \mapsto F_U := \{U \in Cl(X) : x \in U\}$$

is a homeomorphism.

Note that although it may seem at first that F_U is a new notation, it is actually the same definition as our standard F_a. The possible confusion stems from the fact that elements of $Cl(X)$ are subsets of X.

Proof. Firstly, we show that g is well-defined. Let x be an element of X. We want to show that $g(x)$ is a prime filter of $Cl(X)$. To see that $g(x)$ is an up-set of Cl(X), take $V, \in Cl(X)$ with $V \in g(x)$ and $V \subseteq W$. Then $x \in V \subseteq W$, hence $W \in g(x)$.

We show that $g(x)$ is closed under meets. If $U, V \in g(x)$, then $x \in U$ and $x \in V$, so $x \in U \cap V$. Then we have $U \cap V \in g(x)$. So $g(x)$ is a filter.

To see that $g(x)$ is prime, suppose that $U \cup V \in g(x)$. Then $x \in U \cup V$, so $x \in U$ or $x \in V$. This means that at least one of U and V is an element of $g(x)$, so $g(x)$ is a prime filter.

Next we show that g is continuous. To do so, it is sufficient to show that the inverse image of every set in the basis of the topology of $PF(Cl(X))$ is open. Let us name this topology τ_1 for this proof.

Let A be an element in the basis of τ_1. Using the fact that F is a homomorphism (see Lemma 10.6), we find that A is of the form

$$\{F_U \cap F'_V : U, V \in Cl(X)\} = \{F_{U \cap V'} : U, V \in Cl(X)\}.$$

So A is of the form F_W for a certain$W \in Cl(X)$.

We now show that $g^{-1}(A) = g^{-1}(F_W)$ is open. The first equality follows from the definition of $g^{-1}(F_W)$, the second from the definition of F_W, and the third from the definition of $g(x)$.

$$\begin{aligned} g^{-1}(F_W) &= \{x \in X : g(x) \in F_W\} \\ &= \{x \in X : W \in g(x)\} \\ &= \{x \in X : x \in W\} \\ &= W. \end{aligned}$$

As W is a clopen subset of X, the inverse image of A is open for every A in the basis of τ_1. Therefore, g is continuous.

We now prove that g is injective. Take $x, y \in X$ with $g(x) = g(y)$. As X is a Boolean space, X is Hausdorff. Therefore, we can separate every $a, b \in X$ with $a \neq b$ by open sets. As X also has a basis of clopen sets, every open set is a union of clopen sets. Therefore, there are clopen subsets of the open sets separating a and b which still separate a and b. In short, we can separate every $a, b \in X$ with $a \neq b$ by clopen sets.

So only x itself is an element of all clopen subsets containing x. In symbolic language:

$$\bigcap g(x) := \bigcap \{U \in Cl(X) : x \in U\} \subseteq \{x\}.$$

Because $x \in \bigcap g(x)$, we conclude $\bigcap g(x) = \{x\}$. Moreover, if $g(x) = g(y)$, then $\bigcap g(x) = \bigcap g(y)$. We can then conclude $\{x\} = \{y\}$, which implies $x = y$. Thus, g is injective.

Lastly, we show that g is surjective. Let P be an element of $PF(Cl(X))$. As P is a filter, it is closed under intersection. As P is proper, it does not contain $\varnothing$. Therefore, it has the finite intersection property (Definition 10.1). As $PF(Cl(X))$ is a Stone space (apply Lemma 11.2 and Lemma 11.1), $PF(Cl(X))$ is compact. Since P is a collection of closed sets with the finite intersection property in a compact space, P has a non-empty intersection.

Let x, y be arbitrary fixed elements of P with $x \neq y$. We use the same argument as before, when proving that g is injective to conclude that there is a clopen set U with $x \in U$ and $y \in X \setminus U$. We also know that either $U \in P$ or $X \setminus U \in P$, because P is an ultrafilter (see Lemma 9.5). If $U \in P$, then $y \notin \bigcap P$, and if $X \setminus U \in P$, then $x \notin \bigcap P$.

So $\bigcap P = \{z\}$ for a certain $z \in X$. So $P \subseteq g(z)$. As P and $g(x)$ are both prime, hence maximal, filters on $Cl(X)$, we conclude $P = g(z)$. So every $P \in PF(Cl(X))$ is in the image of g.

As X is a compact space, and $PF(Cl(X))$ is Hausdorff, and g is a continuous bijection, g is a homeomorphism. □

From these two theorems we can also conclude that if A and B are isomorphic Boolean algebras, then $PF(A)$ and $PF(B)$ are homeomorphic Stone spaces. Dually, if X and Y are homeomorphic Stone spaces, then $Cl(X)$ and $Cl(Y)$ are isomorphic Boolean algebras.

We can rework our duality theorems using the space of 2-valued homomorphisms rather than the space of prime filters of a Boolean algebra. Since every prime filter is an ultrafilter in the Boolean case, it can be shown that there is a 2-valued homomorphism which sends the elements in the prime filter to 1, and the rest to 0. We will not prove this here. Hence, there is a one-to-one correspondence between prime filters and 2-valued homomorphisms.

For B a Boolean algebra, let $Hom_2(B)$ be the set of 2-valued homomorphisms on B. The topology of $Hom_2(B)$ is defined by the basis R containing the sets of the form $G_b = \{g \in Hom_2(B) : g(b) = 1\}$ for $b \in B$. It can be shown that

these are precisely the clopen sets of $Hom_2(B)$. We can now restate Stone's representation theorem.

11.5 Theorem (Stone's representation theorem with 2-valued homomorphisms)**.** *Let B be a Boolean algebra. Then the map*

$$f : B \to Cl(Hom_2(B)), \text{ given by } b \mapsto G_b = \{g \in Hom_2(B) : g(b) = 1\}$$

is an isomorphism of Boolean algebras.

Now let X be a Stone space. Then the map

$$g : X \to Hom_2(Cl(X)), \text{ given by } x \mapsto g(x), \text{ where } g(x)(P) = \begin{cases} 1 & \text{if } x \in P \\ 0 & \text{if } x \notin P \end{cases}$$

is a homeomorphism.

Moreover, if A and B are isomorphic Boolean algebras, then $Hom_2(A)$ and $Hom_2(B)$ are homeomorphic Stone spaces. Dually, if X and Y are homeomorphic Stone spaces, then $Cl(X)$ and $Cl(Y)$ are isomorphic Boolean algebras.

12 Heyting Duality

One would expect that the dual space of a Heyting algebra would fulfill fewer conditions than the dual space of a Boolean algebra. However, it turns out the Heyting space is a Stone space which fulfills extra conditions. To show the duality between Heyting algebras and Heyting spaces, we will first prove the analogues of Lemma 11.1 and Lemma 11.2.

12.1 Lemma. *If H is a Heyting algebra, then $(PF(H), \subseteq)$ is a Heyting space.*

Proof. As H is a distributive lattice, Lemma 11.1 tells us that $PF(H)$ is a Stone space and thus compact.

Next, we show that $PF(H)$ satisfies the Priestley separation axiom. Let P and Q be elements of $PF(H)$, with $P \nsubseteq Q$. Then there is an $x \in P$ with $x \notin Q$. Therefore, $P \in F_x$, but $Q \notin F_x$. We already know that F_x is clopen for any x in H (see Theorem 11.3; f is well-defined). Moreover, F_x is an up-set of $PF(H)$: if $R \in F_x$ and R is a subset of S, then we have $x \in R \subseteq S$, so $S \in F_x$. Thus, we have a clopen up-set F_x with $P \in F_x$, but $Q \notin F_x$. So $PF(H)$ satisfies the Priestley separation axiom.

The last thing we need to show is that if $U \subseteq PF(H)$ is clopen, then $\downarrow U$ is clopen. Let U be a clopen subset of $(PF(H), \subseteq)$. Because U is open, U is a union of elements in the basis of the topology on $PF(H)$, so these basic elements form an open cover of U. Because U is closed and $PF(H)$ is compact, U is compact. Therefore, our open cover has a finite subcover. Thus, $U = \bigcup_{i=1,\ldots,n} F_{a_i} \cap F'_{b_i}$ for certain $a_i, b_i \in H$. Using the definition of a down-set, we find

$$\downarrow U = \downarrow(\bigcup_{i=1,\ldots,n} F_{a_i} \cap F'_{b_i}) = \bigcup_{i=1,\ldots,n} \downarrow(F_{a_i} \cap F'_{b_i}).$$

We will show that $\downarrow(F_{a_i} \cap F'_{b_i}) = F_{a \to b}$. As $a \to b$ is an element of H, we see that $F_{a \to b}$ is clopen. Since a finite union of clopen sets is again clopen, we can then conclude that $\downarrow U$ is clopen.

Let $a, b \in H$. We saw in Lemma 8.2 that $a \wedge (a \to b) = a \wedge b$, so $a \wedge (a \to b) \leq b$. We will show that $F_a \cap F_{a \to b} \subseteq F_b$. Let $P \in F_a \cap F_{a \to b}$. By definition, both a and $a \to b$ are elements of P. As P is a filter, it is closed under finite meets. Thus, we have $a \wedge (a \to b) \in P$. Moreover, P is an up-set, so we have $b \in P$. Therefore, $P \in F_b$. We have seen that $F_a \cap F_{a \to b}$ is a subset of F_b. A set-theoretic inclusion argument gives $F_a \cap F'_b \subseteq F'_{a \to b}$. As $F_{a \to b}$ is a filter, it is an up-set. Therefore, $F'_{a \to b}$ is a down-set. This, together with $F_a \cap F'_b \subseteq F'_{a \to b}$ allows us to conclude that $\downarrow(F_a \cap F'_b) \subseteq F'_{a \to b}$.

Now it remains to show that $F'_{a \to b} \subseteq \downarrow(F_a \cap F'_b)$. Let $P \in F'_{a \to b}$. Then P is a prime filter of which $a \to b$ is not an element. We wish to show that P is an element of $\downarrow(F_a \cap F'_b)$. Therefore, we want to find a prime filter Q of H with a an element of Q, but not b, and $P \subseteq Q$. We then have $\{a\} \cup P \subseteq Q$. We saw in the previous paragraph that if a and $a \to b \in Q$, then also $b \in Q$. So it is sufficient to show that $a \to b \notin Q$ rather than $b \notin Q$.

Lemma 10.7 tells us that such a prime filter Q exists if the filter G generated by $P \cup \{a\}$ does not contain $a \to b$. We will prove this by contradiction. Assume $a \to b$ to be an element of G. Then there is an $y \in P \cup \{a\}$ for which $y \leq a \to b$, because G is the filter generated by $P \cup \{a\}$. Because $a \to b \notin P$, we must have $y = a \wedge x$ for an $x \in P$. To see this, note that we cannot have $y \in P$, and if $a \leq a \to b$, then we still have $a \wedge x \leq a \leq a \to b$.

As $a \wedge x \leq a \to b$, we can conclude by definition of $a \to b$ that $(a \wedge x) \wedge a \leq b$. The idempotency law then gives $a \wedge x \leq b$, and the definition of $a \to b$ gives $x \leq a \to b$. Since P is an up-set and $x \in P$, we must have $a \to b \in P$. But this is a contradiction with our definition of P. Therefore the filter G generated by $P \cup \{a\}$ does not contain $a \to b$.

Thus, we have a prime filter Q of which a is an element, b is not, and P is a subset. Therefore, P is an element of $\downarrow(F_a \cap F'_b)$. We have now shown that $F'_{a \to b} \subseteq \downarrow(F_a \cap F'_b)$. Therefore, $F'_{a \to b} = \downarrow(F_a \cap F'_b)$. We have shown before that this implies that $\downarrow U$ is clopen. □

We have proven that the prime filter space of a Heyting algebra is indeed a Heyting space. To go from a Heyting space to a Heyting algebra, we need to do something to preserve both the topology and the order structure. To see the effect of the order structure, compare the next lemma with Lemma 11.2. Remember that $CU(X)$ is the set of clopen up-sets of an ordered topological space X.

12.2 Lemma. *Let $(X, \leq)$ be a Heyting space. Then $CU(X, \leq)$ is a Heyting algebra, where implication is defined by $U \to V = (\downarrow(U \cap V'))'$.*

Proof. Firstly, we have to show that implication is well-defined. We want to show that $(\downarrow(U \cap V'))'$ is a clopen up-set for any clopen up-sets U and V of $(X, \leq)$. Because U and V are clopen, $U \cap V'$ is clopen. Because U is a Heyting

space, this means that $(\downarrow U \cap V')$ is clopen. Because $(\downarrow U \cap V')$ is a clopen down-set, its complement $(\downarrow(U \cap V'))'$ is a clopen up-set.

Secondly, we show that $CU(X, \leq)$ is a bounded distributive lattice. It is routine to show that $CU(X, \leq)$ is a subset of the power set of $(X, \leq)$, closed under finite unions and intersections. Therefore, $CU(X, \leq)$ is a sublattice of the power set of $(X, \leq)$, with $0 = \varnothing$ and $1 = X$. Distributivity follows from the distributivity law of sets.

Lastly, we need to prove that our definition of implication has the correct properties. To prove this, it is both necessary and sufficient to show that $U \cap W \subseteq V$ is equivalent with $W \subseteq U \to V$. Let W be a clopen up-set of $(X, \leq)$.

We start by proving the forward implication. Suppose $U \cap W$ is a subset of V. Then, by a simple set-theoretic inclusion argument, we have $U \cap V' \subseteq W'$. Because W is an up-set, W' is a down-set. Therefore, $\downarrow(U \cap V')$ is a subset of W'. Applying complementation on both sides, we find $W \subseteq (\downarrow U \cap V')' = U \to V$.

It remains to prove the reverse implication. Because $U \cap V' \subseteq \downarrow(U \cap V')$, we have

$$U \to V = (\downarrow(U \cap V'))' \subseteq (U \cap V')'.$$

Therefore, for any subset W of $U \to V$, we have

$$\begin{aligned} U \cap W \subseteq U \cap (U \to V) \subseteq U \cap (U \cap V')' = U \cap (U' \cup V) \\ = (U \cap U') \cup (U \cap V) = U \cap V \subseteq V. \end{aligned}$$

The first inequality uses the definition of W, and the second that of $U \to V$. The third equality uses the de Morgan's laws, and the fourth the distributivity laws. The fifth equality uses the properties of the set-theoretic complement, and the last inequality uses the properties of intersection. □

12.3 Theorem (Heyting representation theorem, part 1)**.** *Let H be a Heyting algebra. Then there is a Heyting isomorphism*

$$f : H \to CU(PF(H)), \text{ given by } f(h) = F_h = \{P \in PF(H)) : h \in P\}.$$

Proof. We start by proving that f is a homomorphism. That f preserves join, meet, 0 and 1 follows from Lemma 10.6, so we only need to show that f preserves implication. Let $h, k \in H$. Then $f(h \to k) = F_{h \to k} = (F'_{h \to k})'$. We have proven in Lemma 12.1 that $F'_{h \to k} = \downarrow(F_h \cap F'_k)$. Therefore, $(F'_{h \to k})' = (\downarrow(F_h \cap F'_k))'$ We saw in Lemma 12.2 that this equals $F_h \to F_k$. So, f is a homomorphism.

That f is injective follows from Lemma 10.8.

We now show that f is surjective. Let U be a clopen up-set of $PF(H)$. We want to show that $U = F_a$ for an $a \in H$. Let P be an element of U, and Q an element of U'. Then $P \nsubseteq Q$, because U is an up-set. Thus, there is a certain $a_{PQ} \in H$ which is an element of P, but not of Q. Therefore, $P \in F_{a_{PQ}}$ and $Q \in F'_{a_{PQ}}$. We see that the various $F'_{a_{PQ}}$ cover U'. As $PF(H)$ is compact by Lemma 12.1, we have

$$U' \subseteq \bigcup_{i=1,\ldots,n} (F_{a_{PQ_i}})' = F'_{a_P} \text{ for } a_P = a_{PQ_1} \wedge \cdots \wedge a_{PQ_n}.$$

As $P \in F_{a_{PQ_i}}$ for all a_{PQ_i}, we have $P \in F_{a_P} \subseteq U$.

Because U is the union of the various F_{a_P}, they form an open cover of U. Because U is closed and $PF(H)$ is compact, U must be a finite union

$$\bigcup_{i=1,\ldots,m} F_{a_{P_i}} = F_a \text{ with } a = a_{P_1} \vee \cdots \vee a_{P_m}.$$

Therefore, $U = F_a$ for a certain $a \in H$, so U is in the image of f. □

12.4 Theorem (Heyting representation theorem, part 2)**.** *Let $(X, \leq)$ be a Heyting space. Then there is an isomorphism of Heyting spaces*

$$g : (X, \leq) \to PF(CU(X, \leq), \subseteq), \text{ given by } g(x) = \{U \in CU(X, \leq) : x \in U\}.$$

Proof. We start by proving that g is well-defined. We have to show that for any $x \in X$, $g(x)$ is a prime filter. The argument is similar to that in the proof of Theorem 11.4.

Next, we have to show that g is an order-embedding. Let $x, y \in X$ with $x \leq y$. If $U \in g(x)$, then $x \in U$. As U is an up-set, we must then have $y \in U$. Then $U \in g(y)$, so $g(x) \subseteq g(y)$.

Now, let $u, v \in X$ with $g(u) \subseteq g(v)$ and assume $u \not\leq v$. Then the Priestley separation axiom states that there is a clopen up-set U with $u \in U$, but $v \notin U$. Therefore, $U \in g(u)$ and $U \notin g(v)$. But then $g(u) \not\subseteq g(v)$, which contradicts our assumption. Thus $u \leq v$.

Thirdly, we show that g is continuous. Let U be a clopen up-set of $(X, \leq)$. Consider the basic clopen set $F_U = \{P \in PF(CU(X, \leq)) : U \in P\}$. Then

$$\begin{aligned} g^{-1}(F_U) &= \{x \in X : g(x) \in F_U\} \\ &= \{x \in X : U \in g(x)\} \\ &= \{x \in X : x \in U\} \\ &= U. \end{aligned}$$

The argument is the same as in the Boolean case, see Theorem 11.4. Thus, every inverse image of a clopen set is clopen, so g is continuous.

We now prove that g is surjective. Since X and $PF(CU(X, \leq), \subseteq)$ are both Heyting spaces, we know that X is compact and $PF(CU(X, \leq), \subseteq)$ is Hausdorff. Therefore, $g(X)$ is closed in $PF(CU(X, \leq), \subseteq)$. If g is not surjective, then there is a prime filter P of $CU(X, \leq)$ with $P \notin g(X)$.

As $PF(CU(X, \leq), \subseteq)$ is compact Hausdorff and $\{P\}$ and $g(X)$ are closed and disjoint, there are disjoint open sets U and W with $g(X) \subseteq U$ and $P \in W$. Since W is a union of clopen sets, there is a clopen set V with $P \in V$ and disjoint with $g(X)$.

As V is closed and $PF(CU(X, \leq), \subseteq)$ is compact, V is compact. We may assume $V = F_S \cap F'_T$ for some $S, T \in CU(X, \leq)$ because V is a finite union of such sets. Now, $g^{-1}(V) = \varnothing$ because V and $g(X)$ are disjoint, so

$$\varnothing = g^{-1}(V) = g^{-1}(F_S \cap F'_T) = S \cap T'.$$

The last equality is based on the proof of the continuity of g.

So $\varnothing = S \cap T'$, which implies $S \subseteq T$. But then $V = F_S \cap F'_T = \varnothing$, so $P \notin V$. This contradiction shows that g is surjective.

Lastly, we show that g is a p-morphism. We have to show that for every $x \in X$ and $P \in PF(CU(X, \leq), \subseteq)$ with $g(x) \subseteq P$, there is a $y \in X$ with $x \leq y$ and $g(y) = P$.

Let $x \in X$ and $P \in PF(CU(X, \leq), \subseteq)$ with $g(x) \subseteq P$. Because g is surjective, there is an element y of X with $P = g(y)$. Because $g(x) \subseteq g(y)$ and g is an order-embedding, we have $x \leq y$. □

Once again, we can conclude from these two theorems that if H and K are isomorphic Heyting algebras, then $PF(H)$ and $PF(K)$ are isomorphic Heyting spaces. Moreover, if X and Y are isomorphic Heyting spaces, then $CU(X)$ and $CU(Y)$ are isomorphic Heyting algebras.

13 Intuitionistic propositional logic

In classical propositional logic, any proposition is either true or false. However, in reality there are some statements of which we do not know yet whether they are true or false. A famous example of these open problems is the Riemann hypothesis. If we are only interested in our traditional notion of truth, this does not matter. There are situations, however, where it is of interest to be able to talk about whether a proposition has already been proven, rather than whether such a proof exists in the abstract sense. Intuitionistic logic provides a framework for this.

Intuitionistic logic has its roots in intuitionism, as formulated by L.E.J. Brouwer beginning in 1907. This is a philosophy of mathematics that believes that mathematics is an invention of the mind of mathematicians, rather than an objective truth waiting to be discovered. This means that a proposition A is true if it has been proven, and its negation $\neg A$ is true if it has been proven that A is not true. We see that the law of the excluded middle (either A or $\neg A$ is true for every statement A) cannot hold in the intuitionistic view: there are unproven statements for which neither the statement nor its negation are true *at this point in time*. Once a statement is proven or disproven, it will retain its truth value throughout time. This temporal aspect of truth values is a feature unique to intuitionism amongst the different philosophies of mathematics.

Another point in which intuitionism differs from the classical view of mathematics is the definition of the continuum. The intuitionistic continuum and the classical continuum are incomparable: some of the theorems of classical analysis are disproven intuitionistically, yet there are statements that can be proven in the intuitionistic continuum which do not hold in the classical continuum. As it is of no bearing on intuitionistic propositional logic (IPL), we will not go into detail regarding the intuitionistic continuum here. One example to show just how different the two notions of continuum are: in intuitionism, every total function from $\mathbb{R}$ to $\mathbb{R}$ is continuous.

The constructive definition of truth used by intuitionism means that the classical interpretation of the different connectives will not do, and we need a different interpretation. The Brouwer-Heyting-Kolmogorov-interpretation (BHK-interpretation) defines the different connectives informally.

A formal definition would have to specify exactly what a proof, construction and transformation entail. The different definitions we can use for this actually give rise to different systems of intuitionistic propositional logic, some but not all of which can be shown to be entirely included in classical propositional logic.

13.1 Definition. The BHK-interpretation for IPL

- $\perp$ is not provable.
- A proof of $A \wedge B$ consists of a proof of A and a proof of B.
- A proof of $A \vee B$ consists of a proof of A or a proof of B.
- A proof of $A \to B$ is a construction which transforms any proof of A into a proof of B.
- A proof of $\neg A$ is a construction that derives falsum from any possible proof of A.

We see that $\neg A$ is equivalent to $A \to \perp$. Unlike in classical propositional logic, none of the connectives $\vee, \wedge, \to, \neg$ are redundant.

Though it may seem at first glance that intuitionistic propositional logic has three truth values, true, false, and "undecided", Gödel proved that this is not the case. An intuitive way to see that is to take a statement that has not yet been proven or disproven. If we were to assign a third truth value, e.g. "undecided", and in a century the statement would be proven to be true, we would have to retract the "undecided" truth value. Since we want an assigned truth value to remain the same forever, at this moment (when it has neither been proven nor disproven) the statement cannot have a truth value at all.

A formal system for intuitionistic propositional logic was developed by A. Heyting in 1930. Since the intuitionistic philosophy sees logic as an expression of mathematics, rather than mathematics as an expression of logic, it is impossible, according to Brouwer, to completely formalise intuitionism. From now on we will only use the intuitionistic propositional logic that follows from the formal definition below. Remember that there are several possible interpretations of the connectives, and we use the BHK-interpretation here.

13.2 Definition. Formalisation of IPL. There are 9 axiom schemes:

- $A \wedge B \to A$
- $A \wedge B \to B$
- $A \to A \vee B$
- $B \to A \vee B$

- $A \to (B \to A)$
- $\bot \to A$ (*Ex falsum quodlibet*)
- $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
- $A \to (B \to A \vee B)$
- $(A \to C) \to ((B \to C) \to (A \vee B \to C))$

There is one rule of inference:

- If we have A and $A \to B$, we can infer B. (*Modus ponens*)

We see that formalised intuitionistic propositional logic has the same axiomatisation as classical propositional logic, in terms of connectives. The interpretation of those connectives, however, differs significantly from classical propositional logic. There are many ways to shuffle between axioms and rules of inference. Here we have chosen an axiomatisation in the Hilbert style, with a preference for axioms over inference rules. There are other axiomatisations that work equally well.

14 Looking at logic through algebra

We have found the correspondence between Boolean algebras and Stone spaces, and between Heyting algebras and Heyting spaces. So how does this apply to classical and intuitionistic propositional logic?

14.1 Boolean algebras and classical propositional logic

We have two approaches to classical propositional calculus: the semantic and the syntactic approach. In the semantic approach, every proposition is assigned a truth value, either true or false.

This truth value is not absolute, but is assigned by a **valuation**. This is a Boolean homomorphism from the space of propositions, $CPROP(A)$, with the operations as defined by a truth table (Table 1), to the two-valued Boolean algebra **2**. The set A is an alphabet of atomic propositions. Let $Val(CPROP(A))$ be the set of valuations from $CPROP(A)$ to **2**.

Propositions assigned the truth value 1 are said to be **semantically true** and propositions assigned the truth value 0 are said to be **semantically false**. If a proposition is always true (assigned the truth value 1 in all valuations), it is a **tautology**. To check whether a proposition is a tautology, we use truth tables.

In the syntactic approach we have a formal deduction system: a set of formulas, with some of those designated as axioms, and a finite set of deduction rules. A proposition is true if it can be proven, and is then called a **theorem**. A **proof** of a proposition is a finite list $(a_1, \ldots, a_n)$, where each a_i is either an

Table 1: Truth table of the different operations of CPROP(A).

a	b	a'	$a \vee b$	$a \wedge b$	$a \to b$
0	0	1	0	0	1
0	1	1	1	0	1
1	0	0	1	0	0
1	1	0	1	1	1

axiom, or it can be deduced from a_j, a_k with $j, k < i$. The last element of the list, a_n, is the theorem.

The two approaches give a different notion of truth: semantic truth involves drawing up a truth table and checking whether the proposition is a tautology. Syntactic truth, on the other hand, involves finding a proof. Ideally, we want both notions of truth to be equivalent. In classical propositional logic (CPL), we actually achieve this goal. Every theorem is a tautology. Thus, we cannot prove a statement whose truth depends on its interpretation, which would be disastrous in doing mathematics. We say that CPL is **sound**. Moreover, every tautology is a theorem. Therefore, everything that is always true, regardless of interpretation, can be proven, and we call CPL **adequate**.

When drawing up truth tables or proving propositions, we quickly find that certain propositions are **logically equivalent**: they have the same truth table or both can be proven when assuming the other. Let $\phi \sim \psi$ if ϕ and ψ are logically equivalent, and let $[\phi]$ be the logical equivalence class of ϕ. Then the **Lindenbaum algebra** $CLA(A) = CPROP(A)/_\sim$ is the set of logical equivalence classes.

We can define an order relation on $CLA(A)$ such that $CLA(A)$ is a lattice. The semantic definition is as follows: let $\phi, \psi \in CPROP(A)$. Then $[\phi] \leq [\psi]$ if, for every valuation in which ϕ is true, ψ is also true. Equivalently, we can syntactically define the order relation as: $[\phi] \leq [\psi]$ if ψ can be proven from ϕ. We will show that $CLA(A)$ with this order relation is Boolean.

14.1 Lemma. *Let $CLA(A)$ be the Lindenbaum algebra of $CPROP(A)$, with the order relation defined in the previous paragraph. Then $CLA(A)$ is a Boolean algebra with join $[\phi] \vee^* [\psi] = [\phi \vee \psi]$, meet $[\phi] \wedge^* [\psi] = [\phi \wedge \psi]$, and complement $[\phi]' = [\neg\phi]$. In addition, $1 = [\phi]$ and $0 = [\neg\phi]$ for any tautology ϕ.*

Proof. We will prove this semantically. That $CLA(A)$ is also Boolean with the syntactic definition of order follows from the fact that CPL is both sound and adequate.

We start by checking that the order relation is well-defined. Let $\phi, \psi, \chi, \omega \in CPROP(A)$ with $[\phi] = [\chi]$, $[\psi] = [\omega]$, and $[\phi] \leq [\psi]$. We want to prove that $[\chi] \leq [\omega]$.

Let V be a valuation in which χ is true. We want to prove that ω is also true in V. Because χ and ϕ are logically equivalent, ϕ must be true in V. From this and the assumption that $[\phi] \leq [\psi]$, it follows that ψ is true in V. As ψ and ω are logically equivalent, ω is true in V. Therefore, $\leq$ is well-defined.

Next, we show that $\leq$ is a partial order.

- Reflexivity: Let $\phi \in CPROP(A)$. It is clear that ϕ is true in every valuation in which ϕ is true. Therefore, $[\phi] \leq [\phi]$.
- Antisymmetry: Let $[\phi], [\psi] \in CLA(A)$, with $[\phi] \leq [\psi]$ and $[\psi] \leq [\phi]$. Then ϕ is true in every valuation where ψ is true, and vice versa. Therefore, ϕ and ψ are logically equivalent, so $[\phi] = [\psi]$.
- Transitivity: Let $[\phi], [\psi], [\chi] \in CLA(A)$ with $[\phi] \leq [\psi]$ and $[\psi] \leq [\chi]$. Let V be a valuation in which ϕ is true. By assumption, ψ is also true in V. Therefore, χ must be true in V and thus in every valuation in which ϕ is true. Hence, $[\phi] \leq [\chi]$.

Furthermore, we identify the top and bottom elements of $CLA(A)$. Let ϕ be a tautology, thus true in every valuation V. Its negation $\neg\phi$ is therefore false in every valuation. Now let ψ be an arbitrary element of $CPROP(A)$. In every valuation where ψ is true, ϕ is also true. Therefore, $[\psi] \leq [\phi]$. Also, since $\neg\psi$ is never true, we vacuously find that $[\neg\phi] \leq [\psi]$. Thus, $0 = [\neg\phi]$ and $1 = [\phi]$.

In addition, we need to show that the join, meet and complement of $CLA(A)$ are given by $[\phi] \vee^* [\psi] = [\phi \vee \psi], [\phi] \wedge^* [\psi] = [\phi \wedge \psi]$, and $[\phi]' = [\neg\phi]$.

We start by showing that the least upper bound of $\{[\phi], [\psi]\}$ is $[\phi \vee \psi]$. It is an upper bound, because if ϕ is true in a valuation V, then so is $\phi \vee \psi$. Analogously, if ψ is true in V, then $\phi \vee \psi$ is as well. Moreover, it is the least upper bound: let χ be an upper bound of $\{[\phi], [\psi]\}$. Then, ϕ is true for any valuation V in which χ is true. Therefore, $\phi \vee \psi$ is true for any valuation V in which χ is true. Hence, $[\phi \vee \psi] \leq [\chi]$.

Next, we show that the greatest lower bound of $\{[\phi], [\psi]\}$ is $[\phi \wedge \psi]$. It is a lower bound, because if $\phi \wedge \psi$ is true in a valuation V, both ϕ and ψ are also true. Now, let χ be a lower bound of $\{[\phi], [\psi]\}$. Then, if χ is true in V, so are ϕ and ψ. Hence, $\phi \wedge \psi$ is also true in V. Therefore, $[\chi] \leq [\phi \wedge \psi]$.

Finally, let $\phi \in CPROP(A)$. By definition of meet, $[\phi] \vee^* [\neg\phi] = [\phi \vee \neg\phi]$. Since $\neg\phi$ is true if and only if ϕ is false, $\phi \vee \neg\phi$ is a tautology. Therefore, $[\phi \vee \neg\phi] = 1$. By definition of join, $[\phi] \wedge^* [\neg\phi] = [\phi \wedge \neg\phi]$. However, $\phi \wedge \neg\phi$ is never true, so $[\phi \wedge \neg\phi] = 0$. Therefore, $[\phi]' = [\neg\phi]$.

It remains to prove that $CLA(A)$ is distributive. Let $[\phi], [\psi], [\chi] \in CLA(A)$. Using the definitions of join and meet, we find that

$$[\phi] \wedge^* ([\psi] \vee^* [\chi]) = ([\phi] \wedge^* [\psi]) \vee^* ([\phi] \wedge^* [\chi])$$
$$\text{if and only if } [\phi \wedge (\psi \vee \chi)] = [(\phi \wedge \psi) \vee (\phi \wedge \chi)].$$

It is straightforward to show that $\phi \wedge (\psi \vee \chi)$ and $(\phi \wedge \psi) \vee (\phi \wedge \chi)$ are logically equivalent, using the semantic definitions of $\vee$ and $\wedge$. Therefore, the distributive law is valid in $CLA(A)$, and we can conclude that $CLA(A)$ is Boolean. $\square$

Every valuation uniquely determines a homomorphism from $CLA(A)$ to $\mathbf{2}$ by sending $[\phi]$ to 0 if ϕ is sent to 0 and sending $[\phi]$ to 1 if ϕ is sent to 1.

We have shown that $PF(CPROP(A))$ is isomorphic to $Hom_2(CPROP(A))$. Therefore, it is also isomorphic to $Val(CPROP(A))$. The reworked version of Stone's representation theorem (Theorem 11.5) now tells us that there is an isomorphism $CLA(A) \to Cl(Val(CPROP(A)))$ given by

$$[\phi] \mapsto \{V \in Val(CPROP(A)) : V(\phi) = 1\}.$$

This isomorphism sends every proposition to the set of valuations for which that proposition is true.

14.2 Heyting algebras and intuitionistic propositional logic

As we saw, in intuitionistic propositional logic the law of the excluded middle does not hold. This means that we cannot use Boolean algebras like in the classical case: ϕ and $\neg\phi$ are not true complements of one another.

One of the consequences of not having a true complement for every element is that the logical operations $\vee$ (or), $\wedge$ (and), $\to$ (if ..., then ...), and $\neg$ (not) can not be defined in terms of each other. So instead of doing logic with only $\neg, \vee$, and $\wedge$ or only $\neg$ and $\to$, we need all four operations. This suggests we can use Heyting algebras to take the role in intuitionistic propositional logic similar to Boolean algebras in classical propositional logic. As an example, we can define and order the Lindenbaum algebra of a space of intuitionistic propositions $IPROP(A)$ analogously to the classical case. However, this Lindenbaum algebra is not a Boolean but a Heyting algebra, as we will prove next. To do so, we will use some terminology we encountered before in the classical case. Unless stated otherwise, this terminology is defined analogously in the intuitionistic case.

14.2 Lemma. *Let $IPROP(A)$ be a space of intuitionistic propositions, and let $ILA(A)$ be the Lindenbaum algebra of this space. Let $\phi, \psi \in IPROP(A)$. Then $[\phi] \leq [\psi]$ if, for every valuation in which ϕ is true, ψ is also true. An intuitionistic valuation is not a Boolean, but a Heyting homomorphism.*

Then $ILA(A)$ is a Heyting algebra with join $[\phi] \vee^* [\psi] = [\phi \vee \psi]$, meet $[\phi] \wedge^* [\psi] = [\phi \wedge \psi]$, and implication $[\phi] \to^* [\psi] = [\phi \to \psi]$. In addition, $1 = [\phi]$ and $0 = [\neg\phi]$ for any tautology ϕ.

Proof. That $\leq$ is well-defined and an order relation was proven in Lemma 14.1. Moreover, join and meet in $ILA(A)$ are $[\phi] \vee^* [\psi] = [\phi \vee \psi]$ and $[\phi] \wedge^* [\psi] = [\phi \wedge \psi]$, and $1 = [\phi]$ and $0 = [\neg\phi]$ for any tautology ϕ, according to that lemma. It remains to prove that $[\phi] \to^* [\psi] = [\phi \to \psi]$. We will use Definition 8.1 to prove that this definition of implication has the correct properties. Let $[\phi], [\psi], [\chi] \in ILA(A)$.

First, assume that $[\phi] \leq [\psi] \to^* [\chi]$. We can use the definition of implication to rewrite this to $[\phi] \leq [\psi \to \chi]$. Now, let V be a valuation in which $\psi \wedge \phi$ is true. Then ϕ is true in V, so per assumption $\psi \to \chi$ is true in V. Also, ψ is true

in V. We can now use Modus Ponens on ψ and $\psi \to \chi$ to find that χ is true in V. Hence, $[\psi \wedge \phi] \leq [\chi]$, and using the definition of $\wedge^*$, so is $[\psi] \wedge^* [\phi] \leq [\chi]$.

For the reverse direction, assume that $[\psi] \wedge^* [\phi] \leq [\chi]$. Then we can use the definition of $\wedge^*$ to rewrite this to $[\psi \wedge \phi] \leq [\chi]$. Let V be a valuation in which ϕ is true. We want to show that $\psi \to \chi$ is true in V.

If ψ is true in V, then $\psi \wedge \phi$ is also true in V. Per assumption χ is then true in V. So, if ψ, then χ is true in V, or equivalently, $\psi \to \chi$ is true in V. Therefore, $[\phi] \leq [\psi \to \chi]$. Per definition of implication, we find that $[\phi] \leq [\psi] \to^* [\chi]$. $\square$

In the previous subsection, we saw that the clopen sets of classical valuations of $CPROP(A)$ are isomorphic to the classical Lindenbaum algebra of $CPROP(A)$ through duality. As the classical Lindenbaum algebra of $CPROP(A)$ is Boolean, its dual is the set of valuations on $CPROP(A)$.

Moreover, we found a one-to-one correspondence between valuations and 2-valued homomorphisms. That such a relatively complex result as Stone duality can be achieved with something as simple as 2-valued homomorphisms, is due to the special status of the Boolean algebra **2**.

It proves to be that every non-degenerate Boolean algebra has **2** as a subalgebra. This special status is one of the main things that create the difference between Boolean and Heyting algebras in logic. For Heyting algebras, there is no single algebra which is the subalgebra of every non-degenerate Heyting algebra. Instead every Heyting algebra has a finite well-connected Heyting algebra as a subalgebra, where a Heyting algebra is **well-connected** if $a \vee b = 1$ implies that $a = 1$ or $b = 1$. Thus, all finite well-connected Heyting algebras together take the role fulfilled by **2** in the Boolean case.

That the Boolean instance is a special case of the Heyting one, is reinforced by the fact that **2** is the only well-connected Boolean algebra, up to isomorphism. To see this, consider a Boolean algebra B that is not isomorphic to **2**. Then there is an element $b \in B$ with $0 \neq b \neq 1$, which implies that its complement cannot be either 0 or 1. However, the properties of the complement imply that $b \vee b' = 1$. Therefore, B is not well-connected.

The lack of a single generating algebra implies that the dual space of a Heyting algebra cannot be defined in terms of valuations. As the intuitionistic Lindenbaum algebra of a certain set of propositions is a Heyting algebra, its dual space cannot be expressed in terms of valuations either.

The problem here is that every valuation would have to be a homomorphism to the same (finite) Heyting algebra. What we do know because of duality, is that we can view every prime filter as a homomorphism into a (not necessarily finite) well-connected Heyting algebra. So every prime filter can be linked to a valuation, although it is differently-valued for every prime filter. In contrast, as **2** is the only well-connected Boolean algebra, all Boolean valuations are 2-valued, and we see that the space of prime filters and that of (2-valued) valuations is the same.

References

[1] B. A. Davey and H. A. Priestley. *Introduction to Lattices and Order*. Cambridge University Press, second edition, 2002.

[2] M. van Atten. The development of intuitionistic logic. In *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, winter 2016 edition, 2016.

[3] S. Givant and P. Halmos. *Introduction to Boolean Algebras*. Springer, 2009.

[4] Š. Bilová. Lattice theory - its birth and life. In *Mathematics throughout the ages*. Prometheus, 2001.

[5] P. J. Morandi. Dualities in lattice theory. `http://sierra.nmsu.edu/morandi/notes/Duality.pdf`, 2009.

[6] N. Bezhanishvili. *Lattices of intermediate and cylindric modal logics*. PhD thesis, Universiteit van Amsterdam, 2006.

[7] R. Iemhoff. Intuitionism in the philosophy of mathematics. In *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, winter 2016 edition, 2016.

[8] J. Moschovakis. Intuitionistic logic. In *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, spring 2015 edition, 2015.

[9] N. P. Landsman. Propositielogica. Lecture notes for the course Logic at Radboud University, 2017.

[10] A. Chagrov and M. Zakharyaschev. *Modal Logic*. Oxford University Press, 1997.